Assessment Management Platform QuickStart Guide



The Assessment Management Platform (AMP) is a distributed network of HP scanners (WebInspect, DevInspect, or QAInspect) controlled by a system manager with a centralized database.

Enterprise users in various locations can control any number of HP devices scanning Web applications or Web services. The resulting risk assessment data is gathered in a central SQL database to provide advanced reporting and trending capabilities.

Configuration Requirements

Before installing AMP 9.10, make sure that your system meets the following minimum requirements:

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

AMP Server

- 4 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, 7.0, or 7.5
- Windows Server 2003 SP2 or 2008 SP2 or 2008 R2

AMP Console/Client

- 1 GB of memory
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP Professional SP3 32-bit or Windows Server 2003 SP2 32/64-bit or Windows Vista SP2 32-/64-bit or Windows 7 32-/64-bit or Windows Server 2008 SP2 32-/64-bit
- Microsoft SQL Server Express Edition 2005 SP3 or 2008 SP2 (required only if you want to edit policies, compliance templates, or audit inputs)
- Microsoft Silverlight Runtime v3 (required only if you want to use the Scan Linkage Analyzer and Attachments)

AMP Sensor (WebInspect 9.10)

- 2 GB of RAM
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP Professional SP3 32-bit or Windows Server 2003 Standard SP2 32-bit or Windows Vista SP2 32-/ 64-bit or Windows 7 32-/64-bit or Windows Server 2008 SP2 or R2 32-/64-bit
- Microsoft SQL Server Express Edition 2005 SP3 or SQL Server 2005 SP4 or SQL Server Express 2008 SP2 or SQL Server 2008 SP2 or R2
- 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
- 2.5 GHz processor or better
- Microsoft SQL Server Standard Edition 2005 SP4 or 2008 SP2 or R2
- Windows Server 2003 SP2 32-/64-bit or Windows Server 2008 SP2 or R2 64-bit

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 Server.

AMP Components

AMP 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 designed specifically for non-administrative functions)
- AMP Quality Center service (if integrating with HP Quality Center)
- 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 instructions exclusively from the configurable connection to an AMP Manager.

AMP Software Installation Apply all available service pack upgrades and patches to all operating systems. 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

plates used by clients.

•

Manager.

Typical installations will have one SQL server, one or more consoles, and multiple sensors. These components can be distributed across your network in any way you like, but you must configure at least one of each. The AMP console connects to the AMP server via HTTP/S. This connection must be reachable by the AMP console and the AMP sensor.

Client - A client is any HP scanner (WebInspect or

QAInspect) 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 tem-

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.

When installing components on different machines, begin with the one on which the server will be installed. **Install the server on one machine only**.

Note: Before installing the sensor or the manager, make sure the Microsoft Administrative Tools/Services window is not open.

Server/Manager Installation

- 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.
- On the Activate AMP License window, enter the Activation ID sent to you by HP. If using a proxy server, select Use Proxy Server and provide the requested information.
- 9. Click Next.

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

10. Click Next.

This form is submitted to an HP server, which accesses a corporate database to retrieve and download license information.

- When the AMP License Information window appears, click Next.
- 12. 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 a previous version of AMP, you must have at least "read access" to the database. If you are installing AMP 9 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).
- 13. Click Next.
- 14. On the *Database Selection* window, 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 8 database, select **Use** existing database and select one from the list. You must have owner privileges for that database.
- 15. Click Next.
- 16. For an existing database only, the AMP Database Upgrade window appears. Enter a name for the new database and click **Next**.
- On the Setup AMP Manager WebService window, enter the root Web site and the name of the IIS virtual directory. If you are upgrading, do not choose the same IIS Virtual Directory name used previously.

If you select **Require Secure Channel (SSL)**, add and/or select an SSL certificate. Note: SSL is highly recommended.

These entries create the URLs for the following components.

- 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.
- 20. Click Next.

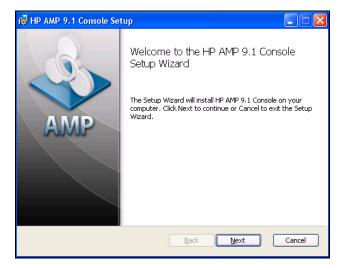
- 21. On the Setup AMP Database User window, specify how the AMP Manager should connect to the AMP database.
 - Windows Authentication The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user 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.
- 24. When the program displays the initialization results, click **Next**.
- 25. On the *Sensor Users* window, click **Add** and enter the user accounts that will be associated with the sensors (WebInspect installations).
- 26. Click Next.
- 27. When installation is complete, the following window appears. Click **Finish**.

Console Installation

1. Start the installation program.



- 2. On the Welcome page, click **Next**.
- Review the license agreement. If you accept, click Next; otherwise click Cancel.

- 4. Select the folder into which you want to install the software and click **Next**.
- 5. Click Next.
- 6. When the process is complete, click **Finish**.

WebInspect (Sensor) Installation

- 1. Start the installation program.
- 2. On the Welcome page, click Next.
- 3. Review the license agreement. If you accept, click **Next**; otherwise click **Cancel**.
- 4. Select the folder into which you want to install the software and click **Next**.

The WebInspect Setup dialog appears.

- 5. Select Configure WebInspect as an AMP Sensor.
- 6. On the AMP Sensor Configuration window, specify 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. See above.
- 8. Click Next.
- 9. Click Install.
- 10. When the process is complete, click **Finish**.

Quality Center Service Installation

If you plan to integrate AMP with an HP Quality Center installation (which would allow you to submit vulnerabilities to Quality Center as defects), you must install the Quality Center service. The AMP QC service must be installed on a machine that also has the Quality Center client application installed.

Note: Beginning with version 11, HP Quality Center has been renamed HP Application Lifecycle Management (ALM). If you are integrating ALM with AMP, you must also install the Connectivity Add-in as part of the ALM installation; select Add-Ins Page from the ALM main window.

AMP QC Service installation can be launched from AMP Server installation wizard.

Configuration information is maintained in a file named QualityCenterService.conf, which is stored on the machine on which the service is installed. The default location is C:\Documents and Settings\All Users\Application Data\HP\AMP\8.0\QualityCenterService.

Refer to the AMP user Guide for configuration information.

Upgrade Considerations

Observe the following guidelines if you are upgrading from AMP 8.1.

- You cannot upgrade to AMP 9 from versions previous to 8.10.
- AMP 9 does not support versions of WebInspect prior to 7.0 and requires WebInspect 8.0, 8.10, 9.0 or 9.10 to support AMP's new scan visualization feature.
- Make a back-up copy of your database.
- The AMP 9 database must be installed on the same database server used by AMP 8.10.
- 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 8.10 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.

Start the AMP Console

- At a machine on which you have installed the AMP Console, click Start > All Programs > HP > HP AMP 9.1 Console > AMP 9.1 Console.
- 2. On the **Log On** tab, select or enter the URL of the AMP manager.
- 3. Select one of the following logon options:
 - To log on using your Windows user account, select Log on as the current Windows user.
 - 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. To use a proxy server to reach the AMP manager, click the **Proxy** tab and select one of the following:
 - Use the Internet Explorer proxy (to use the proxy server specified in Tools/Internet Options/Connections/LAN Settings).
 - Use the proxy below, and then provide the requested information.
- 5. 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.

Create Organizations and Projects

Administrative authority within AMP is distributed across three levels: system, organization, and project. Each level has at least one administrator. The person who installed the AMP software is, by default, the system administrator. If this person does not intend to perform the initial configuration, he must explicitly designate another user as administrator for the default organization and default project.

Note: If you are upgrading from AMP 8.0 and want to migrate your database to AMP 9.10, the AMP Initialize program ports all your sites, roles, and objects to the AMP 9.10 default project.

- 1. Click the Administration group.
- 2. Click the Roles and Permissions shortcut.
- 3. Select AMP System in the Hierarchy pane.
- 4. Click Action and select Add Organization.

Every system must have at least one organization.

- 5. On the *Create Organization* dialog, type a name for the organization and click **OK**.
- 6. In the Hierarchy pane, select the organization you just added.
- 7. Click Action and select Add Project.

Each organization can have one or more projects.

- 8. On the Create Project dialog:
 - a. Type a name for the project in the Name box.
 - b. Select Allow access to all of the organization's current resources.
 - c. In the Scan Permissions group, click Add.
 - d. Type a host name (wild cards allowed), IP address, or IP address range, and click **OK**.
 - e. Click **OK** to close the *Create Project* dialog.

Notice that users who create an organization or project are automatically assigned as administrators of that organization or project.

Select Organization Resources

You can specify which resources are available to an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them.

1. In the Project Hierarchy pane, select the organization you created.

- 2. Click the **Resources** tab.
- 3. Select an item in the Object Type list.

All instances of those object types are displayed in the **Available** column.

4. Click is to move all object types to the **Allowed** column.

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

5. Repeat Steps 3-4 until all resources are in the **Allowed** column.

Define Project Roles

A role is a named collection of permissions. You can allow other users to access the AMP console and perform functions you specify by assigning them to a role, based on their Windows user accounts.

- 1. In the Project Hierarchy pane, select the project you created.
- 2. Click the Roles tab.
- 3. Click Add.
- 4. On the *New Role* dialog:
 - a. Type "Tester" in the Name box.
 - b. From the **Default** list, select the permission that will be assigned, by default, to each activity associated with this role. For this demonstration, click **Allowed**.
 - c. Click **OK**.
- 5. In the Permissions area, expand the nodes to view the activities associated with each category. You can change permission for an individual activity by clicking "Allowed" and then clicking the associated drop-down arrow.

Assign Users to Roles

Note: If you are upgrading to AMP 9.10, the installation program assigns your users to the same roles enumerated for 8.0. If you are upgrading with a database migrated from another domain, users will appear in Roles as <unknown>.

- 1. Select "Tester" from the Role name list.
- 2. Click Add (to the right of the Group or user names list).
- 3. On the Select Users or Groups dialog, select a domain or work group in the **From this location** list.
- 4. In the text box below, type a Windows account name.
- 5. To verify the name, click Check Names.
- 6. Click **OK**.

Select Project Resources

Note: If you are upgrading from AMP 8.0, the installation program automatically assigns all resources to the AMP 9.10 default project.

You can specify which resources are available to projects within an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them. Of those 10 available, you might choose to allow only 5 to be used in your project.

- 1. Click the **Resources** tab.
- 2. Select an item in the Object Type list.

All object types permitted by the organization to be used by the project are displayed in the **Available** column.

 Click is to move all object types to the Allowed column.

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

Start a Scan

- 1. On the AMP console toolbar, click **Web Console**.
- 2. If necessary, click Continue to this website.
- 3. On the AMP Welcome page, click Log On.
- 4. Enter your credentials and click OK.
- 5. On the AMP Web Console navigation pane, click **New Scan**.

-	Internet Explorer provided by Yahoo!	
🗲 🕞 💌 🔝 https://ars2008.	spidynamics.com A/P/WebConsole/ConfigureScan.aspx 🛛 👻 😵 Certificate Error 🔤 😽 🗙	Google
Favorites Configure Scan		
		Logged in as: SPI\David.Thacke
🏝 AMP [™]	Sites > Configure Scan	🔒 Log Off 🥝 He
	and a compare scan	
imple Scan (Switch to A	dvanced)	
impre sean ((switch to a	uvanceu)	
Scan Template		
Use Scan Template:	«None»	~
Create custom Scan from	1 Template	
Scan		
Scan Name*:		
Site		
Site Name*:		
	rt of a site name or URL to filter the site list.	
New Site		
Assessment		
Name:		~
	Optionally select an "In Progress" assessment for the selected site.	
	······	
Description:		
Description:		
New Assessment		

- 6. Provide the requested information. For detailed assistance, click **HeIp**.
- 7. After supplying all options, click Scan Now.

Assessment Management Platform Using Assessments



An assessment is a virtual workspace for your scans and vulnerability information, allowing you to bring together all the results of your web application investigation into one centralized location. Within an assessment, you can combine data from multiple scans, remove duplicate vulnerabilities, add manually found vulnerabilities, and attach documentation such as notes and screenshots. This new concept in AMP v.9 shifts the Quality Assurance focus from individual scans to a repository of findings that are accumulated during the entire testing phase and throughout the life cycle development process.

Correlation between Scans in an Assessment

AMP 9.10 can compare the results of several dynamic scans and determine which vulnerabilities are actually multiple occurrences of the same issue. It performs this correlation by comparing the location of the vulnerability (URL, parameters, etc.), the nature of the vulnerability (cross-site scripting, SQL injection, etc.) and other attributes. This correlation occurs automatically when a scan is added to an assessment. Matched vulnerabilities are grouped into a "finding."

Create an Assessment

- 1 In the Filtered Views group on the navigation pane, click Sites.
- 2 Select a site that has multiple scans.
- 3 Click the drop-down arrow next to the site name and select Add an Assessment.
- 4 Enter an assessment name (such as "Second Quarter") and click Finish.

Add Scans to the Assessment

- 1 On the Assessment Details form, click the **Scans** tab and click **Add**.
- 2 Select two or more scans. In this example, two scans were added to the assessment. Both were conducted against the same site, but one scan used the Quick Scan policy and the other used the All Checks policy (which is more thorough and should uncover additional vulnerabilities).

https://ars2008.	pidynamics.c	MID Web Concolo Maconsmooth						
		Mightine / Web Console / Assessment			2905ea-e8c0 💌 😵 Certi	ficate Error 🛛 😽 🔀	Google	<mark>۶</mark> -
View Favorites I	ools <u>H</u> elp							
S Assessment Del	ails							
TM							Logged in as	: SPI\David.Thacker
	Assessment	s > Assessment Details				🔒 Log Off 🎟 Optio	ns 🔻 Site Filters 🕌	Resources 🥝 Help
🕈 Create From Exi	sting 🗹 Re	name 👼 Report 🗹 Change S	itatus 👻 💷 /	Archive				8
: Second Q		Start Date:	2/4/2011					
In Progres		Completed Date:						
s: All Check	, Quick	Site:	Zero Test					
Add 🗱 Remove 🕸		-						OF
Name	±	Scan URL	Status	Policy	Created	Started	Completed	App Version
II checks	http	//zero.webappsecurity.com/	Complete	All Checks	2/4/2011 9:28:30 AM	2/4/2011 9:28:57 AM	2/4/2011 9:41:25 AM	9.0.301.0
Quick Scan	http	//zero.webappsecurity.com/	Complete	Quick	2/4/2011 9:29:34 AM	2/4/2011 9:29:51 AM	2/4/2011 9:32:01 AM	9.0.301.0
		T	J					3
1	Create From Exc Create From Exc Second Q In Progress All Checks 1296 Comparison Com	Create From Existing Research Create From Existing Research In Progress Standing International 12% International Internat	Assessments > Assessment Details Create From Existing Assessments > Assessment Details Create From Existing Assessments > Assessment Details Completed Date: In Progress Completed Date:	A Seessments > Assessment Details Create From Existing Rename Report Completed Date: V/A Second Quarter Start Date: 2/4/2011 In Progress Completed Date: V/A start Date: 2/4/2011 In Progress Completed Date: V/A In Progress	Assessments > Assessment Details Create From Existing Rename Report Change Status Create From Existing Rename Report Completed Date: N/A Second Quarter Start Date: 2/4/2011 In Progress Completed Date: N/A Second Quarter Start Date: 2/4/2011 Second Quarter Start Date: 2/4/2011 Second Quarter Start Date: 2/4/2011 Second Quarter Start Date: 2/4/2011 Start Start Start Date: 2/4/2011 Start Start Policy Complete Al Checks	Model Total Create From Existing Rename Report Change Status	Create From Existing Repart Completed Date: ViA Second Quarter Second Quarter	Logged in as Log Off III Options I Site Filters & Create From Existing I Rename III Report I Change Status I Start Date: 2/4/2011 In Progress Completed Date: N/A 322 It In Progress Completed Date: N/A 1226 It 0 It 32 63 62 228 It icense: 2 2 Finding III Generate Report III Generate Report III Generate Report III Generate Report III Secure IIII Secure III Secure IIII Secure IIII Secure IIII Secure IIII Secure IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

3 Click the **Findings** tab.

When assessments are updated by adding scans, AMP automatically correlates the scan results into findings, as depicted in the following illustration.

🔁 🕤 🔻 🔝 https:		spidynamics.com		entDetails.aspxi 💌 😵 Certificate Error	🔸 🗙 🛃 Google		ب
File Edit View Far	vorites 1	ools Help					
🍃 Favorites 👘 💽 Asse	essment De	tails					
						Logged in as: S	SPI\David.Thacker
🌯 AM	1P [™]	Dashboard >	Assessment Details	🔒 Log	Off 🎟 Options 🔻 S	site Filters 🗱 Re	esources 🥹 Helj
X Delete 💠 Create	From Ex	isting 🗹 Rena	ime 📕 Report 🗹 Chang	e Status 👻 🂐 Archive			8
Assessment:	Second C)uarter	Start Date:	2/4/2011			
Status:	In Progre	ss	Completed Date:	N/A			
Scan Policies:	All Check	s, Quick	Site:	Zero Test Site			
Risk Score:	1296	😱 110 🦲 1:	39 🦲 8 🦲 69 🛃 28	11			
Number of Scans:	2		Reports 🛛 🥠 Tags 🗍 Prop	·			
Number of Scans:	2 dings 👔 Propertie	Scans 💽 I es 🗣 Send To	Reports 🛛 🤣 Tags 🗍 Prop 👻 🥙 Tags 👻 🄗 Manua	·	Merge Findings		Đ
Number of Scans:	2 dings 👔 Propertie	Scans 💽 I es 🗣 Send To	Reports Ø	erties 🏾 🤐 QC Defects al Findings 👻 Show Ignored 🕞	Merge Findings Severity	Contributing Scans	Contributing Vulns
Number of Scans: Summary Finding Action States (264) Critical (44)	2 dings 👔 Propertie	Scans ∑ I es □→ Send To 1 of 4 First	Reports 💽 Tags Prop Tags 🗨 Hanus Previous 1 2 3 4 Next Check Name	al Findings V Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com	Severity n:80/pfi	Contributing Scans	
Number of Scans: Summary ← Export ← Finding ndings (264) ← Critical (44) ← High (121)	2 dings 👔 Propertie	Scans Scans I	Reports Tags Prop Tags Tags Annual Previous 1 2 3 4 Next Check Name Admin Section Must Requ	al Findings V Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com dre Au http://zero.webappsecurity.com	Severity h:80/pfi E Best Practice h:80/ad High	-	Contributing Vulns
Number of Scans: Stypert Finding (264) Critical (44) Critical (44) Medium (7) Comparison (7) Comparison (7)	2 dings	Scans Signal s D-> Send To 1 of 4 First Check ID T 10987	Reports Tags Prop Tags Tags Annual Previous 1 2 3 4 Next Check Name Admin Section Must Requ	al Findings V Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com	Severity h:80/pfi E Best Practice h:80/ad High	2	Contributing Vulns
Number of Scans:	2 dings	Scans ∑ Scans ∑ Send To 1 of 4 First Check ID ▼ 10987 ▼ 4721	Reports Tags Prop Tags Tags Annual Previous 1 2 3 4 Next Check Name Admin Section Must Requ	Al Findings V Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com ire Au http://zero.webappsecurity.com guratichttp://zero.webappsecurity.com	Severity 180/pfi Best Practice 180/ad High 180/ad Low	2	Contributing Vulns
Number of Scans: I Summary Image: Finding Image: Product of Scans: Image: Product of Scanse ndings Image: Product of Scanse (264) Image: Product of Scanse Image: Product of Scanse Image: Product of Scanse	2 dings	Scans ∑ I as D→ Send To Send To 1 of 4 I First Check ID ∨ 10987 4721 ∨ 2364	Reports Tags Prop 	Al Findings V Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com irre Au http://zero.webappsecurity.com guratichttp://zero.webappsecurity.com ak)	Severity 1:80/pf 1:80/ad → High 1:80/ad → Low 1:80/log → High	2 2 2 2	Contributing Vulns
Number of Scans: (I) Summary	2 dings	Scans Image: Imag	Reports Tags Prop • Tags • Manue Previous 1 2 3 4 Next Neck Name Admin Section Must Requ Admin Section Must Requ Admin Section Must Requ Admin Section Must Requ Admin Section Must Requ Admin Section Must Requ	Al Findings V Show Ignored Al Findings Show Ignored Last Selected 0 of 101 Location http://zero.webappsecurity.com uratic.http://zero.webappsecurity.com guratic.http://zero.webappsecurity.com ak) http://zero.webappsecurity.com	Severity Severity Severity Sest Practice High Odd Odd	2 2 2 2 2	Contributing Vulns Contributing
Number of Scans:	2 dings	Scans Image: Control of a line First 10f4 First Check ID 10987 4721 2364 708 708 208	Reports Tags Prop Tags Tags Manue Previous 1 2 3 4 Next Check Name Admin Section Must Requ ADOVBS Database Config Backup File (Appended .b Backup File (Appended .b	Al Findings C Defects al Findings Show Ignored t Last Selected 0 of 101 Location http://zero.webapsecurity.com guratichttp://zero.webapsecurity.com bak) http://zero.webapsecurity.com bak) http://zero.webapsecurity.com	Severity 180/pf 2 Best Practice 180/ad High 180/ad Low 180/ad High	2 2 2 2 2 2	Contributing Vulns Contributing
Number of Scans: ⓐ Summary ⓐ Finding ⓑ Export ④ Finding hdings ⑤ € ⓒ Crítical (44) ⓒ High (121) ⓒ High (121) ⓒ High (121) ⓒ Gritical (44) ⓒ Gritical (44) ⓒ Best Practice (25 ⓒ Info (6) (101) ⓒ Crítical (66)	2 dings Propertie Page	Scans Image: Signal and the second sec	Reports Tags Prop Tags Manue Previous 1 2 3 4 Next Check Name Admin Section Must Requ ADOVBS Database Config Backup File (Appended Jb Backup File (Appended Bb) Backup File (Appended Bb) Backup File (Appended Bb)	Al Findings C Defects al Findings Show Ignored t Last Selected 0 of 101 Location http://zero.webapsecurity.com guratichttp://zero.webapsecurity.com bak) http://zero.webapsecurity.com bak) http://zero.webapsecurity.com	Severity 180/pf 2 Best Practice 180/ad High 180/ad Low 180/ad High	2 2 2 2 2 2 2 2 2	Contributing Yulns Contributing

The findings in the left column are grouped by contributing scans. Notice that both scans found 66 critical vulnerabilities and one scan found an additional 44 critical vulnerabilities. The Risk Score shows that the assessment contains 110 unique critical vulnerabilities, reflecting that correlation has eliminated the 66 duplicates.



The **Summary** tab on the Assessment Details form also illustrates successful correlation. The dotted bar on the "Finding to Severity" chart represents the total uncorrelated vulnerabilities as compared with the solid bar representing correlated (or unique) vulnerabilities.

Correlation across Assessments

The following example illustrates how false positives can be carried over from one assessment to the next without any user intervention. It also illustrates AMP's new "alias" feature, which allows you to combine scan results from multiple URLs.

We have created three assessments for testing our site at different stages of the standard development process. For demonstration purposes, each assessment contains only one scan (although in practice, each assessment would typically contain multiple scans conducted over a period of time). The Development host is http://127.0.0.1/; the QA host is http://qazero.webappsecurity.com/; the Production host is http://zero.webappsecurity.com/. Because the hosts are different, AMP normally would not correlate the vulnerabilities and findings across the assessments. However, if we designate one of the URLs as the primary and then specify that the other two URLs are equivalent to the primary (thus creating an "alias" for the related URLs), AMP can correlate findings, false positives, and ignored vulnerabilities across all three assessments.

Create a Site

- 1 In the navigation pane, under Actions, click New Site.
- 2 For the site name, enter Zero SDLC.
- 3 For the URL, enter http://zero.webappsecurity.com
- 4 On the Site Details form, click the Aliases tab and then click Add.
- 5 On the Add New Alias dialog, enter http://zero.webappsecurity.com as the primary URL and click Add.
- 6 In the Equivalent URLs box, enter http://127.0.0.1 and click UPD (update).
- 7 Click Add again, enter http://qa-zero.webappsecurity.com and click UPD.

🖉 Site Details - Windows Internet Explorer provided by Yahoo!	2/7/11 2:24:28pm 🗐 🔂
C C - K + K + K + K + K + K + K + K + K + K	🗴 👻 Certificate Error 🤧 🗙 🛃 Google 🖉 🖉
Ele Edit View Favorites Tools Help	
🙀 Favorites 🔣 Site Details	
	Logged in as: SPI\David.Thacken
AMP [™] Sites → Site Details	🔒 Log Off 📟 Options 🔻 Site Filters 🗱 Resources 🥹 Help
🕨 Scan Now 🗟 Repeat Last Scan 🧕 Schedule Scan 🗡 Delete	8
Site: zero SDLC	
Project: Default Organization : Default Project	
URL: http://zero.webappsecurity.com/ Phase:	Edit Alias
Phase: Group:	Primary URL: http://zero.webappsecurity.com/
Auto-Archive: Disabled	Description:
	Add
Assessment: Production phase	Equivalent URLs
Completed: 2/7/2011 2:19:32 PM Policy: Cross-Site Scripting	http://qa-zero.webappsecurity.com/
Risk: 55.00 40 11 40 0 10 20 20 20 20 0	http://127.0.0.1/ DEL
😨 Assessments 📓 Scans 🕜 Schedules 🔯 Reports 🎹 Properties 📉 Notes 🛷 Tags 🚇 QC Defects Al	iases
Page 1 of 1 Selected 0 of 1	
Primary URL 🔺 Description C	ase Sea
http://zero.webappsecurity.com/	
	Save Cancel
Page 1 of 1 Selected 0 of 1	Ð

8 Click Save.

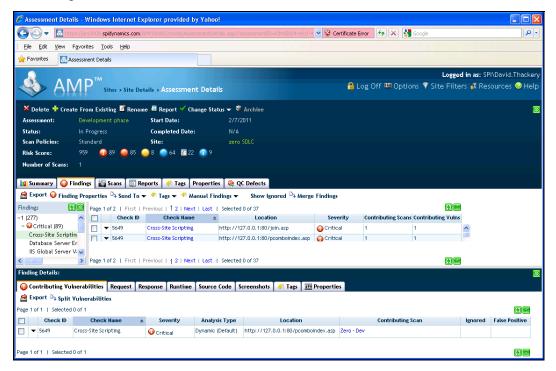
Create Assessment

- 1 In the navigation pane, under Actions, click New Assessment.
- 2 For the site name, enter Zero SDLC.
- 3 For the assessment name, enter Development Phase.
- 4 Click Finish.

Conduct Scans

1 From the Assessment Details form, click the **Scans** tab and then click **New**. Note: if you had already conducted a scan, you could click **Add** to assign an existing scan to the assessment.

- 2 Configure the scan and click Scan Now (or Finish).
- 3 When the scan is complete, navigate to the Assessment Details form.
- 4 Click on the cross-site scripting check name in the Findings tree view (at left).
- 5 Click the pcomboindex.asp cross-site scripting finding to reveal (at the bottom) the list of vulnerabilities that contributed to this finding. Note that the False Positive column is not checked.



- 6 On the Findings tab, check the box next to the Check ID for cross-site scripting at pcomboindex.asp.
- 7 Click Finding Properties.

Assessment Details - Windows Internet Explorer provided by Yal	ioo!
C	Details.aspv?Assessment1D=fd4d33c4-e81f-4 💌 😵 Certificate Error 🛛 🍫 🗙 Google
File Edit View Favorites Tools Help	
👷 Favorites 🔣 Assessment Details	
AMP TM Sites > Site Details > Assessment De	Logged in as: SPI\David.Thackery tails
🗙 Delete 📌 Create From Existing 🧧 Rename 🛎 Report 🗹 Change :	Status 🕶 🖉 Archive 🛛 😒
Assessment: Development phase Start Date:	
Status: In Progress Completed Date:	
Scan Policies: Standard Site:	
Risk Score: 959 🚯 89 🥌 85 🥌 8 🥌 64 💆 22 👔	9 Finding Properties
Number of Scans: 1	✓ Finding Note
Image: Stand of the	Findings Show Ignored
Image: Solution of the sol	
✓ ▼ 5649 Cross-Site Scripting http://127.0.0.1:80/	pcomboindex.asp
☐ ▼ 5649 Cross-Site Scripting http://127.0.0.1:80/	join.asp
□ ▼ 5649 Cross-Site Scripting http://127.0.0.1:80/	
□ ▼ 5649 Cross-Site Scripting http://127.0.0.1:80/	banklogin.asp Oritical future scans, it will automatically be designated as a "false positive."
Solution	
	pcomboindex.asp 🕡 Critical
	rootlogin.asp OK Cancel
♦	rootlogin.asp OCritical
□ ▼ 5649 Cross-Site Scripting http://127.0.0.1:80/	join.asp 🕡 Critical
	pformresults.asp 🗛 Critical
Page 1 of 2 First Previous 1 2 Next Last Selected 1 of 37	
Finding Details:	

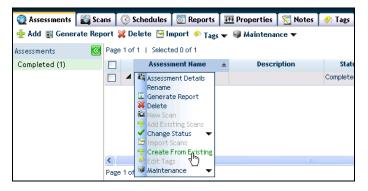
- 8 On the Finding Properties dialog, select **Mark as False Positive** and (optionally) add a note that explains the reason for your conclusion. Note: you can select multiple findings and mark them as false positive.
- 9 Click OK.

In real-world scenarios, you may conduct additional assessments while in the development phase. Then, when moving on to a new assessment, you would mark the previous assessment as complete.

Assessment Deta									
🔊 🗢 🔝 hti	tps://ars2008.spidynamics.com	n/AMP/WebConsole/Assessme	entDetails.aspx?A	ssessmentID=fd4d33c4-e81f	-4 💌 😵 Certificate	Error 😽 🗙 🚼	Google		۶
File Edit View	Favorites Tools Help								
Favorites 🔤 🔣 🕫	Assessment Details								
							Logged	d in as: SP	'I\David.Thack
🍣 🖇		Details > Assessment D	Details		a	Log Off 🏧 Optio	ns 🔻 Site Filte	rs 👪 Res	ources 🥝 He
🗙 Delete 💠 Crea	ate From Existing 🗹 Ren	ame 🏮 Report 🗹 Chang	je Status 🔺 🕸	Archive					
Assessment:	Development phase	Start Date:	2/5	Set in Progress Set to Complete					
Status:	In Progress	Completed Date:	N/	Set to Abandoned					
Scan Policies:	Standard	Site:	zero S	SDLC					
Risk Score:	954 🛛 🙆 88 🥥 85	🦲 8 🦲 64 🛐 22 🎑	9						
	1								
🛿 Summary 🕠	ing Properties 🕞 Send To	-	al Findings 🔻	Show Ignored D> Mer	ge Findings		a 📾		
Summary O	ing Properties >> Send To Page 1 of 2 First	o 👻 🤲 Tags 👻 🤲 Manus Previous 1 2 Next L	al Findings 👻	Show Ignored > Mer		Contributing Scans	Contributing Yulns		
Summary O	ing Properties 🕞 Send To	o 👻 🤲 Tags 👻 🤲 Manus Previous 1 2 Next L	al Findings ▼ Last Selected (Show Ignored D> Mer	ge Findings	Contributing Scans) E Contributing Vulns	~	
Summary Control Score Control Con	ing Properties Page 1 of 2 First Check II 5649 ting 5649	o ♥ ♥ Tags ♥ ♥ Manua Previous 1 2 Next L D Check Name	Last Selected (Show Ignored 0 of 37 Location	Severity				
Summary Second Find Content C	ing Properties >> Send To >> Send To >> Send To >> Send To >> Send To >> Send To Check II >> 5649 tim Er	D 👻 🤻 Tags 👻 🌱 Manua Previous 1 2 Next L D Check Name Cross-Site Scripting	Last Selected (Show Ignored D Mer 0 of 37 Location 7.0.0.1:80/join.asp	Severity				
Summary Control Sector	ing Properties Page 1 of 2 First Page 1 of 2 First Check II V:v	D 👻 🤻 Tags 👻 🌱 Manua Previous 1 2 Next L D Check Name Cross-Site Scripting	Last Selected (http://12: http://12:	Show Ignored ^D ≱ Mer 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp	Severity			~	
Summary Find Export Find dings (277) Cross-Site Script Database Server IIS Global Server	ing Properties Page 1 of 2 First Page 1 of 2 First Check II V:v	D V V Tags V Manue Previous 1 2 Next L D Check Name Cross-Site Scripting Cross-Site Scripting	Last Selected (http://12: http://12:	Show Ignored ^D ≱ Mer 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp	Severity		Contributing Vulns	~	
Summary Constraints Constrain	ing Properties Page 1 of 2 First Page 1 of 2 First Check II V:v	o 🔸 🏞 Tags 🔪 🌾 Manua Previous 1 2 Next L D Check Name Cross-Site Scripting Cross-Site Scripting	al Findings V Last Selected (http://12; http://12; Last Selected (Show Ignored □> Mer. 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp 0 of 37 0	Severity		Contributing Vulns	~	
Summary Second Contributing Value	ing Properties Page 1 of 2 First Check II 5649 V: Page 1 of 2 First Page 1 of 2 First Increabilities Request	o 🔸 🏞 Tags 🔪 🌾 Manua Previous 1 2 Next L D Check Name Cross-Site Scripting Cross-Site Scripting	al Findings V Last Selected (http://12; http://12; Last Selected (Show Ignored □> Mer. 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp 0 of 37 0	Severity Critical Critical		Contributing Vulns	~	
2 Summary 2 Seport Find Cross-Site Soripi Cross-Site Soripi Database Server Di Global Server Composition Contributing Vu Contributing Vu S Export S Split	Ing Properties Send To Page 1 of 2 First Check II Solution For the sendence of the sen	o 🔸 🏞 Tags 🔪 🌾 Manua Previous 1 2 Next L D Check Name Cross-Site Scripting Cross-Site Scripting	al Findings V Last Selected (http://12; http://12; Last Selected (Show Ignored □> Mer. 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp 0 of 37 0	Severity Critical Critical		Contributing Vulns	~	
Export Find dings ((277) Cross-Site Script Database Server IIS Global Server ding Details:	Ing Properties Send To Page 1 of 2 First Check II Solution For the sendence of the sen	D V VI Tags V V Manue Previous 1 2 Next L D Check Name Cross-Site Scripting Previous 1 2 Next L Response Runtime Sc	al Findings V Last Selected (http://12; http://12; Last Selected (Show Ignored □> Mer. 0 of 37 Location 7.0.0.1:80/join.asp 7.0.0.1:80/pcomboindex.asp 0 of 37 0	Severity Critical Critical		Contributing Vulns	~	c) E False Positive

In this example, the QA assessment represents the stage gate at the end of the QA process before moving on to the Production phase. We now need to create a second assessment for the QA phase.

10 In the Site Details form, on the **Assessments** tab, click the drop-down arrow next to the Development Phase assessment and select **Create from Existing**.



This opens the settings page (not shown).

- 11 Enter QA Phase as the name for the new assessment.
- 12 In the Carry Over Information section, select False Positives and Ignored Vulnerabilities.
- 13 Click Finish.
- 14 Conduct a scan of http://qa-zero.webappsecurity.com and then mark the assessment as complete.
- 15 Create a third assessment named Production Phase, conduct a scan of http://zero.webappsecurity.com/, and then mark the assessment as complete.

So now we have three assessments, each marked complete, as illustrated on the Site Details form depicted in the following illustration.

	findows In	tern	et Explorer provided by \	Yahoo!											2/7/	11 2:20:41pm 📒	F
30 - 🔝	https://ars200	8.spi	fynamics.com/AMP/WebConsol	e/SiteDetails.aspx?SiteID=3546	9345-9c32-44e8-b	2c4-4408d0f7d17	Ь		~	😵 Cert	ificate Er	ror 🐓	×	Google			۶
<u>File E</u> dit <u>V</u> iew	F <u>a</u> vorites	<u>T</u> 00	ls <u>H</u> elp														
≿ Favorites 🛛 🔀	Site Details																
															Logged	in as: SPI\David.TI	nacker
🥸 🖇	MP'	M Si	tes » Site Details								🔒 Lo	og Off I	💴 Opt	tions 🔻 S		s 👪 Resources 🤇	
🕨 Scan Now 🗟	Repeat Las	t Sca	n 🧐 Schedule Scan X De	lete													2
Site:	zero SDI																
Project:	Default	Orga	nization : Default Project														
URL:	http://z	ero.v	vebappsecurity.com/														
Phase:																	
Group:																	
Auto-Archive:	Disabled																
Assessment:																	
Completed:			32 PM														
Policy:																	
Risk:	55.00	•	11 🥥0 🌍0 💿0 💈	0 💿 0													
Assessments	👸 Scans	0	ichedules 🛛 🔯 Reports 🗍	🎹 Properties 🛛 📉 Notes	🔶 Tags 🛛 🍭 (QC Defects A	iases										
🛖 Add 📓 Genera	ate Report	💥 Di	elete 😁 Import 🥠 Tags 🔻	🗸 🤍 Maintenance 🔻													
Assessments	💽 Pag	a 1 of	1 Selected 0 of 3														0
			Assessment Name ≜	Description	Status	System Status	-	\bigcirc	\bigcirc	\bigcirc	\$:		8	Risk	# of Scans		
Completed (3)								85	8	64	22	9	1	954	1	Default Project	
Completed (3)			Development phase		Completed	Idle	88			_							
Completed (3)		•	Development phase QA phase Production phase		Completed Completed Completed	Idle Idle	88 73 11	32	1	6 0	7	6	1	515 55	1	Default Project Default Project	

- 16 In the navigation pane under Filtered Views, click Assessments.
- 17 Click the Production Phase assessment name to navigate to the Assessment Details form.
- 18 Click on the cross-site scripting check name in the Findings tree view (at left).
- 19 Click the pcomboindex.asp cross-site scripting finding to reveal (at the bottom) the list of vulnerabilities that contributed to this finding. Note that the False Positive column is checked because this vulnerability was flagged as a false positive in the first assessment (Development Phase) and was carried over through the QA phase and into the Production phase.

C Assessment Details - Windows Internet Explorer provided by Yahoo!			2/7,	'11 2:18:32pm 🔳 🖻 🔀
💽 🕞 💌 🔣 https://ars2008. spidynamics.com /AMP/WebConsole/AssessmentDetails.asp	x?AssessmentID=817698ff-9355-4748-8931-d02e0879e623	🖌 😵 Certificate Error 🤸	🖌 🚼 Google	P -
File Edit View Favorites Tools Help				
🖕 Favorites 🔣 Assessment Details				
			Logged	in as: SPI\David.Thackery
Sites > Site Details > Assessment Details		🔒 Log Off 🎟	Options 🔻 Site Filter	rs 👯 Resources 🥹 Help
🔀 Delete 🌴 Create From Existing 🖉 Rename 👼 Report 🎸 Change Status 👻	🕈 Archive			8
Assessment: Production phase Start Date: 2/				
Status: In Progress Completed Date: N/				
Scan Policies: Cross-Site Scripting Site: ze				
Risk Score: 55 🔒 11 🥌 0 🧽 0 💆 0 🛃 0 🗊 0				
Number of Scans: 1				
	000.0			
Image: Summary with the second sec				
🚔 Export 😡 Finding Properties 🗣 Send To 👻 🦘 Tags 👻 🎋 Manual Findings 🗨	 Show Ignored			
Findings Page 1 of 1 Selected 0 of 12		08		
	Location Severity Cor /zero webanosecurity.com:80/nc Octifical 1	ntributing Scans Contributing Vulns	2	
	CZERT MERADOSECUTION CONTRALICON 4-41 FILICAL			
Page 1 of 1 Selected 0 of 12		0 =		
Finding Details:				
Ocontributing Vulnerabilities Request Response Runtime Source Code	Screenshots 🥠 Tags 🛛 III Properties			
🚔 Export 🖏 Split Vulnerabilities				
Page 1 of 1 Selected 0 of 1			0 =	
Check ID Check Name ± Severity Analysis Type	e Location	Contributing Scan	Ignored False Positive	
□ ▼ 5649 Cross-Site Scripting Ortical Dynamic (Default)) http://zero.webappsecurity.com:80/pc Zero - Prod		✓	
Page 1 of 1 Selected 0 of 1			0e	