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

www.quotium.com

Quotium

Seeker and F5 BIG-IP ASM - Integration

www.quotium.com

Summary

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.

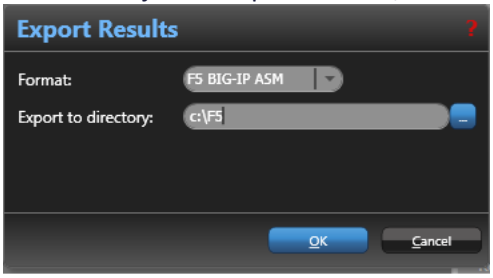
Seeker analyzes the application behavior in response to simulated attacks and detects code vulnerabilities that pose a real threat. F5 BIG-IP ASM allows simple import of Seeker test results, and creates a virtual patch until a code fix will become available.

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

Technical Procedure - Step By Step

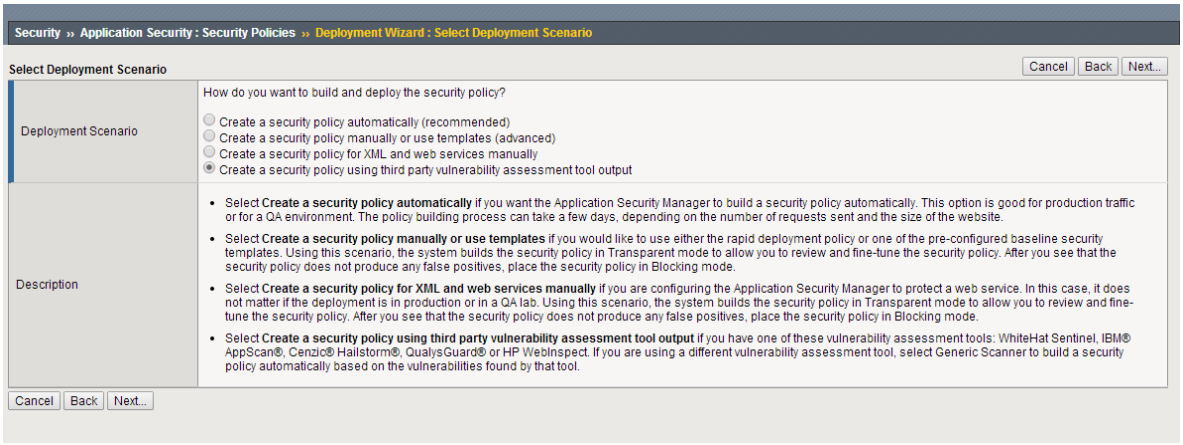
Seeker

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.

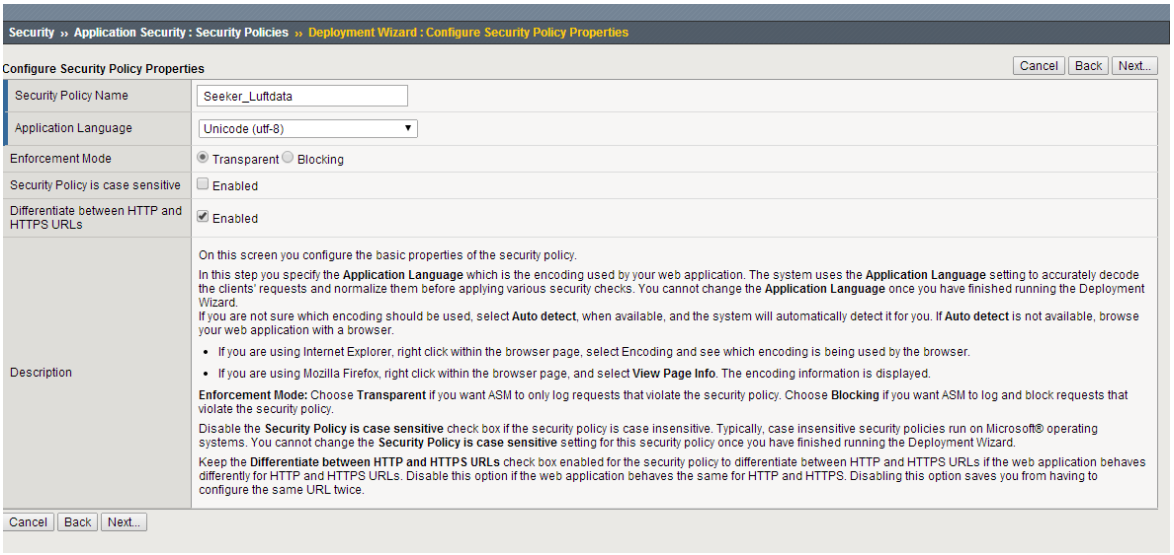


3. Fill in the folder to which results will be exported.
4. The result of this action will create an xml file of <projectName>.xml in the chosen directory.

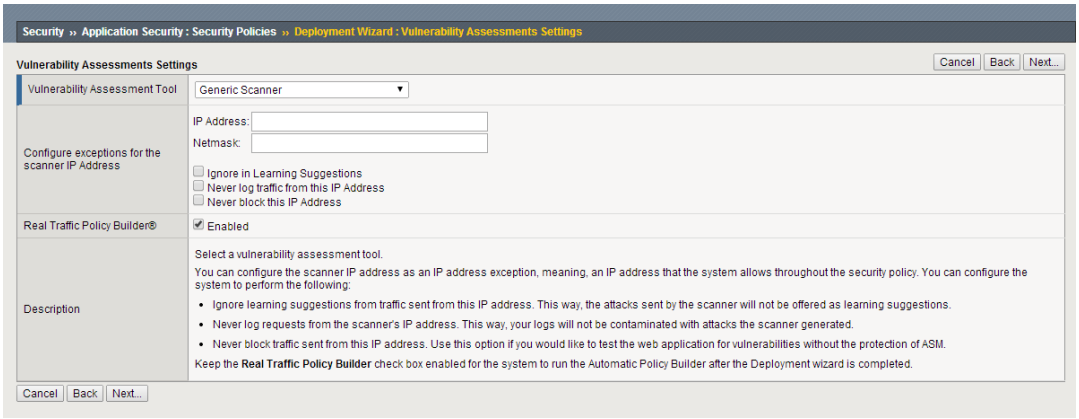
5. F5 BIG-IP ASM
    1. Open the F5 BIG-IP ASM Configuration Utility.
    2. Under Security -> Application Security -> Security Policies, create a new Security policy. In the "Select Deployment Scenario" step, use "*Create a security policy using third party vulnerability assessment tool output*"



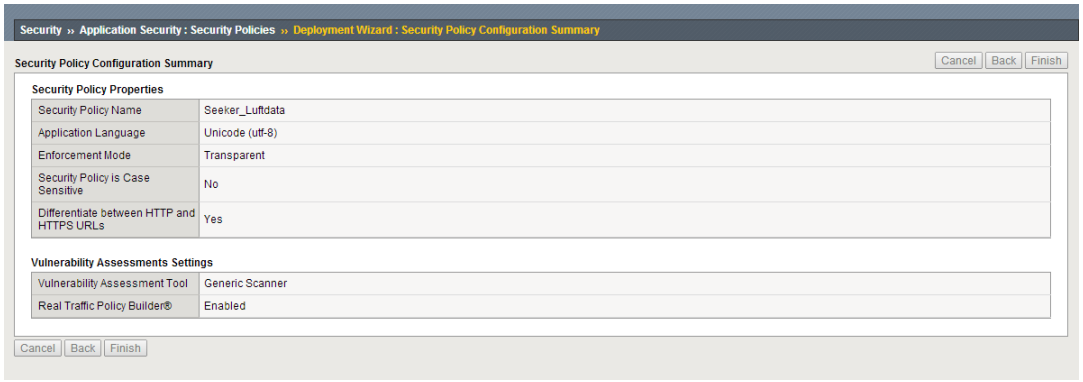
3. Set policy name and attributes



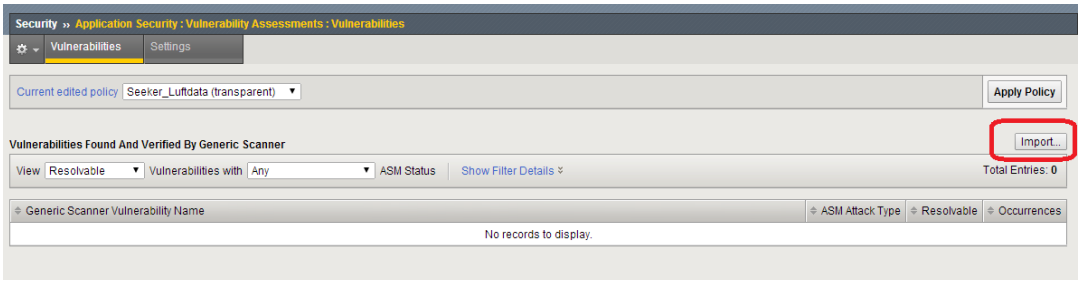
4. Select Quotium Seeker from the Vulnerability Assessment Tool list



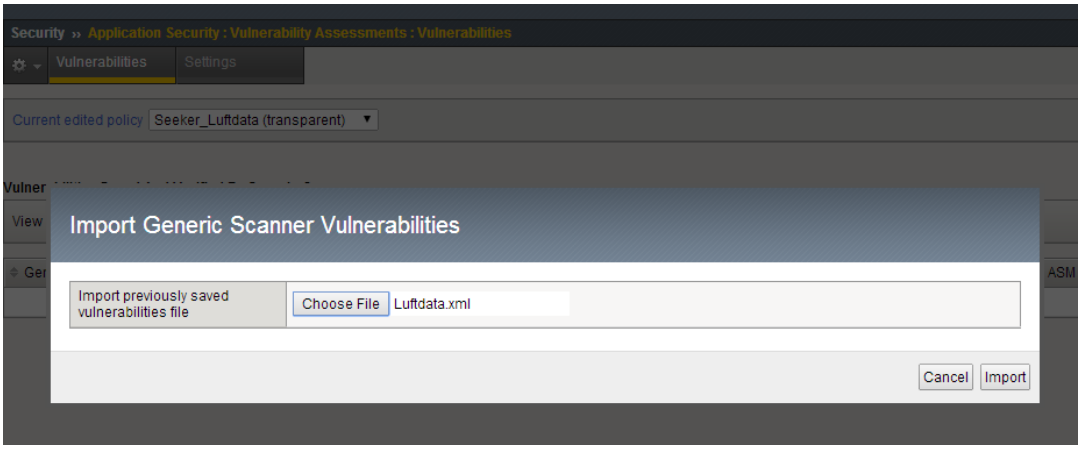
5. Click on Finish



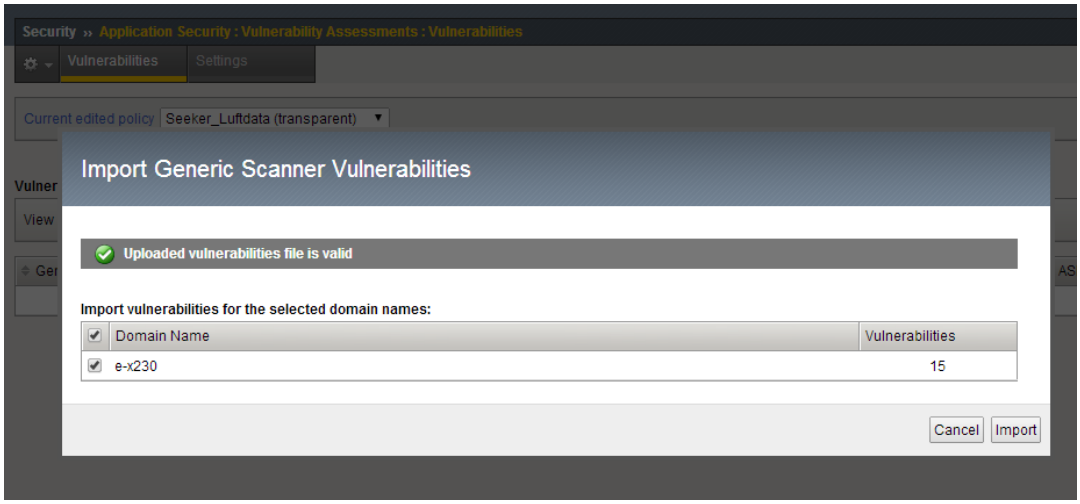
6. Now import the Seeker test results by clicking on the Import button



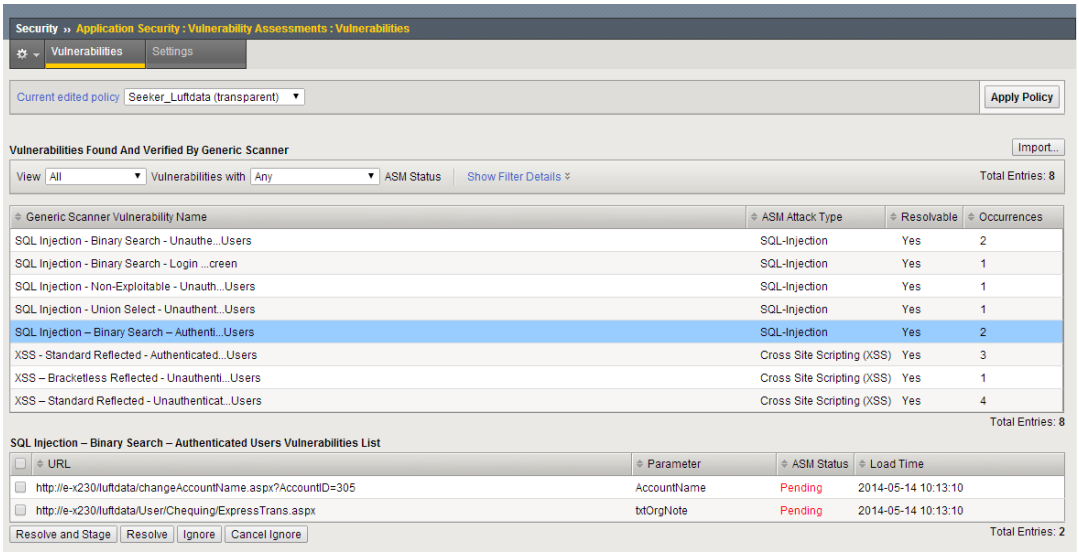
7. Choose Seeker results xml file and click on Import.



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



9. The rules are now ready to use.



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.