



Web Application Security Made ~~Easy~~ **Easier**

Brian A. McHenry

Security Solutions Architect

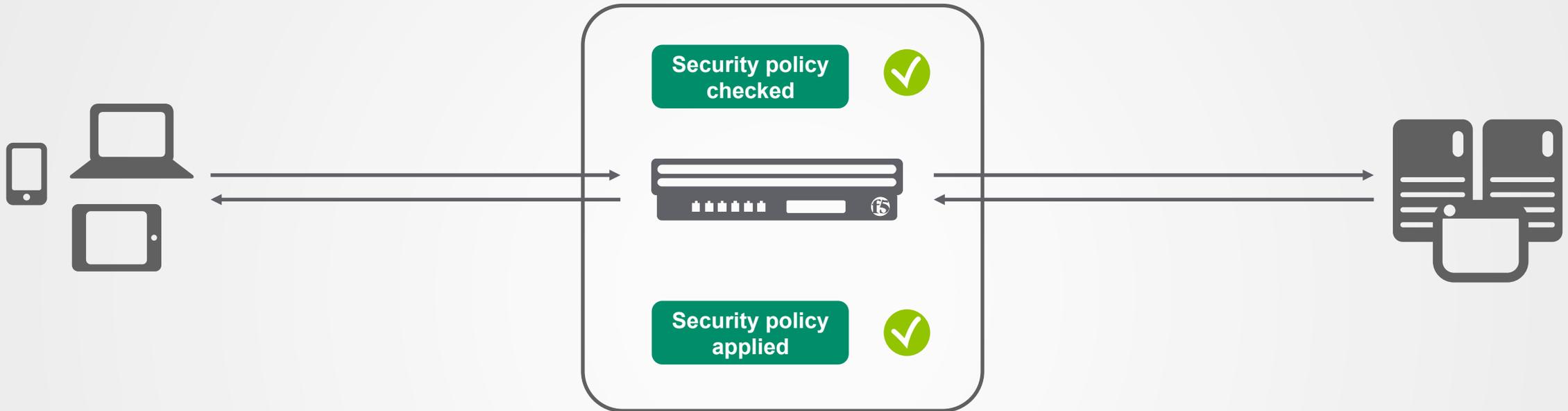
bam@f5.com



Practical Web Application Security Facts

- Remediation rates are low, especially for legacy or 3rd-party applications
- Building WAF policy is one tactic, but can also be challenging
- Applications are like snowflakes; no two alike
- WAF ownership varies, and AppSec expertise varies with it
- A WAF is only as effective as the integration with the SDLC process
- Management resources for WAF are often limited

Policy Deployment Options



DYNAMIC POLICY BUILDER

Automatic

- No knowledge of the app required
- Adjusts policies if app changes

Manual

- Advanced configuration for custom policies

INTEGRATION WITH APP SCANNERS

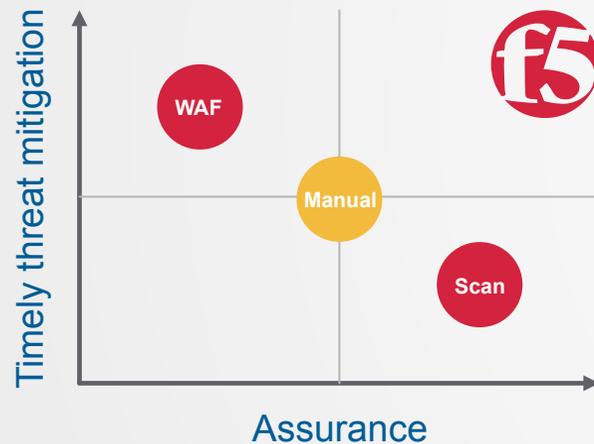
- Virtual patching with continuous application scanning

PRE-BUILT POLICIES

- Out-of-the-box
- Pre-configure and validated
- For mission-critical apps including: Microsoft, Oracle, PeopleSoft

Identify, virtually patch, mitigate vulnerabilities

Scan application with:



Configure vulnerability policy in BIG-IP ASM

The screenshot shows the 'Vulnerability Assessments' section in the BIG-IP ASM interface. It displays a table of vulnerabilities found and verified by the Centric Hallstorm engine.

Centric Hallstorm Vulnerability Name	ASM Attack Type	Resolvable	Severity	Occurrences
Blind SQL Injection	SQL-Injection	Yes	1	1
Check HTTP Methods	Other Application Attacks	Yes	1	1
Cross-Site Scripting	Cross Site Scripting (XSS)	Yes	21	21

Below the table, there is a section for 'Blind SQL Injection Vulnerabilities List' with columns for URL, Parameter, ASM Status, and Load Time. One entry is shown with a 'Pending' status.

Mitigate web app attacks



Configuration

Application Security » Web Applications » Deployment Wizard : Select Deployment Scenario

Select Deployment Scenario

Deployment Scenario	How do you want to build and deploy the security policy? <ul style="list-style-type: none"><input type="radio"/> Create a policy automatically (recommended)<input type="radio"/> Create a policy manually or use templates (advanced)<input type="radio"/> Create a policy for XML and web services manually<input checked="" type="radio"/> Create a policy using third party vulnerability assessment tool output
Description	<ul style="list-style-type: none">• Select Create a policy automatically if you want the Application Security Manager to build a security policy automatically. This option is good for production traffic or for a QA environment. The policy building process can take a few days, depending on the number of requests sent and the size of the website.• Select Create a policy manually or use templates if you would like to use either the rapid deployment policy or one of the pre-configured baseline security templates. Using this scenario, the system builds the security policy in Transparent mode to allow you to review and fine-tune the security policy. After you see that the security policy does not produce any false positives, place the security policy in Blocking mode.• Select Create a policy for XML and web services manually if you are configuring the Application Security Manager to protect a web service. In this case, it does not matter if the deployment is in production or in a QA lab. Using this scenario, the system builds the security policy in Transparent mode to allow you to review and fine-tune the security policy. After you see that the security policy does not produce any false positives, place the security policy in Blocking mode.• Select Create a policy using third party vulnerability assessment tool output if you have a vulnerability assessment tool like WhiteHat Sentinel and would like to build a security policy automatically based on the vulnerabilities found by that tool. Using this scenario, the system builds the security policy in Transparent mode to allow you to review and fine-tune the security policy. After you see that the security policy does not produce any false positives, place the security policy in Blocking mode.

Application Security » Web Applications » Deployment Wizard : Configure Web Application Properties

Configure Web Application Properties

Web Application	wh_demo
Application Language	Unicode (utf-8) ▼
Security Policy is case sensitive	<input checked="" type="checkbox"/>
Description	In this step if this is the first time the wizard is running for this application, you can specify the application language when available, and the system will automatically detect it for you. The system uses the application language for security checks. Disable the Security Policy is case sensitive check box if the web application is case insensitive.

Configuration

Application Security » Web Applications » Deployment Wizard : Vulnerability Assessments Settings

Vulnerability Assessments Settings

Vulnerability Scanner	WhiteHat Sentinel ▼
Sentinel Web API Key	<input type="text"/>
Sentinel Site Name	Custom Sentinel Site Name ▼ Demo Site SE <input type="button" value="Refresh Sentinel Site Names List"/>

Application Security » Web Applications » Deployment Wizard : Vulnerability Assessments Settings

Vulnerability Assessments Settings

Vulnerability Scanner	WhiteHat Sentinel ▼
Sentinel Web API Key	07d5f999-0e44-4afd-9ce9-6eb66e7c62da
Sentinel Site Name	Demo Site PE ▼ <input type="button" value="Refresh Sentinel Site Names List"/>

Importing Vulnerabilities

Application Security » Policy : Vulnerability Assessments : Import Vulnerabilities

Policy Blocking Response Page Vulnerability Assessments Anti-Virus Protection

Current edited policy is [Whitehat-baseline](#) for web application [wh_demo](#)

Change edited web application to: wh_demo

Change edited policy to: Whitehat-baseline (active)

Import WhiteHat Sentinel Vulnerabilities

Import Method

- Download vulnerabilities directly from WhiteHat Sentinel
- Upload previously saved vulnerabilities file

Application Security » Policy : Vulnerability Assessments : Import Vulnerabilities

Policy Blocking Response Page Vulnerability Assessments Anti-Virus Protection

Current edited policy is [Whitehat-baseline](#) for web application [wh_demo](#)

Change edited web application to: wh_demo

Change edited policy to: Whitehat-baseline (active)

Import WhiteHat Sentinel Vulnerabilities

Import Method

- Download vulnerabilities directly from WhiteHat Sentinel
- Upload previously saved vulnerabilities file

No file chosen

Importing Vulnerabilities

Application Security » Policy : Vulnerability Assessments : Vulnerabilities

Policy Blocking Response Page Vulnerability Assessments Anti-Virus Protection

Current edited policy is [Whitehat-baseline](#) for web application [wh_demo](#)

Change edited web application to
wh_demo

Change edited policy to
Whitehat-baseline (active, modified) Go

Apply Policy

- WhiteHat Sentinel Vulnerabilities were successfully imported.
- 92 vulnerabilities were added or updated.

Vulnerabilities Found By WhiteHat Sentinel

Vulnerability ID	<input type="text"/>
Sentinel Vulnerability Name	All
Sentinel Retest Status	All
Sentinel Status	Open
ASM Status	All
Sentinel Severity	All
Sentinel Threat	All
Sentinel Score	All

Go Reset Filter

Automatically Resolvable Vulnerabilities

Manually Resolvable Vulnerabilities

	Sentinel Vulnerability Name	ID	Sentinel					ASM Status
			Severity	Threat	Score	Retest Status	Status	
<input type="checkbox"/>	<input type="checkbox"/> HTTP Response Splitting	3650238	Medium	Medium	9	N/A	Open	Pending
<input type="checkbox"/>	<input type="checkbox"/> Predictable Resource Location	3650244	Medium	Medium	10	N/A	Open	Pending
<input type="checkbox"/>	<input type="checkbox"/> Directory Traversal	3695477	Medium	Medium	13	N/A	Open	Pending
<input type="checkbox"/>	<input type="checkbox"/> Directory Traversal	3695680	Medium	Medium	13	N/A	Open	Pending
<input type="checkbox"/>	<input type="checkbox"/> Directory Traversal	3695674	Medium	Medium	13	N/A	Open	Pending
<input type="checkbox"/>	<input type="checkbox"/> Directory Traversal	3695670	Medium	Medium	13	N/A	Open	Pending

A Deeper Look

Automatically Resolvable Vulnerabilities

Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status						
		Severity	Threat	Score	Retest Status	Status							
<input checked="" type="checkbox"/> HTTP Response Splitting	3650238	Medium	Medium	9	N/A	Open	Pending						
<table border="1"> <tr> <td>ASM Attack Type</td> <td>HTTP Response Splitting</td> </tr> <tr> <td>URL</td> <td>http://71.141.64.43/w3af/audit/response_splitting/response_splitting_err.php?header=None</td> </tr> </table>								ASM Attack Type	HTTP Response Splitting	URL	http://71.141.64.43/w3af/audit/response_splitting/response_splitting_err.php?header=None		
ASM Attack Type	HTTP Response Splitting												
URL	http://71.141.64.43/w3af/audit/response_splitting/response_splitting_err.php?header=None												
<input checked="" type="checkbox"/> Predictable Resource Location	3650244	Medium	Medium	10	N/A	Open	Pending						
<table border="1"> <tr> <td>ASM Attack Type</td> <td>Predictable Resource Location</td> </tr> <tr> <td>URL</td> <td>http://71.141.64.43/http://71.141.64.43/mod_security/w3af/audit/xss/stored/data</td> </tr> </table>								ASM Attack Type	Predictable Resource Location	URL	http://71.141.64.43/http://71.141.64.43/mod_security/w3af/audit/xss/stored/data		
ASM Attack Type	Predictable Resource Location												
URL	http://71.141.64.43/http://71.141.64.43/mod_security/w3af/audit/xss/stored/data												
<input checked="" type="checkbox"/> Directory Traversal	3695477	Medium	Medium	13	N/A	Open	Pending						
<table border="1"> <tr> <td>ASM Attack Type</td> <td>Path Traversal</td> </tr> <tr> <td>URL</td> <td>http://qatest4.qa.wh/w3af/audit/remoteFileInclusion/vulnerable.php?file=../../../../../../../../etc/hosts%00</td> </tr> <tr> <td>Parameter</td> <td>file</td> </tr> </table>								ASM Attack Type	Path Traversal	URL	http://qatest4.qa.wh/w3af/audit/remoteFileInclusion/vulnerable.php?file=../../../../../../../../etc/hosts%00	Parameter	file
ASM Attack Type	Path Traversal												
URL	http://qatest4.qa.wh/w3af/audit/remoteFileInclusion/vulnerable.php?file=../../../../../../../../etc/hosts%00												
Parameter	file												
<input type="checkbox"/> Directory Traversal	3695680	Medium	Medium	13	N/A	Open	Pending						
<input type="checkbox"/> Directory Traversal	3695674	Medium	Medium	13	N/A	Open	Pending						
<input type="checkbox"/> Directory Traversal	3698370	Medium	Medium	13	N/A	Open	Pending						

A Deeper Look

<input type="checkbox"/> Cross Site Scripting	2152204	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Pending
<input checked="" type="checkbox"/> Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
ASM Attack Type	Cross Site Scripting (XSS)						
URLs	Total: 1	In policy: 0	In staging: 0				
Parameters	Total: 11	In policy: 0	In staging: 0				
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=%3Cw%3E&var_xss10=10						
Parameter	var_xss9						
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=%3Cw%3E&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10						
Parameter	var_xss2						
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=<w%3E&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10						
Parameter	var_xss6						
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=%00%3Cw%3E&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10						
Parameter	var_xss4						
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=<w%3E&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=10						
Parameter	var_xss2						
URL	http://71.141.64.43/wh/xss.php?var_xss1=1&var_xss2=2&var_xss3=3&var_xss4=4&var_xss5=5&var_xss6=6&var_xss7=7&var_xss8=8&var_xss9=9&var_xss10=%3Cw%3E						
Parameter	var_xss10						

Resolve, Resolve and Stage

Automatically Resolvable Vulnerabilities | Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status
		Severity	Threat	Score	Retest Status	Status	
<input type="checkbox"/> OS Command Injection	3696959	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
<input checked="" type="checkbox"/> OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
<input checked="" type="checkbox"/> OS Command Injection	3698647	Medium	Medium	14	N/A	Open	Pending

Resolve and Stage | **Resolve** | Retest | Ignore | Unignore

Total Entries: 24 | Page 1 of 2

 Current edited policy is [Whitehat-baseline](#) for web application [wh_demo](#)

Change edited web application to:

Change edited policy to:

 You need to Apply Policy to accept changes made by resolve

Automatically Resolvable Vulnerabilities | Manually Resolvable Vulnerabilities

Sentinel Vulnerability Name	ID	Sentinel					ASM Status
		Severity	Threat	Score	Retest Status	Status	
<input type="checkbox"/> Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated
<input type="checkbox"/> Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> OS Command Injection	3698647	Medium	Medium	14	N/A	Open	Mitigated

Resolve and Stage | **Resolve** | Retest | Ignore | Unignore

Total Entries: 24 | Page 1 of 2

Resolve, Resolve and Stage

<input type="checkbox"/> OS Command Injection	3696959	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/> Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Mitigated
ASM Attack Type	Cross Site Scripting (XSS)						
URLs	Total: 1	In policy: 1	In staging: 0				
Parameters	Total: 11	In policy: 11	In staging: 0				
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=%3Cwhscheck%3E&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=9&var_sql10=10						
Parameter	var_sql2						
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=%00%3Cwhscheck%3E&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=9&var_sql10=10						
Parameter	var_sql2						
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=2&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=7&var_sql8=8&var_sql9=<whscheck>&var_sql10=10						
Parameter	var_sql9						
URL	http://71.141.64.43/wh/sql.php?var_sql1=1&var_sql2=2&var_sql3=3&var_sql4=4&var_sql5=5&var_sql6=6&var_sql7=<whscheck>&var_sql8=8&var_sql9=9&var_sql10=10						
Parameter	var_sql7						

Resolve, Resolve and Stage

Application Security » Parameters : Parameters List

Parameters List | Wildcards Order | Extractions | Character Sets | Sensitive Parameters | Navigation Parameters

Current edited policy is [Whitehat-baseline](#) for web application [wh_demo](#)

Change edited web application to: [wh_demo](#) | Change edited policy to: [Whitehat-baseline \(active, modified\)](#) | [Go](#) | [Apply Policy](#)

Filter: Show parameters by name... | [Go](#)

Legend

- Staging/tightening is on, no learning suggestions are available, staging/tightening period is not over
- Staging/tightening is on, learning suggestions are available
- Staging/tightening is on, no learning suggestions are available, staging/tightening period is over

Parameters List [Create...](#)

<input type="checkbox"/>	Parameter Name	Parameter Value Type	Parameter Level	Created By	Staging	Tightening
<input type="checkbox"/>	*	User-input value	Global Parameter	Policy Builder	No	No
<input type="checkbox"/>	param	User-input value	[HTTP] /w3af/audit/os_commanding/param_osc.php	WhiteHat	No	N/A
<input type="checkbox"/>	param	User-input value	[HTTP] /mod_security/w3af/audit/os_commanding/p aram_osc.php	WhiteHat	No	N/A
<input type="checkbox"/>	var	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql1	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql10	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql2	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql3	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql4	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql5	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql6	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql7	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql8	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A
<input type="checkbox"/>	var_sql9	User-input value	[HTTP] /wh/sql.php	WhiteHat	No	N/A

[Change Level...](#) [Change Type...](#) [Enforce](#) [Delete](#) [Delete All](#)

Total Entries: 14

Ignore, Unignore

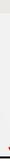
<input type="checkbox"/>	OS Command Injection	3696959	Medium	Medium	14	N/A	Open	Pending
<input checked="" type="checkbox"/>	Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/>	OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated
<input checked="" type="checkbox"/>	Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/>	OS Command Injection	3698647	Medium	Medium	14	N/A	Open	Mitigated

Resolve and Stage Resolve Retest Ignore Unignore Total Entries: 24 Page 1 of 2



<input type="checkbox"/>	OS Command Injection	3696959	Medium	Medium	14	N/A	Open	Pending
<input checked="" type="checkbox"/>	Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Ignored
<input type="checkbox"/>	OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated
<input checked="" type="checkbox"/>	Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Ignored
<input type="checkbox"/>	OS Command Injection	3698647	Medium	Medium	14	N/A	Open	Mitigated

Resolve and Stage Resolve Retest Ignore Unignore Total Entries: 24 Page 1 of 2



<input type="checkbox"/>	Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/>	OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated
<input type="checkbox"/>	Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending
<input type="checkbox"/>	OS Command Injection	3698647	Medium	Medium	14	N/A	Open	Mitigated

Resolve and Stage Resolve Retest Ignore Unignore Total Entries: 24 Page 1 of 2

Retest

- The same attack vectors will be re-sent during a retest.
- Asynchronous

Automatically Resolvable Vulnerabilities		Manually Resolvable Vulnerabilities						
Sentinel Vulnerability Name	ID	Sentinel					ASM Status	
		Severity	Threat	Score	Retest Status	Status		
<input type="checkbox"/> Cross Site Scripting	2152264	Medium	Medium	14	N/A	Open	Pending	
<input type="checkbox"/> OS Command Injection	3695424	Medium	Medium	14	N/A	Open	Mitigated	
<input type="checkbox"/> Cross Site Scripting	2152664	Medium	Medium	14	N/A	Open	Pending	
<input type="checkbox"/> OS Command Injection	3698647	Medium	Medium	14	Retest Requested	Open	Mitigated	

Resolve and Stage | Resolve | Retest | Ignore | Unignore

Total Entries: 24 | Page 1 of 2

- ... after a couple of minutes ...

Automatically Resolvable Vulnerabilities		Manually Resolvable Vulnerabilities						
Sentinel Vulnerability Name	ID	Sentinel					ASM Status	
		Severity	Threat	Score	Retest Status	Status		
<input type="checkbox"/> Cross Site Scripting	3632944	Medium	Medium	14	N/A	Closed	Pending	
<input type="checkbox"/> OS Command Injection	3698647	Medium	Medium	14	N/A	Closed	Mitigated	
<input type="checkbox"/> Cross Site Scripting	3632925	Medium	Medium	14	N/A	Closed	Pending	

Retest

- ASM polls the status of the 'Retest Requested' vulnerabilities each 2 minutes.
- Vulnerabilities are to be retested are queued in the Sentinel. Generally they process in some minutes.
- Can end up with:
 - Opened (vulnerability was not mitigated)
 - Closed (vulnerability was solved)
 - Mitigated (vulnerability was mitigated by ASM)

OS Command Injection		3698647	Medium	Medium	14	N/A	Mitigated	Mitigated
ASM Attack Type	Command Execution							
URL	http://qatest3.qa.wh/mod_security/w3af/audit/os_commanding/param_osc.php?param=/bin/df							
Parameter	param							

“We couldn't have provided safe remote access to SharePoint without the security F5 offers through BIG-IP ASM. And we don't have to spend hours reviewing thousands of vulnerability log entries in order to configure ASM effectively.

- IT Director, Large US Community College



By deploying F5's comprehensive Application Security Manager (ASM) solution, Aura is now enabling customers to fix its security issues within a reasonable timeframe, and subsequently shield and prevent reoccurrences.

