HP WebInspect Enterprise

for the Windows® operating system

Software Version: 10.10

User Guide

Document Release Date: September 2013
Software Release Date: September 2013

Legal Notices

Copyright Notice

Copyright 2013 Hewlett-Packard Development Company, L.P.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Disclaimer of Warranty

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Other Acknowledgements

This product contains the following Apache open source component: Log4Net (**http://logging.apache.org/log4net/**). This component was modified from its original form and incorporated into this software product. To learn more about the apache software license, please visit **http://www.apache.org/licenses/LICENSE-2.0**.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, visit the following URL:

http://h20230.www2.hp.com/selfsolve/manuals

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

For information or assistance regarding WebInspect Enterprise, contact customer support.

You can open a support case for WebInspect Enterprise via e-mail, online, or by telephone. These options are designed to provide easier access and improved customer satisfaction.

E-Mail (Preferred Method)

Send an e-mail to fortifytechsupport@hp.com describing your issue. Please include the product name so we can help you faster.

Online (Fortify Support Portal)

Access your account at the Fortify Support Portal at **https://support.fortify.com**

If you do not have an account, you forgot your username or password, or you need any assistance regarding your account, please contact us at fortifytechsupport@hp.com or (650) 735-2215.

Telephone

Call our automated processing service at (650) 735-2215. Please clearly provide your name, telephone number, the name of the product, and a brief description of the issue.

You can access the HP Application Security Community containing customer forum and blogs at:

http://h30499.www3.hp.com/t5/Application-Security-Community/ct-p/sws-AS

You can also visit the HP software support Web site at:

http://support.openview.hp.com/

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides an efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Welcome

Introduction

WebInspect Enterprise is a distributed network of HP scanners controlled by a system manager with a centralized database. WebInspect Enterprise must be integrated with HP Fortify Software Security Center (SSC) and it provides SSC with information detected through dynamic scans of Web sites and Web services.

This innovative architecture allows you to:

- Conduct a large number of automated security scans using any number of sensors in various locations to scan Web applications and Web services.
- Manage large or small deployments of HP scanners across your organization controlling product updates, scan policies, scan permissions, tools usage and scan results, all centrally from the WebInspect Enterprise Administrative Console.
- Detect, track, and manage your new and existing Web applications and monitor all activity associated with them.
- Independently schedule scans and blackout periods, manually launch scans, and update repository information by using HP scanners or the WebInspect Enterprise Administrative Console.
- Limit exposure to enterprise-sensitive components and data by using centrally defined roles for users.
- Obtain an accurate snapshot of the organization's risk through a centralized database of scan results.
- Facilitate integration with third-party products and deployment of customized Web-based front ends using the WebServices application programming interface (API).

WebInspect Enterprise comprises the following:

- The WebInspect Enterprise Web Console, a browser-based interface designed for non-administrative functions.
- The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console.
- The Guided Scan client application, which is downloaded and installed the first time you launch it in WebInspect Enterprise or Software Security Center.
- Scanners. Two types of scanners are supported:
  - Sensor - This is the WebInspect application when connected to WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans with no direct user interaction through its graphical user interface. It receives its instructions exclusively from the configurable connection to a WebInspect Enterprise Manager.
  - Client - A client is any HP scanner that connects to WebInspect Enterprise to receive license, permissions, updates or scan data, and which also presents a user interface through which scans may be conducted. WebInspect Enterprise controls permissions for a client and also provides the policies used by clients. A client can be configured to upload scan results to WebInspect Enterprise automatically at the completion of the scan or only when specifically instructed by the user.
- Microsoft SQL Server.

For information about system requirements, see the *HP WebInspect Enterprise System Requirements* document. For information about installing or upgrading WebInspect Enterprise, see the *HP WebInspect Enterprise Installation Guide*. You can access these documents from the **Resources** link on the Web Console.

2 Preparing Your System for Audit

Introduction

HP scanners are aggressive Web application analyzers that rigorously inspect your entire Web site for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which scanning policy you apply and the options you select, it can affect server and application throughput and efficiency. When using the most aggressive policies, you should perform this analysis in a controlled environment while monitoring your servers.

Helpful Hints

If your system generates e-mail messages in response to user-submitted forms, you might want to consider disabling your mail server. Alternatively, you could redirect all e-mail messages to a queue and then, following the audit, manually review and delete those messages that were generated in response to forms submitted by HP scanners.

If for any reason you do not want to audit certain directories, you must specify those directories using the Excluded URLs settings of HP scanners.

During an audit of any type, HP scanners submit a large number of requests, many of which have “invalid” parameters. On slower systems, the volume of HTTP requests may degrade or deny access to the system by other users. Additionally, if you are using an intrusion detection system, it will identify numerous illegal access attempts.

Finally, HP scanners test for certain vulnerabilities by attempting to upload files to your server. If your server allows this, HP scanners will record this susceptibility and attempt to delete the uploaded file. Sometimes, however, the server will not allow a file to be deleted. For this reason, part of your post-scan maintenance should include searching for and deleting files whose name begins with “CreatedByHP.”

Using Web Forms

Most Web applications contain HTML or JavaScript forms composed of special elements called input controls (text boxes, buttons, drop-down lists, etc.). Users generally “complete” a form by modifying its input controls (such as entering text or checking boxes) before submitting the form to an agent for processing. Usually, this processing will lead the user to another page or section of the application. For example, after completing a logon form, the user will proceed to the application’s beginning page.

If HP scanners are to navigate through all possible links in the application, they must be able to submit appropriate data for each form. They do so by using a file containing the names of input controls and the associated values that need to be submitted during a scan of your Web site. Each HP scanner includes a

default Web form file containing sample name/value pairs. You can use the Web Form Editor (accessible through the **Tools** menu on the WebInspect Enterprise Administrative Console) to create your own file containing Web form values.

If you select the option to submit forms during a crawl of your site, HP scanners will complete and submit all forms encountered. Although this enables HP scanners to navigate seamlessly through your application, it may also produce the following consequences:

- If, when a user normally submits a form, the application creates and sends e-mail messages or bulletin board postings (to a product support or sales group, for example), HP scanners will also generate these messages as part of their probe.
- If your system writes records to a back-end server (database, LDAP, etc.) based on forms submitted by clients, then forms submitted by HP scanners will create spurious records. Some users, before auditing their production system, create a copy of their database and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit, searching for and deleting records that contain one or more of the form values used by HP scanners. You can determine these values by opening the Web Form Editor.

During the audit phase of a scan, HP scanners resubmit forms numerous times, manipulating every possible parameter to reveal problems in the applications. This will greatly increase the number of messages and database records created.

3 WebInspect Enterprise Administrative Console

Introduction

WebInspect Enterprise presents the following separate user interfaces:

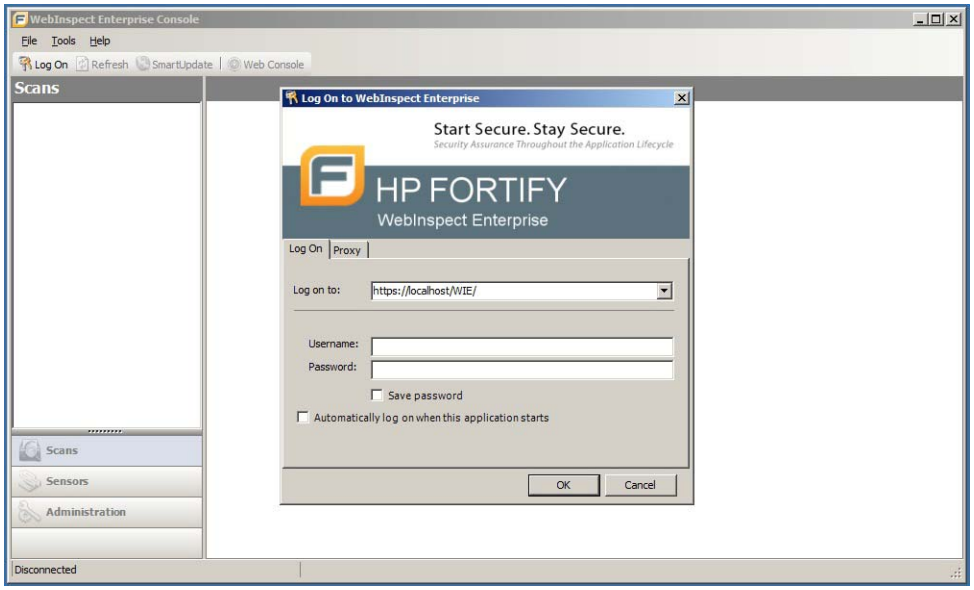
- The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console. It is used for administrative and security functions, as described in this chapter.
- The WebInspect Enterprise Web Console, a browser-based application used for running and managing scans. See Chapter 4, WebInspect Enterprise Web Console.
- Guided Scan, the preferred alternative to the standard Web Site scan. Guided Scan directs you through the best steps to configure a scan that is tailored to your application. The first time you launch Guided Scan in WebInspect Enterprise or Software Security Center, the Guided Scan client application, which includes its own Help system, is downloaded and installed on your local computer. See Chapter 5, Guided Scan.

Logging On

To log on to the Administrative Console:

1. Click **Start** → **HP WebInspect Enterprise 10.10 Console**.

   The *Log On to WebInspect Enterprise* window appears.



This window does not appear if you previously selected the option **Automatically log on when this application starts**.

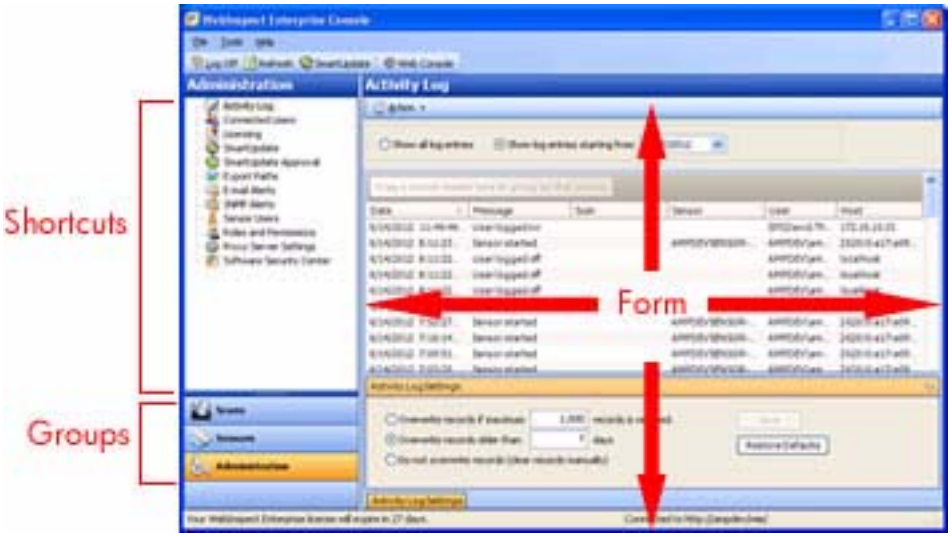
2. Using the **Log on to** list, enter or select the URL of the WebInspect Enterprise manager.
3. Enter the **Username** and **Password** for an account that has permission to access the Administrative Console. This user is permitted to perform all restricted functions.
4. Select the option **Save password** as desired.
5. Select the option **Automatically log on when this application starts** if you want administrators not to have to enter login credentials in the future.
6. To go through a proxy server to reach the WebInspect Enterprise manager:
   a. Click the **Proxy** tab.
   b. Select one of the following:
      – **Use the Internet Explorer proxy** (to use the proxy server specified in **Tools** → **Internet Options** → **Connections** → **LAN Settings**).
      – **Use the proxy below**, and then provide the proxy server's IP address and port number.
   c. Provide a valid **Username** and **Password**.
7. Click **OK**.

If you see a message indicating that the server refused the request, you may have entered your user name and password incorrectly, or your account has not been assigned to a role.

User Interface

The WebInspect Enterprise Administrative Console user interface comprises the following main areas:

- Menu bar
- Toolbar
- Shortcut pane
- Groups pane
- Form



The buttons in the Groups pane represent groups of WebInspect Enterprise functions.

Click a group button to expose associated shortcuts.

Click a shortcut to display a form containing related information or controls associated with the selected function.

In the preceding illustration, the user selected the **Administration** group and then clicked the **Activity Log** shortcut to display a form containing a time-stamped history of WebInspect Enterprise Manager activities.

The Group pane contains the following buttons:

Button	Associated Shortcuts
Scans	Scan Queue Scan Policies
Sensors	Sensors
Administration	Activity Log Connected Users Licensing Smart Update Smart Update Approval Export Paths E-Mail Alerts SNMP Alerts Sensor Users Roles and Permissions Proxy Server Settings Software Security Center

For forms containing lists (grids), you can initiate commands related to a list or to the individual objects on a list. Simply select an object and then choose a command from the **Action** menu (or from the shortcut menu that appears when you right-click an object). The availability of commands depends on the status of the selected object and the permissions granted to you by your assigned role (although system administrators have no restrictions on the functions they can perform).

The following table describes the menus and toolbar buttons.

Menu / Button	Description
File	Allows you to: • Log off the application. • Refresh the display. • Import to SSC a set of projects that were sites discovered by the Web Discovery tool. (This option is also available under the **Action** menu when the Software Security Center shortcut is selected for the Administration group; see Importing Projects Converted from Web Discoveries into SSC on page 49). • Exit the application.
Tools	Allows you to: • Manually initiate a Smart Update. • Configure options for the console. • Launch a tool included in the HP toolkit.
Help	Allows you to: • Open this Help file. • Open your e-mail application to send an e-mail to HP Support. • Open the *About WebInspect Enterprise Console* dialog.
Log On/Off	Log on to or log off from the console application.
Refresh	Refresh the display.
Smart Update	Manually initiate a Smart Update call to the HP server.
Web Console	Log on to the WebInspect Enterprise Web Console.

Scans Group

The **Scans** group contains the following shortcuts:

- Scan Queue
- Scan Policies

Scan Queue

For each scan that is running or waiting to run, this form displays (by default) the name assigned to the scan, the scan's priority, the date and time the scan request was created, the sensor conducting the scan, the scan's status, and the organization and group.

Select a scan request and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a request. The availability of commands depends on the status of the selected scan and on the permissions granted to you by your assigned role. To learn more about roles and permissions, see Roles and Permissions on page 36.

The commands are:

Command	Definition
Stop	Terminate the scan. The results, although incomplete, are available for inspection.
Suspend	Halt the scanning process. You can resume the scan at the point at which it was interrupted.
Resume	Continue the scanning process following a suspension.
Delete	Remove the scan from the WebInspect Enterprise database.
Column Setting	Open the *Column Setting* window, allowing you to specify which columns should appear in the list.

Scan Policies

This form lists all policies configured in your environment. See Appendix A, Policies, for a description of each policy and its components.

Select a policy and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a policy. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Edit	Open the Policy Manager, allowing you to view and modify the selected policy. You must install Microsoft SQL Server Express before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager. The Edit command is available only for custom (non-system) policies.
View	Open the Policy Manager, allowing you to view the selected policy. You must install Microsoft SQL Server Express before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager. The View command is available only for system policies.
Copy	Create a copy of the selected policy. After you rename the policy, the Policy Manager opens and loads the selected policy, allowing you to edit it. Once edited and saved, the policy is added to the list of scan policies.
Delete	Delete the selected policy from the repository. Prepackaged policies cannot be deleted.
Rename	Change the name of a custom policy, Prepackaged policies cannot be renamed (except when copied).
*Import	Import a policy from a standalone HP scanner.
*Export	Export a policy to a standalone HP scanner. Prepackaged policies cannot be exported.

* All sensors in the WebInspect Enterprise system access common policies from the repository. The import and export of policies is useful only if you run the HP scanner independent of the WebInspect Enterprise system and want to incorporate the results of that scan into the WebInspect Enterprise system.

Sensors Group

The Sensors group has one shortcut: Sensors.

A sensor is defined as WebInspect (and only WebInspect) when it is connected to WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans and it provides no user interface.

This form displays the name, host name, status, and version of each sensor in the system. It also displays a status message for each sensor, indicating the result of the most recent action attempted.

Note: If you do not see a list of installed sensors, you must install the Microsoft .NET Framework version 4.0.

Select a sensor and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click the sensor. The availability of commands depends on the permissions granted to you by your assigned role and on the status of the selected sensor.

The commands are:

Command	Definition
Edit Sensor Details	Modify the name, location, and description.
Stop Scan	Abort the scan. The job cannot be resumed.
Suspend Scan	Interrupt the scan. The scan can then be manually resumed later.
Pause Sensor	Temporarily halt the sensor. Note: This feature is a transient state held in memory on the sensor; it will not be remembered if the sensor service is ever restarted. For a long-term status, disable the sensor.
Continue Sensor	Enable the sensor after pausing. If the sensor was running a scan when paused, it will resume the scan automatically.
Enable/Disable	Turn the sensor on or off. You must be a member of the security administrator's group to enable a new sensor.
Rename Sensor	Change the sensor name.
Migrate Sensor	Reassign all schedules, pending scans, etc., from one sensor to another. Used primarily when installing a replacement sensor.
Delete Sensor	Disassociate the sensor from the WebInspect Enterprise system. Note: To enable this command, you must stop the WebInspect Sensor service (**Start** → **Control Panel** → **Administrative Tools** → **Services**), taking the sensor offline.

Administration Group

The Administration group has the following shortcuts:

- Activity Log
- Connected Users
- Licensing
- Smart Update
- Smart Update Approval
- Export Paths
- E-Mail Alerts
- SNMP Alerts
- Sensor Users
- Roles and Permissions
- Proxy Server Settings
- Software Security Center

Activity Log

The Activity Log lists each WebInspect Enterprise activity. Each item includes (by default):

- The time and date the event occurred
- A message indicating the event or activity
- For scan-related events, the URL or IP address or the job name associated with this activity
- The sensor associated with this activity
- The name of the user
- The IP address of the workstation

You can display all entries in the Activity Log or restrict the listing to those activities that occurred on or after a specific date.

To limit the size of the Activity Log, click **Activity Log Settings** (at the bottom of the form).

Actions

You can select a command from the **Action** menu or from the shortcut menu that appears when you right-click an item in the list. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Export Activity Log to [TSV / CSV / XML]	Save the activity log to a text file using either a tab-separated, comma-separated, or XML format.
Clear Activity Log	Delete all entries in the activity log.

Command	Definition
Copy Message(s) to Clipboard	Copy the text in all columns of all selected list entries.
Column Setting	Open the *Column Setting* window, allowing you to specify which columns should appear in the list.

Connected Users

This form lists each user who is currently logged in to the WebInspect Enterprise system. Each item includes:

- Application Type, such as WebInspect Enterprise or WebInspect
- Application Subtype, such as Console or Console-Web
- Application Version
- The user's name
- The user's IP Address
- The time and date when the user connected to the system
- Status
- Message

A summary at the bottom of the panel shows the total number of user licenses in use, the total number of available user licenses, and the timeout period (which you can edit).

Actions

You can select a command from the **Action** menu. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Release User License	Intended for use with licenses that permit multiple users. Disassociate the selected user from the license, allowing another user to occupy that position.
Column Setting	Open the *Column Setting* window, allowing you to specify which columns should appear in the list.

Licensing

This form lists the license information and activation ID issued by HP for the operation of WebInspect Enterprise.

- Activation ID: The unique identifier for the license issued by HP.
- Update: If you upgrade from a trial version or if you otherwise modify the conditions of your license, click this button to update your license.
- User Information: Information about the person to whom the license is granted.
- License Information
  - Licensed IP or Host Ranges: The IP addresses or hosts to which scans are restricted.

  - Bypass DNS: Indicates if the application is allowed to bypass a domain name server.
  - Valid To: The ending date of the period for which the license is valid.
  - Total available sensor licenses: The maximum number of sensors that may be connected to WebInspect Enterprise.
  - Total Scan Count: The maximum number of scans that may be conducted.
  - Maintenance End Date. The date on which the maintenance contract terminates.
- License Usage Information
  - Available Scan Count: Remaining number of scans allowed.
  - Total in use sensor licenses: Number of licensed sensors in use.
  - Total in use concurrent user licenses: Number of concurrent licensed sensors in use.

Smart Update

HP engineers uncover new vulnerabilities almost every day. They develop attack agents to search for these malicious threats and then update the HP corporate database so that you will always be on the leading edge of Web application security.

Use Smart Update to obtain HP's latest adaptive agents, as well as vulnerability and policy information. Each time you log in to the WebInspect Enterprise Administrative Console, it contacts the WebInspect Enterprise manager and downloads any available console binary updates.

If your WebInspect Enterprise manager cannot connect to the Internet, contact HP Support to obtain an offline SmartUpdate utility.

The Smart Update form lists each update package downloaded from HP. Each item includes (by default):

- The time and date the download began.
- The time and date the download ended.
- The status of the event.
- If applicable, an error message describing any problem that occurred.

Select an entry in the SmartUpdate History list to display details about that event.

This form also lists any updates that have been scheduled. Each item includes (by default):

- The name assigned to the update.
- The frequency with which it is scheduled to occur (if it is a recurring event).
- The date and time it last occurred (for recurring events only).
- The date and time it is scheduled to occur.

Actions

You can select a command from the **Action** menu. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Clear Completed Updates	Delete the list of Smart Updates that have been completed.
Add Schedule	Open the *Smart Update Settings* window, allowing you to schedule a Smart Update.
Edit Schedule	Open the *Smart Update Settings* window, allowing you to modify the settings for the scheduled Smart Update selected in the Smart Update Schedules list.
Delete Schedule	Delete the Smart Updates selected in the Smart Update Schedules list.
History Column Setting	Open the *Column Setting* window, allowing you to specify which columns should appear in the Smart Update History section.
Schedule Column Setting	Open the *Column Setting* window, allowing you to specify which columns should appear in the SmartUpdate Schedules section.

If you need to use a proxy server to communicate with the HP Smart Update database, select the **Proxy Server Settings** shortcut in the **Administration** group.

Note that scans cannot start while sensors are receiving a Smart Update. Scheduled scans stay in "pending" state until Smart Update completes. This prevents sensors from picking up partial Smart Updates when they update their local SecureBase from WebInspect Enterprise.

Smart Update Approval

This form lists all binary updates that have been received for WebInspect Enterprise's client products, such as WebInspect and sensors. None of these applications can be updated until an administrator specifically approves the update. Items in the list can be grouped according to product, importance, or approval status.

The possible approval statuses are:

- **Not Approved**—Update has not yet been reviewed by the administrator.
- **Approved**—Update has been approved by the administrator and is available to clients.
- **Decline**—Update has been withheld by the administrator and is not available to clients.

Once administrative approval is obtained, the update becomes available to client applications. For WebInspect, the Smart Update utility displays a window notifying users that an update is available. Users may either accept or reject the update. Updates for sensors (which do not have a user interface) are controlled by the WebInspect Enterprise Manager. If approved updates are available, a sensor will be required to download and apply the update before a scan can be assigned.

Typically, administrators prefer to update a single application instance and test it before performing a system-wide installation. This can be done by manually installing the updates on a test system. Sensor scans can be tested on a non-approved version of WebInspect by selecting the specific sensor when configuring the scan in WebInspect Enterprise.

Ordinarily, sensors that are running a non-approved version of WebInspect (such as a special build developed for a specific customer) will not be selected to run a scan when you choose the **Use Any Available** option. You can remove that restriction, however, by selecting the non-approved sensor on the Sensors form and then selecting the option **Can participate in "Any Available" sensor scans**. Sensors that are newer than the latest approved version are then eligible to be selected.

Actions

You can select a command from the **Action** menu or from the shortcut menu that appears when you right-click an item in the list. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Approve	Make the binary update available to clients.
Decline	Withhold distribution of the binary update.

Note that scans cannot start while sensors are receiving a Smart Update. Scheduled scans stay in "pending" state until Smart Update completes. This prevents sensors from picking up partial Smart Updates when they update their local SecureBase from WebInspect Enterprise.

Export Paths

This form displays a list of destinations (paths) that may be used for saving scan results. WebInspect Enterprise uses these paths to populate the drop-down list from which Web Console users select a location for storing the data.

Actions

Select a path and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an export path. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Add	Open the *Export Path Settings* window, allowing you to specify export paths.
Edit	Open the *Export Path Settings* window, allowing you to modify export paths.
Delete	Remove the path from the form.

Adding or Editing Export Paths

You can designate destinations (paths) that may be used for saving scan results.

1. Click the **Administration** group.
2. Select the **Export Paths** shortcut.
3. To add a path:
   a. Select **Add** from the **Action** menu
   - or -
   Right-click in the **Export Paths** list and select **Add** from the shortcut menu.

b On the *Export Path Settings* dialog, enter a path using the Universal Naming Convention (or click the **Browse** button and select a folder).

   If you browse for a folder and select a local (rather than network) folder, the selection refers to the hard drive of the machine on which the WebInspect Enterprise manager is installed. Also note that the WebInspect Enterprise manager must have access to any location you designate as an export path.

c Click **OK**.

4 To edit a path:

a Select an entry in the **Export Paths** list.

b Select **Edit** from the **Action** menu
   - or -
   Right-click an entry in the **Export Paths** list and select **Edit** from the shortcut menu.

c Modify the path using the Universal Naming Convention (or click the **Browse** button and select a folder).

   If you browse for a folder and select a local (rather than network) folder, the selection refers to the hard drive of the machine on which the WebInspect Enterprise manager is installed. Also note that the WebInspect Enterprise manager must have access to any location you designate as an export path.

d Click **OK**.

5 To delete a path:

a Select an entry in the **Export Paths** list.

b Select **Delete** from the **Action** menu
   - or -
   Right-click an entry in the **Export Paths** list and select **Delete** from the shortcut menu.

You cannot remove an export path that is currently being used or is associated with a scheduled scan.

E-Mail Alerts

You can force WebInspect Enterprise to send an e-mail message whenever certain events occur. Such a message is called an e-mail alert.

This form lists all e-mail alerts configured for the system. Each item includes:

- The name of the alert
- The address of the e-mail recipient
- The IP addresses of scanned sites that may elicit an alert
- The events or actions about which the recipient is to be notified
- The organization
- The group

SMTP Settings

If necessary, click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings if you plan to send e-mail notifications for specific WebInspect Enterprise events.

SMTP Server—The name of the server used for outgoing e-mail.

SMTP Port—The numbered port used for outgoing e-mail.

Sender—The text that will be appear in the "From" field of the e-mail. It need not be a valid e-mail account, but it must be in the format text@text.text , where text is any text you care to enter.

Use SSL—Select this check box to use Secure Sockets Layer (SSL) protocol.

Authentication—If your server requires authentication, select **Basic** or **NTLM**, and then provide a user name and password.

Actions

Select an alert and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an alert. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Add	Specify settings for an alert.
Edit	Modify settings for an alert.
Delete	Remove the alert from the form.

Adding or Editing E-Mail Alerts

You can instruct the WebInspect Enterprise manager to send an e-mail message to someone whenever certain events occur.

1. Click the Administration group.
2. Select the E-mail Alerts shortcut.

   The *E-mail Alerts* form lists all alerts configured for the system.
3. To add an alert:
   a. Select **Add** from the **Action** menu
   - or -
   Right-click in the **E-mail Alerts** list and select **Add** from the shortcut menu.
   b. On the *E-Mail Alert Settings* dialog, enter a name for the alert.
   c. Select either **System**, **Organization**, or **Group**.
   d. If you did not select **System**, choose a group or organization from the list.
   e. In the **Recipient e-mail address** box, enter the e-mail address of the person who should receive the alert. To specify multiple recipients, insert a semicolon between e-mail addresses.
   f. If the alert should be sent only when selected actions occur related to a specific IP address or range of IP addresses, enter the address or range. For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254). Separate multiple addresses or ranges with a semicolon. Enter an asterisk (*) to allow alerts for all IP addresses.
   g. Select one or more actions that will trigger the alert.
   h. Click **OK**.
4. To edit an alert:
   a. Select an entry in the **E-mail Alerts** list.

b Select **Edit** from the **Action** menu.
- or -
Right-click an entry in the **E-mail Alerts** list and select **Edit** from the shortcut menu.

5 To delete an alert:

a Select an entry in the **E-mail Alerts** list.

b Select **Delete** from the **Action** menu
- or -
Right-click an entry in the E**-mail Alerts** list and select **Delete** from the shortcut menu.

SNMP Alerts

You can force WebInspect Enterprise to send a Simple Network Management Protocol (SNMP) message whenever certain events occur. Such a message is called an SNMP alert.

This form lists all SNMP alerts configured for the system. Each item includes:

- The name of the alert
- The IP address of the SNMP alert recipient
- The action or event that will trigger the alert
- The organization
- The group

SNMP Settings

If necessary, click **SNMP Settings** (at the bottom of the form) to configure SNMP settings if you plan to send SNMP notifications for specific WebInspect Enterprise events.

SNMP Host—The IP address of the server that will receive the alert and forward it to the intended recipient.

SNMP Port—The port number for SNMP alerts on the SNMP host.

Community—An SNMP community is a text string that acts as a password for authenticating messages sent between the management station (the SNMP manager) and the device (the SNMP agent). There are typically two types of community names:

- A read-only community name that allows queries of the agent.
- A read-write community name that allows an NMS to perform set operations.

Actions

Select an alert and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an alert. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Add	Specify settings for an alert.
Edit	Modify settings for an alert.
Delete	Remove the alert from the form.

Adding or Editing SNMP Alerts

You can instruct the WebInspect Enterprise manager to send an SNMP message whenever certain events occur.

1. Click the **Administration** group.
2. Select the **SNMP Alerts** shortcut.

   The SNMP Alerts form lists all alerts configured for the system.
3. To add an alert:
   a. Select **Add** from the **Action** menu
   - or -
   Right-click in the **SNMP Alerts** list and select **Add** from the shortcut menu.
   b. Enter a name for this alert.
   c. Select **System**, **Organization**, or **Security Group**.
   d. If you did not select **System**, choose a group or organization from the list.
   e. Enter the IP address of the SNMP-compliant device that should receive the alert. You can specify multiple addresses or a range of addresses. For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254). Separate multiple addresses or ranges with a semicolon.

      Enter an asterisk (*) to allow alerts for all IP addresses.
   f. Select one or more actions that will trigger the alert.
   g. Click **OK**.
4. To edit an alert:
   a. Select an entry in the **SNMP Alerts** list.
   b. Select **Edit** from the **Action** menu.
   - or -
   Right-click an entry in the **SNMP Alerts** list and select **Edit** from the shortcut menu.
   c. If necessary, modify the name of this alert.
   d. Modify the IP address of the SNMP-compliant device that should receive the alert. You can specify multiple addresses or a range of addresses. For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254). Separate multiple addresses or ranges with a semicolon.

      Enter an asterisk (*) to allow alerts for all IP addresses.
   e. Select or deselect one or more actions that will trigger the alert.
5. To delete an alert:
   a. Select an entry in the **SNMP Alerts** list.
   b. Select **Delete** from the **Action** menu.
   - or -
   Right-click an entry in the **SNMP Alerts** list and select **Delete** from the shortcut menu.

Sensor Users

This form lists all WebInspect Enterprise sensor accounts, which exist to run scans on behalf of WebInspect Enterprise users.

You must create at least one Windows user account and assign it to the sensor service.

To add an account:

1 Click the **Administration** group.

2 Select the **Sensor Users** shortcut.

3 Click **Add**.

4 Enter the account assigned to the sensor.

5 Click **OK**.

To remove an account:

1 Select an account from the list.

2 Click **Remove**.

Roles and Permissions

This form allows you to assign administrators for three security levels (system, organization, and group). Administrators can then define roles, assign users to roles, and configure other security-related parameters. For an overview of the WebInspect Enterprise hierarchical structure, see Assign Administrators and Create Roles on page 50.

Roles

A role is simply a named collection of permissions. You can allow other users to access the WebInspect Enterprise system and limit the functions they are allowed to perform by assigning them to a role. Also, a single user may be a member of more than one role.

The roles for each security level (system, organization, and group) contain a different set of permission categories. Each category contains multiple permissions, such as Can Create, Can View, Can Update, Can Delete, etc.

System Roles

System roles contain the following activity categories:

- Activity Log
- Licensing
- SmartUpdate
- E-mail Alerts
- SNMP Alerts
- Export Paths
- Sensors
- Policies

Organization Roles

Organization roles contain the following activity and object categories:

- Blackouts
- Policies

- E-mail Alerts
- SNMP Alerts

Group Roles

Group roles contain the following activity and object categories:

- Project Versions
- Scans
- Scan Templates
- Scheduled Scans
- E-mail Alerts
- SNMP Alerts
- Blackouts
- HP Toolkit

Select an entry in the Security Group Hierarchy tree (WebInspect Enterprise System, an organization, or a group) and then provide the information requested on each of the related tabs that appear in the Permissions section on the right-hand pane.

Actions

You can also choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an object in the Security Group Hierarchy tree. The commands are:

Command	Definition
Add Organization	Create an organization.
Rename Organization	Change the name of an organization.
Remove Organization	Delete an organization.
Add Group	Create a group.
Rename Group	Change the name of a group.
Remove Group	Delete a group
Add User(s) to Roles	Add multiple users to roles. See Add Users to Roles on page 52 for more information.
Role Membership and Removal	Display roles assigned to a selected user or group, and allows you to remove a user or group from a role. See Role Membership and Removal for more information.

Role Membership and Removal

The Role Membership and Removal form displays the roles to which a selected user or group is assigned.

1. Click the **Administration** group.
2. Select the **Roles and Permissions** shortcut.
3. Click **Action** and select **Role Membership and Removal**.

4 Type a user or group name, or click **Browse** to select a user or group.

5 Click **Search**.

If you entered your own user name or the name of a group of which you are a member, WebInspect Enterprise displays all the roles to which you are assigned.

If you enter a user name or group name other than your own, you must be an administrator to see their roles. WebInspect Enterprise displays the roles to which the specified user or group is assigned, but only for those organizations and groups of which you are an administrator.

6 To remove a user or group from a role, select the user or group and click **Remove**.

System Roles and Permissions

When you select **WebInspect Enterprise System** from the Security Group Hierarchy pane, the following tabs appear in the System Permissions section:

- Administrators
- Roles
- Global Roles

From any tab, you can create an organization using the following procedure:

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click **Action** and select **Add Organization**.

Every system must have at least one organization.

3 On the *Create Organization* dialog, type a name for the organization and click **OK**.

Administrators Tab

To add or remove a system administrator:

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click the **Administrators** tab.

3 To add a system administrator:

a Click **Add**.

b On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.

c Click **OK**.

4 To delete a system administrator:

a Select a user group or user name.

b Click **Remove**.

Roles Tab

To create a system role:

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click the **Roles** tab.

3 Click **Add**.

4 On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.

Having separate options for "Allowed," "Unassigned," and "Denied" may seem redundant in a binary world. However, it permits WebInspect Enterprise to resolve conflicting permissions when a user is a member of more than one role. These are the controlling guidelines:

- "Allowed" outranks "Unassigned"—If the permission for a certain activity in Role A is "Allowed" and the permission for the same activity in Role B is "Unassigned," then a user who is a member of both Role A and Role B may perform the activity.
- "Denied" outranks "Allowed"—If the permission for a certain activity in Role A is "Allowed," and the permission for the same activity in Role B is "Denied," then a user who is a member of both Role A and Role B may not perform the activity.
- "Unassigned" (only) equals "Denied"—If a user's permission for a certain activity is "Unassigned" and no other permissions are assigned to that user in another role for the same activity, then the user may not perform the activity.

5 In the Permissions list, expand the nodes to view the activities associated with each category.

6 To assign the same permission to all activities within a single category:

a Click the category name (such as "Activity Log").

b Click the drop-down arrow that appears on the far right end of the row.

c Select a permission.

7 To change permission for a single activity:

a Expand a category.

b Click the activity name (such as "Can view log").

c Click the drop-down arrow that appears on the far right end of the row.

d Select a permission.

To assign groups or users to a role:

1 Select a name from the **Role name** list.

2 Click **Add** (on the far right of the **User group or user names** pane).

3 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.

4 Click **OK**.

You can copy a role and keep it at the system level or assign it to an organization or group.

To copy a role:

1 Click the **Roles** tab.

2 Select a role from the **Role name** list.

3 Click **Copy/Move**.

4 On the *Copy/Move Role* dialog, select the organization or group to which the role will be assigned.

The same role can be assigned to multiple organizations and groups.

5 To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when placed in the location you specify.

6 To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying or moving a system role to an organization or a group.

7 Select the location where this copy of the role should be placed.

You cannot copy a role to an organization or group unless you are an administrator of that organization or group.

8 Click **OK**.

Global Roles Tab

A global role is one that defines permissions for all three hierarchical levels (system, organization, and group). Once it is created, WebInspect Enterprise automatically copies the role to all levels (that is, to the system, to every organization, and to every group). However, you may subsequently remove the global role from specific organizations. Users can be added independently at each level, but permissions can be changed only at the system level, and only on the **Global Roles** tab. Any and all changes to a global role are propagated to each copy at all hierarchical levels.

To create a global role:

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click the **Global Roles** tab.

3 Click **Add** (the button above **Rename**).

4 On the *New Role* dialog, enter a name for the role, select the default permission category that will be assigned to each activity, and click **OK**.

5 In the **Permissions** list, expand the System, Organization and Group permissions and select Unassigned, Allowed, or Denied.

To remove global roles from specific organizations:

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click the **Global Roles** tab.

3 Select a role.

4 If the **All Organizations** check box is selected, clear it.

5 Click an organization from which the selected role should be deleted.

6 Click **Remove**.

To distribute a global role to all organizations:

If you have restricted a global role to certain organizations, you can quickly assign it to all organizations simply by selecting the **All Organizations** option.

1 Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.

2 Click the **Global Roles** tab.

3 Select a role assigned to specific organizations.

4 Select **All Organizations**.

Whenever you create an organization, WebInspect Enterprise will automatically distribute to that organization all global roles for which the **All Organizations** option is selected.

Organization Roles and Permissions

Security within the WebInspect Enterprise system is arranged according to a hierarchy of organizations and groups. You may have one or more organizations, and each organization may have one or more subordinate groups. At installation, there is one organization named Default Organization, which contains one group named Default Group. When you select an organization from the Security Group Hierarchy pane, the following tabs appear in the Organization Permissions section.

- Administrators
- Configuration
- Roles
- Resources
- Move/Copy Objects

Note: When a project version is created in HP Fortify Software Security Center (SSC), it is also created automatically in WebInspect Enterprise, where it is added to the Default Group in the Default Organization. If you want a different group in the same or a different organization to have access to a particular project version in WebInspect Enterprise, use the Administrative Console to move that project version to that group. See Group Roles and Permissions on page 44.

Adding an Organization

Use the following procedure to add an organization:

1. Select the **Administration** group.
2. Click the **Roles and Permissions** shortcut.
3. In the Security Group Hierarchy pane, select **WebInspect Enterprise System**.
4. Click **Action** and select **Add Organization**.

   The *Create Organization* dialog appears.
5. Type a name for the organization in the **Name** field.
6. Click **OK**.

Administrators Tab

To add or remove an organization administrator:

1. Select an organization in the Security Group Hierarchy pane.
2. Click the **Administrators** tab.
3. To add an organization administrator:
   a. Click **Add**.
   b. On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
   c. Click **OK**.
4. To delete an organization administrator:
   a. Select a user group or user name.
   b. Click **Remove**.

Configuration Tab

Maximum Scan Priority

If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. For each organization, you can specify the maximum priority level that may be assigned to scans.

Select the highest priority level that a user in this organization may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

More severe restrictions can be assigned to a group within the organization. For example, if the maximum priority for an organization is 3, the administrator of a group within that organization may set the group maximum priority to either 3, 4, or 5. The group's maximum scan priority may not be set to 1 or 2, however.

Organization Options

Disable Retest Browser Tab - The Retest feature allows you to view the server's response as rendered in a browser. Retesting a cross-site scripting vulnerability, however, may cause the script to loop infinitely on the Browser tab when using Microsoft Internet Explorer. If you are concerned about executing a cross-site scripting attack that may be embedded in your application, this option allows you to disable the Retest feature.

Roles Tab

To create an organization role:

1. Click **Add** (to the right of the **Role name** list).
2. On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.
3. In the **Permissions** list, expand the nodes to view the activities associated with each category.
4. To assign the same permission to all activities within a single category:
   a. Click the category name (such as “Blackouts” or “Policies”).
   b. Click the drop-down arrow that appears on the far right end of the row.
   c. Select a permission.
5. To change permission for a single activity:
   a. Expand a category.
   b. Click the activity name (such as “Can create” or “Can view”).
   c. Click the drop-down arrow that appears on the far right end of the row.
   d. Select a permission.

To assign users to a role:

1. Select a name from the **Role name** list.
2. Click **Add** (on the far right of the **User group or user names** pane).
3. On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
4. Click **OK**.

You can create a copy of a role and place it at any level (system, organization, or group). You can also move a role from one organization to another (which will remove it from the original organization).

You cannot copy or move a role to an organization or group unless you are an administrator of the target organization or group.

To copy or move a role:

1. Select a role from the **Role name** list.
2. Click **Copy/Move**.
3. On the *Copy/Move Role* dialog, select the organization or group to which the role will be assigned.

   The same role can be assigned to multiple organizations and groups. The permissions associated with a role can be copied only between similar levels (that is, from one group to another or from one organization to another).
4. To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when copied to the location you specify.
5. To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying an organization role and assigning it to a group or the system.
6. Select the location where this copy of the role should be placed.
7. To place a copy of the role in the selected location, click **OK**.
8. To move the role from its original location to the selected location, click **Move**.

Resources Tab

You can specify which resources are available to an organization. For example, the WebInspect Enterprise system contains 20 scanning policies. Your organization may choose to allow only 10 of them.

Note: The group administrator may further restrict which resources are available to a group.

1. Select an item in the **Object Type** list.

   If objects of the selected type have never been assigned, all instances of those object types are displayed in the **Available** column.

   If object types have previously been assigned, then object types may be distributed between the **Available** and **Allowed** columns.
2. To move object types from the **Available** column to the **Allowed** column, select one or more object types and click  .
3. To move all object types to the **Allowed** column, click  .
4. To move selected object types from the **Allowed** column and return them to the **Available** column, select one or more object types and click  .
5. To move all objects from the **Allowed** column and return them to the **Available** column, click  .

Move/Copy Objects Tab

You can assign an object to a different organization (and optionally to a group) by either moving it or copying it. Moving an object removes it from its currently assigned location. Copying an object retains its current location while also placing a copy in a new location.

1. Select an organization from the Security Group Hierarchy tree.
2. Select the **Move/Copy Objects** tab.

3. Select an item from the **Object Type** list.
4. Click **Retrieve**.

   All user-created objects of the selected type appear in the **Object Results** list.
5. Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.
6. Click **Move** or **Copy**.
7. On the *Move Objects* or *Copy Objects* window, select an organization from the **Target Organization** list.
8. (Optional) Select a group from the **Security Group** list.
9. Click **Move** or **Copy**.
10. If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list.

    For example, if you are moving a user-created scan template from one organization to another, and that template uses a scan policy that is not in the target organization, then you must also move (or copy) the scan policy.

    a. For each dependent object, click the drop-down arrow in the Action column under Object Dependencies and select the appropriate action (such as **Move to**, **Copy to**, or **Allow**).

    b. Click **Move** or **Copy**.
11. When a dialog appears informing you that all dependencies have been satisfied and prompting you to confirm that transfer, click **Yes**.

Group Roles and Permissions

Each group must be associated with an organization. If you do not want a certain user to see certain scans, you must create separate groups and assign the user to a role in one group or the other.

Note: When a project version is created in HP Fortify Software Security Center (SSC), it is also created automatically in WebInspect Enterprise, where it is added to the Default Group in the Default Organization. If you want a different group in the same or a different organization to have access to a particular project version in WebInspect Enterprise, use the Administrative Console to move that project version to that group.

Adding a Group

Each organization can have one or more groups. Use the following procedure to add a group.

1. Select the **Administration** group.
2. Click the **Roles and Permissions** shortcut.
3. In the Security Group Hierarchy pane, select an organization.
4. Click **Action** and select **Add Group**.

   The *Create Group* dialog appears.
5. Type a name for the group in the **Name** box.
6. If you want the group to have unrestricted access to all resources that are available to the organization, select **Allow access to all of the Organization's current resources**.
7. Select the highest priority level that a user in this group may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. Your choices may be restricted by your organization.

8 In the **Scan Permissions** group, click **Add**.

9 In the **Host** box, type a host name (wild cards allowed), IP address, or IP address range, and click **OK**.

10 In the **Properties** group, you may:

a Change the IP address or host name.

b Change permissions for running a Web Site scan and Web Service scan.

11 Click **OK** to close the *Create Group* dialog.

Notice that users who create a group are automatically assigned as administrators of that group.

Administrators Tab

To add or remove a group administrator:

1 Select a group in the Security Group Hierarchy pane.

2 Click the **Administrators** tab.

3 To add a group administrator:

a Click **Add**.

b On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.

c Click **OK**.

4 To delete a group administrator:

a Select a user group or user name.

b Click **Remove**.

Configuration Tab

Group Maximum Scan Priority

If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. For each group, you can specify the maximum priority level that may be assigned to a scan. Your choices may be restricted by your organization.

Select the highest priority level that a user in this group may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

Group IP and Host Permissions

For each group, the ability to scan web sites is restricted to those IP addresses or hosts specified here.

1 Click **Add**.

2 Enter an IP address or host name and click **OK**.

To specify a range of addresses, enter the lowest numerical address, followed by a dash (-), and then followed by the highest numerical address, such as 134.55.33.4-134.55.33.244.

You can also use wild cards, such as 134.55.33.* and www.mysite.*. Enter only an asterisk (*) to allow all possible IP addresses.

3 In the Properties pane, select **Can Run Scan**, click the drop-down arrow that appears, and select either **Unassigned**, **Allowed**, or **Denied.**

4 Repeat this procedure to specify additional targets.

Roles Tab

1 Select a group in the Security Group Hierarchy pane.

2 Click the **Roles** tab.

To create a group role:

1 Click **Add** (to the right of the **Role name** pane).

2 On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.

3 In the **Permissions** list, expand the nodes to view the activities associated with each category.

4 To assign the same permission to all activities within a single category:

   a Click the category name (such as "Blackouts" or "Policies").

   b Click the drop-down arrow that appears on the far right end of the row.

   c Select a permission.

5 To change permission for a single activity:

   a Expand a category.

   b Click the activity name (such as "Can create" or "Can view").

   c Click the drop-down arrow that appears on the far right end of the row.

   d Select a permission.

To assign users to a role:

1 Select a role from the **Role name** list.

2 Click **Add** (to the right of the **User group or user names** pane).

3 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.

4 Click **OK**.

If your domain server uses the Microsoft Windows 2000 or 2003 operating system, and you have more than 1000 users on your network, you must modify the Lightweight Directory Access Protocol (LDAP) policies used by the Microsoft Active Directory® service. Specifically, you must change the maximum page size that is supported for LDAP responses (which is set by default to 1,000 records). Alternatively, you can limit your search criteria so that fewer than 1000 records will be returned. For detailed information, refer to **http://support.microsoft.com/default.aspx?scid=kb;en-us;315071&sd=tech**.

To copy or move a role:

You can create a copy of a role and place it at any level (system, organization, or group). You can also move a role from one group to another (which will remove it from the original group).

You cannot copy or move a role to an organization or group unless you are an administrator of the target organization or group. Also, you cannot rename or remove a global role.

1 Select a role from the **Role name** list.

2 Click **Copy/Move**.

3 On the *Copy/Move Role* dialog, select the organization or group to which the role will be assigned (or select the WebInspect Enterprise system).

The same role can be assigned to multiple organizations and groups. The permissions associated with a role can be copied only between similar levels (that is, from one group to another or from one organization to another).

4 To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when copied to the location you specify.

5 To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying an organization role and assigning it to a group or the system.

6 Select the location where this copy of the role should be placed.

7 To place a copy of the role in the selected location, click **OK**.

8 To move the role from its original location to the selected location, click **Move**.

Resources Tab

You can specify which resources are available to groups within an organization. For example, the WebInspect Enterprise system contains 20 scanning policies. Your organization may choose to allow only 10 of them. Of those 10 available, you might choose to allow only 5 to be used in your group.

1 Select an item in the **Object Type** list.

If objects of the selected type have never been assigned, all instances of those object types are displayed in the **Available** column.

If object types have previously been assigned, then object types may be distributed between the **Available** and **Allowed** columns.

2 To move object types from the **Available** column to the **Allowed** column, select one or more object types and click > .

3 To move all object types to the **Allowed** column, click >> .

4 To move selected object types from the **Allowed** column and return them to the **Available** column, select one or more object types and click < .

5 To move all objects from the **Allowed** column and return them to the **Available** column, click << .

Move/Copy Objects Tab

You can assign an object to a different group (and optionally to a organization) by either moving it or copying it. Moving an object removes it from its currently assigned location. Copying an object retains its current location while also placing a copy in a new location.

1 Select a group or organization from the Security Group Hierarchy tree.

2 Select the **Move/Copy Objects** tab.

3 Select an item from the **Object Type** list.

4 Click **Retrieve**.

All user-created objects of the selected type appear in the **Object Results** list.

5 Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.

6 Click **Move** or **Copy** (or **Recover**, if restoring deleted project versions).

7 On the *Move Objects* or *Copy Objects* window, select an organization from the **Target Organization** list.

8 Select a group from the **Security Group** list.

9 Click **Move** or **Copy**.

10 If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list.

For example, you are not allowed to move a user-created (custom) policy from Organization A to Organization B if that policy is to be used for a scheduled scan in Organization A.

a For each dependent object, click the drop-down arrow in the Action column under Object Dependencies and select the appropriate action (such as **Move to**, **Copy to**, or **Allow**).

b Click **Move** or **Copy**.

11 When a dialog appears informing you that all dependencies have been satisfied and prompting you to confirm that transfer, click **Yes**.

Proxy Server Settings

If you use a proxy server to communicate with HP for Smart Updates and licensing issues:

1 Click the **Administration** group.

2 Select the **Proxy Server Settings** shortcut.

3 Select the **Use Proxy Server** option.

4 Provide the requested information.

5 Click **Save**.

Smart Update is not available if you use a SOCKS4 or SOCKS5 proxy server configuration. Smart Update is available through a proxy server only when using a standard proxy server.

Software Security Center

To publish scans or import projects to HP Fortify Software Security Center (SSC), the Software Security Center Settings must be configured. Initial settings are established during installation of WebInspect Enterprise. You can modify the settings as follows:

1 Click the **Administration** group.

2 Select the **Software Security Center** shortcut.

3 Enter the following information:

- **WebInspect Enterprise URL**: The URL of the WebInspect Enterprise server.
- **Software Security Center URL**: The URL of the SSC server.
- **Administrator - User Name** and **Password**: Enter the name and password of the user who was assigned to the WebInspect Enterprise System role, as created in SSC. Using the SSC administrator's account is not recommended.

  Web Console users, when publishing scans to SSC, will be required to enter their own credentials.
- **WebInspect Enterprise Service Account - User Name** and **Password:** Enter the name and password of the user who was assigned to the WebInspect Enterprise service account (with the role of WebInspect Enterprise System), as created in SSC.

4 To verify the settings for connection to SSC, click **Test**.

5 To save the settings, click **Save**.

Actions

You can select a command from the **Action** menu. The availability of commands depends on the permissions granted to you by your assigned role. The commands are:

Command	Definition
Import Projects to SSC	Import projects into SSC from a `.csv` file created from IP addresses found using the Web Discovery tool. See Importing Projects Converted from Web Discoveries into SSC.
Synchronize Projects	Synchronize projects between WebInspect Enterprise and SSC. This process generally occurs automatically.
Unregister WebInspect Enterprise	Disconnect WebInspect Enterprise from SSC. Used only if you are moving to another instance of SSC.

Importing Projects Converted from Web Discoveries into SSC

You can use the Web Discovery tool to discover sites over a range of IP addresses and convert the discovered IP addresses to projects in a `.csv` file. Then you can edit the data and import the projects into SSC. The procedure is as follows:

1. Run the Web Discovery tool against the desired range of IP addresses. See Web Discovery on page 201.
2. In the tool, click **File** → **Export** → **To CSV File** to save the set of discovered sites. Specify the desired name and location for the `.csv` file.
3. Open the `.csv` file in Microsoft Excel.
4. Adjust the widths of the following columns as desired:
   - **SSC Project (required)**. By default, the value is the IP address that was discovered.
   - **SSC Project Version (optional)**. By default, the value is **Production**.
   - **URL (optional).** By default, the value is the URL to be used for a scan.
   - **Server Information (optional).** By default, the web platform of the detected server. It appears in project version properties in WebInspect Enterprise, but does not appear in SSC.
5. Edit the file as desired. For example, you can specify SSC project versions that are meaningful to you.
6. Save the edited file.
7. In the WebInspect Enterprise Administrative Console, click **File** → **Import Projects to SSC.**

   The *Create Project Versions from imported CSV files* dialog opens.
8. Browse to the `.csv` file location and click **OK.**

   The projects and project versions are created in SSC.

Common WebInspect Enterprise Administrative Console Tasks

Configure the Console

Use the following procedure to specify settings for the WebInspect Enterprise Administrative Console.

1. From the **Tools** menu, select **Options**.
2. To refresh the display of WebInspect Enterprise information periodically, select the **Automatically refresh display** check box and specify how often (in seconds) the display should be updated.
3. Click **OK**.

Suspend a Scan

After a scan has started, you can suspend it and then later restart it at the point at which it was suspended.

To suspend a scan:

1. Click the **Scans** group.
2. Click the **Scan Queue** shortcut.
3. Select a scan.
4. Select **Suspend** from the **Action** menu (or from the shortcut menu that appears when you right-click a scan).

The scan request displays a status message of "Suspended (Manual)."

Resume a Suspended Scan

To resume a suspended scan:

1. Click the **Scans** group.
2. Click the **Scan Queue** shortcut.
3. Select the scan you want to resume.
4. Select **Resume** from the **Action** menu (or from the shortcut menu that appears when you right-click a scan).

If the sensor that started the scan is available, then that sensor will reload the scan data and resume scanning.

If the sensor that started the scan is now running a different scan, then that sensor will compare the priority of both scans. If the first (suspended) scan has a lower priority, the sensor will place it back in the queue and continue running the current scan. If the first scan has a higher priority, the sensor will suspend the second scan (placing it in the queue), reload the data from the first scan, and resume scanning.

Resumed scans are always assigned to the same sensor on which the scan was initiated.

Stop a Scan

To stop a scan:

1. Click the **Scans** group.
2. Click the **Scan Queue** shortcut.

3 Select the scan you want to stop.

4 Select **Stop** from the **Action** menu (or from the shortcut menu that appears when you right-click a scan).

The scan request is removed from the list.

Pause a Sensor

Use this function to pause a sensor. If a scan is running on that sensor, the job will be suspended.

This feature is used when conducting maintenance on the machine that contains the sensor, or when you simply want to prevent the sensor from accepting any scans.

1 Click the **Sensors** group.

2 Select the sensor you want to pause.

3 Select **Pause Sensor** from the **Action** menu (or from the shortcut menu that appears when you right-click a sensor).

Continue a Paused Sensor

Use this function to enable a sensor that you previously disabled by using the Pause command. If a scan was running on that sensor when the sensor was paused, the scan will resume.

1 Click the **Sensors** group.

2 Select the sensor you want to continue. “Paused” must appear in the Status column.

3 Select **Continue Sensor** from the **Action** menu (or from the shortcut menu that appears when you right-click a sensor).

Perform a Smart Update

Use Smart Update to download HP’s latest adaptive agents and programs, as well as vulnerability and policy information.

To conduct a Smart Update, click the **Smart Update** icon on the toolbar

- or -

click the **Tools** menu and select **Smart Update**.

Note that scans cannot start while sensors are receiving a Smart Update. Scheduled scans stay in “pending” state until Smart Update completes. This prevents sensors from picking up partial Smart Updates when they update their local SecureBase from WebInspect Enterprise.

Schedule a Smart Update

To scheduled a Smart Update:

1 Click the **Administration** group.

2 Click the **Smart Update** shortcut.

3 Click the **Action** menu and select **Add Schedule**.

4 In the General category:

a Type a name for the event in the **Scheduled Smart Update Name** box.

b In the **Start Time** box, specify the date and time when Smart Update should run.

c To change the date, click the drop-down arrow and select a date from the calendar.

d To define an iterative process, click the Recurrence category (in the left column).

5 In the Recurrence category:

a Select the **Recurring** check box.

Do NOT select this option if you want to schedule a one-time-only event.

b Use the **Pattern** group to select the frequency of the event (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.

c Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the Smart Update should occur.

6 Click **OK** to schedule the update.

View Activity Log

You can view information about significant events that occur and are logged by the WebInspect Enterprise manager. Each event is sorted according to the time and date at which the event occurred.

To view the activity log:

1 Click the **Administration** group.

2 Click the **Activity Log** shortcut.

Add Users to Roles

You can add a user to roles at each individual organization or group, repeating the process as often as necessary until the user has been inserted into all desired roles. Although this is quick and easy when dealing with one user and one role, it can be repetitious and time-consuming for multiple roles and users.

The **Action** menu command **Add User(s) to Roles** is a time-saving alternative.

1 On the WebInspect Enterprise Administrative Console, click the **Administration** group.

2 Select the **Roles and Permissions** shortcut.

3 Click the **Action** menu and select **Add User(s) to Roles**.

The *Add User to Roles* dialog opens.

4 Type a user name or group name in the **User/Group name** text box, or click **Browse** to open the *Select SSC Users or Groups* dialog and select a user or group.

5 Select a role from the **Roles** list.

6 If you selected a global role, under Project Hierarchy select which organizations and groups containing that role are to be updated to include the user or group you selected.

7 If you selected **(All Custom Roles)**, under Project Hierarchy select the roles to which the user or group you selected is to be assigned.

8 Click **Apply**.

Create a Master Policy

System administrators can create a custom policy at the system level and assign it to multiple organizations and groups. Subsequent changes to this master policy will automatically propagate to the organization and group level, eliminating the need to update each individual copy of that policy in each organization and group.

You must be a system administrator to create master policies.

Task 1: Enable the feature.

1. On the WebInspect Enterprise Administrative Console, click the **Administration** group.
2. Select the **Roles and Permissions** shortcut.
3. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
4. Click the **Roles** tab.
5. Select or create a role.
6. In the Permissions area, select **Policies**.
7. Select **Allowed** for all Policies permissions.

Task 2: Create a custom policy.

1. Select the Scans group.
2. Click the Scan Policies shortcut.
3. Right-click a policy that you want to use as the template for the new policy and select **Copy** from the shortcut menu.

   WebInspect Enterprise will check for and download any updates to the policy.
4. On the *Copy Policy* dialog, enter a name for the new policy and assign it to an organization.
5. Select the **Use as Master** option.
6. Click **OK**.

Task 3: Modify the policy.

After you save the renamed policy, the Policy Manager opens.

1. Modify the policy to suit your needs.
2. When finished, save your work and close the Policy Manager.

The custom policy now appears in the list of Scan Policies.

Task 4: Add the policy to organizations/groups.

1. Click the **Administration** group and select the **Roles and Permissions** shortcut.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Resources** tab.
4. Select **Policies** from the **Object Type** list.
5. Add the new custom policy to the list of allowed policies. Select the policy from the **Available** list and click  .

4 WebInspect Enterprise Web Console

Introduction

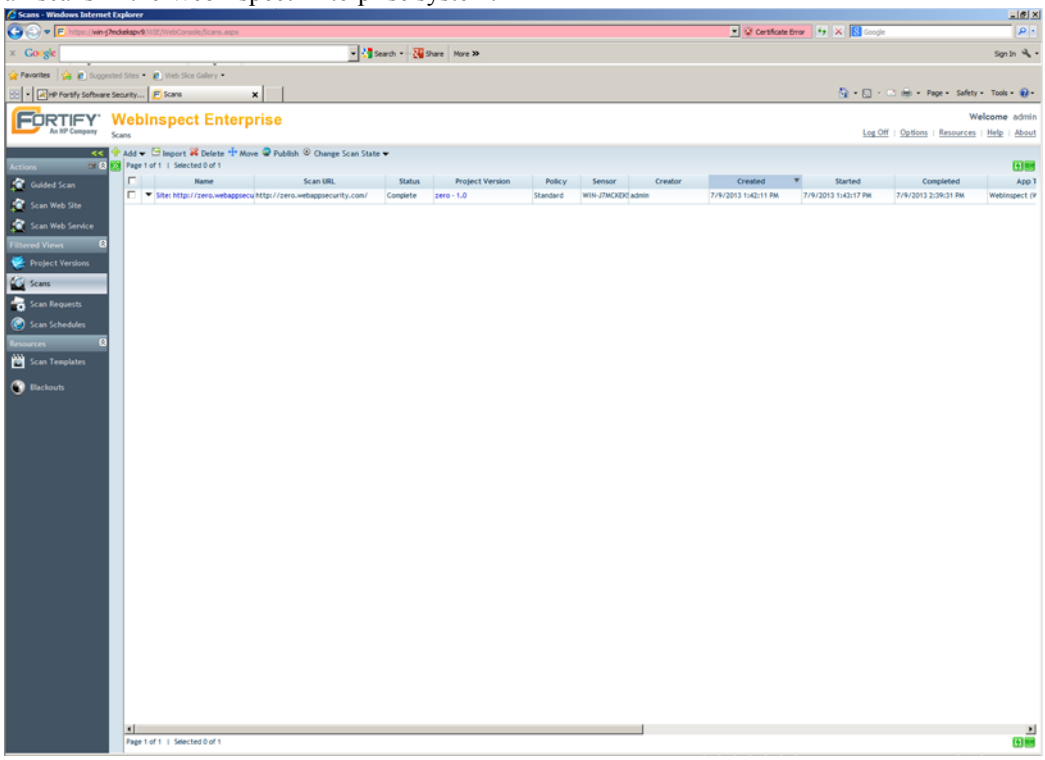
WebInspect Enterprise presents the following separate user interfaces:

- The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console. It is used for administrative and security functions; see Chapter 3, WebInspect Enterprise Administrative Console.
- The WebInspect Enterprise Web Console, a browser-based application used for conducting and managing scans. This chapter describes this Web Console—its user interface, how to configure and run a scan, how to evaluate and modify scan results in the *Scan Visualization* window, and how to publish the scan results to HP Fortify Software Security Center (SSC).
- Guided Scan, the preferred alternative to the standard Web Site scan. Guided Scan directs you through the best steps to configure a scan that is tailored to your application. The first time you launch Guided Scan in WebInspect Enterprise or Software Security Center, the Guided Scan client application, which includes its own Help system, is donwloaded and installed on your local computer. See Chapter 5, Guided Scan.

The WebInspect Enterprise Web Console user interface comprises the following main areas:

- Toolbar - Links in the upper right of the page to capabilities that are available for all WebInspect Enterprise Web Console screens.
- Navigation pane - Left pane to select the action to take or the associated view or form to display in the right pane.
- Views and forms - Displays the view or form selected in the navigation pane.

In the following screen capture, the user has selected the **Scans** button to display a form containing a list of all scans in the WebInspect Enterprise system.



Toolbar

The WebInspect Enterprise Web Console toolbar contains the following links:

- **Log Off** - Logs you off the WebInspect Enterprise Web Console application.
- **Options -** Opens the *Configure Options* window, allowing you to specify various options, including a default group and a Web console time zone, and to enable or disable other options.
- **Resources -** Opens an HP WebInspect Enterprise page on the HP website.
- **Help -** Opens the Help file.
- **About** - Opens a window that displays the WebInspect Enterprise manager version and the database schema version.

In addition, you can click the Fortify logo to return to the home page of the WebInspect Enterprise application.

Options

Click **Options** on the toolbar to configure Web Console options.

Option	Description
Default Group	Select a group that will be used by client applications that cannot specify a group. A client application is WebInspect or any application that uses the WebInspect Enterprise application programming interface (API). Each user account is associated with a default group. If WebInspect Enterprise receives a call to create an object and the calling client application is not aware of the WebInspect Enterprise "group" category, WebInspect Enterprise will use the default group specified here.
Web Console Time Zone	Select the time zone in which you work.
Enable "Scan Web Site" action	This option allows you to initiate a website scan from the Web Console, using the Scan Web Site function in the Actions group. If not selected, **Scan Web Site** does not appear on the navigation pane.
Enable "Scan Web Service" action	This option allows you to initiate a web service scan from the Web Console, using the Scan Web Service function in the Actions group. If not selected, **Scan Web Service** does not appear on the navigation pane.
Enable "New Scan Schedule" action	This option allows you to schedule a scan from the WebInspect Enterprise Web Console, using the New Scan Schedule function in the Actions group. If not selected, **New Scan Schedule** does not appear on the navigation pane.
Enable "New Blackout" action	This option allows you to create and modify blackout periods from the Web Console, using the New Blackout function in the Actions group. If not selected, **New Blackout** does not appear on the navigation pane.

Navigation Pane

The navigation pane is divided into the following sections:

- Actions
- Filtered Views
- Scans
- Resources
- Administration (present only if project versions have been deleted in SSC)

Selecting an option in the navigation pane displays a corresponding form in the Form area.

Actions

Guided Scan

The Guided Scan action launches Guided Scan, the preferred method for performing a website scan. It directs you through the best steps to configure a scan that is tailored to your application. For detailed information, see Chapter 5, Guided Scan.

Scan Web Site

The Scan Web Site action launches the Scan Wizard, which leads you through a series of dialogs that allow you to specify settings (options) for the scan.

Only the most often modified options are presented. To access the complete set of options, click **Advanced Settings** (at the bottom of the window).

This feature is not available and the selection will not appear in the Actions group unless **Enable "Scan Web Site" action** is selected as an option. To enable or disable this feature, click the Options link on the WebInspect Enterprise toolbar.

Scan Web Service

The Scan Web Service action initiates a scan by displaying windows that allow you to specify settings (options) for the scan.

When performing a Web service scan, WebInspect Enterprise crawls a WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a Web Service Test Design (WSD) file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

This feature is not available and the selection will not appear in the Actions group unless **Enable "Scan Web Service" action** is selected as an option. To enable or disable this feature, click the Options link on the WebInspect Enterprise toolbar.

New Scan Schedule

The New Scan Schedule action (disabled by default) allows you to specify settings (options) for a scan and designate the time when the scan should begin.

This feature is not available and the selection will not appear in the Actions group unless **Enable "New Scan Schedule" action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

New Blackout

The New Blackout action (disabled by default) allows you to specify periods when scans are not allowed to be conducted (or, conversely, periods when scans are allowed to be conducted).

This feature is not available and the selection will not appear in the Actions group unless **Enable "New Blackout" action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

Filtered Views

Project Versions

This form displays, in the left column, a list of all defined projects and their component versions.

Note: When a new project version is created in SSC, it automatically appears in the Project Versions here in WebInspect Enterprise.

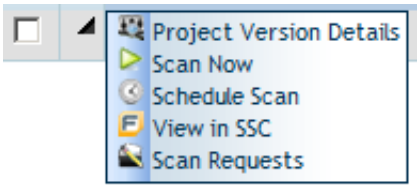
Click a project name to display information about all associated versions, or click a single version name.

For each version selected, this form displays:

- The project version name
- The number of issues detected in each of six categories
- The name of the security group with which this version is associated
- The name of the organization with which this version is associated
- The name of the project with which this version is associated

To view project version details, click a project version name, or click the drop-down arrow to the left of the project version name and click **Project Version Details**.

You can perform additional functions by clicking the drop-down arrow for a specific project version.



The functions unique to this menu are:

Scan Now—Open the *New Scan* form, allowing you to enter scan settings and initiate a scan.

Schedule Scan—Open the *Configure Scheduled Scan* form, allowing you enter scan settings and schedule a scan.

View in SSC—Launch HP Fortify Software Security Center (SSC) and navigate to the **Issues** tab of the Project Version window.

Scan Requests—View all SSC scan requests associated with this project version.

Project Version Details

This form provides complete details about the selected project version, categorized on the following tabs:

- **All Scans**—Lists all scans conducted for the project version and displays (by default) the following information:
  - Scan name
  - Scan status (failed or complete)
  - Date and time the scan was conducted
  - Date and time the scan was published
  - Whether the scan was requested by SSC
  - Number of vulnerabilities detected, categorized by severity

- Published status (Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC)

Icons allow you to add scans, import scans, delete scans, move scans to a different project version, publish scans to SSC, and change the state of a scan. Click a scan name to open the *Scan Visualization* window for that scan. For more information, see Scan Visualization on page 73.

Click the drop-down arrow for a specific scan and select an option to view scan details in the *Scan Visualization* window, move the scan to a different project version, delete the scan, publish scan data to SSC, export the scan data in either XML or FPR format, or perform other functions.

- **Issues**—Displays a list of all vulnerabilities, sorted by severity, detected in this project version, and displays (by default) the following information:
  - Check ID - Identification number of the WebInspect probe that discovered the vulnerability.
  - Check Name - Name of the check that discovered the vulnerability.
  - Vulnerable URL - Location of the vulnerability.
  - Severity - A relative assessment of the vulnerability, ranging from low to critical.
  - Scan - Name of the scan.
  - SSC Status - Indicates whether or not the issue has been uploaded to Software Security Center.
  - Ignored - If a check mark appears in column, a user classified this vulnerability as Ignored (using the Review Vulnerability form).
  - False Positive - If a check mark appears in column, a user classified this vulnerability as a false positive (using the Review Vulnerability form).

  Click the drop-down arrow for a specific issue to view details or view the project version in SSC.

  Click a check name to open the *Issue Details* form. This form has the following tabs:

  - **Vulnerability** - Contains a complete description of the detected vulnerability, including instructions for verifying and fixing the problem.
  - **Request** - Displays the HTTP request sent to the target site as a probe for the vulnerability.
  - **Response** - Displays the HTTP response returned by the target site.
  - **Stack Trace** - This feature is designed to support HP Fortify SecurityScope when it is installed and running on the target server. For certain checks (such as SQL injection, command execution, and cross-site scripting), SecurityScope intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, SecurityScope appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation. See Dashboard on page 77 and Session Info Panel on page 78.
  - **Additional Info** - For Flash files, displays decompiled code.

  An icon allows you to show or hide ignored issues.

- **Scan Templates**—Displays a list of scan templates associated with this project version. and displays (by default) the following information:
  - Template name
  - Security group
  - Organization name
  - Project name
  - Project version

Click the drop-down arrow for a specific template and select options to edit, copy, or delete the template, or display dependencies associated with the template. See Dependencies on page 70 for more information.

Click a template name to open the *Configure Scan Template* window to view or modify template settings.

Icons allow you to create or delete a template, or import a template that contains settings that are optimized for Oracle.

- **Schedules**—Lists all scans scheduled for the project version and displays (by default) the following information:
  - Name of the scheduled scan
  - URL of the scan target
  - Recurrence
  - Project version
  - Sensor
  - Policy
  - Priority
  - Scan type
  - Last occurrence
  - Last occurrence (target)
  - Next occurrence
  - Next occurrence (target)
  - Security group
  - Organization

  Click a schedule name to open the *Configure Scheduled Scan* window to view or modify settings for the scan.

  Click the drop-down menu next to each Check ID to edit, copy, delete, or enable/disable the scheduled scan.

  Icons allow you to add or delete scheduled scans.
- **Properties**—Lists information about the project version, including the project version name and URL, platform information, the contact's name and e-mail address, and host information.
- **Notes**—Allows you to create or view notations associated with the project version.
- **Aliases**—Lists all aliases created for the project version, and displays for each alias the following information:
  - Primary URL for this project version
  - Description of the alias
  - Indication of whether or not the server differentiates between URLs based on case sensitivity.

  Click the drop-down arrow for a specific alias to edit or delete the alias. See Adding or Editing an Alias on page 62 for detailed instructions.

  Icons allow you to add or delete aliases, or recalculate all scans.

You can also perform additional functions using the icons at the top of the form.

Icon	Function
Scan Now	Display scan settings, as entered for the previous scan. You can modify the settings, if desired, before initiating the scan.
View in SSC	Launch SSC application and navigate to the Issues tab of the Project Version window.
Scan Requests	Navigate to the Scan Requests form, where you can process requests issued from SSC.

Publishing Scans to Software Security Center

You can publish a scan to HP Fortify Software Security Center (SSC) from the following locations:

- Project Version Details form, **All Scans** tab with a scan selected, **Publish** button
- Scans form with a scan selected, **Publish** button
- Scan Visualization, **Publish Scan to SSC** button

When you publish a scan, WebInspect Enterprise displays a dialog listing the number of vulnerabilities to be published, categorized by status and severity. To determine the status, WebInspect Enterprise compares previously submitted vulnerabilities (obtained by synchronizing with SSC) with those reported in the current scan. If this is the first scan submitted to a project version, all vulnerabilities will be "New."

If a vulnerability was previously reported, but is not in the current scan, it is marked as "Not Found." You must determine if it was not found because it has been fixed or because the scan was configured differently (for example, you may have used a different scan policy, or you scanned a different portion of the site, or you terminated the scan prematurely). When examining the results, you can change the "pending status" of individual vulnerabilities detected by all but the first scan (by right-clicking an item in the summary pane). However, when publishing, you must specify how WebInspect should handle any remaining "Not Found" vulnerabilities.

1. Under **Default Status of "Not Found" Vulnerabilities**, do one of the following:
   - To retain these "Not Found" vulnerabilities in SSC (indicating that they still exist), select **Retain: Assume all vulnerabilities still marked "Not Found" in the scan are still present**.
   - To change the status from "Not Found" to "Resolved" (implying that they have been fixed), select **Resolve: Assume all vulnerabilities still marked "Not Found" in the scan are fixed**.

   Note: This section may not appear if there are no "Not Found" vulnerabilities.
2. If this scan satisfies a scan request issued from SSC, select **Associate scan with an "In Progress" scan request for the current project version**. See Scan Requests on page 66 for more information.
3. Click **Publish**.

Adding or Editing an Alias

Sometimes, identical Web applications are deployed on different hosts. For example, during the development process, the same application may be deployed and tested on QA.testsite.com, Staging.testsite.com, and finally Production.testsite.com. This becomes problematic when performing a dynamic analysis scan because correlation uses the URL as a key component to match multiple vulnerabilities.

To overcome this problem, you can create an alias for those project versions by identifying all the equivalent URLs and hostnames for the Web application, which allows correlation to occur for all active and future scans.

To create an alias:

1. Select **Project Versions** from the navigation pane.
2. Click the name of a project version for which you want to create an alias.
3. On the *Project Version Details* form, click the **Aliases** tab.
4. Click **Add**.
5. On the Add *New Alias* dialog, in the **Primary URL** box, enter the alias URL (the umbrella under which other scans will be associated). Using the above example, you might enter http://Production.testsite.com. Be sure to include the protocol (for example, http://).
6. If the server differentiates between URLs based on case sensitivity, select **Case Sensitive URL**.
7. Enter a description of the URL.
8. Click **Add**.
9. In the **Equivalent URLs** box, enter the URL of a host that will be covered by this alias. Using the above example, you might enter http://QA.testsite.com.
10. To add other URLs, repeat step 8 and step 9.
11. When finished, click **Save**.
12. When notified that the alias was saved successfully, click **OK**.

The primary URL is listed on the form.

You should set up aliases before publishing. Otherwise, if conflicts occur, you may lose the vulnerability history because the correlation IDs may change. If you add or edit aliases after a scan has been published for that project version, you will be prompted to recalculate.

Note: Correlation is a mathematical calculation that uses a variety of values to determine if the vulnerability is really a duplicate of another vulnerability. You should recalculate whenever you change an alias.

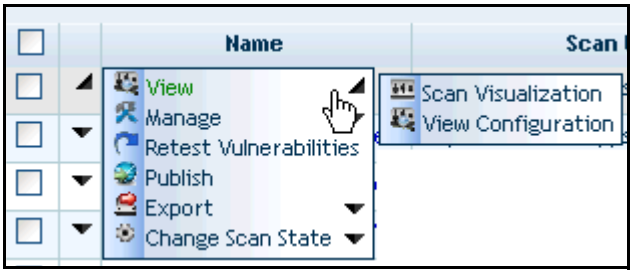
Scans

For each scan in the WebInspect Enterprise database, this form displays (by default) the following information:

- Name - The name assigned to the scan by the user.
- Scan URL - Target Web site URL or IP address.
- Status - Current state of the scan (imported, complete, etc.).
- Project Version - Project version to which this scan is assigned. Click this field to open the associated Project Version Details form.
- Policy - The policy used for the scan.
- Sensor - The sensor that conducted the scan.
- Creator - User name of the person who initiated the scan.
- Created - Date and time the scan object was created or imported.
- Started - Date and time the scan started.
- Completed - Date and time the scan finished.
- App Type - Application type.
- App Version - Application version number.
- Scan Request? - If a check mark appears in this column, the scan was requested by SSC.

- Results? - If a check mark appears in this column, the number of vulnerabilities detected appears in columns sorted by severity.
- Priority - A relative value assigned to the scan; it is used to determine precedence if a sensor scheduling conflict occurs.
- Vulnerabilities (in columns sorted by severity) - Number of vulnerabilities detected.
- Security Group - Name of the security group associated with this scan.
- Organization - Name of the organization associated with this scan.
- SecurityScope Detected - Indicator (Yes/No) whether SecurityScope was detected during the scan.
- Project Name - Name of the project associated with this scan.
- Publish Status - Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC.
- Publish Date - The date on which the scan data was published to SSC.

You can perform additional functions by clicking the drop-down arrow for a specific scan.



The options are:

- **View**
  - **Scan Visualization**—Open the *Scan Visualization* window, allowing you to examine the scan results. You can also click a scan name to open the *Scan Visualization* window. For more information, see Scan Visualization on page 73.
  - **View Configuration**—View (but not edit) the settings used for the selected scan.
- **Manage**
  - **Repeat Scan**—Rescan the target site using the same settings as the original scan.
  - **Copy**—Copy all settings that were used for this scan and paste them into the *Configure Scan* window, allowing you to edit the settings before initiating the scan.
  - **Copy to Schedule**—Copy all settings that were used for this scan and paste them into the *Configure Scheduled Scan* window, allowing you to edit the settings before scheduling the scan.
  - **Create Template from the Scan** - Create a scan template containing the settings that were used to produce this scan**.**
  - **Rename**—Assign a different name to the scan.
  - **Move**—Assign the scan to a different project version.
  - **Delete**—Delete the scan.
- **Retest Vulnerabilities**—Conduct a scan that examines only those portions of the target site in which vulnerabilities were detected during the original scan. WebInspect Enterprise does not conduct a new crawl of the site, but simply retraces the path of vulnerable sessions (as recorded in the original scan) and attacks the resources using the same checks previously employed. The default name of the scan is

"Site Retest - <original scan name>"; for example, the retest of a site that originally resulted in a scan named MySite would produce a scan named Site Retest - MySite. However, you can specify a different name when launching the scan.

- **Publish**—Send scan data to SSC. For more information, see Publishing Scans to Software Security Center on page 62.
- **Export**—Export the selected scan (or settings for the selected scan) to a destination you select.
- **Change Scan State**—Start, stop, resume, or suspend a scan.

Note for Internet Explorer users: When attempting to export scans, errors will result if the Internet option "Do not save encrypted pages to disk" is selected.

You can also perform additional functions using the icons at the top of the form.

Icon	Function
Add	Start a new scan. See Advanced Scan Settings on page 90 for a description of scan settings.
Import	Import a scan. This feature invokes the Scan Uploader, which allows you to assemble scans from WebInspect Enterprise managers and upload them to a project version. Note: WebInspect Enterprise may display the message, "You cannot start application Scan Uploader from this location because it is already installed from a different location." This can occur when you have multiple WebInspect Enterprise managers, or you rename your WebInspect Enterprise manager, or you access the same WebInspect Enterprise manager using different URLs, and you are importing to a WebInspect Enterprise manager that is different from the one into which you previously imported. The workaround solution is to uninstall the Scan Uploader utility and click the Import button again (which will reinstall the utility that is paired with the correct URL). Alternatively, launch the utility using the desktop shortcut instead of the **Import** button. Scans can also be uploaded through the Scan Uploader service provided by the WebInspect Enterprise Services Manager. If you scan a Web site with WebInspect, you can copy the results to a location called a "dropbox." The Scan Uploader service (which is separate from the Scan Uploader utility) can access each dropbox periodically and, if files exist, upload those files to the WebInspect Enterprise Manager. You can configure this feature through the WebInspect Enterprise Services Configuration utility. Configuration is performed as part of product installation; for more information, see the *HP WebInspect Enterprise Installation Guide*, which is available by clicking the **Resources** link on the Web Console.
Delete	Delete the selected scan.
Move	Assign the scan to a different project version.
Publish	Send scan data to SSC. For more information, see Publishing Scans to Software Security Center on page 62.
Change Scan State	Select one of the following: • Start the scan. • Stop the scan (if running). • Resume the scan (if suspended). • Suspend the scan (if running). • Repeat a selected scan.

Scan Requests

This form lists all requests issued by SSC to WebInspect Enterprise to conduct a scan. The possible values for the Status column are Pending, In Progress, and Complete.

For instructions on how an SSC user can generate a scan request, see Creating a Scan Request on page 67.

Use the following procedure to process a request.

1. In the Filtered Views section of the navigation pane, click **Scan Requests**.
2. On the *Scan Requests* window, select a pending request. The information entered by the original requester is displayed on the **Details** tab in the lower pane.

   To restrict the display of scan requests to those that match criteria you specify, simply click  in the header of one or more columns and enter the appropriate filter information.
3. On the **Details** tab in the lower pane, click the **Status** list and select **In Progress**.
4. Click **Create a Web Site Scan** or **Create a Web Service Scan** (or you can postpone running the scan until a later, more convenient time).

   When the scan is complete, review the results. You may want to retest or delete vulnerabilities, mark vulnerabilities as ignored or false positive, attach screenshots, or investigate the scan data in other ways facilitated by WebInspect Enterprise.

   Even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.
5. Publish the scan.
   a. Do one of the following:
      – From the Project Version Details form, select the scan and click **Publish**.
      – From the Scans form, select the scan and click **Publish**.
      – Open a scan in the *Scan Visualization* window and click **Publish**. For more information, see Scan Visualization on page 73.

   b. When the Status Summary is displayed, select **Associate scan with an "In Progress" scan request for the current project version**. The scan will appear on the **Associated Scans** tab of the appropriate scan request in the Scan Request form. See Note below.
6. Return to the *Scan Requests* form and select the request for the scan you have reviewed and published.
7. Click the **Status** list and select **Completed**.
8. Click **Change Status**.

Note: Associating a scan with a scan request is simply a tracking tool that provides a historical record of the scan activity related to a specific request. You can associate scans automatically when publishing (as in step 5, above), or you can associate scans manually, using the following procedure:

1. Select a scan request from the top pane.
2. In the bottom pane, click the **Associated Scans** tab.
3. Click **Associate Scans**.

   The program displays a list of all scans associated with the selected project version that have not been associated with a specific request.
4. Select a scan and click **OK**.

Creating a Scan Request

Use the following procedure in HP Fortify Software Security Center to create a request for WebInspect Enterprise to conduct a dynamic scan.

1. Click the **Projects** tab.
2. Select a project version and click **View Details**.
3. On the **Issues** tab of the *Details* window, click the drop-down arrow on the **Dynamic Scan Request** button and select **Create**.
4. Enter the requested information and click **Submit**.

The request is transmitted to WebInspect Enterprise and placed in the *Scan Requests* form.

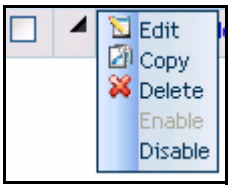
Scan Schedules

This view displays information about each scheduled scan.

Note: This feature is not available and the Action options do not appear in the Filtered Views group unless the **Enable "New Scan Schedule" action** is selected as an option. To enable or disable this feature, click the Options link on the WebInspect Enterprise toolbar.

Click a schedule name to review the settings for the scheduled scan.

You can perform additional functions by clicking the drop-down arrow for a specific scheduled scan.



The functions unique to this menu are:

Edit—Copy all settings that were used for the selected scheduled scan and paste them into the *Configure Scheduled Scan* window, allowing you to edit the settings for this scheduled scan.

Copy—Copy all settings that were used for the selected scheduled scan and paste them into the *Configure Scheduled Scan* window, allowing you to edit the settings and create an additional scheduled scan.

Enable—Activate a disabled scheduled scan. Requests are enabled, by default, when created.

Disable—Deactivate a scheduled scan. The request remains in the grid, but the scan will not be executed unless the request is enabled prior to the scheduled time and date.

You can also perform additional functions using the icons at the top of the form.

Icon	Function
Add	Schedule a scan. See Scheduled Scan Settings on page 110 for a description of settings.
Delete	Remove the scheduled event.

Resources

Scan Templates

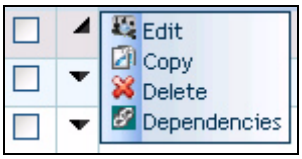
A scan template is any convenient collection of scan settings, potentially including particular macros, that you can reuse when you run scans. This form lists all scan templates that you have permission to view.

For each template, this form displays (by default) the following information:

- Name - The name assigned to the template.
- Security Group - The name of the group.
- Organization Name - The name of the organization to which this group belongs.
- Project Name - The name of the project with which this template is associated.
- Project Version - The version associated with the specified project.

To view or modify details about a template, click the template name.

You can perform additional functions by clicking the drop-down arrow for a specific template.



The functions unique to this menu are:

Edit—Displays the Configure Scan Template form, allowing you to modify the settings defined for the selected template.

Copy—Opens the Configure Scan Template forms, allowing you to modify (if necessary) and save the scan template settings.

Delete—Delete the scan template.

Dependencies—Displays a list of objects (such as scans and scheduled scans) that are linked to this template. You cannot delete this template until you either delete the scheduled scan, assign a different template to the scheduled scan, or cancel the scan (if it is currently running). See Dependencies on page 70 for more information.

You can perform additional functions using the icons at the top of the form.

Icon	Function
Add	Create a template that contains default settings as the base.
Import	Select **Oracle Settings** to create a template that contains settings that are optimized for these sites.
Delete	Delete the selected templates from the list.

Blackouts

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

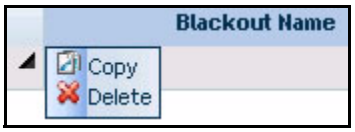
You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

For each blackout defined in the system, the Blackouts form displays (by default) the following information:

- Blackout Name - The identifier for this blackout period.
- Type - Allow or deny scans during this period.
- IP Range - IP address (or range of IP addresses) that are affected by this blackout period.
- Status - Future, or Scans Disallowed, or Scans Allowed.
- Recurrence - One time only, or the defined recurrence pattern.
- Next Occurrence - The date and time when the blackout is next scheduled to start, using the Web Console time zone specified in the Web Console options.
- Next Occurrence (Target) - The date and time when the blackout is next scheduled to start, using the time zone for the location of the target server that is affected by the blackout. This is significant only when the Web Console user and the target server are in different time zones.
- Security Group - Name of the security group with which this blackout is associated.
- Organization - Name of the organization with which this blackout is associated.

To view or modify details about a blackout, click the blackout name.

You can perform additional functions by clicking the drop-down arrow for a specific blackout.



The function unique to this menu is:

Copy—Opens the Configure Blackout form containing blackout settings. You can modify the settings (if desired) and rename the blackout.

You can perform additional functions using the icons at the top of the form.

Icon	Function
Add	Schedule a blackout period. See Blackout Settings on page 111.
Delete	Delete the selected blackout period.

Administration

Deleted Projects

Note: This feature will not appear in the navigation pane until project versions are deleted from SSC and these project versions have scans, scan templates or schedules associated with them.

This form displays, in the left column, a list of project versions that have been removed from HP Fortify Software Security Center. For each version, this form displays:

- The project version name
- The number of issues detected in each of six severity categories

- The name of the security group
- The name of the organization
- The name of the project

Click a version name to view project version details.

System administrators can recover deleted project versions using the Administration - Roles and Permissions feature of the WebInspect Enterprise Administrative Console.

To permanently delete a project version, click the drop-down arrow for a specific project version and select **Purge** (or select one or more project versions and click the **Purge** icon at the top of the form). Purged versions cannot be recovered.

Dependencies

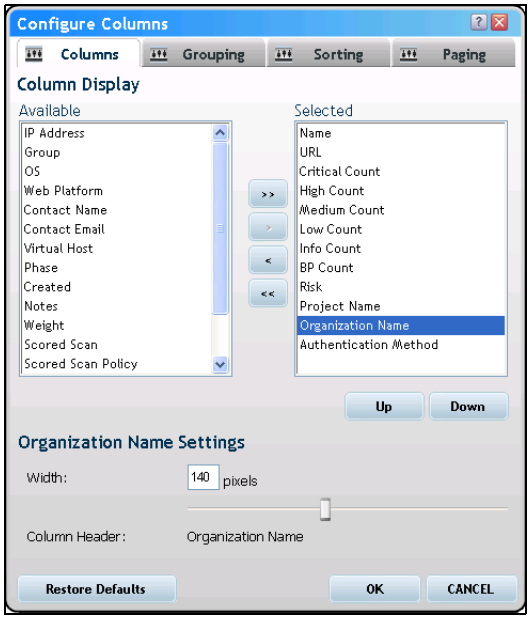
Certain objects in WebInspect Enterprise are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object. For example, if you have a project version that contains scans, you cannot delete that project version unless you first delete the associated scans or assign them to a different project version.

The dependencies are categorized in the following table. Dependent objects must be disassociated from the parent object before the parent object can be deleted.

Parent Object	Dependent Objects
Scan Template	• Scheduled scan • Scan (only if scan has not completed) You cannot delete a scan template until you either delete the scheduled scan, assign a different template to the scheduled scan, or cancel the scan (if it is currently running or paused).
Project Version	Scan You cannot delete a project version until you delete the associated scans or move them to a different project version.
Custom Policy	• Scan • Scheduled scan You cannot delete a custom policy until you either delete the scan or the scheduled scan (or assign a different policy to the scheduled scan).

Editing Form Layouts

Most forms contain an Edit Layout icon  that, when clicked, displays the *Configure Columns* dialog that allows you to change the number of rows on the page, modify column widths, specify which columns are displayed, and sort data by columns.



This dialog has four tabs:

- Columns
- Grouping
- Sorting
- Paging

Columns

Use this tab to specify which columns are displayed on the grid. Column headers listed in the **Selected** list will be displayed. Use the controls illustrated below to move column headers between the **Selected** list and the **Available** list.

To change the column width:

1 Select a column header.

2 Enter a value in the **Width** box (or use the slider to select a width).

3 Click **OK**.

Grouping

You can group objects in views (projects, scans, scan schedules, etc.) according to the available column names. Any grouping you define is applied to every tab on the form you are viewing.

In the following example, scans are grouped by security group and then by policy within each security group.

1 In the navigation pane under Filtered Views, click **Scans**.

2 Click the **Edit Layout** icon .

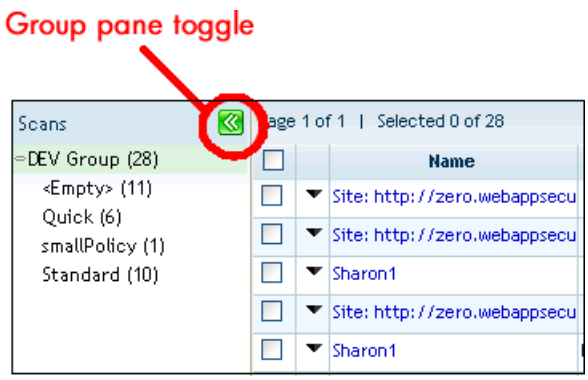
3 On the *Configure Columns* dialog, click the **Grouping** tab.

4 In the **Available** list, select **Security Group** and click >.

5 Select **Policy** and click >. Both column headers are now removed from the **Available** list and appear in the **Selected** list.

6 Click **OK**.

When you return to the **Scans** form, the Group pane displays the grouped results. When you select a group name (such as DEV Group, in this example), WebInspect Enterprise displays only those scans belonging to that group. Redundant items (policy names, in this example) are combined and the number of instances is reported in parentheses following the policy name. You can open or close the pane using the Group pane toggle.



Sorting

To arrange the column data alphabetically, select one or more column headers and then select either **Ascending** or **Descending**.

Paging

To specify the number of rows displayed on a page, select a value from the **Page Size** list.

Scan Visualization

The *Scan Visualization* window emulates the WebInspect graphical presentation of scan data. To open this view, do one of the following:

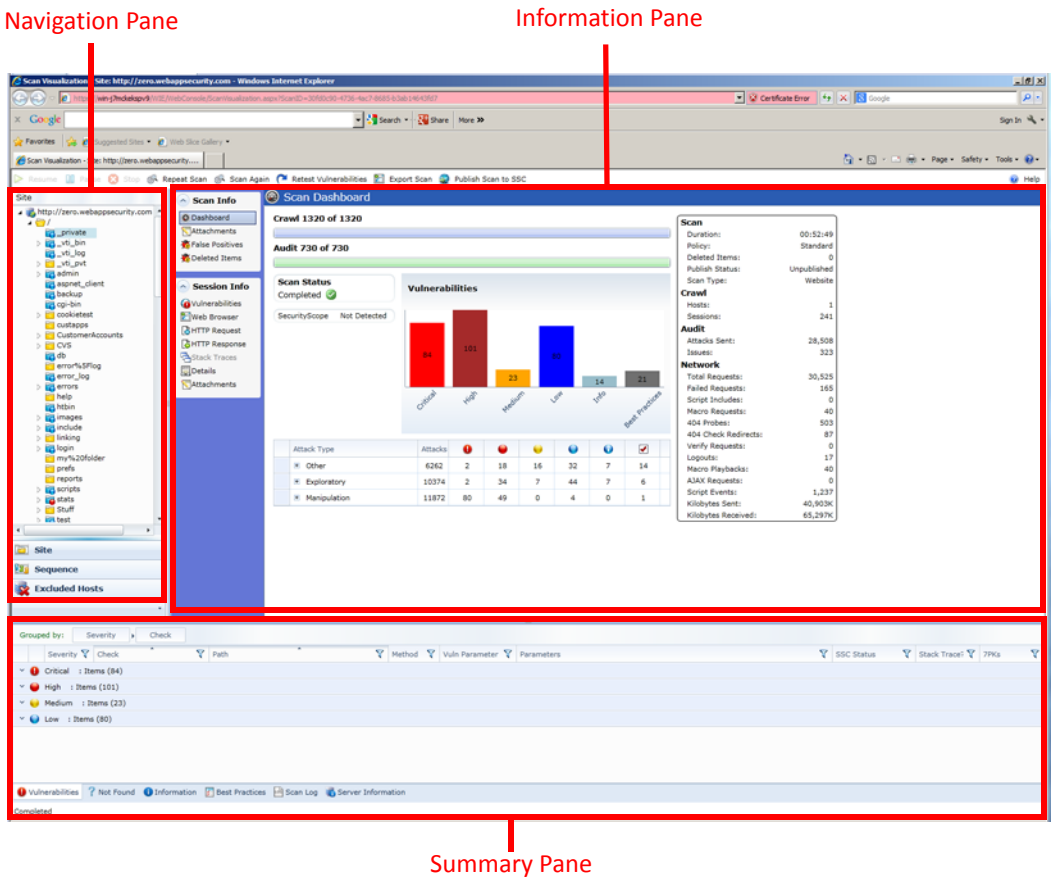
- In the WebInspect Enterprise Web Console, select the **Scans** shortcut from the **Filtered Views** group and click the name of a scan (or click the drop-down arrow for the scan and select **View** → **Scan Visualization**).
- On the Projects tab in SSC, select a project version and click **View Details** (or double-click the project version), click the Scans tab, select a scan, and click **View Scan**. By this method, if you are already working in SSC, you do not need to open WebInspect Enterprise to see the scan results.

The work area of the Scan Visualization window is divided into three regions, as depicted in the following illustration:

• Navigation Pane

• Information Pane

• Summary Pane



Navigation Pane

When conducting or viewing a scan, the navigation pane is on the left side of the *Scan Visualization* window. It includes the **Site**, **Sequence**, and **Excluded Hosts** buttons, which determine the contents (or "view").

Site View

In the Site View, WebInspect Enterprise displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. During the crawl of the site, WebInspect Enterprise selects the check box next to each session (by default) to indicate that the session will also be audited. When conducting a sequential crawl and audit (where the site is completely crawled before being audited), you can exclude a session from the audit by clearing its associated check box before the audit begins.

Sequence View

Sequence view displays server resources in the order they were encountered during a scan.

In both Site view and Sequence view, blue text denotes a directory or file that was identified by WebInspect, rather than a resource that was discovered through a link. For example, WebInspect always submits the request "GET /backup/ HTTP/1.1" in an attempt to discover if the target Web site contains a directory named "backup."

Excluded Hosts View

This view displays a list of all disallowed hosts. These are hosts that may be referenced anywhere within the target site, but cannot be scanned because they are not specified in the Allowed Hosts' Scan Settings.

Navigation Pane Icons

Use the following table to identify resources displayed in the Sequence and Site views.

Icons Used on the Navigation Pane

Icon	Definition
	Server/host: Represents the top level of your site's tree structure.
	Blue folder: A private folder discovered not by crawling, but by attacks that often reveal vulnerabilities.
	Yellow folder: A folder whose contents are available over your Web site.
	Grey folder: A folder indicating the discovery of an item via path truncation. Once the parent is found, the folder will display in either blue or yellow, depending on its properties
	File.
	Query or Post.
	Document Object Model (DOM) event.

Icons Used on the Navigation Pane (cont'd)

Icon	Definition
Icons superimposed on a folder or file indicate a discovered vulnerability	
	A red dot with an exclamation point indicates the object contains a critical vulnerability. An attacker might have the ability to execute commands on the server or retrieve and modify private information.
	A red dot indicates the object contains a high vulnerability. Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
	A gold dot indicates the object contains a medium vulnerability. These are generally non-HTML errors or issues that could be sensitive.
	A blue dot indicates the object contains a low vulnerability. These are generally interesting issues, or issues that could potentially become higher ones.
	An "i" in a blue circle indicates an informational item. These are interesting points in the site, or certain applications or Web servers.
	A red check mark indicates a "best practice" violation.

Each object represents a session, which is a matched set comprising the HTTP request sent by WebInspect to test for vulnerabilities and the HTTP response from the server.

Navigation Pane Shortcut Menu

If you right-click an item in the navigation pane while using the Site view, a shortcut menu presents the following commands:

Navigation Pane Shortcut Commands

Command	Definition
Expand Children	Expands branching nodes in the site tree.
Collapse Children	Contracts branching nodes into the superior node.
Copy URL	Copies the URL of the selected session to the clipboard (the same as selecting **Edit** → **Copy URL**).
View in Browser	Displays the server's HTTP response in a Web browser.

Navigation Pane Shortcut Commands (cont'd)

Command	Definition
Add	Allows you to add a page, directory, or vulnerability discovered by means other than a WebInspect scan (manual inspection, other tools, etc.) for information purposes. You can then add vulnerabilities to those locations so that a more complete picture of the site is archived for analysis. • **Page** - A distinct URL (resource). • **Directory** - A folder containing a collection of pages. Choosing either **Page** or **Directory** invokes a dialog that allows you to name the page or directory and edit the HTTP request and response. • **Variation** - A subnode of a location that lists particular attributes for that location. For example, the login.asp location might have the variation: "(Query) Username=12345&Password=12345&Action=Login" Variations, like any other location. can have vulnerabilities attached to them, as well as subnodes. Choosing **Variation** invokes the *Add Variation* dialog, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response. • **Vulnerability** - A specific security threat. Choosing **Vulnerability** invokes the *Edit Vulnerabilities* dialog, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.
Remove Location	Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities. Note: You can recover removed locations (sessions) and their associated vulnerabilities. Select **Deleted Items** from the Scan Info panel.
Edit Vulnerability	Allows you to add an existing or custom vulnerability to the session, or change the Summary, Implication, Execution, Fix, and Reference Info descriptions associated with the vulnerability.
Review Vulnerability	Allows you to retest the vulnerability or mark it as "ignored" or "false positive." For more information, see Reviewing and Retesting Vulnerabilities on page 82.
Mark as False Positive	Flags the vulnerability as a false positive and allows you to add a note.
Attachments	Allows you to create a note or snapshot associated with the selected vulnerability.

Information Pane

When conducting or viewing a scan, the information pane contains two collapsible information panels (Scan Info and Session Info) and an information display area.

Scan Info Panel

This panel contains the following selections: Dashboard, Attachments, False Positives, and Deleted Items.

Dashboard

The Dashboard displays a summary of the scan results and a graphic representation of the scan progress.

The following table describes the graphics used in the Dashboard.

Dashboard Graphics

Graphic	Explanation
Crawl Gauge	Number of sessions crawled, of the total number of sessions for crawl.
Audit Gauge	Number of sessions audited, of the total number of sessions for audit.
Scan Status	Status: Running, Paused, or Completed.
SecurityScope field	Not Detected or Detected. If SecurityScope is detected, it can provide stack traces for certain checks. For more information, see Session Info Panel on page 78 and Project Version Details on page 59.
Vulnerabilities Graph	Total number of issues identified for the scan sorted by severity level.
Attack Stats Grid	Number of attacks made and issues found, categorized by attack type and audit engine.

The following table describes the statistics presented in the Dashboard.

Dashboard Statistics

Group	Statistic	Explanation
Scan	Duration	Length of time scan has been running (can be incorrect if the scan terminates abnormally).
	Policy	Name of the policy used for the scan. For a retest, the field contains a dash (-), because the retest does not use the entire policy.
	Deleted Items	Number of sessions and vulnerabilities removed by the user from the scan.
	Publish Status	Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC.
	Scan Type	Website or Web Service.
Crawl	Hosts	Number of hosts included in the scan.
	Sessions	Total number of sessions (excluding AJAX requests, script and script frame includes, WSDL includes).
Audit	Attacks Sent	Total number of attacks sent.
	Issues	Total number of issues found (all vulnerabilities, as well as best practices).
Network	Total Requests	Total number of requests made.
	Failed Requests	Total number of failed requests.
	Script Includes	Total number of script includes.

Dashboard Statistics (cont'd)

Group	Statistic	Explanation
	Macro Requests	Total number of requests made as part of macro execution.
	404 Probes	Number of probes made to determine file-not- found status.
	404 Check Redirects	Number of times a 404 probe resulted in a redirect.
	Verify Requests	Requests made for detection of stored parameters.
	Logouts	Number of times logout was detected and login macro executed.
	Macro Playbacks	Number of times macros have been executed.
	AJAX Requests	Total number of AJAX requests made.
	Script Events	Total number of script events processed.
	Kilobytes Sent	Total number of kilobytes sent.
	Kilobytes Received	Total number of kilobytes received.

Attachments

This feature lists all the notes and screenshots that are associated with all the objects in the scan. Attachments are added in the Session Info panel for individual objects, as described in Session Info Panel on page 78.

False Positives

This feature lists all URLs that WebInspect Enterprise originally flagged as containing a vulnerability, but which a user later determined were false positives.

Deleted Items

This feature lists either deleted sessions or deleted vulnerabilities, depending on your selection.

To delete a session, right-click a session in the navigation pane or an item in the summary pane and select **Remove Location** from the shortcut menu.

To delete a vulnerability, you can do the following:

- Right-click an item on the **Vulnerabilities** tab, **Information** tab, or **Best Practices** tab in the summary pane and select **Mark As Ignored** from the shortcut menu.
- Right-click a vulnerable session in the navigation pane, select **Edit Vulnerability** from the shortcut menu, and (on the *Edit Vulnerabilities* dialog) click **Delete**.
- Right-click an item on any tab in the summary pane except **Scan Log**, select **Edit Vulnerability** from the shortcut menu, and (on the *Edit Vulnerabilities* dialog) click **Delete**.

Session Info Panel

WebInspect lists each session created during a scan in the navigation pane using either the Site view or Sequence view. Select a session and then click one of the options in the **Session Info** panel to display related information about that session.

The following table lists the options available in the **Session Info** panel. Some options appear only for specific scans (Web Site Scan or Web Service Scan). Also, options are enabled only if they are relevant to the selected session.

Options in Session Info Panel

Option	Definition
Vulnerabilities	Displays the vulnerability information for the session selected in the navigation pane.
Web Browser	Displays the server's response as rendered by a Web browser for the session selected in the navigation pane. For Web Site scans only; not available for Web Service scans.
HTTP Request	Displays the raw HTTP request sent by WebInspect to the server hosting the site you are scanning.
HTTP Response	Displays the server's raw HTTP response to WebInspect's request. Note: If you select a Flash (.swf) file, WebInspect displays HTML instead of binary data. This allows WebInspect to display links in a readable format.
Stack Traces	Displays stack traces provided for certain checks by SecurityScope, if SecurityScope is detected to be available. For more information, see Dashboard on page 77 and Project Version Details on page 59.
Details	Displays request and response details, such as the size of the response and the request method, for the session selected in the navigation pane. Note that the Response section contains two entries for content type: returned and detected. The **Returned Content Type** indicates the media type specified in the Content-Type entity-header field of the HTTP response. The **Detected Content Type** indicates the actual content-type as determined by WebInspect Enterprise.
Attachments	Displays all notes and screenshots associated with the object selected in the navigation pane (Site or Sequence view). To create an attachment, you can do one of the following: • Right-click a session (Web site scan) or an operation or vulnerability (Web service scan) in the navigation pane and select **Attachments** from the shortcut menu. • Right-click an item on the **Vulnerabilities** tab of the summary pane and select **Attachments** from the shortcut menu. • Select a session (Web site scan) or an operation or vulnerability (Web service scan) in the navigation pane, then select **Attachments** from the Session Info panel and click the **Add** menu (in the information pane).

Summary Pane

When conducting or viewing a scan, use the horizontal summary pane at the bottom of the window to see a centralized display of discovered vulnerabilities. It allows you to access vulnerability information quickly and view WebInspect logging information.

To select the information you want to display, right-click any column header and choose **Columns** from the shortcut menu. The available columns are:

- Severity: A relative assessment of the vulnerability, ranging from low to critical. See below for associated icons.
- Check: A WebInspect probe for a specific vulnerability, such as cross-site scripting, unencrypted log-in form, etc.

- Path: The hierarchical path to the resource.
- Method: The HTTP method used for the attack.
- Vuln Param: The name of the vulnerable parameter.
- Parameters: Names of parameters and values assigned to them.
- Reproducible: Values may be Reproduced, Not Found/Fixed, or New. Column is available for Site Retests only (Retest Vulnerabilities).
- SSC Publish Status: The status as it exists in Software Security Center, if previously published.
- SSC Status: Expected status of the vulnerability when the scan is published to SSC.
- Stack Trace?: Whether or not a stack trace exists for the vulnerability.
- CWE ID: The Common Weakness Enumeration identifier(s) associated with the vulnerability.
- 7PKs: The category in which this vulnerability is classified, using a taxonomy of software security errors developed by the HP Fortify Software Security Research Group.

The summary pane has the following tabs:

- Vulnerabilities
- Not Found
- Information
- Best Practices
- Scan Log
- Server Information

On all tabs, you can filter the data that is presented by clicking on the icons in the column headers.

Vulnerabilities Tab

The **Vulnerabilities** tab lists information about each vulnerability that WebInspect discovered during an audit of your Web presence.

The severity of vulnerabilities is indicated by the following icons.

Critical	High	Medium	Low
			

With a session selected, you can also view associated information by selecting an option from the Session Info panel.

If you right-click an item in the list, a shortcut menu displays the following commands.

Vulnerability Shortcut Menu

Command	Definition
Export All Vulns	Creates a comma-separated values (.csv) file containing all items and displays it in Microsoft Excel.
Change Severity	Change the severity level.
Edit Vulnerability	Display the *Edit Vulnerabilities* dialog, allowing you to modify various vulnerability characteristics.

Vulnerability Shortcut Menu (cont'd)

Command	Definition
Review Vulnerability	Retest the vulnerable session, or mark it as false positive or ignored. For more information, see Reviewing and Retesting Vulnerabilities on page 82. This option is also invoked if you double-click a vulnerability.
Mark As	Flag the vulnerability as either a false positive or ignored. In both cases, the vulnerability is removed from the list. To view a list of all false positives, click **False Positives** in the Scan Info panel. Note: To view (and optionally recover) deleted sessions and vulnerabilities, click **Deleted Items** in the Scan Info panel.
Remove Location	Delete from the navigation pane the session associated with the selected vulnerability and also remove any associated vulnerabilities. Note: To view (and optionally recover) removed sessions, select **Deleted Items** in the Scan Info panel.
Attachments	Create a note or associate an image with the selected vulnerability.
Update SSC Status	Change the status of an issue to be submitted to SSC. Statuses are: New, Existing, Reintroduced, Resolved, Still an Issue, and Not Found. The availability of a specific status is determined by the current status.

Not Found Tab

This tab lists vulnerabilities that were detected by a previous scan in this project version, but were not detected by the current scan. These vulnerabilities are not included in counts on the Dashboard and are not represented in the site or sequence view of the navigation pane. Right-clicking an item in the list presents the same options described for the Vulnerability Shortcut Menu on page 80.

Information Tab

The **Information** tab lists information discovered during a WebInspect scan. These are not considered vulnerabilities. They simply identify interesting points in the site or certain applications or Web servers. When you click a listed URL, the related item in the navigation pane is highlighted.

Right-clicking an item in the list presents the same options described for the Vulnerability Shortcut Menu on page 80.

Best Practices Tab

The **Best Practices** tab lists issues detected by WebInspect that relate to commonly accepted best practices for Web development. Items listed here are not vulnerabilities, but are indicators of overall site quality and site development security practices (or lack thereof).

Right-clicking an item in the list presents the same options described for the Vulnerability Shortcut Menu on page 80.

Scan Log Tab

Use the **Scan Log** tab to view information about activities that occurred during the scan. For instance, the time at which certain audit methodologies are applied against your Web presence are listed here.

Server Information Tab

This tab lists items of interest pertaining to the server. Only one occurrence of an item or event is listed per server.

Reviewing and Retesting Vulnerabilities

After you conduct a scan and report discovered vulnerabilities, developers may correct their code and update the site. You can then open the original scan, select the once-vulnerable session (now supposedly remediated), and select **Review Vulnerability** from the shortcut menu. Assuming that the fundamental architecture of the site has not changed, you can verify that the threat no longer exists without rescanning the entire site (which, in some cases, could require several hours or even days).

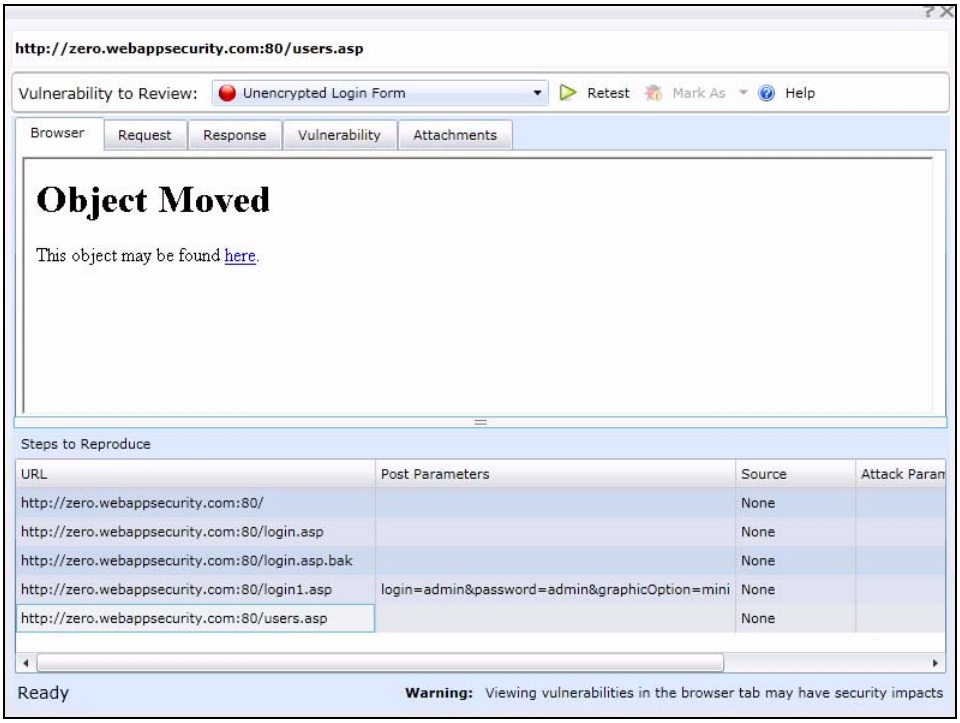
You can use this feature simply to double-check a reported vulnerability, even while the scan is still running.

1 Do one of the following:

- Right-click a vulnerable session in the navigation pane and select **Review Vulnerability**.
- In the summary pane, select either the **Vulnerability**, **Not Found**, **Information**, or **Best Practices** tab, right-click an item in the list, and select **Review Vulnerability**.

2 If multiple vulnerabilities are displayed, select one from the **Vulnerability to Review** list.

In the following illustration, the Unencrypted Login Form check was selected from the summary pane of the *Scan Visualization* window.



3 Use the tabs to display information about the original session (as selected in the **Steps to Reproduce** pane under the URL column):

- **Browser** - The server's response, as rendered in a browser.

Note: This tab may or may not be visible. Retesting a cross-site scripting vulnerability may cause the script to loop infinitely on the **Browser** tab when using Microsoft Internet Explorer. Using the WebInspect Enterprise Administrative Console, the organization administrator can disable this tab. See Configuration Tab on page 42.

- **Request** - The raw HTTP request message.
- **Response** - The raw HTTP response message.
- **Vulnerability** - A description of the vulnerability, its implications, and suggestions on how to fix it.
- **Attachments** - Notes and screenshots associated with the vulnerability, which you may add, view, edit, or delete.

To retest the session for the selected vulnerability:

1. Click **Retest**.
2. Select a sensor and click **OK**.

Results of the retest appear on the Status bar and in the lower pane in the **Response Match Status** column. The remaining client area is split into two panes: the original session is represented in the left pane, and the retested session appears in the right pane.

The status is reported as either "Vulnerability Detected" or "Vulnerability Not Detected."

The reliability of the reported findings is mitigated by the Response Match Status, which may have the following values:

- Match - The resource has not changed significantly; WebInspect Enterprise was able to access the session via the same path used by the original scan.
- Inconclusive - Based on the HTTP response, the resource has changed in a manner that may or may not substantiate the finding that a vulnerability has or has not been detected during the retest.
- Different - The HTTP response is radically different from the response received during the original scan, suggesting major changes to the resource.

If you think that WebInspect Enterprise has erroneously determined that the vulnerability exists, you can remove the vulnerability by clicking **Mark as** and selecting **False Positive** from the drop-down list. Alternatively, you can ignore the vulnerability by selecting **Ignored**.

Editing and Adding Vulnerabilities

After WebInspect Enterprise assesses your application's vulnerabilities, you may want to edit and save the results for a variety of reasons, including:

- Security - If an HTTP request or response contains passwords, account numbers, or other sensitive data, you may want to delete or modify this information before making the scan results available to other persons in your organization.
- Correction - WebInspect Enterprise occasionally reports a "false positive." This occurs when WebInspect Enterprise detects indications of a possible vulnerability, but further investigation by a developer determines that the problem does not actually exist. You can delete the vulnerability from the session or delete the entire session. Alternatively, you can designate it as a false positive; to do so, right-click the session in either the Site or Sequence view and select Mark As False Positive.
- Severity Modification - If you disagree with WebInspect Enterprise's ranking of a vulnerability, you can assign a different level.
- Record Keeping - You can modify any of the report fields associated with an individual vulnerability (Summary, Execution, Recommendation, Implementation, Fixes, and References). For example, you could add a paragraph to the Fixes section describing how you actually fixed the problem.

- Enhancement - If you discover a new vulnerability, you could define it and add it to a session as a custom vulnerability.

Use the procedure below to edit or add a vulnerability.

1. Do one of the following:
   - In the summary pane, right-click an item on any tab except **Scan Log** or **Server Information,** and select **Edit Vulnerability**.
   - In the navigation pane, right-click a session and select **Edit Vulnerability** or **Add** → **Vulnerability**.
2. Select a vulnerability (if the session includes multiple vulnerabilities).
3. To add an existing vulnerability to the session (that is, one that exists in the database), click **Add Existing**.
   a. On the *Add Existing Vulnerability* window, enter part of a vulnerability name, or a complete vulnerability ID number or type.

      Note: The * and % characters can be used interchangeably as wildcards. However, a wildcard is allowed only at the beginning, at the end, or at the beginning and end of a string. If placed within a string (such as "mic*soft,"), these characters will not function as wildcards.

   b. Click **Search**.
   c. Select one or more of the vulnerabilities returned by the search.
   d. Click **OK**.
4. To add a custom vulnerability**,** click **Add Custom**. You can then edit the vulnerability as described in step 6.
5. To delete the vulnerability from the selected session, click **Delete**.
6. To edit the vulnerability, you can modify the check name, check type, severity, or probability. You can also change the descriptions that appear on the **Summary**, **Implication**, **Execution**, **Fix**, and **Reference Info** tabs.
7. Click **OK** to save the changes.

To remove any modifications you made to existing vulnerability descriptions, select a check name and click **Restore Defaults**.

Toolbar

Actions available from the toolbar at the top of the window include the following:

- **Resume** - Continue a scan after you paused the process.
- **Pause** - Halt a scan. Click **Resume** to continue.
- **Stop** - Terminate the scan; it cannot be resumed.
- **Repeat Scan** - Rescan the target site using the same settings as the original scan.
- **Scan Again** - Display settings used for this scan, allowing you to modify them before initiating another scan.
- **Retest Vulnerabilities** - This type of scan examines only those portions of the target site in which vulnerabilities were detected during the original scan. WebInspect Enterprise does not conduct a new crawl of the site, but simply retraces the path of vulnerable sessions (as recorded in the original scan) and attacks the resources using the same checks previously employed. The default name of the scan is

"Site Retest - <original scan name>"; for example, the retest of a site that originally resulted in a scan named MySite would produce a scan named Site Retest - MySite. However, you can specify a different name when launching the scan.

- **Export Scan** - Export the selected scan (or settings for the selected scan) to a destination you select.
- **Publish Scan to SSC** - Send scan data to SSC. For more information, see Publishing Scans to Software Security Center on page 62.

Guided Scan

Guided Scan is the preferred alternative to the standard Web Site scan. Guided Scan directs you through the best steps to configure a scan that is tailored to your application. The first time you launch Guided Scan in WebInspect Enterprise or Software Security Center, the Guided Scan client application, which includes its own Help system, is downloaded and installed on your local computer. For detailed information, see Chapter 5, Guided Scan.

Web Site Scan Wizard

The Web Site Scan Wizard steps you through the process of creating settings for a Web site scan (known in WebInspect as a Basic Scan). The options displayed by default on this and subsequent windows are extracted from the Advanced Settings. Any changes you make will be used for the current scan only. When each dialog appears, provide the requested information as described in the following procedure.

To start the Web Site Scan Wizard, do one of the following:

- Click **Scan Web Site** in the Actions section of the navigation pane in the WebInspect Enterprise Web Console.
- In SSC, select a project version on the Projects tab and click **New Scan** in the Quick Links section. In this case, the **Project** and **Project Version** on the first screen of the scan are automatically populated.

Click **Advanced Settings** at the bottom of any dialog in the wizard to access the full complement of WebInspect Enterprise settings. Any selections you make will be applied to this scan only, and you will not be able to return to the Scan Wizard. See Advanced Scan Settings on page 90.

Web Site Scan

1. Select a **Project** and a **Project Version** from the appropriate lists.
2. In the **Scan Name** box, enter a name or brief description of the scan.
3. Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Scan Template** list. You are not required to use a template. At the end of the Web Site Scan Wizard, you can save the options you have selected as a new template.
4. Select one of the following scan modes:
   - **Crawl Only**: This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click Audit to assess an application's vulnerabilities.

- **Crawl & Audit**: WebInspect maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see SCAN SETTINGS on page 92.
- **Audit Only**: WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

5 Select one of the following scan types:

Standard Scan

WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

a In the **Start URL** box, type or select the complete URL or IP address of the site you want to examine.

If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, WebInspect will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

Scans by IP address will not pursue links that use fully qualified URLs (as opposed to relative paths).

WebInspect supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets.

b If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:

- **Directory only (self)** - WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, WebInspect will assess only the “two” directory.
- **Directory and subdirectories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

List-Driven Scan

Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as a comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility.

If you select **List-Driven Scan**, do one of the following:

- Click **Import** and select a text file or XML file containing the list of URLs you want to scan.
- Click **Manage** to create or modify a list of URLs.

Workflow-Driven Scan

The scanner audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan.

If you select **Workflow-Driven Scan**, do one of the following:

- To select a macro containing the URLs you want to scan, click **Import**.
- To import or remove a macro and to specify allowed hosts, click **Manage**.
- To create a workflow macro, if you have access to the WebInspect Enterprise Administrative Console, click **Tools** → **Workflow Macro Recorder**. See Web Macro Recorder (Unified) on page 264.

6 Click **Next**.

Authentication and Connectivity

1 If you need to access the target site through a proxy server, select **Network Proxy** and then choose an option from the Proxy Profile list.

Note: Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

- **Autodetect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
- **Use Internet Explorer proxy settings on the sensor machine**: Import your proxy server information from Internet Explorer, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured, not on the local system.
- **Use PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **Edit** to enter the location (URL) of the PAC.
- **Use Explicit Proxy Settings**: Specify proxy server settings. If you select this option, click **Edit** to enter proxy information.
- **Use Mozilla Firefox proxy settings on the sensor machine**: Import your proxy server information from Firefox, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured, not on the local system.

2 Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.

3 Select **Site Authentication** to use a recorded macro containing a user name and password that allows you to log on to the target site. The macro must also contain a "logout condition," which indicates when an inadvertent logout has occurred so WebInspect Enterprise can rerun this macro to log on again.

- To browse to select a previously recorded login macro, click  .
- To create a login macro, from the WebInspect Enterprise Administrative Console, click **Tools** → **Login Macro Recorder**. See Web Macro Recorder (Unified) on page 264.
- To remove the login macro name, if any, clear the **Site Authentication** check box.
- A table appears if input parameters were used when the macro was recorded using the Web Macro Recorder (see Web Macro Recorder (Unified) on page 264 and Using Name and Password Parameters on page 282) or if Smart Credentials were used when the macro was created using the Event-Based IE Compatible Web Macro Recorder (see Event-Based IE Compatible Web Macro Recorder (Hidden) on page 252 and Macro Settings on page 262).

Enter a user name and password. When scanning the page containing the input control associated with this entry, WebInspect Enterprise will substitute these credentials for those used in the macro. This feature allows you to create a macro using your user name and password, yet when other persons run the scan using this macro, they can substitute their own user credentials.

4 Click **Next**.

Coverage and Thoroughness

1 Select a policy from the **Audit Depth (Policy)** list.

For descriptions of policies, see Appendix A, Policies.

2 If you want WebInspect to submit values for input controls on forms it encounters while scanning the target site:

a Select **Auto-fill Web forms during crawl**. WebInspect will extract the values from a file that you create using the Web Form Editor.

b Click **Load** to locate and load the file.

3 Click **Next**.

Congratulations

1 If you want to create a template containing the settings you configured for this scan, specify a template name and click **Save**.

2 Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

3 Select a sensor. You can designate a specific sensor to run this scan, or you can elect to run the scan on any available sensor.

4 Click **Scan**.

Note that even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

When the scan completes, the Scan Visualization appears. For detailed information, see Scan Visualization on page 73.

Web Service Scan Wizard

The Web Service Scan Wizard steps you through the process of creating settings for a Web service scan. The options displayed by default on this and subsequent windows are extracted from the Advanced Settings. Any changes you make will be used for the current scan only. When each dialog appears, provide the requested information as described in the following procedure.

To start the Web Service Scan Wizard, click **Scan Web Service** in the Actions section of the navigation pane in the WebInspect Enterprise Web Console.

Click **Advanced Settings** at the bottom of any dialog in the wizard to access the full complement of WebInspect Enterprise settings. Any selections you make will be applied to this scan only, and you will not be able to return to the Scan Wizard.

Web Service Scan

1. Select a project and project version from the appropriate lists.
2. In the **Scan Name** box, enter a name or brief description of the scan.
3. Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Scan Template** list. You are not required to use a template.
4. Click **Import** to open a standard file-selection dialog and choose a Web Service Test Design (WSD) file that you previously created using the Web Service Test Designer. This file contains values for each operation in the service. For more information, see Web Service Test Designer on page 296.
5. Click **Next**.

Authentication and Connectivity

1. If you need to access the target site through a proxy server, select **Network Proxy** and then choose an option from the **Proxy Profile** list.

   Note: Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

   - **Autodetect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
   - **Use Internet Explorer proxy settings on the sensor machine**: Import your proxy server information from Internet Explorer, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured, not on the local system.
   - **Use PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **Edit** to enter the location (URL) of the PAC.
   - **Use Explicit Proxy Settings**: Specify proxy server settings. If you select this option, click **Edit** to enter proxy information.
   - **Use Mozilla Firefox proxy settings on the sensor machine**: Import your proxy server information from Firefox, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured, not on the local system.
2. Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.
3. Click **Next**.

Coverage and Thoroughness

You cannot select a policy. The Simple Object Access Protocol (SOAP) policy is used by default.

Click **Next**.

Congratulations

1. If you want to create a template containing the settings you configured for this scan, specify a template name and click **Save**.
2. Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.
3. Select a sensor. You can designate a specific sensor to run this scan, or you can elect to run the scan on any available sensor.
4. Click **Scan**.

Note that even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

When the scan completes, the Scan Visualization appears. For detailed information, see Scan Visualization on page 73.

Advanced Scan Settings

To access advanced scan settings, click **Advanced Settings** at the lower left of the Web Site Scan Wizard or the Web Service Scan Wizard. The following categories of advanced scan settings are grouped on the left:

- SCAN
- SCAN SETTINGS
- CRAWL SETTINGS
- AUDIT SETTINGS
- SCAN BEHAVIOR
- EXPORT

Each group has one or more subcategories.

SCAN

General

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan

Enter a name for the scan.

Scan URL

Select one of the following scan types.

- Standard Scan

  The scanner performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

  1. In the **URL** box, type or select the complete URL or IP address of the site you want to examine.

     If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, you will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

     An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

     Scans by IP address will not pursue links that use fully qualified URLs (as opposed to relative paths).

     WebInspect supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets.

  2. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:

     – **Directory only (self)** - The scanner will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, the scanner will assess only the "two" directory.

     – **Directory and subdirectories** - The scanner will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.

     – **Directory and parent directories** - The scanner will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

- List-Driven Scan

  Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as a comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility. Do one of the following:

  — Click **Browse** and select a text file or XML file containing the list of URLs you want to scan.

  — Click **View** to view the contents of the selected file.

- Workflow-Driven Scan

  The scanner audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application.

  Click **Browse** and select a macro containing the URLs you want to scan.

- Web Service Scan

  When performing a Web Service scan, the scanner crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

  Click **Browse** to open a standard file-selection dialog and choose a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Priority

Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

Sensor

Select which sensor should conduct the scan. You can choose a specific sensor or select the **Any Available** option.

A sensor can perform only one scan at a time. If it is conducting a scan when another scan is scheduled to occur, then:

- If the currently running scan has a higher priority, the WebInspect Enterprise manager will place the second scheduled scan request in a queue until the first scan finishes or until another sensor becomes available.
- If the currently running scan has a lower priority, the WebInspect Enterprise manager will suspend that scan, assign the second scheduled scan request to that sensor, and then reassign the suspended request to the sensor when the higher priority scan is complete.

Scans that are manually initiated have priority over any scheduled scan.

SCAN SETTINGS

The Project Version setting is reproduced on each settings dialog, allowing you to change your selection at any point. The description of this setting is not repeated in the following topics.

Method

Scan Mode

Select one of the following modes:

- **Crawl Only**—This option completely maps a site's hierarchical data structure, but does not audit the site. The scan is saved to the database, allowing you to open the scan at a later date and conduct an audit.
- **Crawl and Audit**—In this mode, the scanner crawls the entire site, mapping the site's hierarchical data structure, and conducting an audit.
- **Audit Only**—The scanner applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

If the selected scan mode is Crawl and Audit, choose one of the following:

- **Simultaneously**—As a scanner maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed.
- **Sequentially**—In this mode, the scanner crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root. If you select this option, you can specify the order in which the crawl and audit should be conducted.
  - **Test each engine type per session (engine driven)**: The scanner audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.

— **Test each session per engine type (session driven)**: The scanner runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Scan Behavior

You can select any of the following optional behaviors:

- **Use a login macro for forms authentication**—This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent the HP scanner from terminating prematurely if it inadvertently logs out of your application. The drop-down list contains the names of all macros that have been uploaded to WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.

  If you specified login parameters when recording the macro, the scanner will substitute these credentials for those used in the macro when it scans a page containing the input control associated with this entry.

- **Use a startup macro**—This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that the scanner will use to navigate to that area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application. The scanner visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). The drop-down list contains the names of all macros that have been uploaded to WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.

- **Auto-fill Web forms during crawl**—If you select this option, the scanner submits values for input controls found on all HTML forms it encounters while scanning the target site. The scanner will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. Use the **Browse** button to specify the file containing the values you want to use. Alternatively, you can select **Edit** (to modify the currently selected file) or **Create** (to record new Web form values).

General

Scan Details

You may choose the following options:

- **Enable Path Truncation**—Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. The scanner truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ will cause the server to reveal directory contents or will cause unhandled exceptions.

- **Attach debug information in request header**—If you select this option, the scanner includes a "Memo:" header in the request containing information that can be used by support personnel to diagnose problems.

- **Case-sensitive request and response handling**—Select this option if the server at the target site is case-sensitive to URLs.

- **Compress response data**—If you select this option, the scanner saves disk space by storing each HTTP response in a compressed format in the database.

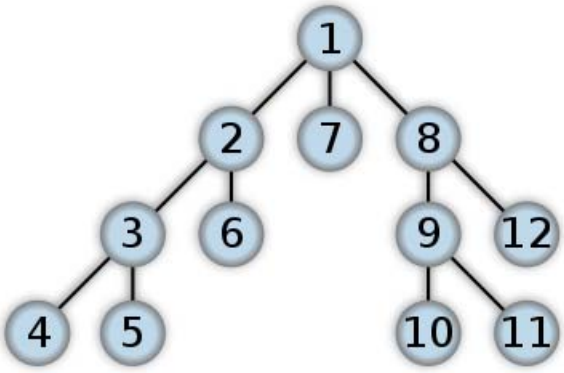
- **Maximum crawl-audit recursion depth**—When an attack reveals a vulnerability, the scanner crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The maximum value is 1000.

Crawl Details

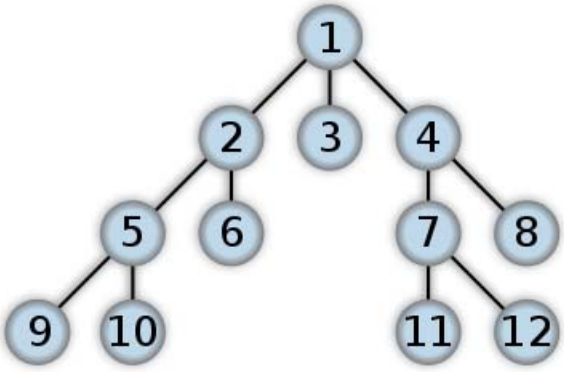
You may choose the following options:

- **Crawler**—Select either **Depth First** or **Breadth First**.

  Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.



  By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



  When performing a depth-first crawl, the scanner pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a "shopping cart" page before accessing the "check-out" page).

- **Enable keyword search audit**—A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.

- **Perform redundant page detection**—Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, scanners would never be able to finish the scan. This option, however, allows scanners to identify and exclude processing of redundant resources.
- **Limit maximum single URL hits to**—Use this field to limit the number of times a single link will be followed during a crawl. Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL.
- **Include parameters in hit count**—If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.

  For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice).
- **Limit maximum link traversal sequence to**—This option restricts the number of hyperlinks that can be sequentially accessed as the scanner crawls the site. For example, if five resources are linked as follows

  Page A contains a hyperlink to Page B

  Page B contains a hyperlink to Page C

  Page C contains a hyperlink to Page D

  Page D contains a hyperlink to Page E

  and if this option is set to “3,” then Page E will not be crawled. The default value is 15.
- **Limit maximum crawl folder depth to**—The Crawl Depth value determines how deeply the scanner traverses the hierarchical levels of your Web site. If set to 1, the scanner drills down one level; if set to 2, the scanner drills down two levels; and so on. The maximum value is 1000.
- **Limit maximum crawl count to**—This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.
- **Limit maximum Web form submissions to**—Normally, when the scanner encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed.

  There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named “State” contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form.

  Use this setting to limit the total number of submissions that the scanner will perform.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

Content Analyzers

JavaScript/VBScript—The JavaScript/VBScript analyzer is always enabled. It allows the scanner to crawl links defined by JavaScript or VisualBasic script, and to create and audit any documents rendered by JavaScript. There are settings associated with the JavaScript/VBScript content analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described below.

Flash—If you enable the Flash analyzer, the scanner analyzes Flash files, Adobe's vector graphics-based resizable animation format. There are no associated settings.

Silverlight—If you enable the Silverlight analyzer, the scanner analyzes the multimedia, graphics, animation, and interactivity elements developed within Microsoft's Silverlight Web application framework. There are no associated settings.

Parser Settings

- **Crawl links found from script execution**—If you select this option, the crawler will follow dynamic links (that is, links generated during execution of JavaScript or Visual Basic script).
- **Reject script includes to offsite hosts**—Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is:

  <script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>

  The scanner will download and parse such files, regardless of their origin or file type, unless you select this option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).
- **Isolate script analysis (out-of-process execution)**—The scanner analyzes and executes JavaScript and VBScript to discover links to other resources. Applications or Web sites containing an inordinate number of links can sometimes exhaust the amount of memory allocated to this process. If this occurs, you can assign this function to a separate (remote) process, which will accommodate an infinite number of links. You may, however, notice a slight increase in the amount of time required to scan the site.
- **Create DOM sessions**—The scanner creates and saves a session for each change to the Document Object Model (DOM).
- **Verbose Script Parser Debug Logging**—If you select this setting *and* if the Application setting for logging level is set to Debug, the scanner logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
- **Log JavaScript Errors**—The scanner logs JavaScript parsing errors from the script parsing engine.
- **Maximum script events per page**—Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999.

Requestor

Requestor Performance

Select one of the following:

- **Use a shared requestor**—The crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of HP scanners and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
- **Use separate requestors**—The crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans. You also specify the maximum number of threads that can be created for each requestor. The crawl requestor can be configured to send up to 25 concurrent HTTP

requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 50. Increasing the thread count will increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

Tip: While most servers can handle a large number of requests, servers in development environments sometimes have limitations on their licensing that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5. Failing to do so may mean that the scanner does not accurately crawl or audit the site because requests are being rejected by the server.

Requestor Settings

You may select the following options:

- **Limit maximum response size to**—Select this option to limit the size of accepted server responses and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
- **Request retry count**—Specify how many times the scanner will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout).
- **Request timeout**—Specify how long the scanner will wait for an HTTP response from the server. If this threshold is exceeded, the scanner resubmits the request until reaching the retry count. If it then receives no response, the scanner logs the timeout and issues the first HTTP request in the next attack series.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct the scanner to terminate a scan by specifying a threshold for the number of timeouts.

- **Consecutive "single host" retry failures to stop scan**—Enter the number of consecutive timeouts permitted from one specific server.
- **Consecutive "any host" retry failures to stop scan**—Enter the total number of consecutive timeouts permitted from all hosts.
- **Nonconsecutive "single host" retry failures to stop scan**—Enter the total number of nonconsecutive timeouts permitted from a single host.
- **Nonconsecutive "any host" retry failures to stop scan**—Enter the total number of nonconsecutive timeouts permitted from all hosts.
- **If first request fails, stop scan**—Selecting this option will force the scanner to terminate the scan if the target server does not respond to the scanner's first request.
- **Response codes to stop scan if received**—Enter the HTTP status codes that, if received, will force termination of the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Session Storage

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the database. This saved information can be used for two purposes.

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, the scanner retrieves the saved data and sends HTTP requests that previously were suppressed.

- Hewlett-Packard support personnel can extract the generated (but not sent) HTTP requests for analysis. Sessions may be rejected for the reasons cited in the following table:

Reject Reason	Explanation
Invalid Host	Any host that is not specified as an Allowed Host.
Excluded File Extension	Files having an extension that is excluded by scan settings.
Excluded URL	URLs or hosts that are excluded by scan settings.
Outside Root URL	If the **Restrict to Folder** option is selected when starting an advanced scan, any resource not qualified by the available options (**Directory only (self)**, **Directory and subdirectories**, or **Directory and parent directories**).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the **Limit maximum crawl folder depth to** option has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the **Limit Maximum Single URL hits to** option has been exceeded.
404 Response Code	The option **Determine File Not Found (FNF) using HTTP response codes** is selected and the response contains a code that matches the requirements.
Solicited File Not Found	The option **Auto detect FNF page** is selected and the scanner determined that the response constituted a “file not found” condition.
Custom File Not Found	The option **Determine FNF from custom supplied signature** is selected and the response contains one of the specified phrases.
Rejected Response	Files have a MIME type that is excluded by scan settings.

Session Storage

The scanner normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

Session Exclusions

The following settings apply to both the crawl and audit phases of a vulnerability scan. To specify exclusions for only the crawl or only the audit, use the Crawl Settings - Session Exclusions or the Audit Settings - Sessions Exclusions.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject**—The scanner will not request files of the type you specify.
- **Exclude**—The scanner will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

Excluded MIME Types

The scanner will not process files associated with the MIME type you specify.

Excluded or Rejected URLs and Hosts

You can identify a URL or host (using a regular expression) and then specify whether you want to exclude or reject it.

- **Reject**—The scanner will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude**—During a crawl, the scanner will not examine the specified URL or host for links to other resources. During the audit portion of the scan, the scanner will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

You must use a regular expression to designate a host or URL.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following regular expression and select **Reject**.

Microsoft\.com

Note that the period (or dot) is preceded by a backslash, indicating that the next character is special (i.e., it is not the character used in regular expressions to match any single character except a newline character).

Example 2

Enter a string such as logout. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the logout example, the scanner will exclude or reject URLs such as logout.asp or applogout.jsp.

Example 3

If you enter /myApp / then the scanner will exclude or reject all resources in the myApp directory, such as: http://www.test.me /myApp /filename.htm.

If you enter /W3SVC[0-9]*/ then the scanner will exclude or reject the following directories:

http://www.test.me/W3SVC55/

http://www.test.me/W3SVC5/

http://www.test.me/W3SVC550/

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either **Host** or **URL**.
3. In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one of the following:
   - **Reject**—Do not send request to targeted URL or host.
   - **Exclude**—Send request, but do not process response.
5. Click **Update**.

Allowed Hosts

Use the Allowed Host settings to add domains that may be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning “WIexample.com,” you would need to add “WIexample2.com” and “WIexample3.com” here if those domains were part of your Web presence and you wanted to include them in the crawl or audit.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter “myco” as an allowed host. As the scanner scans the target site, if it encounters a link to any URL containing “myco,” it will pursue that link and scan that site’s server, repeating the process until all linked sites are scanned. For this hypothetical example, the scanner would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Note that if you specify a port number, then the allowed host must be an exact match.

If you use a regular expression to specify a host, select **Regex**.

HTTP Parsing

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then the scanner will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, “userid” is the parameter you would identify.

Note: You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

The scanner can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, “1234567” is the session information:

http://www.onlinestore.com/bikes/(1234567)/index.html

The regular expression for identifying the parameter would be: /\([\w\d]+\)/

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. The defaults identify ASP.NET cookieless session IDs.

HTTP Parameters Used for Page (Resource) Identification

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

Ex. 1 -- http://www.anysite.com?Master.asp?Page=1

Ex. 2 -- http://www.anysite.com?Master.asp?Page=2

Ex. 3 -- http://www.anysite.com?Master.asp?Page=13;Subpage=4

Ordinarily, the scanner would assume that these three requests refer to identical resources and would conduct a vulnerability assessment on only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

Examples 1 and 2 contain one resource parameter: “Page.”

Example 3 contains two parameters: “Page” and “Subpage.”

To identify resource parameters:

1 Click **Add**.

2 Enter the parameter name.

3 Click **Update**.

The string you entered appears in the Parameter list. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) the scanner should use.

Filters

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use the scanner or those who have access to the raw data. If the text you specify is found, the scanner reports it on the **Information** tab as a “Hidden Reference Found” vulnerability.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

To add a regular expression rule for finding or replacing keywords in requests or responses:

1 In either the **Request Content** or the **Response Content** group, click **Add**.

2 From the **Section** list, select an area to search.

3 In the **Find Condition** box, type (or paste) the string you want to locate (or enter a regular expression that describes the string). You can also click the list button to insert regular expression elements.

4 Type (or paste) the replacement string in the **Replace** box.

5 For case-sensitive searches, select the **Case-Sensitive** check box.

6 Click **Update**.

Cookies/Headers

Standard Header Parameters

You can elect to include referer and/or host headers in scanner requests.

- **Include "referer" in HTTP request headers**—Select this check box to include referer headers in HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
- **Include "host" in HTTP request headers**—Select this check box to include host headers with HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit the scanner performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when the scanner is auditing that site. You can add multiple custom headers. To add a custom header:

1 In the top box, enter the header using the format <name>: <value>.

2 Click **Add**.

The new header appears in the list of custom headers.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by the scanner to the server. To add a custom cookie:

1 In the top box, enter the header using the format <name>=<value>.

For example, if you enter

CustomCookie=ScanEngine

then each HTTP-Request will contain the following header:

Cookie:CustomCookie=ScanEngine

2 Click **Add**.

The new cookie appears in the list of custom cookies.

Proxy

Proxy Settings

Select one of the following options:

- **Direct Connection (proxy disabled)**—Select this option if you are not using a proxy server.

- **Automatically detect proxy settings**—If you select this option, the scanner will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's web proxy settings.
- **Use Internet Explorer proxy settings**—Select this option to use the proxy server settings configured for the Internet Explorer browser on the machine that will conduct the scan.
- **Use Firefox proxy settings**—Select this option to use the proxy server settings configured for the Firefox browser on the machine that will conduct the scan.

  Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

- **Configure a proxy using a PAC file URL**—Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the URL box.
- **Explicitly configure proxy**—Select this option to access the Internet through a proxy server, and then enter the requested information. For proxy servers accepting https connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server.
2. In the **Port** box, enter the port number (for example, 8080).
3. Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

Authentication

Scan Requires Network Authentication

Select this option if users must log on to your Web site or application. Then select an authentication method and specify a user name and password.

Warning: The scanner will crawl all servers granted access by this password (if the sites/servers are included in the "allowed hosts" setting. To avoid potential damage to your administrative systems, do not use a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact HP technical support.

The authentication methods are:

- **Basic**—A widely used, industry-standard method for collecting user name and password information. The Web browser displays a dialog box for a user to enter a previously assigned user name and password and then attempts to establish a connection to a server using the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.
- **NTLM**—An authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network. Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and the scanner has to pass through a proxy server to submit its requests to the Web server, the scanner may not be able to crawl or

audit that Web site. Use caution when configuring a scanner for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

- **Kerberos**—Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service. This authentication method will be successful only if the Web server has been configured to return a response header of "WWW-Authenticate: Kerberos" instead of "WWW-Authenticate: Negotiate."
- **Digest**—The Windows Server 2003 operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.
- **Automatic**—Allow the scanner to determine the correct authentication method. Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.

Use Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. To use client certificates.

1. Select **Use Client Certificate**.
2. Click **Browse** to choose a certificate.

File Not Found

Determine File Not Found (FNF) Using HTTP Response Codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.

- Forced Valid Response Codes (Never an FNF)—You can specify HTTP response codes that should never be treated as a file-not-found response.
- Forced FNF Response Codes (Always an FNF)—Specify those HTTP response codes that will always be treated as a file-not-found response. The scanner will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a semicolon.

Determine File Not Found from Custom Supplied Signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result from 404 pages that are unique to your site.

You can specify a signature using either plain text, a regular expression, or SPI Regex (see Regular Expression Extensions on page 209 for information on SPI Regex).

Auto-Detect File Not Found Page

Some Web sites do not return a status “404 Not Found” when a client requests a resource that does not exist. Instead, they may return a status “200 OK” but the response contains a message that the file cannot be found. Select this check box if you want the scanner to detect these “custom” file-not-found pages.

The HP scanner attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as “Sorry, the page you requested was not found”), with the possible exception being the name of the requested resource. If you select this option, you can specify what percentage of the response content must be the same. The default is 90 percent.

Policy

Scan Policy

A policy is a collection of audit engines and attack agents that a scanner uses when auditing or crawling your Web application. Each component has a specific task, such as testing for cross-site scripting susceptibility, building the site tree, probing for known server vulnerabilities, etc. See Appendix A, Policies, for policy descriptions.

When conducting a Web Service scan, you cannot select a policy.

CRAWL SETTINGS

Link Parsing

The scanner follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (if you select the JavaScript/VBScript analyzer option on the Scan Settings: Content Analyzers panel). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature to identify (using regular expressions) links that you want the scanner to follow.

To add a specialized link identifier:

1. Click **Add**.
2. In the **Custom Links** box, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comments** box.
4. Click **Update**.

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Crawl Settings - Session Exclusions) allows you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited. To add a file extension:

1. Click **Add**.

2 In the **File Extension** box, enter a file extension.

3 Select either **Reject**, **Exclude**, or both.

4 Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. To add a MIME Type:

1 Click **Add**.

2 In the **Exclude Mime-type** box, enter a MIME type.

3 Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option. To add a URL or host:

1 Click **Add**.

2 From the **Type** list, select either **Host** or **URL**.

3 In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.

4 Select one or both of the following:

- **Reject**—Do not send request to targeted URL or host.
- **Exclude**—Send request, but do not process response.

5 Click **Update**.

AUDIT SETTINGS

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Audit Settings - Session Exclusions) allows you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited. To add a file extension:

1 Click **Add**.

2 In the **File Extension** box, enter a file extension.

3 Select either **Reject**, **Exclude**, or both.

4 Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. To add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** box, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option. To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either **Host** or **URL**.
3. In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject**—Do not send request to targeted URL or host.
   - **Exclude**—Send request, but do not process response.
5. Click **Update**.

Attack Exclusions

Excluded Parameters

Use this feature to prevent the scanner from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

1. In the **Excluded Parameters** group, click **Add**.
2. In the **Parameter** box, enter the name of the parameter you want to exclude.
3. Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.
4. Click **Update**.

Excluded Cookies

Use this feature to prevent the scanner from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values. This setting requires you to enter the name of a cookie. In the following example HTTP response ...

Set-Cookie: FirstCookie=Chocolate+Chip; path=/

... the name of the cookie is "FirstCookie."

To exclude certain cookies.

1. In the **Excluded Cookies** group, click **Add**.
2. In the **Parameter** box, type a cookie name or enter a regular expression that you believe will match the cookies you want to exclude.

3 Click **Update**.

Excluded Headers

Use this feature to prevent the scanner from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression using the procedure described below.

1 In the **Excluded Headers** group, click **Add**.

2 In the **Parameter** box, type a header name or enter a regular expression that you believe will match the headers you want to exclude.

3 Click **Update**.

Import Audit Inputs

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs. To load inputs that you previously created using the Audit Inputs Editor, click the **Browse** button next to the **Import Audit Inputs** field.

Attack Expressions

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

ja-jp: Japanese and Japan

ko-Kr: Korean and Korea

zh-cn: Chinese and China (PRC)

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Vulnerability Filters

Select Vulnerability Filters to Enable

By applying certain filters, you can limit the display of vulnerabilities reported during a scan. For example, the “Parameter Vulnerability Roll-Up” filter, when selected, consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.

Click a filter name to view a description of the function it performs.

To add a filter to your default settings, select a filter in the *Available* area and click >. The filter is removed from the **Available** list and added to the **Selected** list.

To disable a filter, select a filter in the **Selected** list and click <. The filter is removed from the **Selected** list and added to the **Available** list.

To add all available filters, click >>.

To remove all selected filters, click <<.

Smart Scan

Enable Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, the scanner will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select this option, you can choose one or both of the identification methods described below.

- **Use regular expressions on HTTP responses to identify server/application types**—This method searches the server response for strings that match predefined regular expressions designed to identify specific servers.
- **Use server analyzer fingerprinting and request sampling to identify server/application types**—This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server type.

Custom Server/Application Type Definitions

If you know the server type for a target domain, you can select it using the Custom Server/Application Type Definitions section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.
2. In the **Host** box, enter the domain name or host, or the server's IP address.
3. Select one or more entries from the **Server/Application** list.
4. Click **OK**.

SCAN BEHAVIOR

Blackout Action

A blackout period is a block of time during which scans are not permitted.

If a blackout period begins while a scan in running, you may either stop the scan or suspend it. The scanner will resume a suspended scan when the blackout period ends.

EXPORT

General

Export Scan Results

Select this option to export the scan results. Then provide the requested information.

- **Export Path**—Select a destination for the exported scan. Export paths are specified by the WebInspect Enterprise administrator.
- **Export Format**—Select how you want the exported file to be formatted. Your choices are WebInspect Scan File or XML.

- **Automatically generate file name**—If you select this option, the name of the file will be formatted as <scan name> <date/time>.[xml or scan]. For example, if the scan name is "mysite" and the scan is generated at 6:30 on April 5, the file name would be "mysite 04_05_2007 06_30.scan [or .xml]." This is useful for recurring scans.

  If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **File name** box.

Scheduled Scan Settings

To schedule a scan, click the **Add** icon and then specify the scan settings. These settings are the same as described in Advanced Scan Settings on page 90, with the following additions:

Note that even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

Schedule

General

Project and Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Scan Template** list. You are not required to use a template.

Schedule

- **Schedule Name**—Enter a name that identifies this scheduled scan.
- **Start Time**—Enter the date and time you want the scan to begin. You can select the date from a calendar popup and the time from a clock popup.
- **Time Zone**—The time zone for the location of the target server specified for the scheduled scan. The time zone defaults to the zone in which you are working (as selected using the *Configure Options* window). If the target server is in a different time zone, you should usually select the server's time zone and specify the **Start Time** using local time. For example, if you are in New York City, USA (UTC-05:00) and the target server is in Rome, Italy (UTC+01:00), and you want to schedule a scan to begin at 8 a.m. Rome time, you could do either of the following:
  - Select the UTC+01:00 time zone (Rome) and specify a **Start Time** of 8 a.m.
  - Select the UTC-05:00 time zone (New York City) and specify a **Start Time** of 2 a.m.
- **Next Scheduled Time**—For a scan that is scheduled to recur, this read-only field displays the time and date of the next scheduled scan.
- **Last Occurred On**—For a scan that is scheduled to recur, this read-only field displays the time and date when a scan last occurred.

Recurrence

The Project Version setting is reproduced on each settings dialog, allowing you to change your selection at any point. The description of this setting is not repeated in the following topics.

Recurring

To schedule a scan, Smart Update, or blackout on a recurring basis, select the **Recurring** check box. Do *not* select this option if you want to schedule a one-time-only event.

Pattern

Use the **Pattern** group to select the frequency of the event (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the scan should occur.

Blackout Settings

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

General

Security Group

Select an organization and group. To associate the blackout with all groups in an organization, select **Use Organization**.

Name

Enter a unique identifier for this blackout period.

Address

The URL or IP address (or range of IP addresses) that are affected by this blackout period. The value can be a single URL or IP address, or a range of IP addresses. If you need to exclude multiple ranges, you must create additional (overlapping) blackout periods. To specify a range, separate the beginning address and ending address with a hyphen. You can use the asterisk (*) as a wild card. The default setting (an asterisk) means all addresses. Wildcards in IP addresses must be at the end of the address as shown below, but wildcards for host names must be at the beginning.

Examples:

192.16.12.1-192.16.12.210

192.16.12.*

*.domain.com

Schedule

- **Start Time**—The date and time at which the blackout period begins. You can enter the data manually or select the date from a calendar popup and the time from a clock popup.
- **End Time**—The date and time at which the blackout period expires. You can enter the data manually or select the date from a calendar popup and the time from a clock popup.
- **Time Zone**—The time zone for the location of the target server that is affected by the blackout. The time zone defaults to the zone in which you are working (as selected using the *Configure Options* window). If the target server is in a different time zone, you should usually select the server's time zone and specify the blackout period using local time. For example, if you are in New York City, USA (UTC-05:00) and the WebInspect Enterprise manager is in Rome, Italy (UTC+01:00), and you want to schedule a blackout to begin at 8 a.m. Rome time, you could do either of the following:
  - Select the UTC+01:00 time zone (Rome) and specify a **Start Time** of 8 a.m.
  - Select the UTC-05:00 time zone (New York City) and specify a **Start Time** of 2 a.m.
- **Duration**—The length of time during which the blackout is in effect. This value is calculated automatically after you specify the **Start Time** and **End Time**. Alternatively, if you specify the **Start Time** and the **Duration**, the **End Time** is calculated. If you edit the **Duration**, the **End Time** is recalculated. The format is:

  d.hh.mm

  where

  d = the number of days

  hh = the number of hours

  mm = the number of minutes

Blackout Type

- **Allow Scans during this period**—Scans of the specified targets are allowed only during the specified time period.
- **Deny Scans during this period**—Scans of the specified targets are prohibited during the specified time period.

Allowing or denying scans works very much like allowing or denying permissions. Deny always takes precedence over allow, so a scan can occur only at a particular time if there are no blackout periods that deny that time. An allow blackout period means that you will deny scans *unless* you are in the allowed range, not that you will allow scans *only* if you are in the allowed range. If you configure two separate "allow" blackout periods, a scan will be allowed only during the union of those periods. For example, if blackout period A allows scans from 1 p.m. to 3 p.m. and period B allows scans from 2 p.m. to 6 p.m., then scans will be allowed only from 2 p.m. to 3 p.m.

Recurrence

Use these settings to schedule a blackout on a recurring basis.

Recurring

Select the **Recurring** check box to impose recurring blackouts. Do *not* select this option if you want to schedule a one-time-only event.

Pattern

Use the **Pattern** group to select the frequency of the blackout (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the blackout should occur.

5 Guided Scan

Introduction

Guided Scan is the preferred method for performing a Web Site Scan in WebInspect Enterprise. It directs you through the best steps to configure a scan that is tailored to your application.

You can launch a Guided Scan in the following ways:

- In the WebInspect Enterprise Web Console, click **Actions** → **Guided Scan**.
- In Software Security Center (SSC), on the **Projects** tab select a project and project version, and click **Guided Scan** in the Quick Links.
- In SSC, open a particular project version in the **Projects** tab, click the **Scans** tab for that project version, and click **Guided Scan**.

The first time you launch a Guided Scan in WebInspect Enterprise or SSC, the Guided Scan client application, which includes its own Help system, is downloaded and installed on your local computer. Next, the Guided Scan wizard opens, as it does each subsequent time you launch a Guided Scan.

The first time you ever launch a Guided Scan, a tutorial appears. You can close this tutorial. Any time the **Tutorial** button in the upper right corner of the page is blue, you can click it to open the tutorial.

If you want to run Guided Scan in Mozilla Firefox, you must download and install the Firefox add-on for the .NET Framework Assistant. To obtain it, click **Add-ons** on the *Mozilla Firefox Start Page* in the Firefox browser and search .NET.

This chapter contains information about the Guided Scan for WebInspect Enterprise, including information about its set of Advanced Scan Settings, which are somewhat different than the advanced scan settings for Web Site Scans.

Starting a Guided Scan

Toolbar Buttons

The following buttons in the toolbar at the top of Guided Scan are available at various times as may be necessary or useful for the scan:

- **Scan Now** (in Scan group) - Skip the remaining Guided Scan steps and go to the *Guided Scan - Settings - Final Review - Validate Settings and Start Scan* page. See Validate Settings and Start Scan on page 124.
- **Open** (in Settings group) - Open scan settings from a file you select, from your own configured default settings, or from the original HP "factory" default settings.
- **Save** (in Settings group) - Save the current scan settings in a file you specify.
- **Advanced** (in Settings group) - Open advanced Scan Settings. See Advanced Scan Settings for Guided Scan on page 126.
- **Browser** (in Verify Site group) - Specify the browser to use to open your target site: Firefox (recommended) or Internet Explorer.
- **New** (in Macro group) - Record a new macro. See Web Macro Recorder (Unified) **on page 264**.
- **Import** (in Macro group) - Import an existing macro. See Web Macro Recorder (Unified) on page 264.
- **Export** (in Macro group) - Save a macro. See Web Macro Recorder (Unified) on page 264.
- **Logout Conditions** (in Macro group) - Open the Logout Condition Editor to manually specify logout conditions when recording or editing a macro. See Web Macro Recorder (Unified) on page 264.
- **Browser** (in Macro group) - Specify the browser to use to record or edit a macro: Firefox (recommended) or Internet Explorer. See Web Macro Recorder (Unified) on page 264.
- **Import Locations** (in Navigate Locations group) - Import a file of key locations that were covered and saved when enhanced coverage of your website was performed.
- **Export Locations** (in Navigate Locations group) - Export to a new file the key locations you have specified when enhancing coverage of your website.
- **Allowed Hosts** (in Navigate Locations group) - List of allowed hosts identified thus far. Each can be enabled or disabled, as long as at least one remains enabled.
- **Browser** (in Navigate Locations group) - Specify the browser to use when enhancing coverage of your website: Firefox (recommended) or Internet Explorer.
- **Import** (in Web Forms group) - Import an existing set of web form values that were entered when your website was previously explored.
- **Export** (in Web Forms group) - Export to a new file the web form values you have entered when exploring your website.
- **New Global** (in Web Forms group) - Add a new global Web form field, that is, a field whose value will be submitted for any input control having the specified name, regardless of the URL at which the scanner encounters it.
- **Show Globals** (toggle button in Web Forms group) - In the **Web Form Values** step, add a list of all global web form values that were used in verifying the site.
- **Show All** (toggle button in Web Forms group) - In the **Web Form Values** step, add lists of all non-global web form values that were used in verifying the site.

Overview of Guided Scan Steps

The Guided Scan progress display in the left pane allows you to see your progress as you specify settings in the right pane for the various pages of your scan. "*Guided Scan* -" and the current step and substeps comprise the name of the wizard page in the title bar. The initial page is *Guided Scan - Site - Start Parameters - Verify Web Site,* for which **Start Parameters** and **1. Verify Web Site** are highlighted in the **Site** step in the left pane. Details for you to complete are displayed in the right pane of each page.

Following is a summary of the steps in the progress display that you will complete:

- **Site** - Specify the Web site to scan and verify you can access it.
  - **Start Parameters**
    - **1. Verify Web Site** - Specify the Web site to scan and verify you can access it.
    - **2. Choose Scan Type** - Select **Standard** scan or, if you are using pre-recorded macros, **Workflows** scan; select scan method (crawl, crawl and audit, or audit); and select scan policy.
- **Login** - Specify authentication settings for login.
  - **Network Authentication**
    - **Configure Network Authentication** - Specify the network authentication method and/or client certificate.
  - **Application Authentication**
    - **1. Select Login Macro** - Specify whether to use a login macro for this site and whether to select, create, or edit one.
    - **2. Record/Edit Login Macro** - Record or edit a login macro.
- **Workflows** - Specify workflows (appears for workflow scans only).
  - **Workflows**
    - **1. Manage Workflows** - Specify whether to select, create, or edit a workflow macro.
    - **2. Record/Edit Workflow** - Record or edit a workflow macro.
- **Active Learning** - Allow Guided Scan to profile your site and recommend optimized scan settings accordingly, and navigate to key site locations.
  - **Optimization Tasks**
    - **Profile your site for optimal settings** - Run the Profiler and see what it recommends.
    - **Enhance coverage of your web site** - Navigate to key locations in your site to ensure that they are well covered.
    - **Web Form Values** - Optionally modify any web form values that Guided Scan recorded while you configured the scan.
- **Settings** - Address configuration errors, optionally save scan settings, specify the project version to scan, and start the scan.
  - **Final Review**
    - **Validate Settings and Start Scan** - Address any errors detected by the wizard, optionally save scan settings for reuse later if desired, specify the project and project version, and begin the scan.

The right pane often includes a yellow instruction bar that guides you through particular steps.

The following sections describe each step in detail.

Site

Start Parameters

1. Verify Web Site

1 In the **Start URL** box, type or select the complete URL or IP address of the site to scan.

If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, WebInspect will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

An invalid URL or IP address results in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

Scans by IP address do not pursue links that use fully qualified URLs (as opposed to relative paths).

WebInspect supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets. Examples:

- http://[::1] — WebInspect scans “localhost.”
- http://[fe80::20c6:29ff:fe32:bae1]/subfolder/ — WebInspect scans the host at the specified address starting in the “subfolder” directory.
- http://[fe80::20c6:29ff:fe32:bae1]:8080/subfolder/ — WebInspect scans a server running on port 8080 starting in “subfolder.”

2 (Optional) To limit the scope of the scan to an area, select the **Restrict to Folder** check box, and then select one of the following options from the list:

- **Directory only (self)** - WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, WebInspect will assess only the "two" directory.
- **Directory and subdirectories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

3 If you must access the target site through a proxy server, click **Proxy** in the lower left of the right pane and then select one of the following options from the **Proxy Settings** list:

- **Direct Connection (proxy disabled)**
- **Auto detect proxy settings**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
- **Use Internet Explorer proxy settings**: Import your proxy server information from Internet Explorer.
- **Use Firefox proxy settings**: Import your proxy server information from Firefox.
- **Configure proxy settings using a PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **Edit** to enter the location (URL) of the PAC.
- **Explicitly configure proxy settings**: Specify proxy server settings as indicated. If you select this option, click **Edit** to enter proxy information.

Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server is not used.

4 Click **Verify** and follow the instructions in the yellow instruction bar.

When the Web site or directory structure appears, you have successfully verified your connection to the Start URL.

5 Click the **Next** icon, which is always available at the top right of the left pane.

The *Guided Scan - Site - Start Parameters - Choose Scan Type* page appears, and in the **Site** step in the left pane, **Start Parameters** and **2. Choose Scan Type** are highlighted.

2. Choose Scan Type

1 Select one of the following scan types:

- **Standard**: WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.
- **Workflows**: If you select this option, an additional **Workflows** step appears in the left pane. That step will later display a table of workflows you have created. WebInspect audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. You do not need to specify a logout condition. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan. You can continue through the Guided Scan wizard's default sequence and later complete the workflow scan settings when the **Workflows** page is highlighted. This procedure assumes that you use the default sequence.

2 (Optional) You can change the default scan name in the **Scan Name** text box.

3 In the Scan Method area, select one of the following scan methods:

- **Crawl Only**: This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click **Audit** to assess an application's vulnerabilities.
- **Crawl and Audit**: WebInspect maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information about simultaneous vs. sequential crawl and audit, see Method on page 126.
- **Audit Only**: WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

4 In the Policy area, select a policy from the drop-down list. For information about policies, see Appendix A, Policies.

5 Click the **Next** icon at the top of the left pane.

By default, the *Guided Scan - Login - Application Authentication - Select Login Macro* page appears, and under the **Login** step in the left pane, **Application Authentication** and **1. Select Login Macro** are highlighted. If you do *not* need to perform *network* authentication, go to Application Authentication on page 121.

If you *do* need to perform network authentication, click **Network Authentication** under the Login step in the left pane. The *Guided Scan - Login - Network Authentication - Configure Network Authentication* page appears, and under the Login step, **Network Authentication** and **Configure Network Authentication** are highlighted. In this case, proceed to Network Authentication on page 120.

Login

Network Authentication

Configure Network Authentication

If your site requires network authentication:

1. Click the **Network Authentication** check box.
2. Select an authentication method from the **Method** options, and then enter your network credentials. The authentication methods are:
   - **Basic.** A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.
   - **NTLM.** NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

     Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use caution when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.
   - **Digest.** The Windows Server 2003 operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.
   - **Automatic.** Allow WebInspect to determine the correct authentication method.
   - **Kerberos.** Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.
   - **Negotiate.** The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice. For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.
3. Complete the **User Name** and **Password** fields.

If you need to use a client certificate for network authentication:

1. Select the **Client Certificate** check box.
2. In the Certificate Store area, select one of the following:
   - **Local Machine** - WebInspect uses a certificate on the local machine based on your selection in the Certificate area.
   - **Current User** - WebInspect uses a certificate for the current user based on your selection in the Certificate area.
3. Select either **My** or **Root** from the drop-down list.
4. To view certificate details in the Certificate Information area, select a certificate in the Certificate area.
5. Click the **Next** icon.

   The *Guided Scan - Login - Application Authentication - Select Login Macro* page appears, and **Application Authentication** and **1. Select Login Macro** are highlighted in the left pane.

Application Authentication

1. Select Login Macro

If your site requires a login macro:

1. Select **Use a login macro for this site**.
2. Do one of the following:
   - Click **Edit** to edit the default login macro shown in the **Automated Login Sequence (Login Macro)** text box.
   - Click  to open a standard file-selection window, allowing you to select a previously recorded macro.
   - Click the **x** to the right of the text box, select **Use a login macro for this site** again, and then click **Create** to record a new macro. The Web Macro Recorder opens in the *Guided Scan - Login - Application Authentication - Record/Edit Login Macro* page, and **Application Authentication** and **2. Record/Edit Login Macro** are highlighted in the left pane.

2. Record/Edit Login Macro

1. Follow the instructions in the yellow instruction bar of the Web Macro Recorder to create or edit a login macro. For more information, see Web Macro Recorder (Unified) on page 264.
2. Click the **Next** icon.

   If you selected a **Standard** scan in the **Site** step, then the *Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings* page appears, and **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane. In this case, go to Active Learning on page 122.

   If you selected a **Workflows** scan in the **Site** step, then the *Guided Scan - Workflows - Workflows - Manage Workflows* page appears, and **Workflows** and **1. Manage Workflows** are highlighted in the left pane. In this case, proceed to Workflows.

Workflows

Workflows

1. Manage Workflows

1 If you selected the **Workflows** scan option, optionally select a workflow in the Workflows table, if any, and click any of the following if available:

- **Record** opens the Web Macro Recorder, allowing you to create a macro. The *Record/Edit Workflow* page appears, **Workflows** and **2. Record/Edit Workflow** are highlighted in the left pane, and the Web Macro Recorder opens. Go to 2. Record/Edit Workflows on page 122.
- **Edit** opens the Web Macro Recorder and loads the selected macro. The *Record/Edit Workflow* page appears, **Workflows** and **2. Record/Edit Workflow** are highlighted in the left pane, and the Web Macro Recorder opens. Go to 2. Record/Edit Workflows on page 122.
- **Delete** removes the selected macro from the Workflows table (but does not delete it from your disk).
- **Import** opens a standard file-selection window, allowing you to select a previously recorded macro (`*.webmacro` file).
- **Export** opens a standard file-selection window, allowing you to save a recorded macro to a `*.webmacro` file.

Note: If you have installed HP Unified Functional Testing (UFT) on your computer, then WebInspect detects this automatically and displays an option to import a UFT (`.usr`) file. See Importing HP Unified Functional Testing (UFT) Files in a Guided Scan on page 124.

2 After you specify and play a workflow macro, it appears in the Workflows table and its Allowed Hosts are added to the *Guided Scan - Workflows - Workflows - Manage Workflows* page. You can enable or disable access to particular hosts.

3 When you have finished managing your workflows, click the **Next** icon. If you did not record or edit a macro, the *Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings* page appears, and **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane. In this case, go to Optimization Tasks on page 122.

2. Record/Edit Workflows

1 Follow the instructions in the yellow instruction bar of the Web Macro Recorder to create or edit a workflow macro. For information about the Web Macro Recorder tool, see Web Macro Recorder (Unified) on page 264.

2 When you complete this step, click the **Next** icon. The *Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings* page appears, and **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane.

Active Learning

Optimization Tasks

Profile site for optimal settings

In this step, the Profiler conducts a preliminary examination of your target Web site. Based on its findings, the Profiler returns a list of suggested changes to particular scan settings in the Settings section. You can accept or reject each recommendation.

For example, the Profiler might detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Profiler's suggestion to configure the required information before continuing.

Similarly, your settings might specify that WebInspect should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it suggests that you modify the WebInspect setting to accommodate this feature.

1 To launch the Profiler, click **Profile**.

Results appear in the Settings area, in addition to the default options for:

- **Disable case sensitivity for crawling**
- **Known Web Technologies and Sites**

2 Accept or reject the suggested settings. To reject, clear the associated check box.

3 Provide the requested information as necessary.

4 Click the **Next** icon.

Several options may be presented even if you do not run the Profiler, as follows:

Auto-fill Web forms during crawl

Select this option if you want WebInspect to submit values for input controls on forms it encounters while scanning the target site. WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. See Web Form Editor on page 188. You may:

- Click the browse button  to locate and load a file.
- Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
- Click **Create** to open the Web Form Editor and create a file.

Add allowed hosts

Use the Allowed Hosts settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See Allowed Hosts on page 140 for more information.

To add allowed domains:

1 Click **Add.**

2 On the *Specify Allowed Host* page, enter a URL (or a regular expression representing a URL) and click **OK.**

Apply sample macro

WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the prepackaged macro containing the login script.

If the profiler does not recommend changes, the Scan Wizard displays the message "No settings changes are recommended. Your current scan settings are optimal for this site."

When you click the **Next** icon, the *Guided Scan - Active Learning - Optimization Tasks - Enhance coverage of your web site* page appears, and **Optimization Tasks** and **Enhance coverage of your web site** are highlighted in the left pane.

Enhance coverage of your web site

To enhance coverage of your application, navigate to its key locations.

See Web Macro Recorder (Unified) on page 264 for detailed information about using the Web Macro Recorder tool to navigate key locations in your application, for Guided Scan to use during the scan.

See the Guided Scan Tutorial for more information about how to use this page of the Guided Scan wizard. To launch the tutorial, click **Tutorial** in the upper right corner of the page.

At any time you can click **Explored Locations** at the bottom left of the page to see a list of the Method, Status, and URL of each location you have accessed.

When you complete the **Enhance coverage of your web site** step, click the **Next** icon. If any web form values were recorded, the *Guided Scan - Active Learning - Optimization Tasks - Web Form Values* page appears, and **Optimization Tasks** and **Web Form Values** are highlighted in the left pane. Proceed to Web Form Values.

If there are no web form values, the *Guided Scan - Settings - Final Review - Validate Settings and Start Scan* page appears, and **Final Review** and **Validate Settings and Start Scan** are highlighted in the left pane. Go to Settings on page 124.

Web Form Values

Guided Scan recorded all of the web form values that you entered while you explored your Web site to enhance coverage. Here you can review and modify the values, which are part of the scan settings that are saved with the scan. In the toolbar, you can click **Export** to save the values to a separate file or click **Import** to use an existing set of values. The scan settings, including the web form values, serve as defaults that you can modify in future scans.

Settings

Final Review

Validate Settings and Start Scan

1. Address any scan configuration errors that have been detected.
2. As desired, select **Click here to save settings** to save the settings to an external file for later use.
3. Specify the **Project** and **Project Version**.
4. In the Scan Now area, review your scan settings, and then click **Start Scan** to begin the scan.

Importing HP Unified Functional Testing (UFT) Files in a Guided Scan

If you have the HP Unified Functional Testing application installed, WebInspect detects it and allows you to import a UTF file (`.usr`) into your workflow scan to enhance the thoroughness and attack surface of your scan. For more information about HP UFT, see **HP Unified Functional Testing** on the HP Web site.

To import a UTF (`.usr`) file into a WebInspect Enterprise Guided Scan:

1. Launch a Guided Scan, and then select **Workflow Scan** as the Scan Type. The following additional text appears under the Workflows scan option:

   HP Unified Functional Testing has been detected. You can import scripts to improve the thoroughness of your security test.

2. Click **Next**.

3. In the **Login** section, WebInspect Enterprise automatically selects the **Application Authentication** option. Complete the fields as indicated, and then click **Next**.
4. On the *Manage Workflows* screen, the Workflow table appears. Click **Import** to display the *Import Scripts* dialog.
5. On the *Import Scripts* dialog, you may:
   - Type the filename.
   - Browse to your file to locate your file with a `.usr` extension. Select **HP Unified Functional Testing** from the drop-down file type, and then navigate to the file.
   - Click **Edit** to launch the HP Unified Functional Testing application.
6. (Optional) On the Import Scripts dialog, you may select either of the following options:
   - **Show HP Unified Functional Testing UI during import**
   - **Open script result after import**
7. Select the `.usr` file to import, and then click **Import**. After your file is successfully imported, the file appears in the Workflows table.
8. Select one of the following from the Workflows table:
   - **Record** - launches the WebInspect Unified Web Macro Recorder. For more information, see Web Macro Recorder (Unified) on page 264.
   - **Edit** - allows you to modify the file using the WebInspect Unified Web Macro Recorder. See Web Macro Recorder (Unified) on page 264.
   - **Delete** - deletes the script from the Workflows table
   - **Import** - imports another file
   - **Export** - saves a file in `.webmacro` format with the name and location you specify
9. Click **Next**.

When the first `.usr` script file is added to the list, its name (or default name) appears in the Workflows table and an Allowed Hosts table is added to the pane.

Adding another `.usr` script file can add more allowed hosts. Any host that is enabled is available to all the listed workflow `.usr` script files, not just the workflow `.usr` file for which it was added. The Guided Scan will play all the listed workflow files and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, WebInspect will crawl or audit the responses from that host. If a check box is not selected, WebInspect will not crawl or audit the responses from that host.

In addition, if a particular workflow `.usr` script uses parameters, a Macro Parameters table is displayed when that workflow macro is selected in the list. Edit the values of the parameters as needed.

After you have completed changes or additions to the Workflow table, proceed in the Guided Scan wizard to complete your settings and run the scan. For more information about recording a new login macro or using an existing login macro, see Web Macro Recorder (Unified) on page 264. That section also provides information about using macros that were recorded in earlier versions of WebInspect using other web macro recorder tools.

Advanced Scan Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Scan Settings described in this section. The Advanced Scan Settings for Guided Scan are similar but not identical to those for a Web Site Scan.

Method

The Method settings broadly determine the type of scan to be conducted.

Scan Mode

Crawl Only

This option completely maps a site's tree structure. After a crawl has been completed, you can click **Audit** to assess an application's vulnerabilities.

Crawl & Audit

As WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed. This is described in the Default Settings as Crawl and Audit (Simultaneously).

Audit Only

WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

Simultaneously

As WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed.

Sequentially

In this mode, WebInspect crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.

If you select **Sequentially**, you can specify the order in which the crawl and audit should be conducted:

- **Test each engine type per session**—WebInspect audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.
- **Test each session per engine type**—WebInspect runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Audit Details

Include search probes (send search attacks)

When selected, WebInspect will send requests for files and directories that might or might not exist on the server, even if those files are not found by crawling the site.

This option is selected by default only when the Scan Mode is set to Crawl & Audit. The option is cleared (unchecked) by default when the Scan Mode is set to Crawl Only or Audit Only.

Navigation

Auto-fill web forms during crawl

If you select this option, WebInspect submits values for input controls found on all forms. The values are extracted from a file you create using the Web form editor. Use the browse button to specify the file containing the values you want to use. Alternatively, you can click **Edit** (to modify the currently selected file) or **Create** (to create a Web form file).

Do not rely on this feature for authentication. If the crawler and the auditor are configured to share state, and if the scanner never inadvertently logs out of the site, then using values extracted by the Web Form Editor for a login form may work. However, if the audit or the crawl triggers a logout after the initial login, then the scanner will not be able to log in again and the auditing will be unauthenticated. To prevent WebInspect from terminating prematurely if it inadvertently logs out of your application, go to Scan Settings - Authentication and select **Use a login macro for forms authentication**.

Prompt for web form values during scan (interactive mode)

If you select this option, WebInspect pauses the scan when it encounters an HTTP or JavaScript form and displays a window that allows you to enter values for input controls within the form. However, if you also select **Only prompt for tagged inputs**, WebInspect will not pause for user input unless a specific input control has been designated **Mark as Interactive Input** (using the Web Form Editor). This pausing for input is termed “interactive mode” and you can cancel it at any time during the scan.

Do not select this option if you want to conduct an unattended scan.

Use Web Service design

This option applies only to Web Service scans.

When performing a Web services scan, WebInspect crawls the WSDL site and submits a value for each parameter in each operation. These values are contained in a file that you create using the Web Service Test Designer tool. WebInspect then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

Use the browse button to specify the file containing the values you want to use. Alternatively, you can click **Edit** (to modify the currently selected file) or **Create** (to create a SOAP values file).

General

Scan Details

Enable path truncation

Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. WebInspect truncates paths, looking for directory listings or unusual errors within each truncation.

Example: If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ may cause the server to reveal directory contents or may cause unhandled exceptions.

Attach debug information in request header

If you select this option, WebInspect includes a "Memo:" header in the HTTP request containing information that can be used by support personnel to diagnose problems. Although the format and content is subject to change without notice, the information may assist advanced users. Two of the more useful constructions are illustrated below.

Attack memo header example:

```
Memo: 197:Auditor.SendAsyncronousRequest:Attack(CID:123:AS:2,
EID:1354e211-9d7d-4cc1-80e6-4de3fd128002,ST:AuditAttack,AT:PostParamManip
ulation,APD:username,I:(1,0),R:False,SM:2,SID:FDF074B3AC41D4ABE4114B3C1A1
14160,PSID:DDAA45FB26C9149DB15AF2D8DDFD5D3A)
Requestor thread ID handling request:197
Originating function in scanner: SendAsyncronousRequest
CheckID:123
Attack Sequence: 2
Originating Engine ID:1354e211-9d7d-4cc1-80e6-4de3fd128002
Session Type: AuditAttack
Attack Type: PostParamManipulation
Attack descriptor (what was attacked): username 'param' was attacked; it
is parameter (1,0) in collection
Smart Mode: 2
Attack Session ID: FDF074B3AC41D4ABE4114B3C1A114160
Parent Session ID :DDAA45FB26C9149DB15AF2D8DDFD5D3A
```

Crawl memo header example:

```
Memo: 180:ProcessSession:Crawler.CreateStateRequest:
SID:2BC3FC705779A6F201810A1E64F7CF83,PSID:A77674B6A5BF9B3B3CEDAEF583C0826
2,ST:Crawl,CLT:HTML
Requestor thread ID handling request:180
Originating function in scanner: ProcessSession:Crawler.CreateStateRequest
Session Type: Crawl
Crawl Link Type: HTML
Session ID: 2BC3FC705779A6F201810A1E64F7CF83
Parent Session ID : A77674B6A5BF9B3B3CEDAEF583C08262
```

Case-sensitive request and response handling

Select this option if the server at the target site is case-sensitive to URLs. Usually, the case sensitivity of a Web server is determined by the server's operating system. Windows is not case-sensitive; UNIX and Linux are. The one exception to this rule concerns Apache, which can be configured with non-case-sensitive page names, even on a UNIX system.

Recalculate correlation data

This feature is used only for comparing scans and should be selected only upon the advice of HP Support personnel if scan comparisons produce questionable results.

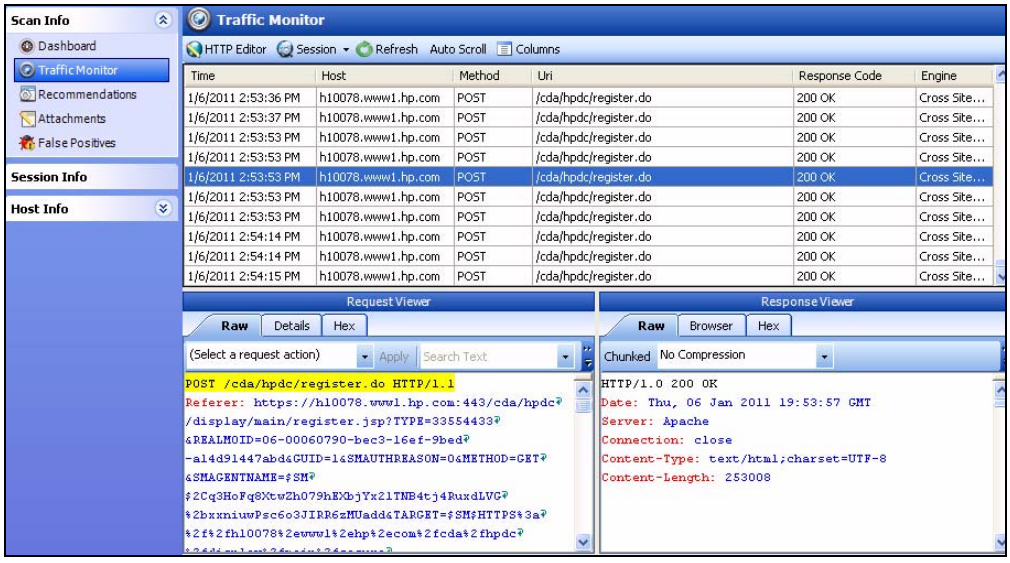
Compress response data

If you select this option, WebInspect saves disk space by storing each HTTP response in a compressed format in the database.

Enable Traffic Monitor Logging

Note: Traffic monitoring is not supported in WebInspect Enterprise version 10.10, but you can configure it for potential use in scan settings you save for use in WebInspect.

While scanning, WebInspect displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site plus those sessions in which a vulnerability was discovered. However, if you select the Traffic Monitor option, WebInspect adds the **Traffic Monitor** button to the Scan Info panel (as shown below), allowing you to display and review every request sent by WebInspect and the associated response received from the server.



Encrypt Traffic Monitor File

Note: Traffic monitoring is not supported in WebInspect Enterprise version 10.10, but you can configure it for potential use in scan settings you save for use in WebInspect.

All sessions are normally recorded in the traffic monitor file as clear text. If you are concerned about storing sensitive information such as passwords on your computer, you can elect to encrypt the file.

Encrypted files cannot be compressed. Selecting this option will significantly increase the size of exported scans containing log files.

Maximum crawl-audit recursion depth

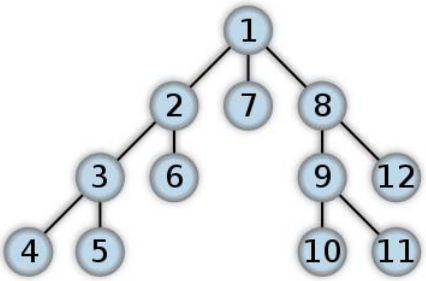
When an attack reveals a vulnerability, WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The default value is 2; the maximum recursion level is 1,000.

Crawl Details

Crawler

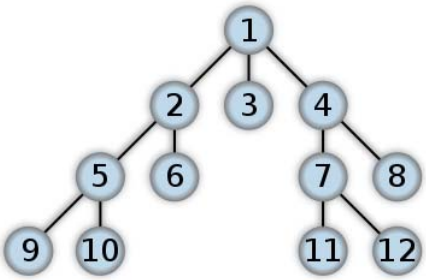
Select either **Depth First** or **Breadth First**.

Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.



Depth-First Tree

By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



Breadth-First Tree

When performing a depth-first crawl, WebInspect pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a "shopping cart" page before accessing the "check-out" page.

Enable keyword search audit

A keyword search, as its name implies, examines server responses and looks for certain text strings that typically indicate a vulnerability. This option is available only for a crawl-only scan.

Perform redundant page detection

Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, WebInspect would never be able to finish the scan. This option, however, allows WebInspect to identify and exclude processing of redundant resources.

Limit maximum single URL hits to

Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL. Use this field to limit the number of times a single link will be followed during a crawl. The default value is 5.

Include parameters in hit count

If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.

For example, if this option is selected, then “page.aspx?a=1” and “page.apsx?b=1” will both be counted as unique resources (meaning that the crawler has found two pages).

If this option is not selected, then “page1.aspx?a=1” and “page.aspx?b=1” will be treated as the same resource (meaning that the crawler has found the same page twice).

Limit maximum link traversal sequence to

This option restricts the number of hyperlinks that can be sequentially accessed as WebInspect crawls the site. For example, if five resources are linked as follows:

Page A contains a hyperlink to Page B

Page B contains a hyperlink to Page C

Page C contains a hyperlink to Page D

Page D contains a hyperlink to Page E

and if this option is set to “3,” then Page E will not be crawled. The default value is 15.

Limit maximum crawl folder depth to

This option limits the number of directories that may be included in a single request. For example, if the URL is

http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7

and this option is set to “4,” then the contents of directories 5, 6, and 7 will not be crawled. The default value is 15.

Limit maximum crawl count to

This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing the scan of a large site.

Limit maximum web form submission to

Normally, when WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed.

There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form.

Use this setting to limit the total number of submissions that WebInspect will perform. The default value is 3.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan. However, this option should be used for sites that enforce a strict order of access to pages. Using the "depth first" and "path retrace" options can obtain a successful scan on these types of sites when a breadth-first crawl fails.

Content Analyzers

Silverlight

If you enable the Silverlight analyzer, WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment.

Flash

If you enable the Flash analyzer, WebInspect analyzes Flash files, Adobe's vector graphics-based resizable animation format.

JavaScript/VBScript

The JavaScript/VBScript analyzer is always enabled. It allows WebInspect to crawl links defined by JavaScript or Visual Basic script, and to create and audit any documents rendered by JavaScript. Crawling links defined by VBScript execution requires selecting the **Enable classic script engine** option (described later in this section).

To increase the speed at which WebInspect conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Configure the settings described below.

Crawl Links found from script execution

If you select this option, the crawler will follow dynamic links (i.e., links generated during JavaScript execution).

Reject script include file requests to offsite hosts

Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is:

```
<script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>
```

WebInspect will download and parse such files, regardless of their origin or file type, unless you select the Reject Script option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).

Create script event sessions

If you select this option, WebInspect creates and saves a session for each change to the Document Object Model (DOM).

Verbose Script Parser debug logging

If you select this setting AND if the Application setting for logging level is set to Debug, WebInspect logs more detailed information about DOM operations that occur during script execution. This can create several hundred megabytes of data for medium and large sites.

Log JavaScript errors

WebInspect logs JavaScript parsing errors from the script parsing engine.

Enable JS Framework UI Exclusions

If selected, the WebInspect JavaScript parser ignores JQuery calendars.

Max script events per page

Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999. The default value is 1000.

Enable classic script engine

The new script engine provided in WebInspect 10.00 operates more like a browser and supports more web applications than did the script engine used in previous WebInspect versions. You can select this option to use the previous script engine instead.

Enable Advanced JS Framework Support

When this option is selected, WebInspect can recognize certain JavaScript frameworks and more intelligently execute script by recognizing patterns that these frameworks use. This option is available only for the new script engine of WebInspect 10.00 and is disabled if you select the **Enable classic script engine** option.

Recommendations

Note: Recommendations are not supported in WebInspect Enterprise version 10.10, but you can configure them for potential use in scan settings you save for use in WebInspect.

While conducting a scan, WebInspect may encounter certain omissions, abnormalities, or anomalies that interfere with or diminish the thoroughness of the scan. If you enable the Recommendations feature, WebInspect records this information and, when the scan is complete (or paused), presents a list of recommendations designed to improve the quality of your scan when you next conduct it.

To enable this feature, select **Run Recommendation Modules when the scan is paused or completed**. You can then select or deselect an individual module by selecting or clearing its associated check box.

To view the recommendations resulting from this analysis, click **Recommendations** in the **Scan Info** panel.

Network Authentication

This module detects that network, proxy, or site authentication is required, but credentials are missing or invalid.

Web Macro

This module tracks the number of times the scanner runs a Web macro to log in to the site and warns if the number seems to be excessive, indicating that the macro may not be functioning properly. Usually this occurs because the macro is unable to log in or contains a poor log-out condition, or the site prevents multiple concurrent log-in sessions.

Note: If the macro worked correctly when it was recorded, the user name or password assigned to the site may have been subsequently changed, or the account may have been blocked or deleted.

The threshold for determining this condition is heuristically set at 10 percent. For example, if the scanner examines 4,000 responses and more than 400 of them (10 percent) indicate that the scanner is logged out of the site, thus causing the scanner to run the macro that logs in to the site, then there is a high probability that the macro is faulty and should be replaced.

You may establish a threshold that is higher or lower than 10 percent, based on your experience. To do so, click Settings and select a different macro ratio.

File Not Found

This module examines the server's responses to requests for files and determines that the scan settings for recognizing a "file not found" condition may be incorrect. It is used only during a crawl-and-audit scan.

Web Service

This module detects the presence of Web service communication within the Web site and advises you to conduct a Web service scan.

Form Values

This module detects the existence of forms containing an input element for which you have not provided a value.

Caution: Using Form Values recommendations can cause an unintended large increase in scan data stored, as well as potential "out of memory" errors during large scans. This module is turned off by default. If it is turned on, data storage problems and out of memory incidents may occur.

Custom Parameters

This module detects the use of URL Rewriting techniques and RESTful services technologies.

Click **Settings** to select options for this feature. The settings are:

- **Similar URLs Percentage of Total in Site** -- In some cases, WebInspect uses a "Similar URLs Percentage of Total in Site" threshold to prevent false positives. You can change this threshold to improve the accuracy of these suggestions in case you encounter false positives. Enter a percentage between 1 and 100.
- **Maximum Custom Parameter Recommendations** -- WebInspect also applies a prioritization algorithm to the recommendations and lists them in order of their estimated accuracy. If you encounter problems or anomalies while attempting to detect custom parameters, you can use the Maximum Custom Parameter Recommendations box to limit the number of recommendations the module will produce. Select either Unlimited, or enter a value between 1 and 10,000.

- **Validate custom parameter recommendations** -- If you select this option, WebInspect validates custom parameter recommendations by sending appropriate requests during the analysis stage and removing those recommendations for which an invalid response is received.

Requestor

A requestor is the software module that handles HTTP requests and responses.

Requestor Performance

Use a shared requestor

If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads.

Use separate requestors

If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

You can also specify the maximum number of threads that can be created for each requestor. When performing a sequential crawl and audit, the crawl requestor can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 50. The default setting is 5 for the crawl requestor and 10 for the audit requestor. Increasing the thread count will increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

If you select "simultaneous crawl and audit" as the scan mode (see Scan Mode on page 126), the Crawl Requestor Thread Count is set to "1" and may not be modified.

If you notice numerous entries on the **Scan Log** tab showing requests timing out, you should reduce the thread count. While most servers can handle a large number of requests, servers in development environments sometimes have limitations on their licensing that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5. Failing to do so may mean that WebInspect does not accurately crawl or audit the site because requests are being rejected by the server.

Requestor Settings

Limit maximum response size to

Select this option to limit the size of accepted server responses, and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (`.swf`) and JavaScript "include" files are not subject to this limitation.

Request retry count

Specify how many times WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.

Request timeout

Specify how long WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, WebInspect resubmits the request until reaching the retry count. If it then receives no response, WebInspect logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds.

Stop Scan If Loss Of Connectivity Detected

There may be occasions during a scan when a Web server crashes or becomes too busy to respond in a timely manner. You can instruct WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

Consecutive 'single host' retry failures to stop scan

Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.

Consecutive 'any host' retry failures to stop scan

Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.

Nonconsecutive 'single host' retry failures to stop scan

Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."

Nonconsecutive 'any host' retry failures to stop scan

Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.

If first request fails, stop scan

Selecting this option will force WebInspect to terminate the scan if the target server does not respond to WebInspect's first request.

Response codes to stop scan if received

Enter the HTTP status codes that, if received, will force WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Session Storage

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the WebInspect database. This saved information can be used for two purposes.

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Hewlett-Packard support personnel can extract the generated (but not sent) HTTP requests for analysis.

Sessions may be rejected for the reasons cited in the following table:

Reasons for Rejecting a Session

Reject Reason	Explanation
Invalid Host	Any host that is not specified in Default (or Current) Scan Settings/Scan Settings/Allowed Hosts.
Excluded File Extension	Files having an extension that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/ Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Audit Settings/ Session Exclusions/Excluded or Rejected File Extensions.
Excluded URL	URLs or hosts that are excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/ Crawl Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected URLs and Hosts.
Outside Root URL	If the Restrict to Folder option is selected when starting an advanced scan, any resource not qualified by the available options (Directory Only, Directory and Subdirectories, or Directory and Parent Directories).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the Limit maximum crawl folder depth to option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the Limit Maximum Single URL hits to option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
404 Response Code	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option Determine File Not Found (FNF) using HTTP response codes is selected and the response contains a code that matches the requirements.
Solicited File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option Auto detect FNF page is selected and WebInspect determined that the response constituted a “file not found” condition.
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option Determine FNF from custom supplied signature is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/ Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

Session Storage

WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

Session Exclusions

These settings apply to both the crawl and audit phases of a WebInspect vulnerability scan. To specify exclusions for only the crawl or only the audit, use the **Crawl Settings - Session Exclusions** or the **Audit Settings - Sessions Exclusions** options in the left pane.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject**—WebInspect will not request files of the type you specify.
- **Exclude**—WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

By default, most image, drawing, media, audio, video, and compressed file types are rejected.

To add a file extension:

1. Click **Add**.

   The *Exclusion Extension* window opens.
2. In the **File Extension** box, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

Excluded MIME Types

WebInspect will not process files associated with the MIME type you specify.

To add a MIME Type:

1. Click **Add**.

   The *Provide a Mime-type to Exclude* window opens.
2. In the **Exclude Mime-type** box, enter a MIME type.
3. If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.
4. Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject**—WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.

- **Exclude**—During a crawl, WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The *Reject or Exclude a Host or URL* window opens.

2. Select either **Host** or **URL**.
3. In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The *Create Exclusion* window opens.

2. Select an item from the **Target** list.
3. If you selected **Query Parameter** or **Post Parameter** as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
   - **Matches Regex**: Matches the regular expression you specify in the **Match String** box.
   - **Matches Regex Extension**: Matches a syntax available from HP's regular expression extensions you specify in the **Match String** box.
   - **Matches**: Matches the text string you specify in the **Match String** box.
   - **Contains**: Contains the text string you specify in the **Match String** box.
5. In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click  .
7. (Optional) Repeat step 2 through step 6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	n/a	contains	Microsoft.com

Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	n/a	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	n/a	matches regex	/W3SVC[0-9]*/

Allowed Hosts

Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl and audit.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As WebInspect scans the target site, if it encounters a link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, WebInspect would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Note that if you specify a port number, then the allowed host must be an exact match.

To add allowed domains:

1. Click **Add**.
2. On the *Specify Allowed Host* window, enter a URL (or a regular expression representing a URL) and click **OK**.

When specifying the URL, do not include the protocol designator (such as http:// or https://).

To edit or remove an allowed domain:

1. Select a domain from the **Allowed Hosts** list.
2. Click **Edit** or **Remove**.

HTTP Parsing

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, “userid” is the parameter you would identify.

You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, “1234567” is the session information:

```
http://www.onlinestore.com/bikes/(1234567)/index.html
```

The regular expression for identifying the parameter would be: /\([\w\d]+\)/

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. The defaults identify ASP.NET cookieless session IDs.

HTTP Parameters Used for Navigation

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

Ex. 1 -- http://www.anysite.com?Master.asp?Page=1

Ex. 2 -- http://www.anysite.com?Master.asp?Page=2;

Ex. 3 -- http://www.anysite.com?Master.asp?Page=13;Subpage=4

Ordinarily, WebInspect would assume that these three requests refer to identical resources and would conduct a vulnerability scan on only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

Examples 1 and 2 contain one resource parameter: “Page.”

Example 3 contains two parameters: “Page” and “Subpage.”

To identify resource parameters:

1. Click **Add**.
2. On the *HTTP Parameter* window, enter the parameter name and click **OK**.

   The string you entered appears in the **Parameter** list.
3. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document. For pages that do not announce their character set, you can specify which character set WebInspect should use.

Custom Parameters

Custom Parameters are used to accommodate sites that use URL rewriting techniques and/or Representation State Transfer (REST) web services technologies. You can write rules for these custom parameters, or you can import rules from a common configuration file written in Web Application Description Language (WADL). In addition to applying these rules that you discretely define or import, WebInspect will attempt (during a scan) to identify custom parameters and create rules to accommodate them. WebInspect will save these rules in the Custom Parameters settings and will suggest them as recommendations.

URL Rewriting

Many dynamic sites use URL rewriting because static URLs are easier for users to remember and are easier for search engines to index the site. For example, an HTTP request such as

http://www.pets.com/ShowProduct/7

is sent to the server's rewrite module, which converts the URL to the following:

http://www.pets.com/ShowProduct.php?product_id=7

In this example, the URL causes the server to execute the php script “ShowProduct” and display the information for product number 7.

When WebInspect scans a page, it must be able to determine which elements are variables so that its attack agents can thoroughly check for vulnerabilities. To enable this, you must define rules that identify these elements. You can do so using either Simplified Syntax or Regular Expression syntax.

Examples:

HTML: User 1 details
Rule: http://samplesite.com/someDetails/{username}/

HTML: User 1 details
Rule: http://samplesite.com/ TwoParameters/Details/{username}/{parameter2}

HTML: User 1 details
Rule: http://samplesite.com/{parameter2}/PreFixParameter/Details/{username}

RESTful Services

A RESTful web service (also called a RESTful web API) is a simple Web service implemented using HTTP and the principles of REST. It has gained widespread acceptance across the Web as a simpler alternative to SOAP- and Web Services Description Language (WSDL)-based Web services.

The following request adds a name to a file using an HTTP query string.

```
GET /adduser?name=Robert HTTP/1.1
```

This same function could be achieved by using the following method with a Web service. Note that the parameter names and values have been moved from the request URI and now appear as XML tags in the request body.

```
POST /users HTTP/1.1
Host: myserver
Content-Type: application/xml
<?xml version=”1.0”?>
<user> <name>Robert</name>
</user>
```

In the case of both URL rewriting and RESTful web services, you must create rules that instruct WebInspect how to create the appropriate requests.

To create a rule:

1. Click **New Rule**.
2. In the Expression column, enter a rule. See Creating Rules for Matrix and Path Parameters on page 144 for guidelines and examples.

The enabled check box is selected by default. WebInspect examines the rule and, if valid, removes the red **X**.

To delete a rule:

1. Select a rule from the **Custom Parameters Rules** list.
2. Click **Delete**.

To disable a rule without deleting it:

1. Select a rule.
2. Clear the check mark in the **Enabled** column.

To import a file containing rules:

1 Click Import 

2 Using a standard file-selection dialog, select the type of file (`.wadl` or `.txt`) containing the custom rules you want to apply.

3 Locate the file and click **Open**.

Enable automatic seeding of rules which were not used during a scan

The most reliable rules for custom parameters are those deduced from a WADL file or created by developers of the Web site. If a rule is not invoked during a scan (because the rule doesn't match any URL), then WebInspect can programmatically assume that a valid portion of the site has not been attacked. Therefore, if you select this option, WebInspect will create sessions to exercise these unused rules in an effort to expand the attack surface.

Double Encode URL Parameters

Double-encoding is an attack technique that encodes user request parameters twice in hexadecimal format in an attempt to bypass security controls or cause unexpected behavior from the application. For example, a cross-site scripting (XSS) attack might normally appear as:

<script>alert('FOO')</script>

This malicious code could be inserted into a vulnerable application, resulting in an alert window with the message “FOO.” However, the web application can have a filter that prohibits characters such as < (less than) > (greater than) and / (forward slash), since they are used to perform Web application attacks. The attacker could attempt to circumvent this safeguard by using a “double encoding” technique to exploit the client’s session. The encoding process for this Javascript is:

Char	Hex encode	Encoded % Sign	Double encoded result
<	%3C	%25	%253C
/	%2F	%25	%252F
>	%3E	%25	%253E

Finally, the malicious code, double-encoded, is:

%253Cscript%253Ealert('XSS')%253C%252Fscript%253E

If you select this option, WebInspect will create double-encoded URL parameters (instead of single-encoded parameters) and submit them as part of the attack sequence. This is recommended when the Web server uses, for example, Apache mod-rewrite plus PHP or Java URL Rewrite Filter 3.2.0.

Creating Rules for Matrix and Path Parameters

There are three ways rules can be created in the system. Rules may be:

- Entered manually
- Generated from a WADL file specified by the user or received through SecurityScope
- Imported from a flat file containing a list of rules

When entering rules manually, you specify the path segments of a URL that should be treated as parameters.

The rules are actually modified URLs that use special characters to designate parts of the actual URL that contain parameters. If URL matches a rule, WebInspect parses the parameters and attacks them. Notable components of a rule (and of a URL) are:

- Scheme (HTTP/HTTPS)
- Authority (username + hostname + port)
- Path (gp/c/{book_name}/)
- Query (anything that follows "?")
- Fragment (anything that follows "#")

Definition of Path Segment

A path segment starts with '/' characters and is terminated either by another '/' character or by end of line. To illustrate, path "/a" has one segment whereas path "/a/" has two segments (the first containing the string "a" and the second being empty. Note that paths "/a" and "/a/" are not equal. When attempting to determine if a URL matches a rule, empty segments are considered.

Special Elements for Rules

A rule may contain the following special elements.

* (Asterisk) May appear in production defined below; presence in non-path productions means that this part of the URL will not participate in matching (or, in other words, will match anything).

{…} (Group) A named parameter that may appear within the path of the rule. The content has no special meaning and is used during reporting as the name of the attacked parameter. The character set allowed within a group is defined in RFC 3986 as *pchar:

- pchar = unreserved / pct-encoded / sub-delims / ":" / "@"
- pct-encoded = "%" HEXDIG HEXDIG
- unreserved = ALPHA DIGIT - . _ ~
- reserved = gen-delims / sub-delims
- gen-delims = : / ? # [ ] @ "
- sub-delims = ! $ & ' ( ) * + , ; =

A group's content cannot include the "open bracket" and "close bracket" characters, unless escaped as pct-encoded element.

The rules for placing * out of path are described below. Within a path segment, any amount of * and {} groups can be placed, provided they're interleaved with plain text. For example:

Valid rule: http://www.amazon.com/gp/c/*={param}

Invalid rule: http://www.amazon.com/gp/c/*{}

Rules with segments having **, *{}, {}* or {}{} entries are invalid.

For a rule to match a URL, all components of the rule should match corresponding components of the crawled URL. Path comparison is done segment-wise, with * and {} groups matching any number of characters (including zero characters), plain text elements matching corresponding plain text elements of the path segment of the URL. So, for example:

http://www.amazon.com/gp/c/{book_name} is a match for these two URLs:

http://www.amazon.com:8080/gp/c/Moby_Dick

http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0

but is not a match for any of these:

https://www.amazon.com/gp/c/Hobbit

http://www.amazon.com /gp/c/Moby_Dick/

http://www.amazon.com/gp/c/Sex_and_the_City/Horror

WebInspect treats elements of path segments matched by {…} groups in the rule URL as parameters, similar to those found in a query. Moreover, query parameters of crawled URLs matched by rule will be attacked along with parameters within the URL's path. In the following example of a matched URL, WebInspect would conduct attacks on the format and price parameters and on the third segment of the path (Singularity_Sky):

http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0

Asterisk Placeholder

The "*" placeholder may appear in the following productions and subproductions of the URL:

- Schema – as in *://www.amazon.com/{param}, which will match both HTTP and HTTPS.
- Authority – as in http://*/{param}, which will match all hosts, ports and userinfos.
  - Userinfo – as in http://*@amazon.com/{param}, which will match any username and password.
    - Username – as in http://*:my_password@amazon.com/{param}, which will match any username with given password.
    - Password – as in http://john:*@amazon.com/{param}, which will match any password for a given username.
  - Hostname – as in http://john:password@*/{param}, which will match any host provided the username and password are as defined.
    - Host fragments – as in http://*.amazon.com/{param}, which will match any host within amazon.com domain.
    - Port – as in http://www.amazon.com:*/{param}, which will match any port for www.amazon.com host.
- Path – cannot be matched as a whole, since * in path matches a single segment or less.
  - Path segments – as in http://www.amazon.com/gp/*/{param}, which will match URLs with schema HTTP, hostname www.amazon.com, path containing three segments (first is exactly "gp", second is any segment, and the third segment will be treated as parameter and won't participate in matching).
  - Part of path segment – as in http://www.amazon.com/gp/ref=*, which will match URLs with schema HTTP, hostname www.amazon.com, path containing two segments (first is exactly "gp", second containing any string with prefix "ref=").
- Query – as in http://www.amazon.com/gp/c/{param}?*, which match any URL with schema HTTP, hostname www.amazon.com, path of three segments (first segment is "gp", second segment is "c" and third segment being a parameter, so it won't participate in matching); this URL also MUST contain a query string of arbitrary structure. Note the difference between rules http://www.amazon.com/gp/c/{param}and http://www.amazon.com/gp/c/{param}?*. First rule will match URL http://www.amazon.com/gp/c/Three_Little_Blind_Mice, while second will not.
  - Key-value pair of query – as in http://www.amazon.com/gp/c/{param}?format=* which will match URL only if query string has exactly one key-value pair, with key name being "format."
  - Key-value pair of query – as in http://www.amazon.com/gp/c/{param}?*=pdf which will match URL only if query string has exactly one key-value pair, with value being "pdf."

- Fragment – as in case http://www.amazon.com/gp/c/{param}#* which match any URL with fragment part being present.

The main benefit of using placeholders is that it enables you to create rules that combine matrix parameters and URL path-based parameters within single rule. For relevant URL

http://www.amazon.com/gp/color;foreground=green;background=black/something?format=dvi

the following rule will allow attacks on all parameters

gp/*/{param}

with the matrix parameter segment being ignored by * placeholder within second segment of the path, but recognized by WebInspect and attacked properly.

In the case of multiple rules matching a given URL, there are two options.

- Stop iterating over the rules once a match is found and so use only the first rule.
- Iterate over all of the rules and collect all custom parameters that match.

For instance, for the following URL

http://mySite.com/store/books/Areopagitica/32/1

the following rules both match

*/books/{booktitle}/32/{paragraph}

store/*/Areopagitica/{page}/{paragraph}

WebInspect will try to collect parameters from both rules to ensure the greatest attack coverage, so all three segments ("Areopagitica", "32" and "1" in the example above) will be attacked.

Filters

Use these settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use WebInspect or those who have access to the raw data or generated reports.

If the text you specify is found, WebInspect reports it on the **Information** tab as a "Hidden Reference Found" vulnerability.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

To add a rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.

   The *Add Request/Response Data Filter Criteria* window opens.

2. In the **Search For Text** box, type (or paste) the string you want to locate (or enter a regular expression representing the string).

   Click  to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an expression).

3 In the **Search For Text In** box, select an area to search:

- For Requests: select **All**, **Headers**, or **Postdata**.
- For Responses: select **All**, **Headers**, or **Body** (that is, the code of the page itself).

4 Type (or paste) the replacement string in the **Replace search text with** box.

5 For case-sensitive searches, select the **Case-Sensitive Match** check box.

6 Click **OK**.

Cookies/Headers

Standard Header Parameters

Include 'referer' in HTTP request headers

Select this check box to include referer headers in WebInspect HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.

Include 'host' in HTTP request headers

Select this check box to include host headers with WebInspect HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when WebInspect is auditing that site. You can add multiple custom headers.

The default custom headers are described in the following table.

Header	Description
Accept: */*	Any encoding or file type is acceptable to the crawler.
Pragma: no-cache	This forces a fresh response; cached or proxied data is not acceptable.

To add a custom header:

1 Click **Add**.

The *Specify Custom Header* window opens.

2 In the **Custom Header** box, enter the header using the format <name>: <value>.

3 Click **OK**.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by WebInspect to the server when conducting a vulnerability scan.

To add a custom cookie:

1 Click **Add**.

The *Specify Custom Cookie* window opens.

2 In the Custom Cookie box, enter the header using the format <name>=<value>.

For example, if you enter

```
CustomCookie=ScanEngine
```

then each HTTP-Request will contain the following header:

```
Cookie: CustomCookie=ScanEngine
```

3 Click **OK**.

Proxy

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server will not be used.

Configure proxy using a PAC file

Load proxy settings from the Proxy Automatic Configuration (PAC) file in the location you specify in the **URL** box.

Explicitly configure proxy

Configure a proxy by entering the requested information.

1 In the **Server** box, type the URL or IP address of your proxy server, followed (in the Port box) by the port number (for example, 8080).

2 Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.

3 If authentication is required, select a method from the **Authentication** list:

Authentication	Description
Basic	A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.
NTLM	NTLM (NT LAN Manager) is an authentication process used by all members of the Windows NT family of products. It uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network. Use NTLM authentication for servers running IIS.
Kerberos	Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.
Digest	The Windows Server 2003 operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.
Automatic	Allow the Web Form Editor to determine the correct authentication method. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
Negotiate	If both the server and client are using Windows 2000 or later, Kerberos authentication is used. Otherwise, NTLM authentication is used. This method is also known as Integrated Windows authentication.

4 If your proxy server requires authentication, enter the qualifying user name and password.

5 If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

Specify Alternative Proxy for HTTPS

For proxy servers accepting HTTPS connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information (described in the previous table).

Authentication

Authentication is the verification of identity as a security measure. Passwords and digital signatures are forms of authentication. You can configure automatic authentication so that a user name and password will be entered whenever WebInspect encounters a server or form that requires authentication. Otherwise, a crawl might be prematurely halted for lack of logon information.

Scan requires network authentication

Select this check box if users must log on to your Web site or application using assigned credentials. You may then select the authentication method and specify the credentials.

WebInspect will crawl all servers granted access by this password. To avoid potential damage to your administrative systems, do not use a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact HP technical support.

See step 3 on page 150 for a description of the available authentication methods.

Client Certificates

Client certificate authentication allows users to present client certificates rather than entering a user name and password. To use client certificates.

1. Select **Enable** in the **Client Certificates** group.
2. Click **Select** to open the *Client Certificates* window.
3. Choose a certificate.
4. Click **OK**.

Client Certificates for Tools

When using Step Mode or other tools that incorporate a proxy (specifically Web Macro Recorder, Web Proxy, Web Brute, and Web Form Editor), you may encounter servers that do not ask for a client certificate, even though a certificate is required. To accommodate this situation, you must edit the `SPI.Net.Proxy.Config` file using the following procedure:

Task 1: Find your certificate's serial number

1. Open Microsoft Internet Explorer.
2. Click **Tools** → **Internet Options**.
3. On the *Internet Options* window, select the **Content** tab and click **Certificates**.
4. On the *Certificates* window, select a certificate and click **View**.
5. On the *Certificate* window, click the **Details** tab.
6. Click the **Serial Number** field and copy the serial number that appears in the lower pane (highlight the number and press Ctrl + C).
7. Close all windows.

Task 2: Create an entry in the SPI.Net.Proxy.Config file

1. Open the `SPI.Net.Proxy.Config` file for editing. The default location is `C:\Program Files (x86)\HP\HP WebInspect Enterprise 10.10 Console`.

2 In the ClientCertificateOverrides section, add the following entry:

<ClientCertificateOverride HostRegex="RegularExpression" CertificateSerialNumber="Number"/>

where:

RegularExpression is a regular expression matching the host URL (example: .*austin\.hp\.com).

Number is the serial number obtained in Task 1.

3 Save the edited file.

Use a login macro for forms authentication

This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent WebInspect from terminating prematurely if it inadvertently logs out of your application. When recording this type of macro, be sure to specify the application's log-out signature. Click the browse button  to locate and load a macro. To record a macro, enter the starting URL in the **Initial recorder location** box and click **Record**. The Web Macro Recorder then opens.

Login Macro Parameters

This section appears only if you have selected **Use a login macro for forms authentication** and the macro you have chosen or created contains fields that are designated as Smart Credentials (if you used the Event-Based IE Compatible Web Macro Recorder) or username and password parameters (if you used the Web Macro Recorder).

If you start a scan using a macro that includes Smart Credentials (or parameters for user name and password), then when you scan the page containing the input elements associated with these entries, WebInspect substitutes the user name and password specified here. This allows you to create the macro using your own user name and password, yet when other persons run the scan using this macro, they can substitute their own user name and password.

Use a startup macro

This type of macro is used to acquire state by logging in to a particular area of the application, but does not contain logic that will prevent WebInspect from logging out. Use this type of macro if you cannot determine a logout signature or if the application cannot log you out.

Click the browse button  to locate the macro. Click **Record** to record a macro.

File Not Found

Determine 'File Not Found' (FNF) using HTTP response codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server.

- **Forced valid response codes (never a FNF)**—You can specify HTTP response codes that should never be treated as a file-not-found response.
- **Forced FNF response codes (always a FNF)**—Specify those HTTP response codes that will always be treated as a file-not-found response. WebInspect will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a comma.

Determine 'FNF' from custom supplied signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result in WebInspect from 404 pages that are unique to your site.

Auto detect 'FNF' page

Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found, or they might redirect to a home page or login page. Select this check box if you want WebInspect to detect these "custom" file-not-found pages.

WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource.

If you select the **Auto detect** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

Policy

Select a policy to be used as the default whenever you start a scan.

You can substitute a different policy when starting a scan through the Scan Wizard, but the policy you select here will be used if you do not select an alternate.

You can also create, import, edit, or delete policies.

Create a Policy

Use the following procedure to create a policy:

1. Click **Create**.

   The Policy Manager tool opens.
2. Select **File** → **New** (or click the New Policy icon).
3. Select the policy on which you will model a new one.
4. Refer to the on-line Help for additional instructions.

Import a Policy

Use the following procedure to import a policy:

1. Click **Import**.
2. On the *Import Custom Policy* window, click the browse button .
3. Using the **Files Of Type** list on the standard file-selection window, choose a policy type:
   - **Policy Files (*.policy)**—Policy files designed and created for versions of WebInspect beginning with release 7.0.
   - **Old Policy Files (*.apc)**—Policy files designed and created for versions of WebInspect prior to release 7.0.
   - **All Files (*.*)**—Files of any type, including non-policy files.

4 (optional) Edit the policy name.

5 Click **OK**.

A copy of the policy is created in the Policies folder (the default location is C:\Documents and Settings\All Users\Application Data\HP\HP WebInspect\Policies\). The policy and all of its enabled checks are imported into SecureBase using the specified policy name.

Delete a Policy

Use the following procedure to delete a policy:

1 Select a custom policy.

Only custom policies may be deleted.

2 Click **Delete**.

Edit a Policy

Use the following procedure to edit a policy:

1 Select a custom policy. Only custom policies may be edited.

2 Click **Edit**.

The Policy Manager tool opens. Refer to the on-line Help for additional instructions.

Advanced Crawl Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Crawl Settings described in this section. The Advanced Crawl Settings for Guided Scan are similar but not identical to those for a Web Site Scan.

The WebInspect crawler is a software program designed to follow hyperlinks throughout a Web site, retrieving and indexing pages to document the hierarchical structure of the site. The parameters that control the manner in which WebInspect crawls a site are available in the Crawl Settings category.

These settings are not displayed if you select the **Audit Only** option in the Scan Settings - Method category.

Link Parsing

WebInspect will follow all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (if you select the JavaScript/VBScript analyzer option on the Crawl Settings - Content Analyzers panel). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, use the Custom Links feature to identify (using regular expressions) links that you want WebInspect to follow.

To add a specialized link identifier:

1 Click **Add**.

The *Specialized Link Entry* window opens.

2 In the **Specialized Link Pattern** box, enter a regular expression designed to identify the link.

3 (Optional) Enter a description of the link in the **Comment** box.

4 Click **OK**.

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the Scan Settings - Session Exclusions panel.

This panel (Crawl Settings - Session Exclusions) allows you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested.

If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1 Click **Add**.

The *Exclusion Extension* window opens.

2 In the **File Extension** box, enter a file extension.

3 Select either **Reject**, **Exclude**, or both.

4 Click **OK**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited.

To add a MIME Type:

1 Click **Add**.

The *Provide a Mime-type to Exclude* window opens.

2 In the **Exclude Mime-type** box, enter a MIME type.

3 If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.

4 Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session (during the crawl) that contains that component.

- **Reject**—WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude**—During a crawl, WebInspect will not examine the specified URL or host for links to other resources. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

To edit the default criteria:

1 Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

The *Reject or Exclude a Host or URL* window opens.

2 Select either **Host** or **URL**.

3 In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.

4 Select either **Reject**, **Exclude**, or both.

5 Click **OK**.

To add exclusion/rejection criteria:

1 Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).

The *Create Exclusion* window opens.

2 Select an item from the **Target** list.

3 If you selected **Query Parameter** or **Post Parameter** as the target, enter the **Target Name**.

4 From the **Match Type** list, select the method to be used for matching text in the target:

- **Matches Regex**: Matches the regular expression you specify in the **Match String** box.
- **Matches Regex Extension**: Matches a syntax available from HP's regular expression extensions you specify in the **Match String** box.
- **Matches**: Matches the text string you specify in the **Match String** box.
- **Contains**: Contains the text string you specify in the **Match String** box.

5 In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.

6 Click  .

7 (Optional) Repeat step 2 through step 6 to add more conditions. Multiple matches are ANDed.

8 If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.

9 Click **OK**.

10 When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	n/a	contains	Microsoft.com

Example 2

Enter “logout” as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the “logout” example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	n/a	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter “username” equals “John.”

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	n/a	matches regex	/W3SVC[0-9]*/

The default setting URL: \?[DNMSCO]=[ADNSM] is used for Apache directory indexing. These are sort options for the listing, which have no real impact on the page contents. An example would be http://www.w3.org/Icons/?C=M;O=A.

Advanced Audit Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Audit Settings described in this section. The Advanced Audit Settings for Guided Scan are similar but not identical to those for a Web Site Scan.

An audit is the probe or attack conducted by WebInspect that is designed to detect vulnerabilities. The parameters that control the manner in which WebInspect conducts that probe are available from the Audit Settings category.

These settings are not displayed if you select the **Crawl Only** option in the Scan Settings - Method category.

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel.

This panel (Audit Settings - Session Exclusions) allows you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested.

If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1 Click **Add**.

The *Exclusion Extension* window opens.

2 In the **File Extension** box, enter a file extension.

3 Select either **Reject**, **Exclude**, or both.

4 Click **OK**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited.

To add a MIME type:

1 Click **Add**.

The *Provide a Mime-type to Exclude* window opens.

2 In the **Exclude Mime-type** box, enter a MIME type.

3 If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.

4 Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session (during the audit) that contains that component.

- **Reject**—WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude**—During the audit portion of the scan, WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

To edit the default criteria:

1 Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

The *Reject or Exclude a Host or URL* window opens.

2 Select either **Host** or **URL**.

3 In the **Host/URL** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.

4 Select either **Reject**, **Exclude**, or both.

5 Click **OK**.

To add exclusion/rejection criteria:

1 Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** list).

The *Create Exclusion* window opens.

2 Select an item from the **Target** list.

3 If you selected **Query Parameter** or **Post Parameter** as the target, enter the **Target Name**.

4 From the **Match Type** list, select the method to be used for matching text in the target:

- **Matches Regex**: Matches the regular expression you specify in the **Match String** box.
- **Matches Regex Extension**: Matches a syntax available from HP's regular expression extensions you specify in the **Match String** box.
- **Matches**: Matches the text string you specify in the **Match String** box.
- **Contains**: Contains the text string you specify in the **Match String** box.

5 In the **Match String** box, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.

6 Click  .

7 (Optional) Repeat step 2 through step 6 to add more conditions. Multiple matches are ANDed.

8 If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.

9 Click **OK**.

10 When the exclusion appears in the **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	n/a	contains	Microsoft.com

Example 2

Enter “logout” as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the “logout” example, WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	n/a	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter “username” equals “John.”

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	n/a	matches regex	/W3SVC[0-9]*/

Attack Exclusions

Excluded Parameters

Use this feature to prevent WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

1. In the **Excluded Parameters** group, click **Add**.

   The *Specify HTTP Exclusion* window opens.

2. In the **HTTP Parameter** box, enter the name of the parameter you want to exclude.

   Click  to insert regular expression notations.

3. Choose the area in which the parameter may be found: **HTTP query data** or **HTTP POST data**. You can select both areas, if necessary.

4. Click **OK**.

Excluded Cookies

Use this feature to prevent WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values.

This setting requires you to enter the name of a cookie. In the following example HTTP response …

Set-Cookie: FirstCookie=Chocolate+Chip; path=/

…the name of the cookie is "FirstCookie."

To exclude certain cookies.

1 In the **Excluded Cookies** group, click **Add**.

The Regular Expression Editor appears.

You can specify a cookie using either a text string or a regular expression.

2 To enter a text string:

a In the **Expression** box, type a cookie name.

b Click **OK**.

3 To enter a regular expression:

a In the **Expression** box, type or paste a regular expression that you believe will match the text for which you are searching.

Click  to insert regular expression notations.

b In the **Comparison Text** box, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** box).

c To find only those occurrences matching the case of the expression, select the **Match Case** check box.

d If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** box.

e Click **Test** to search the comparison text for strings that match the regular expression. Matches will be highlighted in red.

f Did your regular expression identify the string?

NO—Verify that the Comparison Text contains the string you want to identify or modify the regular expression.

YES—Click **OK**.

Excluded Headers

Use this feature to prevent WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression using the procedure described below.

1 In the **Excluded Headers** group, click **Add**.

The Regular Expression Editor appears.

You can specify a header using either a text string or a regular expression.

2 To enter a text string:

a In the **Expression** box, type a header name.

b Click **OK**.

3 To enter a regular expression:

a In the **Expression** box, type or paste a regular expression that you believe will match the text for which you are searching.

Click  to insert regular expression notations.

b In the **Comparison Text** box, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** box).

c To find only those occurrences matching the case of the expression, select the **Match Case** check box.

d If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** box.

e Click **Test** to search the comparison text for strings that match the regular expression. Matches will be highlighted in red.

f Did your regular expression identify the string?

NO—Verify that the Comparison Text contains the string you want to identify or modify the regular expression.

YES—Click **OK**.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs.

To launch the tool, click **Audit Inputs Editor**.

To load inputs that you previously created using the editor, click **Import Audit Inputs**.

For detailed instructions on using the Audit Inputs Editor, see Audit Inputs Editor on page 179.

Attack Expressions

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- ja-jp: Japanese and Japan
- ko-kr: Korean and Korea
- zh-cn: Chinese and China

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Vulnerability Filtering

By applying certain filters (listed below), you can modify the results of a vulnerability scan to accommodate your specific testing environment.

- **Standard Vulnerability Definition**: This filter reports vulnerabilities in the same manner as QAInspect.
- **Standard Vulnerability Definition - New**:
- **403 Blocker**: This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Parameter Vulnerability Roll-Up**: This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **Response Inspection Dom Event Parent-Child**: This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

Adding a Filter

To add a filter to your default settings:

1. In the **Audit Settings** panel in the left column, select **Vulnerability Filtering**.

   All available filters are listed in either the **Disabled Filters** list or the **Enabled Filters** list.

2. To enable a filter, select a filter in the **Disabled Filters** list and click **Add**.

   The filter is removed from the **Disabled Filters** list and added to the **Enabled Filters** list.

3. To disable a filter, select a filter in the **Enabled Filters** area and click **Remove**.

   The filter is removed from the **Enabled Filters** list and added to the **Disabled Filters** list.

Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select **Enable Smart Scan**, you can choose one or more of the identification methods described below.

Use regular expressions on HTTP responses to identify server/application types

This method, employed by previous releases of WebInspect, searches the server response for strings that match predefined regular expressions designed to identify specific servers.

Use server analyzer fingerprinting and request sampling to identify server/application types

This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server/application type.

Custom server/application type definitions (more accurate detection)

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.

The *Server/Application Type Entry* window opens.

2 In the **Host** box, enter the domain name or host, or the server's IP address.

3 (Optional) Click **Identify**.

WebInspect contacts the server and uses the server analyzer fingerprinting method to determine the server type. If successful, it selects the corresponding check box in the **Server/Application Type** list.

Alternatively, if you select the **Use Regular Expressions** option, enter a regular expression designed to identify a server. Click  to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an expression).

4 Select one or more entries from the **Server/Application Type** list.

5 Click **OK**.

A Policies

Introduction

A policy is a collection of vulnerability checks and attack methodologies that HP scanners deploy against a Web application. All policies contain all possible audit engines and agents, but each policy has a different subset of these components enabled. Although your environment may also include custom policies designed by your developers, the standard installation contains the prepackaged policies described in the following section.

Policies

- **Aggressive SQL Injection**—The Aggressive SQL Injection policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs out a more accurate and decisive job, but has a longer scan time.
- **All Checks**—An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the check database. This includes checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.
- **Application**—The Application policy performs a security assessment of your Web application by submitting known and unknown Web application attacks, and only submits specific attacks that assess the application layer. When performing assessments of enterprise level Web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your assessment in terms of speed and memory usage.
- **Assault**—An assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers. An assault scan includes checks that can create denial-of-service conditions.

  You are strongly advised to use assault scans in test environments only.

- **Blank**—This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Criticals and Highs**—Use the Criticals and Highs policy to quickly scan your Web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.

- **Cross-Site Scripting**—This policy performs a security assessment of your Web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a Web site to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **Dev**—A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web application layer only. The Developer policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **DevInspectEclipse**—The DevInspectEclipse policy is the standard policy for use by DevInspect Java Eclipse. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **DevInspectVS**—The DevInspect VS policy is the standard policy for use by DevInspect VS. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **OWASP Top Ten**—Many government agencies suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application.
- **Passive Scan**—The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **Platform**—The Platform policy performs a security assessment of your Web application platform by submitting attacks specifically against the Web server and known Web applications. When performing assessments of enterprise-level Web applications, use the Platform policy in conjunction with the Application policy to optimize your assessment in terms of speed and memory usage.
- **QA**—The QA policy is designed to help QA professionals make project release decisions in terms of Web application security. It performs checks for both known and unknown Web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
- **Quick**—A quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the Web server, Web application server and Web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **Safe**—A safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown vulnerabilities at the Web server, Web application server and Web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.
- **SQL Injection**—The SQL Injection policy performs a security assessment of your Web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the Web application for execution by a backend database.
- **Standard**—A Standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server and Web application layers. A Standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

B WebInspect Enterprise Tools

Introduction

The WebInspect Enterprise Console includes a robust set of tools and configuration options. The following tools are available from the WebInspect Enterprise Console Tools menu:

- Smart Update
- Options
- Encoders/Decoders
- HTTP Editor
- Regular Expression Editor
- Web Proxy
- Web Form Editor
- Web Macro Recorder (Unified)
- Web Service Test Designer
- SQL Injector
- Web Brute
- Web Discovery
- Cookie Cruncher
- Web Fuzzer
- Server Analyzer

In addition, the following tools are also available:

- Policy Manager (accessible from the WebInspect Enterprise Console using the Scan Policies form in the Scans group)
- Audit Inputs Editor (accessible from the Policy Manager's **Tools** menu)

Certain tools are not enabled unless HP WebInspect and the WebInspect Enterprise Console are installed on the same machine.

Options

Use the following procedure to specify settings for the WebInspect Enterprise Console.

1. From the **Tools** menu, select **Options**.
2. To refresh the display of WebInspect Enterprise information periodically, select the **Automatically refresh display** check box and specify how often (in seconds) the display should be updated.
3. Click **OK**.

Policy Manager

A policy is a collection of audit engines and attack agents that HP scanners use when auditing or crawling your Web application. Each component has a specific task, such as testing for susceptibility to cross-site scripting, building the site tree, probing for known server vulnerabilities, etc. These components are organized into the following groups:

- Audit Engines
- Audit Options
- Directory Enumeration
- Unknown Application Testing
- Web Application Servers
- Web Applications
- Web Servers
- Custom Checks

All these components (except for the Audit Engines) are known collectively as attack groups. Each attack group contains subgroups of individual modules (called attack agents) that check your Web site for vulnerabilities.

WebInspect Enterprise contains several prepackaged policies designed to accommodate the majority of users. All policies contain all possible audit engines and agents, but each policy has a different subset of these components enabled. You edit a policy by enabling or disabling audit engines and/or individual attack agents (or groups of agents). You create a policy by editing an existing policy and saving it with a new name.

Views

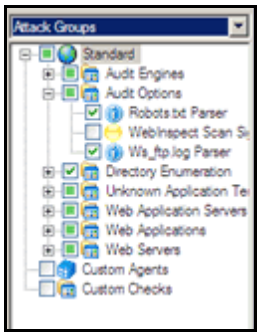
The Policy Manager has the following views, selectable from the **View** menu or by clicking icons on the toolbar:

- Standard
- Search

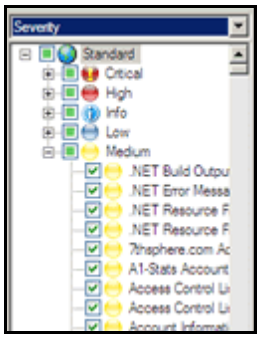
Standard View

This view displays, by default, a list of checks categorized by threat class (according to classifications established by the Web Application Security Consortium). Alternatively, a drop-down list allows you to display all attack agents by severity, or a list of audit engines and attack groups.

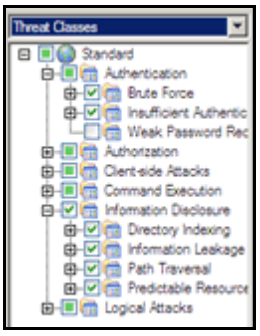
You enable or disable a component by selecting or clearing its associated check box.



Attack Groups



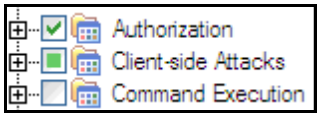
Severity



Threat Classes

The check box next to an unexpanded node indicates the "selected" status of the objects within the node.

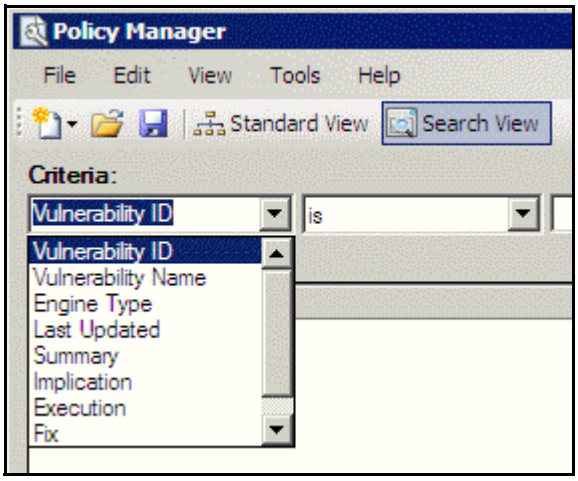
- A check means all objects are selected.
- A green square means some objects are selected.
- An empty box means no objects are selected.



Click the plus sign ⊞ to expand a node.

Search View

The Search view allows you to locate attack agents containing the text you specify in a selected report field (i.e., summary, implication, execution, recommendation, and fix). This feature is used most often to identify checks that you want to disable. For example, if you are scanning an application that does not contain PHP scripting, you could search summary fields for "PHP." When the Policy Manager lists the attack agents that match your search criteria, you could disable an agent by clearing its associated check box. Then, you can either save the modified policy (making the policy changes permanent) or simply apply the modified policy to the current scan.



Creating or Editing a Policy

You cannot permanently change the policies that are packaged with WebInspect Enterprise. However, you may open any of them as a template, modify their contents to create a custom policy, and save the customized policy under a new name. A custom policy may be edited and saved without changing its name.

To edit a policy:

1. On the WebInspect Enterprise Console, click the **Scans** group.
2. Click the **Scan Policies** shortcut.
3. Select a policy.
4. Click the **Action** menu and select **Copy**.

   The WebInspect Enterprise Console downloads the policy from the server and loads it into the Policy Manager.
5. Disable (or enable) an attack group by clearing (or selecting) its associated check box. To disable or enable an individual agent within a group, first expand the group and then edit its check box.
6. To rename an attack group:
   a. Right-click the attack group.
   b. Choose **Rename** from the shortcut menu.
7. To add an attack group:
   a. Right-click any existing attack group and choose **New Attack Group** from the shortcut menu. A highlighted entry named New Attack Group appears.
   b. Right-click the new group and choose **Rename**.
   c. Populate the group by dragging and dropping attack agents onto it.
8. You may also create a custom check. See Creating a Custom Check on page 170 for more information.
9. If you select the **Auto Update** check box, HP scanners determine if any updated or new attack agents downloaded from the HP database should be enabled or disabled, based on the analysis of its sibling agents. For example, if you disable attack agents targeting Microsoft's Internet Information Server (IIS), and you select **Auto Update**, then the scanner will not enable any IIS-related attack agent that it downloads to your system. Conversely, any new or updated attack agents that are related to agents that are enabled in your policy will also be enabled.

   New vulnerability checks downloaded via Smart Update are not added automatically to any custom policies you may have created.
10. Select **File** → **Save As**. Type a name for your custom policy in the **File name** box and then click **Save**. You cannot save a policy using the name of a prepackaged policy (Assault, Blank, Standard, etc.).

Creating a Custom Check

Although HP scanners rigorously inspect your entire Web site for real and potential security vulnerabilities, you may require a custom check to detect vulnerabilities that are unique to your application.

To create a custom check:

1. On the WebInspect Enterprise Console, click the **Scans** group.
2. Click the **Scan Policies** shortcut.
3. Select a policy.

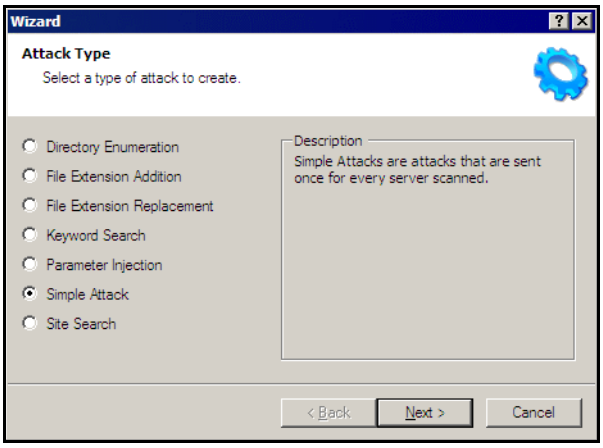
4 Click the **Action** menu and select **Copy**.

The WebInspect Enterprise Console downloads the policy from the server and loads it into the Policy Manager.

5 Make sure the Standard view is selected, with attack groups listed in the left pane.

6 Right-click on **Custom Checks** and select **New Custom Check** from the shortcut menu.

7 When the Custom Check Wizard appears, select an attack type.



The attack types are listed below. See step 9 on page 174 and step 10 on page 175 for entering attack and signature information.

- **Directory enumeration**

  This type of check searches for a directory of the name you specify.

Attack Type:	Directory Enumeration
Attack:	/directory_name/ [where directory_name is the name of the directory you want to find]
Signature:	[STATUSCODE]3\d\d OR [STATUSCODE]2\d\d OR [STATUSCODE]40[13]

- **File extension addition**

  This type of check searches for files with a file extension that you specify.

  During the crawl, whenever the scanner encounters a file of any name and any extension (for example, global.asa), it sends an HTTP request for a file of the same name plus the found extension plus an extension that you specify. For example, if you specify a file extension of .backup, then when the scanner discovers a file named global.asa, it will subsequently search for a file named global.asa.backup.

  A server would normally deny any request for the global.asa file, but if a programmer has left a backup file on the server and the file has a different extension (such as global.asa.backup), then the server might return the file (which contains the full source of the global.asa file).

To create a custom check that searches for files with a specific added extension, enter the following in the Custom Check Wizard:

Attack Type:	File Extension Addition
Attack:	.ext [where ext is the file extension of files you want to locate]. You must include the leading dot or period (.)
Signature:	[STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

- **File extension replacement**

  This type of check searches for files with a file extension that you specify.

  For example, one standard check searches for files having an extension of "old." During the crawl, whenever the scanner encounters a file of any name and any extension (for example, startup.asp), it sends an HTTP request for a file of the same name but with an extension of "old" (for example, startup.old).

  To create a custom check that searches for files with a specific extension, enter the following in the Custom Check Wizard:

Attack Type:	File Extension Replacement
Attack:	ext [where ext is the file extension of files you want to locate]. Do NOT include a leading dot or period (.)
Signature:	[STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Coontent-Type:\sapplication/octet-stream)

- **Keyword search**

  This type of check determines if a specified word or phrase (defined by a regular expression) exists anywhere in the body of the HTTP response.

  The following example searches the HTTP response for a nine-digit number formatted as a social security number (\d = any digit).

Attack Type:	Keyword Search
Attack:	N/A
Signature:	BODY]\d\d\d-\d\d-\d\d\d\d

- **Parameter injection**

  This type of attack replaces an argument value with an attack string.

  Example:

  http://www.samplesite.com/webapp.asp?ValidParameter=ValidArgument

  will be changed to

  http://www.samplesite.com/webapp.asp?ValidParameter=AttackArgument

  There are several variations.

  – Command Execution

    A command execution check combines strings composed of special characters with operating system-level commands. It is an attempt to make the Web application execute the command using the provided string (if the application fails to check for and prohibit the input).

The following example tests for parameter injection by providing spurious input to a program named support_page.cgi; if the HTTP response contains data that matches the regular expression, then the application is vulnerable to command execution.

Attack Type:	Parameter Injection
Attack:	/support_page.cgi?file_name=|id|
Signature:	[BODY]uid= AND [BODY]gid=

– SQL Injection

SQL injection is the act of passing SQL code into an application. These attack strings are composed of fragments of SQL syntax that will be executed on the database server if the Web application uses the string when forming a SQL statement without first filtering out certain characters.

Attack Type:	Parameter Injection
Attack:	’ [an apostrophe]
Signature:	[[STATUSCODE]5\d\d

– Cross-Site Scripting

This issue occurs when dynamically generated Web pages display input that is not properly validated. This allows an attacker to embed malicious JavaScript into the generated page, enabling him to execute the script on the machine of any user who views the malicious page. Any site that allows users to post text messages can be vulnerable to an attack such as this.

The following example tests for cross-site scripting in the Fusion News application:

Attack Type:	Parameter Injection
Attack:	/fullnews.php?id=<script>alert(document.cookie)</script>
Signature:	[ALL]Powered\sby\sFusion\sNews And [ALL]<script>alert\(document\.cookie\)</script>

– Directory Traversal

Directory traversal entails sending malformed URL strings to access non-public portions of the Web server’s content. An attacker will try to access different files on a server by using relative hyperlinks. For example, by adding triplets of two periods and a forward slash (../) to the target URL and by varying the number of directories to traverse, an attacker might find and gain access to a system password file such as www.server.com/../../../../password.

The following example searches for the boot.ini file:

Attack Type:	Parameter Injection
Attack:	/../../../../../../../../../../../boot.ini
Signature:	[ALL]\[boot\sloader\]

– Abnormal Input

Abnormal input attack strings are composed of characters that can cause unhandled exceptions (errors the program is not coded to handle) in Web applications where unexpected input is not prohibited. Unhandled exceptions often cause servers to display error messages that disclose sensitive information about the application’s internal mechanics. Source code may even be disclosed.

The following example sends an extraordinarily long string in an attempt to create a buffer overflow.

Attack Type:	Parameter Injection
Attack:	AAAAA...AAAAA [1000 repetitions of the letter “A”]
Signature:	[STATUSCODE]5\d\d

- **Simple attack**

  This type of attack is sent once for every server scanned.

  The following example attempts to obtain a UNIX password file by appending the attack string to the target URL or IP address:

Attack Type:	Simple Attack
Attack:	/etc/passwd
Signature:	[ALL]root: AND [ALL]:0:0

- **Site search**

  This type of attack is designed to find files commonly left on a Web server. For example, check ID #279 searches for a file named log.htm.

  The following example searches for a file named xanadu.html by appending the attack string to the target URL or IP address:

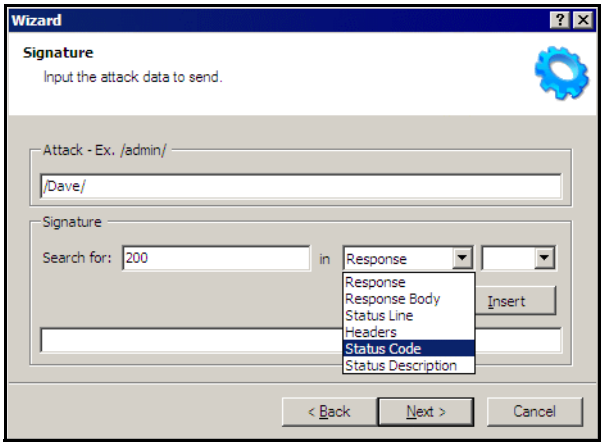
Attack Type:	Site Search
Attack:	xanadu.html
Signature:	[STATUSCODE]2\d\d OR [STATUSCODE]40[1]

  To create a custom check that searches for a file named confidential.txt, enter the following in the Custom Check Wizard:

Attack Type:	Site Search
Attack:	confidential.txt
Signature:	[STATUSCODE]2\d\d AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

8 Click **Next**.

9 In the **Attack** box, enter the data you want to use for the attack. In the following example of directory enumeration, the check will search for a directory named “Dave” by appending the attack string (/Dave/) to the target URL or IP address.



10 You must specify a signature, which is simply a regular expression (i.e., a special text string for describing a search pattern). When the scanner searches the HTTP response and finds the text described by the signature, it flags the session as a vulnerability. You can use the **Search for** box and drop-down lists to help you create the regular expression, or you can type the regular expression directly into the text box at the bottom of the window.

To use the **Search for** box:

a Enter the text you want to locate.

Enter only text; do not enter a regular expression.

b In this example (searching for a directory named "Dave"), the server would return a status code of 200 if the directory exists, so enter "200" in the **Search for** box. Realistically, however, you might also accept any status code in the 200 or 300 series, or a status code of 401 or 403.

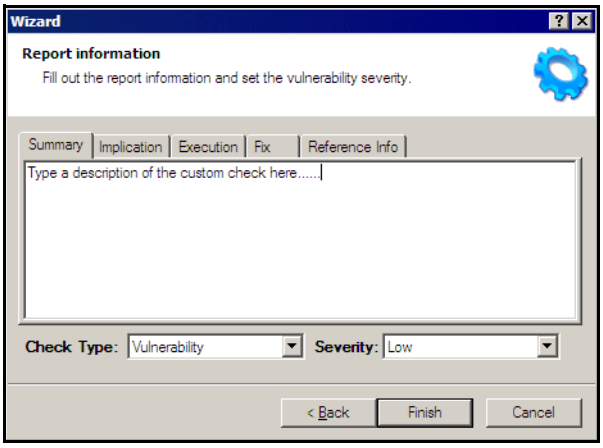
c Click the drop-down arrow to specify the section of the HTTP response that should be searched.

d ()ptional) To create a complex search, click the second drop-down and select a Boolean operator (AND, OR, or NOT).

e Click **Insert**.

f (Optional) For complex searches, repeat step a through step d as needed. You can also edit or replace the regular expression that appears in the bottom text box.

11 Click **Next**.



12 On the Report Information panel, click each tab and enter the text that will appear in the vulnerability description.

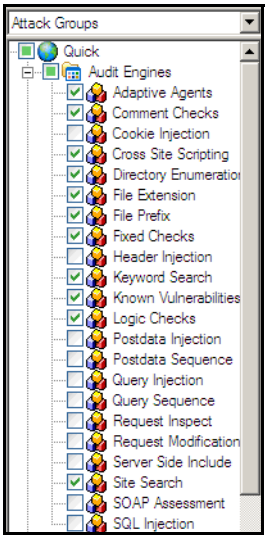
13 Select an entry from the **Check Type** list.

14 Select a severity level from the **Severity** list.

15 Click **Finish**.

16 Change the default name “New Custom Check” to reflect the purpose of the check.

17 Click ⊞ to expand the Audit Engines folder.



18 Ensure that the appropriate audit engine is enabled (with a check mark) for the type of check you created, according to the following table:

Table 1 Correlation of Attack Type to Audit Engine

This Attack Type…	Uses this Audit Engine…
Simple Attack	Fixed Checks
Parameter Injection	Post Data Injection
Site Search	Site Search
File Extension Replacement	File Extension
File Extension Addition	File Extension
Directory Enumeration	Directory Enumeration
Keyword Search	Keyword Search

19 Click **File** → **Save**.

20 Enter a name for the new policy and click **Save**.

All custom checks are added to every policy, but they are not enabled. To enable the custom check in other polices, see Creating or Editing a Policy on page 170.

Disabling a Custom Check

To disable a custom check:

1 Select a custom check.

2 Clear its associated check box.

Deleting a Custom Check

To delete a custom check:

1 Right-click a custom check.

2 Select **Delete** from the short-cut menu.

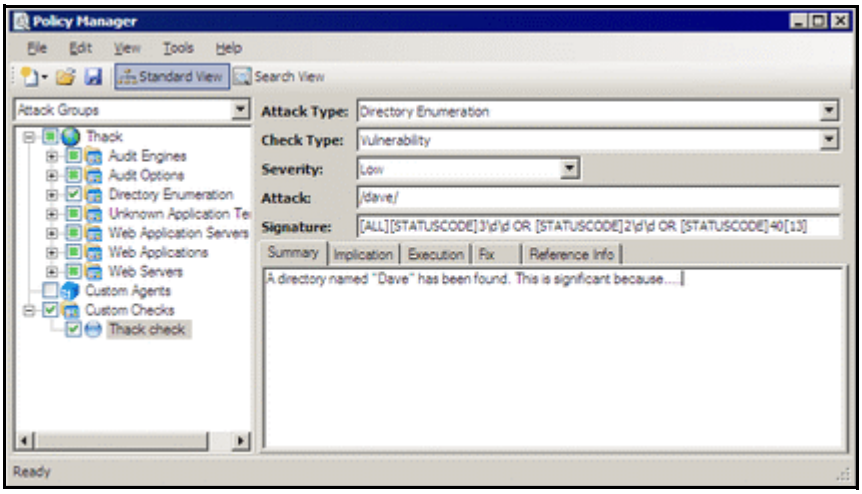
Editing a Custom Check

To edit a custom check:

1 Open a policy.

2 Select a custom check.

3 Using the right pane of the Policy Editor, modify the custom check properties.



4 Click the Save icon.

Searching for Attack Agents

Use the Search view on the Policy Manager to locate specific vulnerability checks (attack agents). You can then elect to include or exclude individual agents.

To search for attack agents:

1 Open a policy in the Policy Manager.

2 Click **View** → **Search**.

3 From the **Criteria** list, select the property that you want to search.

The description of every attack agent contains “report fields” such as summary, implication, execution, fix, and reference information. The Search feature allows you to locate attack agents that contain the text you specify in a selected report field. In addition, you can search for a vulnerability ID, vulnerability name, engine type, or the date when last updated.

4 Choose an operator from the drop-down list (is, is greater than, is less than, contains).

5 In the text box, type the text or number you want to find.

6 Click **Search**.

The Policy Manager lists in the **Checks** area all attack agents that match your search criteria. An active agent will have a check mark next to its name. Select (or clear) a check box to activate (or deactivate) an agent.

7 Click **Save** to save the revised policy.

Policy Manager Icons

The following table illustrates and describes icons that are used in the Policy Manager tree view.

Table 2 Policy Manager Icons

Icon	Definition
	The policy.
	Attack Group Folder: Contains vulnerability assessments.
	Audit Methodology: A set of checks that compose an audit methodology. For example, Site Search is part of the Audit methodology.
	A critical vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify private information.
	A high vulnerability. Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
	A medium vulnerability. Indicates non-HTML errors or issues that could be sensitive.
	A low vulnerability. Indicates interesting issues, or issues that could potentially become higher ones.

Audit Inputs Editor

This tool allows you to create or edit inputs to the audit engines and to a distinct set of checks.

Access the Audit Inputs Editor from the Policy Manager (using the Policy Manager's **Tools** menu) to create or modify an inputs file (<filename>.inputs). You can then specify this file when modifying scan settings.

To modify an inputs file, click the Open icon on the Audit Inputs Editor's toolbar or select **File** → **Open**.

You must import into the WebInspect Enterprise scan configuration the saved file containing your check input modifications. To do so:

1. Create a new scan in the WebInspect Enterprise Web Console.
2. Under Audit Settings, select **Attack Exclusions**.
3. Next to **Import Audit Inputs** (at the bottom of the page), click **Browse**.
4. Select the file you created and click **Open**.

Engine Inputs

To create or modify inputs to audit engines.

1. Click the **Engine Inputs** tab.
2. Click the drop-down arrow.
   a. To apply your modifications to all audit engines, select **<Default>**. The Default parameters are extracted from the scanner's default Audit Settings - Attack Exclusions.
   b. To modify inputs for a specific audit engine, select one from the list.
3. Select an engine input.
4. If you selected one of the following:
   - Excluded Query Parameters
   - Excluded Post Parameters
   - Excluded Cookies
   - Excluded Headers
   - Root Directories

   a. To add an item to the list, click **Add**.
   b. To edit an item, select an item and click **Edit**.
   c. To delete an item, select the item and click **Remove**.
   d. If you selected a specific engine (rather than Defaults), select one of the following options:
      — **Merge with defaults** - The parameters you specified are added to the Defaults list, which apply to all engines.
      — **Replace defaults** - The engine will use the parameters you specified instead of those in the Defaults list.

Note: If you specify a Root Directory, then the engine will attack the object in the directory you specify, rather than the actual root. For example, if an engine normally attacks filename.txt in the default root directory rootdir (/rootdir/filename.txt), then if you specify a root directory of /foobar/, the engine will attack /foobar/filename.txt.

5 If you selected one of the following:

- Header Audit Rules
- Cookie Audit Rules

a Clear the **Use value from defaults** check box.

b Select an option from the drop-down list.

6 Click the **File** menu and select **Save** or **Save As**.

Check Inputs

Certain checks require inputs that accommodate the specific design of the target Web site. The scanner conducts these checks using default values, which you may need to change.

To create or modify inputs for specific checks.

1 Click the **Check Inputs** tab.

2 Select a check (see list below).

3 Enter the requested input values.

4 Click **File** → **Save** (or **Save As**).

4719: IIS Mapping

Microsoft IIS extension handlers historically have been the source of many vulnerabilities. This check probes for each known IIS extension, and flags a vulnerability for each extension/handler that is found to be enabled. However, in certain cases, an extension handler may be legitimately enabled and used by the target Web site.

Required Input: One or more extensions that identify the handlers that are legitimately enabled and which should be excluded. Valid input is printer, idc, idq, ida, htr, htw, stm, shtm, and shtml.

4721: Admin Section Must Require Authentication

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires authentication before allowing access. This check attempts to access a sensitive directory that should require authentication. The default check input is /admin.

Required Input: The directory (relative to the root) containing administrative or sensitive data.

4722: Logins Sent Over Unencrypted Connection

Any area of a Web application that possibly contains sensitive information or access to privileged functionality (such as remote site administration functionality) should utilize SSL or another form of encryption to prevent login information from being sniffed or otherwise intercepted or stolen.

Required Input: Login forms. The name of file containing login form.

4723: Logins Sent Over Query

Information in query strings is directly visible to the end user via the browser interface, which can cause security issues. Recommendations include performing server-side input validation to ensure data received from the client matches expectations.

Required Input: Login forms. The name of file containing login form.

4724: Password Field Masked

Basic Web application security measures include “masking” all passwords entered by a user when logging on to a Web application. Normally, each character in a password entered by a user is instead represented with an asterisk. Recommendations include requiring all password fields in your Web application be masked to prevent other users from seeing this information.

Required Input: The name attribute of input controls containing a password.

4726: Secure Section Only Accessible Via SSL

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires that the pages under the secure section of the site are only accessible via SSL.

Required Input: The name of the secure directory, relative to the root. The default is /secure.

4728: Persistent Cookies

Persistent cookies are stored on the browser’s hard drive. This can cause security and privacy issues depending on the information stored in the cookie and how it is accessed. This check calculates how many seconds until a received cookie is set to expire. If the expiration date/time is less than the specified number of seconds (default: 600), the check considers the cookie’s life span to be excessive, increasing the chances of session ID recovery and session hijacking.

Required Input: The lifetime allowed for cookies (in seconds).

4729: User supplied data without POST

An area of the Web application that possibly contains sensitive information or access to privileged functionality (such as remote site administration functionality) uses query strings to pass information between pages. Information in query strings is directly visible to the end user via the browser interface, which can cause security issues. The input value for this check is a space-separated list of regular expressions that are used to identify sensitive URL parameter names when used in GET queries. Generally, information such as passwords, social security numbers, etc., should not be sent as parameters to GET queries, since the GET query (and thus the sensitive information) can persist in Web server and proxy logs and the Web browser’s history. You will need to adjust the regular expressions accordingly to specify the parameter names your application typically uses to denote sensitive information.

Required Input: Sensitive parameter (a regular expression). An example is:

p|P]ass(word)? [u|U]ser_?([N|n]ame)? [s|S][s|S][n|N]

4731: Script Directory Check

A directory containing an object referenced in a post request or query string should not have a name that could easily be guessed by an attacker. The primary danger from an attacker discovering this directory would arise from the information he could gather from its contents, such as what language was used to code the Web application. This check is used to determine if a dynamic form action points to a file/URL that is in a directory whose name is included in the list.

Required Input: Names of directories containing scripts.

4732: Script File Extension Disclosure

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires the file extension of all scripts to be checked as it may lead to information disclosure related to the technology used by the application. The use of certain CGI-related file extensions can indicate certain types of technology in use, which results in a mild information disclosure. The default list of check input values is generally applicable, but some sites may legitimately use a certain technology (such as Perl) and this check may incorrectly elicit false-positive issues in flagging all Perl extensions (.pl). In such cases, you should remove the legitimate extensions from the list.

Required Input: File extensions of scripts used in the Web application (such as cgi, pl, and py).

5151: Arbitrary Remote File Include

This check attempts to discover if the Web application can fetch and incorporate data from arbitrary URLs supplied by an attacker.

This is the most complex check to configure, because its extreme flexibility enables it to work in many environments and topologies. Basically, the check injects URL values into application parameters, attempting to force the application to make an HTTP request to the supplied URL. This activity looks for "remote file inclusion" vulnerabilities caused by the application attempting to remotely retrieve the specified file/URL and include the response into the application's processing. In certain extreme circumstances found in PHP environments, the application will remotely retrieve the file and execute any PHP script contained therein, making the activity capable of arbitrary code/script execution.

Check 5151 can operate in two modes: static and server (controlled by the "Audit Mode" parameter).

Static Mode

You specify the target external URL as the **Static Mode Target URL**, and a corresponding regular expression signature as the **Static Mode Signature**. If you want to use external targets, then you should use static mode. By default, the check uses static mode and the test URL of "http://15.216.12.12/serverinclude.html?" which is a special page hosted on an HP Web server located on the public Internet at IP address 15.216.12.12. The signature contains a specific value that is returned by the indicated test URL. If you do not want to use the HP Web server (particularly if the target server cannot access the Internet), then you should adjust the test URL (and corresponding signature) to a URL hosted by a server. When configuring static mode:

- Specify a full, absolute URL (i.e., it should begin with "http://").
- For best results, use non-SSL URLs (although SSL URLs are allowed).
- Include a question mark (?) at the end of your URL to ensure the URL is not affected if the application appends additional data to the end of the URL.

Server Mode

In this mode, WebInspect runs its own Web server and attempts to get the target/scanned server to connect to the WebInspect scanning system. The added benefit of Server mode is that it can detect "blind" remote file inclusion vulnerabilities, resulting in potentially fewer false negatives. To use Server mode, the check conceptually needs three pieces of information:

- Server Mode Target IP -- The IP address the server/target should use to access the host (particularly if the scanning system's network IP is different than what the server would need to access, due to a firewall or a multi-homed scanning system). The default value is empty/blank, meaning that it uses the same IP address ultimately used or determined by the Server Mode Server IP.
- Server Mode Server Port -- The port number to run the listening Web server on. Using a specific port may be necessary due to network/access restrictions. The default value is 8181. If you leave this value blank, then the Remote File Include engine will dynamically choose a port between 25000 and 25100.

- Server Mode Server IP -- The local IP address of the scanning system to bind the Web server on, if the system is multi-homed and/or you do not want to bind the Web server listening on the first local IP address. The default value is “0.0.0.0”, which instructs WebInspect to use the first available IP address on the system.

Although the default values fit most configurations, certain circumstances require specific modification.

- If your system has multiple IP addresses (due to multiple network adapters), then you may need to specify the explicit IP address to bind to (i.e., the one that is most appropriate for receiving requests from the system you are scanning). You can determine the list of your system’s IP addresses by running “biconvex” from a Windows command prompt.
- If you are running multiple scans from the same scanning system using server mode, then you should leave the **Server Mode Server Port** value blank, causing WebInspect to dynamically pick the port. This is because two scans cannot run two separate Web servers listening on the same port. One specific port can only be used by one scan at a time.
- If your system is behind a firewall and you are using port-forwarding to receive the incoming HTTP requests, or you are on a network that uses NAT, then the IP address used by the server to access your system will be different from the IP address actually assigned to your system. In this case, you will need to specify the IP address the target server should use for the **Server Mode Target IP**.

Required Inputs: Static mode target URL, Audit mode (static or server), Server mode server IP, Server mode Server port, Server mode target IP, static mode signature (a regular expression)

5546: Privacy Policy Not Present

This check is associated with WebInspect’s compliance policies. Many legislative initiatives require organizations to place a publicly accessible document within their Web application that defines their information privacy policy. If WebInspect does not find the specified file, it creates a vulnerability in the Best Practices category.

Required Inputs: The relative directory and file name of the privacy policy.

10167: Password in Query or Cookie Data

Transmitting password information in a query string or cookie value makes it easy for an attacker to see and tamper with login values. Recommendations include ensuring that login information is sent with a POST request over an encrypted connection and that sensitive account information is stored on the server.

Required Inputs:

- Password Field Names - List of Query or Cookie parameter names containing a password.
- Possible Username List - List of Query or Cookie parameter names containing a username.

10183: Allowed Top-Level Domain

Certain organizations (especially branches of the U.S. federal government) must use a restricted set of DNS top-level domain names (TLDs), such as .gov, .mil, or .fed. This check ensures that all allowed hosts encountered during the scan use one of the specified TLDs. Most public corporations arbitrarily use any TLD they desire (.com, .net, .org, etc.); those corporations should either disable this check (preferable) or change the default values to include .com, .net, and .org (and/or any other appropriate TLDs).

Required Inputs: All allowed top-level domains.

10274: Proxy CONNECT Access

Some proxy servers accept the CONNECT method to make an HTTP connection to another server. Usually, this method should be restricted to internal use only. If it is not restricted, your server can be used by an attacker on the Internet to disguise himself as your own server. Thus, any attack will appear to come from your server. This type of vulnerability is usually caused by not properly configuring the proxy server. Attackers can masquerade as your proxy server when conducting other attacks. Attackers may be able to access internal machines through the CONNECT proxy. This attack can also be used to enumerate your local network.

This check attempts to treat the target server as a proxy server for SSL requests. The check issues a CONNECT request to the target server, which essentially asks the server to make a connection to another external site. You can control which external site is used via the input values for this check. By default, the value "https://www.google.com/" is used, causing the server to make an external request to the host www.google.com on port 443. You may wish to modify this value to point to a more appropriate internal host. If so:

Use a server that has SSL enabled on the standard SSL port 443, if possible. Some proxies refuse connections to ports other than 443 due to explicit configuration.

Use the https:// URL format.

If you need to specify a port other than 443, use the normal URL format to specify a port after the host name (e.g., https://example.com:8443/).

Only the host name and port number are used; the remainder of the URL is ignored.

10275: Proxy GET Access

This check is virtually identical to check 10274, except it issues a proxy-qualified GET request to the target server instead of a CONNECT request. There are many servers that are willing to take a proxy-qualified GET request and treat it as a normal GET request (ignoring the proxy-specific aspects of the request), so it is necessary for the check to evaluate the response content to ensure the response is truly from the external server and not a normal response from the target. That is why check 10275 has two check inputs: one for specifying the external target host, and one for specifying a regular expression to match against the response content. By default the check attempts to access "http://www.google.com/" and looks for the phrase "Google Search" in the response. You will need to adjust the check input values if you need to use a different external host or an internal host. You can change the external target simply by adjusting the target check input value, and then specifying a unique value from the target page as the check input regex value.

- The URL target must begin with http:// or https://. For best results, use http://.
- If you need to specify a specific port other than 80/443, use the normal URL format to specify a port after the host name (such as http://example.com:8080).
- Unlike check 10274, the target URL you specify for 10275 is used in its entirety; if you specify a specific page/URL, then that specific page/URL will be requested.
- Try to select a unique value/phrase from the target URL to use as the response regex value, one that is not likely to appear elsewhere on the target scanned site; using the value in the <title> tags usually is sufficient (you can also include the "<title>" tags in the regex value itself).
- Remember to properly escape any regex-specific metacharacters (periods, parentheses, etc.).
- The check does not follow redirects (HTTP 302 responses), so you will need to specify an explicit final URL destination.

Required Inputs: Proxy GET target and Proxy GET target response (regular expression).

10280: Price-Related Form Fields

Forms containing price-related field names could harbor price manipulation vulnerabilities that would allow the attacker to change the price of the product.

Required Inputs: Names of price-related fields.

10287: Local File Include

Several types of attacks involve malformed filename requests that result in reading local files from the Web server. The Local File Include engine generates requests that contain variously encoded file names, and then evaluates the responses to determine if the contents of those files were recovered.

Mode

The Mode parameter relates to the platform assumptions made by the engine. The default mode value, **Auto**, causes the engine to look for both "c:\windows\win.ini" (Windows) and "/etc/passwd" (Unix) files and to use both Windows and Unix parent directory references accordingly. If the engine gets a visual response that explicitly indicates the underlying platform (Windows vs. Unix), it will automatically switch to using only the values for appropriate target platform for the remainder of the auditing for that application parameter value. If you already know what the underlying platform is before you scan (i.e., Windows vs. Unix), you can change the mode to **Windows** or **Unix**, which can save scan time since it reduces the number of values that need to be sent. At this time the engine does not support platforms that do not use a Windows ("\") or Unix ("/") path separator.

User-Specified File

If you want to use a specific target file, specify it here. There are occasions when the default file name values ("c:\windows\win.ini" and "/etc/passwd") may not work in your environment. For example, your Web application can be hosted on a Windows drive other than 'C:', or your Web application could be operating out of a Unix chroot environment. In both cases, parent directory references will not be able to locate the specified target files even if a vulnerability does exist. For this situation you should either use an existing file that is in the root directory of the same drive/chroot of the Web application, or explicitly create a text file in the root directory of the drive/chroot used by your Web application and place a unique value inside the text file. Then you inform the LFI engine to look for your specific file by setting the **UserOnly** mode option, and specifying the absolute path to your target file in the **User Specified File** check input. You will also need to specify a corresponding User **Specified File Regex** check input value; the regex value should uniquely identify/match the contents of your specified file while not matching any content typically found on the scanned Web site. You can also select the **UserAndAuto** mode, which would let you specify a file and still use the default "c:\windows\win.ini" and "/etc/passwd" values.

User-Specified File Regex

If you use a specific target file, then you need to specify a regular expression that matches the contents of the target file.

Audit Disposition

The Audit Disposition parameter default value **Adaptive** treats Web application parameters in one of two ways: parameters with existing values that resemble file names receive significant (aggressive) scrutiny, while all other parameters receive basic scrutiny. The premise is that if the parameter has a value that resembles a filename, then there is a higher likelihood that the value is used in a file system operation; because of that higher likelihood, it makes sense for the engine to try more variations (particularly minor variations) to ensure that is not the case. However, trying additional minor variations can extend scan time,

because it results in more attacks to be sent. That is why the **Adaptive** disposition tries to determine when it seems appropriate to spend the extra effort in auditing a particular parameter. However, if you desire the utmost level of scrutiny for all parameters, change the Audit Disposition value to **Aggressive**.

Required Inputs: Mode and Audit disposition.

10551: Possible Username or Password Disclosure

Exposing login information on publicly accessible sections of a Web Application could allow an attacker to access sensitive applications and information on a site, or to perform functions according to the privilege level of the login information. Gaining information critical to the success of escalated attacks would also be a likely impact of exploitation. Recommendations include purging the information from publicly accessible content, if possible, or otherwise ensuring proper access controls are in place.

Required Inputs:

- Password field names - Names of client-side script variables containing a password.
- Possible Username List - Names of client-side script variables containing a username.

10963: Cross-Site Request Forgery

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a Web application in which he/she is currently authenticated. With a little help of social engineering (like sending a link via E-mail/chat), an attacker may force the users of a Web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire Web application.

Criteria for identifying Cross-Site Request Forgery (CSRF)

- This check is only run against POST requests.
- The page must be either a login page or a page in restricted session (i.e., an authenticated session). Note: To avoid testing every POST request made during authenticated sessions, the check is run against a URL one time. This means that forms with multiple parameters will be tested one time only and not multiple times like a cross-site scripting or parameter injection check.
- The page is not a re-authentication page. This is to avoid cases where a user is asked to either change a password or provide a password when already in an authenticated session. A re-authentication page is not CSRF vulnerable.
- The page does not contain CAPTCHA. A CAPTCHA page is not vulnerable to CSRF.
- The page is not an error page or an invalid page from the server.

Check inputs are used as heuristics to help the CSRF agent refine detected results. There are a number of criteria used for CSRF detection that help to avoid false positives.

Required Inputs

- Password field names - This field is used to help identify login pages. The matches are string matches.
- Possible Username List - This field is used to help identify login pages. The matches here are string matches.

Optional Inputs

- CSRF Request Black List - This field is used to identify pages that are NOT to be flagged as vulnerable to CSRF. Matching values are identified for the name values in POST parameters.

- CSRF Response Black List - This field is used to identify error pages or invalid pages. The default value here is a combination of two regular expressions and also a string value (CAPTCHA). Matching values are identified on the response body.
- CSRF Response White List - This field is used to elevate the risk associated with this vulnerability for specific pages. By default, CSRF findings are a Medium severity. A match for values in this field will result in the finding being rated as a High severity. Matching values are identified in the response body.

10965: User Data in Query or Cookie

Transmitting password information in a query string or cookie value makes it easy for an attacker to see and tamper with login values. Recommendations include ensuring that login information is sent with a POST request over an encrypted connection and that sensitive account information is stored on the server.

Required Inputs:

- Password Field Names - List of Query or Cookie parameter names containing a password.
- Possible Username List - List of Query or Cookie parameter names containing a username.

Web Form Editor

Most Web applications contain forms composed of input controls (text boxes, buttons, drop-down lists, etc.). Users generally "complete" a form by modifying its controls (such as entering text or checking boxes) before submitting the form to an agent for processing. Usually, this processing will lead the user to another page or section of the application. For example, after completing a login form, the user will proceed to the application's beginning page.

Some sites (such as HP's example banking application zero.webappsecurity.com) contain many different forms for completing a variety of transactions. If the scanner is to navigate through all possible links in the application, it must be able to submit appropriate data for each form.

With the Web Form Editor, you can create or modify a file containing the names of all input controls and the associated values that need to be submitted during a scan of your Web site. These entries are categorized by URL, so even if different controls on different pages have the same name, the Web Form Editor can discriminate between them. Alternatively, you can designate a form entry as "global," meaning that its value will be submitted for any input control having the same name attribute, regardless of the URL at which it occurs.

During a scan, if DevInspect encounters an input control whose name attribute is not matched in the file you create, it will submit a default value (12345).

For server authentication (logging in to a server with a user name and password), you can enter values here or on the **Authentication** tab of the *Settings* window.

If you are using a proxy server, the WebForm Editor will not use the default settings from WebInspect. You must first configure Internet Explorer to use the desired proxy.

There are two ways to create a list of form values:

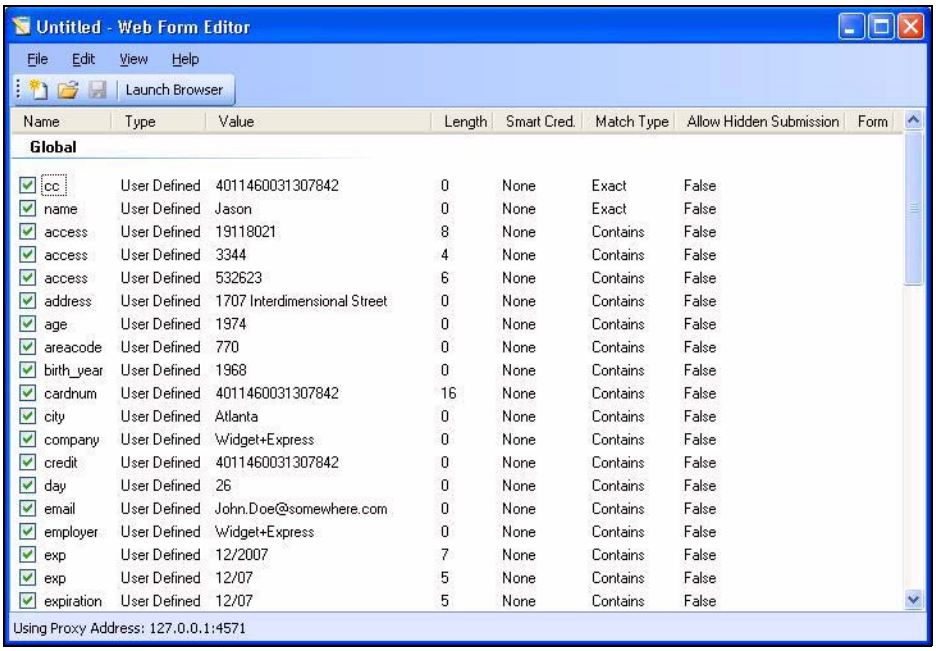
- Create the list manually.
- Record the values as you navigate through the application.

Manually Creating a Web Form List

Use the following procedure to create a Web Form list manually.

1 Click **Tools** → **WebForm Editor**.

The *WebForm Editor* window appears.



The WebForm Editor loads a prepackaged default file.

a To load a different file, select **File** → **Open**.

b To create a new file, select **File** → **New**.

2 Do one of the following:

- To add a Web form value, right-click anywhere in the Web Form Editor's work area and select **Add Global Form Input** from the shortcut (pop-up) menu.
- To modify a Web form value, right-click an entry and select **Modify** from the shortcut (pop-up) menu.

The *Add User-Defined Input* or the *Modify Input* window appears.

3 In the **Name** box, type (or modify) the name attribute of the input element.

4 In the **Length** box, enter either:

- the value that must be specified by the size attribute, or
- zero, for input elements that do not specify a size attribute.

For example, to submit data for the following HTML fragment…

<INPUT TYPE="password" NAME="accessID" MAXLENGTH="6">

…you must create an entry consisting of accessID (Name) and specify a size of "6" (Length).

5 In the **Value** box, type the data that should be associated with the input element (for example, a password).

6 Use the **Match** list to specify how the scanner should determine if this entry qualifies to be submitted for a particular input control. The options are:

- **Exact**—The name attribute of the input control must match exactly the name assigned to this entry.
- **Starts with**—The name attribute of the input control must begin with the name assigned to this entry.

- **Contains**—The name attribute of the input control must contain the name assigned to this entry.

7 Programmers sometimes use input controls with type= “hidden” to store information between client/server exchanges that would otherwise be lost due to the stateless nature of HTTP. Although the Web Form Editor will collect and display the attributes for hidden controls, the scanner will not submit values for hidden controls unless you select **Allow Hidden Submission**.

8 Click **Add** (or **Modify**).

9 If necessary, you can assign additional attributes by right-clicking an entry and using the shortcut menu.

- To submit the form value for any input control having the same name attribute, regardless of the URL at which it occurs, choose **Make Global**.
- To remove an entry, choose **Unselect**. This clears the check mark and removes the entry from processing, but does not delete it from the file.
- To activate an entry, choose **Select**. This creates a check mark and includes the entry for processing.
- To delete an entry, choose **Delete**.
- To designate an entry as a smart credential, select either **Smart Credential Username** or **Smart Credential Password**.

  When recording Web form values, you will often encounter a log-on form requiring you to enter a user name and password. You can safely use your own user name and password, provided that you designate those entries as “Smart Credentials” before saving the file. Your actual password and user name are not saved.

  When scanning the page containing the input control associated with this entry, the scanner will substitute the password specified in the product’s Authentication options. This would be a known user name and password that does not require security. Alternatively, if no user name or password is specified, the scanner will submit the string “FormFillText.”

Recording Web Form Values

The Web Form Editor serves as a proxy that handles HTTP traffic between a browser and a target Web site. By default, it uses the local IP address 127.0.0.1 and any available port. However, you can specify a different IP address and port by clicking **Edit** → **Settings**.

Use the following procedure to capture names and values of input controls on a Web site.

1 To create a list of form values, select **File** → **New** (or click the New icon on the toolbar).

2 To add form values to an existing list, select **File** → **Open** (or click the Open icon on the toolbar) and choose a file using the standard file-selection dialog.

3 Click **Launch Browser**.

4 Using the browser’s **Address** bar, enter or select a URL and navigate to a page containing a form.

Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, the Web Form Editor will not receive such traffic. This is a documented Microsoft defect. To access a site on “localhost” when using IE7, place a period or dot after “localhost” (for example, http://localhost.:8080/test.html).

5 Complete the form and submit it (usually by clicking a button such as **Log In**, **Submit**, **Go**, etc.).

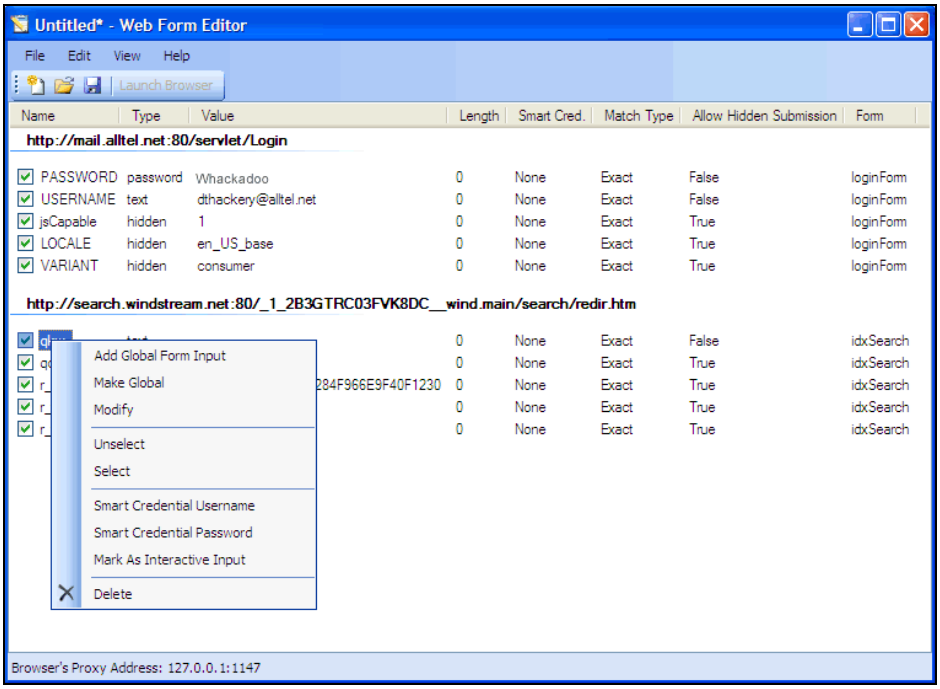
6 Navigate to additional pages and submit forms until you have traversed all the links you wish to follow.

7 The Web Form Editor displays a list of name and value attributes for all input controls found in all forms on the pages you visited.

For example, the first two entries in the following illustration were derived from the following HTML fragment…

```
<form name="loginForm" action="/servlet/Login" method="POST">
<input type="password" size="16" name="PASSWORD">
<input type="text" size="16" name="USERNAME" value="">
<input type="SUBMIT" value="Submit"></form>
```

…and the user entered his name and password.



8 If necessary, you can modify items by right-clicking an entry and using the shortcut (pop-up) menu.

- To submit the form value for any input control having the same name attribute, regardless of the URL at which it occurs, choose **Make Global**.
- To edit an entry, select **Modify**.
- To add an entry, select **Add Global Form Input**. A Global entry is one not associated with a specific URL.
- To remove an entry, choose **Unselect**. This removes the entry from processing, but does not delete it from the file.
- To delete an entry, choose **Delete**.
- To designate an entry as a smart credential, select either **Smart Credential Username** or **Smart Credential Password**.
- To force the scanner to pause and display a window prompting the user to enter a value for this entry, select **Mark As Interactive Input**.

  When a scanner encounters an HTTP or JavaScript form, it will pause the scan and display a window that allows you to enter values for input controls within the form, provided that the scanner's option to **Prompt For Web Form Values** is selected. However, if the scanner's option to **Only Prompt Tagged Inputs** is also selected, the scanner will not pause for user input unless a specific input control has been designated **Mark As Interactive Input** (except for passwords, which always cause the scanner to pause for input).

9 Click **File** → **Save** (or **Save As**).

Importing a Web Form File

You can import a file that was designed and created for earlier versions of the scanner and convert it to a file that can be used by the current Web Form Editor.

1 Click **File** → **Import**.

The *Convert Web Form Values* window appears.

2 Click the ellipses button next to **Select File To Import**.

3 Using a standard file-selection window, locate the XML file created by an earlier version of the Web Form Editor.

4 Click the ellipses button next to **Select Target File**.

5 Using a standard file-selection window, specify a file name and location for the converted file.

6 Click **OK**.

Scanning with a Web Form File

When scanning a site, you specify which Web Form file you want to use by selecting **Auto-fill web forms during crawl** and then selecting a file.

1 Click the **New Scan** action.

2 On the *Configure Scan* window, click **Switch to Advanced**.

3 In the **Scan Settings** group, select **Method**.

4 Select **Auto-fill Web Forms During Crawl**.

5 Click **Browse**.

6 Using the standard file-selection window, select a file containing the Web form values you want to use and click **Open**.

Web Form Editor Settings

To modify the Web Form Editor settings:

1 Click **Edit** → **Settings**.

2 Select either the **General** or **Proxy** category and enter the settings described in the following sections.

3 Click **OK**.

General

Proxy Listener

The Web Form Editor serves as a proxy that handles HTTP traffic between a browser and a target Web site. By default, it uses the local IP address 127.0.0.1 and any available port. However, you can specify a different IP address and port by selecting **Edit** → **Settings**.

To avoid the possibility of specifying a port that is already in use, select **Automatically Assign Port**.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document. For pages that do not announce their character set, you can specify which character set the Web Form Editor should use by selecting an entry from the **Assumed 'charset' Encoding** list.

Proxy

Use these settings to access the Web Form Editor through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the Web Form Editor will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Web Form Logic

When crawling a Web application and submitting Web form values, the scanner analyzes the entries in the Web form values file to determine if a value should be submitted. The logic for determining a match is represented in the following table, ordered from "most preferred" to "least preferred."

Table 3 Rules for Matching Web Form Values

Page-specific form values	Exact Match. Name exact match. Length exact match.	The specific Web page, Web form name, and value length detected on the crawled Web page exactly match a single record in the webformvalues.xml selected for the scan.
	Partial Match. Name-only match. Length allows wildcard.	The specific Web page and Web form name detected on the crawled Web page match a single record in the webformvalues.xml selected for the scan. The field length associated with that form value allows for submission to any field input length (wildcard field length match).
Global form values	Exact Match. Name exact match. Length exact match.	The Web form name and value length detected on the crawled Web page match a single record in the Global Web form values section of the webformvalues.xml selected for the scan.
	Partial Match 1. Name exact match. Length allows wildcard.	The Web form name detected on the crawled Web page exactly matches a form name found in the global values section of the webformvalues.xml selected for the scan. The field length associated with that form value allows for submission to any field input length (wildcard field length match).
	Partial Match 2. Field name starts with Name value. Length exact match.	A Web form value in the file partially matches the field name found. All characters in the Web form value match the beginning of the Web page field name and the field length detected on the crawled Web page match the record in the Global Web form values section of the webformvalues.xml selected for the scan.
	Partial Match 3. Field name starts with Name value. Length allows wildcard.	A Web form value in the file partially matches the field name found. All characters in the Web form value match the beginning of the Web page field name and the field length for the record allows for submission to any field length (wildcard field length match).
	Partial Match 4. Name value included in field name. Length exact match.	A Web form value in the file partially matches the field name found. All characters in the Web form value match a portion of the Web page field name and the field length for the record allows for submission to any field length (wildcard field length match).

Table 3 Rules for Matching Web Form Values (cont'd)

	Partial Match 5. Name value included in field name. Length allows wildcard.	A Web form value in the file partially matches the field name found. All characters in the Web form value match a portion of the Web page field name and the field length for the record allows for submission to any field length (wildcard field length match).
No match	Field name has no exact or partial matches to Web form values.	No Web form value match was found. Submit the specified default value (Default).
No default value	The Web form values file has no default value specified.	No Web form value match was made and the default value is not in the webform values file. Submit "not found."

Web Brute

This tool will determine if your users are employing user names and passwords that an unauthorized intruder might be able to guess easily. For example, if one of your customers is accessing your Web site by using a username of "customer" and a password of "password," you might want to warn that user about his susceptibility and suggest that he change his password and/or username.

Web Brute will attempt a "brute force" attack of a login form or authentication page, using two prepared lists of user names and passwords.

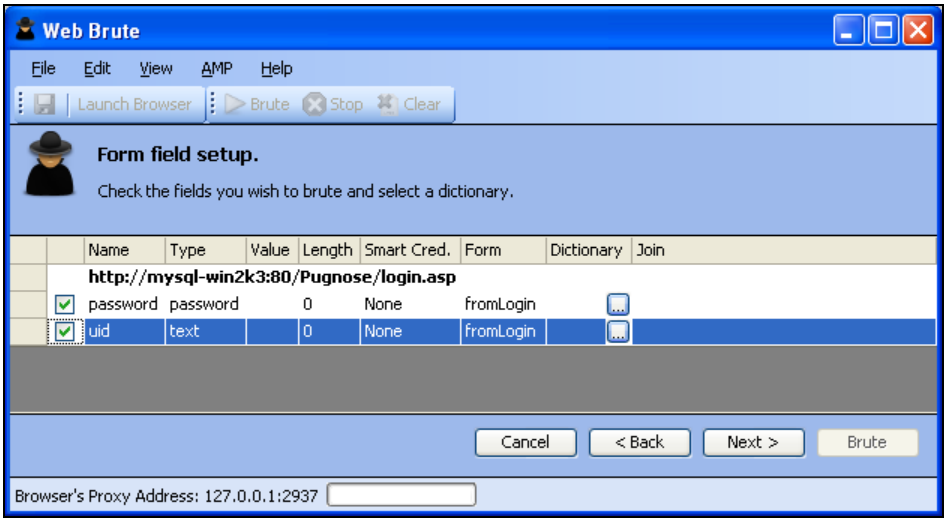
This is an intrusive attack and can break into a secure area. Brute force attacks are intended for testing purposes only, and should not be used against unsuspecting Web sites.

Mounting a Brute Force Attack

To use a brute force authentication attack:

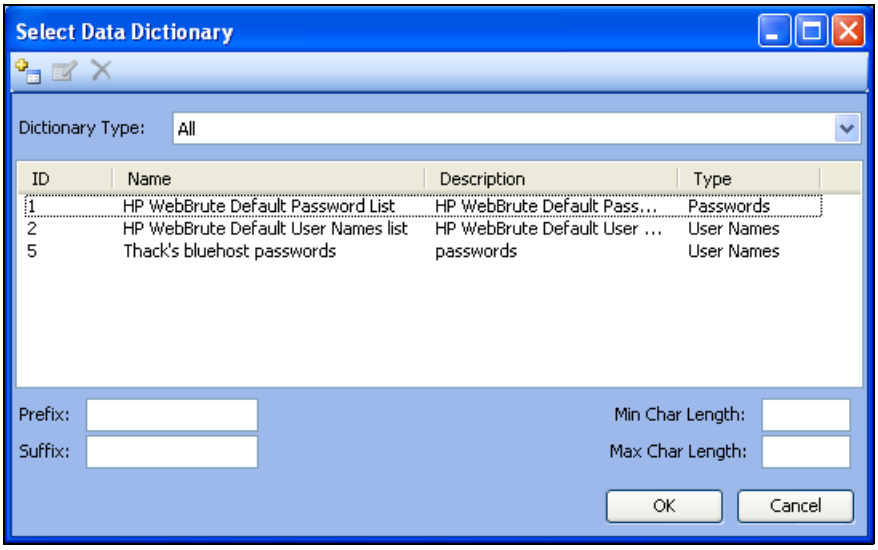
1. On the WebInspect Enterprise Console menu bar, click **Tools** → **Web Brute**.
2. In the **Enter URL** box, type the URL of the site you want attack and click **Next**.
3. Select the authentication method used by the target site. See Authentication on page 103 for a description of the available authentication methods.
4. If necessary, use the **Domain** box to specify the domain that should be used for authentication. Web Brute will prefix this string to each user name that it submits. Do not include a backslash.
5. Click **Next**.
6. If you selected **Web Form** in step 3, a Web browser opens. If necessary, navigate to the login page.

7 On Web Brute's **Form Field Setup** panel, select (check) the fields you want to brute force. If you already know the value that should be entered for a field, remove the check mark, double-click the cell in the **Value** column for that field, and enter the value.



8 For fields you have selected (checked), click [...] in the **Dictionary** column to select a list of names or passwords to be submitted.

The *Select Data Dictionary* window appears, listing all currently defined dictionaries. You can limit the display of dictionary names by selecting an entry in the **Dictionary Type** list.



These dictionaries are in a database that is not directly accessible. To create your own dictionary or merge a list into an existing dictionary, see Creating and Importing Lists on page 197.

9 Select a list.

10 (Optional) Enter the following:

- **Prefix**: A string that will be added to the beginning of each entry in the list.
- **Suffix**: A string that will be added to the end of each entry in the list.

- **Min Char Length**: The minimum number of characters allowed for each entry; entries that are shorter will not be submitted.
- **Max Char Length**: The maximum number of characters allowed for each entry; entries that are longer will not be submitted.

11 Click **OK**.

12 Repeat step 7through step 12 for each authentication field to be submitted.

13 If you want to "join" two or more lists, click the **Join** column associated with each list.

If a list of user names is joined with a list of passwords, then Web Brute will submit user names with passwords in the order in which they appear in the lists. That is, the first name in the user name list will be submitted with the first password in the password list, the second name will be submitted with the second password, etc.

If the two lists are not joined, then Web Brute submits each user name with all passwords. This feature is used most often for Web form authentication where the user must re-enter the password. In this case, Web Brute would use two lists, but the password list would be specified for both the "password" and "confirm password" fields. You would then join these fields, forcing the same password to be submitted for each field.

14 To modify the parameters that Web Brute uses during an authentication attack, select **Edit** → **Settings**. See Web Brute Settings on page 198 for more information.

15 Click **Next**.

16 To see a list of failed name/password attempts (in addition to successful attempts), select **Show Failed**.

17 Click **Brute**.

Web Brute attacks the site and displays the results. If you double-click a result (either successful or failed), Web Brute opens the HTTP Editor, allowing you to inspect both the HTTP request and response.

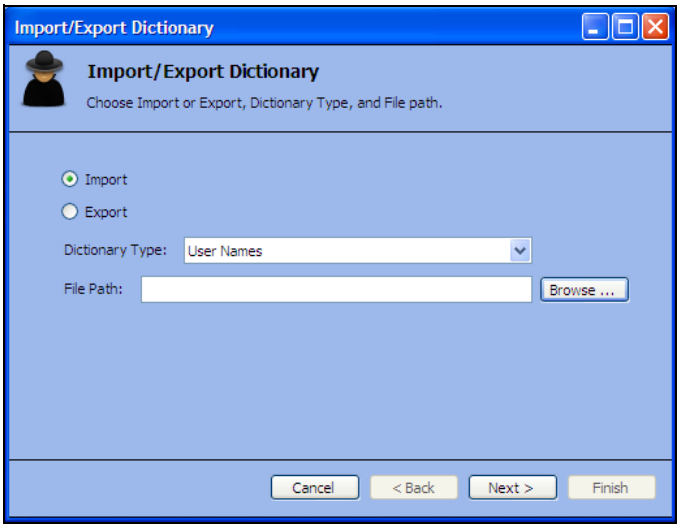
Creating and Importing Lists

To use your own list of passwords or user names, you must first create a list and then import it into Web Brute as a "dictionary," using the following procedure:

1 Create a text file where each entry is delimited by a carriage return and line feed.

2 Click **File** → **Import/Export Dictionary**.

3 On the *Import/Export Dictionary* window, select **Import**.



4 From the **Dictionary Type** list, select either **User Names**, **Passwords**, or **E-mails**.

5 Click **Browse** and select the file containing the list you want to import.

6 Click **Next**.

7 On the *Import Dictionary* window, specify a name for the dictionary and enter a description.

8 Click **Next**.

9 Click **Finish**.

Exporting Dictionaries

Use the following procedure to create a text file from a Web Brute dictionary:

1 Click **File** → **Import/Export Dictionary**.

2 On the *Import/Export Dictionary* window, select **Export**.

3 In the **File Path** box, enter the path and name of the text file in which the dictionary contents will be saved, or click **Browse** and use the *Save As* window to specify the name and path.

4 Click **Next**.

5 On the *Export Dictionary* window, select a dictionary type from the list.

6 Select a dictionary.

7 Click **Next**.

8 Click **Finish**.

9 Click **Done**.

Web Brute Settings

To modify the Web Brute settings:

1 Click **Edit** → **Settings**.

2 Select either the **Options**, **Authentication**, or **Proxy** tab and enter the settings described in the following sections.

3 Click **OK**.

Options

Timeout in seconds

Enter the number of seconds that Web Brute will wait for a response. If a response is not received during this period, Web Brute will resend the request, up to the number of times specified in the Retry Count setting.

Retry Count

Enter the number of times that Web Brute will resend a request that has not been acknowledged.

Apply State

If you select this option, Web Brute will attempt to maintain state during the procedure.

Apply Proxy

If you select this option, Web Brute will use the settings on the Proxy tab to connect to the target site (if the Direct Connection option is not selected).

Logging

Select the types of messages that should be logged.

Max Concurrent Threads

Enter or select the number of requests that Web Brute may send before requiring a response to the first request.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document. For pages that do not announce their character set, you can specify which character set the Web Brute should use.

Authentication

4 If required, select an authentication method and provide credentials. The methods are:

- **None**—Select this option if the site does not require authentication.
- **Automatic Authentication**—This allows Web Brute to determine the correct authentication method.
- **HTTP Basic Authentication**—This is a widely used, industry-standard method for collecting user name and password information. Normally, a Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials. The Web browser then attempts to establish a connection to a server using the user's credentials.
- **NTLM Authentication**—NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

After selecting an authentication method, enter a user name and password. To avoid typographic errors, re-enter the password in the **Confirm Password** box.

Proxy

Use these settings to access the Web Brute through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, Web Brute will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

Specify Alternative Proxy for HTTPS

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Web Discovery

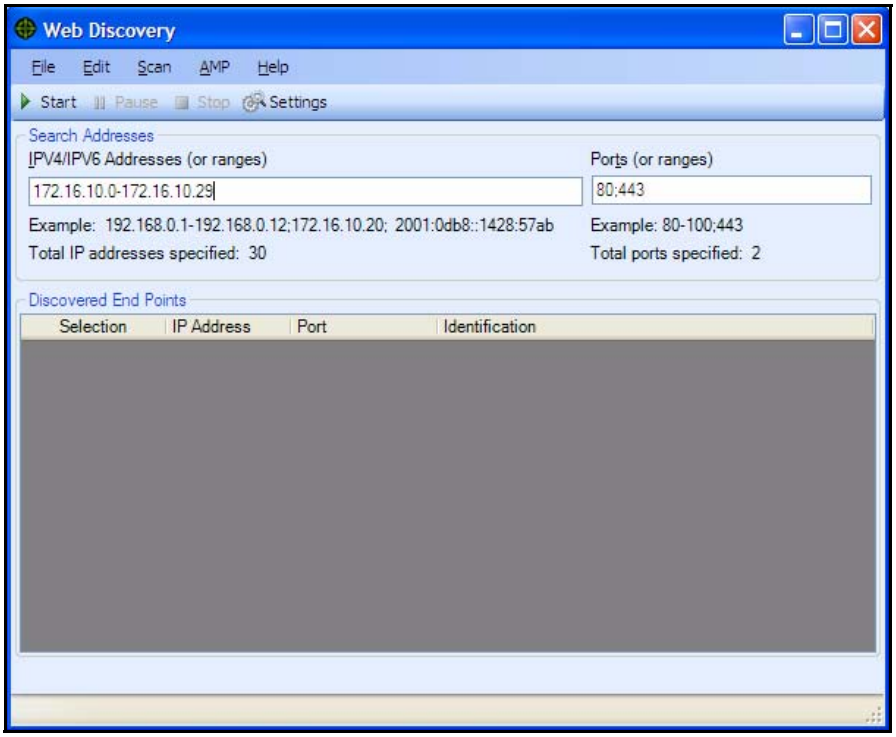
Use Web Discovery to find all open hosts in your enterprise environment.

Web Discovery sends packets to all the open ports (in a range of IP addresses and ports that you specify), searches the server's response for specific information, and then displays the results. There are two predefined packets included with Web Discovery: Web Server and SSL Web Server. They both contain the following HTTP request:

GET / HTTP/1.0

Web Discovery searches the HTTP response for the string "HTTP"; if it finds the string, it displays the IP address, port number, and the text "WebServer," followed by the results of a regular expression search designed to reveal the server's name and version number.

You can save the list of discovered servers in a text file.



Discovering Sites

To run Web Discovery to discover sites:

1. In the **IPV4/IPV6 Addresses (or ranges)** box, type one or more IP addresses (or a range of IP addresses).
   - Use a semicolon to separate multiple addresses.
     Example: 172.16.10.3;172.16.10.44;188.23.102.5
   - Use a dash or hyphen to separate the starting and ending IP addresses in a range.
     Example: 10.2.1.70-10.2.1.90.
2. In the **Ports (or ranges)** box, type the ports you want to scan.
   - Use a semicolon to separate multiple ports.
     Example: 80;8080;443

- Use a dash or hyphen to separate the starting and ending ports in a range. Example: 80-8080.

3 To modify Web Discovery settings, click **Settings**. See Web Discovery Settings on page 202 for more information.

4 Click **Start** to initiate the discovery process.

Results display in the Discovered EndPoints area.

5 Click an entry in the **IP Address** column to view that site in a browser.

6 Click an entry in the **Identification** column to open the *Settings Properties* window and view the raw request and response.

To save the list of discovered servers:

1 Click **File** → **Export** → **To CSV File.**

When you export the data to a `.csv` file, the IP addresses become default SSC project names. You can edit those projects and their associated data in Microsoft Excel and then import the projects into SSC. For more information, see Importing Projects Converted from Web Discoveries into SSC on page 49.

2 Use the standard file-selection window to name and save the file.

Web Discovery Settings

To modify the Web Discovery settings:

1 Click **Edit** → **Settings**.

2 Enter the settings described in the following sections.

3 Click **OK**.

Select Protocols

Choose the packet type you want to send by selecting or clearing the check box next to the protocol name.

Logging

Select the elements you want to log:

- **Log Open Ports**: Logs all available ports found open on the host; saves only Web server information in log file.
- **Log Services**: Logs all services identified during the discovery.
- **Log Web Servers**: Logs Web servers identified.

Enter the file location in the **Log To** box, or click the ellipsis button and use the standard file-selection window to specify the file in which the log entries should be recorded.

Connectivity

Set the following timeouts (in milliseconds):

- **Connection**: The period of time that Web Discovery will wait before stopping a port scan when no information has been returned from an IP address.

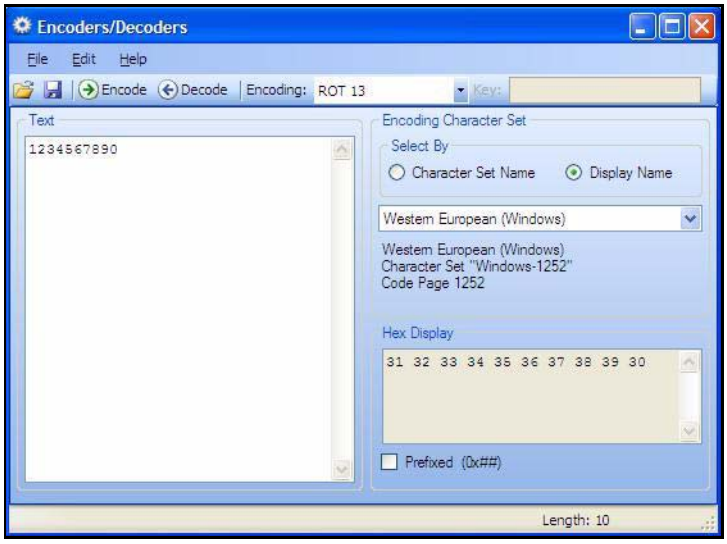
- **Send**: When sending a message to the remote IP endpoint, the transmission is divided into smaller packets. If the IP endpoint does not acknowledge receipt of a sent packet within the specified period of time, the socket is closed and the discovery for that endpoint reports no services.
- **Receive**: When sending a message to the remote IP endpoint, the transmission is divided into smaller packets. If the Web Discovery tool does not receive the sent packet within the specified period of time, the socket is closed and the discovery for that endpoint reports no services.

Adjust the number of open sockets using the **Sockets** box. A higher number of open sockets results in a faster scan. However, a setting that exceeds a server's threshold may result in false positives.

If you are using Windows XP with Service Pack 2 (SP2), your **Open Sockets** setting is set to 10. If you increase this setting, you will increase the likelihood that the scanner will fail to detect servers. This occurs because Microsoft has limited the number of open sockets to 10.

Encoders/Decoders

This tool allows you to encode and decode values using Base64, hexadecimal, MD5, and other schemes. You can also encode a string into a Unicode string and use special characters in URL construction. During the analysis of your scan results, when you encounter a string that you suspect is in an encoded or encrypted format, you can simply copy the string, paste it into the Encoders/Decoders tool, and then click **Decode**.



Encoding a String

To encode a string:

1. Type (or paste) a string into the **Text** area, or load the contents of a file by selecting **File** → **Open**.
2. Select an encoding character set using either the **Character Set Name** or the **Display Name**.
3. Select a cipher type from the **Encoding** list. For more information, see Encoding Types on page 205.
4. If necessary, type a key in the **Key** box. When a valid key is entered, the **Encode** and **Decode** buttons become enabled.
5. Click **Encode**.

   The **Text** area displays the encoded string; the **Hex Display** area displays the hexadecimal value of each character in the encoded string (formatted in the character set that you select).

Decoding a String

To decode a string:

1. Type (or paste) a string in the text area, or load the contents of a file by selecting **File** → **Open**.
2. Select an encoding character set using either the **Character Set Name** or the **Display Name**.
3. Select a cipher type from the **Encoding** list.
4. If necessary, type a key in the **Key** box.
5. Click **Decode**.

You can also use the encoding and decoding capabilities in the HTTP Editor. Right-click while editing a session to access encoding and decoding options.

Manipulating Encoded Strings

The encoded form of a string may contain characters that are non-printable. This often occurs when using a hash-based encoding scheme or any encoding scheme that requires a key. Since non-printable characters cannot be copied to the Windows clipboard, you cannot simply copy from or paste into the Encoder/Decoder. However, there are three methods you can use to work around this limitation:

- Save the encoded string to a file and, when you want to decode it, select **File** → **Open** to load it into the Encoder tool. Then decode it using the original method and (if applicable) key.
- Also, after encoding the string using the chosen encoding method and key, you can encode the resulting string using the base 64 method; then copy the string to the clipboard, paste the clipboard contents, decode using base 64, and decode again using the original method and (if applicable) key.

Encoding Types

The Encoder/Decoder allows you to select the encoding types described below.

- 3DES is a mode of the DES encryption algorithm that encrypts data three times (the string is encrypted, then the encryption is encrypted, and the resulting cipher text is encrypted a third time). The key must be 128 or 192 bits (16 or 24 characters).
- Base64 encodes and decodes triplets of 8-bit octets as groups of four characters, each representing 6 bits of the source 24 bits. Only characters present in all variants of ASCII and EBCDIC are used, avoiding incompatibilities in other forms of encoding.
- Blowfish is an encryption algorithm that can be used as a replacement for the DES algorithm.
- DES (Data Encryption Standard) is a widely-used method of data encryption that can use more than 72 quadrillion different private (and secret) encryption keys. Both the sender and the user must use the same private key.
- HEX is hexadecimal.
- MD5 produces a 128-bit “fingerprint” or “message digest” of whatever data you enter.
- RC2 is a variable key-size block cipher designed by Ronald Rivest. It has a block size of 64 bits and is about two to three times faster than DES in software.
- RC4 is a stream cipher designed by Ronald Rivest. It is a variable key-size stream cipher with byte-oriented operations. Used for file encryption in products such as RSA SecurPC and also used for secure communications, as in the encryption of traffic to and from secure Web sites using the SSL protocol.
- ROT13 is a simple Caesar cipher used for obscuring text by replacing each letter with the letter thirteen places down the alphabet.
- SHA1 is Secure Hash Algorithm, a one-way hash function developed by NIST and defined in standard FIPS 180. SHA-1 is a revision published in 1994; it is also described in ANSI standard X9.30 (part 2).
- SHA256 uses 256-bit encryption.
- SHA384 uses 384-bit encryption.
- SHA512 uses 512-bit encryption.
- ToLower changes uppercase letters to lowercase.
- ToUpper changes lowercase letters to uppercase.

- TwoFish is an encryption algorithm based on an earlier Blowfish.
- Unicode provides a unique number for every character, regardless of the platform, program, or language.
- URL creates values that can be used for URL-encoding non-standard letters and characters for display in browsers and plug-ins that support them.
- XHTML encapsulates the entered data with text tags: <text>data</text>.
- XOR performs an Exclusive OR operation. You must provide a key. If the length of the key string is only one character, that character is ORed against each character in the encode/decode string.

Prefixed

C and languages with a similar syntax (such as C++, C#, Java and JavaScript) prefix hexadecimal numerals with “0x” (for example, 0x5A3). The leading zero allows the parser to recognize a number, and the “x” stands for hexadecimal.

Regular Expression Editor

A regular expression is a pattern that describes a set of strings. Regular expressions are constructed similarly to mathematical expressions by using various operators to combine smaller expressions. Only advanced users with a working knowledge of regular expressions should use this feature.

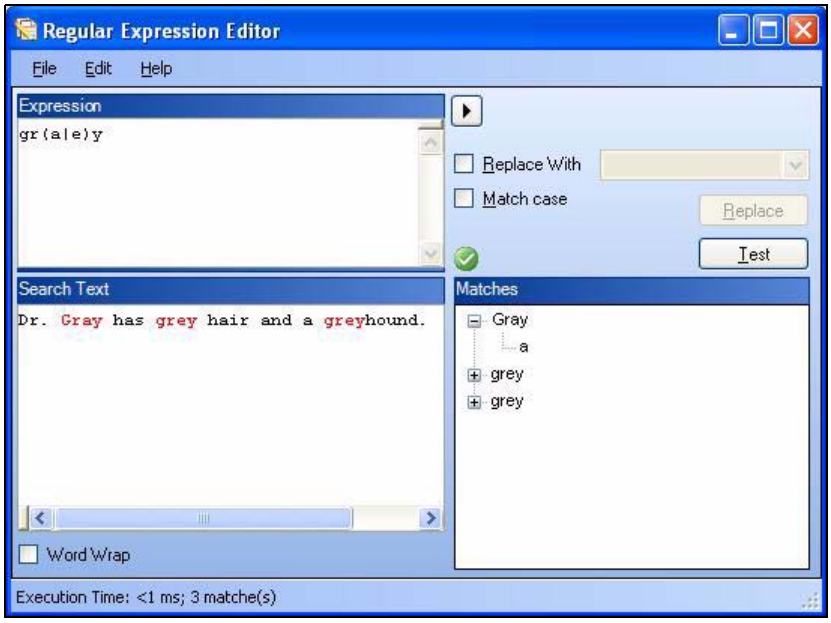
Testing a Regular Expression

Use the Regular Expression Editor to verify regular expressions.

To use the Regular Expression Editor:

1 Click **Tools** → **Regex Editor**.

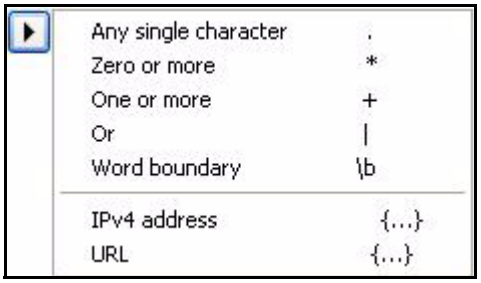
The *Regular Expression Editor* window opens.



2 In the **Expression** box, type or paste a regular expression that you believe will find the text for which you are searching.

For assistance, click  to reveal a list of objects. These include metacharacters and regular expressions that define a URL and an IP address. Click an object to insert it.

Note: You can also use special Regular Expression Extensions to restrict your search to certain areas of an HTTP message.



The Regular Expression Editor examines the syntax of the entered expression and displays  (if valid) or  (if invalid).

3 In the **Search Text** box, type (or paste) the text through which you want to search.

Alternatively, you can load an HTTP request or response message that you previously saved using the HTTP Editor. To do so:

a Click **File** → **Open Request**.

The Request file is actually a session containing data for both the HTTP request and response.

b Using the standard file-selection window, choose the file containing the saved session.

c Select either **Request** or **Response**.

d Click **OK**.

4 To find only those occurrences matching the case of the expression, select the **Match Case** check box.

5 If you want to substitute the string identified by the regular expression with a different string:

a Select the **Replace With** check box.

b Type or select a string using the drop-down combo box.

6 Click **Test** to search the target text for strings that match the regular expression. Matches will be highlighted in red.

7 If you selected the **Replace** option, click **Replace** to substitute all found strings with the replacement string.

Regular Expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used.

Table 4 Characters Used in Regular Expressions

Character	Description
\	Marks the next character as special. /n/ matches the character “n”. The sequence /\n/ matches a linefeed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/([^ec].*|e[^n].*|c[^a].*|.{3,})[/][./]* Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either “z” or “zoo.”
+	Matches the preceding character one or more times. /zo+/ matches “zoo” but not “z.”
?	Matches the preceding character zero or one time. /a?ve?/ matches the “ve” in “never.”

Table 4 Characters Used in Regular Expressions (cont'd)

Character	Description
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never early."
\B	Matches a nonword boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a nondigit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a linefeed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v].
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any nonword character. Equivalent to [^A-Za-z0-9_].

Regular Expression Extensions

Hewlett-Packard engineers have developed and implemented extensions to the normal regular expression syntax. When building a regular expression, you can use the following tags and operators:

Regular Expression Tags

- [BODY]
- [STATUSCODE]
- [STATUSDESCRIPTION]
- [STATUSLINE]
- [HEADERS]
- [ALL]
- [COOKIES]
- [SETCOOKIES]
- [METHOD]
- [REQUESTLINE]
- [VERSION]
- [POSTDATA]

- [URI]
- [TEXT]

Regular Expression Operators

- AND
- OR
- NOT
- [ ]
- ( )

Examples

To detect a response in which (a) the status line contains a status code of “200” and (b) the phrase “logged out” appears anywhere in the message body, use the following regular expression:

[STATUSCODE]200 AND [BODY]logged\sout

To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and having a reference to the path “/Login.asp” anywhere in the response, use the following:

[STATUSCODE]302 AND [ALL]Login.asp

To detect a response containing either (a) a status code of “200” and the phrase “logged out” or “session expired” anywhere in the body, or (b) a status code of “302” and a reference to the path “/Login.asp” anywhere in the response, use the following regular expression:

([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR
([STATUSCODE]302 AND [ALL]Login.asp)

Note that you must include a space (ASCII 32) before and after an “open” or “close” parenthesis; otherwise, the parenthesis will be erroneously considered as part of the regular expression.

To detect a redirection response where “login.aspx” appears anywhere in the redirection Location header, use the following regular expression:

[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx

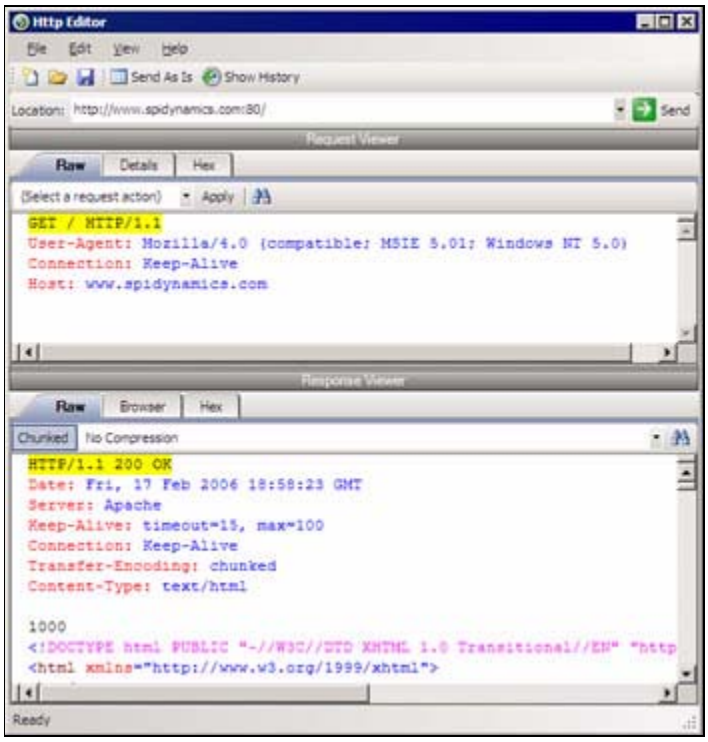
To detect a response containing a specific string (such as “Please Authenticate”) in the Reason-Phrase portion of the status line, use the following regular expression:

[STATUSDESCRIPTION]Please\sAuthenticate

HTTP Editor

Use the HTTP Editor to create or edit requests, send them to a server, and view the response either in raw HTML or as rendered in a browser. The HTTP Editor is a manual hacking tool that requires a working knowledge of HTML, HTTP, and request methods.

To set proxy and authorization parameters, if necessary, select **Edit** → **Settings**.



Request Viewer

The Request Viewer pane contains the HTTP request message, which you can view in three different formats using the following tabs:

- **Raw**—Depicts the line-by-line textual format of the request message.
- **Details**—Displays the header names and field values in a table format.
- **Hex**—Displays the hexadecimal and ASCII representation of the message.
- **XML**—Displays any XML content in the message body (Note: This tab appears only if the request contains XML-formatted data).

Response Viewer

The Response Viewer pane contains the HTTP response message, which you can also view in three different formats using the following tabs:

- **Raw**—Depicts the line-by-line textual format of the response message.
- **Browser**—Displays the response message as rendered in a browser.
- **Hex**—Displays the hexadecimal and ASCII representation of the response message.

- **XML**—Displays any XML content in the message body (Note: This tab appears only if the response contains XML-formatted data).

HTTP Editor Menus

File Menu

The **File** menu contains the following commands:

- **New Request**—Deletes all information from previous sessions and resets the Location URL.
- **Open Request**—Allows you to load a file containing an HTTP request saved during a previous session.
- **Save Request**—Allows you to save an HTTP request.
- **Save Request As**—Allows you to save an HTTP request.
- **URL Synchronization**—When selected, any characters you type into the Address combo box are added to the Request-URI of the HTTP request line.
- **Send As Is**—If you select this option, the HTTP Editor will not modify the request, regardless of any other settings you may select. This allows you to send a purposely malformed message. Authentication and proxy settings are disabled when using this option.

  Note: You may manually edit the request to go through a proxy, but most standard HTTP proxy servers cannot process non-compliant HTTP requests.
- **Exit**—Closes the HTTP Editor.

Edit Menu

The **Edit** menu contains the following commands:

- **Cut**—Deletes selected text and saves it to the clipboard.
- **Copy**—Saves the selected text to the clipboard.
- **Paste**—Inserts text from the clipboard.
- **Find**—Displays a window that allows you to search for text that you specify.
- **Settings**—Allows you to configure request, authentication, and proxy parameters for the HTTP Editor.

View Menu

The View menu contains the following commands:

- **Show History**—Displays a pane listing all HTTP requests sent.
- **Word Wrap**—Causes all text to fit within the defined margins.

Help Menu

The Help menu contains the following commands:

- **HTTP Editor Help**—Opens the Help file with the Contents tab active.
- **Index**—Opens the Help file with the Index tab active.
- **Search**—Opens the Help file with the Search tab active.
- **About HTTP Editor**—Displays information about the HTTP Editor.

Request Actions

The following options are available from the **Request Action** list in the Request Viewer pane.

PUT File Upload

The PUT method requests that the enclosed entity be stored under the supplied Request-URI.

To write a file to a server:

1. Select **PUT File Upload** from the drop-down list on the Request Viewer pane.
2. In the text box that appears to the right of the list, type the full path to a file
   - or -
   Click the Open Folder icon and select the file you want to upload.
3. Click **Apply**. This will also recalculate the content length.

Change Content-Length

In normal mode, if you edit the message body of the request, the HTTP Editor recalculates the content length and substitutes the appropriate value in the Content-length header. However, when using the Send As Is option, the HTTP Editor does not modify the content length. You can force this recalculation before sending the request by selecting **Change Content-Length** and clicking **Apply**.

URL Encode/Decode Param Values

The specification for URLs (RFC 1738, Dec. '94) limits the use of characters in URLs to a subset of the US-ASCII character set. HTML, on the other hand, allows the entire range of the ISO-8859-1 (ISO-Latin) character set to be used in documents, and HTML4 expands the allowable range to include the complete Unicode character set as well. To circumvent this limitation, you can encode non-standard letters and characters for display in browsers and plug-ins that support them.

URL encoding of a character consists of a "%" symbol, followed by the two-digit hexadecimal representation of the ISO-Latin code point for the character. For example:

- The asterisk symbol (*) = 42 decimal in the ISO-Latin set
- 42 decimal = 2A hexadecimal
- URL code for asterisk = %2A

You can use URL encoding to bypass an intruder detection system (IDS) that inspects request messages for certain keywords using only the ISO-Latin character set. For example, the IDS may search for "login" (in ISO-Latin), but not "%4C%4F%47%49%4E" (the URL-encoded equivalent).

To substitute URL code for parameters throughout the entire message, select **URL Encode Param Values** and click **Apply**.

To translate URL-encoded parameters to ISO-Latin, select **URL Decode Param Values** and click **Apply**.

Unicode Encode/Decode Request

The Unicode Worldwide Character Standard includes letters, digits, diacritics, punctuation marks, and technical symbols for all the world's principal written languages, using a uniform encoding scheme. Incorporating Unicode into client-server applications and Web sites offers significant cost savings over the use of legacy character sets. Unicode enables a single software product or a single Web site to be targeted across multiple platforms, languages and countries without re-engineering. It allows data to be transported through many different systems without corruption.

To translate the entire request message into Unicode, select **Unicode Encode Request** and click **Apply**.

To translate the entire request message from Unicode into ISO-Latin, select **Unicode Decode Request** and click **Apply**.

Create MultiPart Post

The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line. You can attempt to upload data by manipulating a POST request message.

To insert data from a file:

1. Select **Create MultiPart Post** from the **Action** list on the Request pane.
2. In the text box to the right of the **Action** list, type the full path to a file
   - or -
   Click the Open Folder icon and select the file you want to insert.
3. Click **Apply**.

Remove MultiPart Post

To remove a file that is part of a multipart request, select **Remove MultiPart Post** from the **Action** list on the Request pane.

Response Actions

The area immediately below the tabs on the Response Viewer pane contains three controls:

- a **Chunked** button
- a **Content Coding** drop-down list
- a button that launches the *Find In Response* dialog, allowing you to search the response for the text string you specify.

Chunked

If a server starts sending a response before knowing its total length, it might break the complete response into smaller chunks and send them in series. Such a response contains the “Transfer-Encoding: chunked” header. A chunked message body contains a series of chunks, followed by a line with “0” (zero), followed by optional footers and a blank line. Each chunk consists of two parts:

- A line with the size of the chunk data, in hex, possibly followed by a semicolon and extra parameters you can ignore (none are currently standard), and ending with CRLF
- The data itself, followed by CRLF

Content Codings

If the HTTP response contains compressed data, you can decompress the data using one of the options from the list.

- **GZIP**—A compression utility written for the GNU project.
- **Deflate**—The “zlib” format defined in RFC 1950 [31] in combination with the “deflate” compression mechanism described in RFC 1951 [29].

Editing and Sending Requests

To edit and send a request:

1. Modify the request message in the Request Viewer pane.

   To change certain features of the request, select an item from the **Action** list and click **Apply**.

2. Click **Send** to send the HTTP request message.

   The Response Viewer pane displays the HTTP response message when it is received.

3. To view the response as rendered in a browser, click the **Browser** tab.

4. You can prepare your next HTTP request using the HTML or JavaScript controls rendered on the **Browser** tab. To use this feature, you must select the **Interactive Navigation** option (click **Edit** → **Settings**).

5. To save a request, select **File** → **Save Requests**.

Searching for Text

To search for text in the request or response:

1. Click  in either the Request Viewer or Response Viewer pane.

2. Using either the *Find in Request* or *Find in Response* window, type or select a string or regular expression.

3. If using a regular expression as the search string, select the **Regex** check box.

4. Click **Find**.

HTTP Editor Settings

To modify the HTTP Editor settings:

1. Click **Edit** → **Settings**.

2. Select either the **Options**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.

3. Click **OK**.

Options

Send As Is

If you select this option, the HTTP Editor will not modify the request, regardless of any other settings you may select. This allows you to send a purposely malformed message. Authentication and proxy settings are disabled when using this option.

Note: You may manually edit the request to go through a proxy, but most standard HTTP proxy servers cannot process non-compliant HTTP requests.

Manipulate Request

If you select this option, the HTTP Editor will modify requests to accommodate the following parameters:

- **Apply State** — If your application uses cookies, URL rewriting, or post data techniques to maintain state within a session, the HTTP Editor will attempt to identify the method and modify the response accordingly.
- **Apply Proxy** — If you select this option, the HTTP Editor will modify the request according to the proxy settings you specify.
- **Apply Filter** — This option appears only when you invoke the HTTP Editor while using WebInspect and a scan tab has focus (that is, after opening or while conducting a scan). If you select this option, the HTTP Editor applies the Filters settings from WebInspect's Default Scan Settings to add search-and-replace rules for HTTP requests and responses. Note that if you change WebInspect's Current or Default Scan Settings, the changes will not be applied.
- **Apply Header** — This option appears only when you invoke the HTTP Editor while using WebInspect and a scan tab has focus (that is, after opening or while conducting a scan). If you select this option, the HTTP Editor applies the Cookies/Headers settings from WebInspect's Default Scan Settings for HTTP requests. Note that if you change WebInspect's Current or Default Scan Settings, the changes will not be applied.

Enable Active Content

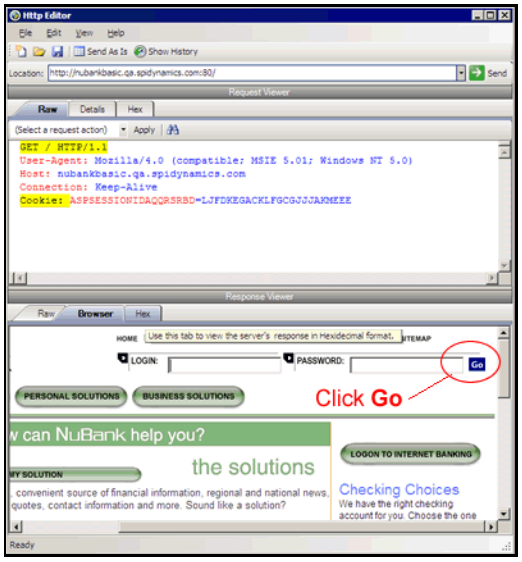
Select this option to allow execution of JavaScript and other dynamic content in all browser windows.

Navigation

In the **Navigation** group, select either **None**, **Interactive**, or **Browser Mode**.

You can view the server's response as rendered in a browser by selecting the **Browser** tab in the Response Viewer (the lower pane). If the **Interactive** feature is enabled, you can prepare your next HTTP request using the HTML or JavaScript controls rendered in the browser.

For example, using the logon page at nubankbasic.qa.spidynamics.com (shown below), you could enter a user name ("admin") and password ("admin"), and then click **Go**.



The HTTP Editor formats the request (which uses the POST method to the login1.asp resource) and displays it in the Request Viewer, as illustrated below. You could then edit the logon message (if required) or simply send it to the server by clicking **Send**.

If you select the **Browser Mode** option, then Interactive mode is enabled, but the HTTP Editor will send the request immediately, without first placing it in the Request Viewer and allowing you to edit it.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document. For pages that do not announce their character set, you can specify which character set the HTTP Editor should use.

Authentication

If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.

After selecting an authentication method, enter a user name and password. To avoid typographic errors, re-enter the password in the **Confirm Password** box.

Proxy

Use these settings to access the HTTP Editor through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the HTTP Editor will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Web Proxy

Web Proxy is a stand-alone, self-contained proxy server that you can configure and run on your desktop. With it, you can monitor traffic from the scanner, a browser, or any other tool that submits HTTP requests and receives responses from a server. It is a tool for debugging and penetration assessment; you can see every request and server response while browsing a site.

You can also create a Startup macro or a Login macro that you can use with WebInspect or WebInspect Enterprise.

Before using Web Proxy with your browser, you must configure your browser's proxy settings. If using Internet Explorer:

1. Click **Tools** → **Internet Options**.
2. Click the **Connections** tab.
3. Click **LAN Settings**.
4. On the *LAN Settings* window, select **Use a Proxy Server for your LAN** and enter the address and port of the proxy server you want to use. By default, Web Proxy uses your local host settings (127.0.0.1:8080).

Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, Web Proxy will not receive such traffic. This is a documented Microsoft defect. To access a site on "localhost" when using IE7, place a period or dot after "localhost" (for example, http://localhost.:8080/test.html).

You should also configure Microsoft Internet Explorer to use HTTP 1.1 through proxy connections. On Internet Explorer:

1. Click **Tools** → **Internet Options**.
2. Click the **Advanced** tab.
3. In the "HTTP1.1 settings" section, select **Use HTTP 1.1 through proxy connections**.

Using Web Proxy

To use Web Proxy with a browser:

1. Click **Tools** → **Web Proxy**.

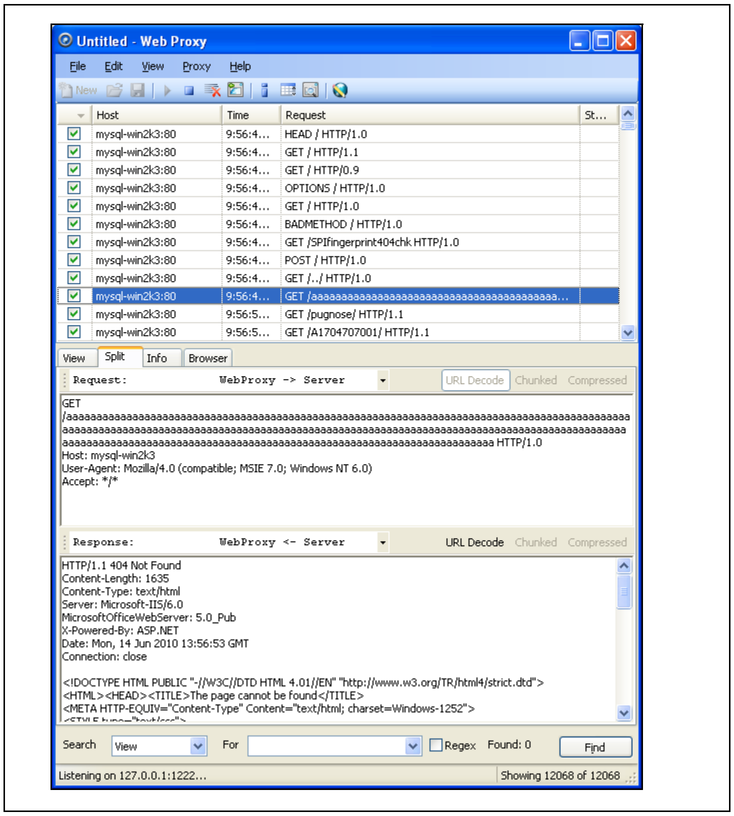
   The *Web Proxy* window opens.

2. Click  or select **Proxy** → **Start**.

   "Listening on <server:port number>" displays in the Web Proxy status bar.

3. Click **Launch Browser**  .
4. Manually navigate the site for which you want to view requests/responses.
5. If Web Proxy receives a request for a certificate from a Web Server, it displays a dialog asking you to locate the certificate. The program then caches your selection on a "per server" basis. Therefore, if you subsequently want to use a different certificate for a particular server, you must clear the cache by stopping and then restarting Web Proxy.
6. When you have browsed to all necessary pages, return to Web Proxy and click  (or click **Proxy** → **Stop**.

7 Each session (a request and matching response) you recorded is listed in the top pane. To view the actual HTTP message, select an entry. The message appears in the bottom frame. By default, the **View** tab is selected.



8 To change the format in which the message is displayed, select one of the tabs (**View**, **Split**, **Info**, or **Browser**).

When using the **View** or **Split** tabs, you can enable or disable URL decoding of requests and responses by selecting the **URL Decode** button. Since most WebInspect attack traffic is URL encoded, this feature makes it easier to analyze HTTP messages. To illustrate, compare the following URL encoded and decoded versions of the same GET request:

- GET / notes.asp?noteid=1%20union%20%20select%200%2c1%2c2%20from%20information_schema.tables%20order%20by%204%20desc%20limit%201 HTTP/1.1
- GET /notes.asp?noteid=1 union select 0,1,2 from information_schema.tables order by 4 desc limit 1 HTTP/1.1

The **Chunked** and **Compressed** buttons are enabled if a response is either chunked-encoded or compressed. This allows you to view the original response received by Web Proxy as well as the de-chunked or decompressed response.

9 To resend a request (with or without editing), select it from the list of displayed sessions and click the HTTP Editor icon (or right-click the request and select HTTP Editor from the context menu).

10 To clear sessions from the list, select one or more sessions and press the Delete key (or click **Edit** → **Clear Selected**). To clear all sessions, click  (or click **Edit** → **Clear All**).

Note: When you clear a session from the Web Proxy list, you also remove it from the captured data. For example, if you have 100 sessions in the list and clear 98 of them, and then save the sessions to a file, only the two remaining sessions will be included. When clearing sessions, ignore the check boxes.

Use the **File** menu to save selected requests to a proxy session file (.psf) and later load them for analysis (using the **File** → **Open** command). You can also save a sequence of requests as a Web Macro that you can use when conducting a WebInspect scan. All **File** menu commands apply to "check-marked" requests.

Use the **File** menu to save selected requests to an xml file and later load them for analysis. You can also save a sequence of requests as a Web Macro that you can use when conducting a scan. All **File** menu commands apply to "check-marked" requests.

Click the top of any column to sort the requests by that selection. For example, to sort the requests by the time they were made, click the top border of the **Time** column.

You must stop Web Proxy when you want to change Web Proxy settings.

Creating a Web Macro

You can use either the Web Macro Recorder or Web Proxy to create a Start macro or a Login macro.

A Start macro is used most often to focus on a particular subsection of an application. It specifies URLs that an HP scanner will use to navigate to the area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application.

A Login macro is used for Web form authentication, allowing the scanner (or the WebInspect Enterprise sensor) to log in to an application. You can also incorporate logic that will prevent the scanner from inadvertently logging out of your application.

To create a macro using sessions captured by Web Proxy:

1. Select the sessions you want to include in the macro by placing a check mark in the left column.
2. Click **File** → **Create Web Macro**.
3. (Optional) On the *Create Web Macro* dialog, select **Enable Check For Logout** and then enter a regular expression that identifies a unique text or phrase that occurs in the server's HTTP response when a user logs out or when a user who is not logged in requests access to a protected URL.

   Background: During a normal scan, the scanner begins crawling your site at the home page. If it encounters a link to another resource (usually through an <A HREF> HTML tag), it will navigate to that URL and continue its assessment. If it follows a link to a logout page (or if the server automatically "logs out" a client after a certain number of minutes), the scanner will not be able to visit additional resources where the client is required to be logged in. When this inadvertent log-out occurs, the scanner must be able to log in again without user intervention. This process hinges on the scanner's ability to recognize when it is no longer logged in.

   In some applications, if the user logs out (by clicking a button or some other control), the server responds with a unique message, such as "Have a nice day." If you specify this phrase as the server's logout condition, the scanner searches every response message for this phrase. Whenever it detects the phrase, the scanner attempts to log in again by sending an HTTP request containing the username and password.

   The scanner can also detect that it has logged out if the server sends a specific message in response to the scanner's attempt to access a password-protected URL. For example, the server may respond with a status code of "302 Object moved." If the scanner knows specifically what to look for in this response, the program will recognize that it has been logged out and can re-establish a logged-in state.

   Using the background example (above), if your server returns a message such as "Have a nice day" when a user logs out of your application, then enter "Have\sa\snice\sday" as the regular expression ("\s" is used in regular expressions to designate a space). A more likely example is where the server returns a 302 status code and references a new URL. In this case, "[STATUSCODE]302 AND [ALL]http://login.myco.com/config/mail?" might be a typical regex phrase.

4 Enter a name in the **Save macro as** box.

5 Click **OK**.

Web Proxy Tabs

Each HTTP session (a single request and the associated response) is listed in the top pane of Web Proxy. When you select a session, Web Proxy displays information about the session in the lower pane. The information displayed depends on which tab you select.

Table 5 Web Proxy Tabs

Tab	Description
View	Use the **View** tab to select which HTTP messages you want to inspect. Options available from the drop-down list immediately below the tab are: **Session**: view the complete session (both request and response) **Request from browser to Web Proxy**: view only the request made by the browser to Web Proxy **Request to server from Web Proxy**: view only the Web Proxy request to the server **Response from server to Web Proxy**: view only the server response to Web Proxy **Response to browser from Web Proxy**: view only the Web Proxy response to the browser
Split	Click the **Split** tab to create two information areas for a single session. For example, you could show the HTTP request message created by the browser (in one area) and the HTTP response generated by the server (in the second area). You can cut, paste, and copy the raw request, and right-click to see a shortcut menu of encoding options. However, you cannot save an edited request from the Web Proxy tool. Use the HTTP Editor to save an edited request.
Info	Use the **Info** tab to view detailed information about the requests. Information includes the number of forms found, header information, and the properties of the page.
Browser	Click the **Browser** tab to view the response as formatted in a browser.

Web Proxy Settings

To access this feature, click **Edit** → **Settings**.

You cannot change settings while Web Proxy is running. Click **Proxy** → **Stop**, change settings, and then restart Web Proxy.

Task 1: Configure General Settings

1 Select the **General** tab.

2 In the **Proxy Listener Configuration** group, enter an IP address and port number. By default, Web Proxy uses address 127.0.0.1 and port 8080, but you can change this if necessary.

Both Web Proxy and your Web browser must use the same IP address and port. If using Internet Explorer, click **Tools** → **Internet Options**; click the **Connections** tab and click **LAN Settings**; on the *LAN Settings* window, select **Use a Proxy Server for your LAN** and enter the address and port of the proxy server you want to use.

To configure Web Proxy on your host to be used by another host, you will need to change the value of the Local IP Address. The default address of 127.0.0.1 is not available to outside hosts. If you change this value to your workstation's current IP address, remote stations can use your workstation as a proxy.

3 Use the **Do Not Record** option to create a regular expression filter that prevents files of specific types from being handled by Web Proxy. The most common types are already excluded as defaults, but other types (MPEG, PDF, etc.) can also be excluded. The purpose is to allow you to focus on HTTP request/response lines and headers by removing clutter from the message.

4 When using the interactive mode, you can force Web Proxy to pause when it:

- Receives a request from the client.
- Receives a response from the server.
- Finds text that satisfies the search rules you create (using the **Flag** tab).

If you select any of these options, Web Proxy will continue only when you click the **Allow** button.

5 In the **Logging** group, select the type of items you want to record in the log file and specify the directory in which the log file should be maintained. If you elect to record requests and/or responses, you can also choose to convert and log the data using Base 64 encoding. This can be useful when responses contain binary data (such as images or Flash files) that you want to examine.

- Raw Request refers to the HTTP message sent from the client to Web Proxy.
- Modified Request refers to the HTTP message sent from Web Proxy to the server.
- Raw Response refers to the HTTP message sent from the server to Web Proxy.
- Modified Response refers to the HTTP message sent from Web Proxy to the client.

6 Most Web pages contain information that tells the browser what language encoding to use. This is accomplished by using a META tag with an HTTP-EQUIV attribute in the HEAD section of the HTML document, as in the following example:

```
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
```

For pages that do not announce their character set, choose an option from the **Assumed 'charset' Encoding** list to select the language (and implied character set) that Web Proxy should use.

Task 2: Configure Proxy Servers Settings

1 Click the **Proxy Servers** tab.

Use this area to add one or more proxy servers through which Web Proxy will route all its requests. Distributing the attack across multiple servers makes detection and counter-measures more difficult, thus mimicking how a hacker might attempt to avoid an intrusion detection system.

If you use multiple proxy servers, Web Proxy will "round-robin" the requests (i.e., Web Proxy will sequence through the list of proxy servers, sending the first request to the first server, the second request to the second server, and so on).

2 In the **Proxy Address** box**,** type the IP address of the server through which you want to route Web Proxy requests.

3 Specify the port number in the **Proxy Port** box.

4 Select the type of proxy (standard, SOCKS4, or SOCKS5) from the **Proxy Type** list.

5 If this proxy server requires authentication, select an authentication method and enter your authentication credentials in the **Username** and **Password** boxes. See Authentication on page 103 for a description of the available authentication methods.

6 Click **Add** to add the server and display its IP address in the **Available Proxy Servers** list.

You can also import a file containing a list of proxy servers by clicking **Import**. The file containing proxy information must be formatted as follows:

- Each line contains one record followed by a line feed and carriage return.
- Each field in the record is separated by a semicolon.
- The fields appear in the following order: address;port;proxytype;user name;password.
- The user name and the password are optional. However, if authorization is not used, you must include two semicolons as placeholders.

Examples:

128.121.4.5;8080;Standard;magician;abracadabra

127.153.0.3;80;socks4;;

128.121.6.9;443;socks5;myname;mypassword

7 If you do not need to use a proxy server to access certain URLs (such as internal testing sites), you can specify one or more hosts in the **Bypass Proxy List** area.

a Click **Add** in the **Bypass Proxy List** group.

The *Bypass Proxy* window appears.

b Enter the host portion of the HTTP URL that should be bypassed.

Do not include the protocol (such as http://).

For example, to bypass a proxy server for this URL

http://zero.webappsecurity.com/Page.html

enter this string

zero.webappsecurity.com

or this string

zero.*

You can also enter an IP address. Note that Web Proxy will not resolve host names to IP addresses. That is, if you specify an IP address and the HTTP request actually contains that numeric IP address, then Web Proxy will bypass a proxy server for that host. However, if the HTTP request contains a host name that resolves to the IP address that you specify, Web Proxy will still send the request to a proxy server.

c Click **OK**.

Task 3: Configure Search-and-Replace Settings

1 Click the **Search and Replace** tab.

Use this tab to create rules for locating and replacing text or values in HTTP messages. This feature provides a highly flexible tool for automating your simulated attacks. Some suggested uses include:

- Masking sensitive data, such as user names and passwords
- Appending a cookie to each request
- Modifying the Accept request-header field to add or delete media types that are acceptable for the response
- Replacing a variable in the Request-URI with a cross-site scripting attack

2 Click **Add** to create a default entry in the table.

3 Click the **Search Field** column of the entry.

4 Click the drop-down arrow and select the message area you want to search.

5 In the **Search For** column, type the data (or a regular expression representing the data) you want to find.

6 In the **Replace With** column, type the data you want to substitute for the found data.

7 Repeat this procedure to create additional search rules.

The request/response rules are applied sequentially, in the order in which they appear. For example, if a rule changes HTTPS to SSL, and if a subsequent rule then changes SSL to SECURE, the result will be that HTTPS is changed to SECURE.

Task 4: Configure Flag Settings

1 Click the **Flag** tab.

This feature allows you to find and highlight keywords in requests or responses.

2 Click **Add** to create a default entry in the table.

3 Click the **Search Field** column of the entry.

4 Click the drop-down arrow and select the message area you want to search.

5 In the **Search** column, type the data (or a regular expression representing the data) you want to find.

6 Click the **Flag** column of the entry.

7 Click the drop-down arrow and select a color with which to highlight the data, if found.

Task 5: Configure Evasion Settings

Evasions are techniques that Web Proxy uses to circumvent intrusion detection systems, monitors, sniffers, firewalls, log parsers, or any device that attempts to shield systems from attack by filtering HTTP requests. Typically, these filters examine portions of the request, searching for "signatures" that indicate malicious threats or potential breeches of system security. If they detect these signatures, they reject the request.

To evade detection, Web Proxy modifies the HTTP request to obscure the signature for which the filter is searching, while retaining integrity sufficient for the message to be processed by the server. Of course, the techniques used by Web Proxy are not always successful. As developers become aware of methods that compromise their product's effectiveness, they incorporate procedures to combat them.

This feature is intended for use as a penetration testing tool. Do not use it or enable it when conducting vulnerability assessment scans.

Use the following procedure to enable evasions:

1 Select the **Evasions** tab.

2 Select **Enable Evasions**.

Choose one or more evasion techniques, as described below.

Method Matching

Web Proxy replaces the GET method with HEAD. This is an attempt to defeat a filter that searches for a signature that begins with GET.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.microsoft.com/ HTTP/1.1
```

Web Proxy sends the following message to the server:

```
HEAD http://www.microsoft.com/ HTTP/1.1
```

URL Encoding

Web Proxy converts characters in the URL to a "%" followed by two hexadecimal digits corresponding to the character values in the ISO-8859-1 character set.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/cgi-bin/filename.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET %2f%63%67%69%2d%62%69%6e%2f%66%69%6c%65%
6e%61%6d%65%2e%63%67%69 HTTP/1.1

Host: zero.webappsecurity.com
```

If the device is looking for "cgi-bin" as the signature, it does not match the string "%63%67%69%2d%62%69%6e" and so the request is not rejected.

Double Slashes

Web proxy converts each forward slash (/) into a double forward slash (//).

For example, the browser sends the following message to Web Proxy:

```
GET http://www.microsoft.com/en/us/secrets.aspx HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET //en//us//secrets.aspx HTTP/1.1

Host: www.microsoft.com
```

If the device is looking for "/secrets.aspx" as the signature, it does not match the string "//secrets.aspx" and so the request is not rejected.

Reverse Traversal

This technique attempts to disguise a request for a certain resource by interjecting references to relative directories, which equates to the original request.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.TargetSite.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /d/../cgi-bin/d/../some.cgi HTTP/1.1
```
[which equates to GET/cgi-bin/some.cgi]

```
Host: www.TargetSite.com
```

Self-Reference Directories

Web Proxy uses the notation for parent directory (../) and current directory (./) to obfuscate the request.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.TargetSite.com/cgi-bin/phf HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /./cgi-bin/./phf HTTP/1.1  [which equates to GET /cgi-bin/phf]

Host: www.TargetSite.com
```

Parameter Hiding

A request can contain parameters that are used to build dynamic page content. These parameters are typically used when search requests or selections are made and take this form:

```
/anypage.php?attack=paramhiding&evasion=blackhat&success...
```

This technique is effective against a device that does not examine that portion of the request following the question mark (?). However, the parameter indicator can be used to potentially mask further relevant data.

For example, the browser sends the following message to Web Proxy:

```
GET /index.htm%3fparam=/../cgi -bin/test.cgi
```

Web Proxy sends the following message to the server:

```
GET /index.htm?param=/../cgi -bin/test.cgi
```

HTTP Misformatting

An HTTP request has a clearly defined structure:

Method<space>URI<space>HTTP/Version<CRLF><CRLF>

However, some Web servers will accept a request that contains a tab character instead of a space, as in the following:

Method<tab>URI<tab>HTTP/Version<CRLF><CRLF>

Any filter that incorporates the space (between the three components) as part of the signature for which it searches will fail to reject the request.

Long URLs

This technique is directed toward devices that do not examine the entire request string, but concentrate only on a subset of a programmable length (such as the first 50 characters). Web Proxy inserts a large number of random characters at the beginning of the request so that the operative portion of the request is pushed beyond the area normally examined by the filter.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/ HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /YPVIFAHD[hundreds of characters]NIWCJBXZPXMP/../ HTTP/1.1
Host: zero.webappsecurity.com
```

DOS/Win Directory Syntax

A Windows-based filter that attempts to detect a specific signature (such as /cgi-bin/some.cgi) might be fooled if a backward slash is substituted for a forward slash (such as /cgi-bin\some.cgi). Windows-based Web servers convert a forward slash to a backward slash when interpreting directory structures, so the notation is valid. However, HTTP rules require the first character of a URI to be a forward slash.

NULL Method Processing

This technique injects a URL-encoded NULL character immediately after the METHOD (such as GET%00). It is designed for a device that attempts to apply string operations on the request, and those string libraries use the NULL character to denote the end of a string. If this ploy is successful, detection of the NULL character prevents the device from examining the remainder of the message.

Case Sensitivity

This technique is designed to evade a filter that searches for a case-specific string.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /CGI-BIN/SOME.CGI HTTP/1.1
Host: zero.webappsecurity.com
```

Web Proxy Interactive Mode

Use Interactive mode to view each browser request and each server response as the messages arrive at Web Proxy. The message will not continue toward its destination until you click **Allow**. This permits you to modify the message before it is delivered.

You can also prevent the message from being sent to the server by clicking **Deny**.

Using the **Proxy** tab on the *Web Proxy Settings* window, you can force Web Proxy to pause after each request, after each response, or after locating specific text in either the request or response.

To turn on interactive mode:

1. Click **Proxy** → **Stop**.
2. Click **Proxy** → **Interactive**
   -or-
   click  on the toolbar.
3. Click **Proxy** → **Start**.

When Web Proxy is in Interactive mode, a check mark appears next to the Interactive command on the **Proxy** menu and the Interactive icon is backlit. Clicking the icon or selecting the command will toggle the Interactive mode on or off.

Smart Update

Each time you log in to the WebInspect Enterprise Console, it contacts the server and downloads any available console binary updates.

You can obtain updates to the SecureBase, as well as binary updates for WebInspect Enterprise-connected products such as WebInspect, through either a manual or scheduled process.

For details, see Smart Update on page 29 and Smart Update Approval on page 30.

Cookie Cruncher

The Cookie Cruncher analyzes cookies to determine the relative ease with which an attacker could predict or determine the value of a session ID generated by a server and delivered to a client via a cookie.

Background

The Web's Hypertext Transfer Protocol (HTTP) is stateless, meaning that each communication is discrete and unrelated to those that precede or follow. Because there is no continuity inherent in the protocol, application designers introduced the concept of "session." A session is defined as all activity by a user with a unique IP address on a Web site during a specified period of time. When a user logs into an application, a session is created on the server to maintain the state for other requests originating from the same user.

Each session has a unique identifier (session ID). This text string is transmitted between the client and the server, and may be stored in cookies, URLs, or hidden fields of Web pages. One problem with session IDs, however, is that many Web sites generate them using algorithms based on easily predictable variables, such as time or IP address. This predictability makes the Web sites vulnerable to session hijacking.

Session hijacking involves an attacker using session IDs to seize control of a legitimate user's session while that session is still in progress. The attacker can then gain complete access to the user's data, and can perform all operations that are normally available to the legitimate owner of the session.

Using the Cookie Cruncher

To use the Cookie Cruncher:

1. In the **URL** box, enter the URL of the site you want to test.

   If you are using the Cookie Cruncher to examine a site you have scanned with WebInspect::

   a. In the WebInspect navigation pane, click the cookies icon 

   . All HTTP responses containing a "Set-Cookie:" header are listed in the information pane.

   b. Double-click one of the listed responses.

   c. Click **Request**.

   d. Copy the request and paste it into the Cookie Cruncher's **Request** area.

2. In the **Sample** box, enter the number of requests the Cookie Cruncher should send to the server (expecting a cookie to be returned). A higher number of samples increases processing time, but produces more reliable result; a minimum of 100 is suggested.

3. Click **Sample**.

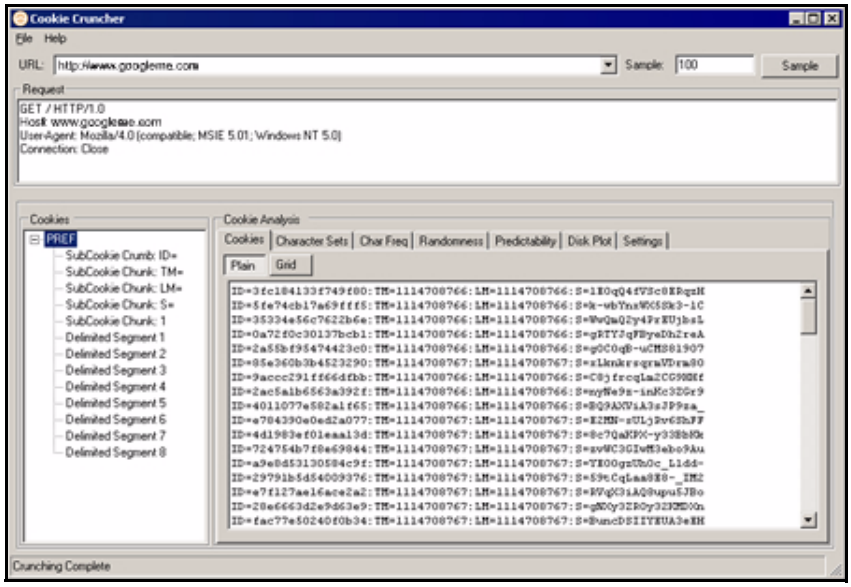
   As cookies are collected, the Cookie Cruncher organizes them into a tree hierarchy displayed in the vertical pane on the left side of the window.

4. Click a cookie in the tree hierarchy to analyze it. If subcookies are found, the Cookie Cruncher modifies the tree hierarchy; click the plus sign ⊞ to expand the level. Repeat as necessary.

5. To view the analysis, select a cookie or subcookie and click the various tabs.

6. To save the sampled cookies for future analysis, click **File** → **Save**.

   Cookie Cruncher cannot open and display a saved cookie file (.sck) if it contains fewer than four cookies.



Subcookies

Subcookies are either portions of cookie values that are common to many cookies, or interpreted values.

When the same string of characters appears in multiple cookies, you can choose that as a subcookie. The recurring expression will be eliminated from the cookies that contain it, and those cookies will be re-analyzed. The portion that is removed (the recurring expression) is called a “subcookie crumb.”

In the following sample, “086-” would be detected as a recurring expression:

086-1123

086-1127

087-6281

086-1132

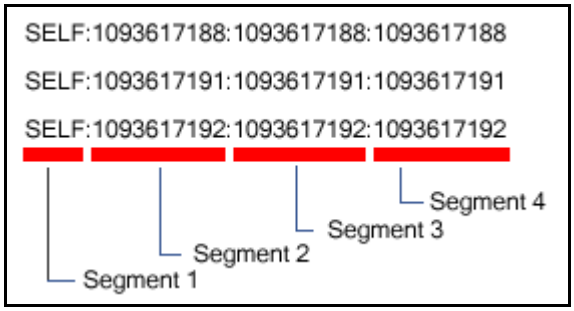
088-0518

087-6282

Analysis of those cookies containing the recurring expression (1123, 1127, 1132) would reveal the (most likely) incrementing cookie values that were interleaved with values from some other source.

If the detected character set of a sample consists of just 10 characters (Q-Z), these characters could possibly represent the digits 0-9. Choosing the re-encode option would run the cookies through an appropriate decoder algorithm (base-10, base-16, base-64, etc.) and re-analyze the cookies.

The “Delimited Segment” option(s) allow you to select the delimited portions of cookies. For example, the following subcookies contain four delimited segments.



To analyze the second segment of all subcookies, you would click the **Select Subcookie** list and select **Delimited Segment 2**.

Cookie Cruncher Tabs

Use the Cookie Cruncher tabs to analyze the sampled cookies. The tabs are:

- Cookies
- Character Sets
- Char Freq
- Randomness
- Predictability
- Disk Plot

Cookies Tab

This tab lists all cookies received from the server. You can view them either in plain or grid format by clicking the appropriate button.

Character Sets Tab

This tab displays the character set used to format the cookie:

A = alphabetic character (letters A-Z)

N = numeric character (numbers 0-9)

H = hexadecimal character (0-F)

T = Text A-Z, a-z

I = Illegal (anything else)

D = delimiter

Char Freq Tab

This tab displays a graph showing the number of times each ASCII character appeared in the total sample of cookies. A pale blue dot indicates an ASCII character whose number of appearances equals the number of cookies. A highlighted character indicates that it may be a delimiter (which is usually a character such as a comma, colon, or semicolon, but could also be something unusual such as “Z”).

Randomness Tab

This tab attempts to differentiate between random and non-random portions of cookies, based on the sample obtained.

Use the Grid view to illustrate the analysis of each column. The color key is:

Red = No randomness (or very little)
Orange = Somewhat random
White = Random

The top row of the grid indicates the numeric position of each character.

The second row displays, for each character position, a number representing the relative randomness of the character. This is actually the average number of bits that change per column from one cookie to the next.

Use the Graph view to illustrate the randomness level in a graphic format. The dashed green line represents the optimum (best practice) level of randomness. The red line represents the randomness of the cookies in the sample. In a well designed cookie, the red line should follow the green line. When the graph view is selected, you can save the graph (in BMP, GIF, PNG, or JPG format) using the **Save Graph** command in the **File** menu.

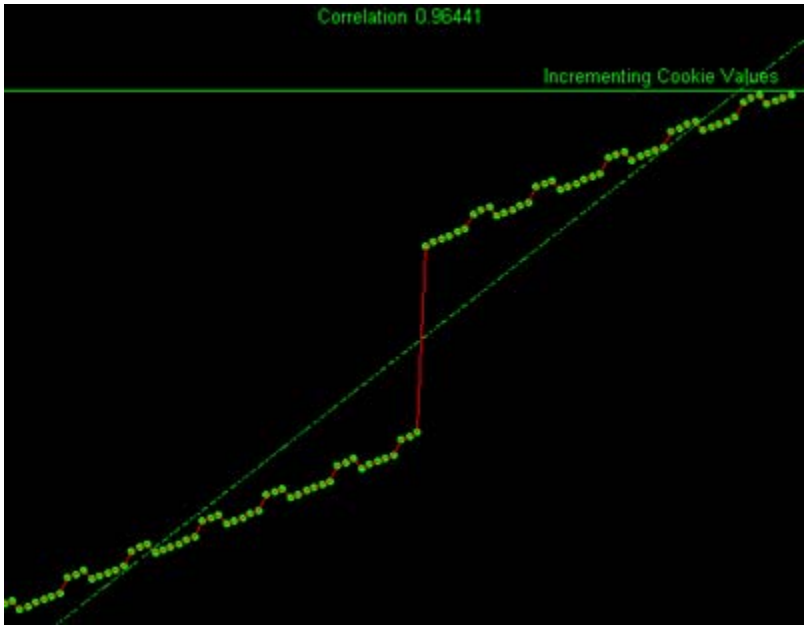
Predictability Tab

The Cookie Cruncher analysis produces a correlation value ranging from 0 to 1 and displays it at the top of the graph. A low value indicates that cookie generation is more random; a higher value indicates greater predictability.

The value of each cookie is plotted (on the Y axis) against the time the cookie was received (on the X axis). A scattered distribution indicates randomness, whereas a pattern approaching a line indicates predictability.

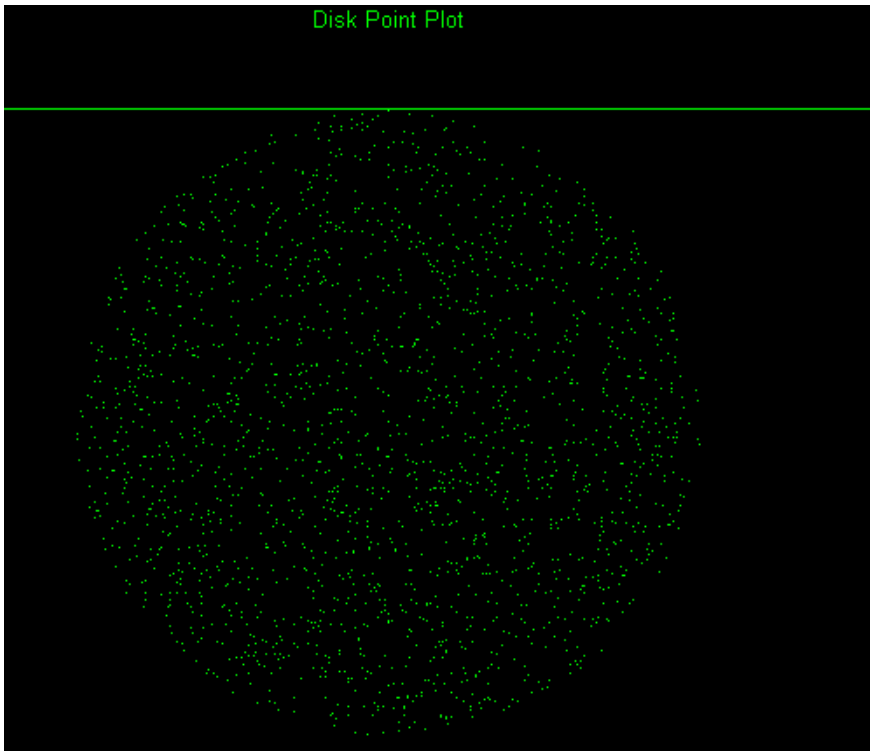
If the correlation is .9 or greater, the graph displays the header “Incrementing Cookie Values” or “Decremented Cookie Values” and draws a “best fit” line.

Only decimal or hexadecimal values can be plotted.



Disk Plot Tab

This graph plots a cookie's value against the sine and cosine functions. When random data is plotted, the points are evenly distributed around the plotting area. Only decimal or hexadecimal values can be plotted.



Cookie Cruncher Settings

To modify the Cookie Cruncher settings:

1. Click **Edit** → **Settings**.
2. Select either the **General**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.
3. Click **OK**.

General

Thread Count

Specify the maximum number of threads that can be created. The Cookie Cruncher can be configured to send up to 75 concurrent HTTP requests before waiting for an HTTP response to the first request. The default setting is 10. Increasing the thread count will increase the speed of the process, but might also exhaust your system resources as well as those of the server you are scanning. While most servers can handle a large number of requests, servers in development environments sometimes have licensing limitations that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5.

Socket Timeout

Specify the maximum number of open sockets permitted. A higher number of open sockets results in a faster process. However, a setting that exceeds a server's threshold may result in false positives.

If the Cookie Cruncher runs on Windows XP with Service Pack 2 (SP2), the number of open sockets should be set to 10.

Custom Delimiters

The Cookie Cruncher interprets certain characters (such as /.-!,:;=) as delimiters. In some cases, you may want to substitute your own list. For example, a cookie having a value of "ABC123456-C:Program" contains two default delimiters — a dash (-) and a colon (:) — and would therefore be split into three parts. However, if you specify only the dash as a delimiter, the cookie would be split into just two parts.

The user-specified list, if present, will cause an extra subcookie type to appear in the tree, in addition to the regularly parsed subcookie types. The subcookie item may not appear when the number of cookies having the delimiter(s) is less than 10 percent of the total cookie sample.

To create a list of custom delimiters, select the **Parse with Custom Delimiters** check box and then enter one or more delimiters in the **Characters** box.

Authentication

Authentication Method

If authentication is required, select a method from the **Authentication** list:

Authentication	Description
Automatic	Allow the Cookie Cruncher to determine the correct authentication method. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
HTTP Basic	A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.
NT LAN Manager (NTLM)	NTLM is an authentication process used by all members of the Windows NT family of products. It uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network. Use NTLM authentication for servers running IIS.

Authentication Credentials

Type a user ID in the **User name** box and the user's password in the **Password** box. To guard against mistyping, repeat the password in the **Confirm Password** box.

Proxy

Use these settings to access the Cookie Cruncher through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the Cookie Cruncher will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Web Fuzzer

"Fuzzing" is an automated software testing technique that generates and submits random or sequential data to various areas of an application in an attempt to uncover security vulnerabilities. For example, when searching for buffer overflows, a tester can simply generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

The Web Fuzzer lets you run several automated tests for common classes of Web application security vulnerabilities such as SQL injection, format strings, cross-site scripting, path traversal, odd characters, and buffer overflows, as well as protocol implementation problems.

Using the Web Fuzzer

To use the Web Fuzzer:

1. Click **Edit** → **Server**.
2. Enter the fully qualified domain name or IP address of a Web site, along with other server configuration information, and click **OK**.
3. Click **Edit** → **Settings**.
4. Configure the settings and click **OK**. For more information, see Web Fuzzer Settings on page 242.
5. To create a session, click **Session** and select either **Create** or **Raw Create**.
   a. If you select **Create**, Web Fuzzer displays a tabbed property sheet that identifies each section of an HTTP request and allows you to replace an HTTP element with generated data or with text that you enter. This structured approach is recommended for novice users. For detailed information, see Using the Session Editor on page 239.
   b. If you select **Raw Create**, Web Fuzzer displays a standard GET request formatted as regular text. You can edit the request. You can also place the cursor anywhere in the request, right-click to invoke a shortcut menu, and then insert a generator that will fuzz the selected HTTP element. If you highlight any portion of the request, the highlighted portion will be replaced by the generator.

Table 6 Fuzzer Generators

Generator	Function
Number	Inserts a whole number, within the range you specify, in each request; you specify the starting and ending number, the increment, and the number of times to loop through the series.
ASCII	Inserts one ASCII character, within the range you specify, in each request; you specify the starting and ending character, and the number of times to loop through the series.
Character	Generates the character you specify and inserts multiple numbers of the character into each request; you specify the minimum and maximum number of characters, and an increment.
Decimal Number	Inserts a fractional number, within the range you specify, in each request; you specify the starting and ending number, the increment, and the number of times to loop through the series.
Guid	Inserts a random Globally Unique Identifier (a 128-bit number) in each request; you specify the number of requests.

Table 6 Fuzzer Generators **(cont'd)**

Generator	Function
WordList Reader	Inserts a string from a text file you specify; the number of requests is determined by the number of paragraphs in the file; all characters in the paragraph are inserted.
SQL Injection	Inserts a string from a text file you specify; the number of requests is determined by the number of paragraphs in the file; all characters in the paragraph are inserted. The default file (sqlinjections.txt) contains the following two entries: ' or 1=1 ' or like '%
Text	Inserts the text you specify in a single request.
Cross-Site Scripting	Inserts a string from a text file you specify; the number of requests is determined by the number of paragraphs in the file; all characters in the paragraph are inserted. The default file (xssinjections.txt) contains the following entry: <script>alert('test')</script>
Method	Inserts a method (GET, POST, PUT, etc.); you specify the protocol version (0.9, 1.0, 1.1, or all).

6 After creating the request, click **OK**.

7 You can use filters so that only those server responses meeting criteria you specify will be displayed.

8 On the *Web Fuzzer Request* window, click **Start**.

The **Sessions** area lists each session (request and response) generated by the tool.

9 To examine the results, click an entry in the **Sessions** list.

- The HTTP request for the selected session appears in the **Request** area.
- The server's response appears on both the **Browser View** and **Raw Response** tabs.

10 To edit the request that you constructed, select a session in the **Sessions** group, then click the **Session** menu and choose either **Edit** or **Raw Edit**.

Filters

A filter consists of a name, description, and rule. The rule is a regular expression that defines the text you want to locate in a particular section of the server's response. For example, if you want to display only those responses that contain the word "error" in the response body and where the response also specifies a status code between 500 and 599, then use the following rule:

[STATUSCODE]5\d\d AND [BODY]\serror\s

Use the following notation to specify a response section:

- [HEADERS]
- [STATUSLINE]
- [STATUSCODE]
- [STATUSDESCRIPTION]
- [ALL]
- [SETCOOKIES]

- [BODY]

You access the *Filters* dialog by selecting **Filters** → **Edit**.

In addition to enabling a specific rule, you must also enable the use of rules in general by selecting **Filters** → **Enable**.

Creating a Filter

To create a filter:

1. Click **Add**.

   The tool creates a rule named Default Rule.
2. Modify the Name, Description, and Rule.
3. Click **Apply** to save the definition.

Using a Filter

To use a filter in a session:

1. Select a filter from the **Filters** list.
2. Select the **Enable** check box.

Deleting a Filter

To delete a filter:

1. Select a filter from the **Filters** list.
2. Click **Delete**.

Editing a Filter

To edit a filter:

1. Select a filter from the **Filters** list.
2. Modify the Name, Description, or Rule.
3. Click **Apply** to save the modifications.

Using the Session Editor

Use this tabbed property sheet to change specific sections of an HTTP request. You can replace an HTTP element with text that you type or paste into a text box, or you can insert a generator that will create multiple requests containing generated data.

To use the Session Editor:

1. Click a tab.
2. Do one of the following:
   - Edit the data appearing in text boxes, or
   - Select the **Use Generator** check box and click **Generator** to insert a generator.
3. To change other areas, click a different tab.

4 After configuring the areas you want to change, click **OK**.

5 When you return to the *Web Fuzzer* window, click **Start**.

Creating a Query String

To create a query string:

1 Click **Add**.

The text “name=value” appears in the list, representing the query string you are creating.

2 Click the **Name** tab.

You can edit the parameter named “name” or you can substitute a generator for it (select the **Use Generator** check box and click **Generator**).

3 Click the **Separator** tab.

You can edit the character that separates the name from the value (usually an equals sign) or you can substitute a generator for it (select the **Use Generator** check box and click **Generator**).

4 Click the **Value** tab.

You can edit the value in the equation or you can substitute a generator for it (select the **Use Generator** check box and click **Generator**).

5 Click the **Format** tab.

You can edit the order in which the equation elements appear, or you can introduce characters between them.

6 In the **Name Value Separator** group, you can edit the character that separates parameters (usually an ampersand) or you can substitute a generator for it (select the **Use Generator** check box and click **Generator**).

7 To add another parameter, click **Add** and repeat step 2 through step 6.

Session Editor Tabs

Method Tab

The GET method is specified by default. You can replace it with any text, or you can insert the Method generator.

Path Tab

You can fuzz three elements related to the path: the name of the file, the file extension, and the character that designates a directory level (usually the forward slash /). You can replace these elements with any text, or you can insert generators.

Query Tab

Some HTTP requests include a query string, with each parameter formatted as parameter=value and separated by an ampersand (&). The resource is separated from the query by a delimiter character (usually a question mark, although other characters can be used depending on the application). For example:

http://www.website.com/category.cfm?model_ID=0&category_ID=12.

Version Tab

The version indicates to the server which HTTP version to use for interpreting the request. Valid versions are 0.9, 1.0 and 1.1. The version information is formatted as "HTTP/version," which is a name-value pair separated by a forward slash (/). You can fuzz all three sections: Protocol, Separator, and Version. You can also fuzz the format by rearranging the order or introducing extraneous characters.

Headers Tab

Headers contain basic information issued by the client to help the server or application handle the request. Common headers are Host and User-Agent. Each header is defined by using the "name: value" syntax. This name-value structure also can be separated into four fuzzing opportunities.

Creating Headers

To create headers:

1. Click **Add**.

   The text "name:value" appears in the list, representing the header you are creating.

2. Click the **Name** tab. You can edit the parameter named "name" or you can substitute a generator for it (select the **Use Generator** check box and click **Generator**).

3. Click the **Separator** tab. You can edit the character that separates the name from the value (usually a colon) or you can substitute a generator for it.

4. Click the **Value** tab. You can edit the "value" text or you can substitute a generator for it.

5. Click the **Format** tab. You can edit the order in which the header elements appear, or you can introduce characters between them.

6. In the **Name Value Separator** group, you can edit the character that separates headers or you can substitute a generator for it.

7. To add another header, click **Add** and repeat step 2 through step 6.

Cookies Tab

Cookies are special headers that contain parameters used by the application to manage users and states. The format of a cookie definition is:

Cookie: name=value;name=value

Each parameter is a name-value pair that can be independently fuzzed.

Creating Cookies

To create cookies:

1. In the **Cookies** group, click **Add**.

   "Cookie:" appears in the list, representing the cookie you are creating.

2. Click **Cookie:** (in the Cookies list) and then click **Add** (in the **Cookie** group).

   The text "name=value" appears.

3. In the **Cookie** group, click the **Cookie Name** tab. You can edit the name or you can substitute a generator for it.

4. Click the **Separator** tab. You can edit the character that separates the name from the value (usually an equals sign) or you can substitute a generator for it.

5 Click the **Value** tab. You can edit the "value" text or you can substitute a generator for it.

6 Click the **Format** tab. You can edit the order in which the header elements appear, or you can introduce characters between them.

7 In the **Name Value Separator** group, you can edit the character that separates headers or you can substitute a generator for it.

8 To add another cookie, repeat this procedure.

Post Data Tab

While a query can be appended to the Request-URI, post data is added to the end of the request. The format is similar to the URI query and is mostly used with the POST method. When post data are used, the request must contain a Content-Length header that indicates the size of the post data. You can fuzz not only the post data, but also the Content-Length value to test how the server or application handles the differences.

When fuzzing the HTTP request message, you affect two main layers of the application environment: server protocol implementation and Web application.

Creating POST Data

To create post data:

1 Click **Add**.

The text "name=value" appears in the list, representing the post data you are creating.

2 Click the **Name** tab. You can edit the parameter named "name" or you can substitute a generator for it.

3 Click the **Separator** tab. You can edit the character that separates the name from the value (usually a colon) or you can substitute a generator for it.

4 Click the **Value** tab. You can edit the "value" text or you can substitute a generator for it.

5 Click the **Format** tab. You can edit the order in which the header elements appear, or you can introduce characters between them.

6 In the **Name Value Separator** group, you can edit the character that separates headers or you can substitute a generator for it.

7 To add another post data element, click **Add** and repeat step 2 through step 6.

Web Fuzzer Settings

To modify the Web Fuzzer settings:

1 Click **Edit** → **Settings**.

2 Select either the **General** or **Proxy** category and enter the settings described in the following sections.

3 Click **OK**.

General

Enable Filters

Select this option to enable filter support.

Auto scroll view

Select this option to enable automatic scrolling in the **Sessions List** view. This will force the view to scroll down to the latest session automatically.

Show ToolTips

Select this option to enable the display of tool tips when you hover your mouse pointer over certain controls.

Sockets

Enter the maximum number of sockets and the sockets send timeout (in seconds).

Protocol Compliance

Select **Enforce Content-Length** to automatically adjust the Content-Length value in the request when needed. If this feature is enabled, you cannot fuzz the content-length header.

Select **Enforce Host header** to include the Host header in all requests. If this feature is enabled, you cannot fuzz the host header.

Proxy

Use these settings to access the Web Fuzzer through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the Web Fuzzer will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a nethod from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.

4 If your proxy server requires authentication, enter the qualifying user name and password.

5 If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

SQL Injector

SQL injection is a technique for exploiting Web applications that use client-supplied data in SQL queries without first removing potentially harmful characters. The SQL Injector supports MS-SQL, Oracle, Postgress, MySQL, and DB2 as database types and also supports multiple language systems including Japanese.

This tool tests for SQL injection vulnerabilities by creating and submitting HTTP requests that may be processed by your SQL Server. If your Web application allows database records to be updated or created using data supplied by the user, the SQL Injector may create spurious records. To avoid this possibility, do not test against your production database. Instead, use a copy of the database, or use a test account that does not have access to the production data, or exclude from audit any pages that may update or delete data from the database. If these alternatives are not feasible, back up your production database before testing at a time when the site has little or no customer traffic.

Using the SQL Injector

To test for susceptibility to SQL injection:

1. If using a proxy server or if the target site requires authentication, click the **Settings** tab and enter the appropriate information. See SQL Injector Settings on page 247 for additional information.
2. Select **File** → **New**
   - or -
   click the New Request icon.
3. In the **Location** box, type or paste the URL that you suspect is susceptible to SQL injection. See examples below.
   - GET method (query parameters are embedded in the URL):
     http://172.16.61.10/Myweb/MSSQL/Welcome.asp?login=aaa&password=bbb
   - POST method (query parameters are included in message body):
     http://172.16.61.10:80/Myweb/MSSQL/Welcome.asp

     Because the SQL Injector defaults to the GET method, you must also edit POST requests on the **Raw** tab (visible if you select **View** → **Show Request**). The edited request would be similar to the following:

     POST /Myweb/MSSQL/POST/2.asp HTTP/1.1

     User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)

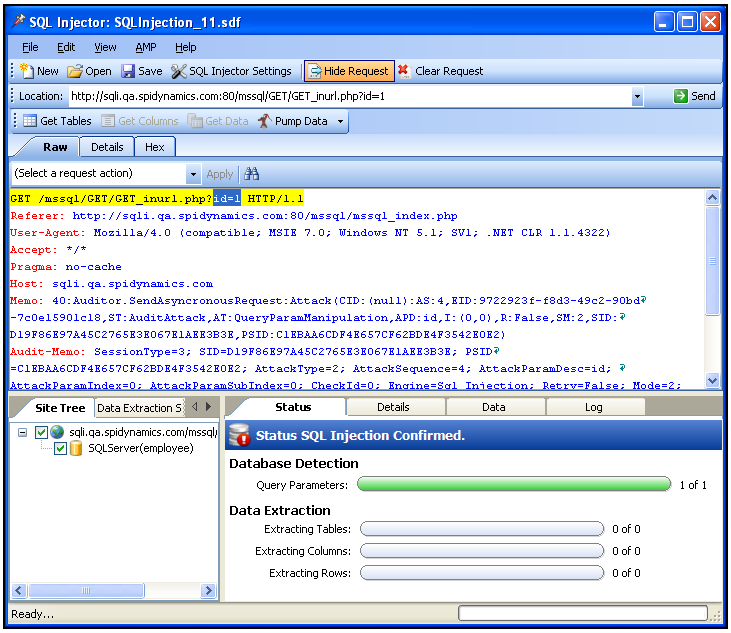
     Host: 172.16.61.10

     Content-Length: 22

     Content-Type: application/x-www-form-urlencoded

     login=qqq&password=aaa
4. Click **Send**.

If SQL injection is successful, “SQL Injection Confirmed” appears on the **Status** tab and the beginnings of a data hierarchy tree appear on the **Site Tree** tab in the lower left pane.



5 To extract all the data from all tables, click **Pump Data**.

Alternatively, you can selectively investigate tables and columns using the following procedure:

a Select **Get Tables**.

The SQL Injector returns the names of all tables in the targeted database.

b Choose tables by selecting or clearing their associated check box.

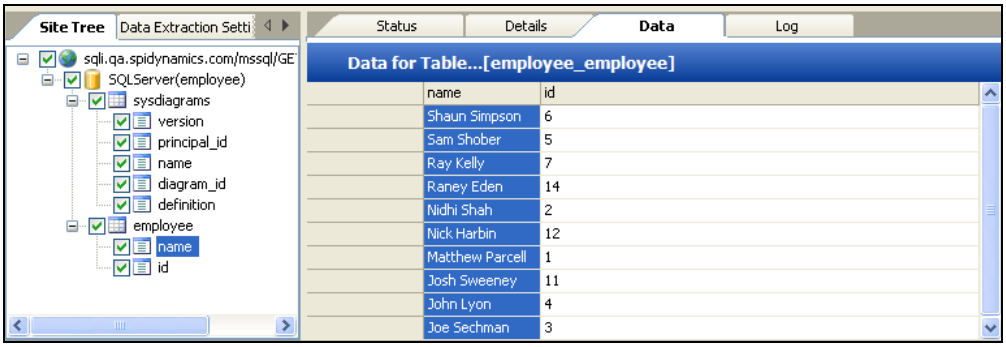
c Click **Get Columns**.

The SQL Injector returns the names of all columns in the selected tables.

d Choose a column by selecting or clearing its associated check box.

e Click **Get Data**.

6 Select a column and click the **Data** tab to column values.



SQL Injector Tabs

Request Pane

The Request pane contains three tabs:

- **Raw** - Displays the text of the HTTP request.
- **Details** - Displays the request segmented by method, request URI, and protocol. Also lists the request header fields and their associated values.
- **Hex** - Displays a hexadecimal representation of the HTTP request.

To toggle the display of the Request pane, click **Show Request**/**Hide Request**.

To delete the request, replacing it with the default http://localhost:80/, click **Clear Request**.

Database Pane

The lower left pane contains two tabs:

- **Site Tree** - Displays the URL, databases, tables, and columns.
- **Data Extraction Settings** - Displays the maximum number of tables, columns, and rows to return when extracting data. These values are extracted from the settings, but can be modified here or in the settings dialog.

Information Pane

The lower right pane contains four tabs:

- **Status** - Displays progress bars for detection and extraction functions.
- **Details** - Displays database information and injectable parameter details.
- **Data** - Displays data extracted from the selected tables and columns.
- **Log** - Displays a synopsis of pertinent functions and the time at which they occurred.

SQL Injector Settings

To modify the SQL Injector settings:

1. Click **Edit** → **Settings**.
2. Select either the **Options**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.
3. Click **OK**.

Options Tab

Timeout in Seconds

Specify the number of seconds that the SQL Injector will wait for a response before terminating the session.

Apply State

If your application uses cookies, URL rewriting, or post data techniques to maintain state within a session, the SQL Injector will attempt to identify the method and modify the response accordingly.

Apply Proxy

If you select this option, the SQL Injector will modify the request according to the proxy settings you specify.

Logging

Select the events you want to log:

- Requests
- Responses
- Errors
- Debug Messages

Log files are stored in xml format in My Documents\SPI dynamics\Tools\SQLInjector\logs.

The beginning of each file name is formatted as YYYY_MM_DD<current-process-id>. The remainder of the name is formatted as follows:

_sqli_debug.log: Contains debugging messages for that session.

_errors.log: Contains errors and exceptions that occurred for that session.

_RequestsResponses.log: Contains all the requests and responses sent and received by the SQL Injector.

Data Extraction

Specify the maximum number of tables, columns, and rows that should be returned when extracting data through a URL that is vulnerable to SQL injection. These values are also displayed in the Database pane on the **Data Extraction Settings** tab. You can change these values using either this tab or the *Settings* dialog.

Also specify the maximum number of concurrent threads that should be used for data extraction.

Inferential/Time-Based Extraction

The SQL Injector can use two different techniques for extracting data when a SQL injection vulnerability is discovered. All attempts are conducted using the inferential technique, which examines the content of the HTTP responses. If this method fails, you can force the tool to use a second technique called time-based extraction. Instead of extracting table data, this method attempts to retrieve the name of the database by sending 4-5 long-running database queries for each character in the database name. Since this can be a rather time-consuming exercise, you can specify the number of characters required to confirm the existence of the SQL injection vulnerability.

Use a macro

Select this option to use a startup macro; then click  to select, edit, or create a macro.

Database File Path

This read-only text box displays the path to the database created by the SQL Injector tool to store attack data and replicate portions of the attacked database.

Authentication Tab

Authentication Method

If the site does not require authentication, select **None**. Otherwise, select a method from the **Authentication** list:

Authentication	Description
Automatic	Allow the SQL Injector to determine the correct authentication method. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
HTTP Basic	A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.
NT LAN Manager (NTLM)	NTLM is an authentication process used by all members of the Windows NT family of products. It uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network. Use NTLM authentication for servers running IIS.

Authentication Credentials

Type a user ID in the **User name** box and the user's password in the **Password** box. To guard against mistyping, repeat the password in the **Confirm Password** box.

Proxy Tab

Use these settings to access the SQL Injector through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the SQL Injector will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Traffic-Mode Web Macro Recorder (Obsolete)

A macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct the HP scanner to begin a scan using this recording.

WebInspect Enterprise versions 10.00 and later include one Web Macro Recorder tool. They do not include the Traffic-Mode Web Macro Recorder that was provided in WebInspect Enterprise version 9.30 or earlier or in Assessment Management Platform (AMP). However, the latest Web Macro Recorder allows you to open, play back, and edit existing traffic-mode macros created in earlier WebInspect Enterprise and AMP versions, and create new traffic-mode macros, using its Internet Explorer browser technology (IE technology) option. When recording new macros, the latest Web Macro Recorder first uses event-based recording and Firefox browser technology by default, but if that fails for some reason, the Web Macro Recorder automatically switches to its traffic-mode IE technology as an alternative recording method. Based on its versatility, the latest Web Macro Recorder is also known as the Unified Web Macro Recorder.

For information about the Unified Web Macro Recorder, see Web Macro Recorder (Unified) on page 264. For more information about how you can use macros recorded with the Traffic-Mode Web Macro Recorder of earlier versions of WebInspect Enterprise and AMP, see Opening Macros Recorded with the Traffic-Mode Web Macro Recorder on page 266.

Event-Based IE Compatible Web Macro Recorder (Hidden)

A macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct the HP scanner to begin a scan using this recording.

WebInspect Enterprise versions 10.00 and later include one Web Macro Recorder tool. By default, it uses event-based functionality and Firefox browser technology to record new macros. The separate Event-Based IE Compatible Web Macro Recorder that was provided in earlier versions is no longer *directly* accessible in WebInspect Enterprise *menus*. In effect, it is hidden. However, as described in this section, the latest Web Macro Recorder allows you to indirectly open, play back, and edit existing event-based macros that were created in earlier versions of WebInspect Enterprise (or Assessment Management Platform—AMP), and create new macros, using the earlier Event-Based IE Compatible Web Macro Recorder.

HP strongly recommends that you use the latest Web Macro Recorder to record all new login macros and workflow macros.

Based on its versatility, the latest Web Macro Recorder is also known as the Unified Web Macro Recorder. For information about the Unified Web Macro Recorder, see Web Macro Recorder (Unified) on page 264. For information about how you can access and use macros recorded with the Event-Based IE Compatible Web Macro Recorder of earlier versions of WebInspect Enterprise (or AMP), see Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266.

Login Macros

A login macro is a recording of the activity that is required to access and log in to a website or web application, typically by entering a user name and password and clicking a button such as Log In or Log On. When you configure a WebInspect Enterprise scan, you usually specify a previously recorded login macro or record a new one at the time for the scan to use.

To prevent WebInspect Enterprise from terminating prematurely if it gets logged out of your application, a login macro should also specify at least one logout condition that definitively indicates that a logout has occurred. During a scan, WebInspect Enterprise can get logged out for a variety of reasons, including:

- Normal logout driven by the target site
- An error condition in the target site such as a timeout
- An error in the macro itself, such as an invalid parameter

Specifying a logout condition as part of the login macro makes it unnecessary for users to manually log back in, perhaps repeatedly, when unexpected logouts occur during a scan. When scanning a site, WebInspect Enterprise analyzes every target site response to determine the state. If the scanner determines at any time that it is logged out, it runs the login macro to log back in, and then it resumes crawling or auditing the site at the point where the logout occurred.

For the procedure to record a login macro, see Recording a Login Macro on page 253.

Workflow Macros

Workflow macros cannot be recorded using this Event-Based IE Compatible Web Macro Recorder tool.

If you open an existing *login* macro in this tool (see Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266, except for Guided Scan) and select **File** → **New** → **Workflow Macro**, the Unified Web Macro Recorder opens, replacing the Event-Based IE Compatible Web Macro Recorder. You can then record a workflow macro using the Unified Web Macro Recorder (see Web Macro Recorder (Unified) on page 264). Of course, it is simpler to just use the Unified Web Macro Recorder in the first place.

Recording a Login Macro

To record a new login macro in the Event-Based IE Compatible Web Macro Recorder (provided in WebInspect Enterprise version 9.30 or earlier and in AMP versions):

1. Open and edit an existing login macro that was created in the Event-Based IE Compatible Web Macro Recorder. See Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266.
2. Select **File** → **New** → **Login Macro**.
3. Click **Record**.
4. In the **Address** box, enter the URL of the target website and click  (or press **Enter**).

   The Web Macro Recorder renders the resource like a browser and records each event on the Events tab in the dockable pane positioned (by default) at the bottom of the window.
5. If necessary, navigate to the login screen.
6. Enter a valid user name and password, and submit the credentials (usually by clicking a button such as Log On, Go, Submit, etc.).
7. Click **Stop** (to the right of the Address bar) or **Stop Recording** (on the Status bar).
8. When prompted to play your macro, click **OK**.

   The macro plays by sequentially executing each enabled event listed on the **Events** tab. A message prompts you to either confirm the success of the macro and specify a logout condition or (assuming that the macro was not successful) troubleshoot the macro.
9. Do one of the following:
   - To specify a logout condition, select **Yes** and click **Finished**. Go to Specifying a Logout Condition.
   - To troubleshoot, select **No** and click **Next**. Go to Troubleshooting a Macro on page 254.

Specifying a Logout Condition

1. Navigate to a page where you are logged out (usually by clicking a button such as **Log Out**, **Log Off**, or **Exit**).
2. Do one of the following:
   - If the browser always displays this page when you log out, click **This page displays when I have logged out** (on the Selection Mode bar that appears directly under the Web Macro Recorder toolbar).
   - If the browser displays a page that contains an element or control that appears only when you are logged out, click **Select Logout Indication** (on the Selection Mode bar) and then click the element or control. For example, if a Login button appears when you have logged out, click **Select Logout Indication** and then click the Login button. Your selection appears on the **Logout Conditions** tab.
   - If you want the scanner to search each page for a condition that matches a regular expression that you create, click **Add Logout Regex**. See Regular Expression Editor on page 207 for details.
3. Select **File** → **Save** (or **Save As**).

Note: You can specify a logout condition at any time by clicking **Actions** → **Add Logout Condition**.

Specifying a Confirmation Element

After recording the macro, you may optionally identify a "confirmation element" that indicates that you have logged in successfully. This is particularly useful for those sites that, following a successful login, display a specific element or control on every page. Some sites, for example, always present a "Log Out" button after the user has logged in. Identifying this confirmation element increases the probability that WebInspect Enterprise will be able to recognize the "logged in" condition.

Once you identify a confirmation element, if the scanner does not detect that element on the page, it assumes the macro has failed and will attempt to replay the macro up to three times. If the confirmation hint is not detected during one of these playbacks, the scanner produces an error and stops trying to use the macro.

1. Navigate to a page that appears after you log in.
2. Click **Actions** → **Add Confirmation Element**.
3. Do one of the following:
   - If this page always appears after you log in, select **This page displays when I have logged in**.
   - Click **Select Confirmation Element** and then click an element on the page that appears only when you are logged in.

Troubleshooting a Macro

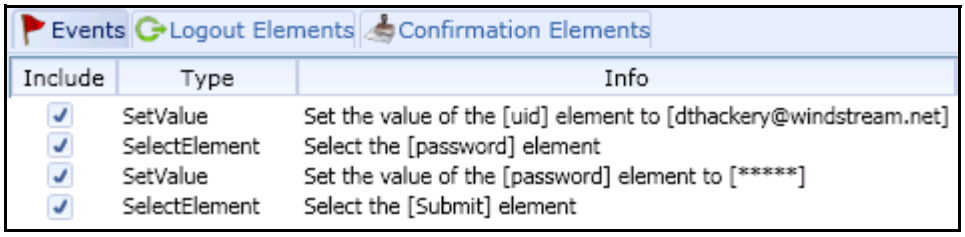
When troubleshooting your recorded macro, you have the following choices:

- **Replay Macro**. Try this solution first. The Web Macro Recorder normally plays the macro at the fastest possible speed, which may compromise performance. Use the slider to select either **Fast** (which is half the speed at which the macro was recorded) or **Original** (which mimics the speed at which the macro was originally recorded).
- **Switch to Unified Macro Recorder**. This closes the Event-Based IE Compatible Web Macro Recorder and opens the Unified Web Macro Recorder. See Web Macro Recorder (Unified) on page 264.
- **Adjust macro hints.** Allows you to add or change confirmation elements and/or logout conditions**.**
- **Re-record Macro**. This choice deletes all data and returns you to the beginning point, where you can try again to create a successful macro.

Editing a macro

After recording a macro, you can modify its contents by excluding certain events.

For example, if you entered the wrong validation credentials while attempting to log in, and then entered the correct credentials, you can remove the erroneous login events simply by clearing the check box (in the Include column of the **Events** tab) next to the event you want to exclude.



Usually, the best practice is to re-record the macro instead of editing it. However, for an extremely lengthy or complex macro, you can first attempt to modify it. Excluded events are not actually removed until you save the macro, so be sure to test the modified macro (by playing it) before you save it.

You might also need to add events for those situations where events are not recorded (such as login elements located in an iframe).

The Web Macro Recorder events are defined in the following table.

Event	Definition
WaitForPageLoad	Wait for the browser to complete the processing of pages.
NavigateTo	Navigate to the specified URL.
WaitForElement	Wait for element to be rendered on current page. This is used most often to render cascading menus.
WaitNumberOfSeconds	Pause for a specific number of seconds.
Click	Simulate a mouse click on an element.
MouseUp	Simulate any mouse button being released over an element.
MouseDown	Simulate any mouse button being pressed while the pointer is over an element.
SetValue	Simulate entering a value associated with an element.
JavaScript	Execute JavaScript.
Blur	Lose focus on the element.
SelectElement	Select the specified element.

Example: Adding Elements for Iframe Login

The most frequently encountered failure to record a login macro occurs when the login elements are contained within an iframe. During recording, you might enter a user name and password, and then click the Signin button, but nothing occurs when you play the macro.

You can edit the recorded events or you can begin by recording a new macro. If you edit the recording:

1. Click **Stop** (on the Status bar).
2. Deselect (remove the checks marks next to) those events that occur after the page is loaded.

Create an event for the user name element

1. Right-click the WaitForPageLoad event and select **Insert new event here** from the shortcut menu.
2. On the *Event Properties* dialog, click the drop-down arrow on the **Type** list and select **Click**.
3. Click **Locate an Element** (at the bottom of the dialog).
4. Move the mouse pointer to and click on the user name element (which may be labeled “name,” “user,” “email address” or other such identifier).
5. When the *Event Properties* dialog displays information about the element, click **OK**.

   Note that the event is added after (following) the event on which you clicked.

Add a value to the user name element

1. Right-click the event that you just added and select **Insert new event here** from the shortcut menu.
2. On the *Event Properties* dialog, select **SetValue** from the **Type** list.

3 Click **Locate an Element** (at the bottom of the dialog).

4 Click the user name element.

5 On the *Event Properties* dialog, enter a user name in the **Value** box and click **OK**.

Create an event for the password element

1 Right-click the event that you just added and select **Insert new event here** from the shortcut menu.

2 On the *Event Properties* dialog, select **Click** from the **Type** list.

3 Click **Locate an Element** (at the bottom of the dialog).

4 Click the password element.

5 When the *Event Properties* dialog displays information about the element, click **OK**.

Add a value to the password element

1 Right-click the event that you just added and select **Insert new event here** from the shortcut menu.

2 On the *Event Properties* dialog, select **SetValue** from the **Type** list.

3 Click **Locate an Element** (at the bottom of the dialog).

4 Click the password element.

5 On the *Event Properties* dialog, enter a password in the **Value** box and click **OK**.

Submit the user name and password

1 Right-click the event that you just added and select **Insert new event here** from the shortcut menu.

2 On the *Event Properties* dialog, select **Click** from the **Type** list.

3 Click **Locate an Element** (at the bottom of the dialog).

4 Click the submit element (which may be labeled “Submit,” “Sign In,” or other such identifier).

5 On the *Event Properties* dialog, click **OK**.

Dynamic Challenge-Response Authentication

Challenge-response authentication is a family of protocols in which the server presents a question (the challenge) and the client must provide a valid answer (the response). In the simplest example, the challenge asks for a password and the valid response is the correct password.

Many websites now present multiple challenges to the user. Typically, when a user first registers with a website, the site presents a list of questions to which the user provides answers that will be used for subsequent authentication. For example:

- What is your favorite color?
- What was the name of your first pet?
- In what town or city were your born?
- What was the make of your first automobile?

When the user later attempts to log in, the website presents two or more of these challenges.

Some sites also create groups of challenges, and present questions from different groups on each subsequent login attempt, as demonstrated in the following example.

When registering for the following example website, the user is asked to provide answers to nine questions, which are arranged into three groups of three questions each, as follows:

Group 1

"What is your name?", "Smith"
"What is your favorite color?", "blue"
"What is the name of your first grade teacher?", "Williams"

Group 2

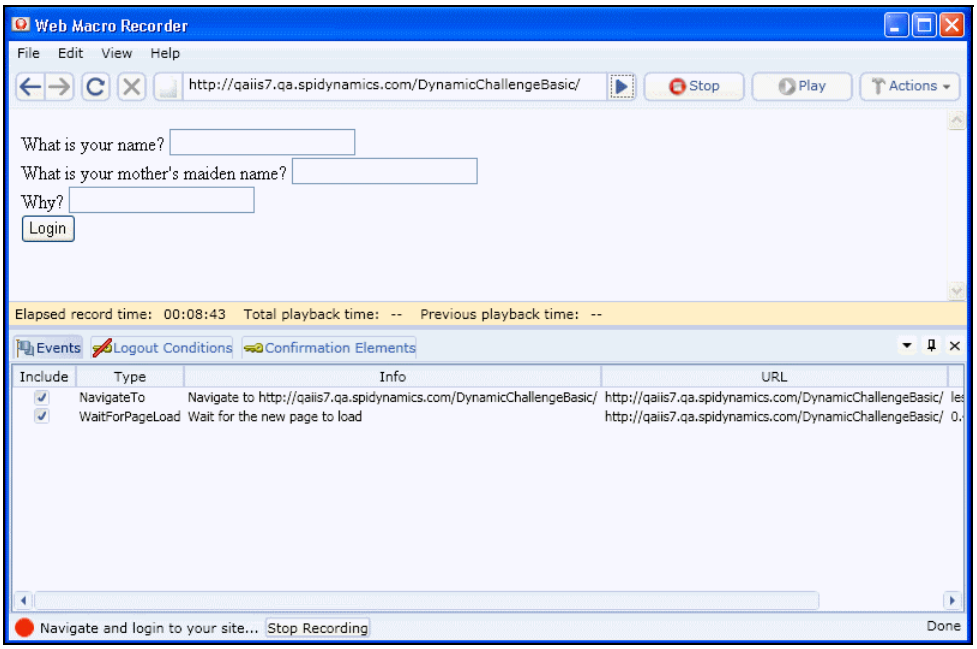
"What is your mother's maiden name?", "Larrimore"
"In what state were you born?", "Delaware"
"What is the name of your favorite pet?", "Rusty"

Group 3

"Why?", "Albatross"
"What is your paternal grandmother's first name?", "Esther"
"What is the capital of the state you live in?", "Atlanta"

In this example, the application randomly selects a number between 1 and 3 (inclusive) and then displays the corresponding ordinal question (first, second, or third) from each group.

1 Start the Web Macro Recorder, click **Record**, and enter the URL of the login page.



The source code for the pertinent area of the form is:

<label for="Q1"> What is your name?</Label><input id="Q1" name="Q1" />

<label for="Q2"> What is your mother's maiden name?</Label><input id="Q2" name="Q2" />

<label for="Q3"> Why?</Label><input id="Q3" name ="Q3" />

<input type="submit" value="Login" />

This illustrates that the label for each question is Q1, Q2, and Q3; similarly, the ID and name for each text box into which the user enters the response is Q1, Q2, and Q3.

2 On the login page, enter a value for each input element and click **Login**.

3 Assuming that you logged in correctly, click **Stop**.

4 When prompted to play your macro, click **Cancel**.

To modify the macro so that it accommodates a random presentation of authentication questions:

1 Navigate to the login page.

2 Click the **Events** tab.

3 Right-click the first SetValue element and choose **Select security question for this element**.

   a Click **Select Security Question** (just below the toolbar).

   b Click on the label for the first security question (in this example, "What is your name?").

   The *Question-Answer Groups* dialog appears.

   c In this example, we know that the first question is a member of the Q1 group. So click the **Add** button, enter "Q1" in the Group Name box, and click **OK**.

   Note: If your program does not divide questions and answers into groups, but presents the same set of questions at each login attempt, ignore the Group Name controls.

   d Click **Click here to add new question/answer pair**.

   e Enter the first question and answer pair. In this example:

   Question: What is your name?

   Answer: Smith

   f Repeat step d and step e, entering the second and third question/answer pairs in Group 1.

   g Click **OK**.

   Note that a **Sec. Questions** column is added to the **Events** tab.

   h Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select **Q1**.

4 Right-click the second SetValue element and choose **Select security question for this element**.

   a Click **Select Security Question** (just below the toolbar).

   b Click on the label for the second security question (in this example, "What is your mother's maiden name?").

   c Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select **Manage**.

   d On the *Question-Answer Groups* dialog, click **Add**, enter a group name of "Q2" and click **OK**.

   e Add the three security question/answer pairs for the Q2 group, following the procedure in step 3.

5 Right-click the third SetValue element and choose **Select security question for this element**.

   a Click **Select Security Question** (just below the toolbar).

   b Click on the label for the third security question (in this example, "Why?").

   c Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select **Manage**.

   d On the *Question-Answer Groups* dialog, click **Add**, enter a group name of "Q3" and click **OK**.

   e Add the three security question/answer pairs for the Q3 group, following the procedure in step 3.

6 Click **Play** to test the macro.

When troubleshooting the macro, it is usually helpful to right-click an entry on the **Events** tab and select **Playback macro to this event**.

Logout Elements

When the *Playback Successful?* dialog appears, the first of three messages at the bottom of the dialog pertains to logout conditions. These are elements, pages, or regular expressions that indicate to the Web Macro Recorder (and the scanner) that the user is no longer logged in to the site or application.

If the message is "Logout hints have been specified for this macro," the Web Macro Recorder has recognized the logout condition you specified.

However, if the message is "Unable to auto-detect logout hints (please add manually)," then one of the following occurred:

- You did not instruct the Web Macro Recorder to automatically detect logout elements (see Event-Based IE Compatible Web Macro Recorder Settings on page 261).
- The Web Macro Recorder was unable to auto-detect elements.
- You did not manually specify a logout condition.

To correct this error, click **Edit** → **Settings** → **Auto-Detection** and do one of the following:

- Select **Auto-detect logout conditions** and choose one or more of the standard logout elements (or create a custom logout element).
- Clear **Auto-detect logout conditions**, click **OK** to save the settings, and then:

  a. Click 

and select **Add Logout Condition**.

  b. Use the Forward and Back buttons  to navigate to a page that contains a logout element.

  c. Do one of the following:

     – Click 

and then click the page element that appears only when you are in a "logged out" condition.

     – If the entire page appears only after the user has logged out, click 

.

     – If you want the scanner to search each page for a logout condition that matches a regular expression that you create, click 

.

To delete a logout condition from the macro, click the **Logout Conditions** tab (in the Web Macro Recorder's lower pane), right-click a condition, and select **Delete**.

Using a Regular Expression for Logout Detection

If you want the scanner (and the Event-Based IE Compatible Web Macro Recorder) to use a regular expression to detect a logged out condition:

1. Select **Add Logout Regex**.

   The Regular Expression Editor opens.

2. Enter a regular expression that identifies a unique text or phrase that occurs in the server's HTTP response when a user logs off or when a user who is not logged on requests access to a protected URL.

   For example, if your server returns a message such as "Have a nice day" when a user logs off your application, then enter "Have\sa\snice\sday" as the regular expression ("\s" is used in regular expressions to denote a space).

The scanner can also detect that it has logged off if the server sends a specific message in response to the scanner's attempt to access a password-protected URL. For example, the server may respond with a status code of "302 Object moved." In this case,

"[STATUSCODE]302 AND [ALL] http://login.myco.com/config/mail?"

might be a typical regular expression. See Regular Expression Extensions on page 209 for more information.

3 Click **OK**.

Confirmation Elements (Hints)

When the *Playback Successful?* dialog appears, the second of three messages at the bottom of the dialog pertains to confirmation elements. These are elements or pages that indicate to the Web Macro Recorder (and the scanner) that the user is logged in to the site or application.

If the message is "Confirmation hints have been specified for this macro," the Web Macro Recorder has recognized the element that you specified as indicating that the user is logged in.

However, if the message is "Unable to auto-detect confirmation hints (please add manually)," then one of the following occurred:

- You did not instruct the Web Macro Recorder to automatically detect confirmation elements (see Event-Based IE Compatible Web Macro Recorder Settings on page 261).
- You instructed the Web Macro Recorder to automatically detect confirmation elements, but the Web Macro Recorder could not recognize the element you specified (or you failed to specify an element).
- You did not manually specify a confirmation element.

To correct this error, click **Edit** → **Settings** → **Auto-Detection** and do one of the following:

- Select **Auto-detect confirmation hints** and choose one or more of the standard elements (or create a custom element).
- Clear **Auto-detect confirmation hints**, click **OK** to save the settings, and then:

  a Click 

and select **Add Confirmation Element**.

  b Use the Forward and Back buttons  to navigate to a page that contains a confirmation element.

  c Do one of the following:

  – Click 

and then click the page element that appears only when you are in a "logged in" condition.

  – If the entire page appears only after the user has logged in, click 

.

Unsupported Elements

While recording your macro, the Event-Based IE Compatible Web Macro Recorder displays a warning if you click an unsupported element. These non-HTML elements include objects created using the following technologies:

- Applets

- ActiveX
- Silverlight
- Flash
- Cross-Domain Iframes

If these objects are not required components of your macro, there is no problem. The Event-Based IE Compatible Web Macro Recorder simply ignores the object and continues to record events as you generate them by navigating through the site.

However, if an unsupported element contains an essential component (such as a login form), the macro will not succeed.

You might avoid this issue by switching to the Unified Web Macro Recorder (see Web Macro Recorder (Unified) on page 264).

Event-Based IE Compatible Web Macro Recorder Settings

To modify the Event-Based IE Compatible Web Macro Recorder settings:

1. Click **Edit** → **Settings**.
2. Select either the **Application** or **Macro** category (described below) and enter the settings.
3. Click **OK**.

Application Settings

General

Show startup window

The startup window appears when the Event-Based IE Compatible Web Macro Recorder is launched. It displays a shortcut menu that allows you to begin creating or editing a login macro.

Compress macro files

Applies a compression algorithm to reduce the size of the saved macro.

Encrypt macro file

Applies an encryption algorithm to the saved macro to provide security.

Network Authentication Credentials

If network authentication is required, provide a user name and password that will allow access to the network.

Troubleshooting

Highlight failed events

If you select this option, the program displays failed events with a background color.

- Red highlight: The macro event caused the macro to fail.
- Orange highlight: The event failed, but playback continued.

Ignore events after final page load

In most cases, the events that occur after loading the final page in the macro are not significant and do not affect the playback of the macro.

Auto-Detection

During the recording process, you can manually specify a logout element and a confirmation element (an object that appears on the page to indicate that you have logged in successfully). If auto-detection is enabled and the program automatically detects a logout element during the recording process, the wizard that appears once playback is complete will reflect this and you will not be prompted to select a logout element.

To instruct the Web Macro Recorder to automatically detect elements, select **Auto-detect logout conditions** and/or **Autodetect confirmation hints**.

To identify which of the standard elements will trigger automatic detection, select or clear the associated check box next to the element in the Standard list.

To create a custom element:

1. Click **Add**.
2. In the **Value** box, enter a text string that appears somewhere within the page.
3. Click **OK**.

   The element appears in the Custom list.
4. In the **Type** column, click the down arrow and select the element type: **Confirmation** or **Logout**.

Proxy

If you need to use a proxy server to access the target website:

1. Select **Use Proxy**.
2. Enter the IP address or host name of the server.
3. Enter the server's port number.

Macro Settings

General

Smart Credentials

If you start a scan using a macro that includes Smart Credentials, then when you scan the page containing the input elements associated with these entries, WebInspect Enterprise will substitute the user name and password specified here. This allows you to create the macro using your own user name and password, yet when other persons run the scan using this macro, they can substitute their own user names and passwords.

To enable this feature, you must first record a macro and then associate one SetValue event in the Events grid as a user name and another SetValue event as a password.

Replacement URL

If you select **Enable URL Replacement**, the host name entered as the Start URL in the Scan Wizard will be dynamically inserted into each URL for this macro. For example, suppose you record a macro for www.testsite.com. At a later point in time, www.testsite.com is renamed to www.testsite2.com. Instead of recording an entirely new macro, you could reuse the original one and enable URL replacement.

IE Dialogs

Microsoft's Internet Explorer may sometimes display dialogs that are not related to the actual content of the web page. For example, the browser's security feature may present a modal dialog with the following message: “Do you want to view only the webpage content that was delivered securely?” If this occurs during playback of a macro, the scanner will halt until the user presses **Yes** or **No**. You can avoid this interruption by selecting **Use IE Dialog Suppression**.

Several conditions are defined by default. You may, however, define a condition that meets your specific requirements. To do so:

1. Click **Add**.
2. Enter the requested information.
   - **Dialog Caption:** Enter the text that appears on the title bar of the dialog box.
   - **Dialog Text:** Enter the text that appears as the message content.
   - **Button:** Enter the text that appears on the button that the macro should automatically “press.”

   The utility that performs this check is case-sensitive, so be sure to enter the text string exactly as it appears.
3. Click **OK**.

Web Macro Recorder (Unified)

Introduction

In WebInspect Enterprise, you use the Web Macro Recorder tool to record macros. A macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct the HP scanner to begin a scan using this recording.

The Web Macro Recorder is the only directly accessible macro recording tool provided in WebInspect Enterprise versions 10.00 and later, but it provides (or provides access to) the capabilities of the three web macro recorders of earlier WebInspect Enterprise or Assessment Management Platform (AMP) versions. Based on its versatility, the Web Macro Recorder is also known as the Unified Web Macro Recorder.

The Web Macro Recorder can be launched in several ways—while configuring a Guided Scan or a Web Site Scan, or outside of a scan in what is known as "stand-alone" mode. For more information, see Accessing the Web Macro Recorder on page 267.

Macros that were *recorded* in a Guided Scan or a Web Site Scan can be *used* in either type of scan.

By default, the Web Macro Recorder uses underlying Firefox browser technology to record and play macros. It can also use Internet Explorer browser technology (also referred to here as IE technology) to record and display web traffic data.

Notes:

- The Web Macro Recorder does not support the recording of Flash or Silverlight applications.
- The TruClient technology used in the Web Macro Recorder is an adaptation of the Ajax TruClient technology originally developed for use with HP LoadRunner and HP Performance Center. It does not incorporate or support all the capabilities of the fully-featured version in those products.
- When you play a macro, the HP scanner does not send any cookie headers that may have been incorporated in the recorded macro.
- If a URL is in a macro, the request is always sent when the macro is played, regardless of any exclusion rules in scan settings.
- When launching the Web Macro Recorder, you may receive the following error message:

  "Exc in ev handl: TypeError: this.oRoot.enable is not a function."

  This can occur if the McAfee SiteAdvisor is installed. Simply acknowledge the message and continue.

Login Macros

A login macro is a recording of the activity that is required to access and log in to a website or web application, typically by entering a user name and password and clicking a button such as Log In or Log On. When you configure a Guided Scan or a Web Site Scan, you usually specify a previously recorded login macro or record a new one at the time for the scan to use.

To prevent a scan from terminating prematurely if it gets logged out of your application, a login macro should also specify at least one logout condition that definitively indicates that a logout has occurred. During a scan, the scanner can get logged out for a variety of reasons, including:

- Normal logout driven by the target site
- An error condition in the target site such as a timeout
- An error in the macro itself, such as an invalid parameter

Specifying a logout condition as part of the login macro makes it unnecessary for users to manually log back in, perhaps repeatedly, when unexpected logouts occur during a scan. When scanning a site, the scanner analyzes every target site response to determine the state. If the scanner determines at any time that it is logged out, it runs the login macro to log back in, and then it resumes crawling or auditing the site at the point where the logout occurred.

As the final step in recording a login macro, the Unified Web Macro Recorder uses sophisticated analysis to try to *automatically* detect a logout condition and specify it in the login macro. In most cases you do not have to identify a logout condition manually. However, you can add or edit logout conditions.

You can specify multiple logout conditions, and if any of them are met, WebInspect Enterprise plays the login macro to log the scanner back in and resume the scan where it left off.

Workflow Macros

A workflow macro is a recording of the login steps (as needed) and the specific URLs to which you manually navigate on a site. When you configure a Guided Scan or a Web Site Scan, you specify a previously recorded workflow macro or record a new one at the time for the scan to use. WebInspect Enterprise audits only the URLs that are recorded in the workflow macro and does not take any hyperlinks encountered during the audit. This type of macro is used most often to focus on a particular subsection of an application. In terms of the macro recording process, the essential differences from login macros are that:

- Workflow macros include only the specific URLs to which a user navigated while recording them, and upon replay workflow macros access only those URLs.
- Workflow macros do not require logout conditions, so the macro recorder user interface excludes logout condition functionality when recording workflow macros.

If your website requires authentication, do not record login steps in a workflow macro. Instead, record a separate login macro to log in to your website.

Upgrade Impacts

WebInspect Enterprise versions 10.00 and later include only one directly accessible “Unified” Web Macro Recorder tool. It enhances the functionality of the three web macro recorders that were available in earlier versions, and its enhancements make login macro recording more automatic, more complete, and more successful.

If you have upgraded from an earlier version of WebInspect Enterprise, review the following aspects of the Unified Web Macro Recorder, as compared to the web macro recorders of version 9.30 and earlier:

- The Unified Web Macro Recorder includes and enhances the TruClient Web Macro Recorder functionality of earlier versions of WebInspect Enterprise, and by default it uses this enhanced functionality to record a new macro. The automatic detection of logout conditions has been significantly improved from earlier versions. As a result, usually you should not need to manually identify a logout condition as part of recording a login macro.

  Macros that were recorded using the TruClient Web Macro Recorder in any earlier version of WebInspect Enterprise can be used in a Guided Scan or a Web Site Scan in WebInspect Enterprise version 10.00 or later.

- When using Internet Explorer browser technology (also referred to here as IE technology), the Unified Web Macro Recorder can open macros that were created in the Traffic-Mode Web Macro Recorder of earlier WebInspect Enterprise (or AMP) versions. For more information, see Opening Macros Recorded with the Traffic-Mode Web Macro Recorder on page 266.

Also, if the Web Macro Recorder cannot successfully record a new macro using the default Firefox browser technology, it automatically switches to IE technology to record the macro. IE technology can also be manually selected. For more information, see Internet Explorer Browser Technology on page 277.

- The Unified Web Macro Recorder does not support opening existing macros that were created in the Event-Based IE Compatible Web Macro Recorder tool of earlier versions of WebInspect Enterprise (or AMP). However, in version 10.00 and later you can indirectly access the Event-Based IE Compatible Web Macro Recorder tool to open and edit existing event-based macros and even to create new ones. For more information, see Event-Based IE Compatible Web Macro Recorder (Hidden) on page 252 and Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266. For recording new event-based macros, HP strongly recommends using the default Firefox technology of the Unified Web Macro Recorder.
- Login and workflow macros created in any of the web macro recorders in any version of WebInspect Enterprise have the file extension `.webmacro`. When you open any macro recorded using any of the types of web macro recorder, WebInspect Enterprise uses information in the macro to determine the appropriate type of macro recorder and functionality to use, within the limitations stated above.

Opening Macros Recorded with the Traffic-Mode Web Macro Recorder

Note that all of the information in this section applies to both workflow macros and login macros that were recorded using the formerly separate Traffic-Mode Web Macro Recorder tool used in earlier versions of WebInspect Enterprise (or AMP).

The Traffic-Mode Web Macro Recorder tool is not provided in WebInspect Enterprise versions 10.00 and later. However, the Unified Web Macro Recorder, when using its built-in IE technology, allows you to open, play back, and edit existing traffic-mode macros created in earlier versions, and create new ones. When recording new macros, the Unified Web Macro Recorder first uses event-based functionality based on Firefox technology by default. If that fails for some reason, the Web Macro Recorder automatically switches to using its IE technology as an alternative recording method. This displays web traffic data in the Web Macro Recorder interface.

The **Browser** button in the toolbar at the top of the Web Macro Recorder allows you to see and specify whether the underlying technology used by the Web Macro Recorder is based on Firefox (the recommended option) or Internet Explorer.

When a macro was created using the Traffic-Mode Web Macro Recorder of earlier WebInspect Enterprise versions and you open it in any of the following ways, it opens using IE technology:

- When configuring a Guided Scan
- When configuring a Web Site Scan
- In the WebInspect Enterprise stand-alone Web Macro Recorder (see Accessing the Web Macro Recorder on page 267)
- From Windows Explorer

In all cases you can edit the macro after you open it when the Web Macro Recorder is using IE technology, and you can use the macro in a Guided Scan or a Web Site Scan.

Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder

The Event-Based IE Compatible Web Macro Recorder tool is no longer directly accessible as a separate tool in WebInspect Enterprise version 10.00 or later. However, these versions include a copy of the tool so that you can open existing login macros that were created using the tool in earlier versions of WebInspect Enterprise (or AMP). The capabilities that are available for such an existing login macro depend on how it is accessed, as follows:

- When configuring a Guided Scan, you can select the login macro and use it in the scan, but you cannot edit it.
- When configuring a Web Site Scan, you can select and optionally edit the login macro in the Event-Based IE Compatible Web Macro Recorder, and use it in the scan.
- In the stand-alone Unified Web Macro Recorder (see Accessing the Web Macro Recorder on page 267), when you try to open the login macro, the macro recorder opens a dialog box that asks if you would like to "switch to event mode."
  - If you answer **Yes**, the macro opens in the Event-Based IE Compatible Web Macro Recorder and you can edit it.
  - If you answer **No**, the dialog box closes and the macro does not open.
- You can select and edit the login macro in the Event-Based IE Compatible Web Macro Recorder if you do either of the following:
  - Open the login macro by double-clicking it from Windows Explorer.
  - In the WebInspect Enterprise Scan Wizard, click **Advanced Settings**, click **Method** under SCAN SETTINGS, and select **Use a login macro for forms authentication.**

Once the Event-Based IE Compatible Web Macro Recorder is open, you can create new login macros with it. However, HP strongly recommends that you create new macros using the Unified Web Macro Recorder, which uses Firefox technology by default and IE technology as necessary.

For more information about the Event-Based IE Compatible Web Macro Recorder tool, see Event-Based IE Compatible Web Macro Recorder (Hidden) on page 252.

Accessing the Web Macro Recorder

The Web Macro Recorder can be launched in several ways—while configuring a Guided Scan or a Web Site Scan, or outside of a scan in "stand-alone" mode. For login macros and workflow macros, the following sections describe how you can record a new macro or select (and optionally edit) an existing macro that was recorded in WebInspect Enterprise version 10.00 or later.

Login Macros

You can record a new login macro or select (and optionally edit) an existing login macro that was recorded in WebInspect Enterprise version 10.00 or later in the following ways:

- When configuring a Guided Scan, specify that the target site requires a login macro, and click **Create** to record a new login macro or select (and optionally edit) an existing login macro.
- When configuring a Web Site Scan, in Step 2 select **Site Authentication** and record a new login macro or select (and optionally edit) an existing login macro.
- In the WebInspect Enterprise Scan Wizard, click **Advanced Settings**, click **Method** under SCAN SETTINGS, and select **Use a login macro for forms authentication** (for existing macros only).
- On the Administrative Console toolbar, click **Tools** → **Login Macro Recorder** to open the Web Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- From Windows Explorer, navigate to a particular recorded login macro and double-click it to open it in the Web Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.

Workflow Macros

You can record a new workflow macro or select (and optionally edit) an existing workflow macro that was recorded in WebInspect Enterprise version 10.00 or later in the following ways:

- When configuring a Guided Scan, specify that the **Scan Type** is **Workflows** and later, in the **Workflows** → **1. Manage Workflows** step, record a new workflow macro or import (and optionally edit) an existing workflow macro.
- When configuring a Web Site Scan, in Step 1 select **Workflow-Driven Scan** and click **Import** or **Manage** to select an existing workflow macro.
- On the Administrative Console toolbar, click **Tools** → **Workflow Macro Recorder** to open the Web Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.

Recording or Editing a Macro

This section describes the tasks involved in interactively recording or editing login macros and workflow macros, using the Web Macro Recorder in stand-alone mode or as it is invoked when recording or editing a macro during configuration of a Guided Scan or a Web Site Scan.

HP strongly recommends initially using the default Firefox technology of the Web Macro Recorder to record a macro. However, if it has not worked for you to successfully record a macro, you can try using its IE technology, which displays web traffic data in the Web Macro Recorder interface as you record and play the macro. To record a macro using IE technology, go to Using IE Technology to Record Web Traffic on page 277 and return to this procedure when instructed to do so.

In the Web Macro Recorder, step-by-step guidance is provided near the top of the screen in a yellow instruction bar. Above that, when you begin the specific process to record or edit a macro for a Guided Scan, a Web Site Scan, or stand-alone Web Macro Recorder operation, the following buttons appear in the toolbar in the Macro group, except as noted:

- **New**. Starts creating a new macro.
- **Import** (Guided Scan only). Allows you to select an existing macro to play and edit.
- **Open** (Web Site Scan and stand-alone Web Macro Recorder only). Allows you to select an existing macro to play and edit.
- **Export** (Guided Scan only). Saves the current macro under the same name or a new name.
- **Save** (Web Site Scan and stand-alone Web Macro Recorder only). Saves the current macro under the same name or a new name.
- **Parameters Editor**. See Parameters Editor on page 282. (This option is not available for a macro that uses IE technology in the Web Macro Recorder or for a macro that was recorded using the Traffic-Mode Web Macro Recorder tool from earlier versions of WebInspect Enterprise or AMP.)
- **Logout Conditions**. See Logout Condition Editor on page 276. (This option appears only for login macros, not workflow macros.)
- **Browser Settings** (Web Site Scan and stand-alone Web Macro Recorder only). See Browser Settings on page 281.
- **Browser: Firefox** or **Browser: IE**. See Internet Explorer Browser Technology on page 277.

At the bottom of the screen for a Guided Scan, you can click the **Recorded Locations** button to expand (or later contract) the list of locations, which has the following columns:

- **Run**. Steps that are selected (checked) are played when you click **Play All**. All steps are stored in the macro when you save it, but only the selected steps are run whenever the macro is played.

- **Excluded**. Select **Url, Directory,** or **Page** to add that type of exclusion rule. The exclusion rule will apply to any requests made by a scan that uses this scan configuration. This column also displays, read only, the causes of any existing exclusions for requests—Custom, Disallowed Host, or, if **Restrict to folder** was selected at the start of configuring the scan, Outside Root.
- **Method**. The method of the request, for example, GET or POST.
- **Status**. The status code of the response to the request, for example, 302 or 200.
- **URL**. The URL of the request.

Task 1: Record or edit the macro

If your website requires authentication, do not record login steps in a workflow macro. Instead, record a separate login macro to log in to your website.

1 Select one of the following procedures, based on the activity you want to perform, and follow the on-screen guidance:

- **Use the Web Macro Recorder in stand-alone mode to record a login macro.**

  If you want to use the Web Macro Recorder in stand-alone mode (not in conjunction with running a scan) in order to record or edit a login macro, on the WebInspect Enterprise toolbar click **Tools** → **Login Macro Recorder** and proceed to step 2 on page 271 (*not* Task 2).

- **Use the Web Macro Recorder in stand-alone mode to record a workflow macro.**

  If you want to use the Web Macro Recorder in stand-alone mode (not in conjunction with running a scan) in order to record or edit a workflow macro, on the WebInspect Enterprise toolbar click **Tools** → **Workflow Macro Recorder** and proceed to step 2 on page 271 (*not* Task 2).

- **Use a login macro in a Guided Scan.**

  If you are completing the **Application Authentication** → **1. Select Login Macro** step of a Guided Scan, select the **Use a login macro for this site** option, and click **Create** to record a new login macro, or click the browse (...) button to navigate to, select, and optionally edit an existing login macro to use in the scan. To clear a previously selected macro from the text box, click the **X** at the right end in the text box. (You cannot edit a macro recorded using the Event-Based IE Compatible Web Macro Recorder tool from earlier versions of WebInspect. For more information, see Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266.)

  If a particular login macro uses parameters, a table of Macro Parameters is displayed when that login macro is selected. Edit the values of the parameters as needed.

  Proceed as follows:

  — If you are recording or editing a login macro, proceed to step 2 on page 271 (*not* Task 2).

  — If you need to select an existing login macro, not record or edit a macro, after selecting a macro, click the **Next** button in the Guided Scan pane and continue configuring the scan.

- **Use workflow macros in a Guided Scan.**

  If you are completing the **Start Parameters** → **2. Choose Scan Type** step of a Guided Scan, select the **Workflows** option in the Scan Type section. Later in the Guided Scan, in the **Workflows** → **1. Manage Workflows** step, workflow macro information is displayed in the right pane.

  Click **Record** to record a new workflow macro or click **Import** to add an existing workflow macro to the list. When a macro in the list is selected, click **Edit** to edit it, **Delete** to remove it from the list, or **Export** to save it with a name and location you specify. (You cannot edit a macro recorded using the Event-Based IE Compatible Web Macro Recorder tool from earlier versions of WebInspect. For more information, see Opening Macros Recorded with the Event-Based IE Compatible Web Macro Recorder on page 266.)

When the first workflow macro is added to the list, its name (or default name) appears in the Workflows table and an Allowed Hosts table is added to the pane. Adding another workflow macro can add more allowed hosts. Any host that is enabled is available to all the listed workflow macros, not just the workflow macro for which it was added. The Guided Scan will play all the listed workflow macros and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, WebInspect will crawl or audit the responses from that host. If a check box is not selected, WebInspect will not crawl or audit the responses from that host.

In addition, if a particular workflow macro uses parameters, a Macro Parameters table is displayed when that workflow macro is selected in the list. Edit the values of the parameters as needed.

Proceed as follows:

— If you are recording or editing a workflow macro, proceed to step 2 on page 271 (*not* Task 2).

— If you need to select one or more existing workflow macros, not record or edit any macros, after adding the macros to the Workflows table, click the **Next** button in the Guided Scan pane and continue configuring the scan.

- **Use a login macro in a Web Site Scan.**

  If you are completing Step 2 of a Web Site Scan and you select the **Site Authentication** option to use a login macro, click **Record** to record a new login macro or click the browse (...) button to navigate to, select, and optionally edit an existing login macro to use in the scan.

  If a particular login macro uses parameters, a table of those parameters is displayed when that login macro is selected. Edit the values of the parameters as needed.

  Proceed as follows:

  — If you are recording or editing a login macro, proceed to step 2 on page 271 (*not* Task 2).

  — If you need to select an existing login macro, not record or edit a macro, after selecting a macro complete Step 2 of the Web Site Scan and continue configuring the scan.

- **Use workflow macros in a Web Site Scan.**

  Note: Parameters are not supported for workflow macros created or used in a Web Site Scan. If you need to use parameters for your workflow macro, use Guided Scan.

  If you are completing Step 1 of a Web Site Scan and you select the **Workflow-Driven Scan** option to use a workflow macro, click **Record** to record a new workflow macro or click **Manage** to navigate to, select, and optionally edit an existing workflow macro to use in the scan.

  If you click **Manage**, or after you record and save a new workflow macro, the *Select Workflow-Driven Scan Macros* dialog box appears. It displays workflow macro information for a list of workflow macros you select. Click **Import** to add an existing workflow macro to the list. (You can also click **Record** here to record a new workflow macro.) When a macro in the list is selected, click **Edit** to edit it, **Remove** to remove it from the list, or **Export** to save it with a name and location you specify.

  When the first workflow macro is added, its name (or default name) appears in the Macros table in the dialog box and a specific entry is added to the Allowed Hosts list. Adding another workflow macro can add more allowed hosts. Any host that is enabled is available to all the listed workflow macros, not just the workflow macro for which it was added. The Web Site Scan will play all the listed workflow macros and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, WebInspect Enterprise will crawl or audit the responses from that host. If a check box is not selected, WebInspect Enterprise will not crawl or audit the responses from that host.

  Proceed as follows:

  — If you are recording or editing a workflow macro, proceed to step 2 (*not* Task 2).

— If you need to select one or more existing workflow macros, not record or edit any macros, after adding the macros to the Macros table complete Step 1 of the Web Site Scan and continue configuring the scan.

2 Follow the guidance in the yellow instruction bar to record or edit the macro. All of your actions will be recorded and displayed in the macro steps pane on the right. You can stop recording at any time.

The instructions differ somewhat between login macros and workflow macros. For example, in workflow macros, you choose where to navigate through the target site, and the URLs are recorded as you navigate, so that you can later replay them by running the macro. Also, workflow macros do not include any logout conditions.

If the website requires users to answer a variable set of questions in order to complete the login process, go to Recording a Macro for a Site with Multiple, Variable Login Questions on page 273 at the appropriate time to create the macro steps required for this case, and then return to Task 2 on page 271.

When you are instructed to play the macro, go to Task 2 on page 271.

Note: In a Guided Scan, if you record or edit a workflow macro for a site that already has a login macro that you specify (in **Application Authentication → 1. Select Login Macro**), for your convenience the login macro automatically plays before you begin recording the workflow macro to ensure that the site is accessible and to obtain and record state information from the site that the workflow macro uses whenever it is played.

Task 2: Play the macro

Play the macro, correcting any errors that occur during the process:

1 When you are instructed to do so, click the **Play** button in the instruction bar.

The macro steps are highlighted as playback progresses. If the macro detects no errors (while using Firefox technology), "Replay succeeded" is displayed at the bottom of the right pane.

If the macro had errors, see Debugging Macros on page 286.

2 Answer the question "Did the macro play correctly?" In other words, indicate whether the login macro successfully logged in to the target site or the workflow macro accessed all the recorded URLs. Successful replay of the macro in step 1 does not guarantee that the macro did what you intended.

If you click **Yes:**

- If you are recording a *login* macro, the macro recorder attempts to automatically detect a logout condition. Proceed to Task 3 on page 272.
- If you are recording a *workflow* macro, go to Task 5 on page 273. Workflows macros do not include logout conditions, so you are skipping tasks associated with logout conditions.

If you click **No**:

- If this is the *first* time you click **No**, the macro recorder automatically:
  - — Adjusts the Script Level slider to level 3 to display and play back *all* of the macro steps. For more information, see Modify Script Levels on page 286.
  - — Plays the macro again.
  - — Asks you again whether the macro succeeded.

  Return to the beginning of this step (step 2 on page 271).
- If this is the *second* time you click **No**, the macro recorder automatically switches to IE technology (as if you started recording the macro by selecting the IE option for the **Browser** button). A new pane for locations appears at the bottom of the Web Macro Recorder interface, rather than a pane for macro steps on the right. You can adjust the height of the locations pane relative to the top

(target site) pane. In a Guided Scan you can also expand and collapse the locations pane by clicking **Recorded Locations** below the pane. Go to Using IE Technology to Record Web Traffic on page 277.

Task 3: Identify a "logout" condition if automatic detection by the macro recorder fails

Note: For workflow macros, skip to Task 5 on page 273. Workflow macros do not have logout conditions.

At this point the target site is at a protected page, that is, a page that can be accessed only when a user is logged in.

To automatically resume a scan that gets logged out, a login macro needs to include at least one condition that represents getting logged out. Then when WebInspect Enterprise recognizes any of the logout conditions, it will automatically restart the macro to log back in and resume the scan where it left off.

After the macro plays back successfully, the Web Macro Recorder uses sophisticated analysis to try to automatically detect a logout condition. At that time, it displays "Detecting Logout Condition..." in the instruction bar. If the Web Macro Recorder succeeds in detecting a logout condition, the login macro is complete, as stated in the instruction bar, and you can proceed to Task 4 on page 273.

You can view the automatically detected logout condition and add other logout conditions by clicking **Logout Conditions** in the toolbar to open the Logout Condition Editor.

If the automatically detected logout condition is identified as the "Auto Redirect" type in the Logout Condition Editor, the Web Macro Recorder generated the displayed regular expression (regex), including the 'Location' header of a redirect (302), to represent the logout condition for the redirect when login state was lost.

If navigation parameters are specified in the scan settings, they are used as applicable at scan time to revise and uniquely identify the URL in the 'Location' header in the regex for the redirect. For information about navigation parameters, see HTTP Parsing on page 177.

If you later determine that the Auto Redirect regex does not work as well as necessary to automatically log back in to the site being scanned, you cannot edit the regex in place, but you can copy it, manually create a new Regex condition that you revise from the copy, and optionally delete the Auto Redirect regex. For more information, see Logout Condition Editor on page 276.

If the automatically detected logout condition is identified as the "Automatic" type in the Logout Condition Editor, the Web Macro Recorder detected a non-302 response, such as a 200.

If you later determine that the Automatic logout condition does not work as well as necessary to automatically log back in to the site being scanned, you can replace it by manually specifying a regular expression (Regex), an object (interface element), or a URL as a logout condition. For more information, see Logout Condition Editor on page 276.

If the Web Macro Recorder fails to detect a logout condition when you record a login macro, it presents an error message and offers to open the Logout Condition Editor, which is the same as clicking **Logout Conditions** in the toolbar. In the Logout Condition Editor, you can manually specify, in recommended order, a regular expression (Regex), an object (interface element), or a URL as a logout condition.

To specify a logout condition if the Web Macro Recorder could not detect one:

1. In the macro, navigate in the target site to a page that users consistently see when they get logged out.
2. Use the Logout Condition Editor to specify a logout condition that is unique to this page. See Logout Condition Editor on page 276.

Task 4: (Optional) Modify the logout conditions

If you have been recording a login macro, this task is optional. It does not apply to workflow macros.

To examine or modify the logout condition, click **Logout Conditions** in the toolbar. You can specify as many different logout conditions as you need, and if any of them is met during a scan, WebInspect Enterprise invokes the login macro to log back in. For more information, see Logout Condition Editor on page 276.

Task 5: (Optional) Parameterize the macro

This task is optional. To parameterize the login credentials or the URL, click **Parameters Editor** in the toolbar. For more information, see Parameters Editor on page 282.

Task 6: (Optional) Save the macro

To save the macro for future use, click **Export** in the toolbar for a Guided Scan, or click **Save** (and then **Save** or **Save As**) in the toolbar for a Web Site Scan. This completes the macro recording procedure.

If you are configuring a Guided Scan or a Web Site Scan, close the Web Macro Recorder to return to the configuration process.

Recording a Macro for a Site with Multiple, Variable Login Questions

Challenge-response authentication is a family of protocols in which the server presents a question (the challenge) and the client must provide a valid answer (the response). In the simplest example, the challenge asks for a password and the valid response is the correct password.

Many websites now present multiple challenges to the user. Typically, when a user first registers with a website, the site presents a list of questions to which the user provides answers that will be used for subsequent authentication. For example:

- What is your favorite color?
- What was the name of your first pet?
- In what town or city were your born?
- What was the make of your first automobile?

When the user later attempts to log in, the website presents two or more of these challenges.

Some sites also create groups of challenges, and present different questions from the groups on each new login attempt, as demonstrated in the following example.

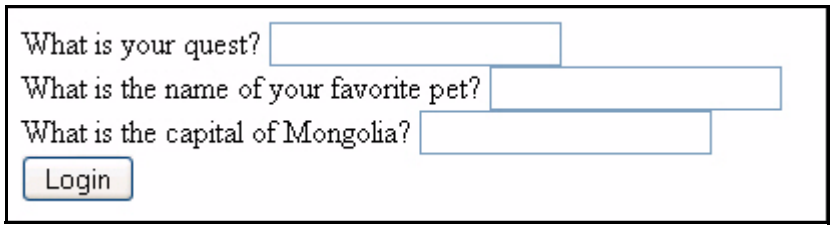
When registering for the following example website, the user is asked to provide answers to nine questions, which are arranged into three groups of three questions each, as follows:

Group 1
Q: What is your quest? A: happiness
Q: What is your name? A: Smith
Q: What is your favorite color? A: blue

Group 2
Q: What is the name of your favorite pet? A: Rusty
Q: What is your mother's maiden name? A: Jones
Q: In what state were you born? A: Delaware

Group 3
Q: What is the capital of Mongolia? A: Ulaanbaatar
Q: What is the name of a sea bird? A: Albatross
Q: What is your paternal grandmother's first name? A: Esther

The login page might look like this (using the first question from each group):



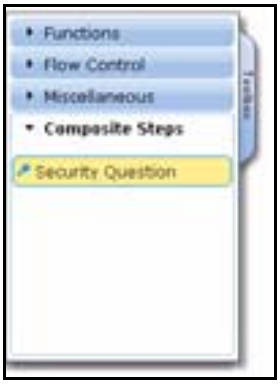
When recording a macro for a challenge/response type of login, you must know all possible question-and-answer combinations, even if only a subset of those combinations might be presented during any one login. You enter these combinations manually, as special steps while recording a macro.

At the point where the target site asks the challenge questions, usually after logging in with username and password credentials, use the following procedure to manually create the required steps for this hypothetical set of nine questions:

1 If you are recording a macro, click **Stop** on the instruction bar to stop the automatic macro recording process.

2 Click the **Toolbox** vertical tab on the left side of the macro steps pane.

3 Click (expand) **Composite Steps**.



4 Click and drag the **Security Question** element to the right pane to create the next macro step.

5 Click the first “Click to choose an object” button in the new step and then, in the target site pane, click the object representing the first question (usually a label).

6 Click the second “Click to choose an object” button in the new step and then, in the target site pane, click the object representing the answer (usually a text box).

7 In the right pane, place your mouse in the upper right corner of the step and click to open the Step Editor.

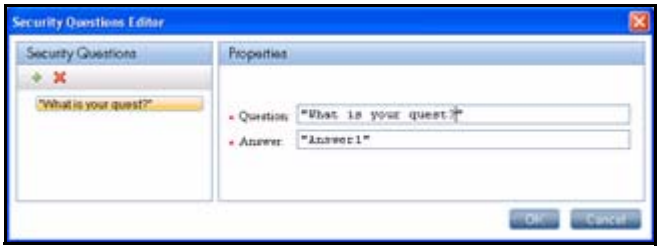
8 Click (expand) **Arguments**.

9 Click  to the right of the expanded arguments to open the Security Questions Editor.

10 In the Security Questions pane of the Security Questions Editor, click  to add a new question.

A new question appears with the default name “Question1.” Its properties include the text box labelled **Question** (also shown with a default value of “Question1”) and the text box labelled **Answer**, with a default value of “Answer1.”

11 In the **Question** text box, type over the default text with the actual question exactly as it appears on the login page, including capitalization and punctuation. Be sure to enclose the text in quotation marks as shown below. The question in the left pane is simultaneously updated.



12 In the **Answer** text box, type the correct response in quotes.

13 Click **OK**.

The **Question** and **Answer** are added to a table below the **Arguments** heading in the macro step. (If you later need to edit an argument, reopen the Security Questions Editor.)

14 Repeat step 9 through step 13 to add the information for the second question that might appear in the same location on the web page (in this example, "What is the name of your favorite pet?").

15 Repeat step 9 through step 13 to add the information for the third question that might appear in the same location on the web page (in this example, "What is the capital of Mongolia?").

This completes the macro step for this particular location on the web page.

16 Refresh the web page until the second set of questions appears. Click in the target site pane and press F5 (or right-click and click **Reload**).

17 Repeat step 2 through step 15 to add another macro step for the second set of three questions and answers at the second location on the web page.

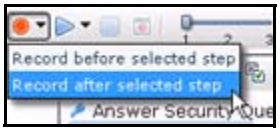
18 Refresh the web page until the third set of questions appears. Click in the target site pane and press F5 (or right-click and click **Reload**).

19 Repeat step 2 through step 15 to add another macro step for the third set of three questions and answers at the third location on the web page.

20 After creating macro steps for all possible question-and-answer combinations, if you need to record further macro steps:

a Select the last step you created.

b Click the drop-down arrow on the **Record** button in the macro steps pane and select **Record after selected step**.



c Add any further steps to the macro as needed.

d Click **Stop** on the instruction bar.

21 To play back the macro, return to Task 2 on page 271 or, if you are using IE technology, return to Task 2 on page 279.

On playback, if the macro cannot find a particular question object or answer object on the page, you can expand **Question Object** or **Answer Object** in the Step Editor for the security question and use the **Highlight** and **Replace** buttons to try to correct the failure. See Highlight an object on page 289 and Replace an object on page 291.

Logout Condition Editor

The Logout Condition Editor allows you to create or edit logout conditions for login macros. For introductory information, see Login Macros on page 264. You can specify as many different logout conditions as you need, and if any of them is met, WebInspect Enterprise invokes the login macro to log back in and resume a scan where it left off. The final set of all logout conditions should cover all the cases of WebInspect Enterprise getting logged out during a scan of the target site.

When the Web Macro Recorder successfully detects a logout condition automatically, it categorizes the logout condition as one of the following types:

- **Auto Redirect**. This type of logout condition is created when the Web Macro Recorder detects that the target site responds with a 302 redirect. It takes the form of a regular expression (regex).
- **Automatic**. This type of logout condition is created when the Web Macro Recorder detects that the target site responds with anything other than a 302 redirect, for example, with a 200.

To add a new logout condition:

1. Click the **Logout Conditions** button in the toolbar.
2. Click  in the left pane (or click the drop-down arrow to the right of  and select **Manual**).
3. In the right pane specify the name of the new condition. (Notice that the name in the left column is simultaneously updated with your changes.)
4. Select which type of logout condition you want to use and complete the information required for that type. In order of recommended priority, the options are:
   - **Regex**. With this option, you will construct a regular expression (regex). A regular expression is a pattern that describes a set of strings. Regular expressions are constructed much like mathematical expressions by using various operators to combine smaller expressions. Only users with a working knowledge of regular expressions should use this feature.

     The regex must reflect the difference between a) the response to a logged-in user's request to access a protected page, and b) the response to the same request from the user, while *not* logged in, to access the same protected page. The general steps to construct the regex are as follows:

     — Start the Web Proxy tool to record web traffic. See Web Proxy on page 219.

     — Log in to the target site legitimately and copy the URL of a protected page.

     — Log out and use the copied URL to try to access the protected page without logging in.

     — Compare the responses and identify a unique aspect of the response to the attempt to access the protected page without logging in.

     — Open the Regular Expression Editor from the WebInspect Enterprise menu **Tools** → **Regex Editor**. See Regular Expression Editor on page 207.

     — Construct a regex that reflects the unique aspect of the response to the attempt to access the protected page without logging in.

     — Copy the regex into the **Regex** field of the Logout Condition Editor.
   - **Object**. After you select this option, click **Click to choose an object**, navigate to a page where the user is logged out and can log back in, and move your mouse over objects on the page until you find one that does not appear on any other page and that indicates that the user is logged out. As you mouse over objects, each one is highlighted in green until you select one or press Esc to stop the selection process. Once you select an object, if you click **Highlight** the Logout Condition Editor is hidden temporarily and the selected object is highlighted by a rapidly flashing red outline.

- **URL**. When you select this option, the currently displayed web page is automatically used as the default value. You can specify a static URL to which the target site redirects users when it logs them out. Do not specify the target site's general login page.

In the Logout Condition Editor, if you click the drop-down arrow to the right of  , and if the **Automatic** option is available and you select it, the Logout Condition Editor closes and the Web Macro Recorder attempts to automatically detect a logout condition.

To delete a logout condition, select it in the left pane and click the red **X**.

Internet Explorer Browser Technology

By default, the Unified Web Macro Recorder tries to create a macro using Firefox technology. However, if it cannot successfully create the macro, it automatically tries again using its Internet Explorer browser technology (also referred to here as IE technology), which displays locations and web traffic data in the Web Macro Recorder interface. For more information, see the procedure for recording a macro (Recording or Editing a Macro on page 268).

In the Unified Web Macro Recorder, you can also manually initiate the use of IE technology as you begin recording a new macro, in case the default Firefox technology of the Web Macro Recorder has not worked. HP strongly recommends that you start by trying the default Firefox technology.

The consequences of selecting IE technology (**Browser: IE**) depend upon the circumstances.

- When recording a macro, selecting IE technology:
  - Switches the macro recorder from the use of custom Firefox technology to Internet Explorer browser control.
  - Records the macro in traffic mode.
- In a Guided Scan, at the **Start Parameters** → **1. Verify Web Site** step or at the **Optimization Tasks** → **Enhance coverage of your web site** step, selecting IE technology implies that using Firefox technology would not work for any aspect of the site, so it:
  - Switches the macro recorder from the use of custom Firefox technology to Internet Explorer browser control.
  - Changes the default script execution engine from the one introduced in WebInspect Enterprise version 10.00 to an engine from earlier WebInspect versions that is compatible with Internet Explorer.
  - Uses Internet Explorer as the default browser for subsequent steps in the scan such as recording a macro or discovering locations in **Active Learning**.

As you record a macro against a target site using IE technology, the Web Macro Recorder displays requested locations (as described in detail in subsequent sections). When you play a macro, the Web Macro Recorder also displays HTTP web traffic for both the requests and their associated responses, but the recorded macro includes only the requests.

For information about compatibility between IE technology in the Unified Web Macro Recorder tool of WebInspect Enterprise version 10.00 or later and macros that were recorded in earlier WebInspect Enterprise or AMP versions using the Traffic-Mode Web Macro Recorder, see Opening Macros Recorded with the Traffic-Mode Web Macro Recorder on page 266.

Using IE Technology to Record Web Traffic

HP strongly recommends initially using the default Firefox technology of the Web Macro Recorder to record a macro. However, the Web Macro Recorder can invoke IE technology automatically if Firefox technology fails or, if you have not been able to successfully record a macro with the Firefox technology, you can

manually invoke IE technology. Using IE technology, the bottom pane of the Web Macro Recorder interface displays requested locations. The actions you take to record and test the macro, guided by the yellow instruction bar at the top of the screen, are essentially the same as for recording a macro using Firefox technology, but the user interface is different, as described in this section.

Proceed as follows, depending on how you are accessing IE technology:

- Proceed to Task 1 on page 278 to record the macro if one of the following applies:
  - You need to *initiate* the use of IE technology when you are just starting to use the stand-alone Web Macro Recorder or just starting to configure a Guided Scan or a Web Site Scan.
  - You need to edit a traffic-mode macro that was recorded in an earlier version of WebInspect Enterprise or AMP.
- Go to Task 2 on page 279 if playback failed twice using Firefox technology and the macro recorder *automatically* invoked IE technology.

Task 1: Record the macro using IE technology

1. Select **Browser: IE** in the Macro section of the Web Macro Recorder toolbar, the Guided Scan toolbar, or the Web Site Scan toolbar, as applicable.

   A new pane for locations appears at the bottom of the Web Macro Recorder interface, rather than a pane for macro steps on the right. You can adjust the height of the locations pane relative to the top (target site) pane. In a Guided Scan you can also expand and collapse the locations pane by clicking **Recorded Locations** below the pane.

   The buttons, check box, and columns in the locations pane are described in step 2.

2. Follow the guidance in the yellow instruction bar to record the macro.

   The instructions differ somewhat between login macros and workflow macros. For example, in workflow macros, you choose where to navigate through the target site, and the URLs are recorded as you navigate, so that you can later replay them by running the macro. Also, workflow macros do not include any logout conditions.

   Note: IE technology does not support websites that require users to answer a variable set of questions in order to log in.

   The following descriptions are provided for information and to assist with debugging. When the on-screen instructions tell you to play the macro, you can proceed to Task 2 on page 279.

   From the first time you navigate to a URL, a table of request data is added to the locations pane. The locations pane has a button bar with the following buttons and check box, which become available as described:

   - **Play Highlighted** button. Available after you highlight a single request (row) by clicking it. Plays the highlighted request if the associated check box in the Run column is selected. Other check boxes in the Run column do not matter.

     The first time you select a request, the locations pane splits into left and right panes. The left pane continues to display the table of request data for each location. In the right pane, the default Details tab is split, with HTTP request data above the associated response data.

   - **Play All** button. Available after you click **Stop** in the instruction bar to stop recording the login steps. Plays only the requests that are selected (checked) in the Run column.

     Note: All steps are stored in the macro when you save it, but only the selected steps are run whenever the macro is played.

   - **Stop** button. Available during playback after you have clicked the **Play All** button. Aborts playback upon completion of the current request.

- **Logout** button. (Does not appear for workflow macros.) Available after you click **Stop** in the instruction bar to stop recording the login steps. Logs you out of the site so that you can determine how the site responds to a subsequent request you play when logged out.
- **Delete Highlighted** button. Available immediately. Deletes the single request (row) you highlighted by clicking it.
- **Delete All** button. Available after you click **Stop** in the instruction bar to stop recording the login steps. Deletes all the requests, regardless of whether they are selected in the Run column.
- **Prompt for login (CAPTCHA)** check box. (Does not appear for workflow macros.) Available immediately. CAPTCHA is a challenge-and-response test designed to ensure that a login response is provided by a person, not generated by a computer. If your target site uses CAPTCHA, select this check box. The macro still detects a logout condition, but WebInspect Enterprise users will need to log in manually at the beginning of a scan and whenever a logout occurs. Selecting this option disables selection of any of the listed requests and closes the right pane that displays HTTP traffic.

Below the button bar, the locations pane lists locations and has the following columns:

- **Run**. Steps that are selected (checked) are played when you click **Play All**. All steps are stored in the macro when you save it, but only the selected steps are run whenever the macro is played.
- **Excluded**. Select **Url, Directory,** or **Page** to add that type of exclusion rule. The exclusion rule will apply to any requests made by a scan that uses this scan configuration. This column also displays, read only, the causes of any existing exclusions for requests—Custom, Disallowed Host, or, if **Restrict to folder** was selected at the start of configuring the scan, Outside Root.
- **Method**. The method of the request, for example, GET or POST.
- **Status**. The status code of the response to the request, for example, 302 or 200.
- **URL**. The URL of the request.

The bottom right pane includes the following tabs:

- **Details** tab. For the selected (highlighted) request in the left pane, shows request data in the top right pane and associated response data in the bottom right pane.
- **State** tab. A collection of all the items that represent state or could represent state, that have been seen across all the locations that the macro has accessed. You can select them in any combination to characterize them as representing a state and you can manually add various types of items. Web applications can require that certain parameters be marked as "stateful."
- **Parameters** tab. (Does not appear for workflow macros.) For login macros, allows you to designate form input fields as being user name or password input so that the macro using IE technology can have user name and password parameters that can be specified at scan time, like macros that use Firefox technology.

Task 2: Play the macro using IE technology

Using IE technology, a pane for locations appears at the bottom of the Web Macro Recorder interface, rather than a pane for macro steps on the right. You can adjust the height of the locations pane relative to the top (target site) pane. In Guided Scan you can also expand and collapse the locations pane by clicking **Recorded Locations** at the bottom of the pane.

1 If the macro has not already been played automatically, click the **Play** button in the instruction bar.

The following descriptions are provided for information and to assist with debugging. You can proceed to step 2 on page 281.

The locations pane has a button bar. Below it, the left pane displays a table of data for each location. In the right pane, the default Details tab is split, with HTTP request data above the associated response data for the request selected in the left pane.

The button bar has the following buttons and check box:

- **Play Highlighted** button. Plays the single request (row) you highlighted by clicking it. Plays the highlighted request if the associated check box in the Run column is selected. Other check boxes in the Run column do not matter.
- **Play All** button. Plays only the requests that are selected (checked) in the Run column.

  Note: All steps are stored in the macro when you save it, but only the selected steps are run whenever the macro is played.
- **Stop** button. Available during playback after you have clicked the **Play All** button. Aborts playback upon completion of the current request.
- **Logout** button. (Does not appear for workflow macros.) Logs you out of the site so that you can determine how the site responds to a subsequent request you play when logged out.
- **Delete Highlighted** button. Deletes the single request (row) you highlighted by clicking it.
- **Delete All** button. Deletes all the requests, regardless of whether they are selected in the Run column.
- **Prompt for login (CAPTCHA)** check box.(Does not appear for workflow macros.) CAPTCHA is a challenge-and-response test designed to ensure that a login response is provided by a person, not generated by a computer. If your target site uses CAPTCHA, select this check box. The macro still detects a logout condition, but WebInspect Enterprise users will need to log in manually at the beginning of a scan and whenever a logout occurs. Selecting this option disables selection of any of the listed requests and closes the right pane that displays HTTP traffic.

The left pane lists locations and has the following columns:

- **Run**. Steps that are selected (checked) are played when you click **Play All**. All steps are stored in the macro when you save it but only the selected steps are run whenever the macro is played.
- **Excluded**. Select **Url, Directory,** or **Page** to add that type of exclusion rule. The exclusion rule will apply to any requests made by a scan that uses this scan configuration. This column also displays, read only, the causes of any existing exclusions for requests—Custom, Disallowed Host, or, if **Restrict to folder** was selected at the start of configuring the scan, Outside Root.
- **Status**. The status code of the response to the request, for example, 302 or 200.
- **Protected**. (Does not appear for workflow macros.) For login macros, a set of options with one selection allowed. The default is the request to the page that the Web Macro Recorder has identified as the most likely to be the protected page. This is also the page from which the Web Macro Recorder attempts to automatically determine a logout condition.
- **URL**. The URL of the request.

The bottom right pane includes the following tabs:

- **Details** tab. For the selected (highlighted) request in the left pane, shows request data in the top right pane and associated response data in the bottom right pane.
- **State** tab. A collection of all the items that represent state or could represent state, that have been seen across all the locations that the macro has accessed. You can select them in any combination to characterize them as representing a state and you can manually add various types of items. Web applications can require that certain parameters be marked as “stateful.”
- **Parameters** tab. (Does not appear for workflow macros.) For login macros, allows you to designate form input fields as being user name or password input so that the macro using IE technology can have user name and password parameters that can be specified at scan time, like macros that use Firefox technology.

If the macro itself detects an inconsistency between an expected status code for a response as determined during macro recording and the actual status code during macro playback, the macro highlights the difference between expected and actual status in the bottom left pane. Investigate and address this condition.

2 Answer the question "Did the macro play correctly?" In other words, indicate whether the login macro successfully logged in to the target site or the workflow macro accessed all the recorded URLs. Successful replay of the macro in step 1 does not guarantee that the macro did what you intended.

If you click **Yes:**

- If you are recording a *login* macro, the macro recorder attempts to automatically detect a logout condition. Return to Task 3 on page 272 and from that task on, perform the same procedures as you would for the Web Macro Recorder using its default Firefox technology.
- If you are recording a *workflow* macro, return to Task 5 on page 273 and from that task on, perform the same procedures as you would for the Web Macro Recorder using its default Firefox technology. Workflows macros do not include logout conditions, so you are skipping tasks associated with logout conditions.

If you click **No**, the instructions advise you to create a new macro or use the Help. For example, see Debugging Macros on page 286 and Resolving Object Identification Issues on page 288.

Browser Settings

When using the Web Macro Recorder in stand-alone mode, click the **Browser Settings** button in the toolbar to display the **Proxy Settings** and **Network Authentication** tabs, described in the following sections. For a Guided Scan or a Web Site Scan, proxy settings and network authentication are configured as part of the scan.

Browser settings are not saved in macros.

Proxy Settings Tab

Select one of the following options:

- **Direct Connection (proxy disabled)**. Select this option if you are not using a proxy server.
- **Auto detect proxy settings**. Select this option to use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's web proxy settings.
- **Use Internet Explorer proxy settings**. Select this option to import the proxy server information from Internet Explorer.
- **Use Firefox proxy settings**. Select this option to import the proxy server information from Firefox.
- **Configure proxy settings using a PAC file**. Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the URL box.
- **Explicitly configure proxy settings**. Select this option to configure a proxy by entering the requested information.
  - **Server**: Enter the URL or IP address of your proxy server.
  - **Port**: Enter the port number (for example, 8080).
  - **Type**: Select a protocol for handling TCP traffic through a proxy server—Standard, SOCKS4, or SOCKS5.
  - **Authentication**: Select an authentication method. See Authentication on page 103 for a description of the available authentication methods.

— **User Name**: Specify a user name.

— **Password**: Specify a password.

— **Bypass Proxy for**: If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), select this option and enter the addresses or URLs in the box. Use commas to separate entries.

Network Authentication Tab

If network authentication is required:

1 Click **Network Authentication**.

2 Select one of the methods. See Authentication on page 103 for a description of the available authentication methods.

3 Specify a **User Name** and **Password** for network authentication.

Select or clear the **Client Certificate** check box. If selected, complete the Certificate Store fields and select a certificate.

Parameters Editor

When recording a macro, you can use the Parameters Editor for two different purposes:

- Creating parameters for the user name and password to allow testers to use their own authentication credentials when starting a scan. For procedures, see Using Name and Password Parameters on page 282.
- Creating a parameter for the URL to allow testers to designate an alternate URL when the macro runs. For example, suppose you record a macro for www.testsite.com. At a later point in time, you rename the site to www.testsite2.com. If you parameterize the URL when you record the macro, you do not need to record a new macro. You simply enter a new host name as the Start URL when you run a scan. For procedures, see Using a URL Parameter on page 284.

When the macro is played during a Guided Scan or a Web Site Scan, it asks the user to specify values for the parameters.

Using Name and Password Parameters

Task 1: Create Parameters

1 After recording and testing your macro, click **Parameters Editor** in the toolbar.

The Parameters Editor opens.

2 Click  to add a parameter.

3 In the **Name** text box, enter a name for the parameter (for example: **Username**).

4 In the **Value** text box, enter the default text (for example: **Enter user name**) that you want testers to see as the value for the parameter as they configure a scan. However, while you are developing the macro, for macro playback to succeed you will probably need to enter your own valid user name and change it to the default text after you verify the macro near the end of this procedure.

5 Click  to add a second parameter.

6 In the **Name** text box, enter a name for the parameter (for example: **Password**).

7 In the **Value** text box, enter the default text (for example: **Enter password here**) that you want testers to see as the value for the parameter as they configure a scan. However, while you are developing the macro, for macro playback to succeed you will probably need to enter your own valid password and change it to the default text after you verify the macro near the end of this procedure.

8 Select **Encrypted** if the Value should be encrypted before transmission to the web server.

9 Click **Close** to close the Parameters Editor.

Task 2: Assign Parameters to Steps

1 Select the macro step that contains the user name.

2 Place your mouse in the upper right corner of the step and click to open the Step Editor.

3 Click (expand) **Arguments**.

4 Highlight the entire contents of the **Value** text box, right-click the highlighted text, and select **Replace with a Parameter**.

5 On the *Enter Parameter Name* dialog, select the parameter (**Username** in this example) from the **Select Parameter** list and click **OK**.

The **Value** takes on the format of a parameter.

6 Select the macro step that contains the password.

7 Place your mouse in the upper right corner of the step and click to open the Step Editor.

8 Click (expand) **Arguments**.

9 Highlight the entire contents of the **Value** text box, right-click the highlighted text, and select **Replace with a Parameter**.

10 On the *Enter Parameter Name* dialog, select the parameter (**Password** in this example) from the **Select Parameter** list and click **OK**.

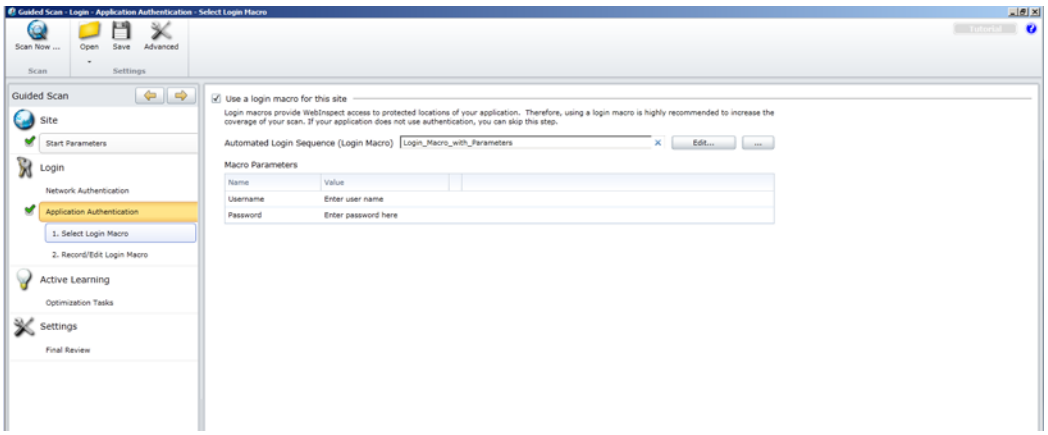
The **Value** takes on the format of a parameter.

11 Play the macro to verify that it logs in correctly.

12 If necessary, reopen the Parameters Editor and change the text in the **Value** text boxes to the default text that you want testers to see, as described in step 4 and step 7 under Task 1 on page 282.

13 Save the macro. (For a Guided Scan, click **Export**. For a Web Site Scan, click **Save**.)

When you start a Guided Scan or a Web Site Scan and select this macro, the parameters appear in the Macro Parameters table for a Guided Scan as shown below, or in the table below the name of the selected login macro in step 2 of a Web Site Scan. The tester simply replaces the parameters with a valid user name and password.



Using a URL Parameter

Task 1: Create Parameter

1. After recording and testing your macro, click **Parameters Editor** in the toolbar.

   The Parameters Editor opens.

2. Click  to add a parameter.
3. In the **Name** text box, enter a name for the parameter (for example: **StartURL**).
4. In the **Value** text box, enter the default text, Host Name, or URL (for example: **www.Placeholder.com**) that you want testers to see as the value for the parameter as they configure a scan. However, while you are developing the macro, for macro playback to succeed or for security reasons you might need to use a different, temporary default text, Host Name, or URL and change it to the default after you verify the macro near the end of this procedure.
5. Click **Close** to close the Parameters Editor.

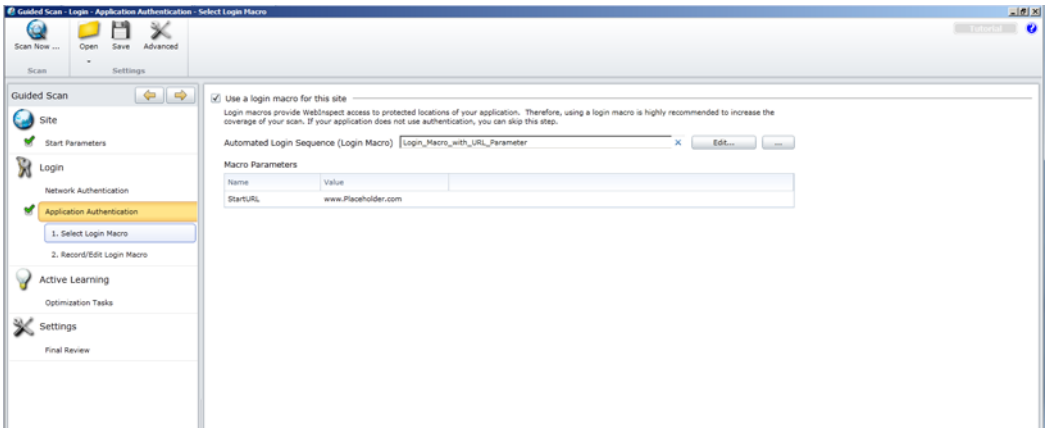
Task 2: Assign Parameters to Steps

1. Select the macro step that contains the URL ("Navigate to...").
2. Place your mouse in the upper right corner of the step and click to open the Step Editor.
3. Click (expand) **Arguments**.
4. Highlight the entire contents of the **Location** text box, right-click the highlighted text, and select **Replace with a Parameter**.
5. On the *Enter Parameter Name* dialog, select the parameter (**StartURL** in this example) from the **Select Parameter** list and click **OK**.

   The **Location** takes on the format of a parameter.

6. Play the macro to verify that it logs in correctly.
7. If necessary, reopen the Parameters Editor and change the text in the **Value** text box to the default text, Host Name, or URL that you want testers to see, as described in step 4 under Task 1 on page 284.
8. Save the macro. (For a Guided Scan, click **Export**. For a Web Site Scan, click **Save**.)

When you start a Guided Scan or a Web Site Scan and select this macro, the parameters appear in the Macro Parameters table for a Guided Scan as shown below, or in the table below the name of the selected login macro in step 2 of a Web Site Scan. The tester either leaves the parameter unchanged (to access the original URL) or enters the URL of the target site.



Enhancing Macros

There are a number of optional enhancements that can be added to macros.

Modify Steps

Modify step arguments and objects by selecting the desired step and expanding the options. This expands the step and allows you to modify the objects and properties. For a detailed list of the step structure, see Toolbox on page 292.

Insert loops

A loop repeats a selected portion of the macro until certain criteria are met or for a specified number of times. To insert a loop, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **For loop** element to the desired location among the macro steps. For more information, see Inserting and Modifying Loops on page 292.

Insert If blocks or If-else blocks and exit steps

To conditionalize a portion of the macro, you can insert If or If-else blocks. To insert an If block, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **If block** element to the desired location among the macro steps. To add an else condition, click the **Add else** link next to the If step title. For more details, open the online Help and find the topic titled Step Arguments.

Exit steps cause a macro to exit the iteration or the entire macro. These can be used with If statements to exit a macro or iteration when a specified condition occurs. To insert an exit step, click **Toolbox**, click (expand) **Flow Control**, and click and drag the **Exit** element to the desired location among the macro steps.

Insert comments

To insert comments into your macro, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Miscellaneous**, and click and drag the **Comment** element to the desired location among the macro steps.

Insert Catch Error Steps

"Catch error" steps are group steps that run their contents if the previous step contains an error. (To group steps, use **Ctrl** + click to select multiple steps, right-click any of them, and click **Group Steps**.) Additionally, the error is "caught" and is not returned. You can define catch error steps to catch any error, or a specific type of error. If there are two catch error steps in a row, they both apply to the same step. To insert a catch error step, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **Catch Error** element to the desired location among the macro steps.

Verify that an object exists

To verify that a string or object exists in the application, insert a verify step:

1. Click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Functions**, and click and drag the **Verify** element to the desired location among the macro steps.
2. Click the object in the verify step.
3. Select the object you want to verify.

Insert generic steps

You can insert a blank step and manually configure it. To insert a generic step, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Functions**, and click and drag the **Generic Object Action** element or the **Generic Browser Action** element to the desired location among the macro steps. Expand the step, and enter the desired step properties. Generic Object Actions perform an unspecified action on an object. Generic Browser Actions perform an unspecified action on the browser such as go back, reload, switch tabs, etc.

Debugging Macros

This section describes the basic steps involved in interactively debugging a macro.

View Replay Errors in Browser

If any steps failed during replay, they are marked with an error icon  . Hover the mouse pointer over these icons to view descriptions of the errors.

Run the Macro Step by Step

The step-by-step replay allows you to view the sequence more slowly and in a controlled manner. To run the macro step by step, select the down arrow next to the **Replay** button in the right (macro steps) pane and select **Replay step by step**. Repeat this procedure after each step to continue the step-by-step replay.

Insert Breakpoints

Breakpoints instruct the macro to stop running during a replay when in interactive mode. They can be used to help debug your macro. To insert a breakpoint, select the desired step and click **Toggle breakpoints**  in the macro steps toolbar (or right-click on the step and click **Toggle Breakpoint** in the popup menu).

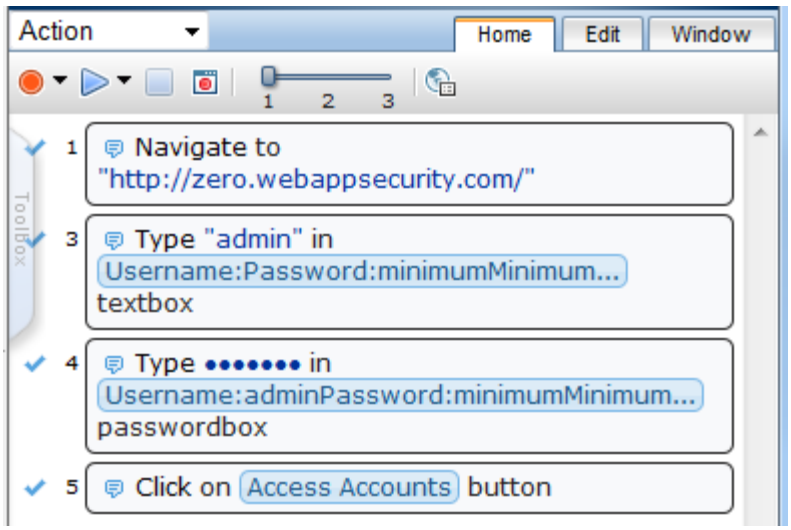
Modify Script Levels

As you record a macro, it assigns a level from 1 to 3 to each step. For example, a level 1 step is essential to the macro. A click step that occurs in an area of the application that has no effect is assigned to level 2. Mouse-over steps are generally considered unnecessary for the macro and are assigned to level 3.

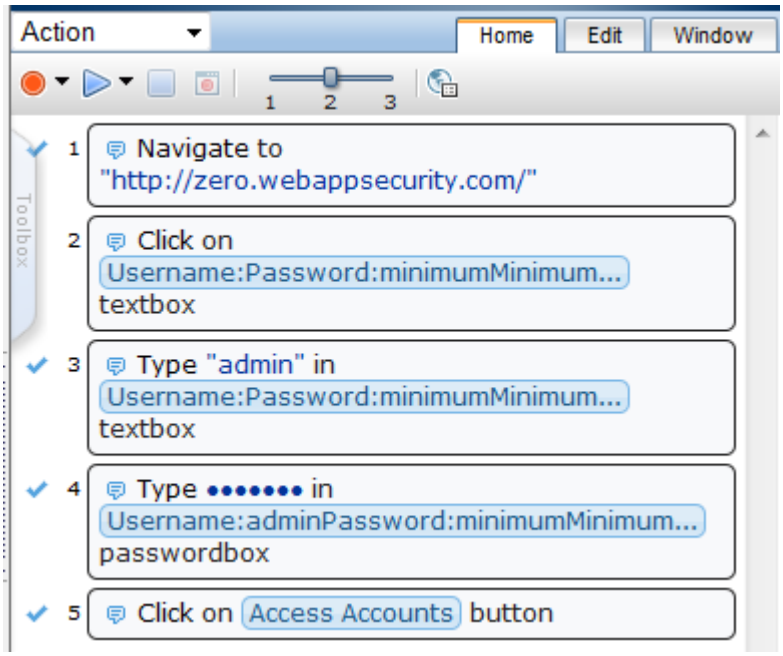
Macro steps are displayed *and played* with the granularity specified as level 1, 2, or 3 in the **Script Level** slider in the macro steps toolbar at the top of the Home tab. The highest granularity is level 3—setting the slider to level 3 displays and plays back all the steps at levels 1, 2, and 3. Using higher granularity might be required for successful playback, but it can cause the macro to take longer to run. By default, the **Script Level** is set to 1.

To modify a macro's replay level, drag the **Script Level** slider in the macro steps toolbar to the desired level.

The following illustration shows a macro for which step 2 is hidden at **Script Level** 1.



When the **Script Level** is changed to 2 as shown below (or if the **Script Level** were changed to 3), then macro step 2, which represents clicking in a text box and is assigned to **Script Level** 2, is also displayed and will run if the macro is replayed.



In certain cases, you may want to manually change the level of a particular step, not the entire macro. For example, you may want to display and play a particular mouse-over step. To change the level of a step:

1. Place your mouse in the upper right corner of the step and click to open the Step Editor for the step.
2. Move the slider at the top of that step (to the right of the step number) to the desired level.

   If the step is part of a group step, both the group step and the individual step must be modified. (To group steps, use **Ctrl** + click to select multiple steps, right-click any of them, and click **Group Steps**.)

Insert Wait Steps

Wait steps cause the macro to pause for a specified amount of time before continuing with the next step. Wait for Object steps cause the macro to wait for a specified object to load before continuing with the next step. Wait steps begin after the End Event of the previous step is reached. This means that the previous step may continue to run after the wait step has been reached.

To insert a wait step, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Functions**, and click and drag the **Wait** element or the **Wait for Object** element to the desired location among the macro steps. Wait steps wait for a specified amount of time. Wait for Object steps wait until the specified object appears in the application. In Wait for Object steps, select the **Click to choose an object** button to select the target object in the application.

Disable/Enable Steps During Replay

To disable or re-enable a macro step during replay, place your mouse in the upper right corner of the step and click to open the Step Editor, and click the  icon in the toolbar for the step. Alternatively, to disable or re-enable one or more steps, use **Ctrl** + click to select them, right-click one of the steps, and click **Disable Steps** or **Enable Steps** on the popup menu.

Disabled steps remain in the macro and can be re-enabled in the future, but are not played.

Make a Step Optional

Some steps can be made optional. An optional step is skipped during replay if its object is not found. To make a step optional, place your mouse in the upper right corner of the step and click to open the Step Editor, and click the  icon in the toolbar for the step. To make a step non-optional again, click the icon again.

Play a Step

To play one step, place your mouse in the upper right corner of the step and click to open the Step Editor, and click the  icon in the toolbar for the step.

Play From a Step to End of Macro

To start playback at one particular step and continue until the end of the macro, select the starting step, right-click on the step, and click **Play From This Step** on the popup menu.

Resolving Object Identification Issues

In dynamic websites, objects that have been recorded can often move or change content. Object identification presents one of the biggest challenges with recording and replaying Web 2.0 applications. This can cause a macro to lose the ability to locate the object.

The Web Macro Recorder includes sophisticated mechanisms to overcome this challenge, including the Highlight, Improve Object Identification, Replace, and Related Object options within steps that have objects. Using these options requires that you select an object in the application. For cases where various actions are required in the application to make the object visible, such as mouse over and mouse click, use the **Ctrl+Alt+F4** option to suspend the object-selection mode until you bring the object into view and press **Ctrl+Alt+F4** again to select the object.

When identifying objects for applications that were recorded in windows, use the Windows tab to make sure that the correct window is selected.

After you perform any of the changes, first replay the single failed step in question and then replay the entire macro again. This will help verify whether the change has solved the issue you encountered.

The following sections describe ways to resolve object identification issues.

Highlight an object

Regardless of which method of object identification is used, place your mouse in the upper right corner of the step and click to open the Step Editor. Click (expand) **Object** and click the **Highlight** button  to check at any time whether an object is visible in the application. If the object is found, it is temporarily surrounded by a flashing red outline. If the object is not found, an error message is displayed. The error could be an issue of pacing and timing, or that the correct page to find the object is not displayed.

Improve Object Identification

If the Highlight option fails, click the  . icon (with tooltip "Improve object identification") next to the selected ID Method for the object. This will let the Web Macro Recorder relearn the properties of the object and compare them to the properties learned during recording. Based on the differences, the necessary adjustments can be made. Depending on how dynamic the application is, you may need to use the Improve Object Identification function more than once.

Once you have done this, try replaying the step again to check whether the problem has been solved.

Consider Alternative Steps

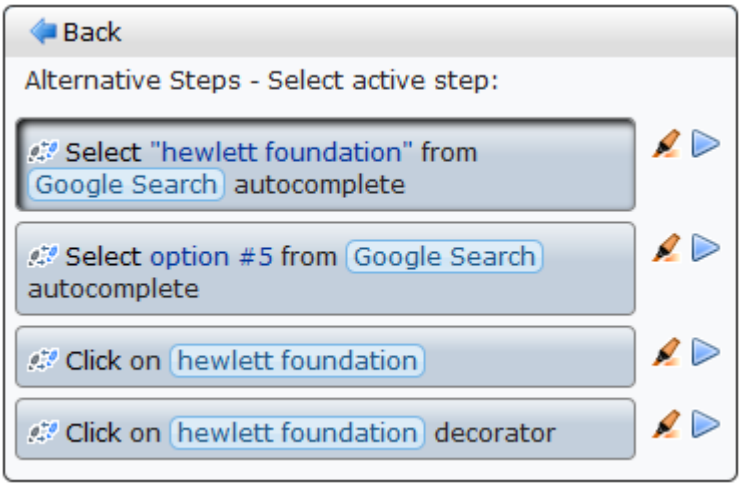
Alternative steps allow you to view multiple ways to perform the same action in a step, where it is possible. You can modify the step for the best or most consistent macro performance, or for debugging purposes.

For example, you may be clicking on an option in a drop down list in which the text changes based on some value. If you try to click based on the text, the step may fail. If you use an alternative step that selects the item in the list based on the ordinal value of the option within the list, the click will succeed regardless of the text.

Steps that have alternative options are labeled with an alternative step icon  on the left. Click the icon to view the alternative options for that step. (If the Step Editor is open, a button labelled **Alternative steps**, with the same icon, appears in the step's toolbar and performs the same function.)

The following screens show an example of alternative steps. After performing a Google search on "hewlett" and selecting "hewlett foundation" as the fifth automatically generated item in the Google search box autocomplete, the step that has alternatives (expanded in the Step Editor) is shown below.

Clicking the icon displays the alternative steps shown below.



The icon to the right of each alternative has the tooltip "Highlight the object in the AUT," where AUT means application under test. This performs the same highlighting function as described in Highlight an object on page 289, with the convenience of being able to highlight each alternative one at a time within the macro step.

Each alternative also has a Play icon so that you can confirm that using an alternative takes the appropriate action for the macro step.

Macro replay succeeded for each alternative.

Click the desired alternative to make it active, and click **Back** to return to normal display of the macro step using the alternative you selected. Replay the macro to test it.

Modify the Object Identification Method

You can modify the way the Web Macro Recorder identifies the object by modifying the object identification method (ID method) in the Object section of the Step Editor. The following options are available:

- **Automatic**. The default and recommended object identification method. The Automatic method allows the Web Macro Recorder to use its internal advanced algorithms to locate the object. If this method does not successfully find the object during replay, click the icon (with tooltip "Improve object identification") and replay the macro again.
- **XPath**. If Automatic identification fails, even after using Improve Object Identification or Related Objects (see Relate objects to other objects on page 291), try using the XPath identification method. This method identifies the object based on an XPath expression that defines the object in the DOM tree. For example, if you need to select the first search result, regardless of the term being searched for, using XPath identification may help.

  Click the drop-down arrow next to the **XPath** edit box to select a suggested XPath for the object. You can click the popup **Edit** button at the right end of the **XPath** edit box to open the XPath Editor and edit the suggested XPath.

  For the XPath ID method, the tooltip for the icon changes to "Regenerate expression." When you click the icon, you can select an object in the interface and thereby create its associated XPath.

- **JavaScript**. JavaScript code that returns an object. For example: document.getElementById("SearchButton") returns an element that has a DOM ID attribute of "SearchButton."

  Using the JavaScript identification method, you can write JavaScript code that references the returned document and you can use CSS selectors and other standard functions.

  For example, the page returned by the server contains multiple links with the same "title" attribute (search results) and we want the script to randomly click on one of the available links.

  Object identification for this case, using the JavaScript identification method, may look similar to the following:

  ```
  var my_results = document.querySelectorAll('a[title="SearchResult"]');

  random(my_results);
  ```

Modify the macro timing

Sometimes objects may not be found because of timing and synchronization issues. For example, the macro may be looking for an object that was in the application, but the macro replayed too quickly and already progressed to another page. If you suspect that the object is not being found because of a timing or synchronization issue, you can insert Wait steps. For more information, see Insert Wait Steps on page 288.

Relate objects to other objects

If the preceding options do not solve the issue, try using the Related Objects option.

If an object becomes difficult to identify on its own, you can label the object based on a different, more stable object. For example, you can select an object that is not dynamic and "relate it" to the target object. Relations are defined visually, relating objects according to their distance in pixels from other objects. Relations are defined per ID method, per object. If more than one relation is defined for an ID method of a given object, both relations must locate the same object for the step to pass. To use this function, place your mouse in the upper right corner of the step and click to open the Step Editor, click (expand) **Object,** click (expand) **Related Objects**, and click  . Follow the directions to create a relation. Verify that it has worked by highlighting both the object and its related object.

Tips:

- Use this feature only if other identification methods have failed, as it may be more resource intensive.
- Use the minimum search area to improve performance.
- Related Objects are sensitive to window sizing. Resizing may alter object positions and relationships. This should be taken into account.
- Each identification method (Automatic, XPath, and JavaScript) has its own set of related objects. These related objects are not shared among identification methods.
- If several relations exist, they all need to be found in order for the identification to succeed.

Replace an object

If you selected the wrong object during recording or an object has permanently changed, you can replace it with a different object without replacing the step. This effectively resets the step, deleting changes made to the original step such as relations. Place your mouse in the upper right corner of the step and click to open the Step Editor, click (expand) **Object**, and click **Replace**  . Select the new object and replay the macro.

Using this option tells the macro recorder that the object currently referenced in the step is incorrect. The macro recorder will remove any current knowledge of the object and learn the object you select. Therefore, you should only use the **Replace** option if the object you used during recording was the wrong one.

Inserting and Modifying Loops

Loops repeat selected portions of the macro until certain criteria are met or for a specified number of iterations. You can insert loops and loop modifiers from the **Flow Control** section of the **Toolbox**.

"For" Loops

"For" loops perform the steps surrounded by the loop until the end condition is met or the code reaches a break statement. Loop arguments use JavaScript syntax. To insert a For loop, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **For loop** element to the desired location among the macro steps.

"Break" statements

Break statements indicate that the current loop should end immediately. For example, if a Break statement is encountered in the second of five iterations in a For loop, the loop will end immediately without completing the remaining iterations. To insert a Break statement, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **Break** element to the desired location among the macro steps.

"Continue" statements

Continue statements indicate that the current loop iteration should end immediately. The loop condition is then checked to determine if the entire loop should end as well. For example, if a Continue statement is encountered in the second of five iterations in a For loop, the second iteration will end immediately and the third iteration will begin. To insert a Continue statement, click the **Toolbox** vertical tab on the left side of the macro steps pane, click (expand) **Flow Control**, and click and drag the **Continue** element to the desired location among the macro steps.

Toolbox

The toolbox, a vertical tab on the left side of the macro steps pane, enables you to add steps to macros. When you click **Toolbox** and click (expand) one of the headings such as **Functions,** you can click and drag a particular element such as **Verify** to add it to the macro steps.

You can click and drag **Toolbox** to move the toolbox up or down. To close the toolbox, click **Toolbox** again.

User interface elements are described in the following table.

Toolbox User Interface Elements

UI Element	Description
Functions	**Verify**. Verify that an object exists in the application. **Wait**. Wait for a specified number of seconds before continuing with the next step. **Wait for Object**. Wait for an object to load before continuing with the next step. **Generic Object Action** or **Generic Browser Action**. Blank steps that can be inserted and manually configured. See Insert generic steps on page 286.

Toolbox User Interface Elements (cont'd)

UI Element	Description
Flow Control	**For Loop**. A logical structure that repeats the steps contained in the loop a specified number of times. **If Block**. A logical structure that runs the steps contained in the block if the condition is met. • **Add else**. Click the **Add else** link to add an **else** section to your **If** block. If the condition is not met, the steps included in the **else** section run. • **Remove else**. Removes the **else** section from the **If** block. Note: If the **else** section contains steps and you click **Remove else**, the steps are deleted. Copy and paste them into the main body of your macro to save them. **Break**. Causes the loop to end immediately without completing the current or remaining iterations. **Continue**. Causes the current loop iteration to end immediately. The macro continues with the next iteration. **Catch Error**. Catches an error in the step immediately preceding and runs the contents of the catch error step. For more information, see Insert Catch Error Steps on page 285. **Exit**. Exits the iteration or the entire macro depending on the specified setting.
Miscellaneous	**Evaluate JavaScript**. Runs the JavaScript code contained in the step. **Evaluate JS on Object**. Runs the JavaScript code contained in the step after the specified object is loaded in the application. **Comment**. A blank step that allows you to write comments in your macro.
Composite Steps	**Security Question.** Allows you to select the interface object (usually a label) that asks a security question and the interface object (usually a text box) where the user provides the answer. Then you specify the text of the question and the answer.

General Settings

Click **General Settings**  in the toolbar of the macro steps pane to open the *General Settings* dialog.

Snapshot Generation

A snapshot is an image of the browser taken at the times specified by the following options:

- **Recording snapshots generation**. Select **Never** (the default) or **Always**. During macro recording, any snapshots that are taken are saved in the same folder as the macro.
- **Replay snapshots generation**. Select **Never**, **On Error** (the default), or **Always**. During a scan, any snapshots that are taken are saved in the log directory.

Replay Options

Specify the following options:

- **Maximum time for object-not-found (seconds)**. Specify the maximum time (in seconds) that the macro recorder will wait for the target object of a replay step to appear.
- **Inter-step interval (milliseconds)**. Specify the minimum interval (in milliseconds) between steps.

- **End-of-network identification timeout (milliseconds)**. Specify the timeout (in milliseconds). The end-of-network timeout for a step is recognized when the specified time has elapsed with no network activity.
- **Clean image cache per user**. If you select this option, the image cache will be cleared during replay.

Log Level

Select one of the following options:

- **Standard logging**. Log only warnings and high-level informational messages.
- **Extended logging**. Log low-level messages, warnings, and high-level informational messages.

Logout Detection

In the **XPath depth** option, specify the depth used for XPath in logout detection by element. The depth determines the number of xpath locators (parents) from the element up to its ancestors.

An element can be located (found) in a page using a path to its location. For example, in the following HTML, to locate , the search can use the following: find body, then find div with id painterId, or the search can use find body-> then find second div.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html lang="en">
  <head>
    <title>colors</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />

  </head>
    <body>
      <div class="container">
        <div class="box">
          <div class="caret" id="red">
            <span></span>
          </div>
        </div>
        <div class="number" id="redNumber">0</div>
        <div class="box">
          <div class="caret" id="green">
            <span></span>
          </div>
        </div>
        <div class="number" id="greenNumber">0</div>
        <div class="box">
          <div class="caret" id="blue">
            <span></span>
          </div>
        </div>
        <div class="number" id="blueNumber">0</div>
      </div>
      <div class="painter" id="painterId">Color</div>
      <script type="text/javascript" language="javascript">initialize();</script>
    </body>

  </html>
```

So, when searching through larger html files with more complex structures, the process can use either a rigid full xpath, or a loose short xpath. The default value is 3.

Encryption

If you select the **Encrypt Macro** option, the entire macro file is encrypted when saved. Otherwise, the file is saved in plain text, which exposes user names and passwords. This option is selected (ON) by default.

Web Service Test Designer

Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services use Simple Object Access Protocol (SOAP) to send XML data between the Web service and the client Web application that initiated the information request. Unlike HTML, which only describes how Web pages are displayed, XML provides a framework to describe and contain structured data. The client Web application can readily understand the returned data and display that information to the end user.

A client Web application that accesses a Web service receives a Web Services Definition Language (WSDL) document so that it can understand how to communicate with the service. The WSDL document describes the programmed procedures included in the Web service, the parameters those procedures expect, and the type of return information the client Web application will receive.

Use the Web Service Test Designer to create a Web Service Test Design file (filename.wsd) containing the values that WebInspect Enterprise should submit when conducting a Web service scan.

Although the following procedure invokes the Web Service Test Designer from the WebInspect Enterprise **Tools** menu, you can also open the designer from the HP Security Toolkit or through the WebInspect Enterprise Scan Wizard by selecting **Scan Web Service** from the WebInspect Enterprise Start page and, when prompted, electing to launch the designer.

When the Web Service Test Designer is launched from the WebInspect Enterprise Scan Wizard, if the WSDL has not yet been configured, the designer will automatically import the WSDL, assign "auto values" to each parameter, and invoke all operations. This does not occur when you launch the tool from the WebInspect Enterprise **Tools** menu or from the HP Security Toolkit.

1. Select **Tools** → **Web Service Test Designer**.
2. On the startup dialog, select one of the following:
   - **New Web Service Test** - Design a new Web Service test.
   - **Open Web Service Test** - Edit a design that you previously created.

   The following procedure assumes that you are creating a design.
3. Do one of the following:

   - In the **Import WSDL** box, type or select the URL of the WSDL site and click **Import WSDL**  .

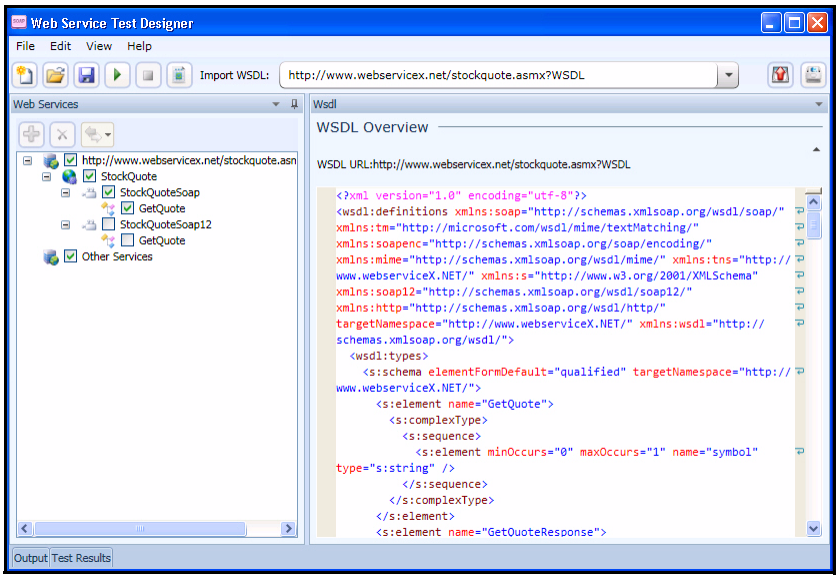
     Example: http://www.webservicex.net/stockquote.asmx?WSDL.

   - Click **Browse for WSDL**  and select a WSDL file that you previously saved locally.

   If authentication is required, or if SOAP requests need to be made through a proxy server, see Web Service Test Designer Settings on page 304 for more information.

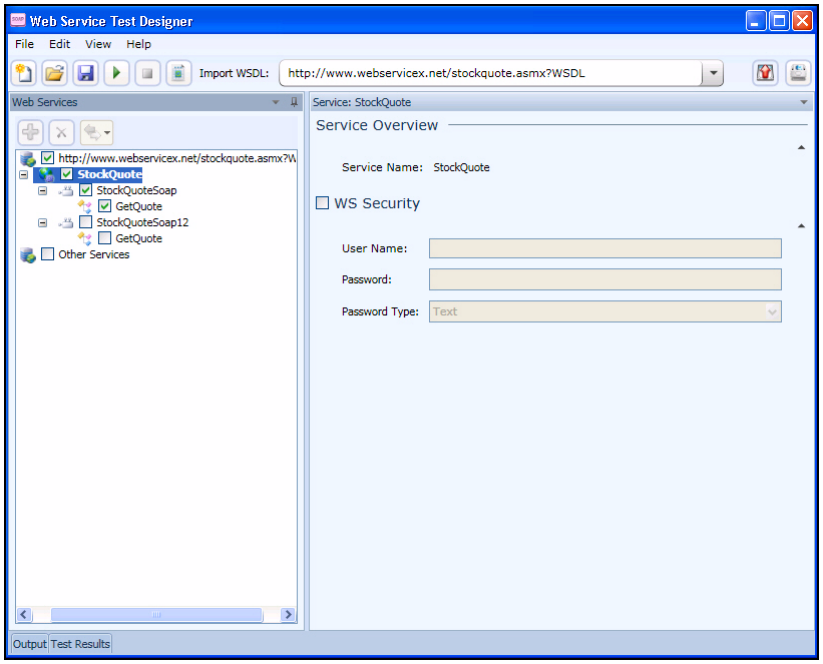
   Also note that "Other Services" appears by default. This feature is used to add services manually when a service is not associated with a WSDL. See Manually Adding Services on page 299 for more information. Remove the check mark next to this item.

The WSDL endpoint (typically represented by a simple http URL string) appears in the left pane, followed by the service name and a hierarchical listing of the operations defined for that service. The right pane (by default) contains the WSDL URL and, when available, the namespace, binding namespace, and the port location.



The above illustration shows a simple WSDL that returns the current stock price and other related information when the user submits a corporate symbol used by the New York Stock Exchange.

4 Select the service in the left pane to display service overview information in the right pane.

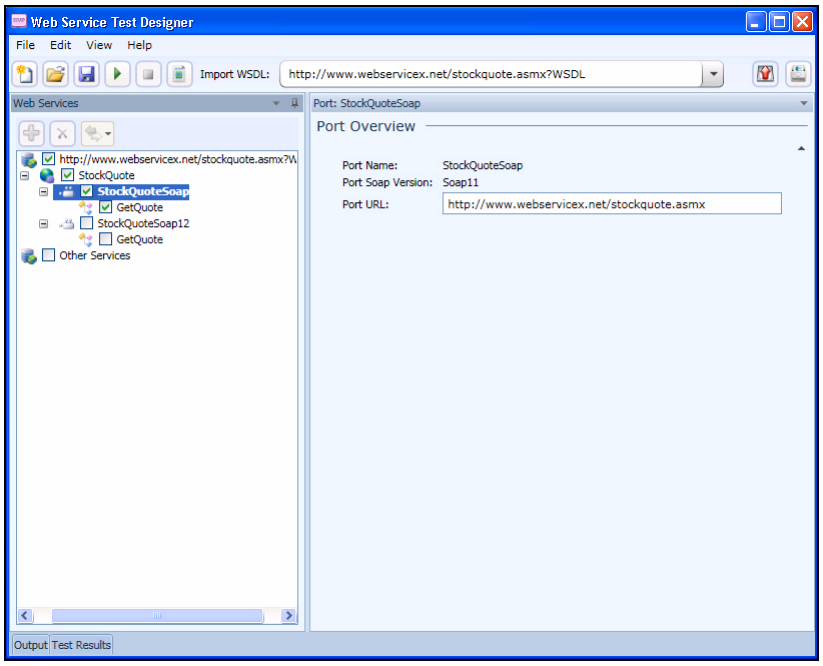


Note that if the description of the WSDL includes both SOAP version 1.1 and version 1.2, and if the operations in both descriptions are the same, the versions are assumed to be identical and the services in version 1.1 only are configured. If you wish to attack both versions, then you must select the check box for each version 1.2 operation.

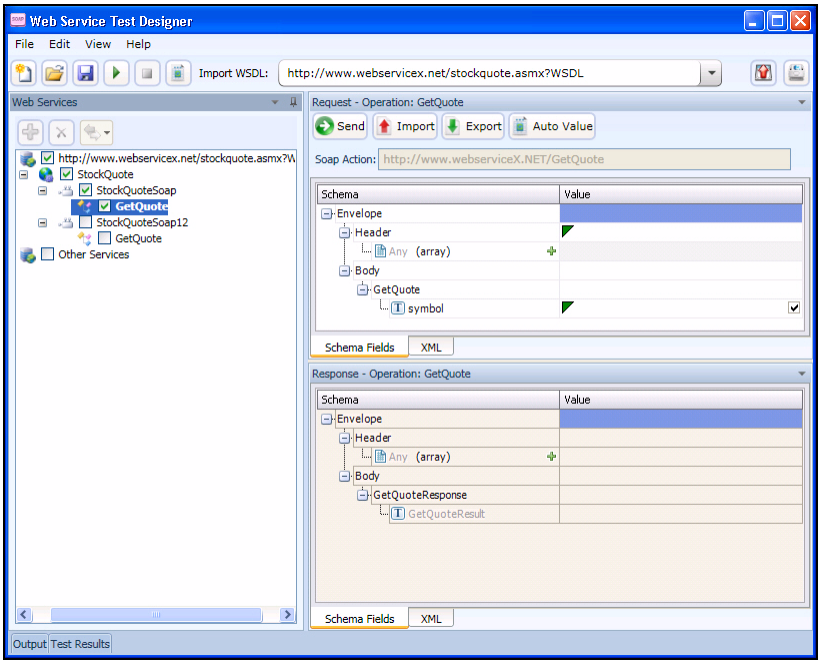
If authentication is required, select **WS Security** and provide the required credentials.

5 Select a service transport in the left pane to display the port information in the right pane. A port defines an individual endpoint by specifying an address for a binding.

RPC-encoded services require manual configuration. The **Schema Fields** tab is populated using a default SOAP schema. You can obtain the desired SOAP message from a developer or a proxy capture, and then paste the message into the **XML** tab (or import the saved message from a file). You can then click **Send** to test the operation.



6 Click an operation to display schema for the request (in the top half of the right pane) and the response (in the lower half).



7 Enter a value for each parameter in the operation. In this example, the user entered HPQ (the NYSE symbol for Hewlett-Packard).

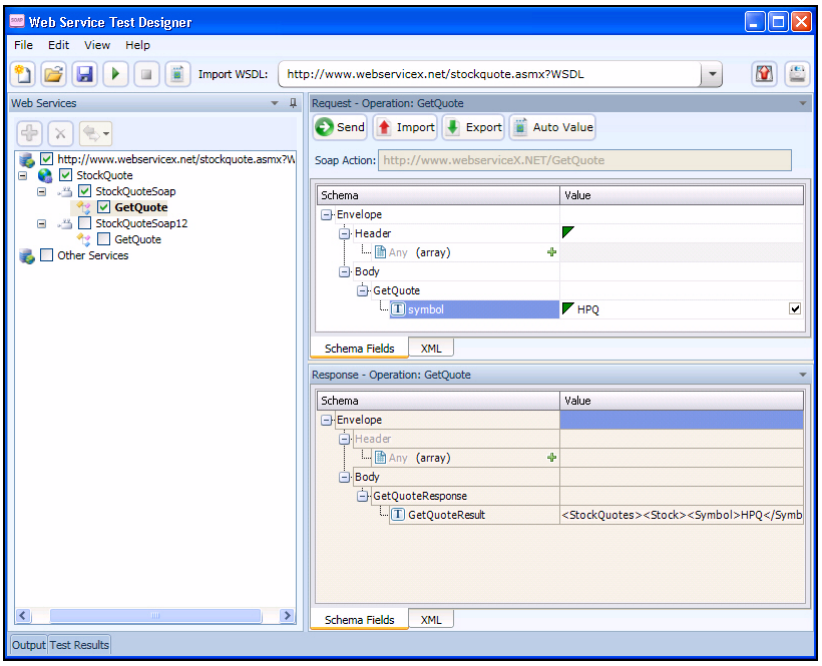
If you click **Auto Value**, the designer assigns a value to the operation. This value is either:

- Obtained from the GlobalValuesDefault.xpr file, if the file contains an entry that matches the name of the parameter; see Global Values Editor on page 300 for more information.
- Created by the designer, based on the data type. In this example, the designer would populate the parameter “symbol” with the value “symbol1.”

See Using Autovalues for more information.

8 Click **Send**  .

Results appear in the lower portion. You can alternate between the Schema and XML views by clicking the appropriate tabs.



9 When you have assigned and tested values for each operation (although only one operation is depicted in this example):

a Click **File** → **Save**.

b Using the standard file-selection dialog, select a name and location for the Web Service Design file (.wsd).

If the WSDL contains multiple operations, data is saved for each operation regardless of whether or not the operation is checked. A check mark simply indicates that the operation will be used for auditing.

Manually Adding Services

You may encounter a Web service that does not have a WSDL associated with it.

For example, the WebInspect Enterprise Recommendations module monitors scans to detect omissions, abnormalities, or anomalies that interfere with or diminish the thoroughness of a scan. If it detects SOAP requests during a Web Site scan, it suggests that you conduct a Web Service scan of that site and creates a Web Service Test Design file (filename.wsd) for that purpose. A WSDL file probably will not be available.

You may create a service manually, as shown in the following example.

1 Right-click the default “Other Services” service and select **Add Service**.

New Service 1 appears in the Web Services tree in the left pane.

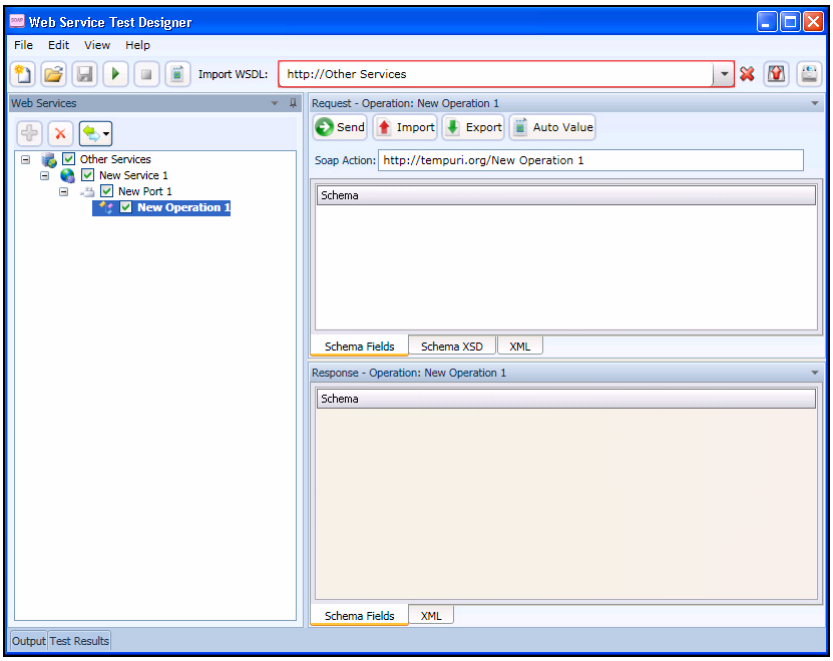
2 If authentication is required, select **WS Security** and provide the required credentials.

3 Right-click New Service 1, select **Add Port**. and then choose either **SOAP 1.1** or **SOAP 1.2**.

New Port 1 appears in the Web Services tree.

4 In the **Port URL** box, enter the correct URL to the service.

5 Right-click New Port 1 and select **Add Operation**.



Note: To change service, port, or operation names, double-click the name.

6 You can import a file containing a SOAP envelope (possibly obtained using the Web Proxy tool) or you can copy and paste a SOAP envelope that you obtained from a developer onto the **XML** tab.

If importing from a proxy capture, the SOAP action will be in the HTTP header (Soapaction=<action_name>).

7 If necessary, modify the values using either the **Schema Fields** tab or the **XML** tab.

8 To test the service, click either **Send** or **Run All**.

Global Values Editor

You can create a library of name/value parameters for operations that you frequently encounter. After importing a WSDL file, if you click Set Auto Values  , the Web Service Test Designer searches the Global Values file for the names of parameters contained in the WSDL operations. If it finds a matching name, it inserts the associated value from the file into the parameter value field.

To add a global value:

1 Click **Edit** → **Global Values Editor**.

The Global Values Editor opens and displays the contents of the default xml parameter registry (xpr) file named GlobalValuesDefault.xpr.

2 Click **Add**.

This creates an entry with the default name of [Name] and a default value of [Value].

3 Click anywhere on the entry and substitute an actual name and value for the default.

4 Repeat step 2 and step 3 to create additional entries.

5 Do one of the following:

- Click **OK** to save and close the file.
- Click **Save As** to create and close the file using a different file name and/or location.

Importing and Exporting Operations

You can build a library of operations and their assigned values, allowing you to quickly modify other Web service designs or exchange these components with other developers/testers. Each module is saved as an XML file, such as the following request used in the preceding example:

```
<Envelope xmlns="http://www.w3.org/2003/05/soap-envelope">
 <Header />
 <Body>
  <GetQuote xmlns="http://www.webserviceX.NET/">
   <symbol>HPQ</symbol>
  </GetQuote>
 </Body>
</Envelope>
```

To save or import an operation:

1 Select an operation in the left pane.

2 Click **Import Request**  to load the operation.

3 Click **Export Request**  to save the operation.

Using Autovalues

Use the Autovalues feature as an alternative to manually entering specific values for each parameter. The Web Service Test Designer analyzes each parameter and inserts a value that is likely to fulfill the service requirement. This can save considerable time when dealing with large web services.

After selecting a WSDL file:

1 Place a check mark next to each operation you want to autofill.

2 Click **Set Auto Values**.

The following message appears: “Would you like the default values to be replaced with the defined global values?”

If you click **Yes**, any values you may have entered manually will be erased. Also, if any parameter name in any operation matches a parameter name in the Global Values file, the associated value in the file will be substituted for the value that would normally be generated for the operation.

If you click **No**, the function terminates.

3 Click **Yes**.

4 Click **Run All Tests**.

The Web Service Test Designer submits the service request, with values inserted for each operation.

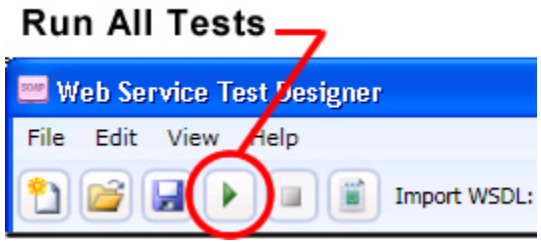
5 Click the **Test Results** tab (at the bottom of the window).

6 If an operation returned an error, double-click the operation to open it in the Request pane and manually provide a value.

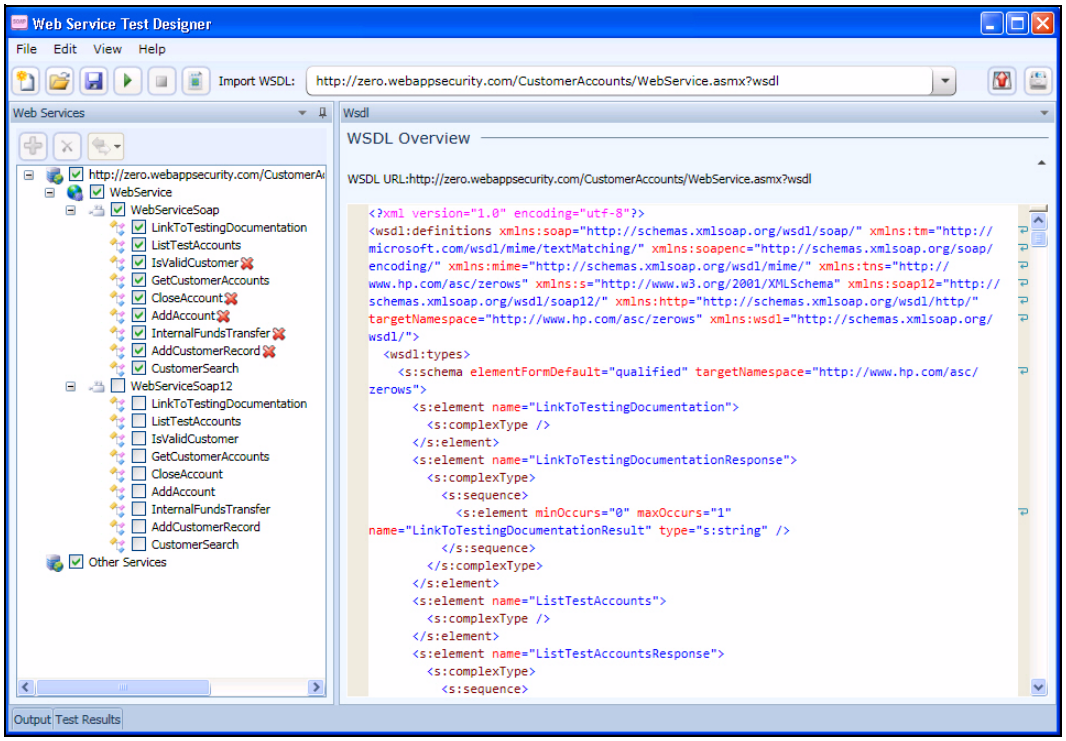
Testing Your Design

You can, at any time, test the configuration of any or all operations.

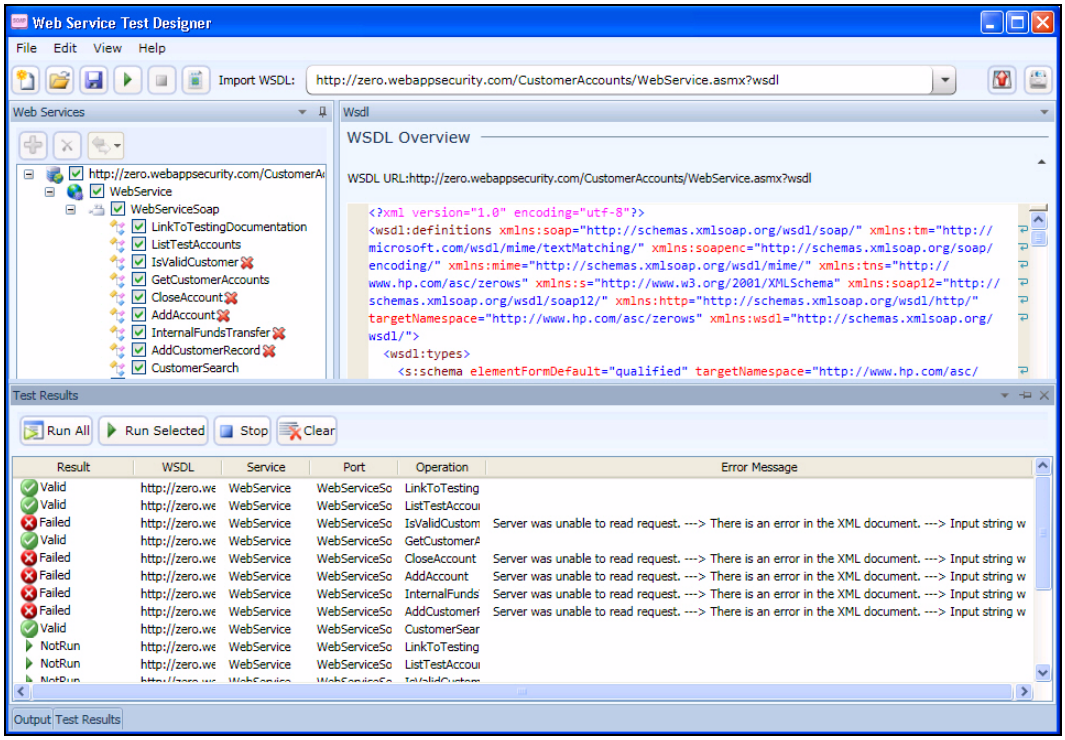
After importing the WSDL, click **Run All Tests**.



The designer attempts to submit all selected operations and displays the results.



To open the special Test Results pane, click **Test Results** on the Status bar.



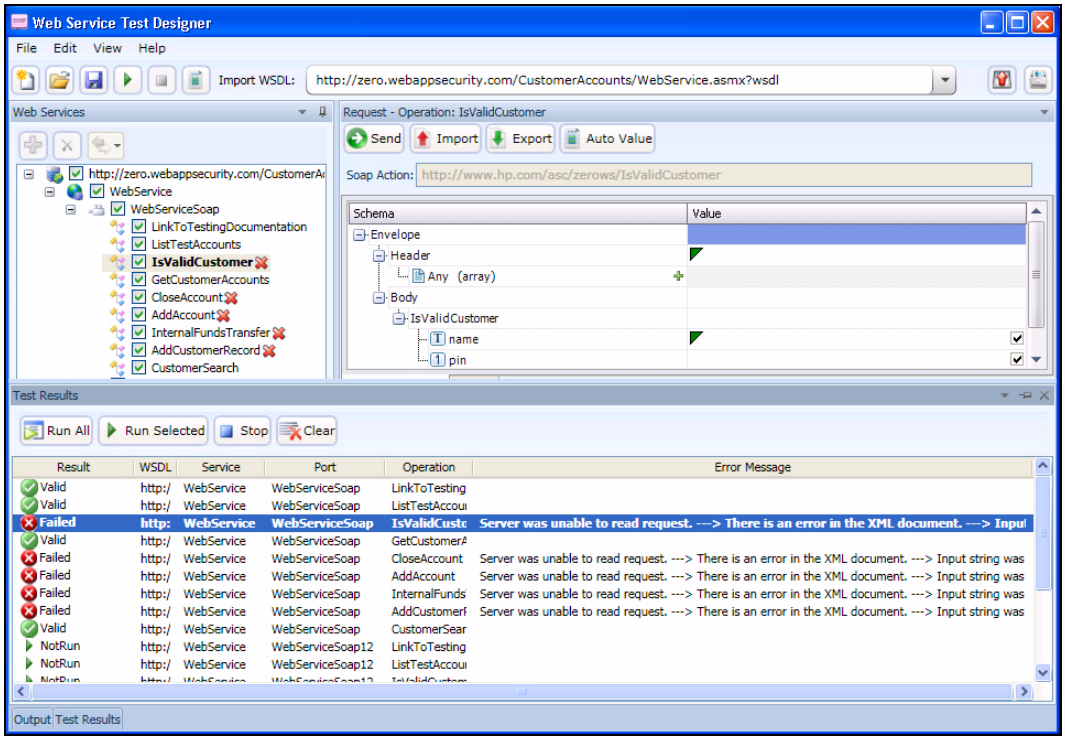
The Test Results pane displays the following information:

- Result – The test outcome. Possible values are:
  - Valid: The operation succeeded without a server error or SOAP fault.
  - Not Run: The operation was not submitted because it was not selected (no check mark) or the Stop button was pressed before the operation was submitted.
  - Pending: The Run button has been pressed but the operation has not yet been submitted.
  - Failed: The request was unsuccessful, the server returned an error message, or a SOAP fault was received.
- WSDL – The WSDL associated with the item
- Service – The service associated with the item
- Port – The port associated with the item
- Operation – The operation the item represents
- Error Message – Explanation for failure

The Test Results toolbar contains the following buttons:

- Run All – The designer submits the service request for each checked operation.
- Run Selected – The designer submits the service request for operations selected in the Test Results pane.
- Stop – Cancels the sending of service request.
- Clear – Removes all items from the Test Results pane.

If you double-click an item in the Test Results pane, the designer highlights the related operation in the Schema Fields pane, where you can enter values for each parameter.



Web Service Test Designer Settings

The Web Services Designer has two categories of settings:

- Network Proxy
- Network Authentication

To access settings, click **Edit** → **Settings**.

Network Proxy

1 Select a profile from the Proxy Profile list:

- **Direct**: Do not use a proxy server.
- **Auto Detect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
- **Use Internet Explorer**: Import your proxy server information from Internet Explorer.
- **Use PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the URL box.
- **Use Explicit Proxy Setting**s: Access the Internet through a proxy server using information you provide in the Explicitly Configure Proxy section.
- **Use Mozilla Firefox**: Import proxy server information from Firefox.

Note: Electing to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy will not be used.

2 If you selected **Use PAC File**, enter the location of the PAC file in the **URL** box.

3 If you selected **Use Explicit Proxy Settings**, provide the following information:

a In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).

b From the **Type** list, select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.

c If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.

d If your proxy server requires authentication, enter the qualifying user name and password.

e If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

4 Click **Save**.

Network Authentication

If server authentication is not required, select **None** from the **Method** list. Otherwise, select an authentication method and enter your network credentials.

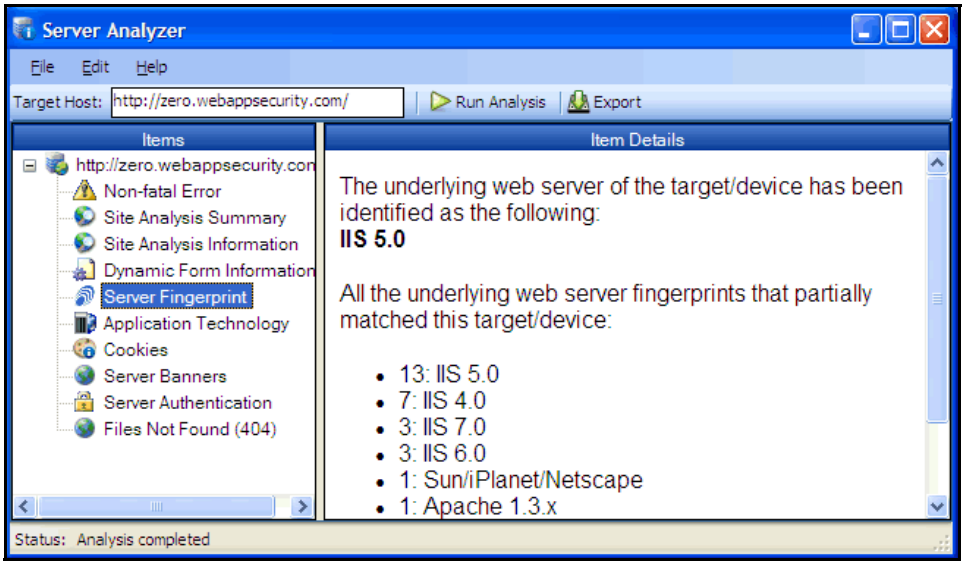
Server Analyzer

The Server Analyzer interrogates a server to determine the server's operating system, banners, cookies, and other information.

Analyzing a Server

To analyze a server:

1. In the **Target Host** box, enter the URL or IP address of the target server.
2. If host authentication is required, or if you are accessing the host through a proxy server, select **Edit** → **Settings** and provide the requested information. See Server Analyzer Settings for detailed information.
3. Click the **Run Analysis** icon.



Server Analyzer Settings

To modify the Server Analyzer settings:

1. Click **Edit** → **Settings**.
2. Select either the **Host Authentication** or **Proxy** category and enter the settings described in the following sections.
3. Click **OK**.

Authentication Method

If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.

Authentication Credentials

Type a user ID in the **User name** box and the user's password in the **Password** box. To guard against mistyping, repeat the password in the **Confirm Password** box.

To use these credentials whenever the Server Analyzer encounters a password input control, select **Submit these credentials to forms with password input fields**.

Proxy

Use these settings to access the Server Analyzer through a proxy server.

Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

Auto detect proxy settings

If you select this option, the Server Analyzer will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Configure a proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information.

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a method from the **Authentication** list. See Authentication on page 103 for a description of the available authentication methods.
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** box. Use commas to separate entries.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Exporting Results

To export the results of the analysis to an HTML file:

1. Click **File** → **Export**.
2. On the *Export File* window, select or enter a location and file name.
3. Click **Save**.

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z