

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

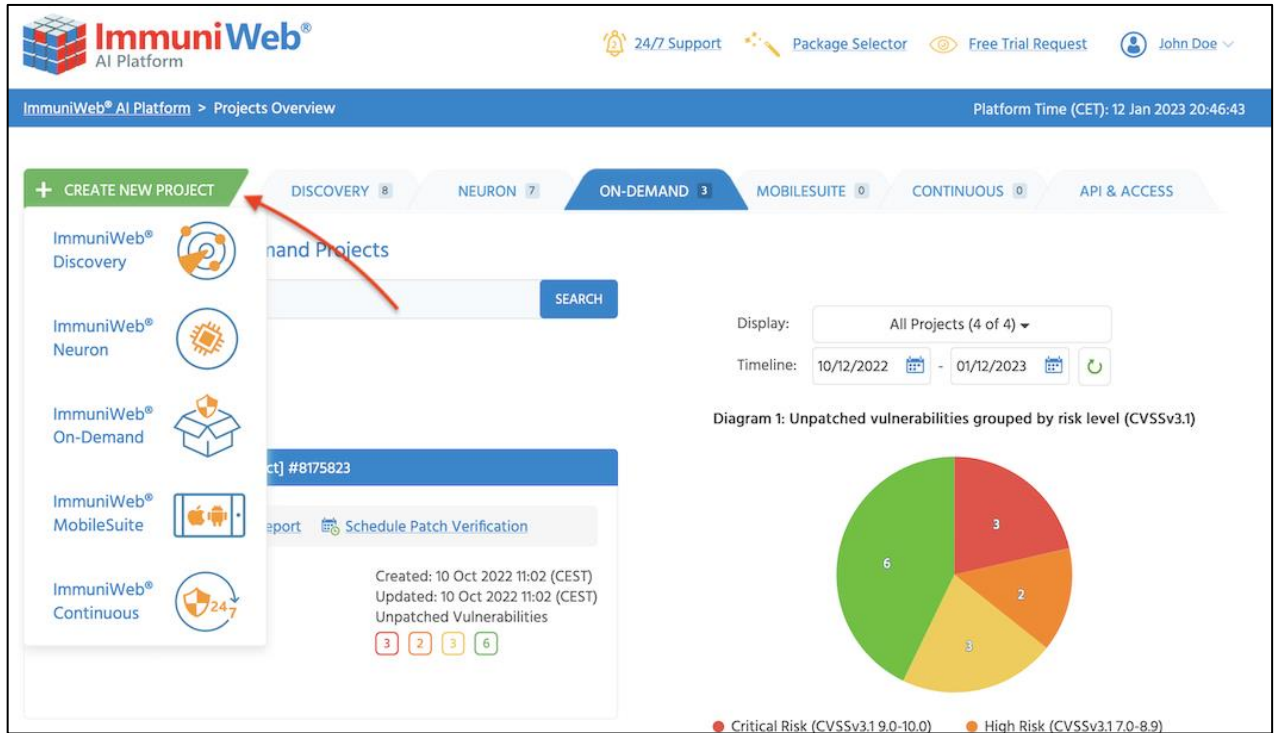
Technical requirements:

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

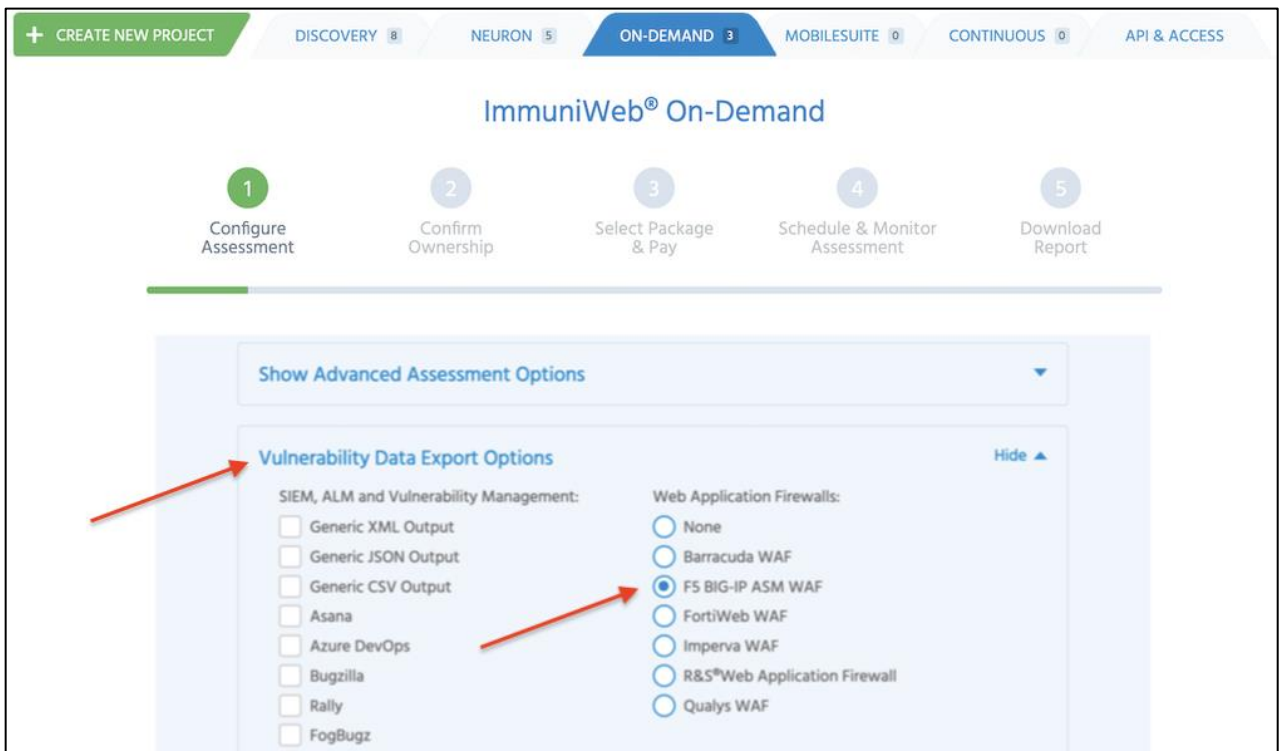
Please note that demo or PoC reports cannot be used to import vulnerability data into F5 BIG-IP[®]

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:

The screenshot shows the ImmuniWeb On-Demand Express Pro dashboard for a project named 'demo.example.com'. The dashboard includes a progress bar with five steps: 1. Configure Assessment, 2. Confirm Ownership, 3. Select Package & Pay, 4. Schedule & Monitor Assessment, and 5. Download Report. Below the progress bar, there are options to Edit, Permissions, Support, Security Seal, and Delete. The main content area is divided into two sections: 'PROJECT DATA [UPDATED: 10 OCT 2022]' and 'PROJECT HISTORY'. The 'PROJECT DATA' section contains a message: 'The report and vulnerability data will be automatically deleted in 99 days:' followed by buttons for 'View Report', 'Export Vulnerability Data' (highlighted with a red arrow), 'Manage API Keys', and 'Download Invoice [Paid]'. The 'PROJECT HISTORY' section lists several events, including 'Report Deletion Scheduled for: 22 Apr 2023 21:07 (CET)', 'Report Delivered: 10 Oct 2022 11:02 (CET)', 'Assessment Started: 10 Oct 2022 11:02 (CET)', 'Assessment Date Selected: 10 Oct 2022 11:02 (CET)', 'Payment Received: 10 Oct 2022 11:02 (CET)', 'Ownership Confirmed: 10 Oct 2022 11:02 (CET)', and 'Project Created: 10 Oct 2022 11:02 (CET)'. At the bottom, there are buttons for 'Schedule patch verification assessment:' and 'Rate your satisfaction with the assessment:'.

- 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:

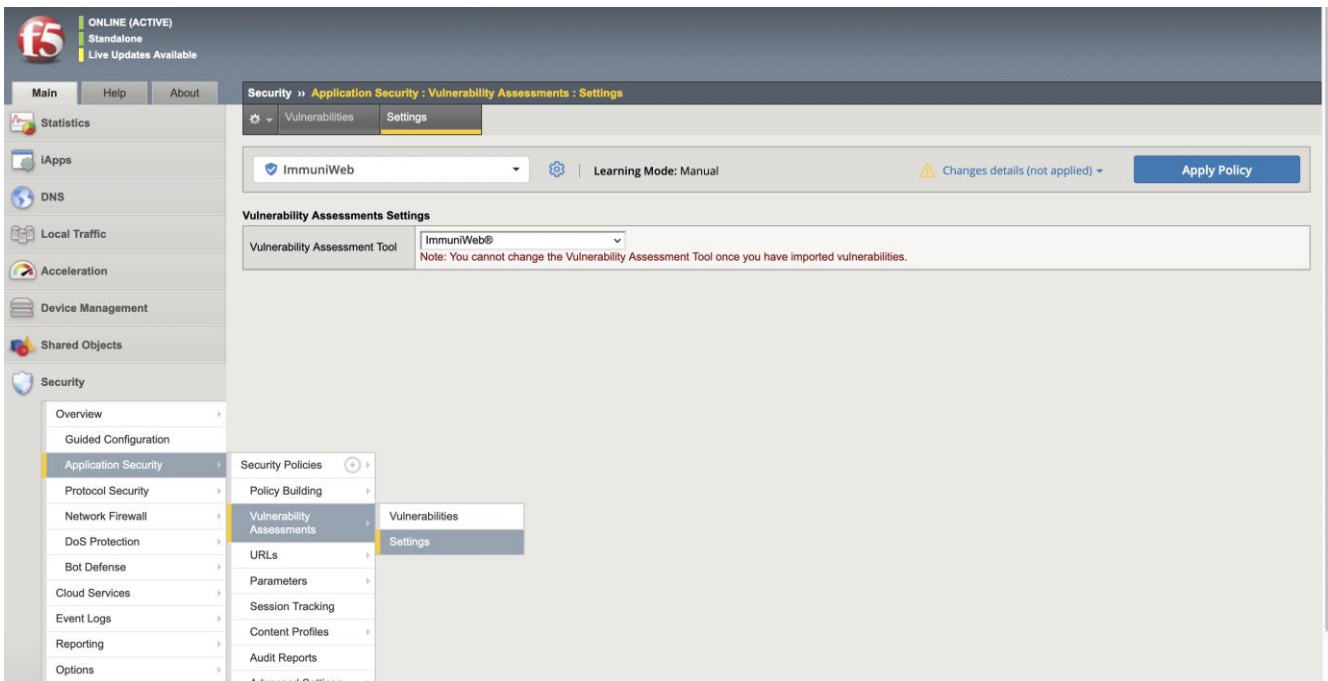
The screenshot shows the ImmuniWeb Continuous dashboard under the 'Unpatched Vulnerabilities' tab. The dashboard displays a list of recently detected vulnerabilities that are not patched yet. The list includes columns for Vulnerability, ID, Risk, CWE-ID, CVE-ID, Detected, Status, and Actions. The first vulnerability is 'Stored XSS in https://demo.example.com' with a MEDIUM risk level, detected on 28 Dec 2022, and status 'Patch Verification'. The second vulnerability is 'Misconfigured TLS Encryption' with a WARNING risk level, detected on 27 Dec 2022, and status 'Unpatched'. The third vulnerability is 'Outdated and Vulnerable JS Libraries (1)' with a WARNING risk level, detected on 27 Dec 2022, and status 'Unpatched'. The 'Export' button is highlighted with a red arrow.

Vulnerability	ID	Risk	CWE-ID	CVE-ID	Detected	Status	Actions
Stored XSS in https://demo.example.com demo.example.com	413268926	MEDIUM	Cross-Site Scripting CWE-79	N/A	28 Dec 2022	Patch Verification	Info, Print, Share
Misconfigured TLS Encryption demo.example.com	209742225	WARNING	Security Warning	N/A	27 Dec 2022	Unpatched	Info, Print, Share
Outdated and Vulnerable JS Libraries (1) [continuous.example.com]	797155351	WARNING	Security Warning	N/A	27 Dec 2022	Unpatched	Info, Print, Share

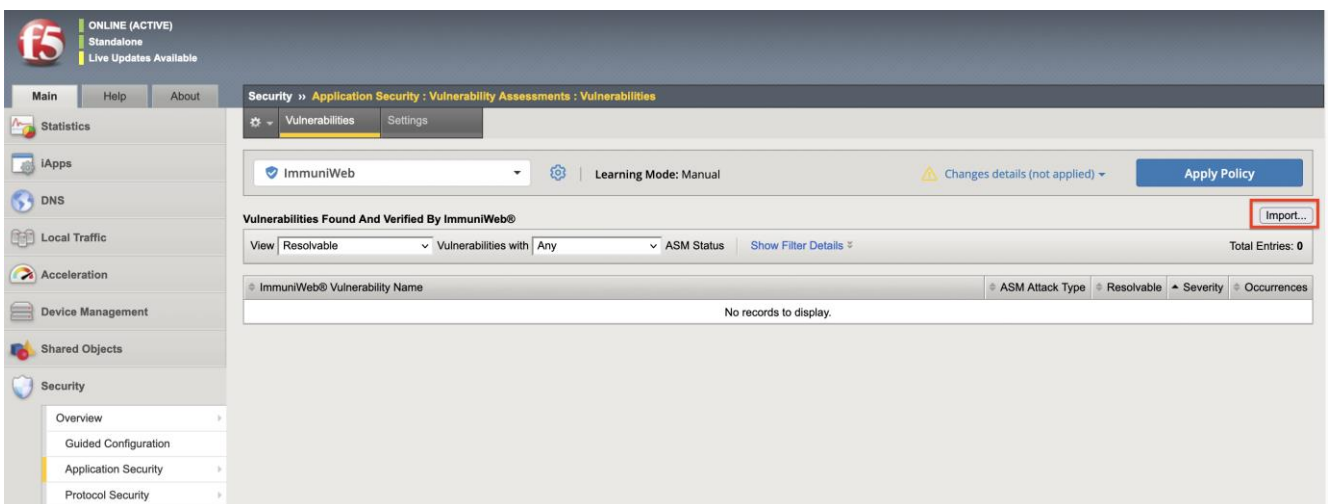
- Save the XML file on your local or network drive.

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.