HP Assessment Management Platform

for the Windows® operating system

Software Version: 8.00

User Guide

Document Release Date: March 2009
Software Release Date: March 2009

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Acknowledgements

Other Acknowledgements

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 AMP, contact customer support at 1.800.633.3600. You will need to enter your Service Agreement ID (SAID) number.

You can access the HP Application Security Center customer forum and blogs at

http://www.communities.hp.com/securitysoftware/

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 find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

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

Contents

1 Welcome

Introduction

The Assessment Management Platform (AMP) from HP is based on the industry's most successful and accurate Web application assessment tools: WebInspect, DevInspect, and QAInspect.

As the leader in Web application security, HP delivers the most thorough and dependable tools for evaluating Web application vulnerabilities. Since their introduction, HP scanners have quickly become the most important tools used by developers throughout the entire software development life cycle.

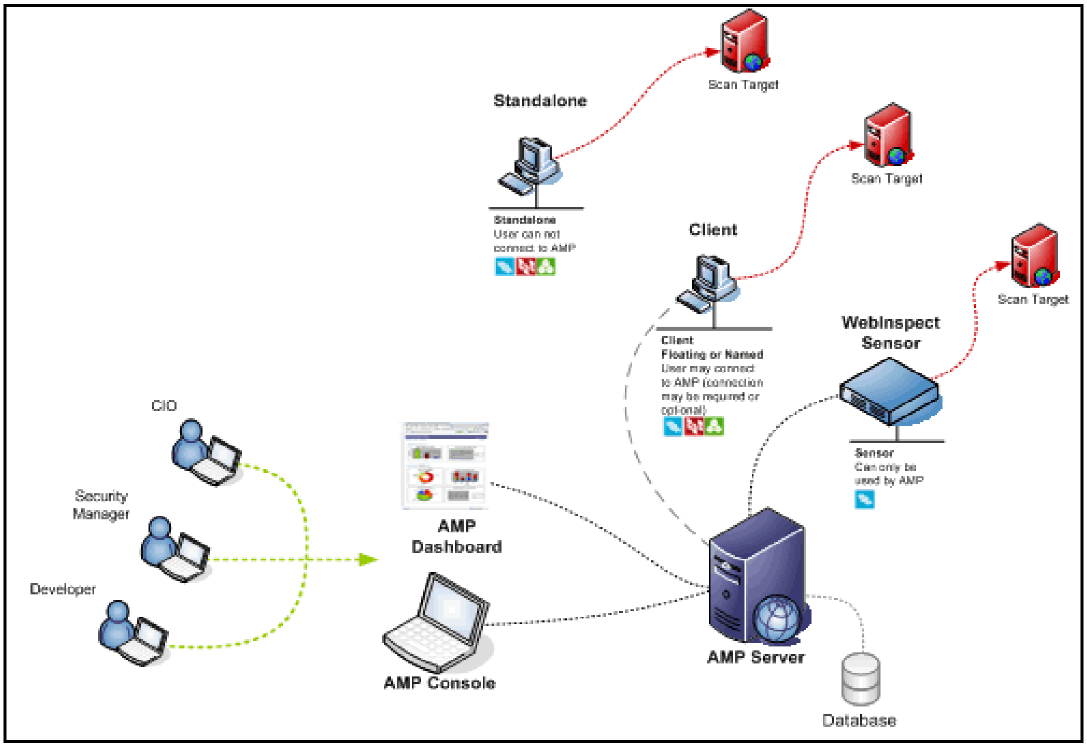
Yet despite our scanners' impressive ability to detect security flaws in Web-based applications, developers of large, intricate Web sites could not easily integrate their assessment results into a centralized repository that would provide an accurate view of the overall enterprise susceptibility.

That's why we developed AMP.

Features and Benefits

AMP is a distributed network of HP scanners controlled by a system manager with a centralized database. This innovative architecture allows you to:

- Conduct a large number of automated security assessments using any number of HP scanners to assess Web applications and SOAP 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 AMP console.
- Detect, track, and manage your Web applications and monitor all activity associated with them.
- Independently schedule scans and blackout periods, manually launch scans, generate reports, and update repository information by using HP scanners or the AMP 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 and policy compliance through a centralized database of scan results, reporting, and trend analysis.
- Facilitate integration with third-party products and deployment of customized Web-based front ends using the Web Services application programming interface (API).



New Features and Enhancements for AMP 8.00

Web Console Login/Logout

The user must now log in to the Web Console (and also has the ability to log out). This functionality was added so that users logging in and out would appear in the Activity log. In addition, the user can now see all users logged into Web consoles (by clicking the Administration group and selecting Connected Users).

Tagging

AMP 8.00 introduces the concept of tagging to allow data to be grouped and categorized as appropriate for the enterprise. These tags are name/value pairs (such as. “project=AMP” or “region=North America”).

Tagging on Objects

An object can be assigned multiple tags, but each tag must have a different name. The AMP system will then allow these custom field values to be displayed as columns in object grids or used in reporting for sorting and grouping the data.

Discovery Site Tags

When configuring a Discovery Scan, you can specify a tag name that will be assigned to all sites found during the scan.

Grouping

AMP 8.00 also allows the user to group data so that all objects sharing a given attribute can be viewed and accessed at once. This grouping can be either on standard data fields or custom tags defined for the object. For example, if severity is selected as the grouping option for vulnerabilities, then the different severity levels would be shown in a new collapsible group pane located to the left of the Vulnerability grid. When “Critical” is selected in the grouping pane, the vulnerability grid will be updated to just show vulnerabilities with critical severity.

Reporting

A new reporting utility provides the following functionalities:

- Report Designer - From the AMP Console, you can launch a report designer to create or modify reports. This allows you to provide additional information or remove data that is not relevant to your organization.
- Session Report - You can now generate session-based reports that show the HTTP request and response, as well as an appendix of all checks found.
- Additional Enterprise Reports - Three new enterprise reports provide information about all sites in the system:
  - Average Risk by Site and Month
  - Vulnerability Counts by Severity and Site Tag

— Vulnerability Counts by Category and Site Tag

- Reports across multiple scans - When you select multiple scans for a report, the data will be combined into one report (rather than generating the same report multiple times).

Scan Visualization

The ability to track the progress of a scan has been greatly enhanced in AMP 8.00. While a scan is running, you can track the following details:

- Vulnerabilities - You no longer need to wait for the scan to complete before obtaining information about discovered vulnerabilities.
- Crawled URL information - Each URL that is crawled is displayed, along with its response time and status code. When the scan is complete, you can see the details for the session (response, request, and additional information, when applicable) and generate a session report.
- Scan log - The Scan log is now visible from the Web console.
- Scan activity - Scan activity messages (showing the time, sensor, user, and sensor host) are available from the Web console.

Vulnerability Details

Vulnerability details can now be viewed from the vulnerability list. When you click the vulnerability name, a bottom-tabbed pane is rendered showing the summary, request, response, tags, and properties associated with the vulnerability. This detail pane is updated as new vulnerabilities are selected in the grid, allowing you to compare a specific detail about multiple vulnerabilities. The vulnerability Properties tab has fields that allow you to mark a vulnerability as false positive or ignored, or to add a note concerning the vulnerability.

Enhancements

- Improved Web Console user interface - Most non-administrative functions have been moved from the AMP Console to the AMP Web Console. There is no longer any shared functionality between the two consoles. In addition, the Web Console has been improved with increased use of AJAX, a new navigation menu, and breadcrumbs.
- Multiple selection for object permissions - The administrator can select multiple objects and set their permissions in one transaction.
- Improved site filters - Sites can now be filtered on tag name values, risk scores, and scan date ranges.
- Improved international support - Input validation now handles Asian character sets.
- Large scan file upload support (Zip-64) - Large scans (greater than 2GB) can now be imported to and exported from AMP.
- Import/Export Site lists in XML - Site lists can now be imported and exported in XML format in addition to CSV format.

2 Installation

Introduction

The Assessment Management Platform comprises the following:

- The AMP server/manager
- The AMP console (which provides the graphical user interface to the system manager)
- The AMP Web console (a browser-based interface to the system manager, designed specifically for non-administrative functions)
- Scanners

Two types of scanners are supported:

- Sensor - This is the WebInspect application when connected to AMP 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 an AMP Manager.
- Client - A client is any HP scanner (WebInspect, QAInspect, or DevInspect) that connects to AMP to receive license, permissions, updates or scan data, and which also presents a user interface through which scans may be conducted. AMP controls permissions for a client and also provides the policies and compliance templates used by clients. A client can be configured to upload scan results to AMP automatically at the completion of the scan or only when specifically instructed by the user.

Typical installations contain one SQL server, one or more consoles, and multiple scanners. These components can be distributed across your network in any way you like, but you must configure at least one of each.

You cannot install this software remotely. You must run the installation program on each server or PC that you intend to integrate into the AMP system, beginning with the SQL server. For that reason, you may prefer to save the installation program to your hard drive and copy it to a CD, or save it to a network location that can be accessed by each machine on which you expect to install a component.

System Requirements

Before installing AMP, make sure that your system meets the minimum requirements listed below.

All Products

- Microsoft .NET 3.5 SP1
- Microsoft Internet Explorer 7.0 or 8.0, or FireFox 2.x or 3.x
- An active Internet or intranet connection

➤ Note: If you are installing software on a machine that does not have an Internet connection, see "If You Are Not Connected to the Internet" on page 17.

AMP Server

- 2 GB of RAM
- 5 GB (remote database) or 20 GB of free disk space (local database)
- 2.5 GHz processor or better
- Microsoft IIS 6.0
- Windows Server 2003 SP1 or Windows Server 2008

AMP Console/Client

- 1 GB of memory
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP SP2 or Windows Server 2003 SP1 or Windows Server 2008 or Windows Vista

AMP Sensor (WebInspect 8)

- 2 GB of memory
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP Professional SP2, Windows Server 2003 Standard SP1, Windows Vista SP1
- SQL Server 2005 Express SP1
- The minimum screen resolution for WebInspect is 1024 x 768. For best performance, use a screen display of 1280x1024.

AMP Database

- 2 GB of RAM
- 20 GB of free disk space
- 2 GHz processor or better
- Microsoft SQL Server 2005
- Windows Server 2003 SP1

For an AMP environment to support Internet Protocol version 6 (IPv6), the IPv6 protocol must be deployed on each AMP Console, AMP Sensor, and the AMP Manager.

Upgrading from Previous Versions

Observe the following guidelines if you are upgrading from a previous version of AMP.

- AMP 8.00 does not support versions of WebInspect prior to 7.0 and requires WebInspect 8.00 in order to support AMP's new scan visualization feature.
- Make a back-up copy of your database.
- The AMP 8.00 database must be installed on the same database server used by previous installations, but AMP 8.00 no longer supports SQL Server 2000. Therefore, you must either upgrade your existing SQL Server 2000 installation to SQL Server 2005 or you must migrate your AMP 3.x database to a SQL Server 2005 instance. To migrate your existing database, first make a backup and then restore the backup on a computer running SQL Server 2005.
- Before upgrading, use your SQL Server configuration tools to confirm that the hard drive on your database server contains free space equal to at least 3-4 times the size of your existing database. This is because you need to have room for the new database and about 2-3 times the database size for the SQL Server transaction log. For example, if you have a 30 GB AMP 3.x database, then you will need at least 90-120 GB of free disk space for the upgrade to succeed. Once the upgrade has succeeded, you should be able to shrink your new database’s transaction log to a more reasonable size.
- Side-by-side installation with AMP 3.x is not permitted. Therefore, when upgrading from version 3.x, the installation will automatically uninstall the previous AMP installation and will populate default configuration settings with the data that was specified during the previous AMP installation. The installation will walk you though the process of upgrading your existing AMP 3.x database. The data stored in your AMP 3.x database will remain intact, because it basically migrates the data to a new database.
- The AMP 8.00 reporting infrastructure is greatly improved from AMP 3.x. AMP 3.x Report Graphics no longer exist and Report Templates are vastly different in AMP 8.00. The AMP 3.x Report Graphics' Cover and Page images will be upgraded to AMP 8.00 Report Resources and the Cover Header and Footer text will be stored as “Master Template” report definition parameters in custom Report Templates. The Company Name and Page footer text is no longer used by the reporting code, so this information will not migrated. In AMP 8.00, Report Templates basically combine selected report definitions with the user-specified report definition parameters. Therefore, on upgrade, many AMP 8.00 Report Templates will be created combining the selected AMP 3.x Report Graphics and Report Templates. Each Scan, Discovery Scan, Schedule Scan, Schedule Discovery Scan, Report Template and custom run report will create a unique AMP 8.00 Report Template.
- The AMP 3.x Developer Reference, Comparison, and Scan Log reports are no longer available and Attack Status report sub-options are not upgraded.
- Existing AMP 3.x reports will be saved and you can still download and view the report, but they cannot be viewed interactively or exported to different formats like the AMP 8.00 reports. To support this, these reports must be rerun.

Server/Manager Installation

When installing components on different machines, begin with the machine on which the server/manager will be installed.

Install the server on one machine only.

1 Start the installation program.

2 On the Welcome page, click **Next**.

3 Review the license agreement. If you accept, select the check box and click **Next**; otherwise click **Exit**.

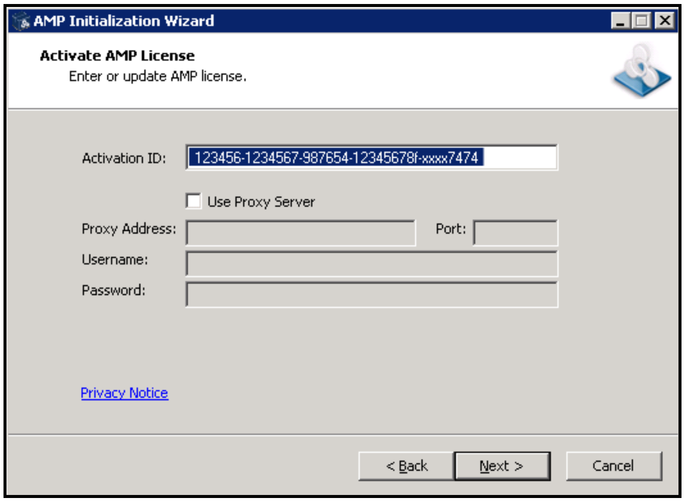
4 Select the folder into which you want to install the software and click **Next**.

5 When ready to install, click **Install**.

6 After installation, click **Finish**.

7 When the Initialization Wizard appears, click **Next**.

8 Enter the Activation ID sent to you by HP.



AMP Initialization Wizard

Activate AMP License

Enter or update AMP license.

Activation ID: 123456-1234567-987654-12345678f-xxxx7474

□ Use Proxy Server

Proxy Address: Port:

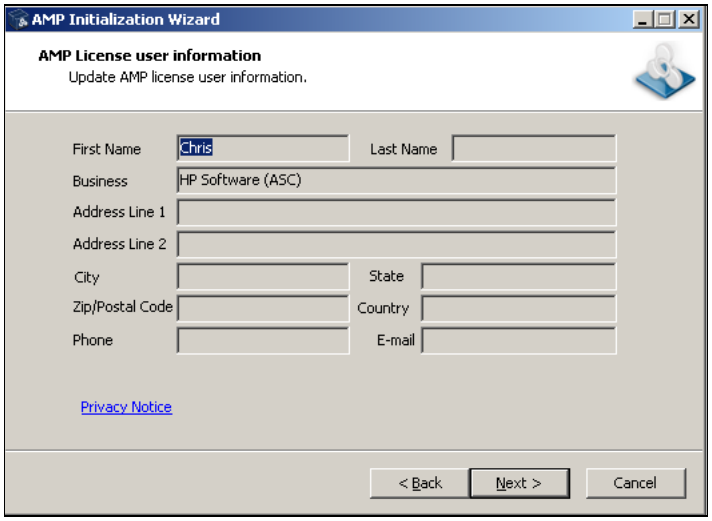
Username:

Password:

9 If using a proxy server, select **Use Proxy Server** and provide the requested information.

10 Click **Next**.

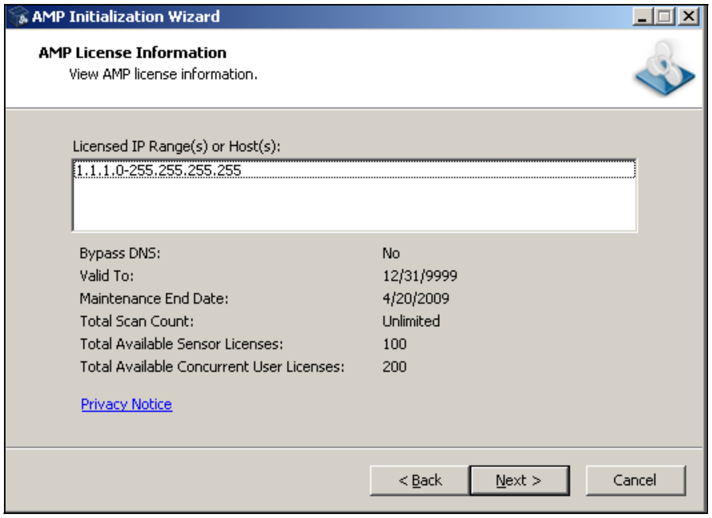
The *AMP License User Information* window displays user information as submitted to HP.


AMP Initialization Wizard
AMP License user information
Update AMP license user information.
Privacy Notice
< Back
Next >
Cancel

First Name	Chris	Last Name	
Business	HP Software (ASC)		
Address Line 1			
Address Line 2			
City		State	
Zip/Postal Code		Country	
Phone		E-mail	

11 Click **Next**.

The *AMP License Information* window displays information about the license token.



Licensed IP Range(s) or Host(s):

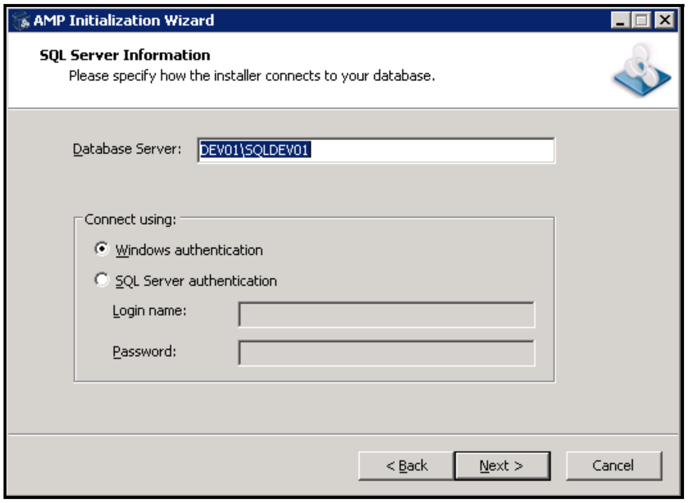
1.1.1.0-255.255.255.255

Bypass DNS:	No
Valid To:	12/31/9999
Maintenance End Date:	4/20/2009
Total Scan Count:	Unlimited
Total Available Sensor Licenses:	100
Total Available Concurrent User Licenses:	200

12 Click **Next**.

13 On the SQL Server Information panel, enter the name of the SQL Server and select the authentication method that will be used. If you are upgrading from an AMP 3.5 database, you must have at least “read access” to the database. If you are installing AMP 8.00 for the first time, then you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).

Note: SQL Server 2000 is no longer supported. If upgrading, you must migrate the database to SQL Server 2005.



AMP Initialization Wizard

SQL Server Information

Please specify how the installer connects to your database.

Database Server: DEV01\SQLDEV01

Connect using:

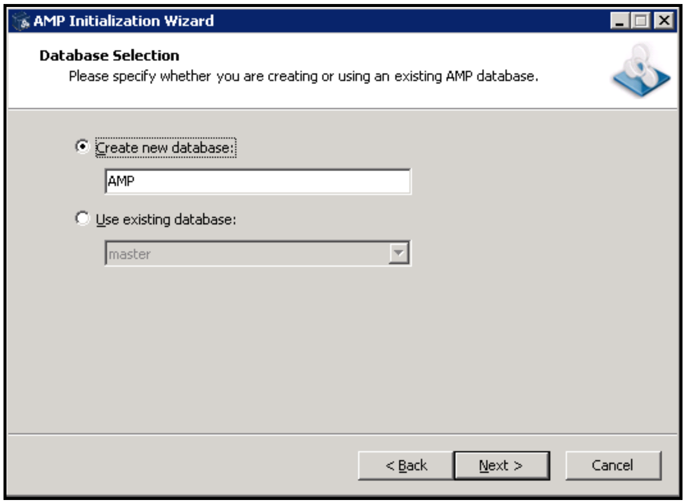
● Windows authentication

○ SQL Server authentication

Login name:

Password:

14 Click **Next**.



AMP Initialization Wizard

Database Selection

Please specify whether you are creating or using an existing AMP database.

● Create new database: AMP

○ Use existing database: master

15 On the *Database Selection* window:

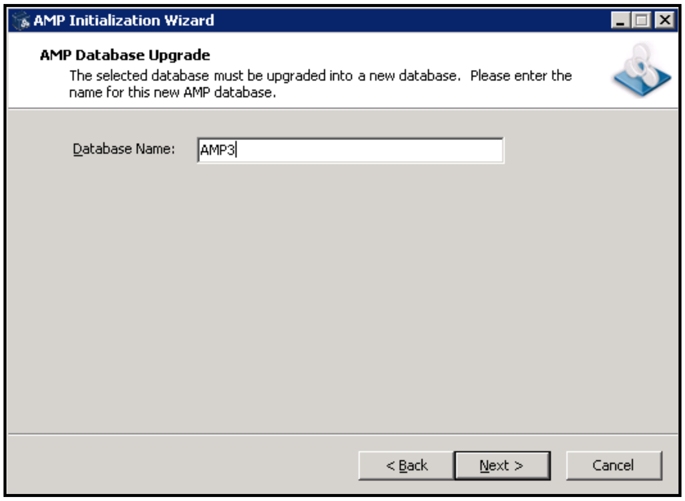
a Choose one of the following:

— To use a new database, select **Create new database** and enter the database name. You must have privileges to create this database.

— To upgrade from an AMP 3.5 database or to select a previous installation of AMP 8.00, select **Use existing database** and select one from the list. You must have owner privileges for that database.

b Click **Next**.

16 For an existing database only, the *AMP Database Upgrade* window appears. Enter a name for the new database and click **Next**.

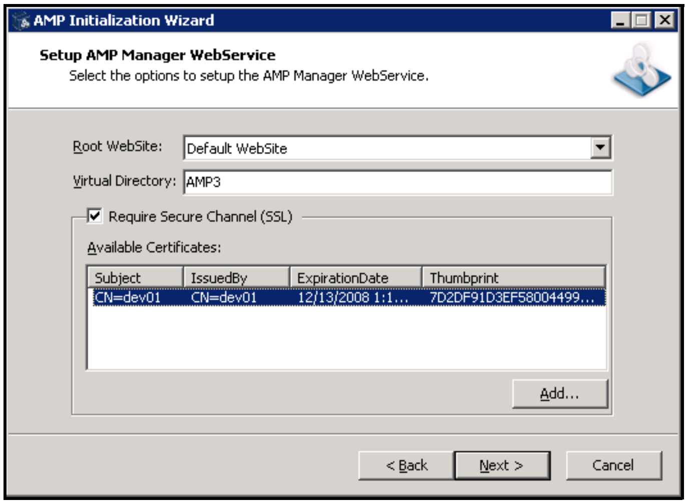


AMP Database Upgrade

The selected database must be upgraded into a new database. Please enter the name for this new AMP database.

Database Name: AMP3

17 On the *Setup AMP Manager WebService* window, enter the root Web site and the name of the IIS virtual directory.



Setup AMP Manager WebService

Select the options to setup the AMP Manager WebService.

Root WebSite: Default WebSite

Virtual Directory: AMP3

☑ Require Secure Channel (SSL)

Available Certificates:

Subject	IssuedBy	ExpirationDate	Thumbprint
CN=dev01	CN=dev01	12/13/2008 1:1...	7D2DF91D3EF58004499...

⚠ Caution: If you are upgrading, do not choose the same IIS Virtual Directory name used for previous AMP installations.

If you select **Require Secure Channel (SSL)**, add and/or select an SSL certificate. For security reasons, HP recommends that you use SSL.

These entries create the URLs for the:

AMP Console:

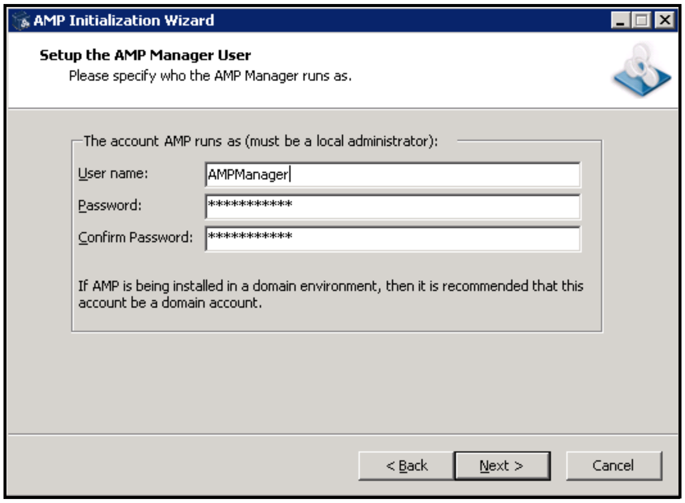
http(s)://<AMP server computer name>/<virtual directory name>/

AMP Web Console:

http(s)://<AMP server computer name>/<virtual directory name>/WebConsole

18 Click **Next**.

19 On the *Setup the AMP Manager User* window, enter the local or domain user account that you want to associate with the AMP Manager Web Service. For AMP to work properly, this account must be a local administrator. This enables the AMP Manager to install service packs and patches released by HP.



AMP Initialization Wizard

Setup the AMP Manager User

Please specify who the AMP Manager runs as.

The account AMP runs as (must be a local administrator):

User name: AMPManager

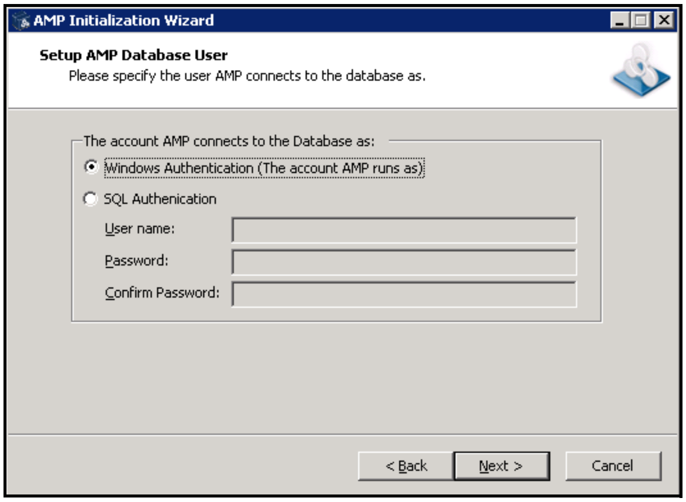
Password: ************

Confirm Password: ************

If AMP is being installed in a domain environment, then it is recommended that this account be a domain account.

20 Click **Next**.

21 On the *Setup AMP Database User* window, specify how the AMP Manager should connect to the AMP database.



AMP Initialization Wizard

Setup AMP Database User

Please specify the user AMP connects to the database as.

The account AMP connects to the Database as:

● Windows Authentication (The account AMP runs as)

○ SQL Authenication

User name:

Password:

Confirm Password:

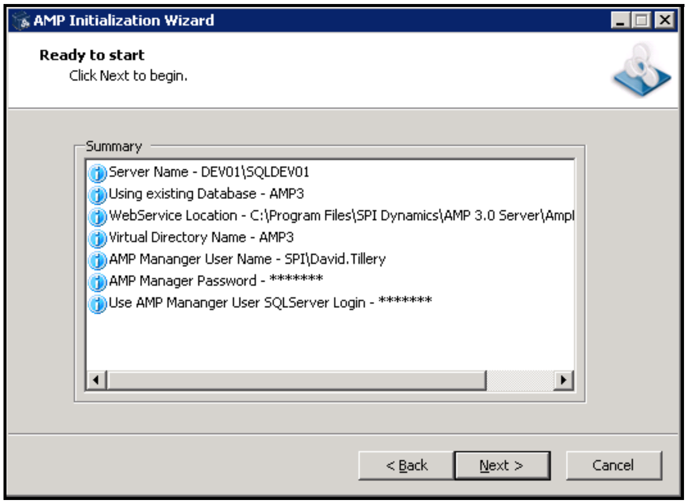
- **Windows Authentication -** The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the AMP Server and the database computers.
- **SQL Authentication -** Enter the SQL server user name and password.

22 Click **Next**.

23 On the *Ready To Start* window, verify your previous choices.

- To change settings, click **Back**.

- To begin configuration, click **Next**. The program creates and populates the database, and initializes other database and system components.



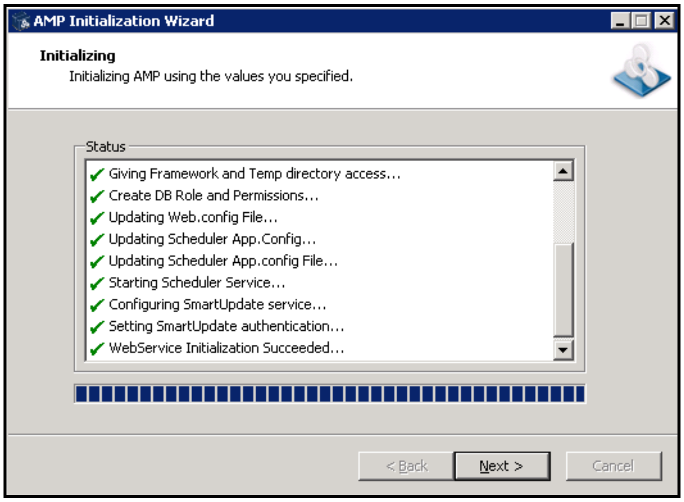
Ready to start

Click Next to begin.

Summary

Server Name - DEV01\SQLDEV01
Using existing Database - AMP3
WebService Location - C:\Program Files\SPI Dynamics\AMP 3.0 Server\Ampl
Virtual Directory Name - AMP3
AMP Manager User Name - SPI\David.Tillery
AMP Manager Password - *******
Use AMP Mananger User SQLServer Login - *******

24 The program displays the initialization results. Click **Next**.



Initializing

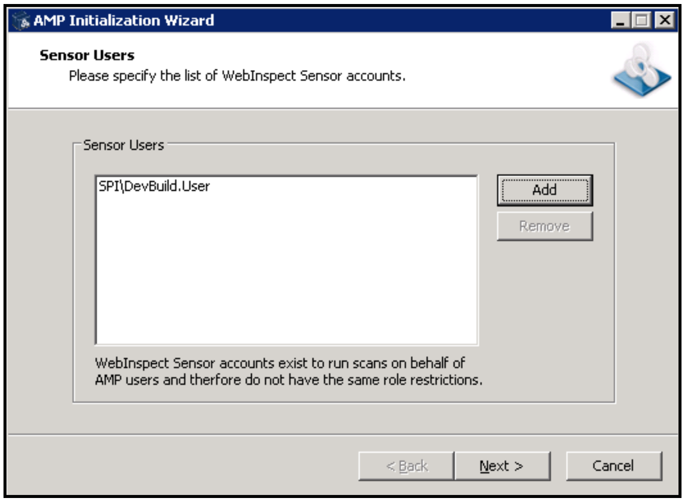
Initializing AMP using the values you specified.

Status

✓ Giving Framework and Temp directory access...
✓ Create DB Role and Permissions...
✓ Updating Web.config File...
✓ Updating Scheduler App.Config...
✓ Updating Scheduler App.config File...
✓ Starting Scheduler Service...
✓ Configuring SmartUpdate service...
✓ Setting SmartUpdate authentication...
✓ WebService Initialization Succeeded...

25 On the *Sensor Users* window, click **Add** and enter the user accounts that will be associated with the sensors (WebInspect 8.00 installations).

If you are upgrading from AMP 3.5, the accounts listed as sensor users are those that previously were assigned to the “Act as a Sensor” role. This role has been removed from AMP 8.00.


AMP Initialization Wizard

Sensor Users

Please specify the list of WebInspect Sensor accounts.

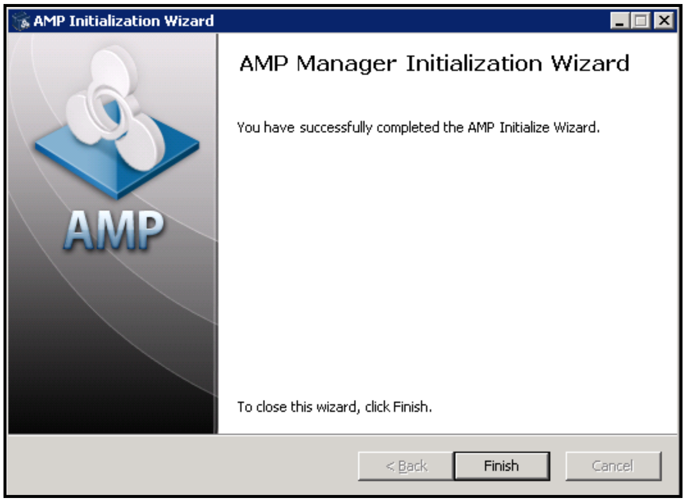
Sensor Users

SPI\DevBuild.User

WebInspect Sensor accounts exist to run scans on behalf of AMP users and therfore do not have the same role restrictions.

26 Click **Next**.

27 When installation is complete, the following window appears. Click **Finish**.


AMP Initialization Wizard

AMP Manager Initialization Wizard

You have successfully completed the AMP Initialize Wizard.

To close this wizard, click Finish.

Console Installation

Use the following procedure to install the AMP console.

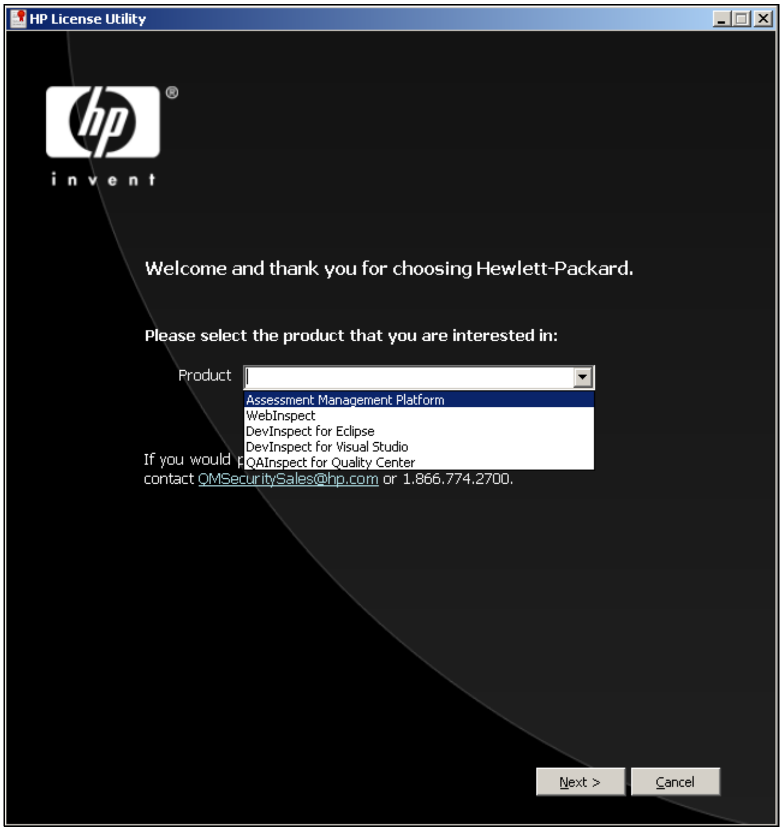
1. Start the installation program.
2. On the Welcome page, click **Next**.
3. Review the license agreement. If you accept, select **I accept the terms in the License Agreement** and click **Next**; otherwise click **Cancel**.
4. Select the folder into which you want to install the software and click **Next**.
5. Click **Install**.
6. When the process is complete, click **Finish**.

If You Are Not Connected to the Internet

HP provides an offline licensing tool for use when installing software on a machine that does not have an Internet connection. You will create a file containing information about the computer and transfer the file to a portable device (diskette or flash drive). You will then go to an Internet-connected computer and run a program that will transmit the file to an HP server, which will download a license file that you can copy and install on the computer that is not connected to the Internet.

1. Collect the machine-specific information from the isolated machine using the following steps.
   - a. Close all HP applications. Also close Visual Studio, if present.
   - b. Run C:\Program Files\HP\AMP Server\AmpInitialize\LicenseUtilitySetup.exe. This installs the License Utility.
   - c. Run the License Utility: Click **Start** → **All Programs** → **HP** → **HP License Utility** → **HP License Utility**.

d For the **Product** field, select **Assessment Management Platform** and click **Next**.



HP License Utility

Welcome and thank you for choosing Hewlett-Packard.

Please select the product that you are interested in:

Product

If you would p

contact QMSecuritySales@hp.com or 1.866.774.2700.

invent
Assessment Management Platform
WebInspect
DevInspect for Eclipse
DevInspect for Visual Studio
QAInspect for Quality Center
Next >
Cancel

e Select “Prepare a license request on a non-Internet connected PC” and click **Next**.

f Paste or type in the activation token that was sent via e-mail.

g Enter a description, such as “Trial License Mar 2007" or “Security Team Workstation #4.”

h Click **Finish** to proceed with the data collection.

i In the resulting Save As dialogue, direct the application on where to save the output file Assessment Management Platform_LicenseReq.xml.

2 Transfer the following files to a new, temporary directory on another machine that has Internet access. This process may involve a USB drive, floppy diskette, CD-RW, etc. The default location for these files is

C:\Program Files\HP\HP AMP 8.00 Server\AMPInitialize.

- Assessment Management Platform_LicenseReq.xml
- LicenseUtilitySetup.exe

3 Activate the trial license from the Internet-connected machine and save the license output file. The tool connects to the HP licensing portal, activates the appropriate license token, and builds an updated Assessment Management Platform_LicenseReq.xml file.

a Run LicenseUtilitySetup.exe.

b In the utility, select “Request a license from the SPI license service using a previously prepared request” and click **Next**.

c Leave the Web Service URL field at its default value: https://download01.spidynamics.com/LicenseService/service.asmx

- d For the **PC Information File** field, browse to the Assessment Management Platform_LicenseReq.xml file that was moved back to this machine.
- e For the **License Path** field, direct the application on where to save the output file Assessment Management Platform_LicenseReq.xml.
- f Click **Finish**.

4 Transport the new Assessment Management Platform_LicenseReq.xml back to the isolated machine via USB Drive or other device. The LicenseUtilitySetup.exe may be left behind or deleted. For each product, the destination location is similar, but follows the examples below. A zero-byte XML file may already exist with this name in the destination folder. As a general safety practice, this older copy should be renamed or otherwise backed-up prior to applying the new XML file. AMP: C:\Documents and Settings\All Users\Application Data\SPI Dynamics\Licenses\Amp

5 Launch the now-licensed application on the isolated machine. With its updated Assessment Management Platform_LicenseReq.xml file, it is now running with an activated token. This may be verified in the following location: AMP Console...Administration > Licensing

➤ Note: Searching your hard drive for the pre-existing Assessment Management Platform_LicenseReq.xml file may be complicated by Microsoft's default omission of hidden directories. Be sure to enable this feature.

Sensor Installation

Use the following procedure to install WebInspect as a sensor. For client installation, refer to the WebInspect, DevInspect, or QAInspect User Manuals.

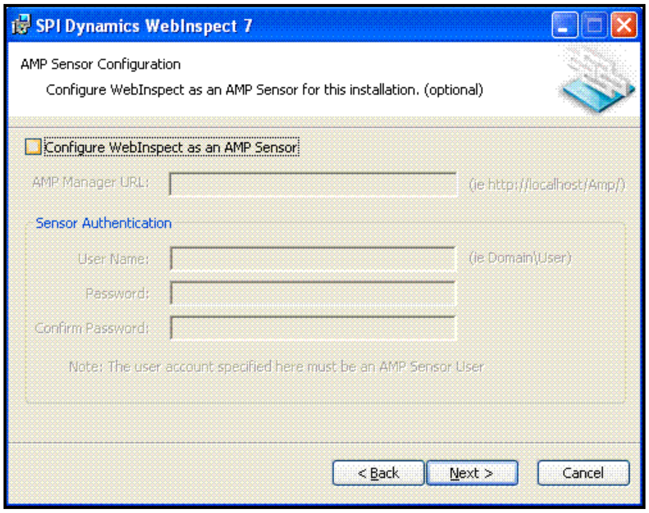
1 Start the installation program.

2 On the Welcome page, click **Next**.

3 Review the license agreement. If you accept, select **I accept the terms in the License Agreement** and click **Next**; otherwise click **Cancel**.

4 Select the folder into which you want to install the software and click **Next**.

The *AMP Sensor Configuration* window appears.



SPI Dynamics WebInspect 7

AMP Sensor Configuration

Configure WebInspect as an AMP Sensor for this installation. (optional)

□ Configure WebInspect as an AMP Sensor

AMP Manager URL: (ie http://localhost/Amp/)

Sensor Authentication

User Name: (ie Domain\User)

Password:

Confirm Password:

Note: The user account specified here must be an AMP Sensor User

5 Select **Configure WebInspect as an AMP Sensor.**

6 Enter the URL of the AMP manager.

7 In the **Sensor Authentication** group, enter the Windows account credentials for this sensor. Be sure to add this account to the list of sensor users using the AMP Administration module.

8 Click **Next**.

9 When ready to install, click **Install**.

10 When the process is complete, click **Finish**.

Time Stamping and Scheduling

There may be installations where the manager and the console reside in different time zones. To accommodate this, the AMP manager uses Coordinated Universal Time (also known as Greenwich Mean Time or Zulu time) for all time storage and manipulation. When a time is to be displayed on the console, the manager converts the time to conform to the time zone in which the console resides. Alert e-mails and reports, however, are time-stamped according to the zone in which the manager resides.

Universal Time does not honor daylight saving time. Therefore, scheduled scan times will change by one hour after the transition between daylight saving time and standard time. To illustrate, suppose you schedule a scan to occur daily at 4 P.M. and you are in the Eastern time zone of the United States during the daylight saving time period. The AMP manager records the settings and will begin the scan each day at 8 P.M. Universal Time (which is the equivalent of 4 P.M. Eastern daylight time). However, when the transition to standard time occurs, your scheduled scan will begin at 3 P.M. local time instead of 4 P.M. Even though you set your clocks back one hour, the Universal Time continued unchanged.

3 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 in a scan report and will attempt to delete the 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 “CreatedBySPIDynamics.”

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 a 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) 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 an assessment, 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.

4 Getting Started

Introduction

After installing the AMP software, allow the AMP server to initialize its database, and then perform the following tasks to configure your system and prepare the installation for scanning.

Log On

The windows account of the person who installs the AMP console software is assigned, by default, to the role of security administrator. This role is granted all permissions with no IP restrictions. No one else can log on until the security administrator assigns other users to roles.

1. Start the AMP Console.

   The *Log On to AMP* dialog appears.

2. On the **Log On** tab, select an AMP manager from the **Log on to** list.

3. Select one of the following logon options:

   a. To log on using your Windows user account, select **Log on as the current Windows user**.

   b. To use a different account, select **Log on as**, then enter the user name and password for an account that has permission to access the console. For new installations, use the account name and password of the user who installed the AMP server software. This user is permitted to perform all restricted functions.

4. If you select **Automatically log on when this application starts**, users are logged on with their Windows account, bypassing the logon dialog.

5. To go through a proxy server to reach the AMP manager:

   a. Click the **Proxy** tab.

   b. Select one of the following:

      – **Use the Internet Explorer proxy**.

      – **Use the proxy below**, and then provide the proxy server's IP address and port number.

   c. Provide a valid user name and password.

6. Click **OK**.

Note: If you see the message "The AMP Server refused the request," you may have entered your user name and password incorrectly, or your account has not been assigned to a role.

Configure the Console

After installing a license, you can specify settings for the console.

To specify console settings:

1. From the **Tools** menu, select **Options**.

   The *Options* window opens.

2. To refresh the display of AMP information periodically, select **Automatically refresh display** and specify how often (in seconds) the display should be updated.

3. Click **OK**.

Create Roles for Users

A role is simply a named collection of permissions. You can allow other users to access the AMP console and limit the functions they are allowed to perform by assigning them to a role.

The Roles form contains the name and description of each role defined for the system. When installed, the Assessment Management Platform is configured with the following built-in roles.

- **Security Administrator**: Granted all permissions with no IP restrictions. The user account of the person who installed the AMP software is assigned to this role. The Administrator can change the default permissions assigned to the Security Technician and the Manager.
- **Security Technician**: Granted permission to perform all functions except for policy modifications. The administrator must edit the IP ranges if IP restrictions on this role are desired.
- **Manager**: Granted permission to perform all functions except for starting scans and modifying policies. The administrator must edit the IP ranges if IP restrictions on this role are desired.

Permissions

The AMP manager determines a user’s accessibility to functions and objects based on permissions granted to the role to which the user is assigned. It evaluates those permissions according to the following hierarchical criteria.

- The user who creates an object is awarded ownership and has full control over that object, regardless of the permissions associated with the role to which he is assigned. Note that ownership can be reassigned, however.
- Next, the AMP manager examines permissions for the roles to which the user is assigned. If no “allow” permissions are granted, then the user has no access.
- If the user is assigned to multiple roles and if one role has an “allow” permission for a certain function while one of the other roles has neither “allow” nor “deny” permissions for that same function, then the user is granted access. However, if one role has an “allow” permission and another role has a “deny” permission for the same function, then the user is denied access. The “deny” permission nullifies any “allow” permission.

Default Roles and Permissions

An administrator may configure the system to award permissions for new objects based on the role of the user who created the object. For example, when users in role A create objects, users in role B might be able to view (but not delete) these objects.

To accommodate users who are assigned to multiple roles, you can designate one role as the default. The AMP manager then uses this default role to assign permissions to objects created by that user.

However, due to the extreme flexibility of the AMP configuration, the AMP manager theoretically may be unable to determine a user's default role. If this occurs, then if the user who created the object:

- Is assigned to the role that has been designated as the system default, the AMP manager assigns permissions based on the system default role.
- Is not assigned to the system default role, only the user has "allow" permissions for the object.

Create or Modify Roles

Use the following procedure to create, delete, or modify roles.

1. Click the **Administration** group.
2. Select the **Roles and Permissions** shortcut.

   The Roles form contains the name of each role defined for the system.
3. To delete a role:
   a. Select a role in the Roles form.
   b. Click **Action** (or right-click a role) and select **Delete Role** from the menu.
   c. When prompted to confirm the action, click **Yes**.
4. To add a role:
   a. Click **Action** (or right-click the Roles pane) and select **Add Role** from the menu.

      The *New Role* dialog box appears.
   b. Type a name in the **Name** box and click **OK**.
5. To modify permissions for a role:
   a. Select a role in the Roles form.

      Example: Select **Manager**.
   b. Select an item in the Role Permissions pane (expanding categories, if necessary).

      Example: Expand the **Scans Options and Settings** group and select **Scan Templates**.
   c. Select either **Allow** or **Deny** for each of the permissions associated with the selected object type.
   d. Repeat steps b-c until all permissions have been assigned.

In this example, anyone assigned to the Manager role will be allowed to interact with new Scan Templates (regardless of who creates them) according to the allow/deny permissions you select.

You can also restrict access to existing objects (a particular Scan Template, in this example).

To restrict object access:

1. Select a Role and a Role Permissions object.
2. Select an existing instance an the object from the **Securable Objects** list.

   Example: If you select **Scan Templates**, all existing Scan Templates are listed under **Securable Objects**.
3. Select either **Allow** or **Deny** for each of the permissions associated with the selected object type.
4. Repeat steps 2-3 until all permissions have been assigned.
5. To reassign ownership of the object, click the browse button in the **Security Properties** area (at the bottom of the pane).

Example Role Permissions

Use the following procedure to set permissions for a role with minimal authority.

1. Select the **Administration** group.
2. Click the **Roles and Permissions** shortcut.
3. If necessary, create a role.
   a. Click **Action** and select **Add Role**.
   b. Enter a role name.
   c. Click **OK**.
4. Select a role.
5. Allow role to create scans:
   a. In the Role Permissions pane, expand the Scan Options and Settings group.
   b. Select Scans.
   c. Select **Allow** for the following permissions:
      – Create
      – Create Priority Level 1 Scan
      – Create Priority Level 2 Scan
      – Create Priority Level 3 Scan
      – Create Priority Level 4 Scan
      – Create Priority Level 5 Scan
      – Create Custom Scan

      Note: If you do not want to allow users in this role to create custom scans, you must create scan templates; then, to grant access to a specific template, you must select the template (in the Securable Objects pane) and select **Allow** for the permission “Can be viewed.”
6. Create a site permission:
   a. Click **Action**.
   b. Select **Add Site Permission**.

c. Enter a host name, a single IP address, or a range of IP addresses.

d. Click **OK**.

7. Allow role to access sites specified in a site permission object:

a. In the Role Permissions pane, expand the Site Permissions group.

b. Select one of the entries.

c. For the permission "Run Scan," select **Allow**.

d. For the permission "Renerate Report," select **Allow**.

8. Allow role to create reports:

a. In the Role Permissions pane, expand the Reports group.

b. Select Reports.

c. For the permission "Create" select **Allow**.

9. Allow role to use or create report resources:

a. In the Role Permissions pane, expand the Reports group.

b. Select Report Resources.

c. For the permission "Create," select **Allow**.

10. Allow role to use or create report templates:

a. In the Role Permissions pane, expand the **Reports** group.

b. Select **Report Templates**.

c. For the permission "Create," select **Allow**.

d. To use existing templates:

— Select the **Report Templates** shortcut under **Roles and Permissions**.

— Select a template listed on the Report Templates form.

— Click **Action** and select **Edit Permissions**.

— Select a role.

— For the permission "View," select **Allow**.

Assign Users to Roles

Use the following procedure to assign a user to a role.

1. Click the **Administration** group.
2. Select the **Roles** shortcut.
3. Select a role.
4. Click **Actions** (or right-click the role) and select **Add User to Role** from the menu.

   The *Select Users Or Groups* dialog appears.
5. Select a domain or workgroup from the **From this location** list.
6. In the text box below, type a Windows account name.
7. To verify the name, click **Check Names**.
8. Click **OK**.

Alternatively, you can select from a list of account names.

After selecting a domain or workgroup:

1. Click **Advanced**.
2. Select a location.
3. Click **Find Now** to return a list of all accounts associated with the selected location. To filter the list, use the controls in the **Search Criteria** group first.
4. Select one or more accounts or groups and click **OK**.

➤ Note: 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.

Assign Default Role to User

A user's default role determines how permissions are assigned to objects created by that user. If the user is a member of only one role, the permissions of that role are assigned to the object. However, if the user is assigned to multiple roles, the AMP manager must be able to select the appropriate permission set.

Normally, the AMP manager can resolve this issue by analyzing permissions of the roles to which the user is assigned. Sometimes, however, this is not possible. Therefore, you should assign a default role to any user who is a member of more than one role.

1. Select the **Administration** group.
2. Click the **Roles** shortcut.
3. In the Roles pane, click the plus sign ⊞ next to the name of a role to display the user accounts in that role.
4. Select a user account.
5. Select a role from the **Assigned Default Role** list.

Set E-mail Options

If you want the AMP manager to send e-mail alerts whenever certain events occur, follow the steps below to specify e-mail settings:

1. Click the **Administration** group.
2. Click the **E-mail Alerts** shortcut.
3. Click the **SMTP Settings** tab (at the bottom of the form).
4. In the **SMTP Server** box, enter the name of the server used for outgoing e-mail.
5. In the **SMTP Port** box, enter the numbered port used for outgoing e-mail.
6. In the **Sender** box, enter the text that will be appear in the “From” field of the e-mail, followed by the actual e-mail address.

   Example: AMP System Message <jdoe@mycompany.com>
7. Select the **Use SSL** check box if you want to use Secure Sockets Layer (SSL) protocol.
8. To enforce authentication, select **Basic** or **NTLM** and supply a user name and password.
9. Click **Save**.

Enable E-mail Alerts

You can force the AMP manager to send an e-mail message to someone whenever certain events occur.

Use the following procedure:

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 form and select **Add** from the shortcut menu.
   b. Enter the e-mail address of the person who should receive the alert.
   c. If the alert should be sent only when selected actions occur related to a specific host, 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.

      Leave this field blank to allow alerts for all hosts or IP addresses.
   d. Select one or more actions.
4. To edit an alert:
   a. Select an entry in the E-mail Alerts form.

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

5. To delete an alert:

   a. Select an entry in the E-mail Alerts form.

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

6. Click **OK**.

Set SNMP Options

If you want the AMP manager to send SNMP alerts whenever certain events occur, follow the steps below to specify settings:

1. Click the **Administration** group.
2. Click the **SNMP Alerts** shortcut.
3. Click the **SNMP Settings** tab (at the bottom of the form).
4. In the **SNMP Host** box, enter the IP address of the server that will receive the alert and forward it to the intended recipient.
5. In the **SNMP Port** box, enter the port number for SNMP alerts on the SNMP host.
6. In the **Community** box, enter an SNMP community. A 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.

7. Click **Save**.

Enable SNMP Alerts

You can force the AMP manager to send a Simple Network Management Protocol (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 form and select **Add** from the shortcut menu.

b Enter a name for this alert in the **Name** box.

c If the alert should be sent only when selected actions occur related to a specific host, 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.

Leave this field blank to send e-mail alerts regardless of the host or IP address associated with the action.

d Select one or more actions that will trigger the alert.

4 To edit an alert:

a Select an entry in the SNMP Alerts form.

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

5 To delete an alert:

a Select an entry in the SNMP Alerts form.

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

6 Click **OK**.

You must also configure the SNMP settings on the SNMP Alerts form in the **Administration** group.

Create Allowed Paths

When users start a scan manually, the scan results are automatically saved to a directory on their hard drive. For a scheduled scan, however, you must create a list of locations where users can save scan results or exported reports. These locations are used only for scheduled scans.

To add a path:

1 Select the **Action** menu and click **Add Allowed Path**.

The program adds a path to the list.

2 Right-click the path and select **Edit** from the shortcut menu.

3 Edit the entry to create a new path.

The entry must conform to the Universal Naming Convention. The Universal Naming Convention (also known as Uniform Naming Convention) is a PC format for specifying the location of resources on a local-area network (LAN). UNC uses the following format:

\\server-name\shared-resource-pathname\...\shared-resource-pathname

For example, if you wanted to schedule a scan and save the generated report in a directory named reports which is a subdirectory of WebSiteA on the shared server named absmith, you would write the allowed path as:

\\absmith\WebSiteA\reports

To delete a path:

1 Select a path from the list.

2 Click the **Action** menu and select **Delete**.

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

Perform a Smart Update

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

Use Smart Update to download SPI Dynamic's latest adaptive agents and programs, as well as vulnerability and policy information.

You should update your Assessment Management Platform each time you use it, or you can schedule a Smart Update to occur unattended outside normal working hours.

To manually initiate an update of your SecureBase vulnerabilities database:

1 On the AMP console toolbar, click **Smart Update**.

2 When a message displays indicating that the process has started, click **OK**.

To schedule a Smart Update:

1 Select the **Administration** group.

2 Click the **Smart Update** shortcut.

3 Select **Add** from the **Action** menu.

4 When the *Smart Update Settings* dialog appears, select each category in the left column and provide the requested information. For detailed assistance, see the Help file for each settings category.

5 When all the settings are configured to your liking, click **OK**.

Smart Update through a Proxy Server

Use the following procedure if you need to use a proxy server to communicate with the HP Smart Update database.

Important: Smart Update functions properly only with a standard HTTP proxy server.

1 Select the **Administration** group.

2 Click the **SmartUpdate** shortcut.

3 Select **Use Proxy Server for Smart Update**.

4 In the **Server** box, type the URL or IP address of your proxy server.

5 In the **Port** box, enter the port number (for example, 8080).

6 If your proxy server requires authentication, enter a user name and password.

7 Click **Save**.

5 AMP Console

The Assessment Management Platform presents two separate user interfaces:

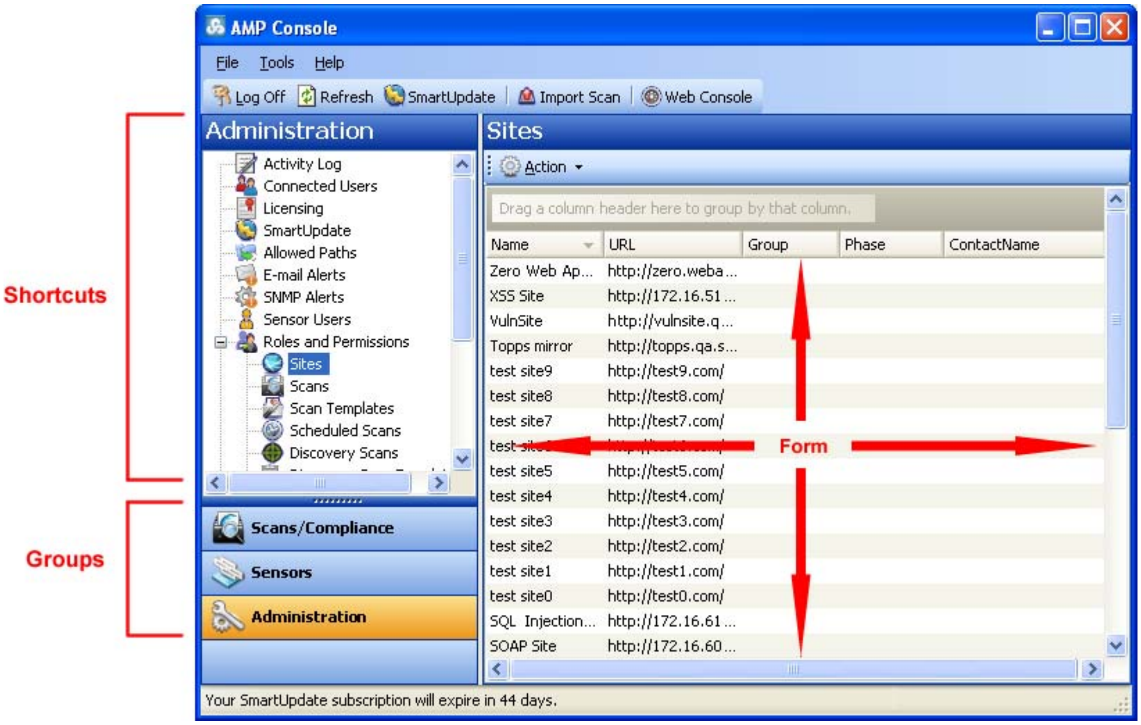
- The AMP Console, used for administrative and security functions.
- The AMP Web Console, a browser-based application used for running and managing scans.

This chapter describes the AMP Console.

The AMP Console user interface comprises five main areas:

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

The buttons in the Group pane represent groups of AMP functions. Click a group to expose available shortcuts. Click a shortcut to display a form containing a list of objects.



Name	URL	Group	Phase	ContactName
Zero Web Ap...	http://zero.weba...			
XSS Site	http://172.16.51...			
VulnSite	http://vulnsite.q...			
Topps mirror	http://topps.qa.s...			
test site9	http://test9.com/			
test site8	http://test8.com/			
test site7	http://test7.com/			
test site6	http://test6.com/			
test site5	http://test5.com/			
test site4	http://test4.com/			
test site3	http://test3.com/			
test site2	http://test2.com/			
test site1	http://test1.com/			
test site0	http://test0.com/			
SQL Injection...	http://172.16.61...			
SOAP Site	http://172.16.60...			

Your SmartUpdate subscription will expire in 44 days.

In the above illustration, the user selected the **Administration** group and then clicked the **Sites** shortcut under Roles and Permissions to display a form containing a list of all sites.

The Group pane contains the following buttons:

Button	Associated Shortcuts
Scans/Compliance	Scan Queue Scan Policies Compliance Templates
Sensors	Sensors
Administration	Activity Log Connected Users Licensing Smart Update Allowed Paths E-Mail Alerts SNMP Alerts Sensor Users Roles and Permissions • Sites • Scans • Scan Templates • Scheduled Scans • Discovery Scans • Discovery Scan Templates • Scheduled Discoveries • Reports • Report Templates • Report Resource • Report Definitions • Blackouts Risk Level Proxy Server Settings

You can initiate commands related to the list or to the individual objects on the 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 on the permissions granted to you by your assigned role.

Scans/Compliance Group

The **Scans/Compliance** group contains three shortcuts:

- Scan Queue
- Scan Policies
- Compliance Templates

Scan Queue

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

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, seeRoles and Permissions on page 51.

The commands are:

Command	Definition
Stop	Abort 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 AMP database.
Edit Permissions	Specify permissions for the selected scan request. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.
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 B, Policies and Components, 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
View	View the selected policy. You must install Microsoft SQL Server Express SP1 before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager.
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 WebInspect unit.
*Export	Export a policy to a standalone WebInspect unit. Prepackaged policies cannot be exported.
Edit Permissions	Specify permissions for the selected scan policy. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

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

Compliance Templates

This form lists all compliance templates configured in your environment. For each template, the list specifies the name, product, system, and the date it was last updated. A check mark in the **System** column indicates that the template is one of the prepackaged templates distributed with AMP (as opposed to a template customized by the user).

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

➤ Note: You must install Microsoft SQL Server Express SP1 before you can edit or view compliance templates.

The commands are:

Command	Definition
View	View a template.
Copy	Copy the selected template.
Delete	Remove the selected template from the repository, unless the policy has "read only" status.
Rename	Change the template name; used for creating a custom template.
*Import	Import a template from a standalone WebInspect unit.
*Export	Export a template to a standalone WebInspect unit.
Edit Permissions	Specify permissions for the selected scan policy. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

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

The available templates are described below:

21CFR11

Part 11 of Title 21 of the United States Code of Federal Regulation (commonly abbreviated as "21 CFR 11") includes requirements for electronic records and electronic signatures. To assist medical companies in compliance, the US Food and Drug Administration (FDA) has published guidance for the proper use of electronic records and electronic signatures for records that are required to be kept and maintained by FDA regulations. The guidance outlines "criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."

Due to the law and FDA guidance, medical companies and organizations dealing with highly sensitive medical information are being required to ensure that electronic records and electronic signatures are trustworthy, reliable, and generally an equivalent substitute for paper records and handwritten signatures. As interaction between equipment, operators, and computers becomes commonplace, it is important to establish a secure means to communicate and store information.

Basel II

Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The BCBS is the international rule-making body for banking compliance. In 2004, central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries endorsed the publication of "International Convergence of Capital Measurement and Capital Standards: a Revised Framework," the new capital adequacy framework commonly known as Basel II.

Basel II essentially requires banks to increase their capital reserves or demonstrate that they can systematically and effectively control their credit and operational risk. The framework defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events,” and highlights hacking and information theft through inadequate systems security as loss events. While banks around the world are experts at managing risk by virtue of operating in global financial markets, they are relatively new at understanding and controlling the risks inherent with operating online banking systems and keeping customer data secure.

Banks that practice effective information and systems security are able to demonstrate to regulators that they should qualify for lower capital reserves through reduced operational risk. The Basel II framework insists that banks demonstrate that an effective system of policies and processes are in place to protect information and that compliance to these policies and processes is ensured, but is not prescriptive in how banks should implement security policies and processes. The international standard ISO/ICE 17799 Code of Practice for Information Security Management provides guidelines for implementing and maintaining information security and is commonly used as a model for managing and reporting operational risk related to information security in the context of Basel II.

CA OPPA

The California Online Privacy Protection Act (OPPA) was established in 2003 to require all businesses and owners of commercial web sites in the state of California to conspicuously post and comply with a privacy policy that clearly states the policies on the collection, use, and sharing of personal information. The policy identifies the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.

Any business, organization, or individual that operates a Web site that collects private personal information for a person residing in the state of California is bound by the provisions of the law, so the California OPPA has a much greater impact nationally than is typical for state legislation.

CASB 1386

California Senate Bill 1386 has established the most specific and restrictive privacy breach reporting requirements of any state in the United States. The law was enacted to force businesses, organizations, and individuals holding private personal information for legitimate business purposes to inform consumers immediately when their personal information has been compromised. The law also gives consumers the right to sue businesses in civil court for damages incurred through the compromise of information. Any business, organization, or individual that holds private personal information for a person residing in the state of California is bound by the provisions of the law.

COPPA

The Children’s Online Privacy Protection Act (COPPA) was enacted in 2000 to protect the online collection of personal information about children under the age of 13. COPPA’s goal was to protect children’s privacy and safety online in recognition of the easy access that children often have to the Web. The law requires that Web site operators post a privacy policy on the site and outlines requirements for Web site operators to seek parental consent to collect children’s personal information in certain circumstances.

The law applies not only to Web sites that are clearly directed toward children but to any Web site that contains general audience content where the Web site operators have actual knowledge that they are collecting personal information from children. An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

DCID

This directive establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems. For purposes of this directive, intelligence information refers to sensitive compartmented information and special access programs for intelligence under the purview of the Director of Central Intelligence.

DoD Instruction 8500.2

Department of Defense Instruction 8500.2 implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. This instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the U.S. Department of Defense.

EU Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. Like all other European Union privacy legislation, this directive also requires that personal data be collected, stored, changed or disseminated only with a citizen's express consent and with full disclosure as to the use of the data. The directive also prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. The United States has developed a Safe Harbor framework for U.S. organizations that are required to comply with this directive.

EU Directive on Privacy and Electronic Communications

European Union Directive on Privacy and Electronic Communications is part of a broader “telecoms package” of legislation that governs the electronic communications sector in the European Union. The directive reinforces a basic European Union principle that all member states must ensure the confidentiality of communications made over public communications networks and the personal and private data inherent in those communications. The directive governs the physical communication networks as well as the personal data that is carried on it.

FISMA

The United States Congress passed the E-Government Act of 2002 in recognition of the importance of information security to the economic and national security interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity and availability. FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

GLBA

The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions must protect consumers' personal financial information. The main provision affecting Web application security in the financial industry is the GLBA Safeguards Rule.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) mandates the privacy and security of personal health information from the various threats and vulnerabilities associated with information management. For more information on using HP scanners to achieve HIPAA compliance, read the HIPAA white paper.

ISO17799

This is the most commonly accepted international standard for information security management. Use this policy as a baseline in crafting a compliance policy to meet the needs of your organization and its security policy.

ISO27001

ISO/IEC 27001 is an information security management system standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. The basic objective is to help establish and maintain an effective information management system using a continual improvement approach. ISO 27001 specifies the requirements for the security management system itself. It is the standard, as opposed to ISO 17799, against which certification is offered. Additionally, ISO 27001 is “harmonized” with other management standards, such as ISO 9001 and ISO 14001.

JPIPA

Japan enacted the Personal Information Protection Act (JPIPA) in 2003 to protect individuals' rights and personal information while preserving the usefulness of information technology and personal information for legitimate purposes. The law establishes responsibilities for businesses that handle personal information for citizens of Japan and outlines potential fines and punishments for organizations that do not comply. The act requires businesses to communicate their purpose in collecting and using personal information. They must also take reasonable steps to protect personal information from disclosure, unauthorized use or destruction.

NERC

The North American Electric Reliability Council (NERC) was established in 1968 with the mission of ensuring that the electric system of the United States is reliable, adequate and secure. After President Bill Clinton issued Presidential Decision Directive 63 in 1998 to define infrastructure industries critical to the United States' national economy and public well-being, the U.S. Department of Energy designated the NERC to act as the coordinating agency for the electricity industry, which was named one of the eight critical infrastructure industries.

NIST 800-53

The United States Congress passed the E-Goverment Act of 2002 in recognition of the importance of information security to the economic and national interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity, and availability.

OMB

This policy addresses major application security sections that were defined in December 2004 by the Office of Management and Budget for federal agency public Web sites. These are information resources funded in whole or in part by the federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-federal user group and support the proper performance of an agency function. Drop down section 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. Click here for more information on OWASP and its top 10 Web application vulnerabilities.

OWASP Top 10 2007

The Top 10 list for 2007 removes several important issues, such as unvalidated input, buffer overflows, denial of service, and insecure configuration management, and adds other important ones, such as cross-site request forgery and cryptography.

PCI Data Security

The Payment Card Industry (PCI) Data Security Policy requires that all PCI Data Security members, merchants, and service providers that store, process or transmit cardholder data verify all purchased and custom Web applications, including internal and external applications.

PIPEDA

Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) is a new law that protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity. The Act, based on ten privacy principles developed by the Canadian Standards Association, is overseen by the Privacy Commissioner of Canada and the Federal Court. As of January 1, 2004, all Canadian businesses are required to comply with the privacy principles set out by PIPEDA. The Act covers both traditional, paper-based and on-line business.

Safe Harbor

The European Commission's Directive on Data Protection prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. Upon passage of this comprehensive European legislation, all businesses and organizations in the United States that share data with European Union organizations were obligated to comply with the regulations, which could have disrupted many types of trans-Atlantic business transactions. Due to the differences in approaches taken by the United States and European Union nations in protecting personal data privacy, the U.S. Department of Commerce, in consultation with the European Commission, developed a streamlined “Safe Harbor” framework through which U.S. organizations could comply with the Directive on Data Protection.

Organizations participating in the Safe Harbor are committed to complying with these seven principles designed to ensure that personal data is properly used, controlled and protected: Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement. Of particular significance to information technology:

The Notice principle requires organizations to inform individuals about the purposes for which it collects information, such as through a privacy policy.

The Security principle states that organizations will take reasonable precautions to protect personal data.

The Enforcement principle mandates that organizations have procedures in place for verifying that security commitments are satisfied, such as through comprehensive security testing.

Sarbanes-Oxley

The Sarbanes-Oxley Act, which falls under the umbrella of the U.S. Securities and Exchange Commission (SEC), was enacted on July 30, 2002. It focuses on regulating corporate behavior for the protection of financial records, rather than enhancing the privacy and security of confidential customer information. For more information on using HP scanners to achieve Sarbanes-Oxley compliance for your Web applications, read the Sarbanes-Oxley white paper.

UK Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. The United Kingdom implemented the protections mandated by the directive through its Data Protection Act of 1998, summarized as follows:

- Personal data should be processed fairly and lawfully and only with consent.
- Personal data should be obtained only for specified and lawful purposes, and should not be further processed in any manner incompatible with those purposes.
- Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data should be accurate and kept up to date.
- Personal data processed for any purpose should not be kept for longer than is necessary for that purpose.
- Personal data should be processed in accordance with the rights of data subjects.
- Appropriate technical and organizational measures should be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Sensors

The Sensors group has one shortcut: Sensors.

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

This form displays the name, host name, and status 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 3.5 Service Pack 1.

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

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.
Stop Discovery Scan	Abort the Discovery scan.
Pause Sensor	Disable the sensor.
Continue Sensor	Enable the sensor. If the sensor was running a scan when paused, it will resume the scan automatically.
Enable/Disable	Turn the server 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 AMP system. Note: To enable this command, you must stop the “AMP Sensor for WebInspect” service (Start/Control Panel/Administrative Tools/Services), taking the sensor offline.
Edit Permissions	Allows you to modify the security settings for the selected sensor. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

Administration

The Administration group has 11 shortcuts:

- Activity Log
- Connected Users
- Licensing

- Smart Update
- Allowed Paths
- E-Mail Alerts
- SNMP Alerts
- Sensor Users
- Report Designers
- Roles and Permissions
- Risk Level
- Proxy Server Settings

Activity Log

The Activity Log lists each Assessment Management Platform 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 Windows credentials 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).

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.
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 AMP system. Each item includes:

- The user’s name
- The time and date when the user connected to the system

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.

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 the Assessment Management Platform.

- Activation ID: The unique identifier for the license issued by HP.
- User Information: Information about the person to whom the license is granted.
- License Information
    - Licenses 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 AMP.
    - Total Available Client Licenses: The maximum number of clients that may be connected to AMP.
    - Total Scan Count: The maximum number of scans that may be conducted.
- License Usage Information

Important: If the AMP console is installed on a machine that does not have Internet access, see If You Are Not Connected to the Internet on page 17 for instructions on activating the application.

Smart Update

HP engineers uncover new vulnerabilities almost every day. They develop attack agents to search for these malicious threats and then update our 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.

The Smart Update form contains a procedure log and a list of scheduled updates.

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 list.

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.

Allowed Paths

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

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

The commands are:

Command	Definition
Add	Open the *Allowed Path Settings* window, allowing you to specify allowed paths.
Edit	Open the *Allowed Path Settings* window, allowing you to modify allowed paths.
Delete	Remove the path from the form.
Edit Permissions	Specify permissions for the selected Allowed Path. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

E-Mail Alerts

You can force AMP to send an e-mail message to someone 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

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 AMP 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.

Commands

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.
Edit Permissions	Specify permissions for the selected alert. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

SNMP Alerts

You can force AMP 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.

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 AMP 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.

Commands

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.
Edit Permissions	Specify permissions for the selected alert. You can also add or delete roles, and add or remove users. The enabled options depend on the permissions associated with the role to which you are assigned.

Sensor Users

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

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

To add an account:

1. Click **Add**.
2. Enter the account assigned to the sensor.
3. Click **OK**.

To remove an account:

1. Select an account from the list.

2 Click **Remove**.

Roles and Permissions

This form allows you to add or delete roles, define security settings for a role, and assign users to roles.

Roles

A role is simply a named collection of permissions. You can allow other users to access the AMP console and limit the functions they are allowed to perform by assigning them to a role.

The Roles list contains the name and description of each role defined for the system. When installed, AMP is configured with the following built-in roles.

- Security Administrator: Granted all permissions with no IP restrictions. The user account of the person who installed the AMP console software is assigned to this role. The Administrator can change the default permissions assigned to the Security Technician and the Manager.
- Security Technician: Granted permission to perform all functions except for policy modifications. The administrator must edit the IP ranges if IP restrictions on this role are desired.
- Manager: Granted permission to perform all functions except for starting scans and modifying policies. The administrator must edit the IP ranges if IP restrictions on this role are desired.

Role Permissions

To define a role's security settings for managing various types of objects:

1. Select a role (Security Administrator, Security Technician, etc.).
2. Select a category or subcategory of objects (sites, scan policies, scheduled scans, etc.).
3. For each listed permission, select either **Allow** or **Deny**.

AMP determines a user's accessibility to functions and objects based on permissions granted to the role to which the user is assigned. It evaluates those permissions according to the following hierarchical criteria.

- The user who creates an object is awarded ownership and has full control over that object, regardless of the permissions associated with the role to which he is assigned. Note that ownership can be reassigned, however.
- Next, AMP examines permissions for the roles to which the user is assigned. If no "allow" permissions are granted, then the user has no access.
- If the user is assigned to multiple roles and if one role has an "allow" permission for a certain function while another role has neither "allow" nor "deny" permissions for that same function, then the user is granted access. However, if one role has an "allow" permission and another role has a "deny" permission for the same function, then the user is denied access. The "deny" permission nullifies any "allow" permission.

Default Roles and Permissions

An administrator may configure the system to award permissions for new objects based on the role of the user who created the object. For example, when users in role A create objects, users in role B might be able to view (but not delete) these objects. To accommodate users who are assigned to multiple roles, you can designate one role as the default. The AMP manager then uses this default role to assign permissions to objects created by that user.

However, due to the extreme flexibility of the AMP configuration, the AMP manager theoretically may be unable to determine a user's default role. If this occurs, then if the user who created the object:

- Is assigned to the role that has been designated as the system default, the AMP manager assigns permissions based on the system default role.
- Is not assigned to the system default role, only the user has "allow" permissions for the object.

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

The commands are:

Command	Definition
Add Role	Create a role.
Copy Role	Copy a role and assign a new name to it.
Rename Role	Change the name of a role.
Delete	Remove the selected role from the system.
Edit Permissions	Modify the administrative security settings for a role.
Make System Default Role	Designate the selected role as the default.
Add User to Role	Assign a user to the selected role.
Remove User from Role	Remove the selected user from the role.
Add Site Permission	Specify a host name, IP address, or range of IP addresses that the selected role may access.
Delete Site Permission	Remove the selection from the list of host names, IP addresses, or ranges of IP addresses that the selected role may access.

To define security settings for individual objects, select an object type in the list below **Roles and Permissions**.

1. Select a category (sites, scans, etc.).
2. Select a specific object in the list.
3. Select **Edit Permissions** from the **Action** menu (or right-click an object and select **Edit Permissions** from the shortcut menu).
4. Select a role.
5. For each function (view, update, etc.), select either **Allow** or **Deny**.

Object Permissions

You can also restrict access to existing objects using the following procedure.

1. Select an object category listed under Roles and Permissions in the shortcuts pane.
2. Select an existing instance the object listed on the form.

   For example, if you select Scan Templates, all existing Scan Templates are listed on the Scan Templates form.
3. Click the **Action** menu and select **Edit** Permissions.
4. On the *Security Settings for <ObjectName>* window, select a role.

   If the desired role is not listed, click **Add Role** and select the role for which you want to assign permissions.
5. In the **Permissions for <Role>** column, select either **Allow** or **Deny** for each of the permissions associated with the selected object type.

   To remove all permissions for a role, you can alternatively select the role and click **Delete Role**.
6. Repeat steps 4-5 to assign permissions for other roles.
7. To reassign ownership of the object, click the browse button in the **Security Properties** area (at the bottom of the pane).

Risk Level

Each vulnerability in the HP SecureBase has an associated severity level ranging from critical to informational. SQL Injection, for example, is rated as critical, while Server Statistics Information Disclosure is considered a medium risk.

The AMP manager can calculate a “risk level” for each scan, based on the number of vulnerabilities detected, the severity of those vulnerabilities, and a value that you assign to each severity category.

Example:

Vulnerability Category	Assigned Risk (Weight)	Number of Vulnerabilities	Weighted Value
Critical	8	4	32
High	6	7	42
Medium	3	9	27
Low	1	7	7
Best Practices	1	7	7
Informational	0	12	0
		Scan Risk Level Total = 115	

Proxy Server Settings

If you use a proxy server to communicate with HP for Smart Updates and licensing issues, select Use Proxy Server and then provide the requested information.

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.

Common AMP Console Tasks

Configure the Console

Use the following procedure to specify settings for the AMP console.

1 From the **Tools** menu, select **Options**.

2 To refresh the display of AMP 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/Compliance** group.

2 Click the **Scan Queue** shortcut.

3 Select the scan you want to suspend.

4 From the **Action** menu, select `Suspend`.

-or-

Right-click a scan request and select **Suspend** from the shortcut menu.

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

Resume a Suspended Scan

To resume a suspended scan:

1 Click the **Scans/Compliance** group.

2 Click the **Scan Queue** shortcut.

3 Select the scan you want to resume.

4 From the **Action** menu, select **Resume**

-or-

Right-click a scan request and select **Resume** from the shortcut menu.

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/Compliance** group.
2. Click the **Scan Queue** shortcut.
3. Select the scan you want to stop.
4. From the **Action** menu, select **Stop**.

   -or-

   Right-click a scan request and select **Stop** from the shortcut menu.

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 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**.

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.

      Note: 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, 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 AMP 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.

Create E-Mail Alerts

You can instruct the AMP 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 Select **Add** from the **Action** menu, or right-click in the E-mail Alerts list and select **Add** from the shortcut menu.

4 On the *E-Mail Alert Settings* dialog, enter the name and e-mail address of the person who should receive the alert.

5 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.

6 Select one or more actions that will trigger the alert.

7 Click **OK**.

8 If necessary, click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings, as follows:

- **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.

Create SNMP Alerts

You can force the AMP manager to send a Simple Network Management Protocol (SNMP) message whenever certain events occur.

1 Click the **Administration** group.

2 Select **SNMP Alerts**.

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

4 Enter a name for this alert in the **Name** box.

5 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 send e-mail alerts regardless of the IP address associated with the action.

6. Select one or more actions that will trigger the alert.
7. Click **OK**.
8. If necessary, click **SNMP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol settings, as follows:
   - **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 a network management system to perform set operations.

Create Allowed Paths

To add or edit a path:

1. Click the **Administration** group.
2. Select the **Allowed Paths** shortcut.
3. In the **Path** box, enter path using the Universal Naming Convention

   -or-

   click the browse button to select a path from a tree diagram of the network.

   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 AMP server is installed.
4. Click **OK**.

6 AMP Web Console

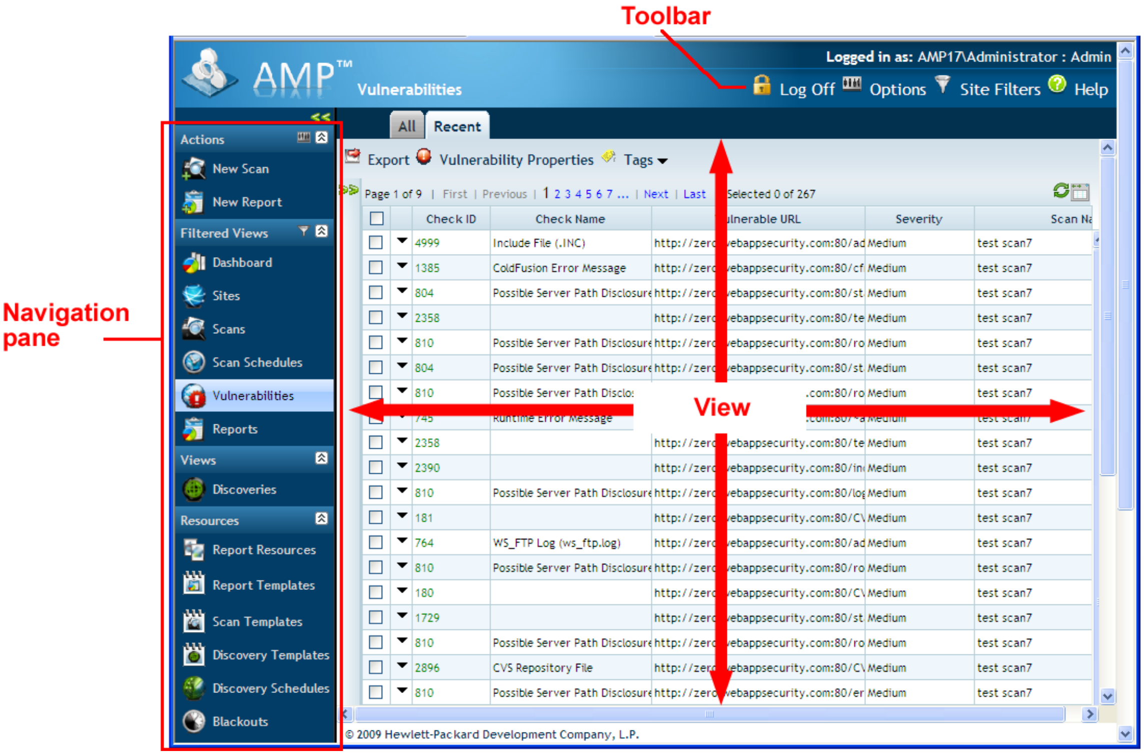
The Assessment Management Platform presents two separate user interfaces:

- The AMP Console, used for administrative and security functions.
- The AMP Web Console, a browser-based application used for conducting and managing scans.

This chapter describes the AMP Web Console.

The AMP Web Console user interface comprises three main areas:

- Toolbar
- Navigation pane
- Views and Forms



Page 1 of 9 | First | Previous | 1 2 3 4 5 6 7 ... | Next | Last | Selected 0 of 267

□		Check ID	Check Name	lnerable URL	Severity	Scan Na
□	▼	4999	Include File (.INC)	http://zer ebappsecurity.com:80/ad	Medium	test scan7
□	▼	1385	ColdFusion Error Message	http://zer ebappsecurity.com:80/cf	Medium	test scan7
□	▼	804	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/st	Medium	test scan7
□	▼	2358		http://zer ebappsecurity.com:80/te	Medium	test scan7
□	▼	810	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/ro	Medium	test scan7
□	▼	804	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/st	Medium	test scan7
□	▼	810	Possible Server Path Disclo	.com:80/ro	Medium	test scan7
□	▼	745	Runtime Error Message	.com:80/~a	Medium	test scan7
□	▼	2358		http://zer ebappsecurity.com:80/te	Medium	test scan7
□	▼	2390		http://zer ebappsecurity.com:80/in	Medium	test scan7
□	▼	810	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/lo	Medium	test scan7
□	▼	181		http://zer ebappsecurity.com:80/C\	Medium	test scan7
□	▼	764	WS_FTP Log (ws_ftp.log)	http://zer ebappsecurity.com:80/ad	Medium	test scan7
□	▼	810	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/ro	Medium	test scan7
□	▼	180		http://zer ebappsecurity.com:80/C\	Medium	test scan7
□	▼	1729		http://zer ebappsecurity.com:80/st	Medium	test scan7
□	▼	810	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/ro	Medium	test scan7
□	▼	2896	CVS Repository File	http://zer ebappsecurity.com:80/C\	Medium	test scan7
□	▼	810	Possible Server Path Disclosure	http://zer ebappsecurity.com:80/er	Medium	test scan7

© 2009 Hewlett-Packard Development Company, L.P.

Toolbar

The AMP Web Console toolbar contains the following icons:

Logs you off the AMP Web Console application.

Opens the *Configure Options* window, allowing you to set AMP Web Console options.

Opens the *Configure Site Filters* window, allowing you to specify the type of data displayed in filtered views.

Opens the Help file.

Options

Click Options on the toolbar to specify basic Web Console options.

Include Information Counts in Dashboard Charts

Informational items are not considered vulnerabilities. They simply identify interesting points in the site, or certain applications or Web servers discovered during an assessment or crawl. They normally are not represented in the dashboard charts.

Default to Advanced scan settings

When you initiate a scan, AMP displays one of the following option sets:

- Advanced : The full set of scanning options are presented.
- Simple: Only the scan template, site, and scan URL options are presented; for all other parameters, the scanner uses those settings specified in the Advanced option set.

If you select **Default to Advanced**, AMP displays the Advanced option set. If you do not select this option, AMP displays the Simple option set. In either case, however, you can switch from one to the other when you begin the scan.

Enable New Scan Action

This option allows you to initiate a scan from the AMP Web Console, using the New Scan function in the Actions group.

Enable New Scan Schedule Action

This option allows you to schedule a scan from the AMP Web Console.

Enable New Blackout Action

This option allows you to create and modify blackout periods from the AMP Web Console.

Enable New Report Action

This option allows you to generate a report, using the New Report function in the Actions group.

Site Filters

AMP provides two default filters that determine which data will be displayed when using filtered views (which are Dashboard, Sites, Scans, Scan Schedules, Vulnerabilities, and Reports). These default filters are:

- All - Actually filters no data, allowing you to see all results.
- Recent - Limits the display of scan-related data to files created within the last three months.

Filters are represented by tabs that appear on each filtered view. You can create additional filters that allow you to view only those data that conform to a particular area of interest.

For more information and instructions on creating filters, see Filtered Views on page 62.

Navigation Pane

The Navigation pane is divided into four sections:

- Actions
- Filtered Views
- Views
- Resources

Selecting an option in the Navigation pane displays a corresponding form in the View area.

Actions

New Scan

The New Scan action initiates a vulnerability scan by displaying windows that allow you to specify settings (options) for the scan. Either of two option sets are displayed:

- Advanced: The full set of scanning options are available. See Advanced Scan Settings on page 77 for details.
- Simple: Only the scan template, site, and scan URL options are available. See Simple Scan Settings on page 76 for details. For all other parameters, the scanner uses those settings specified in the Advanced option set.

You can switch from one option set to the other by selecting **Switch to Advanced** or **Switch to Simple** at the top of the dialog.

To specify which option set is displayed by default, click Options.

New Report

The New Report action displays windows that allow you to specify settings for predefined enterprise reports. See Report Settings on page 99 for details.

➤ Note: To generate a scan report, select the Scans view, choose one or more scans, and then click the Generate Report icon.

Filtered Views

Dashboard, Sites, Scans, Scan Schedules, Vulnerabilities, and Reports are termed “filtered views” because you can create filters that limit the display of data to a subset that you specify.

For very large installations, displaying details about all sites may consume considerable CPU, database, and intranet resources, even to the point where refreshing the display may interfere with or degrade system usability. To avoid this, or to simply focus on a specific subset of sites, you can use filters to prevent the display of information that is not in your area of interest.

The results will appear under a tab labeled with the filter name, and that tab will appear on all filtered views. The data displayed on each of those views, under the tab you create, is extracted exclusively from the sites that meet the criteria you specify when creating the filter.

Follow the steps below to create a filter:

1. Click the Site Filters icon on the toolbar.
2. On the Configure Site Filters page, click **New**.
3. Replace the default “New Filter” name with a name of your choice.
4. To force this filter to appear automatically (as a tab) whenever you log on, select **Default Filter**.
5. From the **Date Selector** list, choose either **Created**, **Started**, **Completed**, or **Latest**.

   “Latest” is a relative reference to the other three times. Note that the “created” date for an imported scan is the date on which it was imported.

   a. To view scans occurring within an absolute time period, select **Use Date Range**.0
   b. Click the calendar icon next to the **From** box and select the beginning of the date range.
6. Click the calendar icon next to the **To** box and select the end of the date range.
   - If you omit a “From” date, all scans prior to the “To” date will be listed.
   - If you omit a “To” date, all scans occurring since the “From” date will be listed.
7. To view scans that occurred within a certain number of months, select **Use Relative Date** and enter the number of months.
8. To view scans within a specific risk score range, define the range by entering scores in the **From** and **To** boxes.
9. To view only those scans associated with specific groups, clear the **Include All** check box and then move the group name from the **Available** column to the **Selected** column.
10. To view only those scans associated with specific phases, clear the **Include All** check box and then move the phase name from the **Available** column to the **Selected** column.
11. To view only those scans associated with specific tags, clear the **Include All** check box and then move the tag name from the **Available** column to the **Selected** column.

Important: If you select a combination of groups, phases, or tags, then only those sites that are members of all selected qualifiers will be displayed.

12 Click **Save**.

When you select a filtered view, a tab labeled with the filter name appears in the client area.

Dashboard

The Dashboard displays charts and graphs compiled from the AMP database. They are:

- Top 5 Vulnerabilities - A bar chart showing the five vulnerabilities most often reported.
- Weighted Application Risk - A bar chart showing, for each site, the weighted values for each vulnerability category (critical, high, medium, low, and informational).
- Severity Breakout - A pie chart that illustrates the relative number of vulnerabilities by category.
- Weighted Risk Trend Analysis - A graph that indicates, by month, the total number of vulnerabilities discovered in the last scan conducted for the month for each site in the defined groups.
- Vulnerabilities by Phase - A bar chart that illustrates, for all sites assigned to each specific phase, the total number of vulnerabilities, delineated by severity.
- Lifecycle Vulnerability Trend - A graph showing the total number of vulnerabilities detected, by phase, over a period of time.

To view the raw data, click a graphic.

Dashboard Layout

Follow the steps below to rearrange the charts and graphs on the Dashboard.

➤ Note: You cannot rearrange the dashboard if you are using Firefox.

1 Click the Dashboard Layout hyperlink (below the toolbar).

2 Click the Close button on each image to remove it from the display and add the image name to the Page Catalog.

3 To recreate the page:

a Select a zone from the **Add to** list.

b Select one or more images that you want to place in the selected zone.

c Click **Add**.

d Repeat until all images have been placed.

4 Click **Close**.

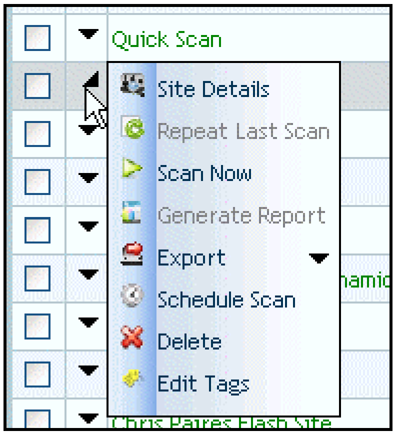
Sites

This form lists all sites that you have permission to view. If a scan request has been completed successfully, the list also contains starting and completion time stamps as well as the total number of vulnerabilities found, sorted by severity (if you have not modified the column settings).

This information is identical to the listings on the Scans form, except the information here is grouped by site.

To view or modify details about the site, click the site name.

You can perform additional functions by clicking the dropdown arrow next to a site name.



The functions unique to this menu are:

Scan Now - Allows you to configure settings for a scan of the selected site and initiate the scan.

Schedule Scan - Allows you to configure settings for the selected site, including the date and time when the scan should be conducted. When configuration is complete, the pending scan request is added to the Scan Schedules form.

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

Icon	Function
Add	Create a site. See Site Settings on page 104 for a description of site settings.
Generate Report	Select options and create a report for the selected site.
Repeat Last Scan	Scan the selected site using the parameters that were chosen for the previous scan.
Vulnerabilities	Display a list of vulnerabilities that were detected during the most recent scan conducted in the selected site.
Delete	Remove the selected site from the list.
Import	Load a comma-separated file containing site catalog details.
Export	Save a file containing site catalog details in either comma-separated value (csv) or Extensible Markup Language file (.xml) format.
Tags	Add, edit, or remove tags for the selected site. See Tags on page 79 for more information.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
▦	Change the number of rows on the page, modify column widths, specify which columns are displayed, and sort data by columns.

Scans

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

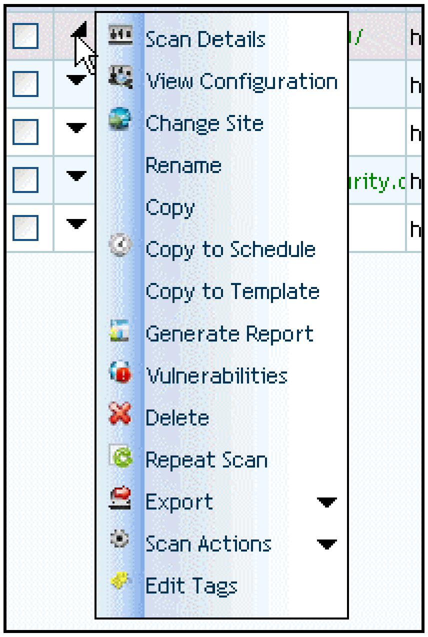
- Name assigned to the request
- Target Web site URL or IP address
- Site to which this scan is assigned
- Policy used for the scan
- Sensor conducting the scan
- Date and time the scan request was created
- Date and time the scan started and completed
- Application type and version
- Scan status.

If a check mark appears in the **Results** column, the number of vulnerabilities detected appears in columns sorted by severity.

To view scan details, click a scan name.

To view site details, click a site name.

You can perform additional functions by clicking the dropdown arrow next to a scan name.



The functions unique to this menu are:

View Configuration - Allows you to view (but not edit) the settings used for the selected scan.

Rename - Allows you to assign a different name to the scan.

Copy - Copies all settings that were used for this scan and pastes them into the Configure Scan windows, allowing you to edit the settings before initiating the scan.

Copy to Schedule - Copies all settings that were used for this scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings before placing the scan request into the Scheduled Scans form.

Copy to Template - Copies all settings that were used for this scan and pastes them into the Configure Scan Template windows, allowing you to edit the settings before creating the template. You cannot copy an imported scan to a template.

Export - Exports the selected scan or the settings for the selected scan.

Note for Internet Explorer users: When attempting to export scans from the Scans view, 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:

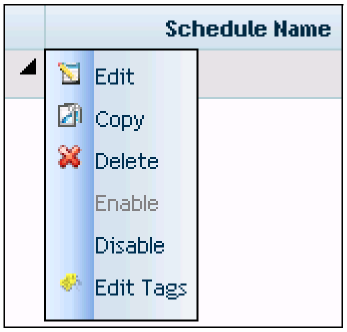
Icon	Function
Add	Start a new scan. See Advanced Scan Settings on page 77 for a description of scan settings.
Generate Report	Specify report settings for the selected scan.
Vulnerabilities	Display a list of vulnerabilities detected by the selected scan.
Delete	Delete the selected scan.
Repeat Scan	Repeat the selected scan.

Icon	Function
Scan Actions	Stop, resume, or suspend a selected scan.
Change Site	Reassign one or more scans to a different site.
Tags	Add, edit, or remove tags for the selected scan.

Scan Schedules

This view displays information about each scheduled scan request.

You can perform additional functions by clicking the dropdown arrow next to a schedule name.



The functions unique to this menu are:

Edit - Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings for this scheduled scan request.

Copy - Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings and create an additional scheduled scan request.

Enable - Activates a disabled scheduled scan request. Requests are enabled, by default, when created.

Disable - Deactivates a scheduled scan request. 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 105 for a description of settings.
Delete	Remove the scheduled event.
Tags	Add, edit, or remove tags for the selected scheduled scan.

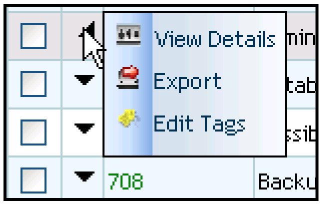
Vulnerabilities

This view is a composite list of all vulnerabilities detected by all scans in the system (or all vulnerabilities for the selected site or scan).

To view detailed information about a vulnerability, click the check ID.

To include vulnerabilities that have been marked as "ignore," select **Show Ignored Vulnerabilities** (at the bottom of the form).

You can perform additional functions by clicking the dropdown arrow next to a check ID.



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

Icon	Function
Export	Create an XML-formatted file containing information about one or more selected vulnerabilities. The file is opened in a browser, and you may save the file using the browser's File menu. This option is useful when submitting vulnerability information to another security system.
Vulnerability Properties	For the selected vulnerabilities (one or more), you can: • Append a note • Mark as false positive • Ignore
Tags	Add, edit, or remove tags for the selected vulnerabilities.

Reports

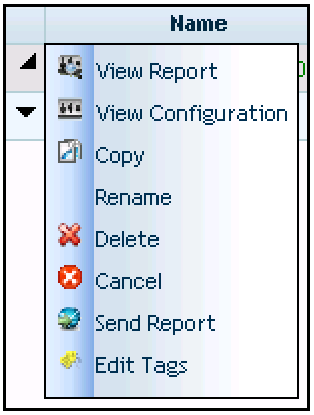
This form lists all reports that you have permission to view.

Each entry, by default, contains the following:

- Report name
- URL of the scanned site
- Status
- Description
- Name of the user who created the report
- Format
- Type
- Scan Count
- Template name
- Date and time the report was created
- Date and time the report was completed

To view a report, click the report name.

You can perform additional functions by clicking the dropdown arrow next to a check ID.



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

Icon	Function
View	View the selected report.
Delete	Remove the selected report.
Cancel	Halt a report that is being generated.
Tags	Add, edit, or remove tags for the selected report.

Views

Discoveries

This view displays information about each Discovery scan request.

A Discovery scan is an attempt to discover and identify Web servers within a range of IP addresses and ports that you specify. To do so, the scanner sends packets to the IP addresses and searches the HTTP response messages for specific information. For example, one of the predefined packets sent by the scanner contains the following HTTP request:

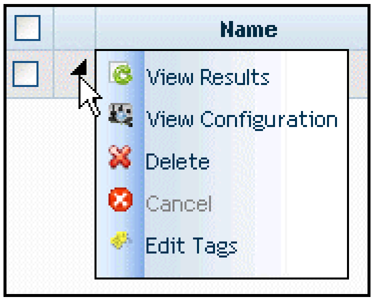
```
GET / HTTP/1.0
```

The scanner searches the HTTP response for the string “HTTP”; if it finds the string, it records 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.

For each Discovery scan request, the form displays the IP address and port ranges, the date and time the scan request was created, the time and date the scan started and completed, and the scan's status.

To view the results for a listed Discovery scan, click an entry in the Name column.

You can perform additional functions by clicking the dropdown arrow next to a discovery name.



The function unique to this menu is:

View Configuration - Copies all settings that were used for this Discovery scan and pastes them into the Configure Discovery Scan windows. The settings cannot be edited.

You can perform additional functions by clicking the dropdown arrow next to a discovery name.

Icon	Function
Add	Create a Discovery scan request. See Discovery Scan Settings on page 106.
Delete	Remove the selected Discovery scan request
Cancel	Halt a Discovery scan that is being generated
Tags	Add, edit, or remove tags for the selected Discovery scan.

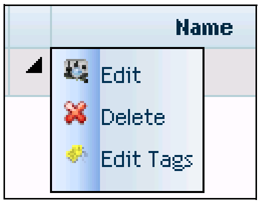
Resources

Report Resources

This view lists resources (such as graphics and style sheets) that are available for inclusion in a report.

To edit a resource, click an entry in the Name column.

You can perform additional functions by clicking the dropdown arrow next to a template name.



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

Icon	**Function**
Add	Add a resource.
Delete	Delete the selected resource.
Tags	Add, edit, or remove tags.

To associate a different file with the current resource name:

1. Click an image name in the Name column.
2. Click **Browse**.
3. Using the *Choose File* dialog, select an image.
4. Click **Open**.

The selected file is uploaded to the AMP server.

To add an image:

1. Click **Add**.
2. Enter a name for the image in the **Name** box.
3. Click **Browse**.
4. Using the *Choose File* dialog, select an image.
5. Click **Open**.

The selected file is uploaded to the AMP server.

Note: You cannot add or edit stylesheets.

Report Templates

This view lists all report templates for which you have permission to view.

To view or modify template settings, click the template name.

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

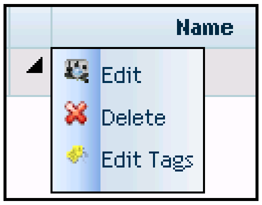
Icon	**Function**
Add	Create a report template. See
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template.

Scan Templates

This view lists all scan templates that you have permission to view.

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

You can perform additional functions by clicking the dropdown arrow next to a template name.



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

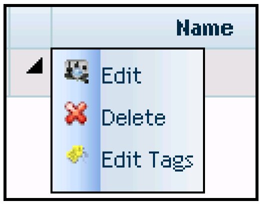
Icon	Function
Add	Create a template. See Scan Template Settings on page 100.
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template.

Discovery Templates

This form lists all discovery templates that you have permission to view.

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

You can perform additional functions by clicking the dropdown arrow next to a template name.



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

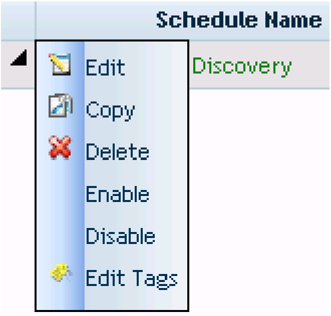
Icon	Function
Add	Create a template. See Discovery Template Settings on page 108.
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template.

Discovery Schedules

This form displays information about each Discovery scan that has been scheduled.

To view settings for a scheduled Discovery scan, click an entry in the Schedule Name column.

You can perform additional functions by clicking the dropdown arrow next to a schedule name.



The functions unique to this menu are:

Copy - Copies all settings that were used for the selected scheduled discovery scan and pastes them into the Configure Scheduled Discovery windows, allowing you to edit the settings and create an additional scheduled discovery scan request.

Enable - Activates a disabled scheduled discovery scan request. Requests are enabled, by default, when created.

Disable - Deactivates a scheduled discovery scan request. 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 perform additional functions using the icons at the top of the form.

Icon	Function
Add	Schedule a Discovery scan. See Discovery Schedule Settings on page 111.
Delete	Delete the selected Discovery scan request.
Tags	Add, edit, or remove tags for the selected Discovery scan.

Blackouts

This form displays information about each blackout period defined for the system.

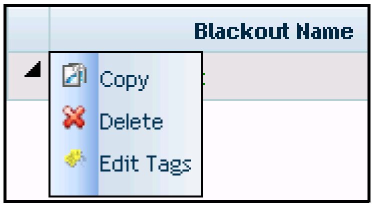
A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

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.

Note: Discovery scans are not subject to or controlled by blackout periods.

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

You can perform additional functions by clicking the dropdown arrow next to a blackout name.

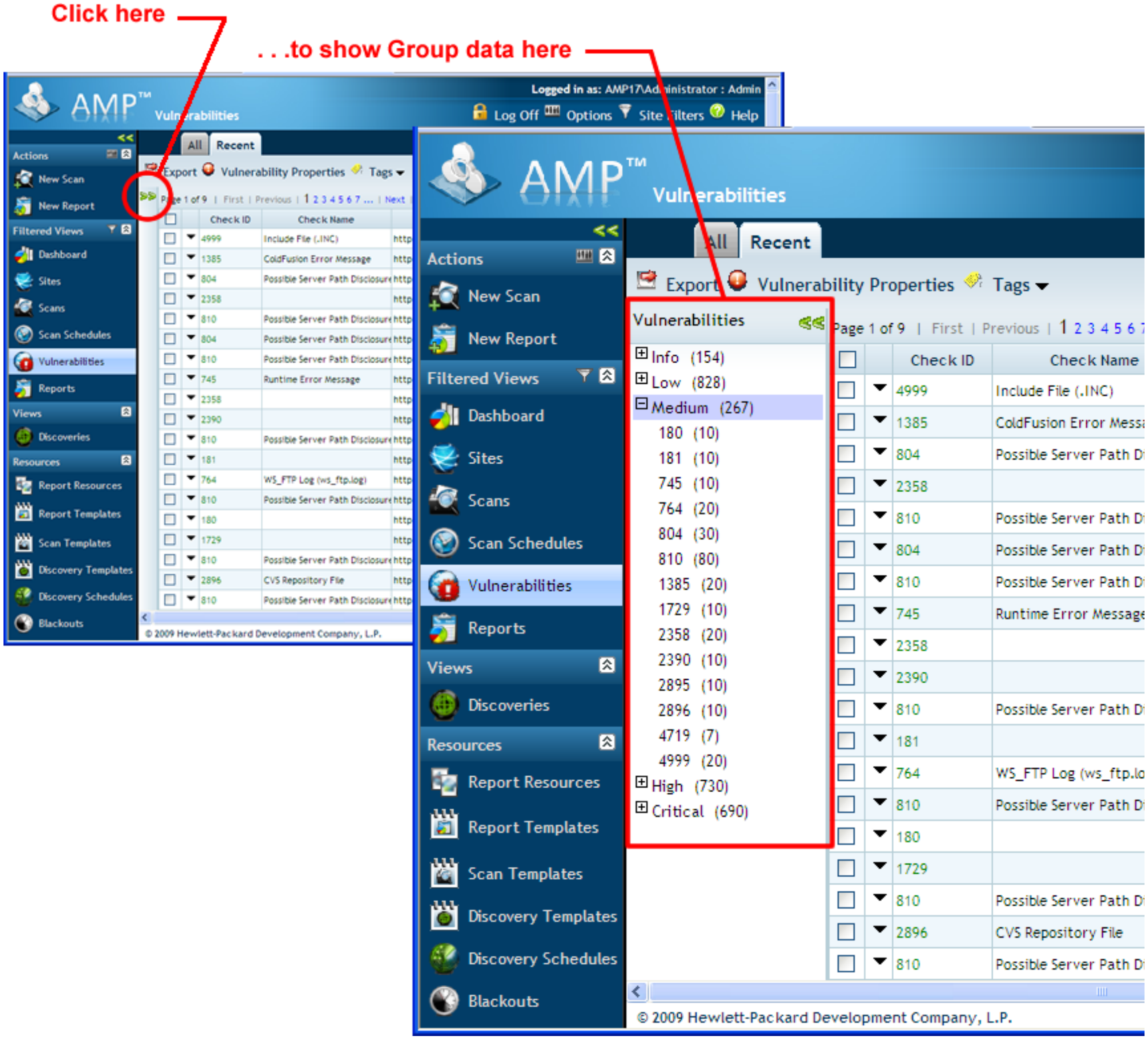


You can perform additional functions using the icons at the top of the form.

Icon	Function
Add	Schedule a blackout period. See Blackout Settings on page 114.
Delete	Delete the selected blackout period.
Tags	Add, edit, or remove tags for the selected blackout period.

Grouping Results

The Results Group pane allows you to display data sorted according to rules you define using the Column Grouping feature. You can show or hide the Results Group pane by clicking the toggle icon depicted in the following illustration. This example shows 2,669 vulnerabilities sorted by severity and check name.



Click here

. . .to show Group data here

Vulnerabilities

⊞ Info (154)
⊞ Low (828)
⊟ Medium (267)
180 (10)
181 (10)
745 (10)
764 (20)
804 (30)
810 (80)
1385 (20)
1729 (10)
2358 (20)
2390 (10)
2895 (10)
2896 (10)
4719 (7)
4999 (20)
⊞ High (730)
⊞ Critical (690)

Check ID	Check Name
4999	Include File (.INC)
1385	ColdFusion Error Messa
804	Possible Server Path D
2358	
810	Possible Server Path D
804	Possible Server Path D
810	Possible Server Path D
745	Runtime Error Message
2358	
2390	
810	Possible Server Path D
181	
764	WS_FTP Log (ws_ftp.lo
810	Possible Server Path D
180	
1729	
810	Possible Server Path D
2896	CVS Repository File
810	Possible Server Path D

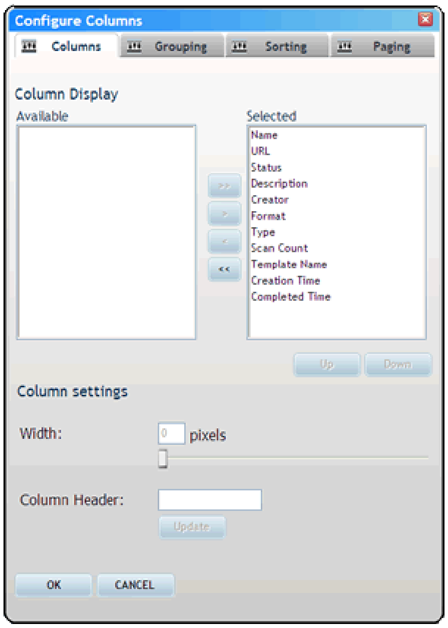
You can group objects in views (scans, sites, vulnerabilities, etc.) according to the available column names and tags. Any grouping you define is applied to every tab on the form you are viewing.

In this example, vulnerabilities are grouped by severity and then by check name within each severity category.

1 In the Navigation pane, click **Vulnerabilities**.

2 Click the Edit Layout icon ▦ (at the top right of the Vulnerabilities list).

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



4 In the **Available** list, select **Check Name** and click **>**.

5 Select **Severity** and click **>**.

Both column headers are now removed from the **Available** list and appear in the **Selected** list.

6 Select **Severity** and click **Up**.

The order determines how the data is sorted. In this example, vulnerabilities will be listed by severity and then by check name within each severity category.

7 Click **Severity** and choose **Descending** from the list at the bottom of the dialog.

8 Click **OK**.

When you return to the Vulnerabilities view, the Results Group pane displays the grouped results. When you select a parent group name (such as Low), AMP displays only those vulnerabilities having a severity level in the selected category. Redundant items (check names, in this example) are combined and the number of instances is reported in parentheses following the check name.

You can open or close the pane using the Results Group pane toggle.

Simple Scan Settings

Scan Template

Instead of specifying each individual setting that an HP scanner requires 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.

Some templates allow you to change the settings. To do so, select the Create custom scan from template check box.

You are not required to use a template.

Scan

Enter a unique name for the scan.

Site

Click in the **Site Name** box and select a site from the list.

To create a site, enter a name, click **New Site**, and then provide the requested information.

Scan URL

In the **URL** box, type the complete URL or IP address of the site you want to examine (or select one from the Suggested URLs list).

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/.

Authentication

If your Web site requires authentication, select this option and then choose one of the following methods:

- Use Intelligent Authentication - Select this option if you want the HP scanner to submit the user name and password you specify whenever it encounters Web forms containing a password input control.
- Use Login Macro - Select this option to use a macro for Web form authentication. When recording this type of macro, be sure to select **Enable Check For Logout** and then specify the application's log-out signature. Select a macro from the list or click **Browse** to locate a macro.

Reporting

Select this option to create a report of your scan findings. Then select either **Report Template** or **Report Definition**, and select a template or definition from the list.

Advanced Scan Settings

Categories of settings appear as groups in the left column. They are:

- Scan
- Scan Settings
- Crawl Settings
- Audit Settings
- Scan Behavior
- Reports
- Export

Each group has one or more subcategories.

Scan

General

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, but if you do, you may also select the following options:

- Create custom scan from template - When you select this option, all settings for this scan (including any deviations from the template) will be saved and permanently associated with the scan request. A rescan (or a scheduled scan) will use the saved settings and not the template. This is useful when you intend to conduct a series of identical scans and do not want to introduce any subsequent modifications that someone may make to the template. Your assigned role may not allow you to select this option.
- Customize Scan Settings - Select this option if you want to modify any of the scan settings prescribed by the template. If the selected template does not allow modifications, this option is not enabled.

Scan

Enter a unique name for the scan.

Site

Click inside the Site Name box to display a list of all sites defined for your system; then select a site name. To create a site, enter a name and click New Site.

Scan URL

In the URL box, type or select the complete URL or IP address of the site you want to examine. URLs that were previously scanned and assigned to the site you selected above (or are associated with the template you selected) are listed in the Suggested URLs box.

An improperly formatted 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/. If you select Restrict To Folder, you can limit the scope of the assessment to the area you choose from the drop-down list. They are:

- Directory Only - The HP 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 HP scanner will assess only the “two” directory.
- Directory and subdirectories - The HP 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 HP 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.

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 AMP Manager will place the second 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 AMP Manager will suspend that scan, assign the second 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.

Tags

Tags are user-configurable fields designed to help you group or sort various lists, such as scans, sites, blackout periods, and vulnerabilities.

For example, you might want to categorize your sites geographically into four regions. To do so, you could create a tag named "Region" and assign four possible values to it: North, East, West, and South. You could then assign one of these tags to every site.

Similarly, you could create a tag named "Tester" and then assign as possible values the name of each Quality Assurance engineer who is responsible for conducting scans. You could then assign one of these tags to each scan, allowing you to group together all scans conducted by the same person.

To create tags:

1. Enter a name in the **Tag Name** box.
2. In the **Tag Value** box, enter one of the values to be associated with the tag name.
3. Click **Add**.
4. Repeat steps 2-3 to create additional values for the tag name.

To select a tag for the function you are performing:

1. If necessary, click ⊞ to expand the list of values associated with a tag name.
2. Select a value.
3. Click **Add**.

To remove a tag:

1. Select a tag value in the **Selected** list.
2. Click **Remove**.

Scan Settings

Method

The scan template settings are reproduced on each settings dialog, allowing you to change the template selection at any point. The description of the settings is not repeated in the following topics.

Scan Mode

Select one of the following modes:

- Crawl and audit (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.
- Crawl and audit (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.
- 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.
- Recorded macro-crawl with audit - Using this option, the scanner audits only those resources that you previously recorded in the Web macro that you specify. The scanner will not follow any links to other resources.
- 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.

Sequential Crawl and Audit Behavior

If you selected Crawl and Audit (Sequentially) above, you can specify the order in which the crawl and audit should be conducted.

- Test each session per engine type - 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.
- Test each engine type per session - 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.

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. When recording this type of macro, be sure to select **Enable Check For Logout** and then specify the application's log-out signature. The drop-down list contains the names of all macros that have been uploaded to AMP. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.
- 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 AMP. 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. 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 select **Edit** (to modify the currently selected file) or Create (to record new Web form values).
- Auto-fill SOAP messages during crawl - This option applies only to Web Service assessments. When performing a Web service assessment, the scanner crawls the WSDL site and submits an arbitrary enumeration value for each parameter in each operation. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection. You can tailor these attacks to your WSDL by creating a file containing specific values that should be submitted. This feature is especially useful when an operation requires submission of a password, license number, or other specific parameters. Click **Browse** to select the file containing the values you want to use.

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, WebInspect saves disk space by storing each HTTP response in a compressed format in the database.
- Enable Traffic Monitor Logging - 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, allowing you to display and review every single HTTP request sent by WebInspect and the associated HTTP response received from the server.
- Encrypt Traffic Monitor File - 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, 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 recursion level is 1,000.

Crawl Details

You may choose the following options:

- Crawler - The scanner can crawl a site in two different ways, depending on which option you select. In breadth-first crawling, the scanner crawls Web pages in the order their URLs are discovered. Conversely, depth-first crawling follows each possible path to its conclusion and then backtracks, returning to the most recent node it hadn't finished exploring. 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.
- 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

Flash - If you enable the Flash analyzer, the scanner analyzes Flash files, Adobe's vector graphics-based resizeable animation format.

JavaScript/VBScript - Choosing to analyze script can significantly increase the amount of time required for the scanner to crawl a site. To increase the speed at which the scanner conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Note: If you do not elect to analyze JavaScript, the scanner cannot assess resources revealed through the execution of AJAX.

If you choose to analyze script, click the parser name (JavaScript/VBScript) and 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 execution of JavaScript or Visual Basic script).

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>

The scanner 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.).

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.

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.

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 WebInspect 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 50 concurrent HTTP requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 25. The default setting is 3 for the crawl requestor and 5 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.

Tip: If you notice numerous entries on the Scan Log tab showing requests timing out, you should reduce the number of concurrent requests that WebInspect is sending to the server. 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

You may select the following options:

- Limit maximum response size to - Select this option to limit the size of accepted server responses; then specify the maximum size (in kilobytes).
- 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).
- 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.

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 WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

- Consecutive "single host" retry failures - Enter the number of consecutive timeouts permitted from one specific server.
- Consecutive "any host" retry failures - Enter the total number of consecutive timeouts permitted from all hosts.
- Nonconsecutive "single host" retry failures - Enter the total number of nonconsecutive timeouts permitted from a single host.

- Nonconsecutive “any host” request failures - Enter the total number of nonconsecutive timeouts permitted from all hosts.
- 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 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 in Default (or Current) Scan Settings/Scan Settings/Allowed Hosts.
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 assessment, 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 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 having a MIME type that is excluded by settings .

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

The following settings apply to both the crawl and audit phases of a vulnerability assessment. 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 assessment, 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/

Follow the steps below 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 to be crawled. 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 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

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 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.

➤ 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 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.

Follow the steps below 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 WebInspect requests.

- 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. Follow the steps below 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 WebInspect to the server when conducting a vulnerability assessment. Follow the steps below 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.
- Auto 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 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. 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: SOCKS4, SOCKS5, or standard.
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

Assessment 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. 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.

- 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 type. Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.

If you want the scanner to submit this user name and password whenever it encounters Web forms containing a password input control, select Use Intelligent Authentication.

Use Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. Follow the steps below to use client certificates.

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

File Not Found

Determine “file not found” 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. 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 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 in WebInspect from 404 pages that are unique to your site.

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 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

Assessment Type

Select either **Web Site** or **Web Service**.

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 B, Policies and Components for policy descriptions.

For a Web Service assessment, you can select only the SOAP 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.

Follow the steps below 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. Follow the steps below 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. Follow the steps below 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. Follow the steps below 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. Follow the steps below 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. Follow the steps below 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. Follow the steps below 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.”

Follow the steps below 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 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**.
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**.

Audit Inputs Editor

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 editor, click the **Browse** button next to the **Import Audit Inputs** button.

Attack Expressions

Additional Regular Expression Languages

You may select **ja-JP**, which is the language code and country code representing Japanese and Japan (as used by the CultureInfo class in the .NET Framework Class Library).

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 an assessment. For example, the “Parameter Vuln 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 Assessment

Enable Smart Assessment

Smart Assessment 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 more of the identification methods described below.

- Use regular expressions on HTTP responses - 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 - 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 **Server** box, enter the domain name or host, or the server's IP address.
3. (Optional) Click **Identify**.

   The scanner contacts the server and displays its type, as revealed using the server analyzer fingerprinting method. Alternatively, if you select the **Use Regular Expressions** option, enter a regular expression designed to identify a server.
4. Select one or more entries from the **Server/Application Type** list.
5. Click **Update**.

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.

Reports

General

Generate Report

Select this option to create a report.

Automatically generate report name

Select this option if you want AMP to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.

Report Name

If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **Report Name** box.

Description

Enter a brief description of the report.

Export Report

Select this option to export a report, and then provide the following information.

- Output Type - Choose a format for the exported report. The choices are:
- Export Path - Enter or select a destination for the exported report. Because the AMP Manager service writes the output , the specified path must be writable by the Manager service user. You should use a UNC pathname (e.g., \\AmpServer\Amp\Output\) so that it will be accessible to both the AMP Manager and end users. You may alternatively specify a drive letter and path (e.g., C:\Amp\Output\), but the path will apply to the AMP Manager server and may not be accessible to end users.
- Automatically generate file name - Select this option if you want the AMP manager to assign a name to the exported report based on the time and date. Otherwise, clear this option and enter a name in the **File name** box.

Options

Report Type

Select one of the following options and then select the template or definition from the appropriate list;

- Use Report Template
- Use Report Definition

Report Definitions

The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.

E-mail

To send a copy of a report by e-mail:

1. Type an e-mail address in the **New E-mail Recipient** box.
2. Click `Add`.

Repeat as necessary

Export - General

Export Scan Results

Select this option to export the scan results. Then provide the requested information.

- Export Path - Enter or select a destination for the exported scan. Because the AMP Manager service writes the output, the specified path must be writable by the Manager service user. You should use a UNC pathname (e.g., \\AmpServer\Amp\Output\) so that it will be accessible to both the AMP Manager and end users. You may alternatively specify a drive letter and path (e.g., C:\Amp\Output\), but the path will apply to the AMP Manager server and may not be accessible to end users.
- 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.

Report Settings

Categories of settings appear in the left column. They are:

- General
- Options
- Tags

General

Automatically generate report name

Select this option if you want the AMP manager to assign a name to the file based on the time and date. Use this option if you are generating reports for recurring scans and you want to preserve each report.

If you want to specify a file name, clear the **Automatically generate report name** option and then type the name in the **Report Name** box. Do not use this option for recurring scans unless you want to overwrite the old report each time the scan is conducted.

Description

Enter a brief description of the report.

Options

Report Type

Select one of the following options and then select the template or definition from the appropriate list;

- Use Report Template
- Use Report Definition

Report Definitions

The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as reports. See Tags on page 79 for instructions on creating tags.

Report Template Settings

Template

Enter a name and a brief description of the report template, and then select a style sheet from the **Report Style Sheet** list.

Master Report

Select a master report from the available list, and then enter report parameters for the selected master report.

Report Definitions

Select a report type from the available list, and then enter the requested information in the Report Definitions group.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled report templates. See Tags on page 79 for instructions on creating tags.

Scan Template Settings

Settings for a scan template are the same as those described for a scan (see Advanced Scan Settings on page 77), except for the following:

Scan

General

Scan Template Name

Enter a name for this template.

Custom Scan Settings

If you select Can customize scan settings when applying this template, users may modify the settings prescribed by this template.

Maximum Priority

Specify the maximum priority that can be assigned to a scan that uses this template.

Restrict To Folder

If you select this option, you can limit the scope of the assessment to the area you choose from the drop-down list. They are:

- Directory Only - The HP 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 HP scanner will assess only the “two” directory.
- Directory and subdirectories - The HP 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 HP scanner will begin crawling and/or auditing at the URL you specify

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scan templates. See Tags on page 79 for instructions on creating tags.

Sensors

Select one or more sensors from the available list. The selected sensors will be available for creating a scan when this scan template is used.

To allow unrestricted access to sensors, select the **Use Any Available** check box.

To restrict access to specific sensors:

1. If necessary, clear the **Use Any Available** check box.
2. To add a sensor, select a sensor in the **Available** area and click **>**. The sensor is removed from the **Available** list and added to the **Selected** list.
3. To remove a sensor, select a sensor in the **Selected** list and click **<**. The sensor is removed from the **Selected** list and added to the **Available** list.
4. To add all available sensors, click **>>**.
5. To remove all selected sensors, click **<<**.

Scan URLs

If you select **Allow user to specify any URL**, the template will not restrict scans based on URL. Alternatively, you can clear this option and then create a list of URLs from which a user must select.

To create a list of allowed URLs:

1. Clear the **Allow user to specify any URL** check box.
2. In the text box, enter the complete URL or IP address of a site you want to allow users to scan. An improperly formatted URL or IP address will result in an error. If you want to scan from a certain point in a hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.
3. Click **Add**.

Reports - General

Can customize scan report settings when applying this template

Select this check box to allow users to modify scan report settings.

Generate Report

Select this check box to generate a report after the scan is complete.

If this option is enabled, you can also select the following:

- **Automatically generate report name** - Select this option if you want the AMP manager to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
- **Report Name** - If you want to specify a name, clear the **Automatically generate report name** check box and then type the name in the **Report Name** box.
- **Description** - Enter a brief description of the report.
- **File Format** - Click the dropdown arrow and select a format.
- **Export Report** - Select this option to export a report.
  - **Automatically generate file name** - Select this option if you want the AMP manager to assign a name to the exported report based on the time and date.
  - **File Name** - If you want to specify a name, clear the Automatically generate file name check box and then type the name in the Report Name box.
- E-Mail Recipients - To e-mail the report, enter an e-mail address in the **New E-Mail Recipient** box and click Add.

Reports - Templates

Select one or more report templates from the available list. The selected templates will be available for configuring a report when this template is used.

To allow unrestricted access to report templates, select the **Use Any Available** check box.

To restrict access to specific templates:

1. If necessary, clear the **Use Any Available** check box.
2. To add a template, select a template in the **Available** area and click **>**. The template is removed from the **Available** list and added to the **Selected** list.

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

4 To add all available templates, click **>>**.

5 To remove all selected templates, click **<<**.

Reports - Compliance Templates

Select one or more compliance templates from the available list. The selected templates will be available for configuring a compliance report when this template is used.

To allow unrestricted access to templates, select the **Use Any Available** check box.

To restrict access to specific templates:

1 If necessary, clear the **Use Any Available** check box.

2 To add a template, select a template in the **Available** area and click **>**. The template is removed from the **Available** list and added to the **Selected** list.

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

4 To add all available templates, click **>>**.

5 To remove all selected templates, click **<<**.

Reports - Resources

Select one or more report resources from the available list. The selected resources will be available for configuring a report when this template is used.

To allow unrestricted access to resources, select the **Use Any Available** check box.

To restrict access to specific resources:

1 If necessary, clear the **Use Any Available** check box.

2 To add a resource, select a resource in the **Available** area and click **>**. The resource is removed from the **Available** list and added to the **Selected** list.

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

4 To add all available resources, click **>>**.

5 To remove all selected resources, click **<<**.

Reports - Report Allowed Paths

Select one or more allowed paths from the available list. The selected allowed paths will be available for saving a report when this template is used.

To allow unrestricted access to allowed paths, select the **Use Any Available** check box.

To restrict access to specific allowed paths:

1 If necessary, clear the **Use Any Available** check box.

2 To add an allowed path, select an allowed path in the **Available** area and click **>**. The allowed path is removed from the **Available** list and added to the **Selected** list.

3 To remove an allowed path, select an allowed path in the **Selected** list and click **<**. The allowed path is removed from the **Selected** list and added to the **Available** list.

4 To add all available allowed paths, click **>>**.

5 To remove all selected allowed paths, click **<<**.

Export - Allowed Paths

Select one or more allowed paths from the available list. The selected allowed paths will be available for exporting a report when this template is used.

To allow unrestricted access to allowed paths, select the **Use Any Available** check box.

To restrict access to specific allowed paths:

1 If necessary, clear the **Use Any Available** check box.

2 To add an allowed path, select an allowed path in the **Available** area and click **>**. The allowed path is removed from the **Available** list and added to the **Selected** list.

3 To remove an allowed path, select an allowed path in the **Selected** list and click **<**. The allowed path is removed from the **Selected** list and added to the **Available** list.

4 To add all available allowed paths, click **>>**.

5 To remove all selected allowed paths, click **<<**.

Site Settings

General

Site Name

Enter a name that identifies this site.

URL

Enter a fully qualified domain name or an IP address.

Phase

(Optional) Enter the name of a phase or select an existing name from the Phase list. If you assign phases to sites, you can display only those sites that are members of a specific phase.

Group

(Optional) Enter the name of a group or select an existing name from the Group list. If you create groups of sites, you can display only those sites that are members of a specific group.

Authentication

If authentication is required, select a type from the list.

Weight

Weight is used to calculate the risk score that appears on the Sites form. The risk score for a site is equal to the risk score of the most recent completed scan of that site multiplied by the value you enter here. It allows the user to indicate that some sites are more important or have a higher risk than others. For example, the risk associated with vulnerabilities in an external-facing site could be weighted higher than vulnerabilities in an internal-only site because of the level of exposure. The weight can be any value between zero and 10.

Host

Add or select an IP address for each server that hosts a portion of the Web site.

If the Web site is configured on a server that hosts more than one domain name, select **Virtual Host**.

Information

Platform

- Operating System: Enter the name of the operating system used by servers at this site.
- Web Platform: Specify the Web platform.

Contact

Enter the name and e-mail address of the contact person.

Notes

Enter any notes about this site that may be helpful.

Tags

Tags are user-configurable fields designed to help you group or sort sites and other objects. See Tags on page 79 for instructions on creating tags.

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 77, with the following additions:

Schedule

General

Schedule Name

Enter a name that identifies this scheduled scan request.

Start Time

Enter the date and time you want the scan to begin. If you click the drop-down arrow, you can select the date from a calendar.

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 the scan last occurred.

Recurrence

To schedule a scan, Smart Update, or blackout on a recurring basis:

Recurring

Select this 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, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to 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 event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled scan requests. See Tags on page 79 for instructions on creating tags.

Discovery Scan Settings

General

Discovery Template

Instead of specifying each individual setting that the scanner requires every time you conduct a scan, you can create templates that contain different settings and then simply select a template from this list. You are not required to use a template. If you specify a template, you can deviate from those template settings (for this scan only) if you select the Create custom discovery from template option.

Discovery Name

Enter a unique name for this discovery scan.

Discovery Sensor

Choose a sensor to conduct the scan. You can choose a specific sensor or select the Any Available option.

Scan Discovered Sites

If you do not, under any conditions, want to scan a discovered site, select **Never scan**.

If you want to assess the vulnerabilities of a discovered site that is not already in the site catalog, select **Scan new sites only**. To scan all discovered sites, regardless of whether they have been scanned previously, select **Always scan**. If you choose either of the two scanning options, then:

- The Discovered Site Scan Settings group appears. Use the Selected Sensor list to choose the sensor that will scan the discovered site, then select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority takes precedence.
- Several settings panels appear in the left navigation pane. Use these to configure settings for scanning the discovered site. These settings are the same as described in Advanced Scan Settings on page 77.

Tags

See Tags on page 79 for instructions on creating tags.

1. Enter a name in the **Tag Name** box.
2. In the **Tag Value** box, enter one of the values to be associated with the tag name.
3. Click **Add**.
4. Repeat steps 2-3 to create additional values for the tag name.

To select a tag for a Discovery scan:

1. If necessary, expand the list of values associated with a tag name.
2. Select a value.
3. Click **Add**.

Settings

Use Discovery Template

Instead of specifying each individual setting that the scanner requires every time you conduct a scan, you can create templates that contain different settings and then simply select a template from this list. You are not required to use a template. If you specify a template, you can deviate from those template settings (for this scan only) if you select the Create custom discovery from template check box.

IP Range

Select an entry from the list, or type a range of addresses using the following guidelines:

To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.

Example: 172.16.10.2-172.16.10.99

You can specify multiple individual addresses or ranges by separating each entry with a semicolon or comma.

Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254

Port Range

Select an entry from the list or type a range of port numbers, using a hyphen to separate the lowest port number from the highest. Separate multiple entries with a semicolon.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, AMP will close the socket and terminate the scan.

Socket Count

Adjust the number of open sockets by moving the slider. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be 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.

Run script when a new site is discovered

If you select this check box, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- SPIIPAddress - The IP address of the site
- SPIPort - The port number
- SPIProtocol - The protocol (HTTP or HTTPS)

Use the **Command** text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).

Discovered Site Tags

Add or select the tags to be used when scanning a site that is revealed by this Discovery scan.

Discovery Template Settings

To create a scan Discovery template, click Add and then specify the template settings, which are described below:

Discovery

General

Discovery Template Name

Enter a unique identifier for this template.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, the scanner will close the socket and terminate the scan.

Socket Count

Adjust the number of open sockets by moving the Open Sockets slider. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be 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.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as Discovery scan templates. See Tags on page 79 for instructions on creating tags.

Sensors

Select one or more sensors from the available list. The selected sensors will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to sensors, select the **Use Any Available** check box.

To restrict access to specific sensors:

1. If necessary, clear the **Use Any Available** check box.
2. To add a sensor, select a sensor in the **Available** area and click **>**. The sensor name is removed from the **Available** list and added to the **Selected** list.
3. To remove a sensor, select a sensor in the **Selected** list and click **<**. The sensor name is removed from the **Selected** list and added to the **Available** list.
4. To add all available sensors, click **>>**.
5. To remove all selected sensors, click **<<**.

IP Ranges

Specify the IP addresses that will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to IP addresses, select the **Allow user to specify any IP Ranges** check box.

To restrict access to specific IP addresses:

1. If necessary, clear the **Allow user to specify any IP Ranges** check box.
2. In the **IP Range** box, type a range of addresses or multiple individual addresses using the following format:
   - To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.

     Example: 172.16.10.2-172.16.10.99
   - You can specify multiple individual addresses or ranges by separating each entry with a semicolon.

     Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254
3. Click **Add**.

4. Repeat for additional entries.

Port Ranges

Specify the ports that will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to port numbers, select the **Allow user to specify any Port Ranges** check box.

To restrict access to specific ports:

1. If necessary, clear the **Allow user to specify any Port Ranges** check box.
2. In the **Port Ranges** box, type a range of port numbers or multiple individual port numbers using the following format:
   - To specify a range, type the lowest port number in the range followed by a hyphen and then the highest port number in the range.

     Example: 1-8080
   - You can specify multiple individual ports or ranges by separating each entry with a semicolon.

     Example: 1-55;80;443;8080
3. Click **Add**.
4. Repeat for additional entries.

Scan Discovered

General

Scan Discovered Sites

Specify if and how you want discovered sites to be scanned.

- Never Scan: Discovered sites will be reported, but not scanned.
- Scan new sites only: Sites that have not been scanned previously will be scanned.
- Always scan: All discovered sites will be scanned, even if that site already exists in the scan database.

If you choose to scan a discovered site, settings options appear in the left column. These settings are the same as those described for a scan (see Advanced Scan Settings on page 77). In addition, there is a Sensors option (in the Scan Discovered group) that allows you to select the sensor that should be used for conducting the scan of a discovered site.

Run Script

If you select this check box, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- SPIIPAddress - The IP address of the site
- SPIPort - The port number
- SPIProtocol - The protocol (HTTP or HTTPS)

Use the **Command** text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).

Custom Scan Settings

This option appears if you elect to scan a discovered site. Select this check box if you want to permit the user to change scan settings when applying this template.

Maximum Priority

This option appears if you elect to scan a discovered site. Assign a priority to scans conducted with this template. Priority ranges from 1 (the highest) to 5 (the lowest).

Discovery Schedule Settings

To schedule a Discovery scan, click Add and then specify the settings. These are the same settings used for scheduling a scan, which are described Scan Schedules on page 67.

Schedule

General

Schedule Name

Enter a name that identifies this scheduled scan request.

Start Time

Enter the date and time you want the scan to begin. If you click the drop-down arrow, you can select the date from a calendar.

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 the scan last occurred.

Recurrence

Use these settings to schedule a scan on a recurring basis.

Recurring

Select this check box to conduct recurring scans.

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, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to 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 event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled scan requests. See Tags on page 79 for instructions on creating tags.

Discovery

General

Discovery Template

Instead of specifying each individual setting that the scanner requires every time you conduct a scan, you can create templates that contain different settings and then simply select a template from this list. You are not required to use a template. If you specify a template, you can deviate from those template settings (for this scan only) if you select the Create custom discovery from template option.

Discovery Sensor

Choose a sensor to conduct the scan. You can choose a specific sensor or select the Any Available option.

Scan Discovered Sites

If you do not, under any conditions, want to scan a discovered site, select **Never scan**.

If you want to assess the vulnerabilities of a discovered site that is not already in the site catalog, select **Scan new sites only**. To scan all discovered sites, regardless of whether they have been scanned previously, select **Always Scan**. If you choose either of the two scanning options, then:

- The Discovered Site Scan Settings group appears. Use the **Selected Sensor** list to choose the sensor that will scan the discovered site, then select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority takes precedence.
- Several settings panels appear in the left navigation pane. Use these to configure settings for scanning the discovered site.

Settings

Use Discovery Template

Instead of specifying each individual setting that the scanner requires every time you conduct a scan, you can create templates that contain different settings and then simply select a template from this list. You are not required to use a template. If you specify a template, you can deviate from those template settings (for this scan only) if you select the Create custom discovery from template check box.

IP Range

Select an entry from the list, or type a range of addresses using the following guidelines:

- To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.

  Example: 172.16.10.2-172.16.10.99

- You can specify multiple individual addresses or ranges by separating each entry with a semicolon or comma.

  Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254

Port Range

Select an entry from the list or type a range of port numbers, using a hyphen to separate the lowest port number from the highest. Separate multiple entries with a semicolon.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, AMP will close the socket and terminate the scan.

Socket Count

Adjust the number of open sockets by moving the slider. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be 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.

Run script when a new site is discovered

If you select this check box, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- SPIIPAddress - The IP address of the site
- SPIPort - The port number
- SPIProtocol - The protocol (HTTP or HTTPS)

Use the Command text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).

Discovered Site Tags

Add or select the tags to be used when scanning a site that is revealed by this Discovery scan.

Tags are user-configurable fields designed to help you group or sort various objects, such as Discovery scans. See Tags on page 79 for instructions on creating tags.

Blackout Settings

General

Name

Enter a unique identifier for this blackout period.

Addresses

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, but wildcards for host names must be at the beginning.

Examples:

192.16.12.1-192.16.12.210

192.16.12.*

*.domain.com

Start Time

The date and time at which the blackout period begins.

End Time

The date and time at which the blackout period expires.

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 of the specified targets are allowed only during the specified time period.
- Deny: Scans of the specified targets are prohibited during the specified time period.

Allow and deny work very much like allow and deny for 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 deny scans UNLESS you are in the allowed range, as opposed to 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 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 this 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, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to 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 event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as blackout periods. See Tags on page 79 for instructions on creating tags.

7 Reporting

Introduction

You can create a report using one of the standard templates or you can create a unique report by selecting options from the list of available components.

You can also generate a compliance report, which provides a pass/fail score for each statement in the compliance portion of the policy used for auditing your site. The summary area reports, for each statement, the total number of checks, the number of checks that passed, and the percentage that passed. The detail area provides a description of each vulnerability.

Generating a Report

There are two ways to create a report. You can schedule a report to be generated as part of a scheduled scan, or you can manually initiate a report after any scan (including a scheduled one) is complete.

Manual Report

To initiate a report manually:

1. Select the **Scans** group and click the **Scans** shortcut
   -or-
   Select the **Reports** group and click the **Generate Report** shortcut.
2. Select a scan with a check mark in the **Results** column. You can also select multiple scans using the CTRL or SHIFT keys.
3. Click the **Action** menu and select **Generate Report**.

   The *Report Settings* dialog appears. There are three categories of settings: General, Options, and Graphics.
4. On the General settings:
   a. Select a naming convention:
      - If you want the AMP manager to assign a name to the file based on the time and date, select **Automatically generate report name**. Use this option if you are generating reports for recurring scans and you want to preserve each report.
      - If you want to specify a file name, clear the **Automatically generate report name** check box and then type the name in the **Name** box. Do not use this option for recurring scans unless you want to overwrite the old report each time the scan is conducted.

   b. Enter a brief description of the report.

c Select a format from the **Output Type** list.

5 Click the **Options** category and select one of the following report types:

- **Report Template**
- **Compliance Template**

6 If you select **Report Template**, choose an entry from the **Report Template** list.

If you want to modify the contents of the template, select **Customize selected report template**, modify the description, and select the components you want to generate. Where necessary, click the plus sign next to a category to expand the structure and view additional choices. The report components are:

- **Executive Summary** — Basic statistics, plus charts and graphs that reflect your application's level of vulnerability.
- **Vulnerability** — Detailed report of each vulnerability (selectable by severity), with recommendations concerning solutions. You can also include HTTP requests and responses.
- **Alert View** — List of each successful attack agent and the URLs on which the associated vulnerability was discovered (as the information appears on the Alert tab of the Summary pane).
- **QA Summary** — List of the URLs of all pages containing broken links, server errors, external links, and timeouts. You can select one or more of these categories.
- **Crawled URLs** — Sequential list of the URLs that were inspected, the HTTP request and the HTTP response. You can select one or more of these categories.
- **Attack Status** — Lists the name, ID number, and severity rating of all attack agents, and indicates if the agent is enabled and if the target application passed or failed the agent's test.
- **Developer Reference** — Totals and detailed description of each form, JavaScript, e-mail, comment, hidden control, and cookie discovered on the Web site. You can select one or more of these reference types.
- **Trend** – This report allows you to monitor your development team's progress toward resolving vulnerabilities. For example, you save the results of your initial scan and your team begins fixing the problems. Then once a week, you rescan the site and archive the results. To quantify your progress, you run a trend report that analyzes the results of all scans conducted to date. The report includes a graph showing the number of vulnerabilities, by severity, plotted on a time line defined by the date on which each scan was conducted.

  Important: To obtain meaningful results, make sure you conduct each scan using the same policy.
- **Aggregate** — This report allows you to combine the scan results of multiple servers. It lists the total number of vulnerabilities, by severity, and displays an associated bar chart. It also tabulates the vulnerabilities for each individual server.
- **Comparison** — This report graphs the results of each selected scan, plotting the number of vulnerabilities for each vulnerability category (i.e., critical, high, medium, low, and information). You may optionally include a list of all URLs scanned and a list of URLs mapped to each specific vulnerability.
- **Scan Log** — Sequential list of the activities conducted by the scanner during the scan (as the information appears on the **Scan Log** tab of the Summary pane).

- **False Positive** — This report lists all URLs that originally were flagged as containing a vulnerability and which a user later determined were false positives.

7 If you select **Compliance Template**, choose one of the listed templates.

8 Click the **Graphics** category.

  a Choose a set of graphics from the **Report Graphics** list.

  b If you want to modify any of the graphics or the headers and footers, select **Customize the selected report graphics**.

9 Click **OK** to generate the report.

The AMP manager will create an entry on the Reports form, where you can view the report.

Scheduled Report

Follow the steps below to create a report automatically with a scheduled scan:

1 Click the **Schedules** group.

2 Click the **Scheduled Scans** shortcut.

  You can also use the Calendar to schedule a scan.

3 From the **Action** menu, select **Add**.

4 When the *Scan Settings* dialog appears, select the categories in the left column and provide the requested information.

5 On the Report panel, select **General**.

  a If you are using a template that does not include a report, select **Customize report settings**.

  b Select **Generate Report** and enter the requested information (described above).

6 On the Report panel, select **Options** and enter the requested information (described above).

7 If you want to send an e-mail containing a hyperlink to the generated report, click **E-Mail**.

8 If you want to export the scan report, then on the Report panel, select **Export**.

  a Select **Export Scan Results**.

  b Specify a location and format for the exported file.

  c Select a naming convention:

  If you want the AMP manager to assign a name to the file based on the time and date, select **Automatically generate report name**. Use this option if you are generating reports for recurring scans and you want to preserve each report.

  If you want to specify a file name, clear the **Automatically generate report name** check box and then type the name in the **Name** box. Do not use this option for recurring scans unless you want to overwrite the old report each time the scan is conducted.

9 Click **OK** to generate the report.

Creating a Report Template

AMP provides seven predefined report templates:

- Standard
- Comprehensive
- Basic
- Developer
- QA
- Executive
- False Positive

Each template has a different selection of report components.

You cannot delete or change a predefined template. However, you can create a template that contains any combination of report options. Unlike the predefined (locked) templates, you can modify or delete the templates that you create.

Follow the steps below to create a report template:

1. Click the **Reports** group.
2. Click the **Report Templates** shortcut.
3. Click the **Action** menu and select **Add**.
4. Provide a name and description for the template.
5. Specify components to include in the report by selecting the appropriate check boxes. Where necessary, click the plus sign to expand a category.
6. When done, click **OK**.

Viewing a Report

You must first generate a report. You can do this either manually or as part of a scheduled scan.

Follow the steps below to view a report:

1. Click the **Reports** group.
2. Click the **Reports** shortcut.
3. Select a report and choose **View** from the **Action** menu (or from the shortcut menu that appears when you right-click a selection).
   - If you select a report created using the Adobe portable document format (.pdf), Adobe Reader opens and displays the report. Adobe Reader 7.0 or newer is required.
   - If you select a report in HTML format, the AMP server delivers the selected report in a .zip format. Select **Save** (do not select **Open**) and save the .zip file in the location you choose. Then, offline (outside the AMP user interface) extract the .zip file contents and open the HTML file using an appropriate application (such as Internet Explorer or, if you want to publish the report, Microsoft Word).

Possible Problems

PDF report does not open in browser.

If the program prompts you to save a .pdf file instead of opening it, then you are connected to the AMP console via SSL, you are using Microsoft Internet Explorer, and you have set your Internet options so that encrypted pages are not saved to disk.

To enable viewing of a .pdf report with Internet Explorer:

1. Click **Tools** and select **Internet Options**.
2. Click the **Advanced** tab.
3. In the **Security** group, clear **Do not save encrypted pages to disk**.

PDF report displays a blank page in browser.

This may occur if you alternate between secure and nonsecure connections to the AMP console. To resolve, enter the following command from the command line: IISReset.

The HTML file fails to download.

This occurs if your browser is not allowing downloads. On Microsoft Internet Explorer, check these settings:

1. Click **Tools**.
2. Select **Internet Options**.
3. Click the **Security** tab.
4. Click **Custom level**.
5. In the **Downloads** group, File download, select **Enable**.

Other Precautions

Clear your browser cache. For Internet Explorer:

1. Click **Tools** → **Internet Options.**
2. On the **General** tab, click **Browsing History/Delete** (7.0) or **Temporary Internet Files/Delete files** (6.0).

Check for newer versions of cached pages. For Internet Explorer:

1. Click **Tools** → **Internet Options**.
2. On the **General** tab, click **Browsing History/Settings** (7.0) or **Temporary Internet Files/Settings** (6.0).
3. Under **Check for newer versions of stored pages**, select **Every time I visit the webpage** (7.0) or **Every visit to the page** (6.0).

Exporting a Report

Follow the steps below to export a report:

1. Click the **Reports** group.

2. Click the **Reports** shortcut.
3. Select a report.
4. Choose **Export Report** from the **Action** menu (or from the shortcut menu that appears when you right-click a selection).
5. On the *Save As* dialog, in the **File name** field, type a name for the exported report.
6. Select the directory in which you want to save the report.
7. Click **Save** to export your report in the chosen format.

A AMP Tools

Introduction

The AMP Console includes a robust set of tools and configuration options. These are:

- Smart Update
- Options
- Encoders/Decoders
- HTTP Editor
- SOAP Editor
- Regex Editor
- Web Proxy
- Web Form Editor
- Web Macro Recorder
- SQL Injector
- Web Brute
- Web Discovery
- Cookie Cruncher
- Web Fuzzer
- Server Analyzer
- Report Designer
- Policy Manager (accessible from the Scan Policies form in the Scans/Compliance group)
- Audit Inputs Editor (accessible from the Policy Manager's **Tools** menu)
- Compliance Manager (accessible from the Compliance Templates form in the Scans/Compliance group)

Certain tools are not enabled unless HP WebInspect and the AMP Console are installed on the same machine.

Options

Use the following procedure to specify settings for the AMP console.

1 From the **Tools** menu, select **Options**.

2 To refresh the display of AMP information periodically, select the **Automatically refresh display** check box and specify how often (in seconds) the display should be updated.

3 In the **Scan History** group, enter the maximum number of URLs that will appear in the drop-down list that you use when specifying which URL you will scan.

4 To delete the history, click **Clear URL History**.

5 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.

AMP 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

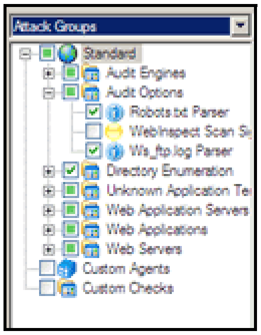
The Policy Manager has two different views, selectable from the **View** menu or by clicking icons on the toolbar. They are:

- Standard
- Search

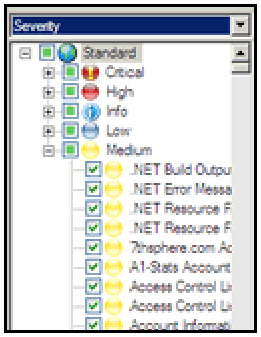
Standard View

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.

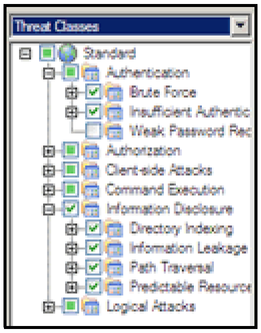
You enable or disable a component by selecting or clearing its associated check box.



Attack Groups



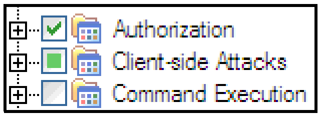
Severity



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.

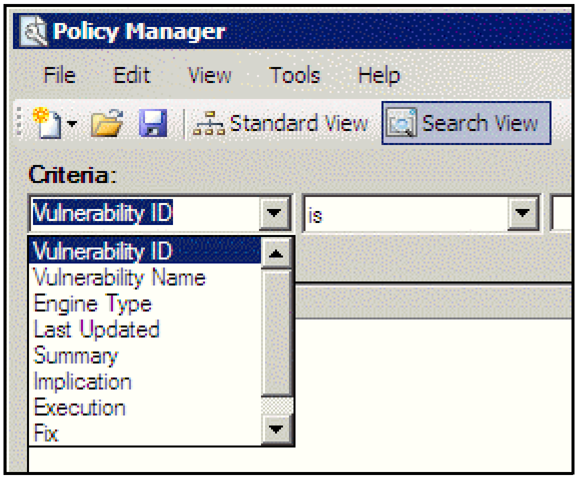


Click the plus sign ⊞ to expand a node.

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.

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 AMP. 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.

Follow the steps below to edit a policy:

1 On the AMP Console, click the **Scans/Compliance** group.

2 Click the **Scan Policies** shortcut.

3 Select a policy.

4 Click the **Action** menu and select **Copy**.

The AMP Console downloads the policy from the AMP 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 127 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.

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.

Follow the steps below to create a custom check:

1 On the AMP Console, click the **Scans/Compliance** group.

2 Click the **Scan Policies** shortcut.

3 Select a policy.

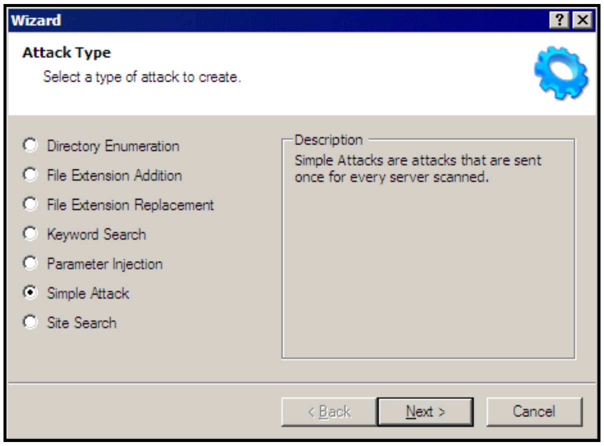
4 Click the **Action** menu and select **Copy**.

The AMP Console downloads the policy from the AMP 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.



Wizard

Attack Type

Select a type of attack to create.

○ Directory Enumeration
○ File Extension Addition
○ File Extension Replacement
○ Keyword Search
○ Parameter Injection
● Simple Attack
○ Site Search

Description

Simple Attacks are attacks that are sent once for every server scanned.

The attack types are listed below. See Steps 9-10 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.

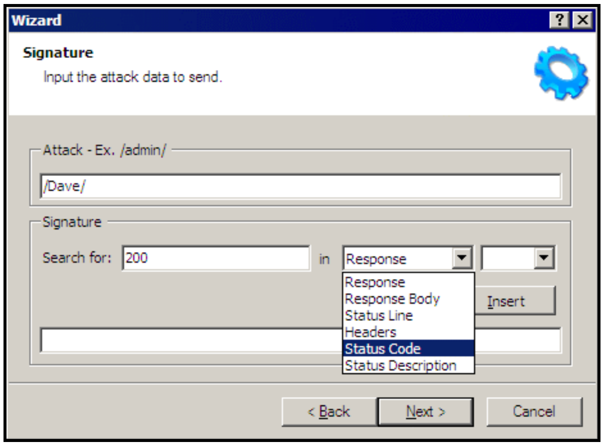
  The following example searches for a file named xanadu.html by appending the attack string to the target URL or IP address:

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.

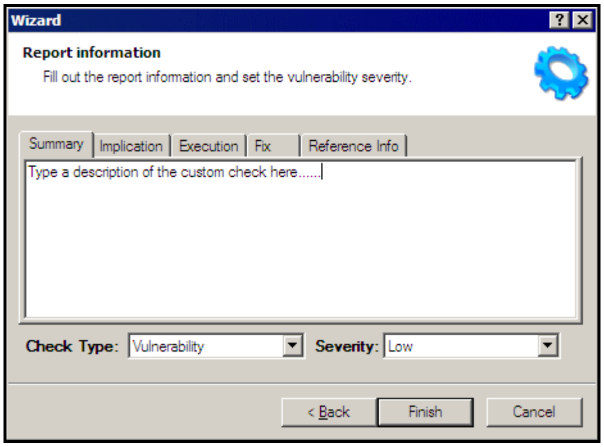
c Click the drop-down arrow to specify the section of the HTTP response that should be searched.

d (optional) 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 steps a-d as needed. You can also edit or replace the regular expression that appears in the bottom text box.

11 Click **Next**.


Wizard
Report information
Fill out the report information and set the vulnerability severity.
Summary
Implication
Execution
Fix
Reference Info
Type a description of the custom check here......
Check Type: Vulnerability
Severity: Low
< Back
Finish
Cancel

12 On the Report Information panel, click each tab and enter the text that will appear in the vulnerability description.

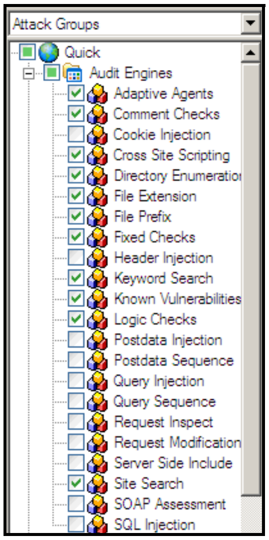
13 Select an entry from the **Check Type** list.

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.



Attack Groups

- ▣ Quick
  - ▣ Audit Engines
    - ☑ Adaptive Agents
    - ☑ Comment Checks
    - ☐ Cookie Injection
    - ☑ Cross Site Scripting
    - ☑ Directory Enumeratio
    - ☑ File Extension
    - ☑ File Prefix
    - ☑ Fixed Checks
    - ☐ Header Injection
    - ☑ Keyword Search
    - ☑ Known Vulnerabilities
    - ☑ Logic Checks
    - ☐ Postdata Injection
    - ☐ Postdata Sequence
    - ☐ Query Injection
    - ☐ Query Sequence
    - ☐ Request Inspect
    - ☐ Request Modification
    - ☐ Server Side Include
    - ☑ Site Search
    - ☐ SOAP Assessment
    - ☐ SQL Injection

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 126.

Disabling a Custom Check

Follow the steps below to disable a custom check:

1. Select a custom check.
2. Clear its associated check box.

Deleting a Custom Check

Follow the steps below to delete a custom check:

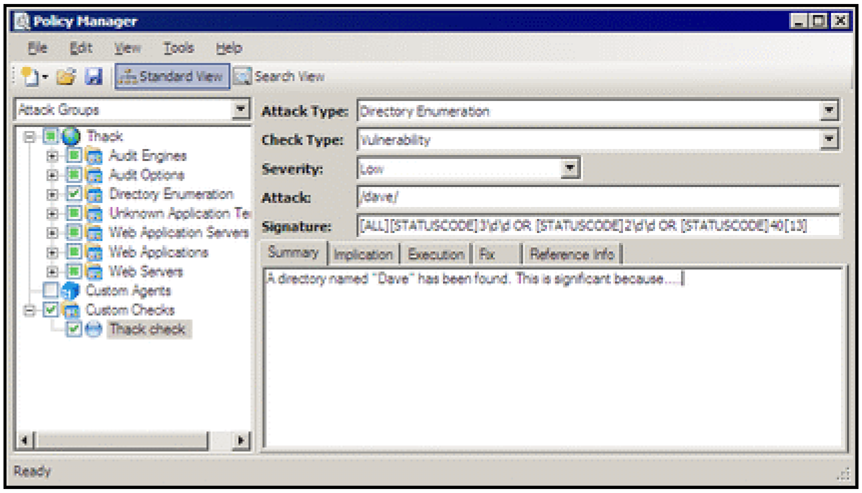
1. Right-click a custom check.
2. Select **Delete** from the short-cut menu.

If you delete a custom check from a policy, you delete it from all policies and from the entire system.

Editing a Custom Check

Follow the steps below 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.



Attack Type: Directory Enumeration

Check Type: Vulnerability

Severity: Low

Attack: /dave/

Signature: [ALL][STATUSCODE]3\d\d OR [STATUSCODE]2\d\d OR [STATUSCODE]40[13]

A directory named "Dave" has been found. This is significant because.....

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.

Follow the steps below 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 WebInspect the saved file containing your check input modifications. To do so:

1. On the WebInspect menu bar, click **Edit** → **Default Settings**.
2. Under Audit Settings, select **Attack Exclusions**.
3. Click **Import Audit Inputs**.
4. Select the file you created and click **Open**.

Engine Inputs

Follow the steps below 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 WebInspect 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 Unselect 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. WebInspect conducts these checks using default values, which you may need to change.

Follow the steps below 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 **OK** (if you launched the Audit Inputs Editor from Default or Current Settings) or click **File** → **Save** (or **Save As**, if you launched the Audit Inputs Editor from the Policy Manager).

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://216.183.127.201/serverinclude.html?" which is a special page hosted on an HP Web server located on the public Internet at IP address 216.183.127.201. 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.

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.

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:

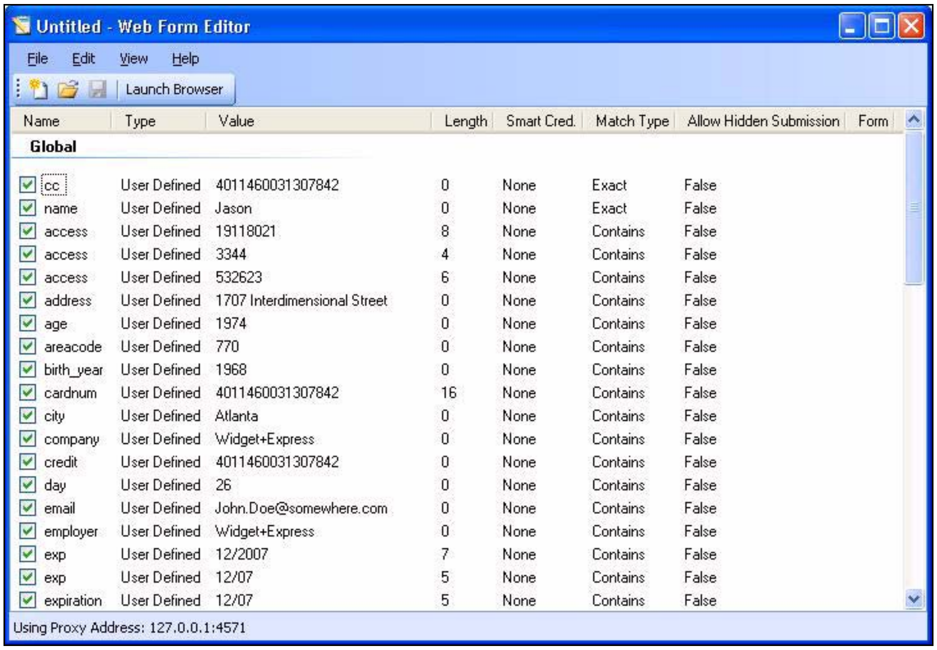
- Create the list manually.
- Record the values as you navigate through the application.

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.



Name	Type	Value	Length	Smart Cred.	Match Type	Allow Hidden Submission	Form
Global							
☑ cc	User Defined	4011460031307842	0	None	Exact	False	
☑ name	User Defined	Jason	0	None	Exact	False	
☑ access	User Defined	19118021	8	None	Contains	False	
☑ access	User Defined	3344	4	None	Contains	False	
☑ access	User Defined	532623	6	None	Contains	False	
☑ address	User Defined	1707 Interdimensional Street	0	None	Contains	False	
☑ age	User Defined	1974	0	None	Contains	False	
☑ areacode	User Defined	770	0	None	Contains	False	
☑ birth_year	User Defined	1968	0	None	Contains	False	
☑ cardnum	User Defined	4011460031307842	16	None	Contains	False	
☑ city	User Defined	Atlanta	0	None	Contains	False	
☑ company	User Defined	Widget+Express	0	None	Contains	False	
☑ credit	User Defined	4011460031307842	0	None	Contains	False	
☑ day	User Defined	26	0	None	Contains	False	
☑ email	User Defined	John.Doe@somewhere.com	0	None	Contains	False	
☑ employer	User Defined	Widget+Express	0	None	Contains	False	
☑ exp	User Defined	12/2007	7	None	Contains	False	
☑ exp	User Defined	12/07	5	None	Contains	False	
☑ expiration	User Defined	12/07	5	None	Contains	False	

Using Proxy Address: 127.0.0.1:4571

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 (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 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.”
- If you select **Mark As Interactive Input**, the scanner will pause the scan and display a window prompting the user to enter a value for this entry (if the scan options include the settings **Prompt For Web Form Values During Scan** and **Only Prompt Tagged Inputs**).

  It is not necessary to tag passwords with **Mark As Interactive Input**.

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.).

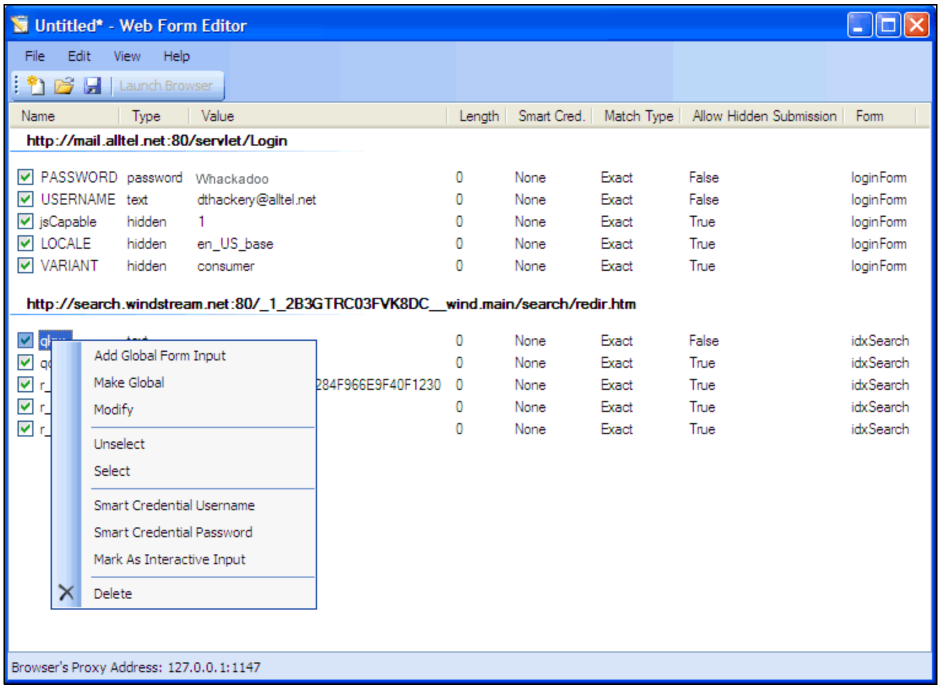
6 Navigate to additional pages and submit forms until you have traversed all the links you wish to follow.

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.


Untitled* - Web Form Editor
File
Edit
View
Help
Launch Browser
Add Global Form Input
Make Global
Modify
Unselect
Select
Smart Credential Username
Smart Credential Password
Mark As Interactive Input
Delete

Name	Type	Value	Length	Smart Cred.	Match Type	Allow Hidden Submission	Form
http://mail.alltel.net:80/servlet/Login							
☑ PASSWORD	password	Whackadoo	0	None	Exact	False	loginForm
☑ USERNAME	text	dthackery@alltel.net	0	None	Exact	False	loginForm
☑ jsCapable	hidden	1	0	None	Exact	True	loginForm
☑ LOCALE	hidden	en_US_base	0	None	Exact	True	loginForm
☑ VARIANT	hidden	consumer	0	None	Exact	True	loginForm
http://search.windstream.net:80/_1_2B3GTRC03FVK8DC__wind.main/search/redir.htm							
☑ q			0	None	Exact	False	idxSearch
☑ q			0	None	Exact	True	idxSearch
☑ r_		284F966E9F40F1230	0	None	Exact	True	idxSearch
☑ r_			0	None	Exact	True	idxSearch
☑ r_			0	None	Exact	True	idxSearch

Browser's Proxy Address: 127.0.0.1:1147

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 WebInspect 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

Follow the steps below 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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).

Table 3 Rules for Matching Web Form Values (cont’d)

	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).
	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

Follow the steps below to use a brute force authentication attack:

1 On the AMP 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**.

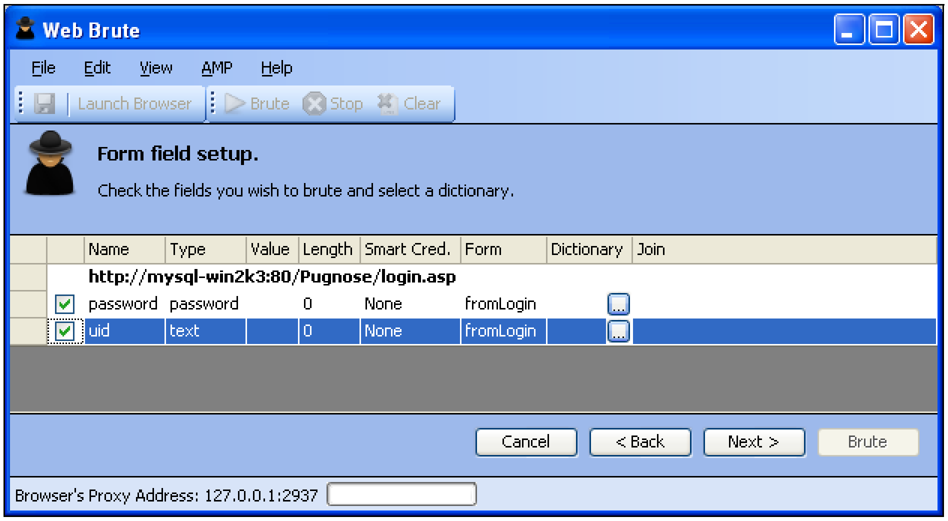
3 Select the authentication type used by the target site. See Table 9 on page 114 for a description of the available authentication types.

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.



Form field setup.

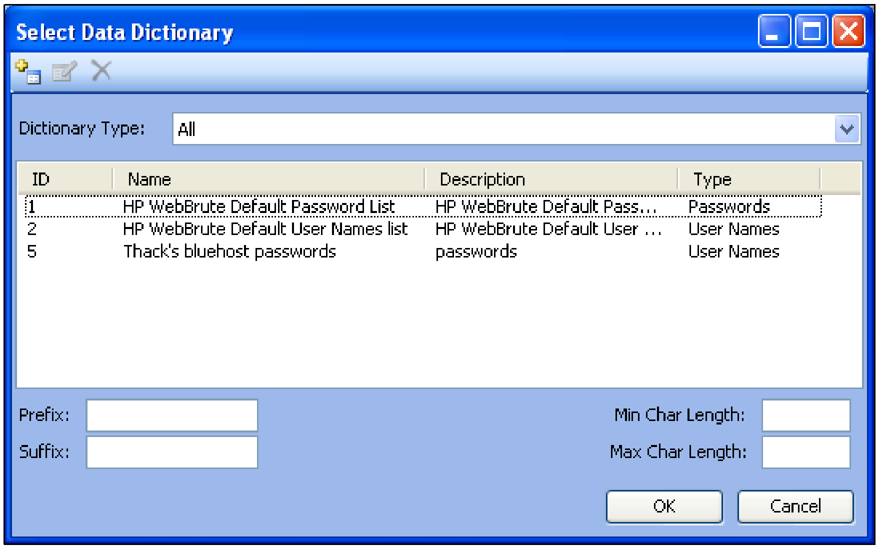
Check the fields you wish to brute and select a dictionary.

	Name	Type	Value	Length	Smart Cred.	Form	Dictionary	Join
	http://mysql-win2k3:80/Pugnose/login.asp							
☑	password	password		0	None	fromLogin	...	
☑	uid	text		0	None	fromLogin	...	

Browser's Proxy Address: 127.0.0.1:2937

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.



Dictionary Type: All

ID	Name	Description	Type
1	HP WebBrute Default Password List	HP WebBrute Default Pass...	Passwords
2	HP WebBrute Default User Names list	HP WebBrute Default User ...	User Names
5	Thack's bluehost passwords	passwords	User Names

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 154.

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 steps 7-11 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 155 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.

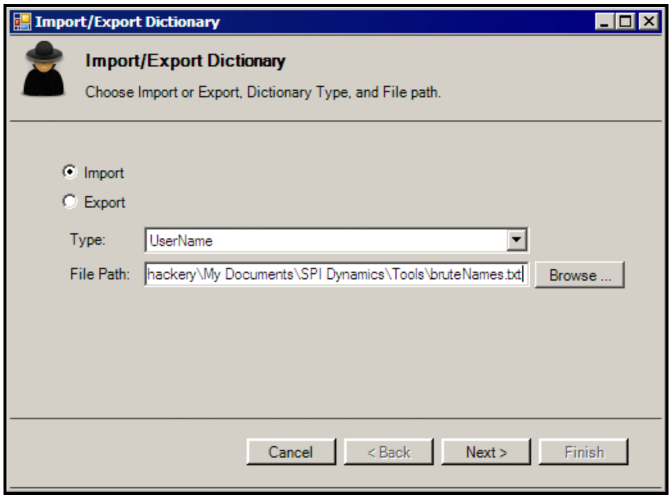
Creating and Importing Lists

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**.



Import/Export Dictionary

Choose Import or Export, Dictionary Type, and File path.

● Import

○ Export

Type: UserName

File Path: hackery\My Documents\SPI Dynamics\Tools\bruteNames.txt

4 From the **Type** list, select either **UserName** or **Password**.

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 From the **Type** list, select either **UserName** or **Password**.

4 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.

5 Click **Next**.

6 On the *Export Dictionary* window, select a dictionary.

7 Click **Next**.

8 Click **Finish**.

9 Click **Done**.

Web Brute Settings

Follow the steps below 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 type.
- **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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.

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.

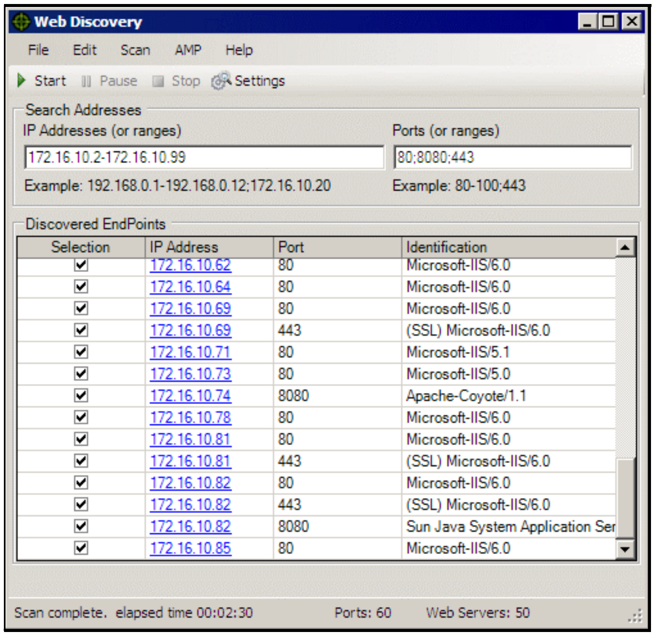
Web Discovery

Web Discovery will send packets to all the open ports (in a range of IP addresses and ports that you specify), search the server's response for specific information, and then display 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 will search 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.



Search Addresses

IP Addresses (or ranges): 172.16.10.2-172.16.10.99

Example: 192.168.0.1-192.168.0.12;172.16.10.20

Ports (or ranges): 80;8080;443

Example: 80-100;443

Discovered EndPoints

Selection	IP Address	Port	Identification
☑	172.16.10.62	80	Microsoft-IIS/6.0
☑	172.16.10.64	80	Microsoft-IIS/6.0
☑	172.16.10.69	80	Microsoft-IIS/6.0
☑	172.16.10.69	443	(SSL) Microsoft-IIS/6.0
☑	172.16.10.71	80	Microsoft-IIS/5.1
☑	172.16.10.73	80	Microsoft-IIS/5.0
☑	172.16.10.74	8080	Apache-Coyote/1.1
☑	172.16.10.78	80	Microsoft-IIS/6.0
☑	172.16.10.81	80	Microsoft-IIS/6.0
☑	172.16.10.81	443	(SSL) Microsoft-IIS/6.0
☑	172.16.10.82	80	Microsoft-IIS/6.0
☑	172.16.10.82	443	(SSL) Microsoft-IIS/6.0
☑	172.16.10.82	8080	Sun Java System Application Ser
☑	172.16.10.85	80	Microsoft-IIS/6.0

Scan complete. elapsed time 00:02:30 Ports: 60 Web Servers: 50

Discovering Sites

To discover sites using Web Discovery:

1 In the **IP 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 159 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**.

2 Use the standard file-selection window to name and save the file.

Web Discovery Settings

Follow the steps below 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 packets you want to send by selecting or clearing the check box next to the packet's 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.

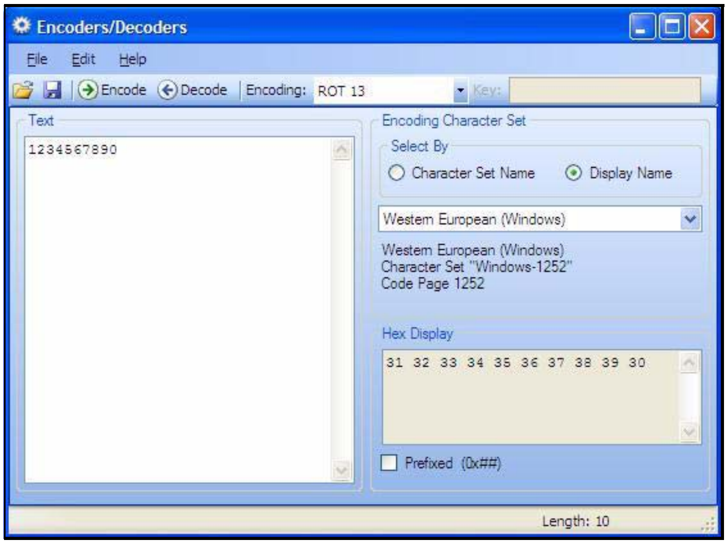
- **Receive**: When sending a message to the remote IP endpoint, the transmission is divided into smaller packets. If the Web Discovery tool does not receive the sent packet within the specified period of time, the socket is closed and the discovery for that endpoint reports no services.

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.

Encoder/Decoder

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: ROT 13

Text

```
1234567890
```

Encoding Character Set

Select By: ○ Character Set Name ● Display Name

Western European (Windows)

Western European (Windows)
Character Set "Windows-1252"
Code Page 1252

Hex Display

```
31 32 33 34 35 36 37 38 39 30
```

□ Prefixed (0x##)

Length: 10

Encoding a String

Follow the steps below 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 162.

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

Follow the steps below 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).
- SHA-256 uses 256-bit encryption.
- SHA-384 uses 384-bit encryption.
- SHA-512 uses 512-bit encryption.
- ToLower changes upper-case letters to lower-case.
- ToUpper changes lower-case letters to upper-case.
- 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.

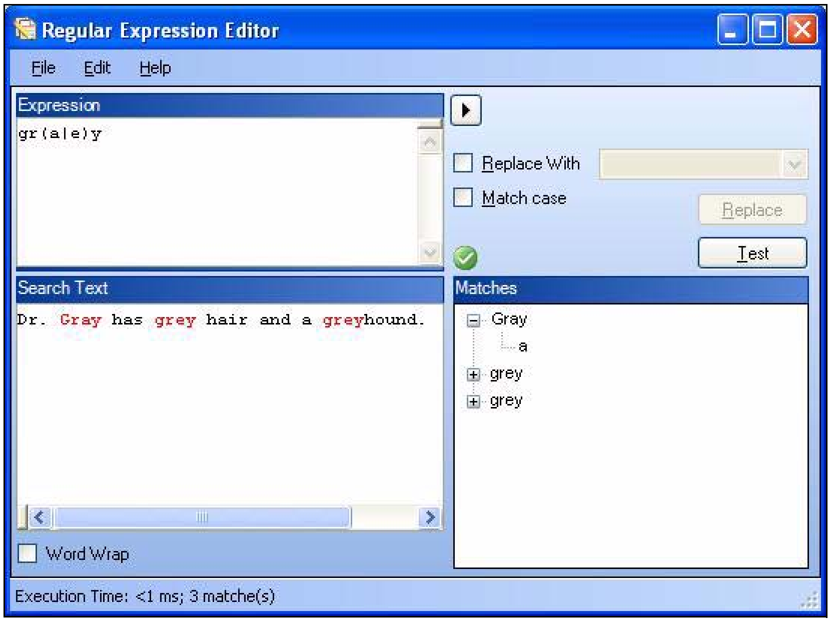
Testing a Regular Expression

Use the Regular Expression Editor to verify regular expressions.

Follow the steps below to use the Regular Expression Editor:

1 Click **Tools** → **Regex Editor.**

The *Regular Expression Editor* window opens.



Expression: gr(a|e)y

Search Text: Dr. Gray has grey hair and a greyhound.

Matches:
- Gray
  - a
- grey
- grey

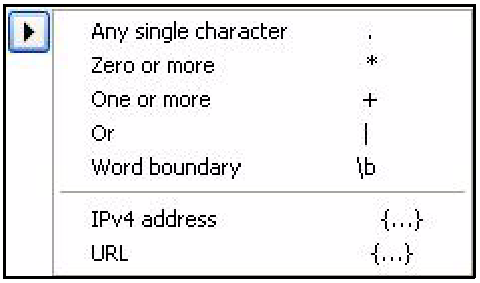
□ Replace With
□ Match case
□ Word Wrap

Execution Time: <1 ms; 3 matche(s)

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/[^(en|ca)].*/.* . 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.”

Table 4 Characters Used in Regular Expressions (cont'd)

Character	Description
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	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]

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

SOAP Editor

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 understands how to communicate with the service. The WSDL document describes what programmed procedures the Web service includes, what parameters those procedures expect, and the type of return information the client Web application will receive.

SOAP uses HTTP and XML as the means to exchange information so that programs on one platform can communicate with a program on the same or a different operating system. Use the SOAP Editor to generate SOAP requests automatically, and to manually edit SOAP requests and responses. You can also create and save a file containing values that should be submitted by an HP scanner when conducting a Web services assessment.

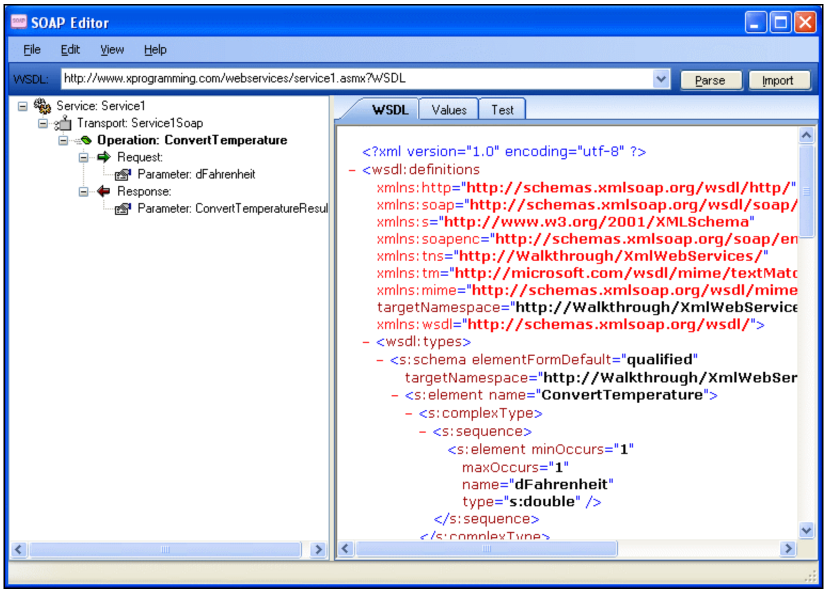
Submitting SOAP Requests

To submit SOAP requests:

1. Click **Tools** → **Soap Editor.**
2. Do one of the following:
   - In the **WSDL** box, type or select the URL of the WSDL site (example: http//:www.xprogramming.com/webservices/service1.asmx?WSDL).
   - Click **File** → **Import WSDL** (or click **Import**) and select a WSDL file that you previously saved locally (using the **Export WSDL** feature).

   Note: If authentication is required, or if SOAP requests need to be made through a proxy server, see SOAP Editor Settings on page 170 for more information.
3. Click **Parse**.

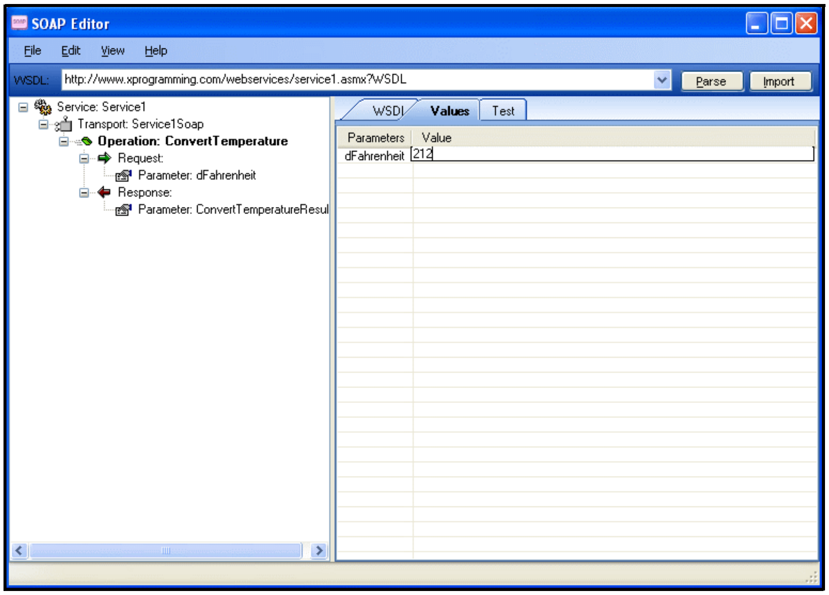
The SOAP editor lists all discovered operations.



WSDL: http://www.xprogramming.com/webservices/service1.asmx?WSDL

```
  <?xml version="1.0" encoding="utf-8" ?>
- <wsdl:definitions
    xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/
    xmlns:s="http://www.w3.org/2001/XMLSchema"
    xmlns:soapenc="http://schemas.xmlsoap.org/soap/en
    xmlns:tns="http://Walkthrough/XmlWebServices/"
    xmlns:tm="http://microsoft.com/wsdl/mime/textMatc
    xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime
    targetNamespace="http://Walkthrough/XmlWebService
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  - <wsdl:types>
    - <s:schema elementFormDefault="qualified"
        targetNamespace="http://Walkthrough/XmlWebSer
      - <s:element name="ConvertTemperature">
        - <s:complexType>
          - <s:sequence>
              <s:element minOccurs="1"
                maxOccurs="1"
                name="dFahrenheit"
                type="s:double" />
            </s:sequence>
          </s:complexType>
```

4 Click the **Values** tab and enter the Request parameters you want to submit.



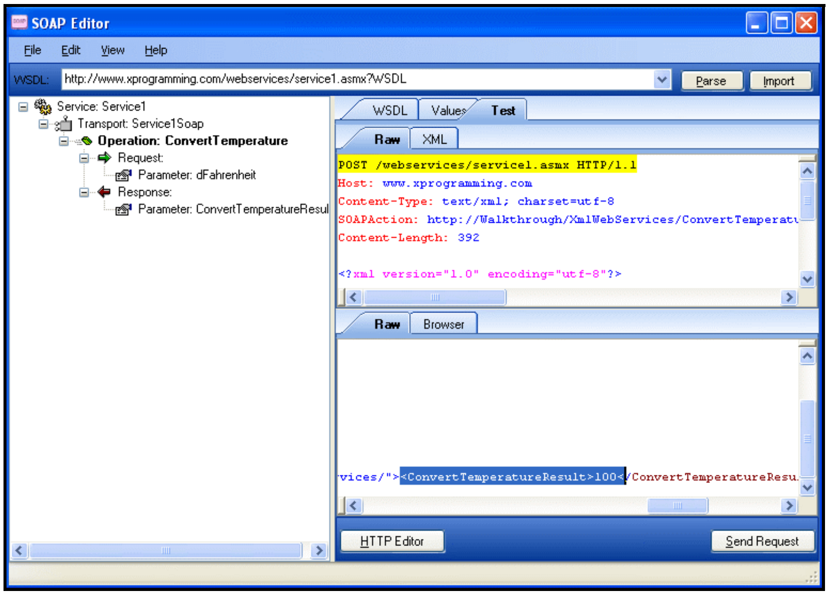
WSDL: http://www.xprogramming.com/webservices/service1.asmx?WSDL

Parameters	Value
dFahrenheit	212

5 Click the **Test** tab.

6 Select an operation. If necessary, edit the raw request on the Request Viewer **Raw** tab (the top pane). View the schema by clicking the **XML** tab.

7 Click **Send Request** to submit the request using the values you entered on the **Values** tab. The Response Viewer (the lower pane) displays the server response.



WSDL: http://www.xprogramming.com/webservices/service1.asmx?WSDL

```
POST /webservices/service1.asmx HTTP/1.1
Host: www.xprogramming.com
Content-Type: text/xml; charset=utf-8
SOAPAction: http://Walkthrough/XmlWebServices/ConvertTemperatu
Content-Length: 392

<?xml version="1.0" encoding="utf-8"?>
```

```
vices/"><ConvertTemperatureResult>100</ConvertTemperatureResu
```

8 (Optional) Click **HTTP Editor** (at the bottom of the Response Viewer) to view and edit the raw HTTP request. See HTTP Editor on page 174 for more information.

9 To save the values in a file that the scanner can use when conducting a Web service assessment, click **File** → **Save Values**.

When performing a Web service assessment, the scanner crawls the WSDL site and submits an arbitrary enumeration value for each parameter in each operation. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

You can tailor these attacks to your WSDL by creating a file containing specific values that should be submitted, and by selecting the option to “Auto-fill SOAP messages during crawl.”

You can create one Values file for each WSDL, or you can create a file containing values for all WSDLs that you intend to scan.

If you create individual files, be sure to clear all values before selecting a different WSDL (click **File** → **New Values**).

SOAP Editor Settings

Follow the steps below to modify the SOAP 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

Authentication Method

If the WSDL site does not require authentication, select **None**. Otherwise, select a type from the **Authentication** list:

Table 5 Authentication Types

Authentication	Description
Automatic	Allow the SOAP Editor to determine the correct authentication type. 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.

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 SOAP Editor should use.

Proxy

Use these settings to access the SOAP 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 SOAP 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 (as described in the preceding table).

SOAP Editor Menus

The SOAP Editor contains the following menus:

File

- **Open Values** - Load a Values file into the SOAP Editor. Use this function to edit a Values file or to add values for a different WSDL.

- **Save Values** - Create a file containing values you specify for request parameters.
- **New Values** - Clear all values in the SOAP Editor.
- **Import WSDL** - Load a WSDL file that you previously exported.
- **Export WSDL** - Save the current WSDL file to a local location.
- **Exit** - Close the SOAP Editor.

Edit

Settings - Create or edit SOAP Editor settings.

View

Word Wrap - Adjust lines of text to fit within the available viewing area.

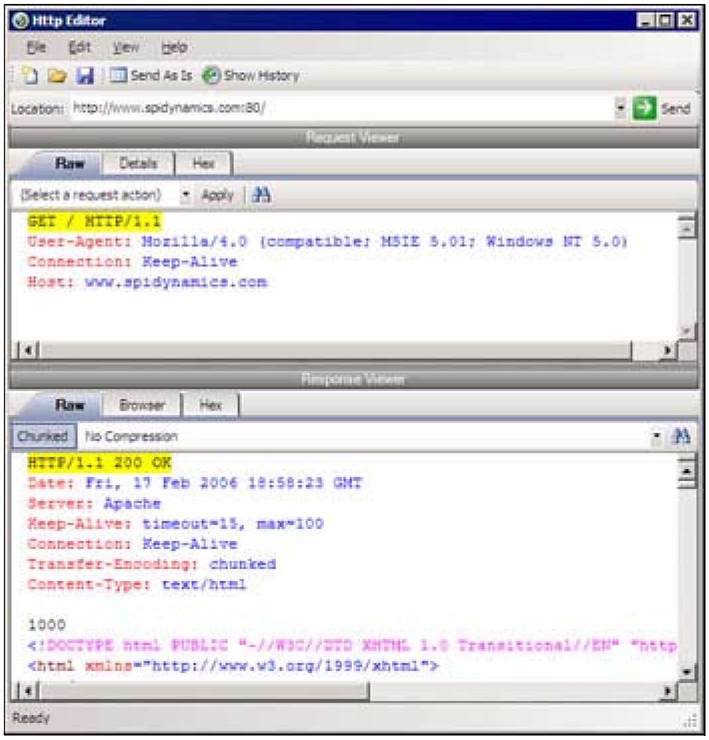
Help

- **SOAP Editor Help** - Open the Help file to the default topic.
- **Index** - Open the Help file, displaying the index pane.
- **Search** - Open the Help file, displaying the search pane.
- **About SOAP Editor** - Open a window that displays information about the SOAP Editor.

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**.



```
GET / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Connection: Keep-Alive
Host: www.spidynamics.com
```

```
HTTP/1.1 200 OK
Date: Fri, 17 Feb 2006 18:58:23 GMT
Server: Apache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

1000
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http
<html xmlns="http://www.w3.org/1999/xhtml">
```

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

Follow the steps below 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

Follow the steps below 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

Follow the steps below 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.

Enable Active Content

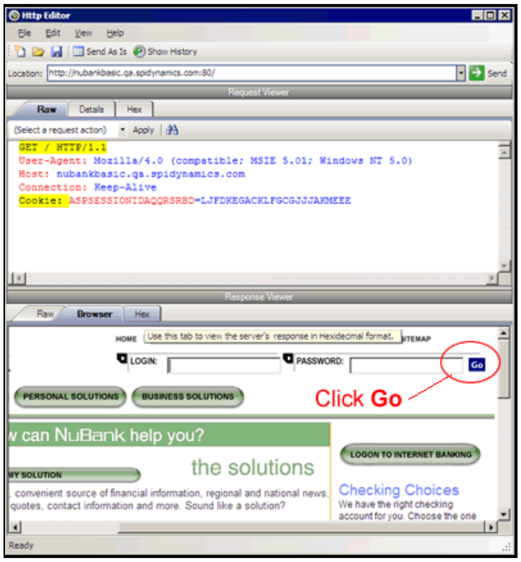
Select this option to allow execution of JavaScript and other dynamic content in all browser windows.

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**.



Location: http://nubankbasic.qa.spidynamics.com:80/

```
GET / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: nubankbasic.qa.spidynamics.com
Connection: Keep-Alive
Cookie: ASPSESSIONIDAQQRSRBD=LJFDKEGACKLFGCGJJJAKMEEE
```

Use this tab to view the server's response in Hexidecimal format.

w can NuBank help you?

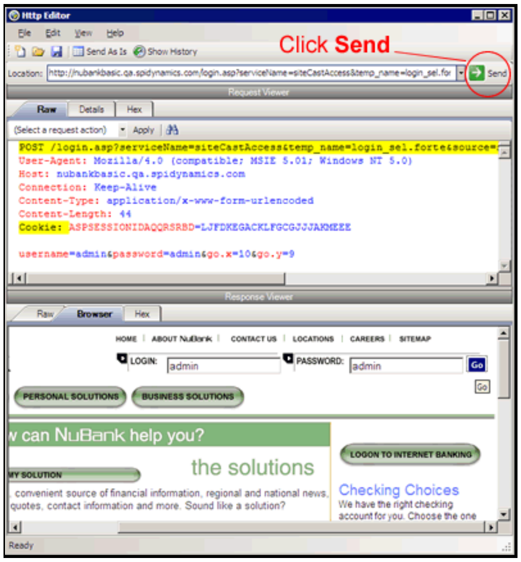
the solutions

, convenient source of financial information, regional and national news, quotes, contact information and more. Sound like a solution?

Checking Choices

We have the right checking account for you. Choose the one

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**.



Http Editor
File Edit View Help
Send As Is Show History
Click Send
Location: http://nubankbasic.qa.spidynamics.com/login.asp?serviceName=siteCastAccess&temp_name=login_sel.for
Send
Request Viewer
Raw Details Hex
(Select a request action) Apply
Response Viewer
Raw Browser Hex
HOME ABOUT NuBank CONTACT US LOCATIONS CAREERS SITEMAP
LOGIN: admin PASSWORD: admin Go
PERSONAL SOLUTIONS BUSINESS SOLUTIONS
LOGON TO INTERNET BANKING
Ready

```
POST /login.asp?serviceName=siteCastAccess&temp_name=login_sel.forte&source=
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: nubankbasic.qa.spidynamics.com
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Cookie: ASPSESSIONIDAQQRSRBD=LJFDKEGACKLFGCGJJJAKMEEE

username=admin&password=admin&go.x=10&go.y=9
```

v can NuBank help you?

the solutions

MY SOLUTION

convenient source of financial information, regional and national news, quotes, contact information and more. Sound like a solution?

Checking Choices

We have the right checking account for you. Choose the one

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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.

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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 (as described in the preceding table).

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 the Access Management Platform (AMP).

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).

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

Follow the steps below to use Web Proxy with a browser:

1 Click **Tools** → **Web Proxy**.

The *Web Proxy* window opens.

2 Click ▶ or select **Proxy** → **Start**.

"Listening" displays in the Web Proxy status bar.

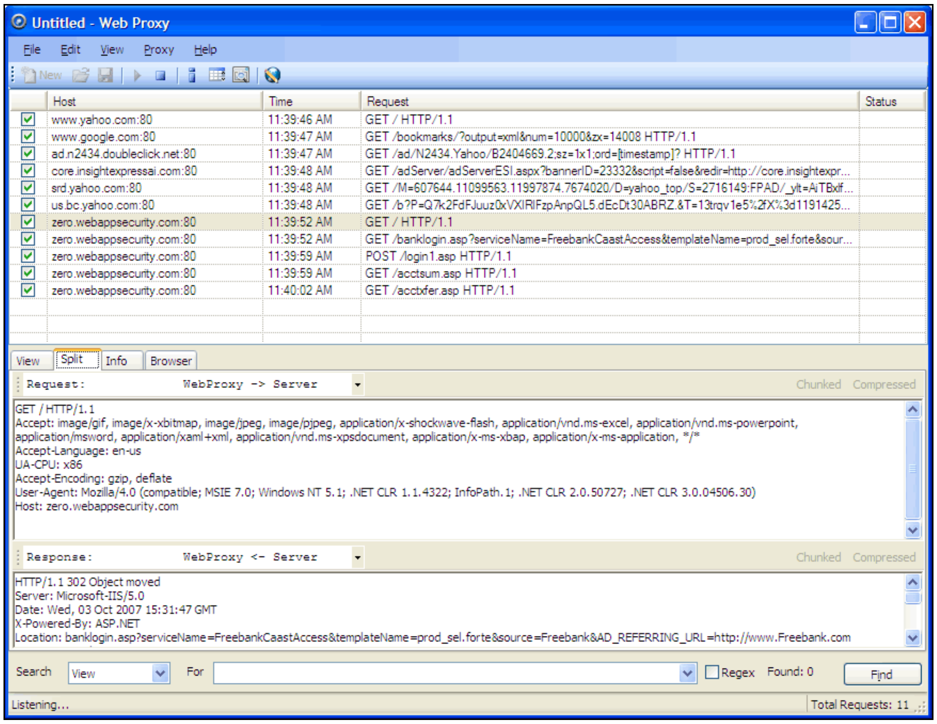
3 Open your Web browser and manually navigate the site for which you want to view requests/responses.

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).

4 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.

5 When you have browsed to all necessary pages, return to Web Proxy and click ■ (or click **Proxy** → **Stop**.

6 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.



	Host	Time	Request	Status
☑	www.yahoo.com:80	11:39:46 AM	GET / HTTP/1.1	
☑	www.google.com:80	11:39:47 AM	GET /bookmarks/?output=xml&num=10000&zx=14008 HTTP/1.1	
☑	ad.n2434.doubleclick.net:80	11:39:47 AM	GET /ad/N2434.Yahoo/B2404669.2;sz=1x1;ord=[timestamp]? HTTP/1.1	
☑	core.insightexpressai.com:80	11:39:48 AM	GET /adServer/adServerESI.aspx?bannerID=23332&script=false&redir=http://core.insightexpr...	
☑	srd.yahoo.com:80	11:39:48 AM	GET /M=607644.11099563.11997874.7674020/D=yahoo_top/S=2716149:FPAD/_ylt=AiTBxlf...	
☑	us.bc.yahoo.com:80	11:39:48 AM	GET /b?P=Q7k2FdFJuuz0xVXIRIFzpAnpQL5.dEcDt30ABRZ.&T=13trqv1e5%2fX%3d1191425...	
☑	zero.webappsecurity.com:80	11:39:52 AM	GET / HTTP/1.1	
☑	zero.webappsecurity.com:80	11:39:52 AM	GET /banklogin.asp?serviceName=FreebankCaastAccess&templateName=prod_sel.forte&sour...	
☑	zero.webappsecurity.com:80	11:39:59 AM	POST /login1.asp HTTP/1.1	
☑	zero.webappsecurity.com:80	11:39:59 AM	GET /acctsum.asp HTTP/1.1	
☑	zero.webappsecurity.com:80	11:40:02 AM	GET /acctxfer.asp HTTP/1.1	

```
Request:              WebProxy -> Server
```

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, application/xaml+xml, application/vnd.ms-xpsdocument, application/x-ms-xbap, application/x-ms-application, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: zero.webappsecurity.com
```

```
Response:             WebProxy <- Server
```

```
HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Wed, 03 Oct 2007 15:31:47 GMT
X-Powered-By: ASP.NET
Location: banklogin.asp?serviceName=FreebankCaastAccess&templateName=prod_sel.forte&source=Freebank&AD_REFERRING_URL=http://www.Freebank.com
```

7 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, 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.

8 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).

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 AMP sensor) to log in to an application. You can also incorporate logic that will prevent the scanner from inadvertently logging out of your application.

Follow the steps below 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 6 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 8081, 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 type and enter your authentication credentials in the **Username** and **Password** boxes. See Table 9 on page 114 for a description of the available authentication types.

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:

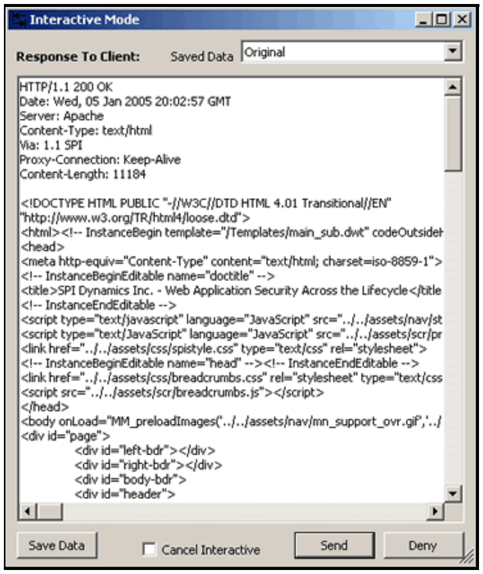
```
GET /CGI-BIN/SOME.CGI HTTP/1.1

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.



```
HTTP/1.1 200 OK
Date: Wed, 05 Jan 2005 20:02:57 GMT
Server: Apache
Content-Type: text/html
Via: 1.1 SPI
Proxy-Connection: Keep-Alive
Content-Length: 11184

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_sub.dwt" codeOutsideH
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="doctitle" -->
<title>SPI Dynamics Inc. - Web Application Security Across the Lifecycle</title
<!-- InstanceEndEditable -->
<script type="text/javascript" language="JavaScript" src="../../assets/nav/st
<script type="text/JavaScript" language="JavaScript" src="../../assets/scr/pr
<link href="../../assets/css/spistyle.css" type="text/css" rel="stylesheet">
<!-- InstanceBeginEditable name="head" --><!-- InstanceEndEditable -->
<link href="../../assets/css/breadcrumbs.css" rel="stylesheet" type="text/css
<script src="../../assets/scr/breadcrumbs.js"></script>
</head>
<body onLoad="MM_preloadImages('../../assets/nav/mn_support_ovr.gif','../
<div id="page">
          <div id="left-bdr"></div>
          <div id="right-bdr"></div>
          <div id="body-bdr">
          <div id="header">
```

Follow the steps below to turn on interactive mode:

1 Click **Proxy** → **Stop**.

2 Click **Proxy** → **Interactive**
-or-

click **i** 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 AMP Console, it contacts the AMP server and downloads any available console binary updates.

You can obtain updates to the SecureBase, as well as binary updates for AMP-connected products such as WebInspect, through either a manual or scheduled process.

Manual Smart Update

The AMP server will contact the Hewlett-Packard data center via the Internet to check for new or updated adaptive agents, vulnerability checks, and policy information.

1. On the AMP Console toolbar, click **Smart Update**.

   A message informs you that Smart Update was started.

2. Click **OK**.
3. To view the results of the update:
   a. Click the **Administration** group.
   b. Select the Activity Log shortcut and examine the messages related to Smart Update.

Scheduled Smart Update

Use the following procedure to schedule a Smart Update.

1. On the AMP Console, click the **Administration** group.
2. Click the **Smart Update** shortcut.
3. Click the **Action** menu and select **Add Schedule**.

   The *Smart Update Settings* window opens.

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.

      Note: 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, 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.

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

Follow the steps below 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, follow these steps:

   a. In the WebInspect navigation pane, click the cookies icon Cookies. 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**.

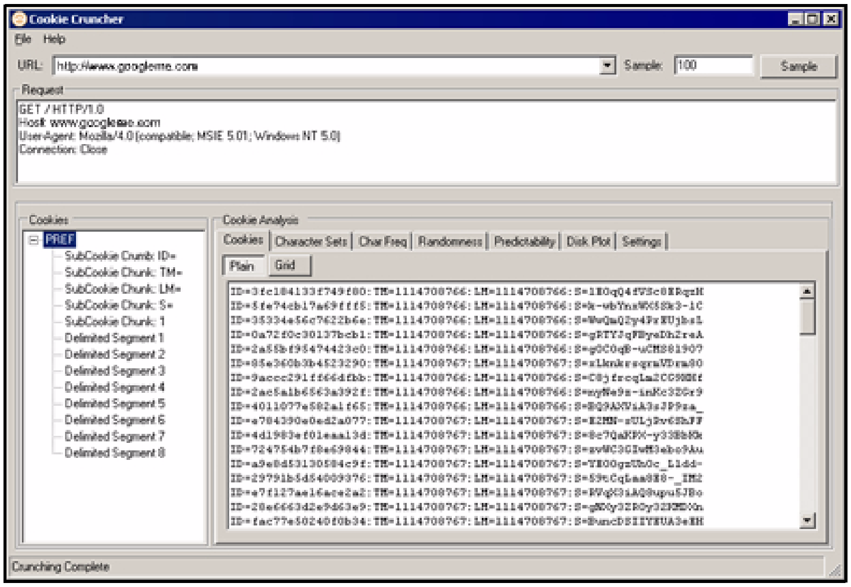
   As cookies are collected, the Cookie Cruncher organizes them into a tree hierarchy displayed in the vertical pane on the left side of the window.

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.



```
GET / HTTP/1.0
Host: www.googleme.com
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Connection: Close
```

```
PREF
  SubCookie Crumb: ID=
  SubCookie Chunk: TM=
  SubCookie Chunk: LM=
  SubCookie Chunk: S=
  SubCookie Chunk: 1
  Delimited Segment 1
  Delimited Segment 2
  Delimited Segment 3
  Delimited Segment 4
  Delimited Segment 5
  Delimited Segment 6
  Delimited Segment 7
  Delimited Segment 8
```

```
ID=3fc184133f749f80:TM=1114708766:LM=1114708766:S=1E0qQ4fVSc0ERqzH
ID=5fe74cb17a69fff5:TM=1114708766:LM=1114708766:S=k-wbYnsWX5Sk3-1C
ID=35334e56c7622b6e:TM=1114708766:LM=1114708766:S=WwQmQ2y4PrEUjbsL
ID=0a72f0c30137bcb1:TM=1114708766:LM=1114708766:S=gRTYJqFHysDh2reA
ID=2a55bf95474423c0:TM=1114708766:LM=1114708766:S=gOC0qB-uCH581907
ID=85e360b3b4523290:TM=1114708767:LM=1114708767:S=zLknkrsgraVDra80
ID=9accc291ff66dfbb:TM=1114708766:LM=1114708766:S=C8jfrcqLa2CG9HEf
ID=2ac5a1b6563a392f:TM=1114708766:LM=1114708766:S=myNe9s-inKc3ZGr9
ID=4011077e582a1f65:TM=1114708766:LM=1114708766:S=BQ9AXViA3sJP9sa_
ID=e704390e0ed2a077:TM=1114708767:LM=1114708767:S=E2MN-sULj2v6ShFF
ID=4d1983ef01eaa13d:TM=1114708767:LM=1114708767:S=8e7QaKPX-y33BbKk
ID=724754b7f0e69044:TM=1114708767:LM=1114708767:S=zvWC3GIwH3ebo9Au
ID=a9e8d53130584c9f:TM=1114708767:LM=1114708767:S=YE0OgzUhOc_L1dd-
ID=29791b5d54009376:TM=1114708767:LM=1114708767:S=59tCqLaa8E8-_IM2
ID=e7f127ae16ace2a2:TM=1114708767:LM=1114708767:S=RVgX3iAQ9upu5JBo
ID=28e6663d2e9d63e9:TM=1114708767:LM=1114708767:S=gNXy3ZROy3ZHMDXn
ID=fac77e50240f0b34:TM=1114708767:LM=1114708767:S=BuncDSIIYEUA3eEH
```

Crunching Complete

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

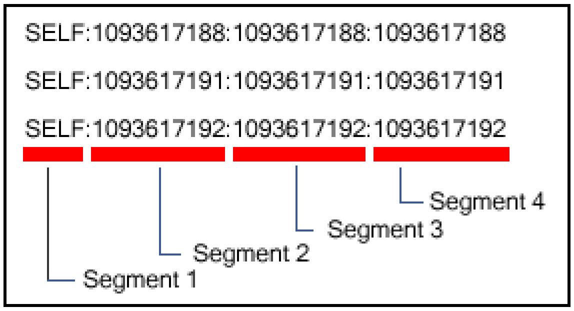
088-0518

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.



```
SELF:1093617188:1093617188:1093617188
SELF:1093617191:1093617191:1093617191
SELF:1093617192:1093617192:1093617192
```

To analyze the second segment of all subcookies, you would click the **Select Subcookie** list and select **Delimited Segment 2**.

For more information, see the white paper *Automated Cookie Analysis*.

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.

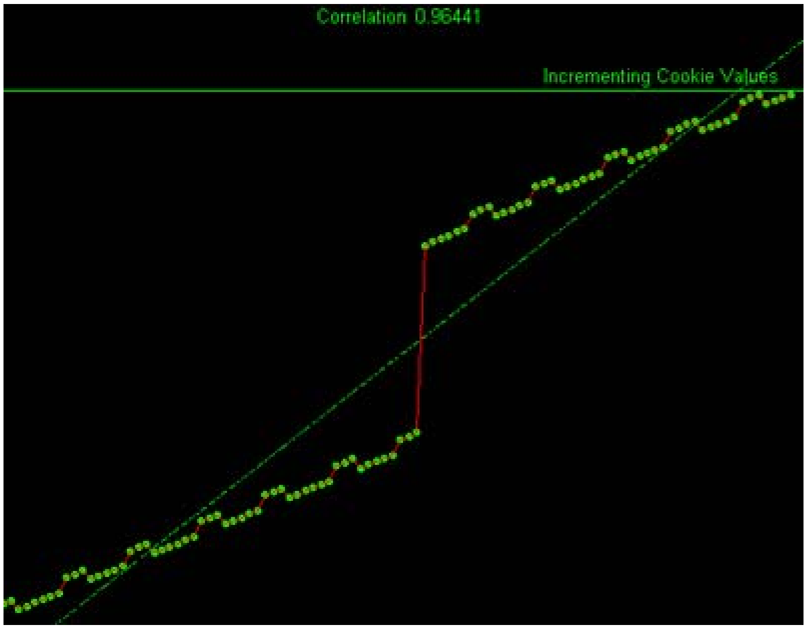
Predictability Tab

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.

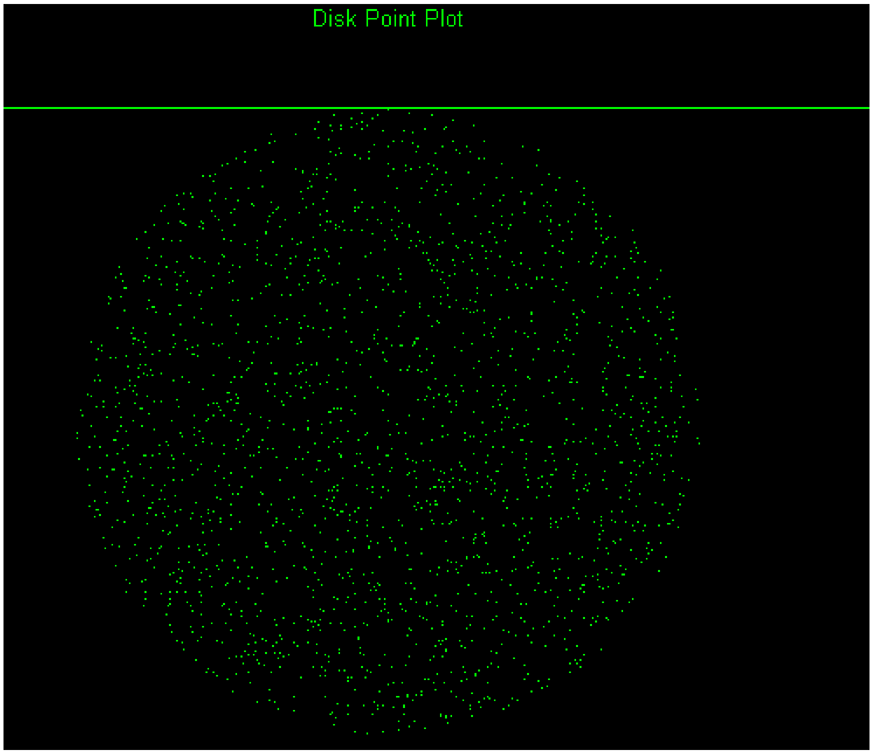
If the correlation is .9 or greater, the graph displays the header “Incrementing Cookie Values” or “Decremented Cookie Values” and draws a “best fit” line.

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

Follow the steps below 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 type from the **Authentication** list:

Authentication	Description
Automatic	Allow the Cookie Cruncher to determine the correct authentication type. 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 (as described in the preceding table).

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

Follow the steps below 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 208.
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 205.
   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 7 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.

Table 7 Fuzzer Generators **(cont'd)**

Generator	Function
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.
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

Follow the steps below 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

Follow the steps below to use a filter in a session:

1. Select a filter from the **Filters** list.
2. Select the **Enable** check box.

Deleting a Filter

Follow the steps below to delete a filter:

1. Select a filter from the **Filters** list.
2. Click **Delete**.

Editing a Filter

Follow the steps below 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.

Follow the steps below to use the Session Editor:

1. Click a tab.
2. You can either:
   - 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

Follow the steps below 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 Steps 2-6.

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

Follow the steps below 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 Steps 2-6.

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

Follow the steps below 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 steps 1-7.

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

Follow the steps below 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 Steps 2-6.

Web Fuzzer Settings

Follow the steps below 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 (as described in the preceding table).

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

Follow the steps below 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 212 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.

   If the scanner has detected a potential SQL injection vulnerability, you can copy the HTTP Request used for that session and paste it onto the **Raw** tab of the **Request** area of the SQL Injector. Similarly, if using the HTTP Editor, simply copy and paste the raw request.

   - 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

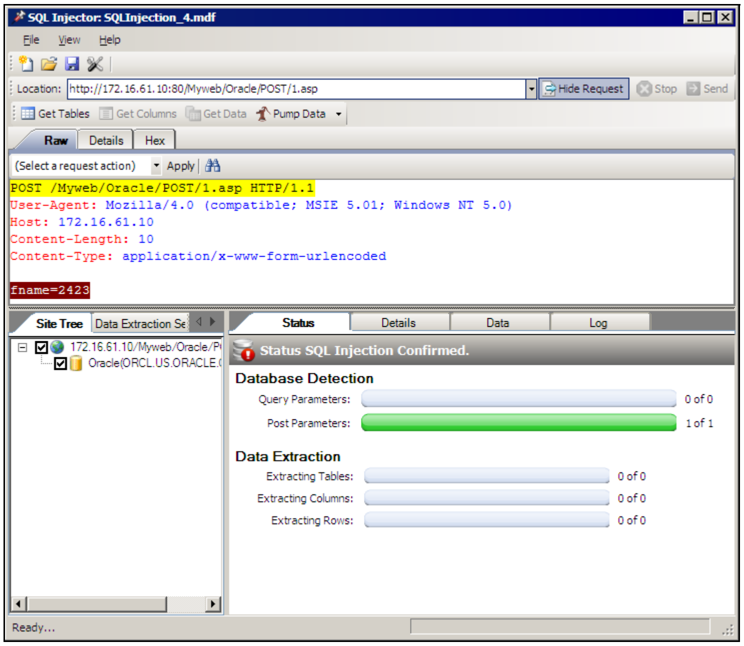
     Content-Length: 22

     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.



```
POST /Myweb/Oracle/POST/1.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 172.16.61.10
Content-Length: 10
Content-Type: application/x-www-form-urlencoded

fname=2423
```

Status SQL Injection Confirmed.

Database Detection

Query Parameters: 0 of 0

Post Parameters: 1 of 1

Data Extraction

Extracting Tables: 0 of 0

Extracting Columns: 0 of 0

Extracting Rows: 0 of 0

5 To extract all the data from all tables, click **Pump Data**.

Alternatively, you can selectively investigate tables and columns using the following procedure:

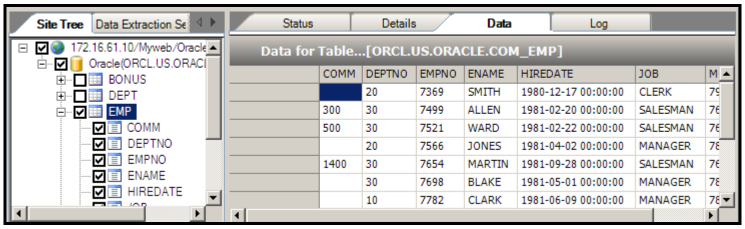
a Select **Get Tables**.

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**.

6 Click the **Data** tab to display values for the selected columns.



Data for Table...[ORCL.US.ORACLE.COM_EMP]

COMM	DEPTNO	EMPNO	ENAME	HIREDATE	JOB	M
	20	7369	SMITH	1980-12-17 00:00:00	CLERK	79
300	30	7499	ALLEN	1981-02-20 00:00:00	SALESMAN	76
500	30	7521	WARD	1981-02-22 00:00:00	SALESMAN	76
	20	7566	JONES	1981-04-02 00:00:00	MANAGER	78
1400	30	7654	MARTIN	1981-09-28 00:00:00	SALESMAN	76
	30	7698	BLAKE	1981-05-01 00:00:00	MANAGER	78
	10	7782	CLARK	1981-06-09 00:00:00	MANAGER	78

SQL Injector Tabs

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

Follow the steps below 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

Timeout in Seconds

Specify the number of seconds that the SQL Injector will wait for a response before terminating the session.

Manipulate Request

If you select this option, the SQL Injector 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 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 SQL injection is possible. Also specify the number of concurrent threads that should be used for data extraction.

Use a macro

Select this option to use a startup macro; then click ... to select, edit, or create a macro.

Authentication

Authentication Method

If the site does not require authentication, select **None**. Otherwise, select a type from the **Authentication** list:

Authentication	Description
Automatic	Allow the SQL Injector to determine the correct authentication type. 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 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 (as described in the preceding table).

Compliance Manager

HP scanners employ an extensive arsenal of attack agents designed to detect security flaws in Web-based applications. They probe your system with thousands of HTTP requests and evaluate each individual response. This session-based assessment reports each vulnerability, pinpoints its location in the application, and recommends corrective actions you should take. It is, basically, a quantitative analysis of your system.

You can also perform a qualitative analysis by grading how well your application complies with certain government-mandated regulations or corporate-defined guidelines. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers using Web-based applications to provide “procedures for creating, changing, and safeguarding passwords.” With HP scanners, you can assess your application and then generate a Compliance Report that measures how well your application satisfies this HIPPA rule.

How It Works

You create a compliance template that associates requirements with one or more attack agents or vulnerabilities. For example, you might include the statement (or question) “The application will not use any ‘hidden’ fields.” The attack agent that tests for compliance to this requirement is Hidden Form Value, ID #4727 (which is one of the agents in the Unknown Application Testing group).

Compliance templates are completely flexible. You can enable or disable individual requirements. You can also modify requirements by adding or removing attack agents or threat classes. For maximum flexibility, you can even create your own agents and associate them with a user-defined requirement.

AMP includes sample compliance templates that you can edit to fit your company’s specific requirements.

Creating/Editing a Compliance Template

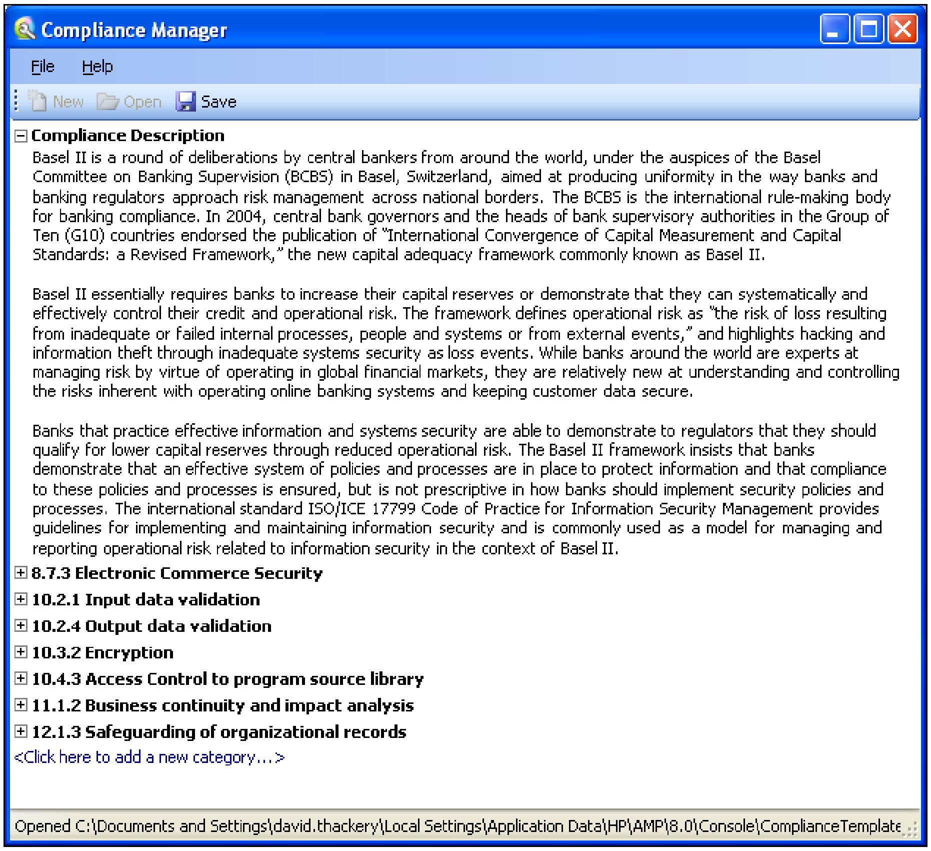
Follow the steps below to create (edit) a compliance template.

1. Click the **Scans/Compliance** group.
2. Click the **Compliance Templates** shortcut.
3. Select a template and then select **Copy** from the **Action** menu.

   ➤ Note: After creating a custom template, you can edit it by selecting **Edit** from the **Action** menu (or from the context menu).

4. If you have access to any custom policies, the *Select Custom Policy* dialog appears, prompting you to choose a custom policy. This occurs to accommodate any custom checks that you may have created in that policy. If there are no custom checks, or if you do not want to include custom checks, click **No**.
5. On the *Copy Compliance Template* dialog, rename the template and click **OK**.

The *Compliance Manager* window opens, displaying template contents. The following illustration depicts the Basil II template.



⊟ **Compliance Description**

Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The BCBS is the international rule-making body for banking compliance. In 2004, central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries endorsed the publication of "International Convergence of Capital Measurement and Capital Standards: a Revised Framework," the new capital adequacy framework commonly known as Basel II.

Basel II essentially requires banks to increase their capital reserves or demonstrate that they can systematically and effectively control their credit and operational risk. The framework defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events," and highlights hacking and information theft through inadequate systems security as loss events. While banks around the world are experts at managing risk by virtue of operating in global financial markets, they are relatively new at understanding and controlling the risks inherent with operating online banking systems and keeping customer data secure.

Banks that practice effective information and systems security are able to demonstrate to regulators that they should qualify for lower capital reserves through reduced operational risk. The Basel II framework insists that banks demonstrate that an effective system of policies and processes are in place to protect information and that compliance to these policies and processes is ensured, but is not prescriptive in how banks should implement security policies and processes. The international standard ISO/ICE 17799 Code of Practice for Information Security Management provides guidelines for implementing and maintaining information security and is commonly used as a model for managing and reporting operational risk related to information security in the context of Basel II.

⊞ **8.7.3 Electronic Commerce Security**

⊞ **10.2.1 Input data validation**

⊞ **10.2.4 Output data validation**

⊞ **10.3.2 Encryption**

⊞ **10.4.3 Access Control to program source library**

⊞ **11.1.2 Business continuity and impact analysis**

⊞ **12.1.3 Safeguarding of organizational records**

<Click here to add a new category...>

Opened C:\Documents and Settings\david.thackery\Local Settings\Application Data\HP\AMP\8.0\Console\ComplianceTemplate

6 Click the plus sign ⊞ to expand a node.

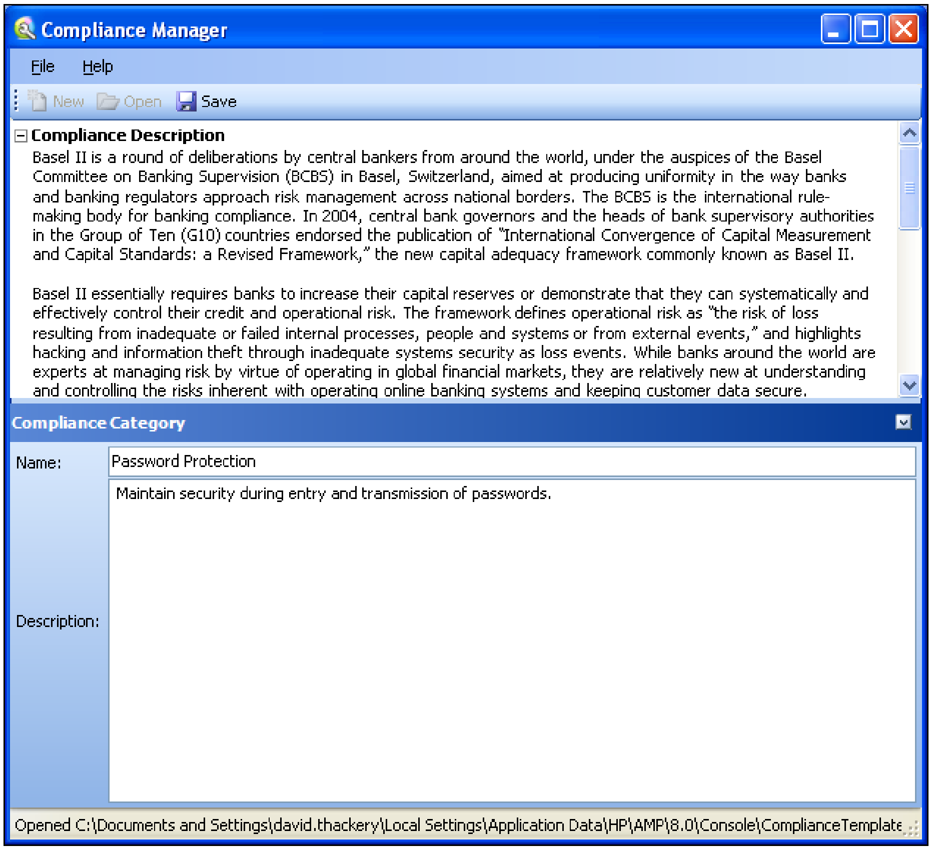
7 To edit a section, right-click the section and select **Edit**.

8 To remove a section, right-click the section and select **Remove**.

9 To add a category, click the phrase "<Click here to add a new category...>."

"New Category" appears.

10 Click the phrase “New Category” and, in the editing area, enter the name and description of the new category (“Password Protection” in this example).



⊟ **Compliance Description**

Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The BCBS is the international rule-making body for banking compliance. In 2004, central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries endorsed the publication of "International Convergence of Capital Measurement and Capital Standards: a Revised Framework," the new capital adequacy framework commonly known as Basel II.

Basel II essentially requires banks to increase their capital reserves or demonstrate that they can systematically and effectively control their credit and operational risk. The framework defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events," and highlights hacking and information theft through inadequate systems security as loss events. While banks around the world are experts at managing risk by virtue of operating in global financial markets, they are relatively new at understanding and controlling the risks inherent with operating online banking systems and keeping customer data secure.

Compliance Category

Name: Password Protection

Description: Maintain security during entry and transmission of passwords.

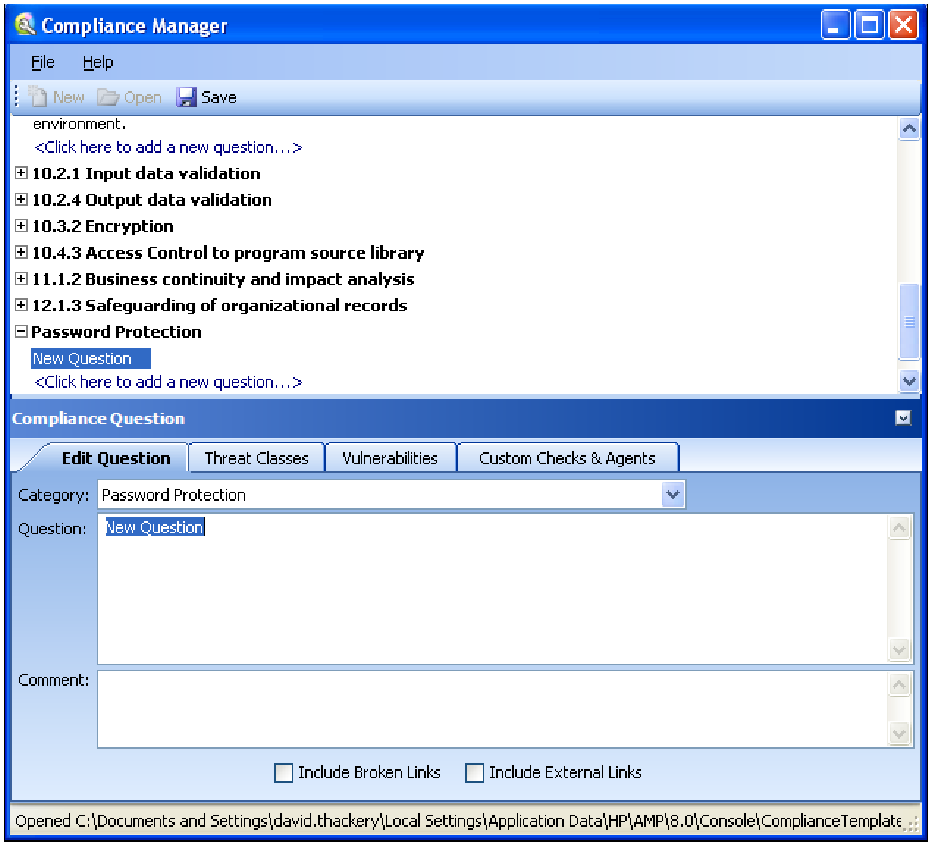
Opened C:\Documents and Settings\david.thackery\Local Settings\Application Data\HP\AMP\8.0\Console\ComplianceTemplate

11 Click the plus sign ⊞ to expand the node labeled Password Protection.

12 Click the phrase “<Click here to add a new question...>.”

13 Click the phase “New Question.”

The editing area displays tabs allowing you to create a question related to the category “Password Protection.”



environment.
<Click here to add a new question...>
⊞ 10.2.1 Input data validation
⊞ 10.2.4 Output data validation
⊞ 10.3.2 Encryption
⊞ 10.4.3 Access Control to program source library
⊞ 11.1.2 Business continuity and impact analysis
⊞ 12.1.3 Safeguarding of organizational records
⊟ Password Protection
New Question
<Click here to add a new question...>

Category: Password Protection

Question: New Question

Comment:

☐ Include Broken Links ☐ Include External Links

Opened C:\Documents and Settings\david.thackery\Local Settings\Application Data\HP\AMP\8.0\Console\ComplianceTemplate

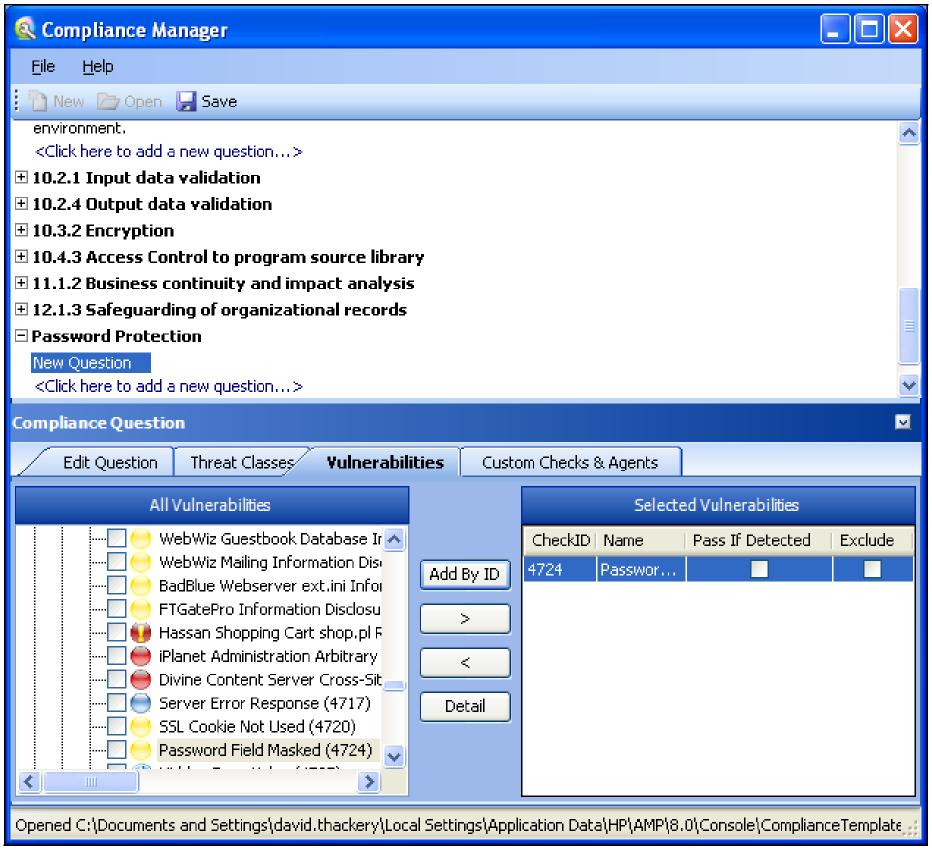
14 In the **Question** area, type a question related to the category (such as, “Is each character of entered password displayed as an asterisk?”

15 You can associate this question with threat classes, vulnerabilities defined by HP, or a custom check or agent that you previously created. For this example, click the **Vulnerabilities** tab and then click **Add By ID**.

You can also select a vulnerability and click ▶ to include it in the **Selected Vulnerabilities** section for this question.

16 On the *Add Check By ID* dialog, enter 4724 and click **OK**. [4724 is the ID number of the “Password Field Not Masked” check.]

The check you specified appears in the **Selected Vulnerabilities** area


Compliance Manager
File
Help
New
Open
Save
environment.
<Click here to add a new question...>
10.2.1 Input data validation
10.2.4 Output data validation
10.3.2 Encryption
10.4.3 Access Control to program source library
11.1.2 Business continuity and impact analysis
12.1.3 Safeguarding of organizational records
Password Protection
New Question
<Click here to add a new question...>
Compliance Question
Edit Question
Threat Classes
Vulnerabilities
Custom Checks & Agents
All Vulnerabilities
WebWiz Guestbook Database Ir
WebWiz Mailing Information Dis
BadBlue Webserver ext.ini Infor
FTGatePro Information Disclosu
Hassan Shopping Cart shop.pl F
iPlanet Administration Arbitrary
Divine Content Server Cross-Sit
Server Error Response (4717)
SSL Cookie Not Used (4720)
Password Field Masked (4724)
Add By ID
>
<
Detail
Selected Vulnerabilities

CheckID	Name	Pass If Detected	Exclude
4724	Passwor...	□	□

Opened C:\Documents and Settings\david.thackery\Local Settings\Application Data\HP\AMP\8.0\Console\ComplianceTemplate

17 The **Selected Vulnerabilities** area contains two check boxes:

- **Pass If Detected** - Select this option if the check is designed to confirm an attribute that contributes to application security. You might use this if, for example, you develop a custom check that checks for the existence of a file (such as Privacy Policy.html) that is part of your compliance program.
- **Exclude** - Select this option if you add a group of checks, but want to exclude specific ones.

In this example, do not select either check box.

18 Continue adding threat classes, vulnerabilities, or custom checks until you have included all that sufficiently test your application for the compliance question.

19 Create additional questions and categories using the above procedures until the compliance template is complete.

20 Click **Save**.

Testing for Compliance

Follow the steps below to test your Web site for compliance:

1 Create a compliance template.

2 Scan your Web site.

3 In the AMP Web Console, select the **Scans** view.

4 Select a scan and click **Generate Report**.

5. Provide the requested information.
6. On the Options settings, do one of the following:
   - Select **Use Report Template** and then select **Compliance** from the **Report Template** list.
   - Select **Use Report Definition** and then select **Compliance** from the **Report Definition** list; provide the requested information for report definitions.
7. Click **Finish**.

Web Macro Recorder

A macro is a recording of the HTTP requests that are generated when you navigate through a Web site or application using the Web Macro Recorder. You can instruct the scanner to use this recording to enter your Web site and (optionally) navigate through your application.

Any activity you record in a macro will override the scanner settings. For example, if you specify a URL in the Excluded URL setting, and then you actually navigate to that URL when creating a macro, the scanner will ignore the exclusion when it replays the macro.

When starting a Web site assessment, you have four opportunities to specify a macro.

- **Recorded macro-crawl with audit** — This type of macro is used most often to focus on a particular subsection of the application. The scanner audits only those URLs that are recorded in the macro and does not follow any hyperlinks encountered during the audit. You do not need to specify a logout condition (i.e., an algorithm that enables the scanner to detect when it has inadvertently logged out of an application).
- **Use a macro for entry** — This macro should contain sessions recorded during a login procedure. When starting a scan, the scanner plays the macro, visiting each URL that was accessed when the macro was recorded. It then begins crawling (and, optionally, auditing) the last session in the macro, following any hyperlinks it encounters. All sessions that precede the last URL are not audited or crawled. A logout condition is not required. This type of macro is most useful when using a shared requestor. This option is not available if you select Recorded Macro - Crawl with Audit.
- **Use a login macro for forms authentication** — This macro should contain sessions recorded during a login procedure and incorporates logic that will prevent the scanner from terminating prematurely if it inadvertently logs out of your application. When scanning a site, the scanner analyzes every server response to determine the state. If at any time the scanner determines it is logged out, it runs this macro to log in, and then resumes crawling or auditing the site at the point where the logout occurred. When recording this type of macro, you must specify a logout condition.
- **Use a start-up macro** — This type of macro specifies URLs that the scanner will use to navigate to a particular area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application.

Note that when you play a macro, the HP scanner will not send any cookie headers that may have been incorporated in the recorded macro.

Creating a Macro

Follow the steps below to create a macro:

Task 1: Prepare the Web Macro Recorder

1. Close all browsers.
2. Start the Web Macro Recorder.
3. Click **Edit** → **Settings** to configure general settings and proxy settings.
4. You can exclude the recording of requests containing certain objects by selecting **Filter Rules** from the Macro Recorder's **View** menu. See Filter Rules on page 230 for more information.

Task 2: Browse the Web Site

1 Do one of the following:

- Select **File** → **New**.
- Click the New icon on the toolbar.
- Click the Record icon.

2 Using the browser's Address bar, enter or select a URL.

Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, the Web Macro Recorder 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).

3 Browse the pages that you want to include in your macro.

4 If you want to include a login, be sure to navigate to a page that requires Web form authentication. Then enter a valid user name and password, and submit the data (usually by clicking a button such as **Log On**, **Go**, **Submit**, etc.).

5 When finished, close the browser.

If recording a login macro, do not log out before closing.

Task 3: Finish the Macro

1 When you close the browser, a dialog box displays the message:

"Are you recording a login macro? (By clicking Yes, auto-detection of the logout condition will be performed.)"

Explanation: When a scanner encounters a hyperlink to another resource, it navigates to that URL and continues 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 logout occurs, the scanner can either run this macro to log in or request user intervention. In either case, the process hinges on the scanner's ability to recognize when it is no longer logged in.

— Click **Yes** if you want the Web Macro Recorder to analyze the recorded sessions and attempt to detect a "logout" condition.

— If you do not require a "logout" condition, click **No** and go to Step 6.

— If you want to specify a condition manually, click **No** and go to Step 3.

— If your application uses URL rewriting or post data techniques to maintain state within a Web site, click **No**. See URL Rewriting and Request Parameters on page 225 for further instructions.

2 If the attempt to detect a logout condition is successful, a dialog box displays the following message:

"Would you like to test your login macro?"

a To bypass the test, click **No**. Go to Step 3.

b To test the macro, click **Yes**.

   c. On the *Test Login Macro* window, the **Address** box contains the URL of a page believed to be viewable only after logging in. If this is, indeed, a "protected"" page, click **Go**. Otherwise, enter the URL of a protected page.

   d. Browse to various sections of the site to verify that you are logged in.

   e. Log out and verify that you are prompted to replay the macro.

   f. Click **Done**.

3. If the attempt to detect a logout condition is not successful, or if you elected to bypass the auto-detect feature:

   a. On the **Sessions** tab, select a session that you accessed after logging in and click **Detect Logout Condition** (on the toolbar). Do not select the session where you actually logged in.

   b. If the Macro Recorder is unable to determine the logout condition, try selecting other sessions.

   c. If the Macro Recorder is still unable to determine a logout condition, you can manually enter one. Click **Edit Logout Condition** and, on the *Logout Condition Editor* window, select either **Use Regular Expression Extensions** or **Use Text Matching**.

4. For a login macro, you may want to delete extraneous sessions (i.e., those not related to or required by the login procedure). To do so, remove the check mark from the unneeded sessions. You should then click **Test Login Macro** to ensure that you retained all necessary sessions.

5. Specify which action the scanner should take if it detects that it has logged out of the application. Click either **Play Macro** or **Launch Interactive** (which will allow you to manually log back in).

   Note: If you select **Launch Interactive**, the scanner pauses the scan and presents a dialog allowing you to enter log-in information. This is useful when scanning a site that incorporates a CAPTCHA (i.e., a challenge-response test placed within Web forms to ensure that the response is not generated by a computer). This feature is also used when the Web Macro Recorder is not able to determine a logout condition and the user is not able to define the condition using regular expressions or text matching.

6. To save the macro, click **File** → **Save** (or **Save As**) or click 💾.

Editing the Logout Condition

You can create or edit the criteria used by the Web Macro Recorder to detect a "logged out" condition.

To access the feature, click **Edit Logout Condition**.

If detection of a logout is not required, select **Do no use logout condition**. Otherwise, you can instruct the Web Macro Recorder to use either a regular expression or text matching.

Regular Expression Extensions

If you want the Web Macro Recorder to use a regular expression to detect a logged out condition:

1. Select Use **Regular Expression Extensions for a logout signature**.

2 Type (or edit) 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.

3 Click **OK**.

Text Matching

This technique for recognizing “logged out” or “logged in” state assumes that you know that certain text strings will be displayed when either condition occurs. For example, a site may display pages that contain the text “Log In” (usually a hyperlink) whenever a user is not logged in. Similarly, the site may display pages containing text such as “Sign Out,” “Log Out,” or “Log Off” when the user is logged in.

1 Select **Use text matching to determine logged-in state**.

2 Under the **Text fragments that indicate logged out state** column, click **Add**.

3 In the pop-up window that appears, enter a text string and click **OK**. For example, you might enter “Log In” or “sign in”; note that the search is not case-sensitive.

4 Repeat Step 2-3 if additional or alternative text fragments are also present during a “logged out” state.

5 In the **Number of text fragments to match** box, enter the number of specified strings that must exist on a page before the Web Macro Recorder considers that page to be in a “logged out” state.

6 Under the **Text fragments that indicate logged in state** column, click **Add**.

7 In the pop-up window that appears, enter a text string and click **OK**. For example, you might enter “Log Out” or “Sign out.”

8 Repeat Step 6-7 if additional or alternative text fragments are also present during a “logged in” state.

9 In the **Number of text fragments to match** box, enter the number of specified strings that must exist on a page before the Web Macro Recorder considers that page to be in a “logged in” state.

10 (Optional) Click **Advanced**.

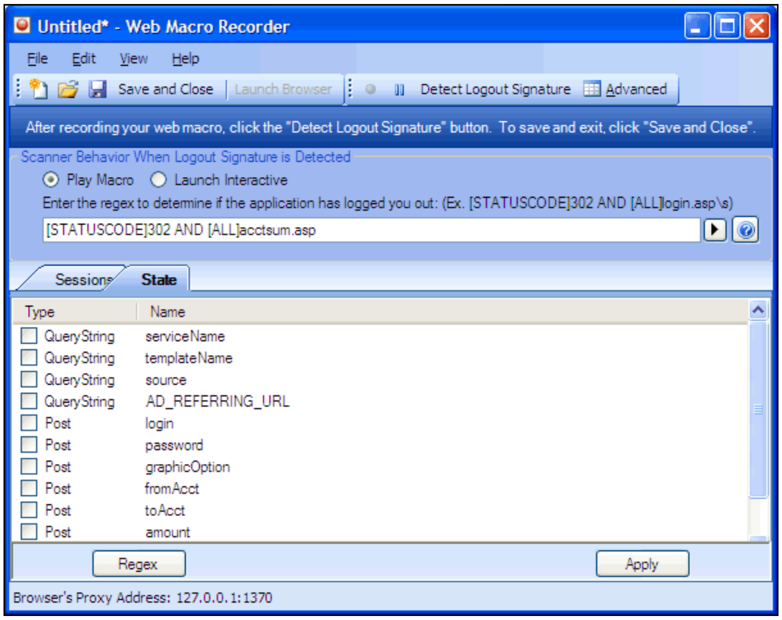
  a In the pop-up dialog, enter a URL that should be used to evaluate the state if a page does not contain enough text fragments.

  b Click **OK**.

11 Click **OK**.

URL Rewriting and Request Parameters

If your application uses URL rewriting or request parameters to maintain state within a Web site, select the **State** tab.



After recording your web macro, click the "Detect Logout Signature" button. To save and exit, click "Save and Close".

Scanner Behavior When Logout Signature is Detected

● Play Macro ○ Launch Interactive

Enter the regex to determine if the application has logged you out: (Ex. [STATUSCODE]302 AND [ALL]login.asp\s)

[STATUSCODE]302 AND [ALL]acctsum.asp

Type	Name
□ QueryString	serviceName
□ QueryString	templateName
□ QueryString	source
□ QueryString	AD_REFERRING_URL
□ Post	login
□ Post	password
□ Post	graphicOption
□ Post	fromAcct
□ Post	toAcct
□ Post	amount

Browser's Proxy Address: 127.0.0.1:1370

You must identify which parameters are used for state management. 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, a recorded macro 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 to the Web Macro Recorder.

➤ Note: You need to identify parameters only when the application uses URL rewriting, posted data or query parameters to manage state. It is typically not necessary when using cookies to manage state. Exception: Delete (uncheck) any cookie that is required for normal operation.

The Web Macro Recorder 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:

/\([\w\d]+\)/

1 To enter a regular expression, click **Regex** and then use the Regular Expression Editor to create an expression. When you click OK (on the regular Expression Editor), the expression is added to the **Type/Name** list.

2 Select a parameter in the **Type/Name** list (such as “login” in the preceding illustration).

3 Click **Apply**.

4 To save the macro, select **File** → **Save** (or **Save As**)
-or-

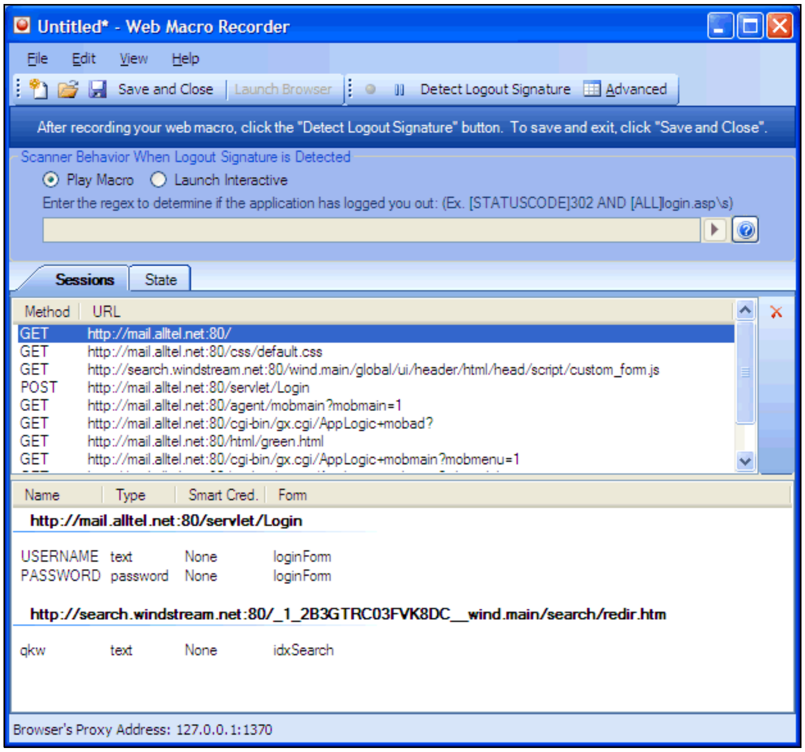
click 💾.

Inspecting and Editing a Macro

As you navigate through the target Web site, the Web Macro Recorder transcribes each session, displaying on the **Sessions** tab the method and URL associated with each HTTP request sent to the server.

1 Select a session on the **Sessions** tab.

If the associated HTTP response includes “text” or “password” input controls, their name and type are displayed in the lower pane.



After recording your web macro, click the "Detect Logout Signature" button. To save and exit, click "Save and Close".

Scanner Behavior When Logout Signature is Detected

● Play Macro ○ Launch Interactive

Enter the regex to determine if the application has logged you out: (Ex. [STATUSCODE]302 AND [ALL]login.asp\s)

Method	URL
GET	http://mail.alltel.net:80/
GET	http://mail.alltel.net:80/css/default.css
GET	http://search.windstream.net:80/wind.main/global/ui/header/html/head/script/custom_form.js
POST	http://mail.alltel.net:80/servlet/Login
GET	http://mail.alltel.net:80/agent/mobmain?mobmain=1
GET	http://mail.alltel.net:80/cgi-bin/gx.cgi/AppLogic+mobad?
GET	http://mail.alltel.net:80/html/green.html
GET	http://mail.alltel.net:80/cgi-bin/gx.cgi/AppLogic+mobmain?mobmenu=1

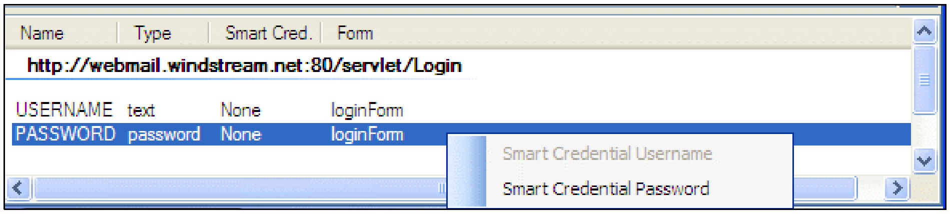
Name	Type	Smart Cred.	Form
http://mail.alltel.net:80/servlet/Login			
USERNAME	text	None	loginForm
PASSWORD	password	None	loginForm
http://search.windstream.net:80/_1_2B3GTRC03FVK8DC__wind.main/search/redir.htm			
qkw	text	None	idxSearch

Browser's Proxy Address: 127.0.0.1:1370

In this example, the form and the controls were rendered by the following HTML statements:

```
<form name="loginForm" action="/servlet/Login" method="POST">
<input type="text" size="16" name="USERNAME" value="">
<input type="password" size="16" name="PASSWORD">
```

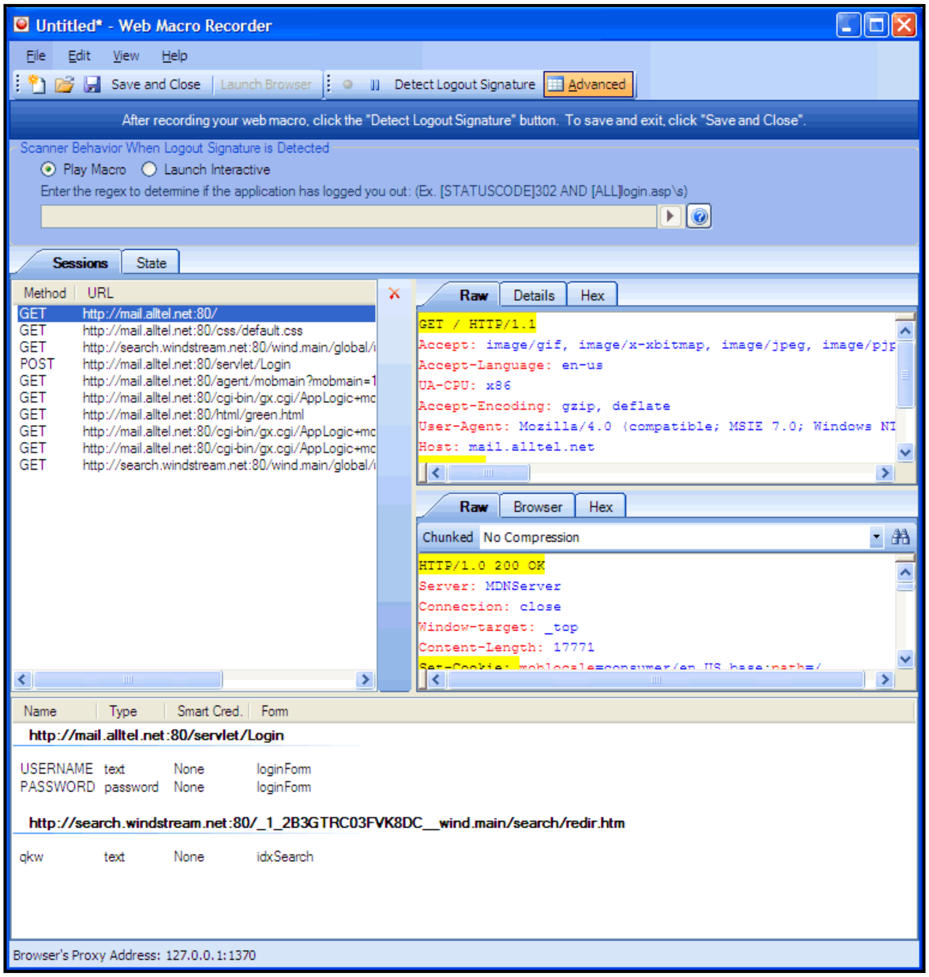
2 You can designate a control as a "Smart Credential" user name or password. Right-click the control name and select an option from the shortcut menu, as shown below.



Name	Type	Smart Cred.	Form
http://webmail.windstream.net:80/servlet/Login			
USERNAME	text	None	loginForm
PASSWORD	password	None	loginForm

If you start an assessment using a macro that includes Smart Credentials, then when you scan the page containing the input elements associated with these entries, the scanner will substitute the password specified in the Authentication options (or, if no user name is specified, the name of the current Windows user). This allows you to create the macro using your own user name and password, yet when someone else runs the scan using this macro, the scanner will submit that user's name and password.

3 If you click the **Advanced** button, the Web Macro Recorder displays the contents of the HTTP request and response in separate panes.



After recording your web macro, click the "Detect Logout Signature" button. To save and exit, click "Save and Close".

Scanner Behavior When Logout Signature is Detected

● Play Macro ○ Launch Interactive

Enter the regex to determine if the application has logged you out: (Ex. [STATUSCODE]302 AND [ALL]login.asp\s)

Method	URL
GET	http://mail.alltel.net:80/
GET	http://mail.alltel.net:80/css/default.css
GET	http://search.windstream.net:80/wind.main/global/i
POST	http://mail.alltel.net:80/servlet/Login
GET	http://mail.alltel.net:80/agent/mobmain?mobmain=1
GET	http://mail.alltel.net:80/cgi-bin/gx.cgi/AppLogic+mc
GET	http://mail.alltel.net:80/html/green.html
GET	http://mail.alltel.net:80/cgi-bin/gx.cgi/AppLogic+mc
GET	http://mail.alltel.net:80/cgi-bin/gx.cgi/AppLogic+mc
GET	http://search.windstream.net:80/wind.main/global/i

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjp
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
Host: mail.alltel.net
```

Chunked No Compression

```
HTTP/1.0 200 OK
Server: MDNServer
Connection: close
Window-target: _top
Content-Length: 17771
Set-Cookie: moblocale=consumer/en_US_base;path=/
```

Name	Type	Smart Cred.	Form
http://mail.alltel.net:80/servlet/Login			
USERNAME	text	None	loginForm
PASSWORD	password	None	loginForm
http://search.windstream.net:80/_1_2B3GTRC03FVK8DC__wind.main/search/redir.htm			
qkw	text	None	idxSearch

Browser's Proxy Address: 127.0.0.1:1370

4 You can also edit an HTTP request if, for example, you need to change or remove headers, or edit passwords or user names. Simply right-click a session and select **Edit with HTTP Editor** from the shortcut menu to launch the HTTP Editor.

5 You can exclude a specific session from the macro by clearing its associated check box, or you can delete a session by selecting the session and clicking the red **X** on the right side of the **Sessions** list (or by right-clicking a session and selecting **Delete Session** from the pop-up menu).

Web Macro Recorder Settings

Follow the steps below to modify the Web Macro Recorder settings:

1 Click **Edit** → **Settings**.

2 Select either the **General** or **Proxy** category (described below) and enter the settings.

3 Click **OK**.

General

Proxy Listener

The Web Macro Recorder 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.

To avoid the possibility of specifying a port that is already in use, select **Automatically Assign Port**.

Save Files in clear text

Select this option if you do not want to save macros in an XML format using Base 64 encoding (which is the default). Saving files in clear text allows you to read the XML tags. The actual data, however, is not rendered in ASCII format and is not human readable.

Keep window always on top

Select this option to keep the Web Macro Recorder displayed on your screen when you switch programs or windows.

Keep params as state only during macro playback

This option affects how the Post and Query parameters in the **State** tab are used. If this setting is off, then the Post and Query parameters that are checked are imported into the scan settings in the **HTTP Parameters Used For State** list. If this setting is on, then the Post and Query parameters that are checked are used as state only during the playback of the macro being recorded.

Automatically follow redirects during playback

If this option is selected, then for any sessions in the macro being recorded that result in a redirect (a 301 or 302 status code, for example), the new redirect will automatically be followed when the macro is played back. The session that is recorded (that is the result of the redirect) will not be played back.

Prompt for credentials when websever requests authentication

If you select this option, the Web Macro Recorder displays a dialog allowing you to enter a user name and password whenever the server requires authentication to access a site (that is, whenever the server returns a “401 Unauthorized” status).

Note: Certain AJAX, Flash, and ActiveX controls may elicit a 401 status code when authentication, in fact, is not required. You can recognize this situation when the Web Macro Recorder prompts for credentials, but a browser accessing the site does not. For sites where this occurs, this option should not be selected.

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 Macro Recorder should use.

Proxy

Use these settings to access the Web Macro Recorder 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 Macro Recorder 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 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

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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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 Macro Recorder Menus

The Web Macro Recorder contains the following menus:

File

- **New** - Launch Internet Explorer and begin recording.
- **Open** - Load a previously recorded macro for editing.
- **Save** - Save a macro.
- **Save As** - Save an edited macro under a different file name.
- **Exit** - Close Web Macro Recorder.

Edit

- **Cut** - Delete the selected string and save it to the clipboard.
- **Copy** - Copy the selected string to the clipboard.
- **Paste** - Insert contents of the clipboard.
- **Edit with HTTP Editor** - Open the HTTP Editor and load the selected session.
- **Delete Session** - Remove the selected session from the macro.
- **Start Capture** - Begin recording HTTP requests.
- **Stop Capture** - End recording to HTTP requests.
- **Find** - Specify a string and search for it when using the Advanced view.
- **Settings** - Modify Web Macro Recorder settings.

View

- **Launch Browser** - Open Internet Explorer to navigate through Web site.
- **Test Login Macro** - Open the *Test Login Macro* window to verify creating of a logout condition.
- **HTTP Editor** - Open the HTTP Editor.
- **Toolbars** - View or hide the Detect Logout Condition, Test Login Macro, and Advanced buttons.
- **Filter Rules** - Select a resource type or status code to exclude. For example, sessions where the server response contains an HTTP status code of “404 Object Not Found” are normally not useful. Similarly, sessions that request images are normally not necessary when

creating a macro, and simply add clutter to the session list. By selecting **Images** from the Filter Rules list, you avoid the needless recording of sessions such as GET http://www.mywebsite.com:80/services.gif.

- **Advanced** - View or hide panes that display the contents of HTTP requests and responses. Note that when editing a saved macro, pages will not be rendered in the **Browser** tab.

Help

- **Web Macro Recorder Help** - Open the Help file to the default topic.
- **Index** - Open the Help file, displaying the index pane.
- **Search** - Open the Help file, displaying the search pane.
- **About Web Macro Recorder -** Open a window that displays information about the Web Macro Recorder.

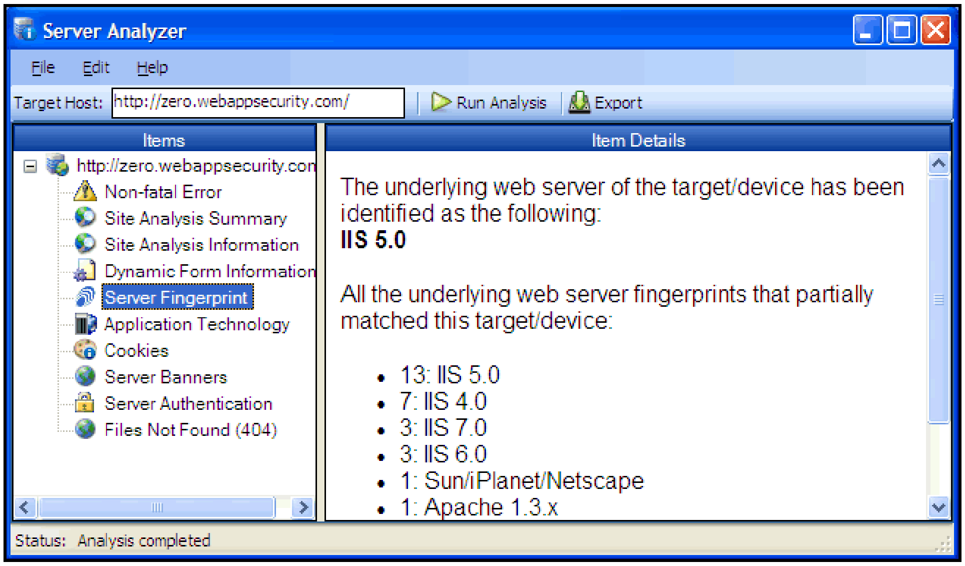
Server Analyzer

The Server Analyzer interrogates a server to determine the server's operating system, banners, cookies, and other information.

Analyzing a Server

Follow the steps below 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.



Target Host: http://zero.webappsecurity.com/

http://zero.webappsecurity.con

The underlying web server of the target/device has been identified as the following:
IIS 5.0

All the underlying web server fingerprints that partially matched this target/device:

- 13: IIS 5.0
- 7: IIS 4.0
- 3: IIS 7.0
- 3: IIS 6.0
- 1: Sun/iPlanet/Netscape
- 1: Apache 1.3.x

Status: Analysis completed

Server Analyzer Settings

Follow the steps below 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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.

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 type from the **Authentication** list. See Table 9 on page 114 for a description of the available authentication types.
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

Follow the steps below 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**.

Report Designer

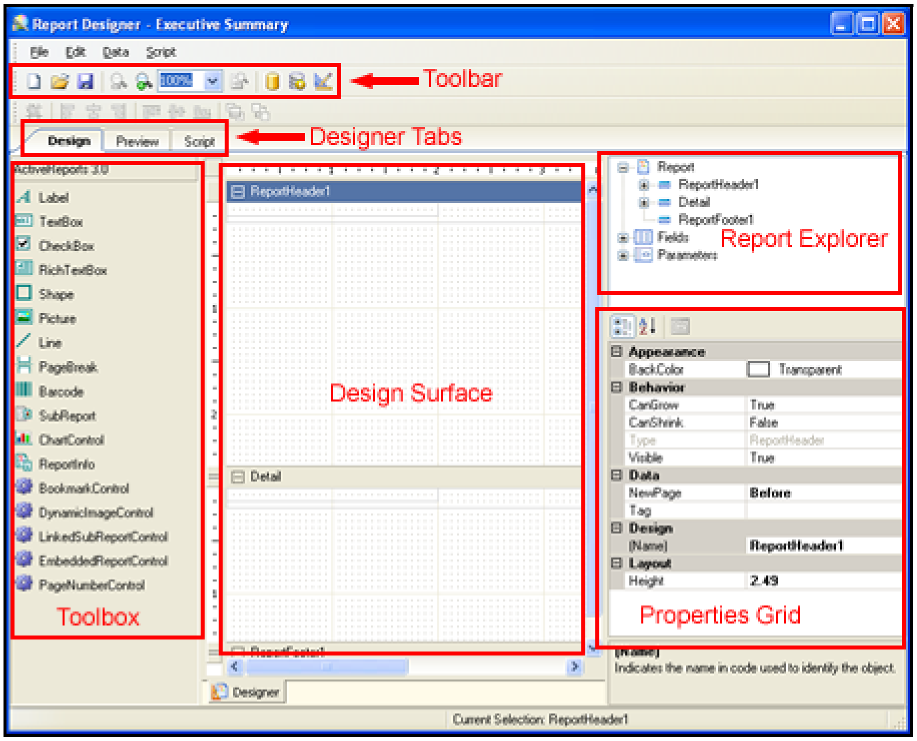
The Report Designer is an HP integration of the ActiveReports® 3.0 report designer developed by Grape City - Data Dynamics. It provides the ability to create and modify reports.

For complete information on using ActiveReports, refer to the ActiveReports User Guide and Class Library.

User Interface

The Report Designer contains six main components, as depicted in the following illustration:

- Toolbar
- Designer Tabs
- Toolbox
- Design Surface
- Report Explorer
- Properties Grid



Appearance	
BackColor	□ Transparent
Behavior	
CanGrow	True
CanShrink	False
Type	ReportHeader
Visible	True
Data	
NewPage	**Before**
Tag	
Design	
(Name)	**ReportHeader1**
Layout	
Height	**2.49**

(Name)
Indicates the name in code used to identify the object.

Current Selection: ReportHeader1

Toolbar

The Report Designer toolbar is illustrated below.

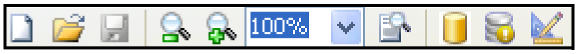


Table 8 Report DesignerToolbar

Icon	Function	Description
	New	Opens the *Create Report Definition* window, allowing you to select the queries to be included in the report.
	Open	Opens the *Open a Report* dialog, allowing you to select a report or subreport for editing.
	Save	Saves the open report.
	Zoom In	Increases the magnification of the design surface at 50 percent increments.
	Zoom Out	Decreases the magnification of the design surface at 50 percent increments.
100% ▾	Magnification Percentage	Allows you to select a magnification setting for the design surface.
	Actual Size	Returns the magnification of the design surface to 100 percent.
	Set Data Source	Allows you to specify the scan that will provide the data.
	Set Custom Data Source	Allows you to specify a custom data source.
	Parameter Designer	Opens the Parameter Designer tool.

Menus

The Report Designer contains the following menus:

Table 9 Report Designer Menus

Menu	Command	Description
File	New	Opens the *Create Report Definition* dialog, allowing you to select a definition for a new report.
	Open	Opens the *Open a Report* dialog, allowing you to select a report for editing.
	Save	Saves the open report.
	Save As	Saves the open report to a file you specify.
	Export	Saves the report in a format you specify.
	Enable Console Output	If enabled, WebInspect presents a pane (at the bottom of the window) that displays the status of each report page being generated. If a problem is encountered, this pane displays an exception message and stack trace. This pane is also visible on the Preview tab of the Report Designer.
	Exit	Terminates the Report Designer.
Edit	Parameter Designer	Opens the Parameter Designer tool.
	Modify/Create Report	Opens the *Modify Report Definition* dialog, allowing you to change the report definition.
	Delete	Deletes the selected object.
	Cut	Deletes the selected object and saves it to the clipboard.
	Copy	Copies the selected object to the clipboard.
	Paste	Inserts the contents of the clipboard.
	Undo	Reverses the last operation performed.
	Redo	Reverses the last Undo operation.
Data	Set Scan and Report Inputs	Allows you to select a scan and specify report parameters.
	Set Custom Data Source	Opens the *Report Data Source* dialog, allowing you to connect to various sources.
	Edit Global Styles	Opens the Report Styles Editor. Use this to create or modify a style sheet.
	Edit Report Styles	Opens the Report Styles Editor. Use this to create or modify styles for the report on which you are currently working
	Edit Report Settings	Opens the *Report Settings* dialog, allowing you to modify many facets of your report.
Script	Import	Allows you to select a script from the script library to import into the designer.

Table 9 Report Designer Menus (cont'd)

Menu	Command	Description
	Compile	Compiles the script.
	Find	Opens the **Script** tab and presents the *Find/Replace* dialog, allowing you to search for the text you specify.
	Script Editor	Opens the Script Editor.

Designer Tabs

The Report Designer contains the following three tabs.

Design Tab

By default, when you create or open a report, the Design tab is selected. Use this area to perform all design-time and run-time functions associated with your report, such as creating a layout, binding to data sources, creating event-handling methods, and more.

Script Tab

Selecting the Script tab opens the script editor, which gives you the ability to add scripting to your report. The Script editor allows you to create event-handling methods. In the Report Events tab on the right, there is a combo box where you can select any report section to attach an event-handling method.

Preview Tab

The Preview tab allows you to view what your report looks like at run time with actual scan data. This makes it easy to quickly see the run-time impact of changes you make in the designer or the code-behind. Use the Preview toolbar to navigate the report and add annotations.

Toolbox

The toolbox displays a variety of controls. To add a control, drag it from the toolbox and drop it on the design surface (canvas), where you can modify its size, position, alignment, and properties.

- Barcode — Inserts an ActiveReports Barcode control; can be bound to a database field.
- ChartControl — Inserts a chart in any of a variety of styles.
- Checkbox — Inserts a check box; can be bound to a database field.
- Label — Inserts a new static label control; can be bound to a database field.
- Line — Inserts a line control.
- PageBreak — Inserts a page break within a selection.
- Picture — Inserts an image loaded from a file; can be bound to a database field.
- ReportInfo — Displays report information in a number of format strings such as {PageNumber} of {PageCount}: can be bound to a database field.
- Textbox — Inserts a textbox; can be bound to a database field
- Shape — Inserts a rectangle, circle or square shape.

- Subreport — Inserts a Subreport control to link to another report.
- RichTextBox — Inserts an ActiveReports RichTextBox control; can be bound to a database field.
- BookmarkControl — Inserts a hyperlink in the table of contents; clicking the hyperlink navigates to the bookmark.

  Note: Bookmark text can formatted as follows:

  {=MainReportName}\<static-text>\{=<field-name>}

  where

  MainReportName is optional (and doesn't need to appear first)

  \ indicates the beginning of a hierarchical level

  <static-text> is any text you assign to the bookmark

  <field-name> is the name of a bound or calculated field
- DynamicImageControl — Allows you to associate an image selector control with an image (using the Parameter Designer), so the user can select an image a run time. Can be bound to a database field.
- LinkedSubreportControl — Creates a link to the subreport you select. Use the AssociatedFields property to pass values to the subreport.
- EmbeddedReportControl — Allows you to design a subreport “on the fly” (rather than using a LinkedSubreportControl) using the DataTableField property.
- PageNumberControl — Allows you to place a page number in the report (usually in the page footer).

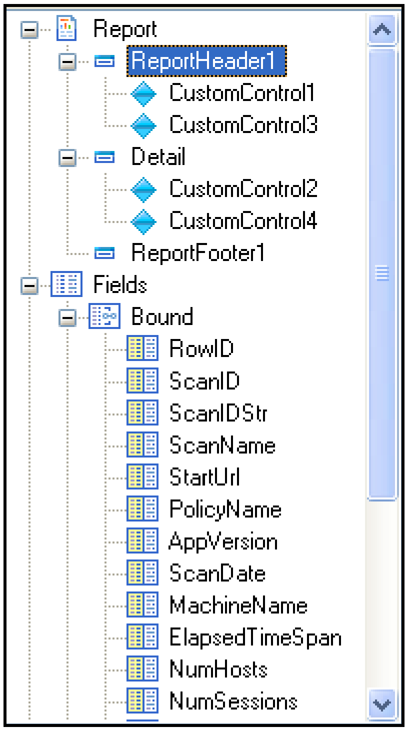
Design Surface

The default design surface contains the following base components:

- PageHeader section--This section can be used to print column headers, page numbers, page titles, or any information that needs to be printed once at the top of each page. Bound controls in the PageHeader or PageFooter are not supported. The data in such controls may not be synchronized with the data displayed in other sections on the page.
- Detail section--This section is the body of the report that prints once for each record in the data source. A report's layout may contain only one Detail section.
- PageFooter section--This section can be used to print page totals, page numbers or any other information that needs to be printed once at the bottom of each page.
- Designer/Script/Preview tabs--The Designer and Script tabs can be clicked to toggle between design and script views, while the Preview tab allows for a fully functional design-time preview of how a report will look and behave at run time.

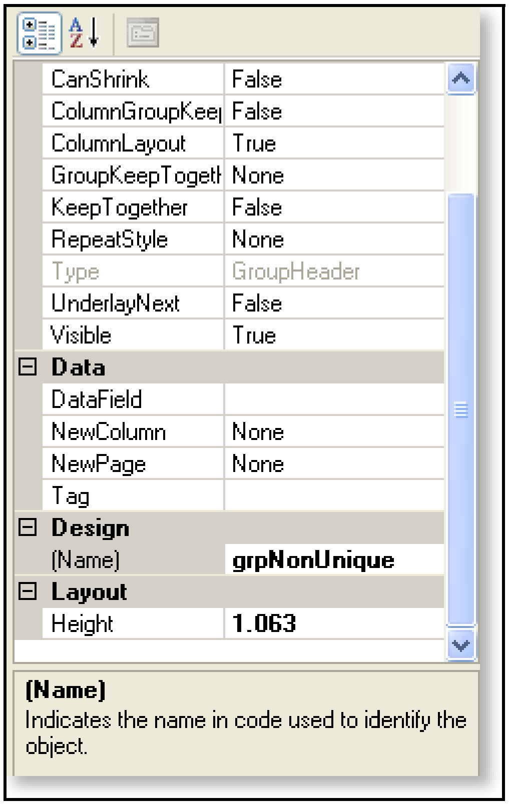
Report Explorer

The Report Explorer serves as the information focal point for your report. From it, you can gain a quick overview of the elements that compose the report, remove individual controls, add parameters and calculated fields, bind data fields to text box controls, and modify properties and report behavior via the Properties grid.



Properties Grid

The Properties Grid allows you to view or modify properties for an object selected on either the Design Surface or the Report Explorer.



CanShrink	False
ColumnGroupKee	False
ColumnLayout	True
GroupKeepTogeth	None
KeepTogether	False
RepeatStyle	None
Type	GroupHeader
UnderlayNext	False
Visible	True
Data	
DataField	
NewColumn	None
NewPage	None
Tag	
Design	
(Name)	**grpNonUnique**
Layout	
Height	**1.063**

(Name)
Indicates the name in code used to identify the object.

Creating a Report

1 Open or create a report definition.

To create a report definition:

a Click **File** → **New** (or click the New icon on the toolbar).

b Create a report definition.

c Enter a name and (optionally) a brief description for the report.

d Select a report context: either **Scan** or **Session**.

When a scan is open, users can generate a session report by right-clicking a session and selecting **Generate Session Report** from the context menu.

e If you want the report name to be included in the list of WebInspect reports, select **Exposed in Product**.

Typically, you do not select this option if you are creating a subreport.

f If you are creating a header/footer template, select **Header/Footer Template**.

g Select one or more views from the View Name list. To see the view parameters and fields, click the view name.

h Click **OK**.

To open a report definition:

a Click **File** → **Open** (or click the Open icon on the toolbar).

b Select a report or subreport.

c Click **OK**.

2 Design your report. For complete information on using ActiveReports, refer to the ActiveReports User Guide and Class Library.

3 To modify the script associated with this report, click the **Script** tab.

4 To modify or create parameters associated with this report, click **Edit** →**Parameter Designer**.

5 To modify the styles associated with this report, click **Data** → **Edit Report Styles**.

6 To preview your work:

a Click the **Preview** tab.

b On the *Generate a Report* dialog, select a scan and click **Next**.

c If the report includes parameters, select parameters.

d Click **Finish**.

Report Script Editor

Use the Report Script Editor to create or modify scripts maintained in a script library. You can then import these scripts into reports.

All scripts must be written using the C# language.

The Report Script Editor menu bar contains the following menus:

Table 10 Report Script Editor Menus

Menu	Command	Description
File	Save	Save the script to a library.
	Refresh	Redisplay the script.
	Exit	Terminate the Script Editor.
Edit	Find	Open a *Find/Replace* dialog, allowing you to search for and optionally replace text in the script.
Script	Import	Incorporate a script library into the script you are developing.
	Compile	Compile the script.
Help	Help	Open the Help file.

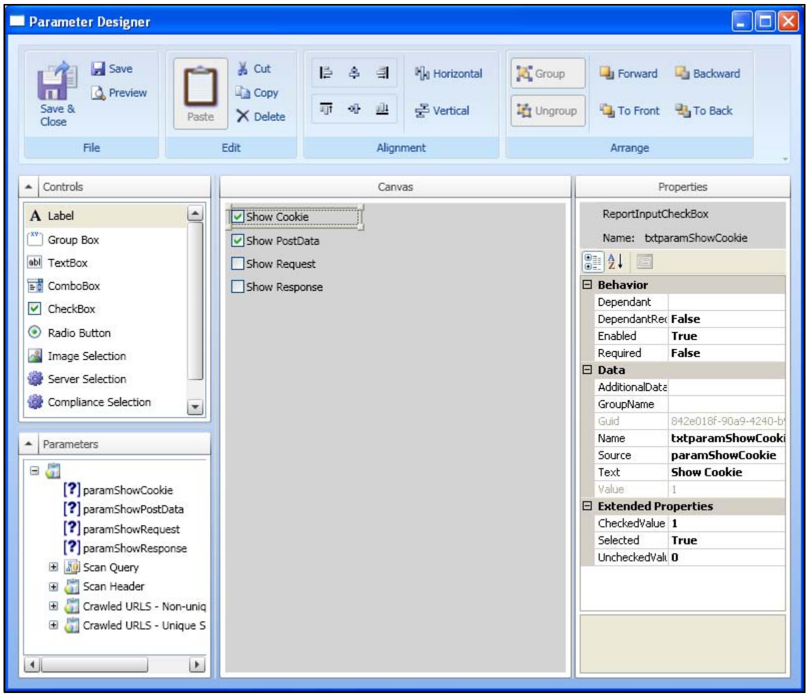
Parameter Designer

Reports have three types of inputs that can be used for filtering data or supplying custom content to reports. They are:

- **Data View parameters (query parameters)** – Data View parameters are used to pass values to the underlying Data View of the report for filtering data. Parameter names begin with @.
- **Report Parameters** – Report parameters are used to pass values entered by the user to the report. These values are then used by the report to alter report behavior or format.
- **Replacements** – Replacements are tokens that exist in the data view. Replacement inputs are used to pass values to these tokens. Replacements are used to change the sort order of a data view or to provide additional criteria to the data view.

Users have the opportunity to provide values for these inputs when generating a report. Before a user can be prompted to enter inputs, however, report designers must specify which inputs will be displayed to the user and how they will be presented. This is accomplished by using the Parameter Designer.

To open the Parameter Designer, from an open report in the Report Designer, click the Parameter Designer icon on the toolbar or choose **Parameter Designer** from the **Edit** menu.



☑ Show Cookie
☑ Show PostData
□ Show Request
□ Show Response

ReportInputCheckBox

Name: txtparamShowCookie

Behavior	
Dependant	
DependantRe(	**False**
Enabled	**True**
Required	**False**
Data	
AdditionalData	
GroupName	
Guid	842e018f-90a9-4240-b
Name	**txtparamShowCooki**
Source	**paramShowCookie**
Text	**Show Cookie**
Value	1
Extended Properties	
CheckedValue	**1**
Selected	**True**
UncheckedVal(	**0**

The Parameter Designer has five areas.

Toolbar

The toolbar provides easy access to all of the functions of the designer:

- **Save and Close** – Saves the current design to the report and closes the *Parameter Designer* window.
- **Save** – Saves the current design to the report.
- **Preview** – Opens a window showing what the designed inputs will look like at run time.
- **Cut, Copy, Paste, Delete** – Manipulate controls on the canvas.
- **Alignment** – Align one or more selected controls on the canvas.
- **Group/Ungroup** – A designer can group two or more selected controls on the canvas. When controls are grouped together, they can be moved together on the canvas.
- **Forward** – Bring the selected control forward one layer.
- **Backward** – Send the selected control backward one layer.
- **To Front** – Bring the selected control to the top most layer.
- **To Back** – Send the selected control to the bottom most layer.

Canvas

The canvas is the design area, which constitutes a visual representation of the parameters that are presented at run-time. Controls can be added, modified, and deleted from the canvas.

Properties Grid Pane

This area displays the properties of object(s) selected in the design canvas or the Parameters pane, whichever has the focus.

Controls Toolbox

The Controls toolbox lists the types of controls that may be added to the report. They include, in addition to the standard self-explanatory controls, the following special controls:

- **Server Selection** - A drop-down list of available servers in the selected scan.
- **Compliance Selection** - A list of compliance templates; suitable for compliance reports only.
- **Sort Control** - Allows you to select how you want the report data to be sorted.

To add a control, drag it from the toolbox and drop it on the canvas.

Report Parameters Pane

This pane displays a hierarchical representation of all parameters available to the current report and its subreports. Icons indicate the parameter type.

Query

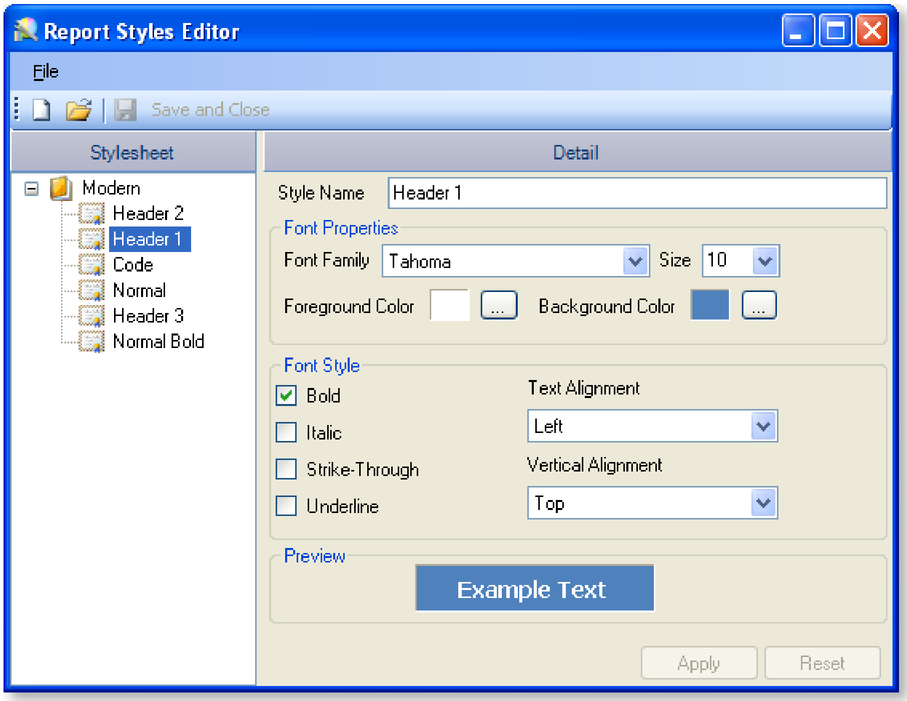
Report [?]

Replacement

Report Styles Editor

When creating or modifying a report, the Report Designer uses the style sheet that is specified as the default. If you want to create or modify styles for the report on which you are currently working, select **Edit Report Styles** from the **Data** menu. New styles will be added to the report; modified styles will override the default definition for this report.

Conversely, if you want to create or modify a style sheet, select **Edit Global Styles** from the **Data** menu. You can then edit or create stylesheets, and specify the style sheet that will be initially assigned to all reports as the default.



Style Name: Header 1

Font Family: Tahoma

Size: 10

Foreground Color: □ ...

Background Color: ■ ...

☑ Bold

□ Italic

□ Strike-Through

□ Underline

Text Alignment: Left

Vertical Alignment: Top

Report Structure

Report Structure

A report section contains a group of controls that are processed and printed at the same time as a single unit. ActiveReports defines the following section types.

Report Header

A report can have one report header section that prints at the beginning of the report. This section generally is used to print a report title, a summary table, a chart or any information that needs only to appear once at the report's start.

Report Footer

A report can have one report footer section that prints at the end of the report. This section is used to print a summary of the report, grand totals, or any information that needs to print once at the report's end.

Page Header

A report can have one page header section that prints at the top of each page. Unless the page contains a report header section, the page header will be the first section that prints on the page. The page header section is used to print column headers, page numbers, a page title, or any information that needs to appear at the top of each page in the report.

Page Footer

A report can have one page footer section that prints at the bottom of each page. It is used to print page totals, page numbers, or any other information that needs to appear at the bottom of each page.

Group Header/Footer

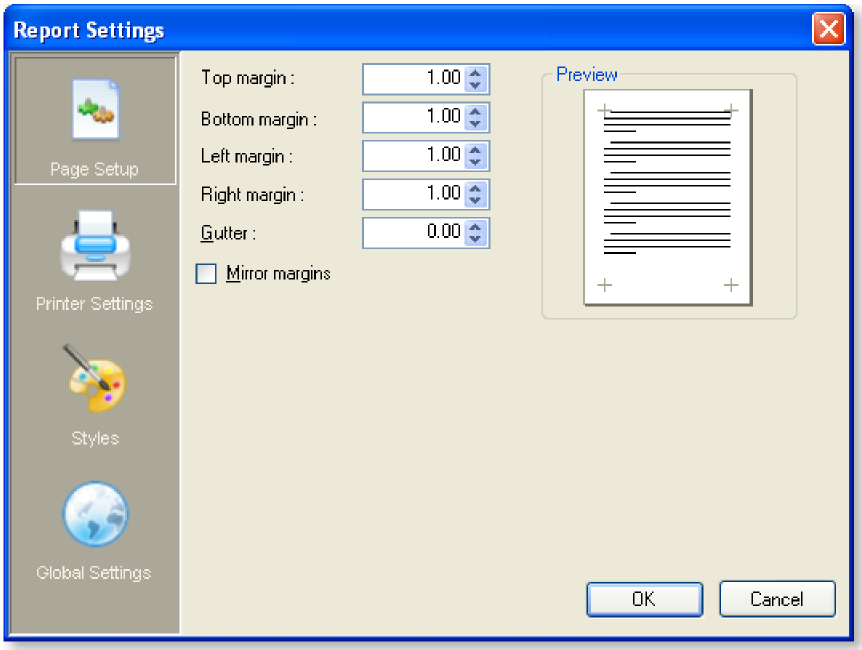
A report can consist of single or multiple nested groups, with each group having its own header and footer sections. The header section is inserted and printed immediately before the detail section. The footer section is inserted and printed immediately after the detail section.

Detail

A report has one detail section. The detail section is, in some cases, the body of the report and one instance of the section is created for each record in the report.

Report Settings

You can modify facets of your report, such as the page setup, printer settings, styles, and global settings of your report at design time. To make changes, access the *Report Settings* dialog by selecting Data > Edit Report Settings.



Report Settings

Top margin : 1.00

Bottom margin : 1.00

Left margin : 1.00

Right margin : 1.00

Gutter : 0.00

□ Mirror margins

Charts

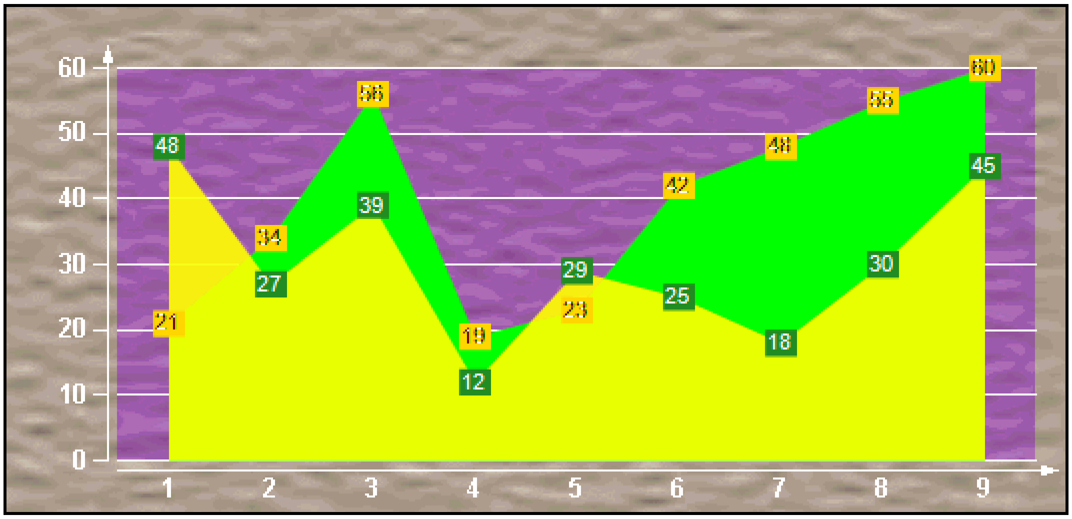
Chart Types

Chart types include Common Charts, 3D Charts, and XY Charts. See the on-line Help for more extensive illustrations of chart types.

Common Charts

- **Area Charts**

  Use an area chart to compare trends over a period of time or in specific categories.



  Number of Y values/data points: 1

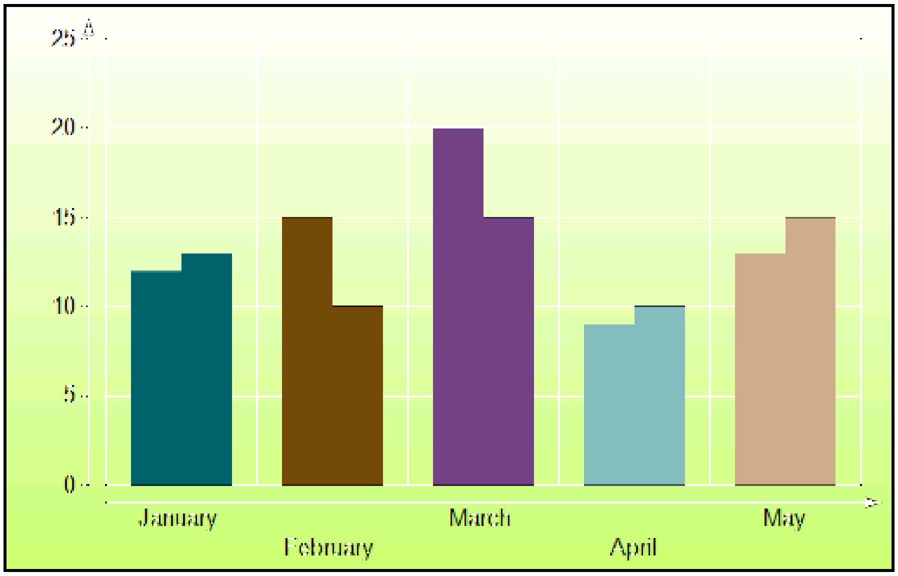
  Number of Series: 1 or more

  Marker Support: Series or Data Point

  Custom Properties: None

- **Bar2D Charts**

  Use a bar chart to compare values of items across categories.



  Number of Y values/data point: 1

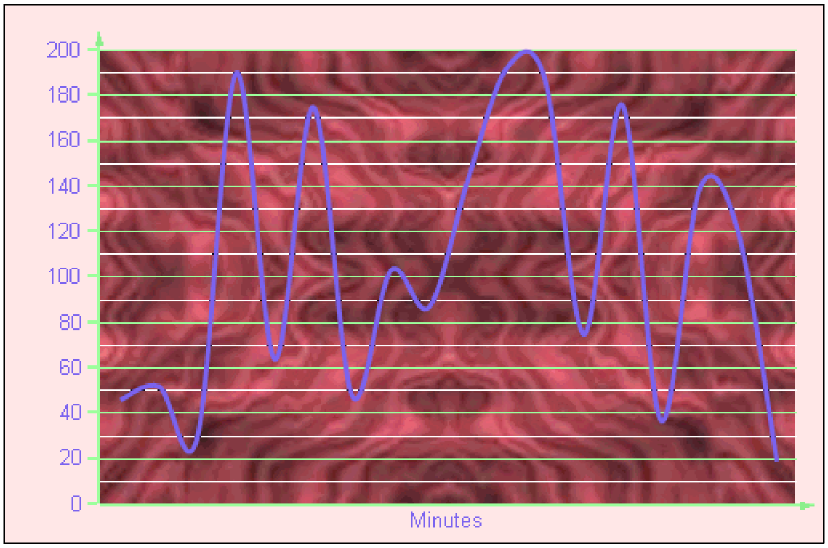
  Number of Series: 1 or more

  Marker Support: Series or Data Point

  Custom Properties: Gap gets or sets the space between the bars of each X axis value

- **Bezier Charts**

  Use a Bezier or spline chart to compare trends over a period of time or in certain categories. It is a line chart that plots curves through the data points in a series.



  Number of Y values/data point: 1

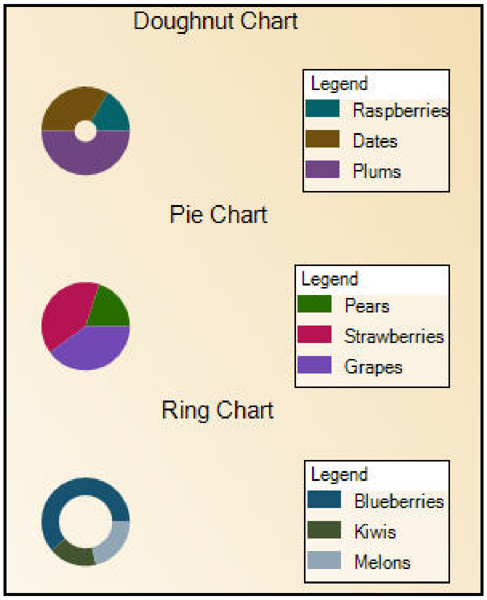
  Number of Series: 1 or more

  Marker Support: Series or Data Point

  Custom Properties: None

- **Doughnut/Pie Charts**

  A doughnut chart shows how the percentage of each data item contributes to the total.



  Number of Y values/data point: 1

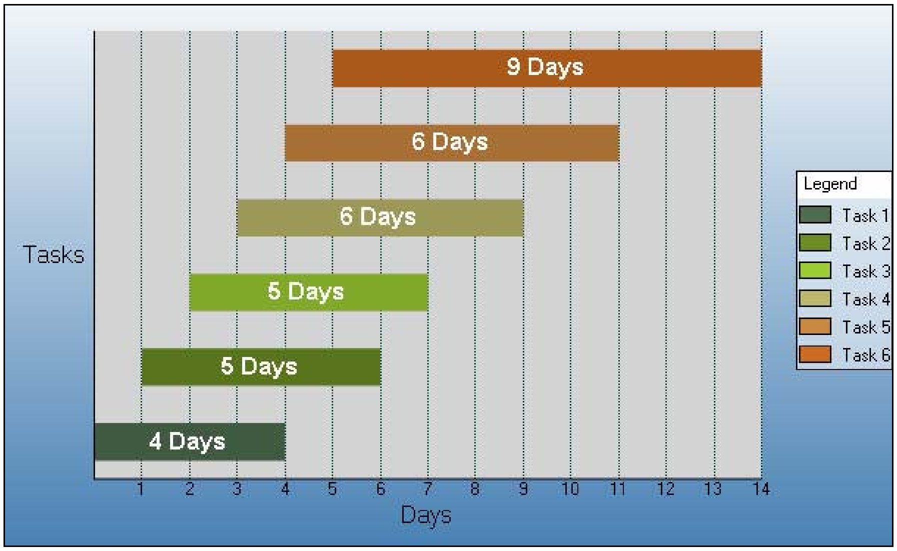
  Number of Series: 1

  Marker Support: Series or Data Point

Custom Properties: ExplodeFactor gets or sets the amount of separation between data point values. HoleSize gets or sets the inner radius of the chart. OutsideLabels gets or sets a value indicating whether the data point labels appear outside the chart. StartAngle gets or sets the horizontal start angle for the series.

- **Gantt Charts**

  The Gantt chart is a project management tool used to chart the progress of individual project tasks. The chart compares project task completion to the task schedule.



Number of Y values/data point: 2

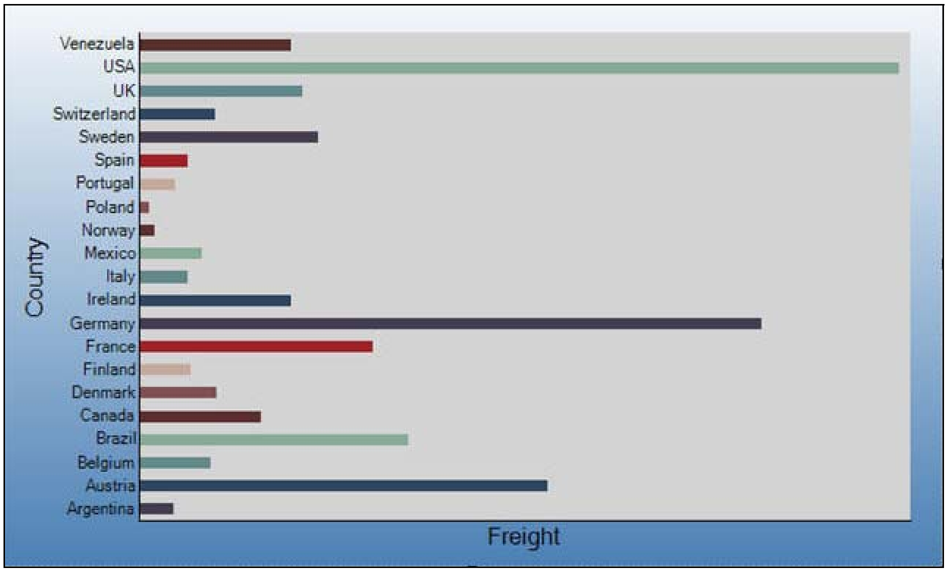
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value.

- **HorizontalBar Charts**

  Use a horizontal bar chart to compare values of items across categories with the axes reversed.



Number of Y values/data point: 1

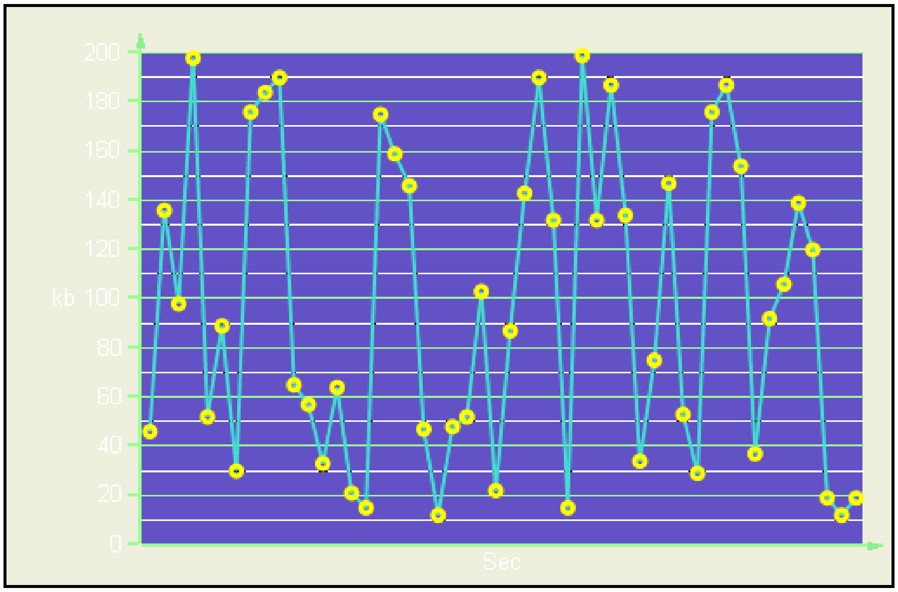
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value.

- **Line Charts**

  Use a line chart to compare trends over a period of time or in certain categories.



Number of Y values/data point: 1

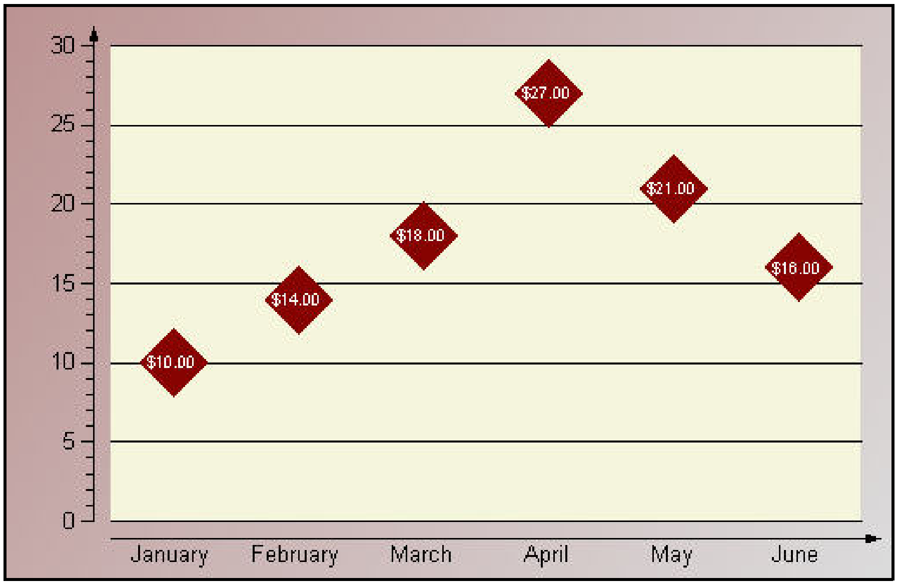
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **Scatter Charts**

  Use a scatter chart to compare values across certain categories.



Number of Y values/data point: 1

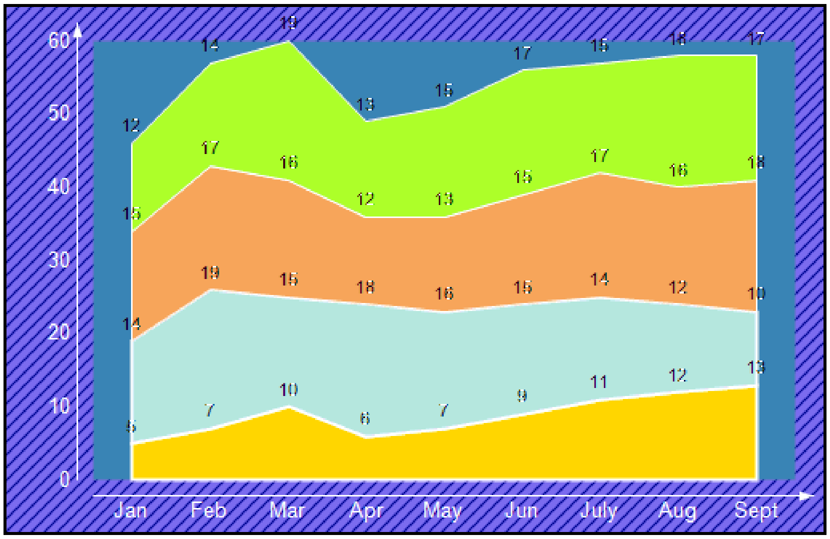
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **StackedArea Charts**

  A stacked area chart is an area chart with two or more data series stacked one on top of the other. Use this chart to show how each value contributes to a total.



Number of Y values/data point: 1

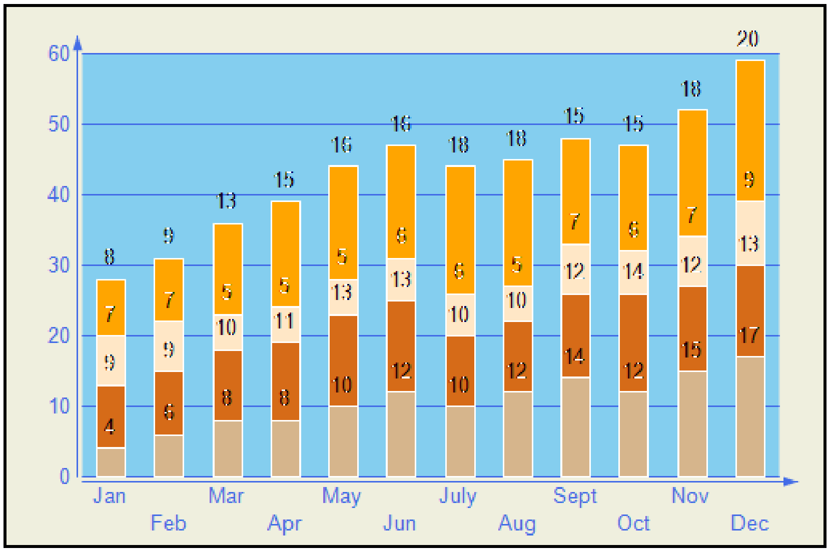
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **StackedBar Charts**

  A stacked bar chart is a bar chart with two or more data series stacked one on top of the other. Use this chart to show how each value contributes to a total.



Number of Y values/data point: 1

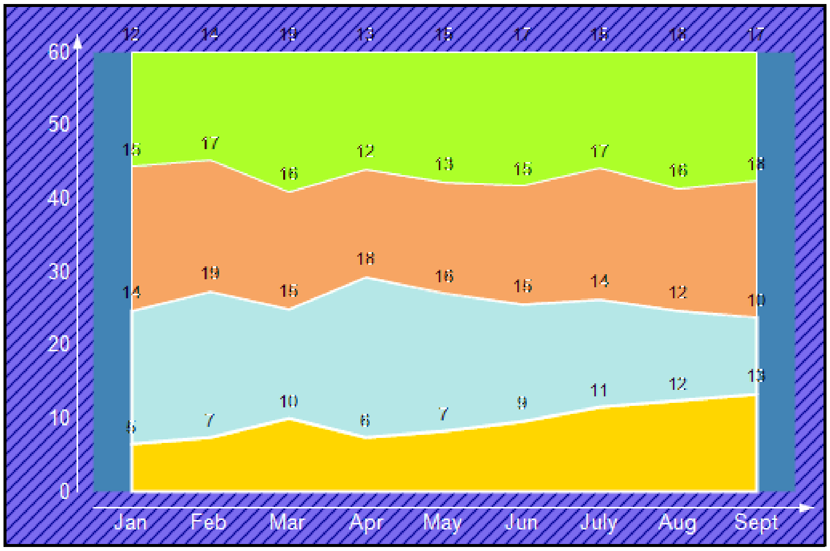
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value

- **StackedArea100Pct Charts**

  A stacked area 100 percent chart is an area chart with two or more data series stacked one on top of the other to sum up to 100 percent. Use this chart to show how each value contributes to a total with the relative size of each series representing its contribution to the total.



  Number of Y values/data point: 1

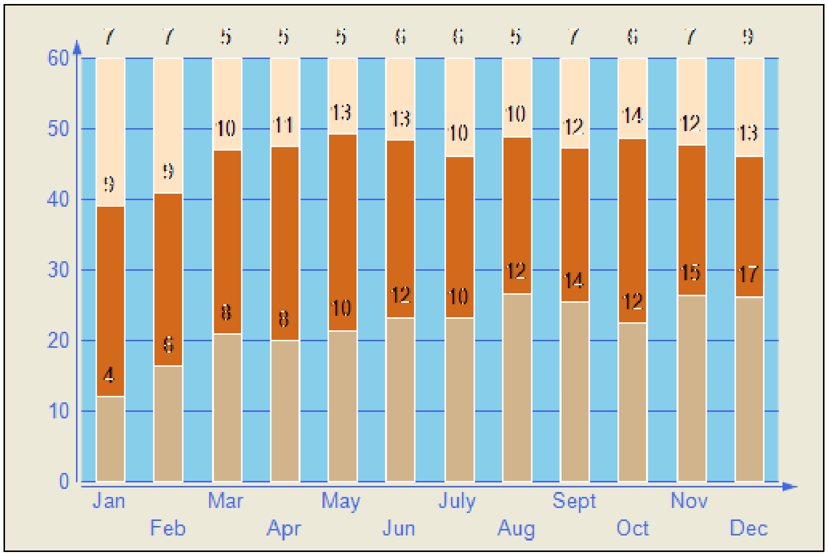
  Number of Series: 1 or more

  Marker Support: Series or Data Point

  Custom Properties None

- **StackedBar100Pct Charts**

A StackedBar100Pct chart is a bar chart with two or more data series stacked one on top of the other to sum up to 100 percent. Use this chart to show how each value contributes to a total with the relative size of each series representing its contribution to the total.



Number of Y values/data point: 1

Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value

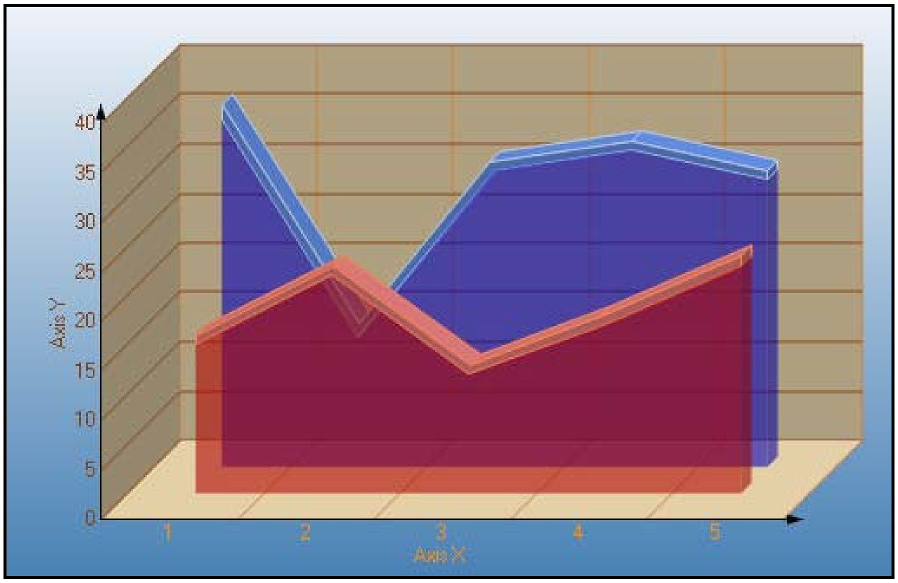
3D Charts

This topic illustrates some of the three dimensional chart types that you can create with the Chart control.

Note: To see a chart in three dimensions, open the *ChartArea Collection* dialog, and in the Projection section, change the ProjectionType from Identical to Orthogonal.

- **Area3D Charts**

Use a 3D area chart to compare trends in two or more data series over a period of time or in specific categories, allowing the data to be viewed side by side.



Number of Y values/data point: 1

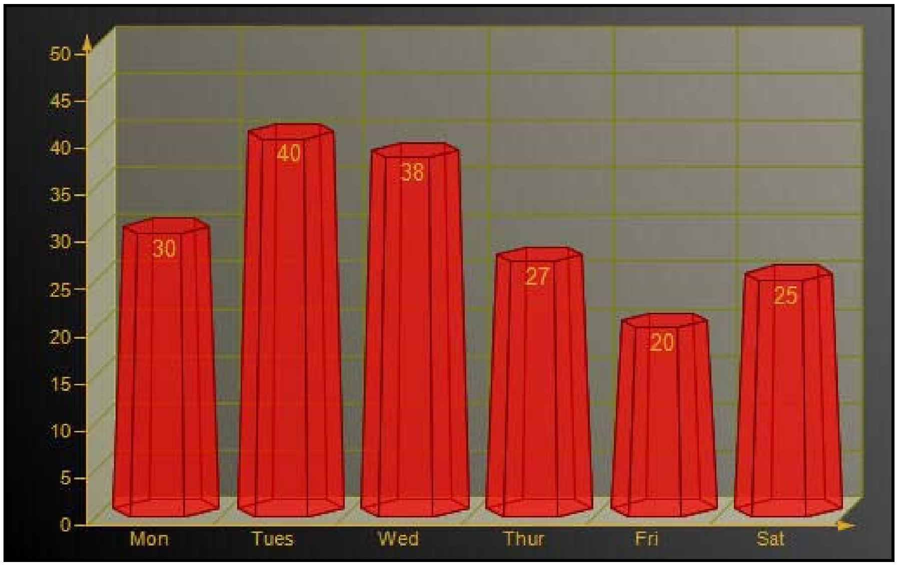
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: LineBackdrop gets or sets the backdrop information for the 3D line. Thickness gets or sets the thickness of the 3D line. Width gets or sets the width of the 3D line.

- **Bar3D Charts**

  Use a 3D bar chart to compare values of items across categories, allowing the data to be viewed conveniently in a 3D format.



Number of Y values/data point: 1

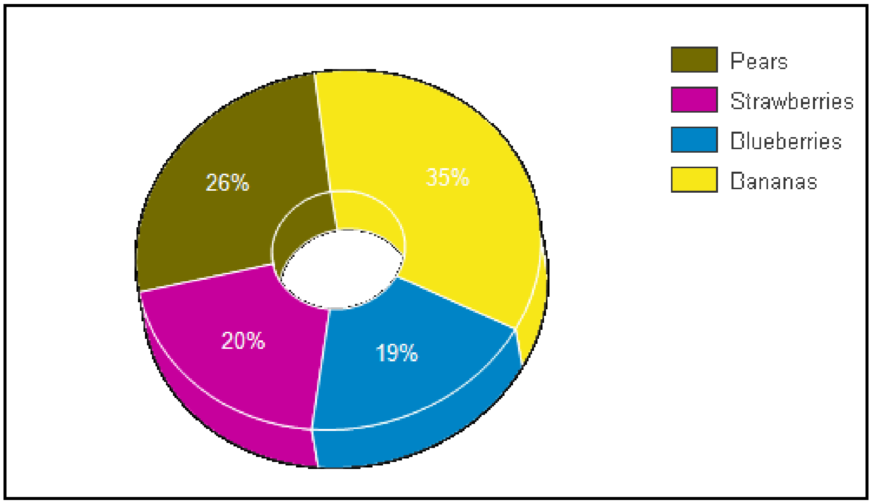
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: BarTopPercent gets or sets the percentage of the top of the bar that is shown for Cone or Custom BarTypes. BarType gets or sets the type of bars that is displayed. Gap gets or sets the space between the bars of each X axis value. RotationAngle gets or sets the starting horizontal angle for custom 3D bar shapes. Can only be used with the Custom BarType. VertexNumber gets or sets the number of vertices for the data point, used to create custom 3D bar shapes. Can only be used with the CustomBarType. Bars must contain 3 or more vertices.

- **Doughtnut3D Pie Charts**

  A 3D doughnut chart shows how the percentage of each data item contributes to a total percentage, allowing the data to be viewed in a 3D format.



A 3D doughnut chart shows how the percentage of each data item contributes to a total percentage, allowing the data to be viewed in a 3D format.

Number of Y values/data point: 1

Number of Series: 1

Marker Support: Series or Data Point

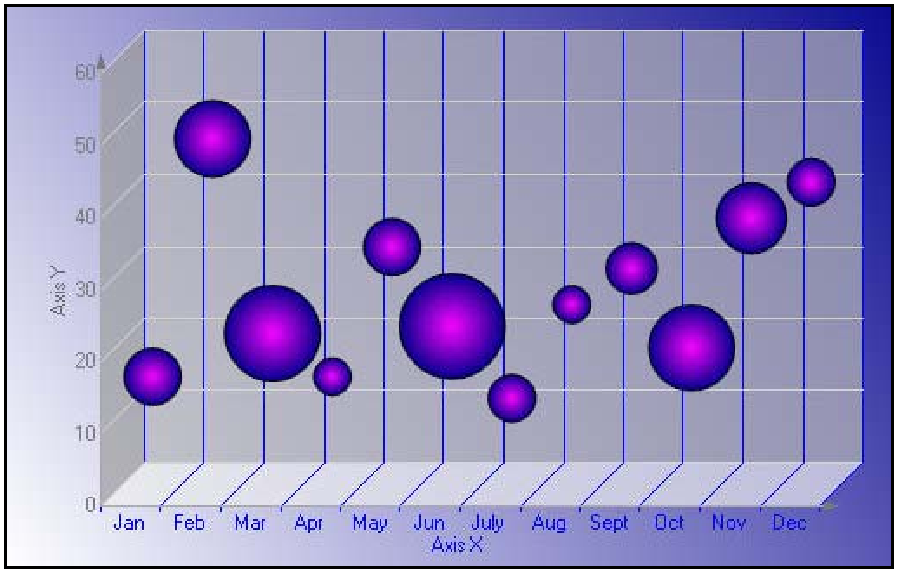
Custom Properties: ExplodeFactor gets or sets the amount of separation between data point values. The value must be less than or equal to 1. To explode one section of the doughnut chart, set ExplodeFactor on the data point instead of on the series. HoleSize gets or sets the inner radius of the chart. If set to 0, the chart will look like a pie chart. The value must be less than or equal to 1. OutsideLabels gets or sets a value indicating whether the data point labels appear outside of the graph. StartAngle gets or sets the horizontal start angle for the series data points.

XY Charts

Some of the XY chart types you can create with the Chart control are described below.

- **Bubble Charts**

The Bubble chart is an XY chart in which bubbles represent data points. The first Y value is used to plot the bubble along the Y axis, and the second Y value is used to set the size of the bubble. The bubble shape can be changed using the series Shape property.



Number of Y values/data point: 2

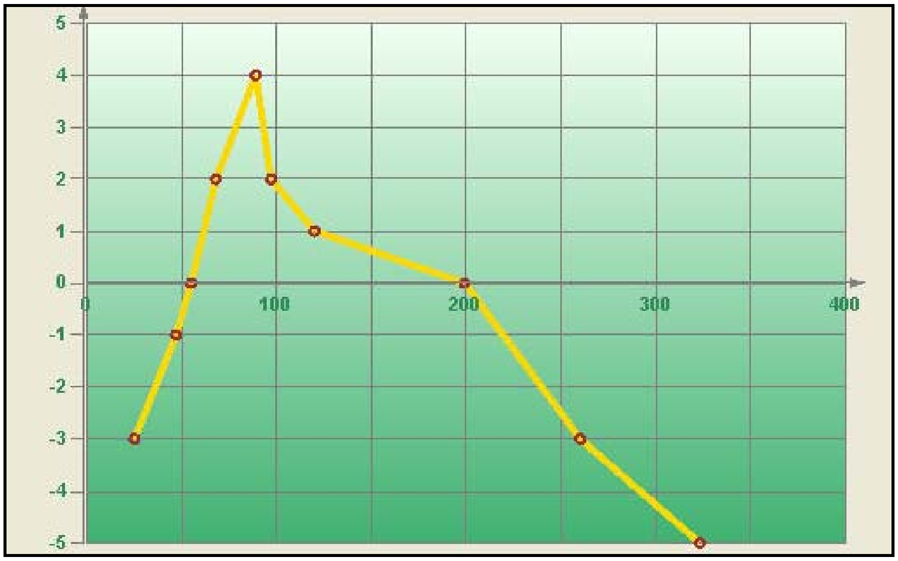
Number of Series: 1 or more

Marker Support: Series or Data Point. Marker labels use the second Y value as the default value.

Custom Properties: MaxSizeFactor gets or sets the maximum size of the bubble radius. Values must be less than or equal to 1. Default is .25. MaxValue gets or sets the bubble size that is used as the maximum. MinValue gets or sets the bubble size that is used as the minimum. Shape gets or sets the shape of the bubbles. Uses or returns a valid MarkerStyle enumeration value.

- **LineXY Charts**

  A line XY chart plots points on the X and Y axes as one series and uses a line to connect points to each other.



Number of Y values/data point: 1

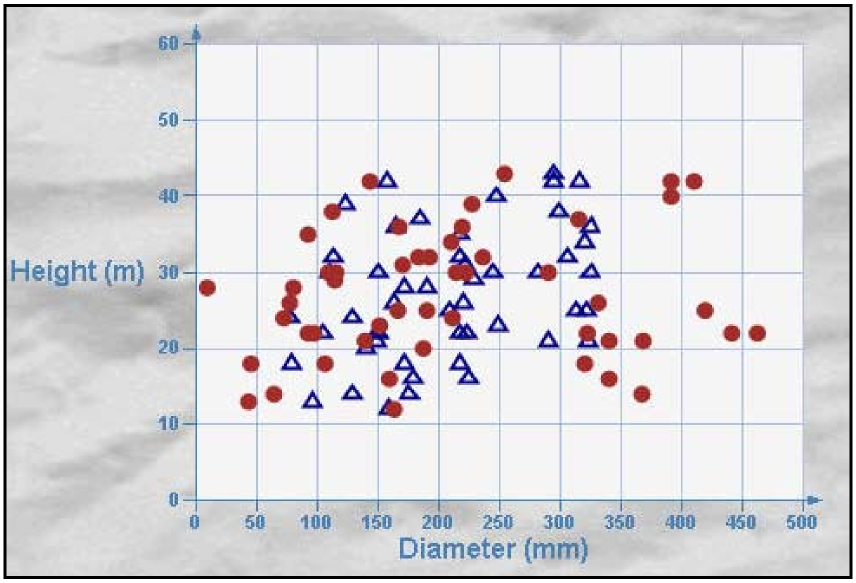
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **PlotXY Charts**

  A plot XY chart shows the relationships between numeric values in two or more series sets of XY values.



Number of Y values/data point: 1

Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

Chart Data

Data-Bound Charts

The Chart control provides several ways to bind your charts to data at design time.

- Adding Data with the Wizard

  To open the Chart Wizard, right-click the chart and select Wizard. In the Chart Wizard, once you have added a series, you can create a data adapter to contain the data for your chart, if needed. When a data source is available, the Value X and Y values can be set for the series in the chart wizard from the expressions and/or data columns retrieved from the data source.

- Adding Data with the Chart Designer

  Once a data source is set up, you can easily bind data to a series using the Chart Designer. Choose the Series section on the left, and on the **General** tab, after a series has been added to the chart, set the ValueY property by selecting the name of the data expression you wish to assign to the series.

- Adding Data through the *Chart Data Source* Dialog

To set the data source for the chart through the *Chart Data Source* dialog, click the DataSource property.

After the DataSource for the chart is set, add a series to the chart. To do this, open the *Series Collection Editor* dialog by clicking the ellipsis button which appears when you click next to the Series property in the *Properties* window, then click the **Add** button. To bind the series to an expression or dataset column returned by your data source, set the ValueMembersY or ValueMembersX property of the series by selecting it from the drop-down list.

Unbound Charts

The Chart control makes it easy to set the data source for a chart control, series, or data points collection at run time.

Below is a list of objects that can be used as data sources.

- dataset
- dataset Column
- Data Table
- SqlCommand/OleDbCommand
- SqlDataAdapter/OleDbDataAdapter
- Array

Below are some examples of binding to different data sources at run time.

dataset

The Chart control's DataSource property can be set to a dataset at run time. The following code demonstrates setting up a dataset, setting the DataSource property to the dataset, creating a series, and setting the ValueMembersY property to the dataset expression at run time.

```
// C#

// create the series

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist

    Security Info=False";

System.Data.OleDb.OleDbConnection m_cnn = new
System.Data.OleDb.OleDbConnection(m_cnnString);

System.Data.OleDb.OleDbDataAdapter oDBAdapter;

 // create the dataset

System.Data.DataSet oDS;

oDBAdapter = new System.Data.OleDb.OleDbDataAdapter("SELECT ShipCountry,
SUM(Freight) AS

    Expr1 FROM Orders GROUP BY ShipCountry", m_cnnString);

oDS = new System.Data.DataSet();

oDBAdapter.Fill(oDS, "Expr1");
```

```
// set the DataSource and ValueMembersY properties

this.ChartControl1.DataSource = oDS;

s.ValueMembersY = "Expr1";

this.ChartControl1.Series.Add(s);
```

dataset Column

In the Chart control, the ValueMembersX and ValueMembersY properties of a series can be set to a dataset column. The following code demonstrates creating a series, setting up a dataset, setting the DataSource property to the dataset, and setting the ValueMembersY and ValueMembersX properties to dataset columns at run time.

```
// C#

// create the series

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist

    Security Info=False";

System.Data.OleDb.OleDbConnection m_cnn = new
System.Data.OleDb.OleDbConnection(m_cnnString);

System.Data.OleDb.OleDbDataAdapter oDBAdapter;

 // create the dataset

System.Data.DataSet oDS;

oDBAdapter = new System.Data.OleDb.OleDbDataAdapter("SELECT * from Orders
WHERE OrderDate

    < #08/17/1994#", m_cnnString);

oDS = new System.Data.DataSet();

oDBAdapter.Fill(oDS, "Orders");

 // set the DataSource, ValueMembersY, and ValueMembersX properties

this.ChartControl1.DataSource = oDS;

this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].ValueMembersY =
oDS.Tables["Orders"].Columns[7].ColumnName;

this.ChartControl1.Series[0].ValueMemberX =
oDS.Tables["Orders"].Columns[8].ColumnName;
```

Data Command

A chart's data source can be set to a SqlCommand or OleDbCommand. The following code demonstrates creating a series, creating an OleDbCommand, setting the DataSource property to the data command, and setting the ValueMembersY property for the series at run time.

```
// C#

// create the series
```

```
DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist

    Security Info=False";

System.Data.Oledb.OleDbConnection m_cnn = new
System.Data.Oledb.OleDbConnection(m_cnnString);

string query = "SELECT ShipCountry, SUM(Freight) AS Expr1 FROM Orders GROUP
BY ShipCountry";

 // create the OleDbCommand and opent the connection

System.Data.Oledb.OleDbCommand command = new
System.Data.Oledb.OleDbCommand(query, m_cnn);

command.Connection.Open();

 // set the DataSource and ValueMembersY properties

this.ChartControl1.DataSource = command;

this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].ValueMembersY = "Expr1";

 // close the connection

m_cnn.Close();
```

Array

The Chart control allows the data source for the data points collection to be set to an array. The following code demonstrates creating a series, creating an array, and using the DataBindY method to set the data source for the data points collection at run time.

```
// C#

// create the series

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

 // create the array

double [] a = {1,4,2,6,3,3,4,7};

// set the data source for the data points collection

this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].Points.DataBindY(a);
```

Calculated and Sequence Series Charts

The Chart control allows you to bind a formula to the ValueMembersY property of a series to create a calculated or sequence series for your chart.

Calculated Series

You can easily create a calculated series based on the values of one or more series by setting the ValueMembersY property of a series to a formula. To reference a series in the formula, use the name of the series. The following code demonstrates creating two series, one bound to a data array and the other bound to a formula based on the Y values of the first series.

```
// C#

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

DataDynamics.ActiveReports.Chart.Series cS = new
DataDynamics.ActiveReports.Chart.Series();

double [] a = { 1,4,2,6,3,3,4,7};

 this.ChartControl1.Series.AddRange(new DataDynamics.SharpGraph.Windows.Series[]
{s, cS});

this.ChartControl1.Series[0].Name = "Series1";

this.ChartControl1.Series[0].Points.DataBindY(a);

this.ChartControl1.Series[1].ValueMembersY = "Series1.Y[0]+10";
```

Sequence Series

Set a sequence series by specifying the minimum value, maximum value, and step for the series. The following code shows how to set the ValueMembersY property at run time to create a sequence series.

```
// C#

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].ValueMembersY = "sequence(12,48,4)";
```

Chart Effects

Colors

In the Chart control, colors can be used in different ways to enhance the chart's appearance, distinguish different series, point out or draw attention to data information such as averages, and more.

Color Palettes

The Chart control includes several pre-defined color palettes that can be used to automatically set the colors for data values in a series. The pre-defined palettes are as follows:

- Cascade (default) A cascade of eight cool colors ranging from deep teal down through pale orchid.
- Confetti A sprinkling of bright and pastel colors.
- Iceberg A range of the soft blues and greys found in an iceberg.
- Springtime The colors of spring, in deep green, two vivid colors and five pastels.
- None All data is drawn using the same teal color.

These enumerated values are accessed through the Series class with code like the following.

```
// C#

this.ChartControl1.Series[0].ColorPalette = DataDynamics.ActiveReports.Chart.

ColorPalette.Iceburg;
```

Gradients

Gradients can be used in object backdrops to enhance the visual appearance of various chart items. Gradients can be used in the following chart sections:

- Chart backdrop
- Chart area backdrops
- Wall backdrops
- Title backdrops
- Legend backdrops
- Legend item backdrops (for custom legend items)
- WallRange backdrops
- Series backdrops
- Data point backdrops
- Marker backdrops
- Marker label backdrops
- Annotation TextBar backdrops

3D Effects

Using the projection and viewpoint settings, you have the ability to display your 3D chart at or from any angle needed to provide the desired view or call attention to a specific chart section.

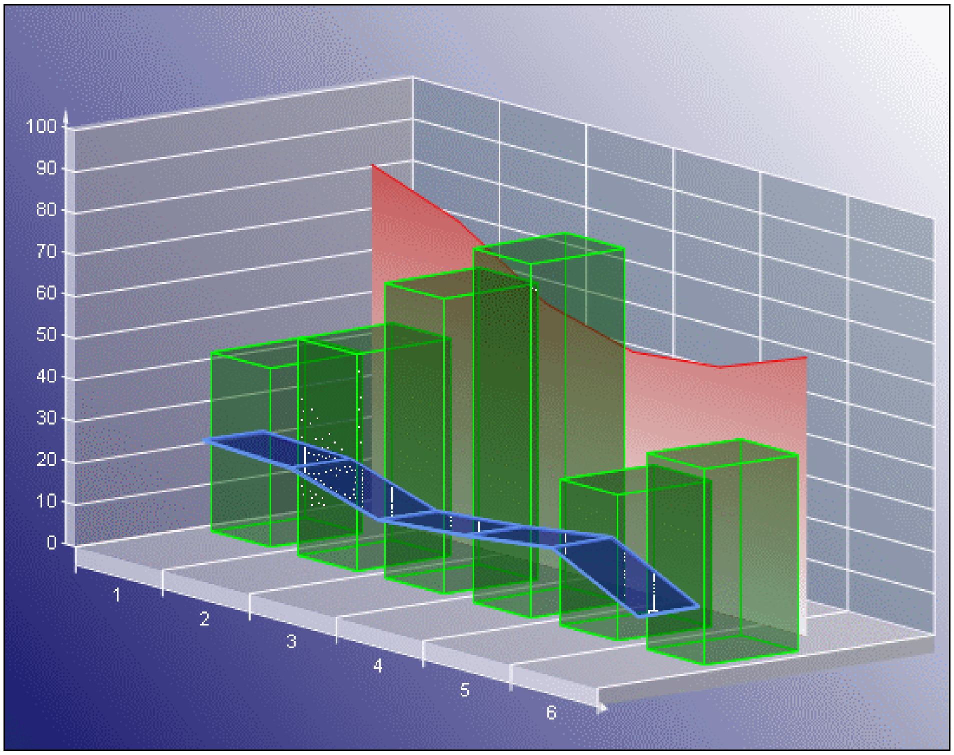
Projection

Determine the projection for a 3D chart using three factors: the ZDepth ratio, the projection type, and the projection DX and DY values.

- ZDepth ratio The Z depth ratio is the level of depth the Z axis has in the chart. Values range from 0 (for a 2D chart) to 1.0.
- ProjectionType The type of projection used for the chart. In order to show charts three dimensionally, the ProjectionType in the ChartArea Collection editor must be set to Orthogonal. To access this dialog box, click the ellipsis button next to the ChartAreas (Collection) property in the *Properties* window.
- ProjectionDX The origin position of the Z axis in relation to the X axis. This property is valid only when the ProjectionType is Orthogonal.
- ProjectionDY The origin position of the Z axis in relation to the Y axis. This property is valid only when the ProjectionType is Orthogonal.
- HorizontalRotation The HorizontalRotation property allows you to set the degree (-90° to 90°) of horizontal rotation from which the chart is seen.
- VerticalRotation The VerticalRotation property allows you to set the degree (-90° to 90°) of vertical rotation from which the chart is seen.

Lighting

The Chart control provides the ability to completely customize lighting options for 3D charts.



Directional Light Ratio

Using the DirectionalLightRatio property, you can control the directional or ambient intensity ratio.

Light Type

By setting the Type property to one of the enumerated LightType values, you can control the type of lighting used in the chart. The settings are as follows:

- Ambient An ambient light source is used. It is equal to DirectionalLightRatio = 0.
- InfiniteDirectional An infinite directional light source (like the sun) is used.
- FiniteDirectional A point light source is used.

Light Source

You can also set the Source property to a Point3d object, which controls the location of the light source.

Alpha Blending

The Backdrop class in the Chart control has an Alpha property which employs GDI+, and is used to set the transparency level of each object's backdrop. GDI+ uses 32 bits overall and 8 bits per alpha, red, green, and blue channels respectively to indicate the transparency and color of an object. Like a color channel's levels of color, the alpha channel represents 256 levels of transparency.

The default value of the Alpha property is 255, which represents a fully opaque color. For a fully transparent color, set this value to 0. To blend the color of the object's backdrop with the background color, use a setting between 0 and 255.

In the Chart control, you can use the Color.FromArgb method to set the alpha and color levels for a particular chart element. The following example shows how you can use the method to set the alpha and color values for the chart backdrop.

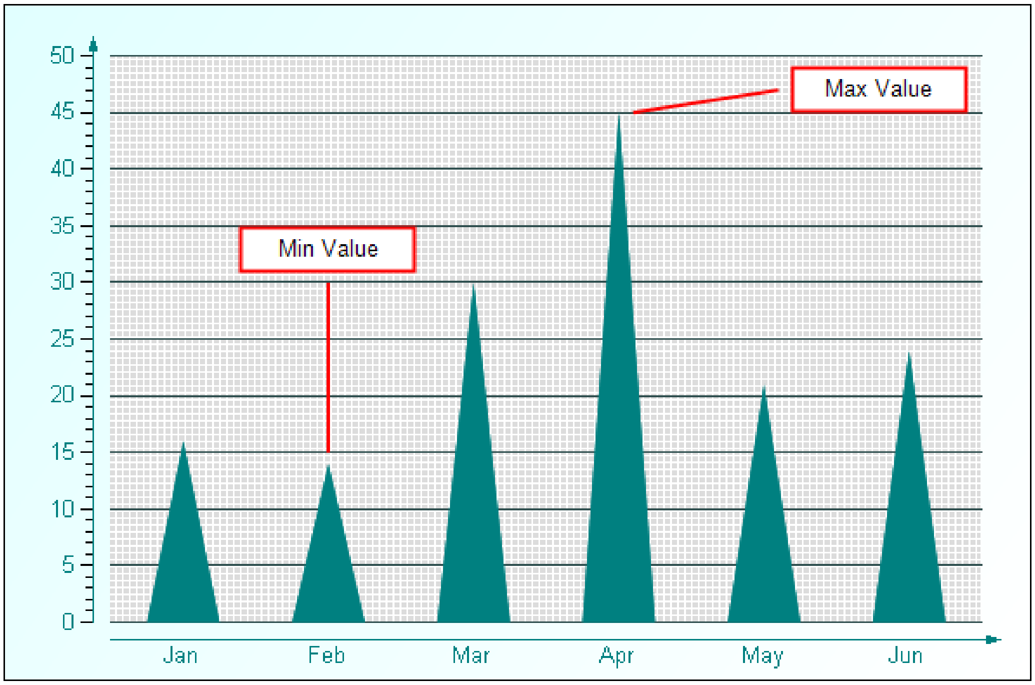
```
// C#

this.ChartControl1.Backdrop = new DataDynamics.ActiveReports.Chart.

BackdropItem(Color.FromArgb(100, 0, 11, 220));
```

Changing the alpha level of a chart element reveals other items that are beneath the object. Because you can set the alpha level for any chart element that supports color, you can create custom effects for any chart. For example, you can use alpha blending to combine background images with a semi-transparent chart backdrop to create a watermark look.

Chart Control Items

Annotations

The Chart control offers a built-in annotation tool to allow you to include floating text bars or images in your charts or call attention to specific items or values in your charts using the line and text bar controls included in the Annotation Collection Editor.

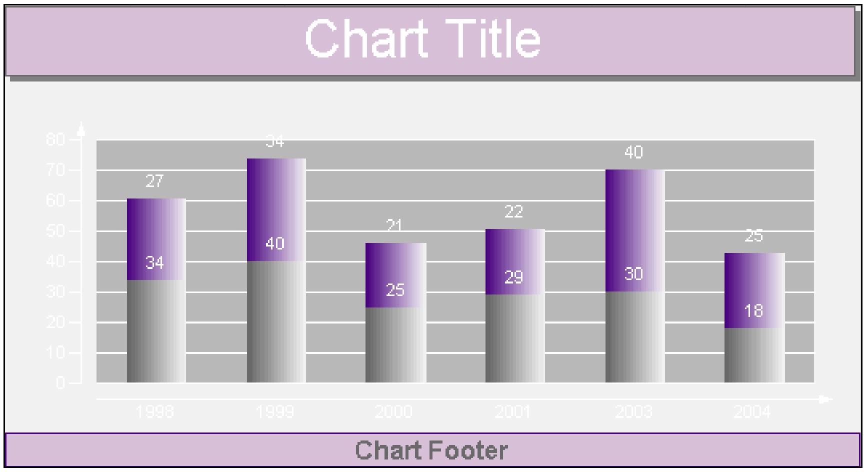


The following properties are important when setting up annotations for your chart:

- Start Point: sets the starting point (X and Y axis values) for an annotation line.
- End Point: sets the end point (X and Y axis values) for an annotation line.
- Anchor Placement: sets the position of the anchor point for the text bar on the chart surface.
- Anchor Point: sets the point (X and Y axis values) where the text bar will be anchored based on the anchor placement selected.

Titles and Footers

The Chart control allows you to add custom titles to your charts. The Titles collection is accessible from the SharpGraph object. With the ability to add as many titles as needed, dock them to any side of a chart area, change all of the font properties, add borders and shadows, make the background look the way you want it, and change the location of the text, you can easily make your titles look the way you want them to look.

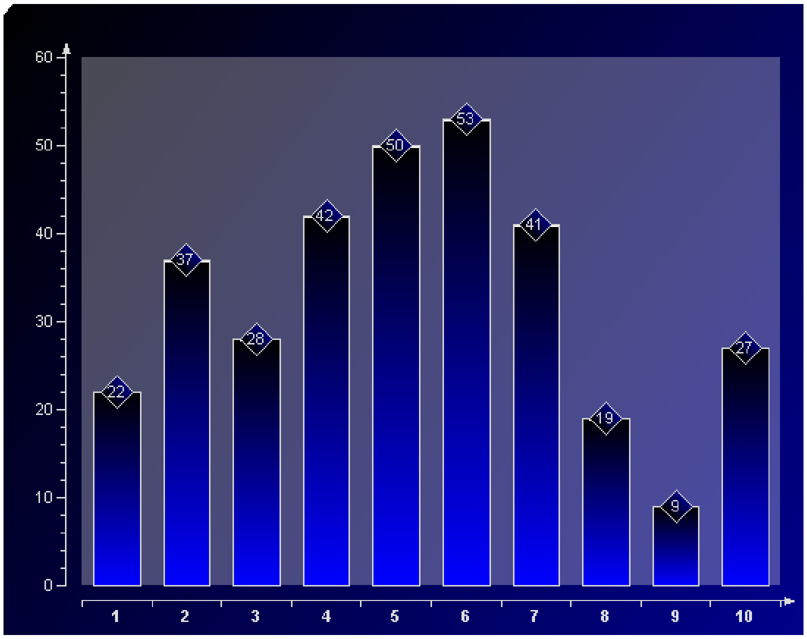


Legends

The Chart control automatically creates a legend item for each series added to a chart at design time and sets the Legend property for each series by default. However, the legend's Visible property must be set to True for the legend to show with the chart. The text for each default legend entry is taken from the Name property on the series. Each Series to be shown in the Legend must have a Name. If the Name property is not set, the Series does not show up in the Legend.

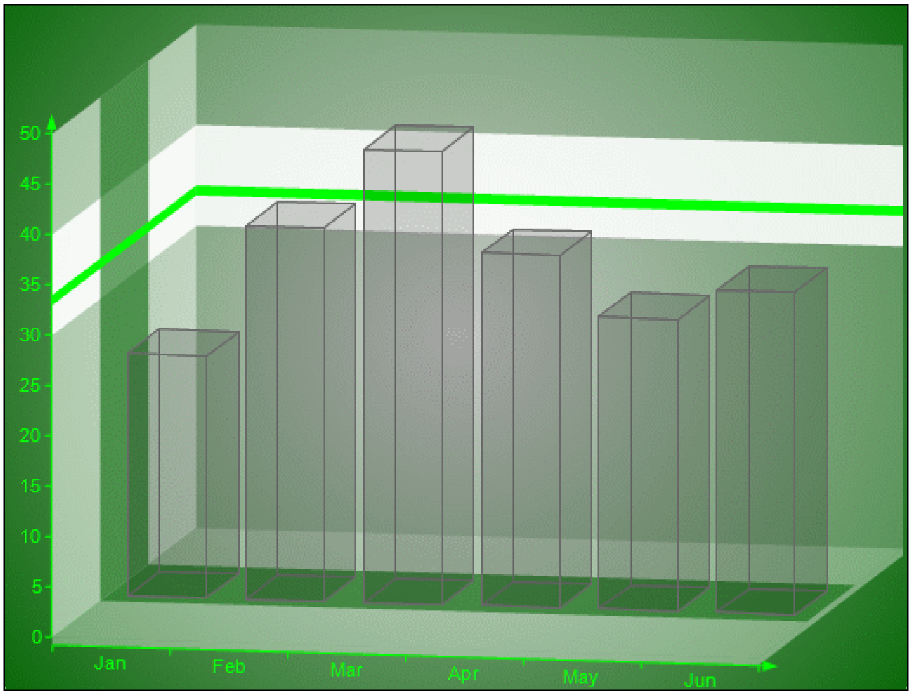
Markers

Markers are used to show specific data series values in a chart.



Constant Lines and Stripes

The Chart control supports constant lines and stripes through the use of the WallRanges collection. It allows you to display horizontal or vertical lines or stripes in a chart to highlight certain areas. For example, you could draw a stripe in a chart to draw attention to a high level in the data or draw a line to show the average value of the data presented.



Important properties

- EndValue--Sets the end value on the primary axis for the wall range.
- StartValue --Sets the start value on the primary axis for the wall range.
- PrimaryAxis--Sets the axis on which the wall range should appear.

Chart Axes and Walls

Standard Axes

The Chart control provides the means to change axis settings at design time or run time. Chart axes make it possible to view and understand the data plotted in a graph.

Axis Types

Most 2D charts contain a numerical axis (AxisY) and a categorical axis (AxisX). 3D charts include another numerical axis (AxisZ). These axes are accessible at run time from the ChartArea object and allow you to control the settings for each, including scaling, labels, and various formatting properties. For any of the scaling or labeling properties you set to show up at run time, you will need to set the Visible property of the axis to True.

Changing Axis Settings

Axis settings can be changed at design time by clicking on a Chart control and using the *Properties* window or at run time in code from the chart's ChartArea object.

Scaling

For normal linear scaling on a numeric axis, you will need to set the Max and Min properties for the axis, which correspond to the numerical values in the chart's data series. You will also need to set the Step property of the MajorTick to show the major numerical unit values. The Step property controls where labels and/or tick marks are shown on the numerical axis.

```
// C#

this.ChartControl1.ChartAreas[0].Axes["AxisY"].Max = 100;

this.ChartControl1.ChartAreas[0].Axes["AxisY"].Min = 0;

this.ChartControl1.ChartAreas[0].Axes["AxisY"].MajorTick.Step = 10;
```

The Chart control also supports logarithmic scaling which allows you to show the vertical spacing between two points that corresponds to the percentage of change between those numbers. You can set your numeric axis to scale logarithmically by setting the IsLogarithmic property on the axis to True and setting the Max and Min properties of the axis.

Labeling

To show labels on an axis, you will need to specify the value for the LabelsGap property, set your LabelsFont properties, and set LabelsVisible to True. These properties can be set in the AxisBase Collection editor, which is accessed at design time by clicking the ellipsis button next to the ChartAreas (Collection) property, then the Axes (Collection) property of the ChartArea.

NOTE: Labels render first, and then the chart fills in the remaining area, so be sure to make the chart large enough if you use angled labels.

You can specify strings to be used for the labels instead of numerical values on an axis by using the Labels collection property at design time or assigning a string array to the Labels property at run time. You can also specify whether you want your axis labels to appear on the outside or inside of the axis line using the LabelsInside property. By default, labels appear outside the axis line.

Secondary Axes

By default, a Chart object includes secondary X and Y axes (AxisX2 and AxisY2). At design time or run time, you can specify a secondary axis to plot data against by setting all of the appropriate properties for AxisX2 or AxisY2, including the Visible property.

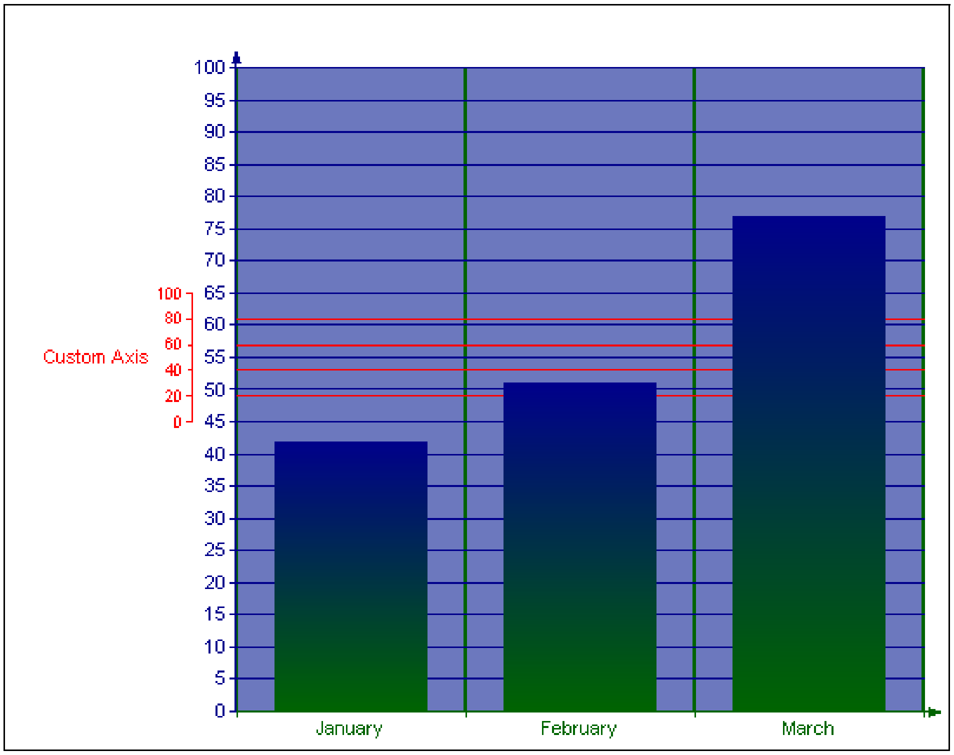
If you want to use two axes to show the same data as it appears on two different scales, you can set the primary axis to show the actual data value scale, for example, and set the secondary axis to show a logarithmic scale.

Custom Axes

The Chart control supports the creation of additional custom axes through the use of the chart's CustomAxes collection. Once a custom axis has been added to the collection, in addition to setting the normal axis properties, you will need to set the following properties:

- Parent - The Parent property allows you to choose the primary or secondary axis on which your custom axis resides.
- PlacementLength - The PlacementLength property allows you to set the length of the custom axis in proportion to the Min and Max property values you have already set for the parent axis.

- PlacementLocation - The PlacementLocation property allows you to set the starting location value for the custom axis to appear in relation to the parent axis.



Gridlines and Tick Marks

Gridlines and tick marks are generally used to help increase the readability of a chart.

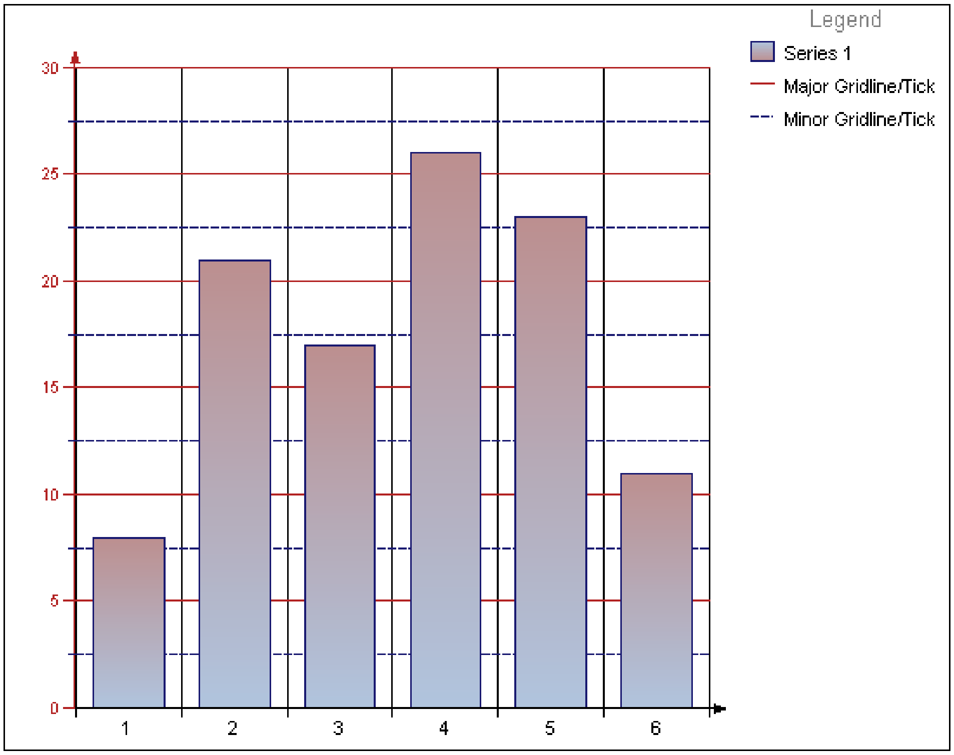
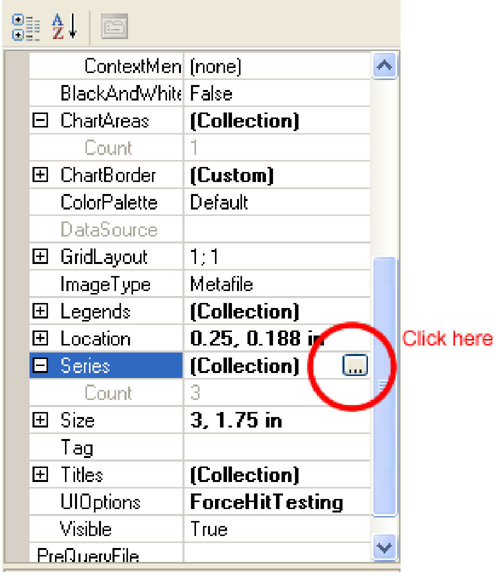


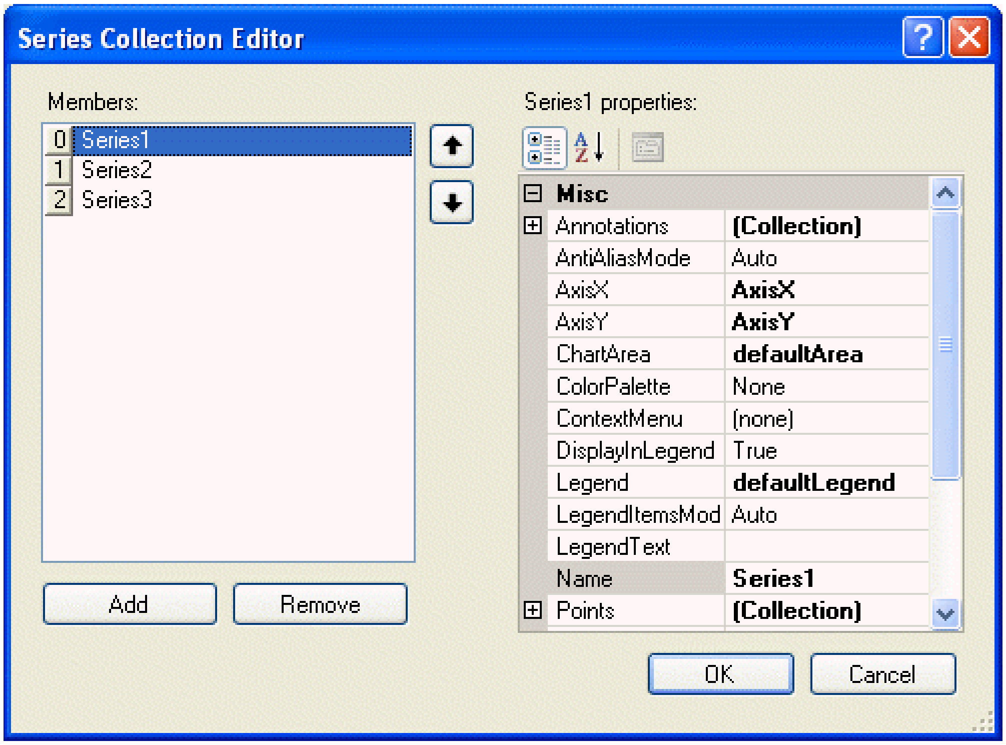
Chart-Specific Properties

Each chart type in the Chart control contains specific properties that apply to it. Set the chart type and chart-specific properties in the *Series Collection Editor* dialog box accessed through the Series property in the property grid and in the *DataPoint Collection* dialog box accessed through the Points property in the *Series* dialog box.



ContextMen	(none)
BlackAndWhit	False
⊟ ChartAreas	**(Collection)**
Count	1
⊞ ChartBorder	**(Custom)**
ColorPalette	Default
DataSource	
⊞ GridLayout	1; 1
ImageType	Metafile
⊞ Legends	**(Collection)**
⊞ Location	**0.25, 0.188 in**
⊟ Series	**(Collection)**
Count	3
⊞ Size	**3, 1.75 in**
Tag	
⊞ Titles	**(Collection)**
UIOptions	**ForceHitTesting**
Visible	True
PreQueryFile	

Click here



Series Collection Editor

Members:

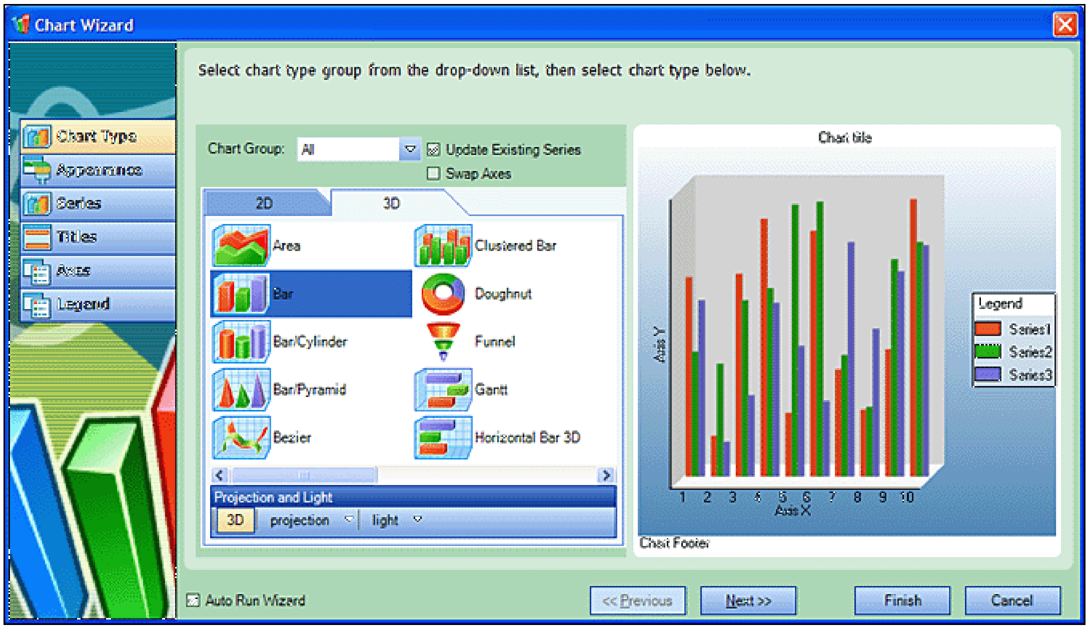
0 Series1
1 Series2
2 Series3

Series1 properties:

⊟ **Misc**	
⊞ Annotations	**(Collection)**
AntiAliasMode	Auto
AxisX	**AxisX**
AxisY	**AxisY**
ChartArea	**defaultArea**
ColorPalette	None
ContextMenu	(none)
DisplayInLegend	True
Legend	**defaultLegend**
LegendItemsMod	Auto
LegendText	
Name	**Series1**
⊞ Points	**(Collection)**

Chart Wizard

The chart control features an easy-to-use wizard. The chart wizard automatically runs when you first add a chart control to a report. If you prefer not to have the wizard run automatically, uncheck the Auto Run Wizard check box at the bottom of the wizard..



Select chart type group from the drop-down list, then select chart type below.

Chart Group: All

☒ Update Existing Series

☐ Swap Axes

Projection and Light: 3D projection light

☐ Auto Run Wizard

Walk-Through: Creating a Report

In this exercise, you will build a report similar to the vulnerability (classic) report, but not as intricate.

Task 1: Build the master report.

1 Click **File** → **New**.

2 On the *Create Report Definition* window, enter the following:

Name: My vulnerability report

Description: Sample report

3 In the Context list, select **Scan**.

4 Select **Exposed in Product**.

5 In the **View Name** list, select **Basic - Server Information**.

6 Click **OK**.

7 Right-click the PageHeader caption and select Delete.

8 Right-click the Detail caption and select **Insert** → **Report Header/Footer**.

9 In the toolbox, drag LinkedSubReportControl into the ReportHeader section.

10 On the *Choose a Report* dialog, expand the Vulnerability (classic) group, select **ScanHeader**, and click **OK**.

11 Position the element and extend it to the right margin.

12 Click the ReportHeader caption.

13 In the Properties grid, set CanShrink = True.

14 Click the Detail caption.

15 In the Properties grid, set CanShrink = True.

Task 2: Add a Link to a Subreport

1 In the toolbox, drag a LinkedSubReportControl into the Detail section.

2 On the *Choose a Report* dialog, expand the Vulnerability (classic) group, select **ServerHeader**, and click **OK**.

3 Position the element and extend it to the right margin.

4 With the ServerHeader selected, in the Properties grid under Associated Fields, click **@ServerID** and select ServerID.

5 Click the **Preview** tab.

6 When prompted to design parameters, select **No**.

7 Select a scan and click **Next**.

8 When prompted to select a report, click **Finish**.

9 Click **File** → **Save**.

Task 3: Create a Subreport

1 Click **File** → **New**.

2 On the *Create Report Definition* window, enter or select the following:

   a For the Name, enter “My vulnerability by server.”

   b For the Description, enter “Sample report.”

3 From the **Context** list, select **Scan**.

4 Clear the **Exposed in Product** check mark.

5 In the **View Name** list, select *Basic - Vulnerability by Session*.

6 Click **OK**.

7 Delete the PageHeader caption (right-click the caption and select **Delete**).

8 In the Properties grid, set CanShrink = True.

9 Right-click the Detail caption and select **Insert** → **Group Header/Footer**.

10 In the Properties grid:

   a Set CanShrink = True.

   b Change the name to GroupServer.

   c For the DataField, select Server.

11 Drag a BookmarkControl to the GroupServer area.

12 In the Properties grid, select BookmarkText and enter the following:

```
{=MainReportName}\{=Server}
```

Task 4: Add a chart to the report

1 Click **Edit** → **Modify/Create Report**.

2 Select **Aggregate - Severity Summary by Server** and click **OK**. This query will be used to generate a chart.

3 Drag a ChartControl onto the design area.

4 On the Chart Wizard, click the **2D** tab and select **Bar**.

5 Click **Finish**.

6 Resize the chart and arrange it to your liking.

7 With the chart selected, go to the Properties grid, click **AssociatedQuery**, and select the query you just added: Aggregate - Severity Summary by Server.

8 Right-click the chart and select Wizard.

9 Select **Series** from the list in the left-hand pane.

10 Assign a series to each severity category: critical, high, medium, low, informational, and best practice.

- a Select **Series1**, and in the Series Properties area and enter “Critical” for the Name.
- b In the Data Binding area, select the Y axis and select **Critical** from the drop-down list.
- c Repeat this process for each series; click **Add New Item** where necessary.

11 Click **Finish**.

12 With the chart selected, go to the Properties grid and click **@ServerID** under AssociatedFields and select VulnerabilityCount.

Task 5: Add a section for the Check ID, Check Severity, and Check Name, and Summary

1 Right-click the Detail caption and select **Insert** → **Group Header/Footer**.

2 Collapse the footer.

3 Click the GroupHeader.

4 In the Properties grid:

- a Change the name to “groupCheck.”
- b Set CanShrink = True
- c For the DataField, select “checkid.”

5 Drag a TextBox to the groupCheck section.

6 In the Properties grid:

- a For Name, enter txtSeverity
- b For DataField, select “checkseverity.”

7 Drag another TextBox into the groupCheck section and place it to the right of the first TextBox.

8 In the Properties grid:

- a Change the name to “txtCheckName.”
- b Set CanShrink = True
- c For the DataField, select “checkname.”

d For ClassName, select Normal Bold.

9 Drag a Label into the area.

10 In the Properties grid:

a Change the name to lblSummary.

b For Text, enter Summary.

11 Drag a RichTextBox onto the canvas; place it below the summary label and extend it to the right.

12 In the Properties grid:

a Change the name to txtSummary.

b For the DataField, select ReportSection_Summary.

13 Drag a BookmarkControl and place it anywhere on the groupCheck canvas

14 On the Properties grid:

a For BookMarkText, enter {=MainReportName}\Checks\{=Checkid}.

b For the Name, enter BookmarkChecks.

Task 6: Add an area for the HTTP Request

1 Right-click on the Detail caption and select **Insert** → **Group Header/Footer**.

2 Collapse the group footer.

3 On the Properties grid:

a Set CanShrink =True.

b For the Name, enter groupRequest.

4 Drag a RichTextBox to the groupRequest canvas. Size it and extend it to the right margin.

5 On the Properties grid:

a Set CanShrink =True.

b For the Name, enter txtRequest.

c For the DataField, select RequestText.

d For TruncateVulnerability, select True.

e For HighlightVulnerability, select True

Task 7: Add an area for the HTTP Response

1 Drag a RichTextBox to the groupRequest canvas. Size it and extend it to the right margin.

2 On the Properties grid:

a Set CanShrink =True.

b For the Name, enter txtResponse.

c For the DataField, select ResponseText.

d For TruncateVulnerability, select True.

e For HighlightVulnerability, select True

Task 8: Populate the Detail section.

1 Drag the bound field “fullURL” to the Detail section.

2 Click the Parameter Designer icon on the toolbar.

3 In the Parameter Designer Canvas area, delete all parameters (click in the area, press Ctrl + a, and then press **Delete**).

4 Click **Save and Close**.

Task 9: Add/Modify the script

1 Click the **Script** tab on the Report Designer.

2 Change the method name “myEventHandler” to “onGroupCheckFormat.”

3 Delete all the script and replace with the following:

```
using System;

using DataDynamics.ActiveReports;

using HP.AppSec.Reporting.ReportScript;

namespace Script.Events

{

    public class MyEventClass

    {

        /*

         * You can declare fields, events and methods just like in c#...

         * in fact this is C#!

         */

         /*

         * Script event handlers, MUST have this method signature

         */

       public void OnGroupCheckFormat(ScriptReportObject report, EventArgs
ea)

        {

                     int nSeverity = (int)report.Fields["checkseverity"];

                     TextBox txtSeverity =
report.CurrentSection.Controls["txtSeverity"] as TextBox;

                     if (nSeverity <= 10)

                     {

                           txtSeverity.Text = "Informational";

                     }

                     else if( 10 < nSeverity && nSeverity <= 25)

                     {

                           txtSeverity.Text = "Low";
                     }
                     else if( 25 < nSeverity && nSeverity <= 50)
                     {
                           txtSeverity.Text = "Medium";
                     }
                     else if( 50 < nSeverity && nSeverity <= 75)
                     {
                           txtSeverity.Text = "High";
                     }
                     else if( 75 <  nSeverity && nSeverity <= 100)
                     {
                           txtSeverity.Text = "Critical";
                     }
        }
    }
}
```

4. After entering the script, click the **Report Events** tab (in the lower right) and select **groupCheck** from the drop-down list.
5. For the Section Format Event, select Script.Events.MyEventClass.onGroupCheckFormat.
6. Save the report.

Task 10: Add a pre-query to the master report

1. Open MyVulnerability report (listed under Custom Reports on the *Open a Report* dialog).
2. Click **Edit** → **Modify/Create Report**.
3. From the **View Name** list, select **PreQuery - Vulnerability.**

   A pre-query improves performance by first determining if any data is available for the report.
4. Drag a LinkedSubReportControl onto the Detail area.
5. From the *Choose a Report* dialog, select My vulnerability by server and click **OK**.
6. Position the control and extend it to the right margin.
7. On the Properties grid:
   a. Under AssociatedFields, click **@serverID** and select serverID.
   b. For PreQueryFile, select PreQuery - Vulnerability.
8. Click **Save**.
9. Click the **Preview** tab.
10. Note and correct any improperly positioned controls, then save your work.

B Policies and Components

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

- **All Checks**: An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the check database. This scan includes all checks that are listed in the compliance reports that are available in HP's Web application and Web services vulnerability assessment products. This includes checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.
- **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.
- **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.
- **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.

- **Application Only**: The Application Only 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.
- **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.

- **Developer**: 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.
- **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 Only**: The Platform Only 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 Only policy in conjunction with the Application Only 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.
- **SOAP**: Most Web services use SOAP (Simple Object Access Protocol) to send XML data between the Web service and the client Web application making the information request. Use the SOAP policy to determine the security vulnerabilities of your Web service. Applying the SOAP policy against a Web site is not recommended. For more information on auditing Web services, see Web Services.
- **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.
- **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.

Policy Components

A policy is a collection of audit engines and inspection agents that WebInspect uses when scanning or crawling your Web application. 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

Audit Engines

WebInspect uses the following audit engines.

- **Adaptive Agents**: Certain vulnerabilities require a large amount of logic when checking for them. For example, a buffer overflow JRun check might cause a server to crash if conducted through a vulnerability database. Instead, an adaptive agent with the proper amount of logic can be written to prevent such a problem. With this smart approach, WebInspect continuously applies appropriate assessment resources that adapt to the specification application environment.
- **Comment Checks**: The comment audit examines each session for filenames and/or URLs in comments. Upon finding a filename or URL, the audit will check to see if the file or URL exists.
- **Cookie Injection**: Cookies and headers are just as vulnerable to injection attacks as text fields in forms. Cookie injection occurs when unvalidated data is sent by a user's browser as part of a cookie. The Cookie Injection audit engine attempts certain traditional parameter injection attacks against different cookie values.
- **Cross-Site Scripting**: This engine runs the cross-site scripting parameter injections attacks. Cross-site scripting is caused by insufficient filtering of client-supplied data that is returned to Web users by the Web application.
- **Directory Enumeration**: Directory enumeration finds all directory paths and possibilities on the application server, including hidden directories that could possibly contain sensitive information. This helps WebInspect create a full and accurate map of the targeted site.
- **File Extension**: Network administrators and developers often leave backup files and scripts on the Web server. These files commonly contain information that can be used to breach a site's security. Extension checking involves replacing extensions on files, and then looking for older or backup versions stored on the site. For example, an attacker who finds hi.asp might search for hi.old and hi.back, and retrieve the script's source code. Data extension checking involves adding file extensions to find old renamed files left on the server. For example, an attacker might find hi.asp, and then search for hi.asp.bak or hi.asp.old. WebInspect will attempt to locate all files left on your server that could be used by an attacker.
- **File Prefix**: Network administrators and developers often leave backup files and scripts on the Web server. These files commonly contain information that can be used to breach a site's security. Prefix checking involves affixing a value to file names, and then looking for older or backup versions stored on the site. For example, an attacker who finds hi.asp might search for *copy of hi.asp* and retrieve the script's source code.

- **Fixed Checks**: This audit performs checks for files with known vulnerabilities. This audit is the same as the ABS Checks audit, with the exception being that the Fixed Checks audit does not probe the directory structure before sending the attacks.
- **Header Injection**: Cookies and headers are just as vulnerable to injection attacks as text fields in forms. HTTP header injection occurs when HTTP headers are dynamically generated with user input that includes malicious content. The Header Injection audit engine attempts certain traditional parameter injection attacks against different types of HTTP headers.
- **Keyword Search**: Information disclosure attacks focus on ways of getting a Web site to reveal system-specific information or confidential data, including user data, that should not be exposed to anonymous users. The Keyword Search audit engine examines every response from the Web server for information, such as error messages, directory listings, credit card numbers, etc., that is not properly protected by the Web site.
- **Known Vulnerabilities**: This audit engine examines your Web site for files with known vulnerabilities. The audit will perform a probe of directories known to contain these files and then send requests based on any discovered directories.
- **Local File Inclusion**: Local file reading/inclusion vulnerabilities exist when an attacker can influence the application to read (presumably arbitrary) files specified by the attacker. The engine submits to the Web application various values that contain various combinations of relative and absolute file names for specific known files. The engine considers the attack a success if the contents of those files are displayed.
- **Logic Checks**: This audit performs checks based on previously discovered vulnerabilities.
- **Postdata Injection, Postdata Sequence**: Since manipulating a query string is as easy as typing text in the address bar of a browser, many Web applications rely on the POST method coupled with the use of forms (rather than GET) to pass data between pages. Since browsers normally don't display POST data, some programmers are lulled into thinking that it is difficult or impossible to change the data, when in fact the opposite is true. WebInspect will determine your application's susceptibility to attacks that rely on the POST method of parameter manipulation.
- **Query Injection, Query Sequence**: Web applications often use query strings as a simple method of passing data from the client to the server. Query strings are a way to add data calls to a hyperlink, and then retrieve that information on the linked page when it is displayed. By manipulating query strings, an attacker can easily steal information from a database, learn details about the architecture of your Web application, or possibly execute commands on your Web server.

  When conducting an audit, WebInspect implements advanced query string manipulation to ascertain the feasibility of command execution on your server(s), and determines the vulnerability of your Web applications to query string manipulation.
- **Request Inspect**: During the crawl of a Web application to map its internal structure, the Request Inspect engine applies the regular expressions that are associated with checks to the requests being sent.
- **Request Modification**: Several types of attacks involve malformed requests that result in a failed response from the Web server. The Request Modification engine generates requests that are derived from other requests that match a pattern, and then evaluates the response to determine if these types of attacks are possible.

- **Server Side Include**: During the course of normal operations, many Web applications will accept a full URL as an expected and returned parameter value. This audit engine will manipulate that process and determine if an attacker could exploit any vulnerabilities within the application by including commands and other functions within the URL accepted by the application.
- **Site Search**: This can be considered the information-gathering stage, employing the same tactics an intruder would use to learn as much as possible about your Web application before launching an attack. Site search is used to locate resources such as documents, applications and directories on the server that are not intended to be viewed by Web users. Disclosure of such resources can reveal confidential data, information about internal server and application configurations and settings, administrative access to the site, and application source code.
- **SOAP Assessment**: Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services utilize SOAP (Simple Object Access Protocol) to send XML data between the Web service and the client Web application making the information request. SOAP assessment involves checking for security vulnerabilities inherent within that transport mechanism.
- **SQL Injection**: SQL Injection is an attack in which hackers use SQL statements via an Internet browser to extract, add, or modify data, create a denial of service, bypass authentication, or execute remote commands. The SQL Injection engine detects the following attacks:
- Injection through user input, such as malicious strings in Web forms
- Injection through cookies, such as modified cookie fields that contain attack strings
- Injection through server variables, such as headers that are manipulated to contain attack strings

Audit Options

WebInspect uses the following audit options.

- **Robots.txt Parser**: This engine parses any robots.txt files found within the scan for links to add to the WebInspect crawler engine.
- **Ws_ftp.log Parser**: This engine parses any Ws_ftp.log files it finds and will add links to the site directory tree.

Directory Enumeration

This group of agents, used mainly by the Directory Enumeration engine, searches the site's tree structure for commonly occurring directories. Individual checks are grouped alphabetically from A (which begins with the search for a directory named Accounting) to Z (which ends with the search for a directory named Zips). This group also includes checks for other types of commonly occurring directories, such as those associated with Microsoft FrontPage and Microsoft Internet Information Server log files (W3SVCnn).

Unknown Application Testing

This group of agents conducts a wide variety of tests and probes, searching for files that may contain information that a hacker might find useful. The following are among the hundreds of vulnerabilities detected by this group:

- Remote execution on the system is possible.
- Files exist that may contain password or administrative information.
- Backup files containing source code may be retrieved.
- Shell files exist that would allow an attacker to execute commands on the Web server.
- Statistics and log files exist that may contain sensitive information.
- Cross-site scripting is possible
- Basic authorization can be bypassed.
- Parameter manipulation is possible
- Files can be uploaded

For detailed information about all the possible agents, open the Policy Manager, expand the Unknown Application Testing node, and click on any agent.

Web Application Servers

This group of agents looks for known vulnerabilities associated with Web application servers. It also determines if known flaws in certain scripting languages can be exploited on the target system. For detailed information about all the possible agents, open the Policy Manager, expand the Web Application Servers node, and click on any agent.

Web Applications

This group of agents looks for known vulnerabilities associated with hundreds of Web applications. They are categorized as follows:

- Big Brother Network Monitor
- Citrix
- Content Management/Weblogs (which includes phpWebSite, Basit, Cafelog b2, RSA ClearTrust, osCommerce and others)
- e107
- FrontPage
- Microsoft Terminal Services
- Minor (a large collection of individual agents ranging from A-1 Stats to zml.cgi)
- PHP-Nuke
- Web Connection
- WebTrends
- WebMail
- Xerox Docushare

For detailed information about all the possible agents, open the Policy Manager, expand the Web Applications node, and click on any agent.

Web Servers

This group of agents looks for known vulnerabilities associated with the following Web servers:

- Apache
- IIS
- Lotus Domino
- Minor (a collection of servers including ATPhttpd, 4D, Abyss, Alibaba, BadBlue, and others)
- Netscape/iPlanet
- Novell
- Secure IIS
- Sun
- Website Pro
- WebSphere Proxy
- Zeus

For detailed information about all the possible agents, open the Policy Manager, expand the Web Servers node, and click on any agent.

Custom Checks

A custom check is a user-defined probe for a specific vulnerability that the standard WebInspect repertoire does not address. Use the Policy Manager to create custom checks and integrate them into your policies. See Creating a Custom Check on page 143 for more information.

Index