

Seeker and F5® BIG-IP® ASM™ - Integration

www.quotium.com

Quotium

Seeker and F5 BIG-IP ASM - Integration

www.quotium.com

Summary

Introduction.....	2
Problem Description.....	2
Seeker’s Integration with F5 BIG-IP ASM	2
Technical information - Step By Step	2
Seeker.....	2
F5 BIG-IP ASM.....	3
About Seeker	6

F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, taglines/slogans, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5.

Introduction

Problem Description

Seeker allows quick detection of website vulnerability. Seeker provides the exact line of code as well as remediation as part of its test results.

Sometimes, the tested website is already deployed in production, and waiting for a fix is not an option. In such cases, there is a need to block the potential vulnerability.

F5 BIG-IP Application Security Manager (ASM) is a flexible Web application firewall (WAF) that enables granular application visibility, comprehensive vulnerability assessment, and attack protection with application security.

Seeker's Integration with F5 BIG-IP ASM

Quotium and F5 have integrated their Seeker and BIG-IP ASM products to create a solution that identifies and verifies vulnerabilities and creates application security policies to mitigate them with one keystroke.

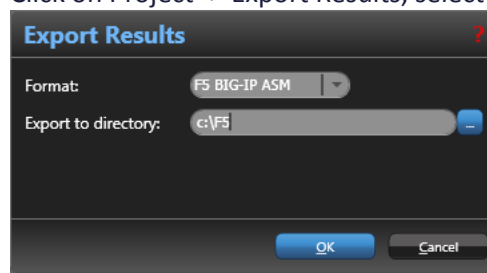
Seeker analyzes the application behavior in response to simulated attacks and detects code vulnerabilities that pose a real threat. F5 BIG-IP ASM allows simple import of Seeker test results, and creates a virtual patch until a code fix will become available.

This integration applies for Seeker versions 3 and above, and BIG-IP ASM 11.3 and above.

Technical Procedure - Step By Step

Seeker

1. Open a Seeker project with test results to export.
2. Click on Project -> Export Results, select F5 BIG-IP ASM format and click OK.



3. Fill in the folder to which results will be exported.
4. The result of this action will create an xml file of <projectName>.xml in the chosen directory.

5. F5 BIG-IP ASM

1. Open the F5 BIG-IP ASM Configuration Utility.
2. Under Security -> Application Security -> Security Policies, create a new Security policy. In the "Select Deployment Scenario" step, use "Create a security policy using third party vulnerability assessment tool output"

Security >> Application Security : Security Policies >> Deployment Wizard : Select Deployment Scenario

Select Deployment Scenario

Deployment Scenario	<p>How do you want to build and deploy the security policy?</p> <p> <input type="radio"/> Create a security policy automatically (recommended) <input type="radio"/> Create a security policy manually or use templates (advanced) <input type="radio"/> Create a security policy for XML and web services manually <input checked="" type="radio"/> Create a security policy using third party vulnerability assessment tool output </p>
Description	<ul style="list-style-type: none"> Select Create a security 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 security 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 security 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 security policy using third party vulnerability assessment tool output if you have one of these vulnerability assessment tools: WhiteHat Sentinel, IBM® AppScan®, Cenzi® Hailstorm®, QualysGuard® or HP WebInspect. If you are using a different vulnerability assessment tool, select Generic Scanner to build a security policy automatically based on the vulnerabilities found by that tool.

3. Set policy name and attributes

Security >> Application Security : Security Policies >> Deployment Wizard : Configure Security Policy Properties

Configure Security Policy Properties

Security Policy Name	Seeker_Luftdata
Application Language	Unicode (utf-8)
Enforcement Mode	<input checked="" type="radio"/> Transparent <input type="radio"/> Blocking
Security Policy is case sensitive	<input type="checkbox"/> Enabled
Differentiate between HTTP and HTTPS URLs	<input checked="" type="checkbox"/> Enabled
Description	<p>On this screen you configure the basic properties of the security policy.</p> <p>In this step you specify the Application Language which is the encoding used by your web application. The system uses the Application Language setting to accurately decode the clients' requests and normalize them before applying various security checks. You cannot change the Application Language once you have finished running the Deployment Wizard.</p> <p>If you are not sure which encoding should be used, select Auto detect, when available, and the system will automatically detect it for you. If Auto detect is not available, browse your web application with a browser.</p> <ul style="list-style-type: none"> If you are using Internet Explorer, right click within the browser page, select Encoding and see which encoding is being used by the browser. If you are using Mozilla Firefox, right click within the browser page, and select View Page Info. The encoding information is displayed. <p>Enforcement Mode: Choose Transparent if you want ASM to only log requests that violate the security policy. Choose Blocking if you want ASM to log and block requests that violate the security policy.</p> <p>Disable the Security Policy is case sensitive check box if the security policy is case insensitive. Typically, case insensitive security policies run on Microsoft® operating systems. You cannot change the Security Policy is case sensitive setting for this security policy once you have finished running the Deployment Wizard.</p> <p>Keep the Differentiate between HTTP and HTTPS URLs check box enabled for the security policy to differentiate between HTTP and HTTPS URLs if the web application behaves differently for HTTP and HTTPS URLs. Disable this option if the web application behaves the same for HTTP and HTTPS. Disabling this option saves you from having to configure the same URL twice.</p>

4. Select Quotium Seeker from the Vulnerability Assessment Tool list

Security >> Application Security : Security Policies >> Deployment Wizard : Vulnerability Assessments Settings

Vulnerability Assessments Settings Cancel Back Next

Vulnerability Assessment Tool: Generic Scanner

Configure exceptions for the scanner IP Address

IP Address:
Netmask:

Ignore in Learning Suggestions
 Never log traffic from this IP Address
 Never block this IP Address

Real Traffic Policy Builder® Enabled

Description

Select a vulnerability assessment tool. You can configure the scanner IP address as an IP address exception, meaning, an IP address that the system allows throughout the security policy. You can configure the system to perform the following:

- Ignore learning suggestions from traffic sent from this IP address. This way, the attacks sent by the scanner will not be offered as learning suggestions.
- Never log requests from the scanner's IP address. This way, your logs will not be contaminated with attacks the scanner generated.
- Never block traffic sent from this IP address. Use this option if you would like to test the web application for vulnerabilities without the protection of ASM.

Keep the **Real Traffic Policy Builder** check box enabled for the system to run the Automatic Policy Builder after the Deployment wizard is completed.

Cancel Back Next

5. Click on Finish

Security >> Application Security : Security Policies >> Deployment Wizard : Security Policy Configuration Summary

Security Policy Configuration Summary Cancel Back Finish

Security Policy Properties

Security Policy Name	Seeker_Luftdata
Application Language	Unicode (utf-8)
Enforcement Mode	Transparent
Security Policy is Case Sensitive	No
Differentiate between HTTP and HTTPS URLs	Yes

Vulnerability Assessments Settings

Vulnerability Assessment Tool	Generic Scanner
Real Traffic Policy Builder®	Enabled

Cancel Back Finish

6. Now import the Seeker test results by clicking on the Import button

Security >> Application Security : Vulnerability Assessments : Vulnerabilities

Vulnerabilities Settings Apply Policy

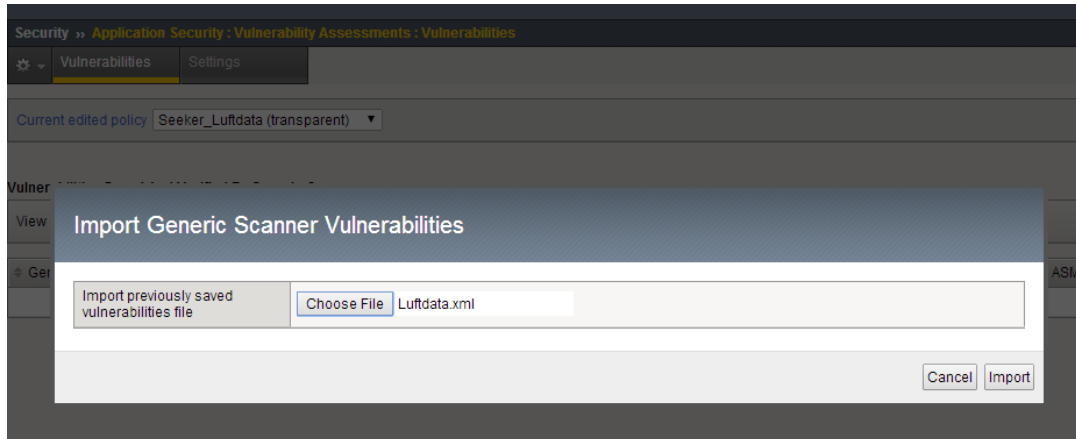
Current edited policy: Seeker_Luftdata (transparent)

Vulnerabilities Found And Verified By Generic Scanner Import

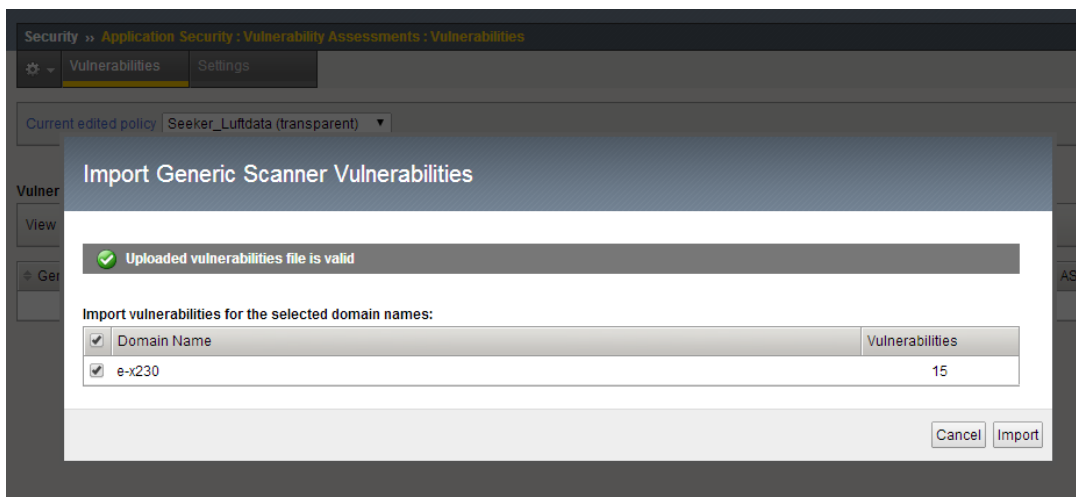
View: Resolvable | Vulnerabilities with: Any | ASM Status | Show Filter Details | Total Entries: 0

Generic Scanner Vulnerability Name	ASM Attack Type	Resolvable	Occurrences
No records to display.			

7. Choose Seeker results xml file and click on Import.



8. Review the import results and click on the Import button.



9. The rules are now ready to use.

The screenshot displays the 'Vulnerabilities' section of the Quotium application security tool. It shows a list of vulnerabilities found and verified by a generic scanner. The interface includes a navigation menu, a current policy dropdown, and an 'Apply Policy' button. Below the navigation, there are filter options for 'View' (All) and 'Vulnerabilities with' (Any), along with an 'ASM Status' and 'Show Filter Details' link. The main table lists vulnerabilities with columns for 'Generic Scanner Vulnerability Name', 'ASM Attack Type', 'Resolvable', and 'Occurrences'. One vulnerability, 'SQL Injection - Binary Search - Authenti...Users', is highlighted in blue. Below the main table, there is a section for 'SQL Injection - Binary Search - Authenticated Users Vulnerabilities List' with columns for 'URL', 'Parameter', 'ASM Status', and 'Load Time'. Two URLs are listed with their respective parameters and 'Pending' status.

Generic Scanner Vulnerability Name	ASM Attack Type	Resolvable	Occurrences
SQL Injection - Binary Search - Unauth...Users	SQL-Injection	Yes	2
SQL Injection - Binary Search - Login ...creen	SQL-Injection	Yes	1
SQL Injection - Non-Exploitable - Unauth...Users	SQL-Injection	Yes	1
SQL Injection - Union Select - Unauthent...Users	SQL-Injection	Yes	1
SQL Injection - Binary Search - Authenti...Users	SQL-Injection	Yes	2
XSS - Standard Reflected - Authenticated...Users	Cross Site Scripting (XSS)	Yes	3
XSS - Bracketless Reflected - Unauthent...Users	Cross Site Scripting (XSS)	Yes	1
XSS - Standard Reflected - Unauthentical...Users	Cross Site Scripting (XSS)	Yes	4

URL	Parameter	ASM Status	Load Time
<input type="checkbox"/> http://e-x230/luftdata/changeAccountName.aspx?AccountID=305	AccountName	Pending	2014-05-14 10:13:10
<input type="checkbox"/> http://e-x230/luftdata/User/Chequing/ExpressTrans.aspx	txtOrgNote	Pending	2014-05-14 10:13:10

About Seeker

Seeker is the run-time code & data analysis application security testing solution for the software development life-cycle. By analyzing application behavior in response to simulated attacks, Seeker detects code vulnerabilities that pose a real threat. It assists in vulnerability management by generating exploits that demonstrate the risk to business critical data. Seeker is the perfect application security testing solution for the SDLC; it can be fully automated and works great in Agile and continuous integration environments.