Introduction (Solution Overview)

The following guide describes how to export a list of detected vulnerabilities from penetration testing reports on ImmuniWeb® Platform and import them into BIG-IP® Application Security Manager™.

Use cases:

- ImmuniWeb® On-Demand: export all detected vulnerabilities found during web application penetration testing, and import them into your F5 BIG-IP®
- ImmuniWeb Continuous: export all detected vulnerabilities found during continuous web application penetration testing, and import them into your F5 BIG-IP®
- ImmuniWeb MobileSuite: export all detected vulnerabilities found during mobile application penetration testing, and import them into your F5 BIG-IP®

The entire process consists of 3 steps, detailed on the following pages:

1. How to initially configure the project on ImmuniWeb® AI Platform.....2
2. How to export the list of detected vulnerabilities on ImmuniWeb® AI Platform.....3
3. How to import the list of vulnerabilities into F5 BIG-IP® Advanced WAF®) 4

Step-by-step Guidance

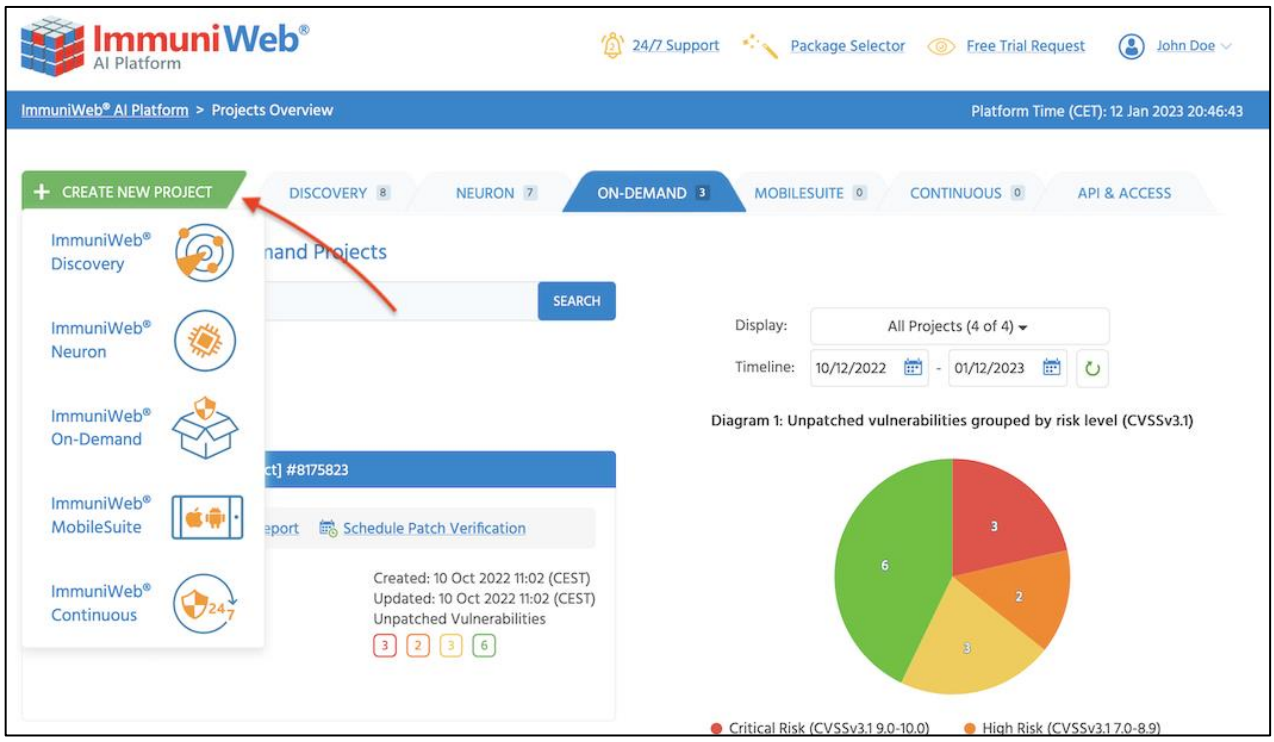
Technical requirements:

- You need F5 BIG-IP® version 16.0.x or later
- You need to have and ImmuniWeb account with access to a pentesting report

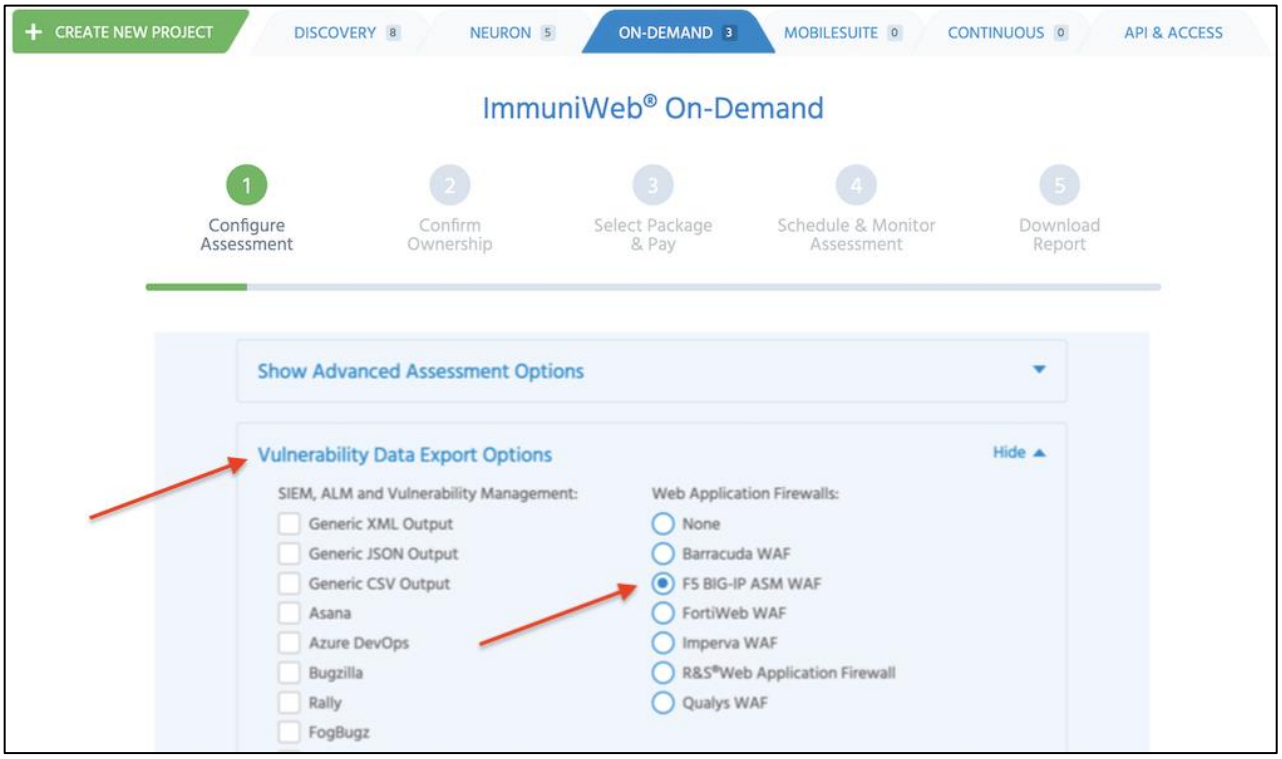
Please note that demo or PoC reports cannot be used do import vulnerability data into F5 BIG-IP®

1. How to initially configure the project on ImmuniWeb® AI Platform

- Login to ImmuniWeb® AI Platform and create new On-Demand, Continuous or MobileSuite assessment project:

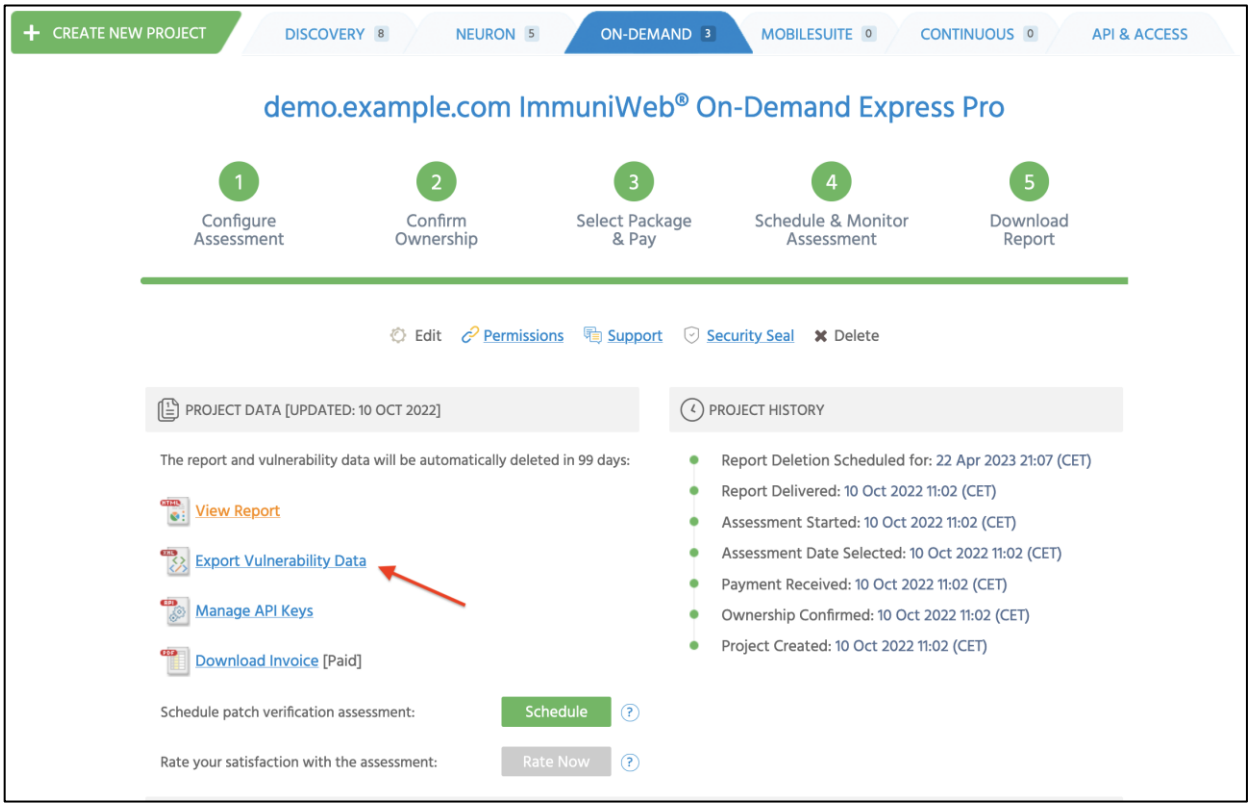


- On the first step of the project creation wizard, click on the "Show Vulnerability Data Export Options" section to expand it. Then select "F5 BIG-IP® ASM WAF" from the list of available Web Application Firewalls:

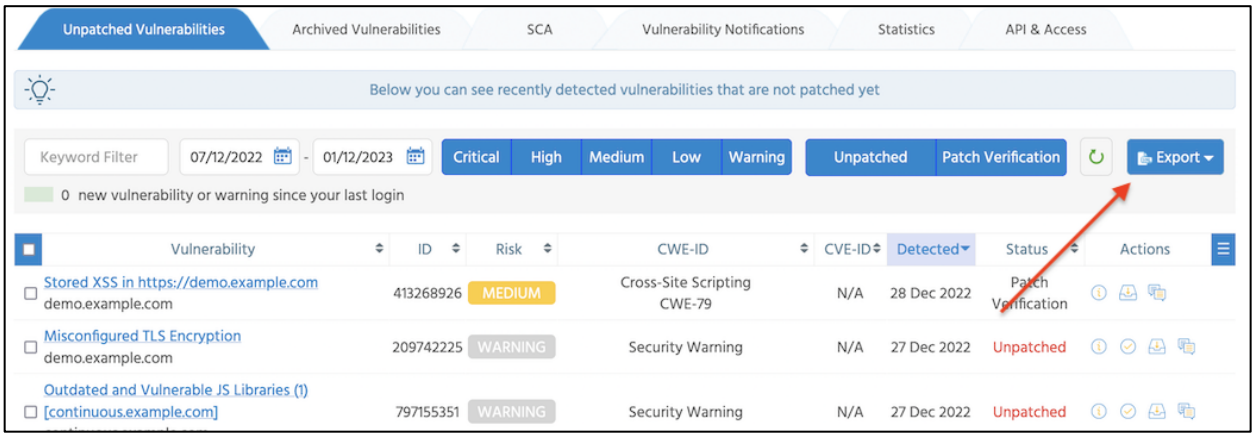


2. How to export the list of detected vulnerabilities on ImmuniWeb® AI Platform

- For ImmuniWeb On-Demand or MobileSuite projects, once the assessment is finished, you can download a JSON file with a security policy for BIG-IP® Advanced WAF® by clicking on the "Export Vulnerability Data" button:



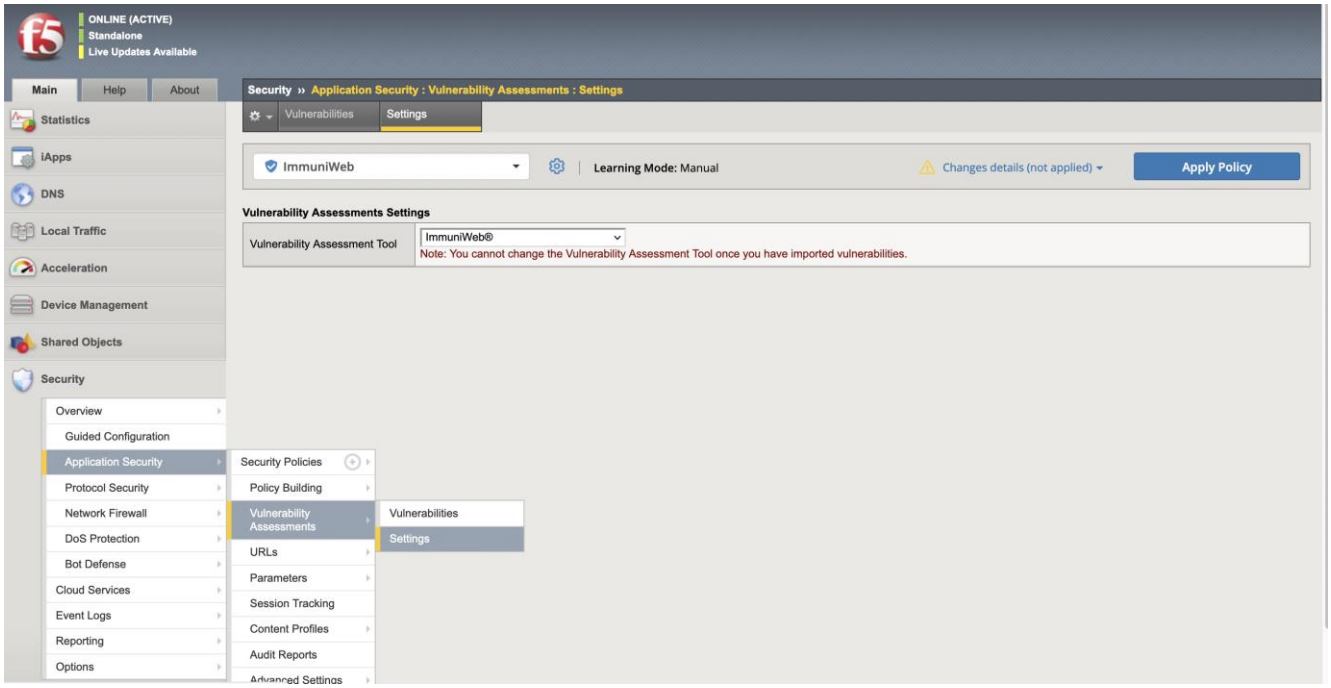
- For ImmuniWeb Continuous project, at any time when there are vulnerabilities in "Unpatched Vulnerabilities" or "Archived Vulnerabilities" tabs of the dashboard, you can download a JSON file with a security policy for BIG-IP® Advanced WAF® by clicking "Export" button:



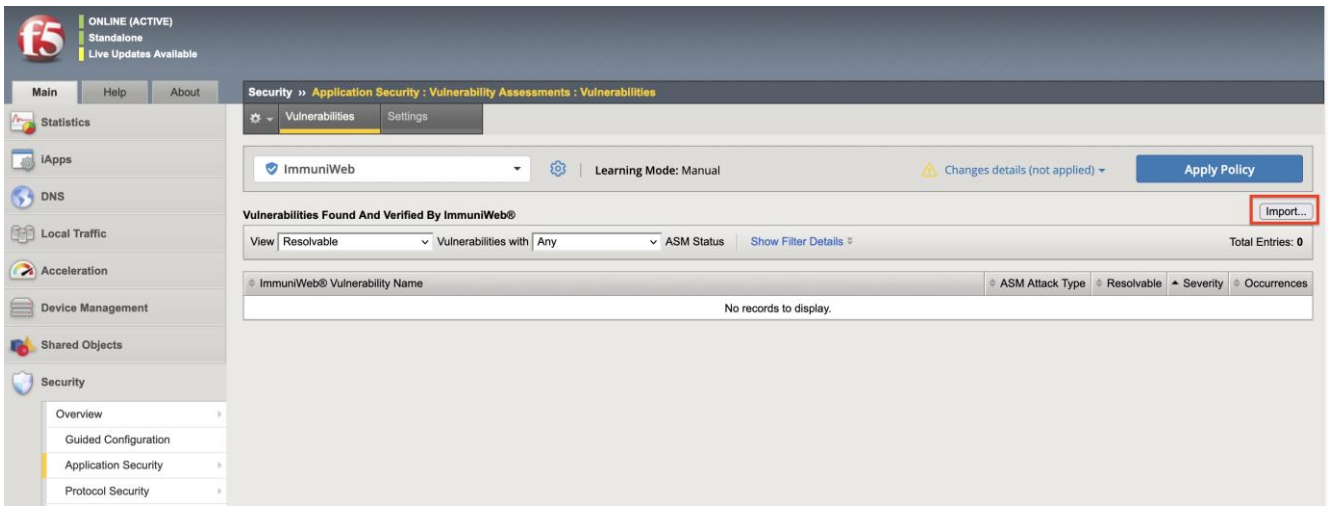
- Save the XML file on your local or network drive.

3. How to import the list of vulnerabilities into F5 BIG-IP® Advanced WAF®)

- Login to BIG-IP® Configuration Utility. In the left-side menu go to: Security -> Application Security -> Vulnerability Assessments -> Settings. Then select ImmuniWeb® from the "Vulnerability Assessment Tool" dropdown list.



- Navigate to Vulnerabilities tab and click on the "Import" button and then the "Browse…" button to select the XML file previously exported from ImmuniWeb.



- Click "Apply Policy" button to apply updates to the selected security policy. The virtual patching for the selected vulnerabilities shall now be deployed. Consider removing the XML files with vulnerability data from any insecure or temporary locations.