Alteon WAF Demolab Guide

Written by Tal Yerushalmi

Advanced Solutions, Application Security Expert

Version 9.0

January, 2024

TABLE OF CONTEXT

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

Demo Overview & Topology

Welcome to the Alteon WAF Demo Lab. This guide demonstrates fundamental web application attacks, WAF security policy construction using automatic policy generation, API security, defense messaging and reporting, and advanced bot management and mitigation with Bot Manager.

The lab features a Windows VM remote desktop that serves as the management station. The VM and guide supply you with all necessary tools to showcase the scenarios outlined in this lab guide.

The demo features a continuous traffic generator that produces both legitimate and attack traffic directed towards a single virtual server, identified as Hackazon:80 within the Cyber Controller. This traffic generator is designed to enable swift demonstration of analytics without inundating logs and events from other applications. As a result, it facilitates the display of general analytics for Hackazon:80, as well as specific, scenario-based analytics or events for the remaining applications.

The Management station provides access to the following components:

- Chrome Browser with pre-configured bookmarks
- Cyber Controller – Version 10.0.1.0
- Alteon Secure VA – ADC01 – Version 33.0.8.0 / 7.6.19.0
- Alteon Secure VA – ADC02 – Version 33.0.8.0 / 7.6.19.0
- Virtual DefensePro X – version 10.1.0.0
- Application Servers hosting the following vulnerable web applications:
    - HackmeBank
    - bWAPP
    - Hackazon
    - Juice-Shop

The Management Station connects to three networks:

- External Network – Used for external connectivity via RDP and Gateway to the Internet.
- Internal MNG Network (172.31.0.0/16) – Gives us access to the management segment.
- Internal Data Network (172.17.17.0/24 & 172.17.18.0/24)– Gives us access to the HTTP Data segment.

Tools used in the demo:

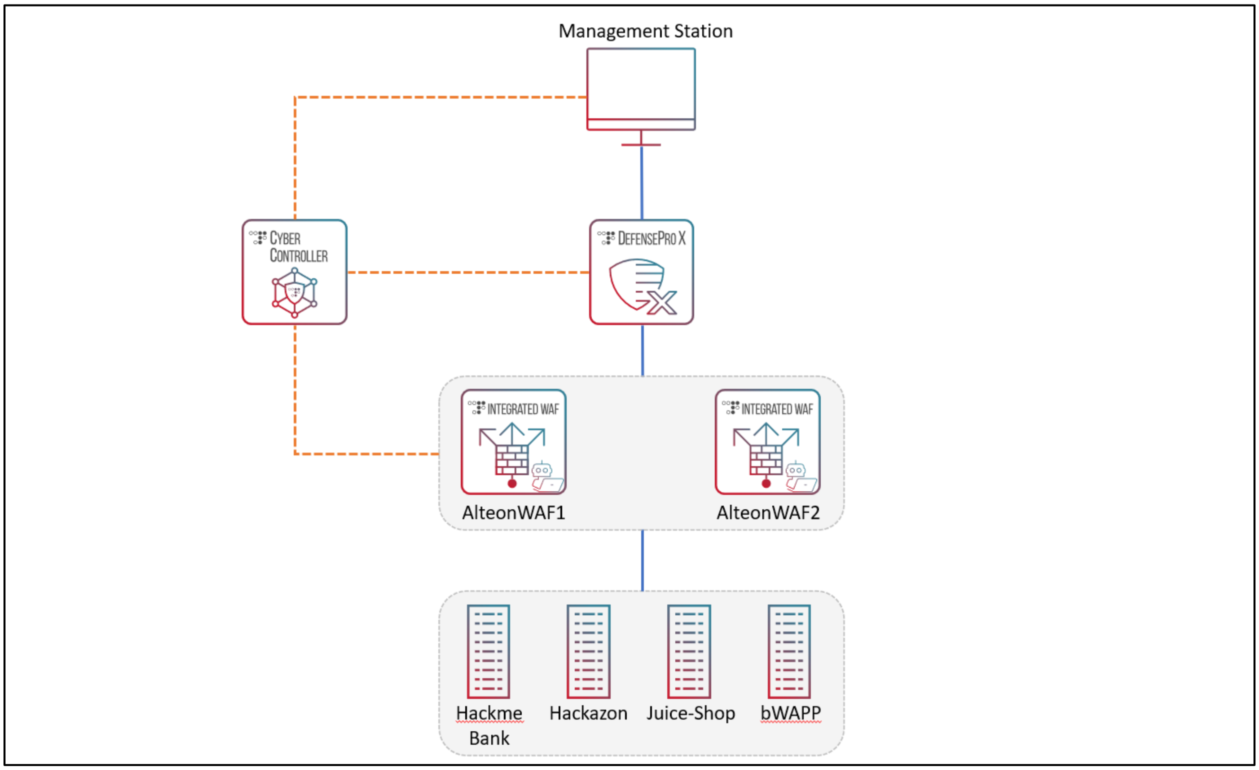
The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Burp Suite
- Postman

Credentials:

- Windows Client – radware:radware
- Vision – radware: Radware1!
- Alteons – radware:Radware1!
- DP – radware:Radware1!
- Vulnerable Web Site HackmeBank – jc:jc789 or jm:jm789
- Vulnerable Web Site Hackazon – test_user:123456
- Vulnerable Web Site Juice Shop – admin@juice-sh.op:admin123
- Bot Manager Portal – demolab@radware.com:BOTM@123

Lab Diagram:



The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

WAF Security Module

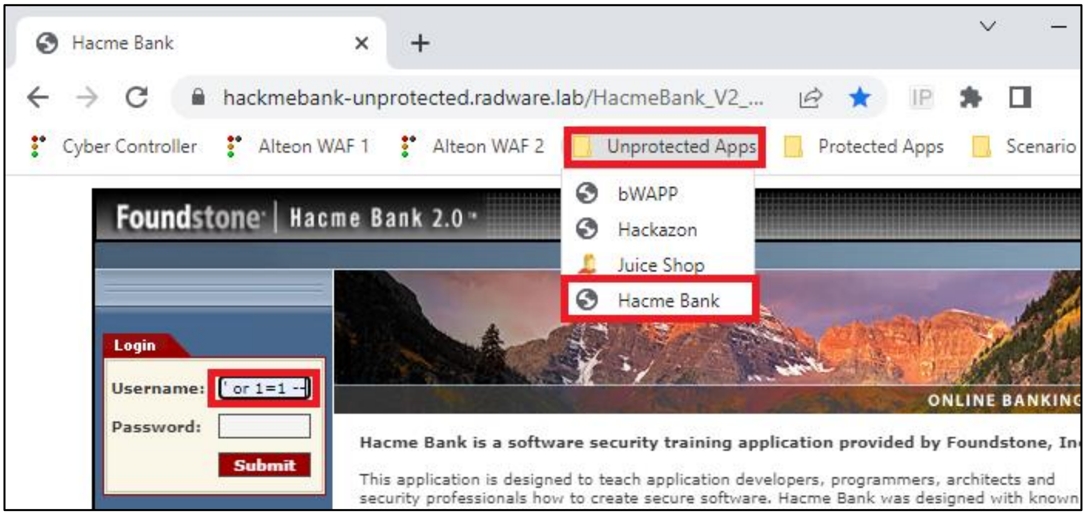
The WAF security module section presents a variety of scenarios that demonstrate numerous web application attacks, as well as the distinct features and capabilities Alteon WAF offers to effectively mitigate these attacks.

Scenario 1 - Login Using SQL Injection

In this scenario, we demonstrate a basic **SQL Injection attack** on a login page. The payload ' or 1=1-- , which represents an always TRUE expression in SQL, tricks the database into flagging the user as TRUE regardless of the actual value. We will perform the attack on both **unprotected** and **protected** versions of the web application.

Attack Unprotected Web Application

- Launch **Google Chrome**.
- Open the **Unprotected Apps Folder** located in the **bookmark bar** and click on **Hackme Bank.**
- Type ***' or 1=1--*** in the username field
- Click Submit to login to Hackme Bank web site without legitimate username and password.



Username: ' or 1=1 --

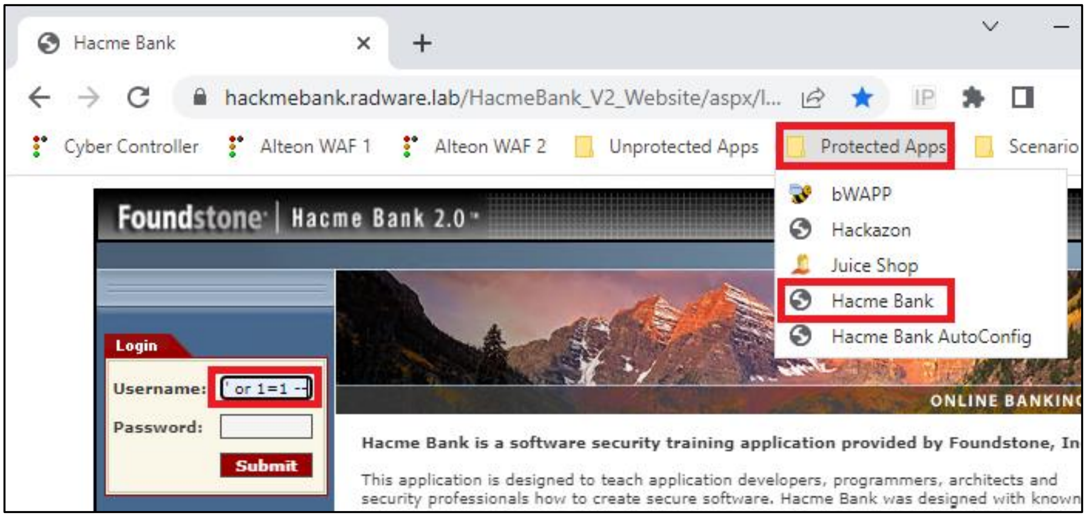
Password:

Hacme Bank is a software security training application provided by Foundstone, In

This application is designed to teach application developers, programmers, architects and security professionals how to create secure software. Hacme Bank was designed with known

Attack Protected Web Application

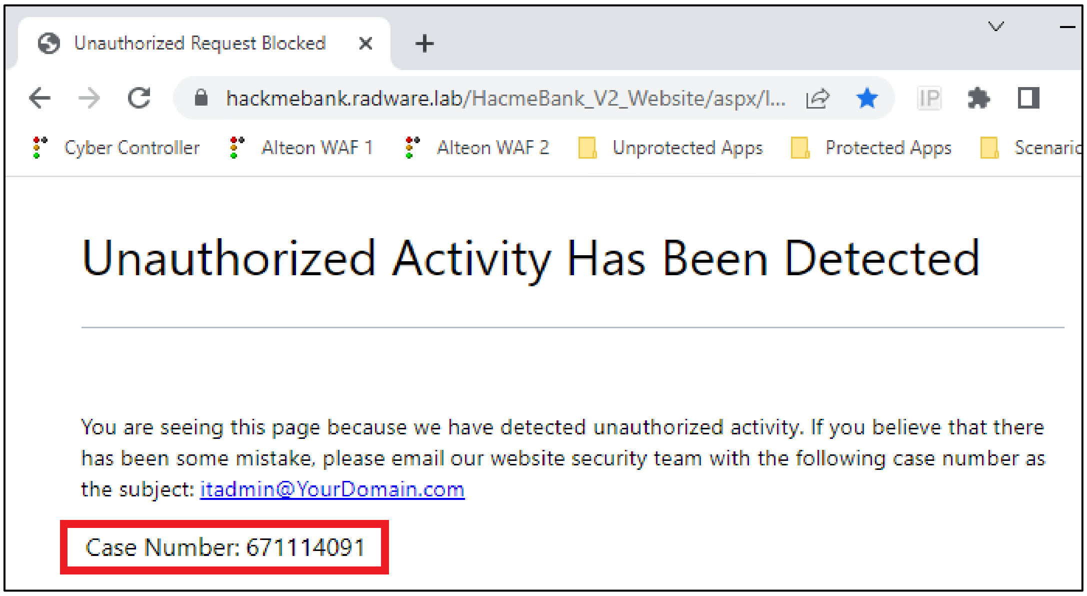
- Open the **Protected Apps Folder** located in the **bookmark bar** and click on **Hackme Bank.**
- Type *' or 1=1--* in the username field



Hacme Bank is a software security training application provided by Foundstone, In

This application is designed to teach application developers, programmers, architects and security professionals how to create secure software. Hacme Bank was designed with known

In the **protected version** of the web application, we encounter a security page because **Alteon WAF** has identified the payload and blocked the attack.


Unauthorized Request Blocked
hackmebank.radware.lab/HacmeBank_V2_Website/aspx/l...
Cyber Controller
Alteon WAF 1
Alteon WAF 2
Unprotected Apps
Protected Apps
Scenario

Unauthorized Activity Has Been Detected

You are seeing this page because we have detected unauthorized activity. If you believe that there has been some mistake, please email our website security team with the following case number as the subject: itadmin@YourDomain.com

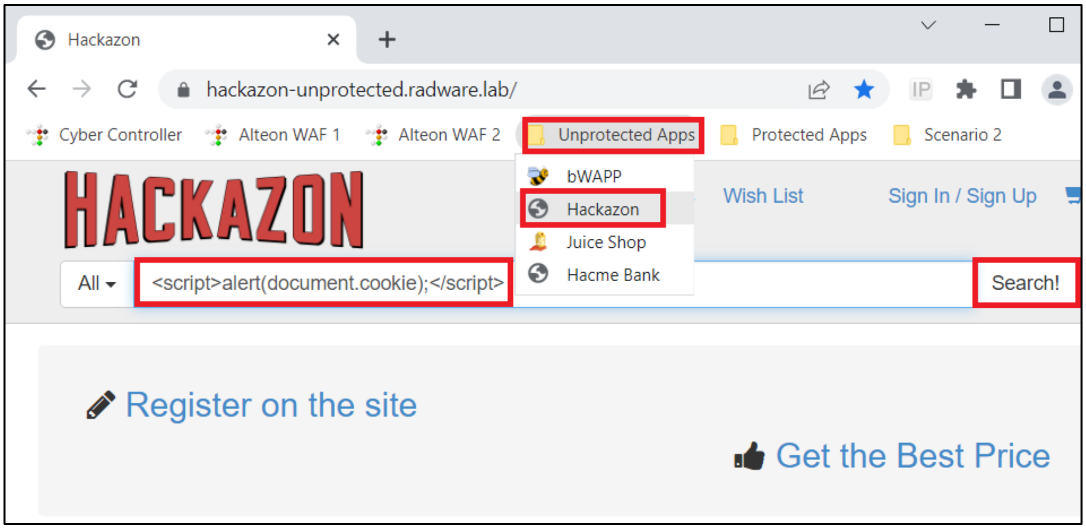
Case Number: 671114091

Scenario 2 – XSS Injection

In this scenario, we will perform an **XSS injection** attack on our website. This specific injection creates an alert pop-up displaying the user's session ID header. In more serious attacks, this information could be sent to a third party, allowing the attacker to hijack the user's session and impersonate them.

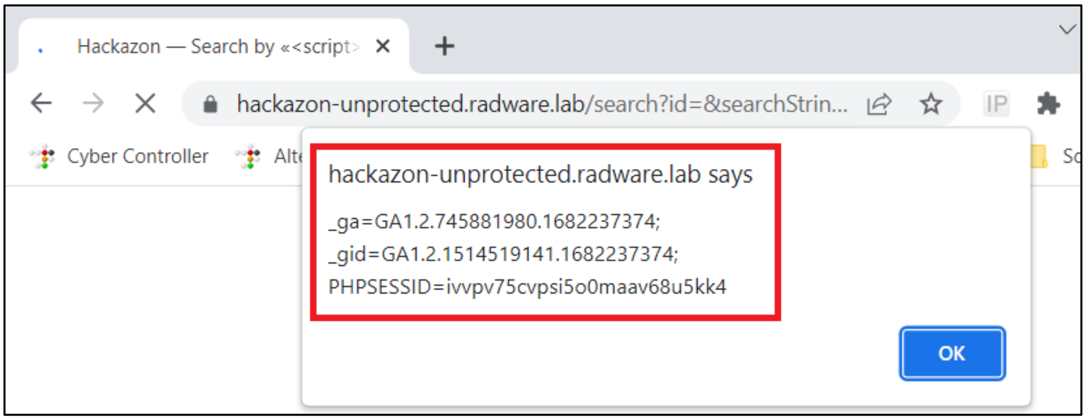
Attack Unprotected Web Application:

- Open **Google Chrome.**
- Open the **Unprotected Apps** Folder located in the **bookmark bar** and click on **Hackazon.**
- Locate the product search bar and enter the following payload:
  <script>alert(document.cookie);</script>
- **Note**: Alternatively, use the shortcut located in the bookmark bar under the Scenario 2 folder, named XSS Unprotected Website.



- Observe the pop-up displaying the PHPSESSID, indicating a successful XSS injection.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

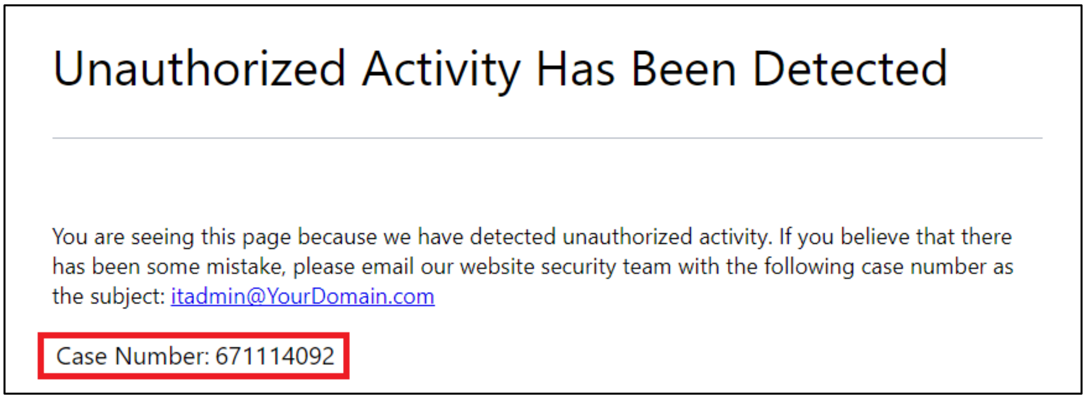

Hackazon — Search by «<script>
hackazon-unprotected.radware.lab/search?id=&searchStrin...
Cyber Controller
Alte
OK

hackazon-unprotected.radware.lab says

_ga=GA1.2.745881980.1682237374;
_gid=GA1.2.1514519141.1682237374;
PHPSESSID=ivvpv75cvpsi5o0maav68u5kk4

Attack Protected Web Application:

- Open the **Protected Apps** Folder located in the **bookmark bar** and click on **Hackazon.**
- Locate the product search bar and enter the following payload: *<script>alert(document.cookie);</script>*
- **Note:** Alternatively, use the shortcut located in the bookmark bar under the Scenario 2 folder, named **XSS Protected Website.**
- Observe that the attack is blocked this time, and a **Security Page** is displayed.
- Copy the **Case Number** to a notepad for the next scenario.



Unauthorized Activity Has Been Detected

You are seeing this page because we have detected unauthorized activity. If you believe that there has been some mistake, please email our website security team with the following case number as the subject: itadmin@YourDomain.com

Case Number: 671114092

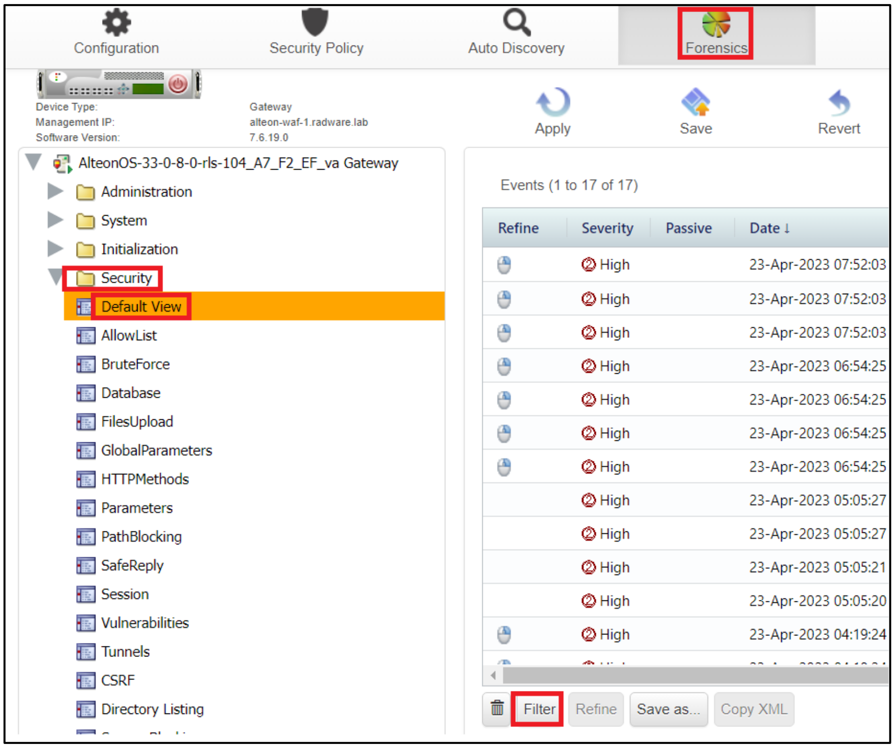
In this scenario, the XSS injection was successful on the unprotected website but was effectively blocked by the Alteon WAF in the protected version of the site.

Scenario 3 – Show Forensics Based on Case Number

In this scenario, we will use the case number from the previous scenario (XSS) security page and search it in Alteon WAF's Forensics to cross between the security page to the security event.

Note: This scenario is based on the security page case number you received in scenario 2.

- Click on **Forensics** tab in the upper menu.
- On the left bar, click on **Default View** under Security folder.
- Click on the **Filter** button.



Device Type: Gateway
Management IP: alteon-waf-1.radware.lab
Software Version: 7.6.19.0

- AlteonOS-33-0-8-0-rls-104_A7_F2_EF_va Gateway
  - Administration
  - System
  - Initialization
  - Security
    - Default View
    - AllowList
    - BruteForce
    - Database
    - FilesUpload
    - GlobalParameters
    - HTTPMethods
    - Parameters
    - PathBlocking
    - SafeReply
    - Session
    - Vulnerabilities
    - Tunnels
    - CSRF
    - Directory Listing

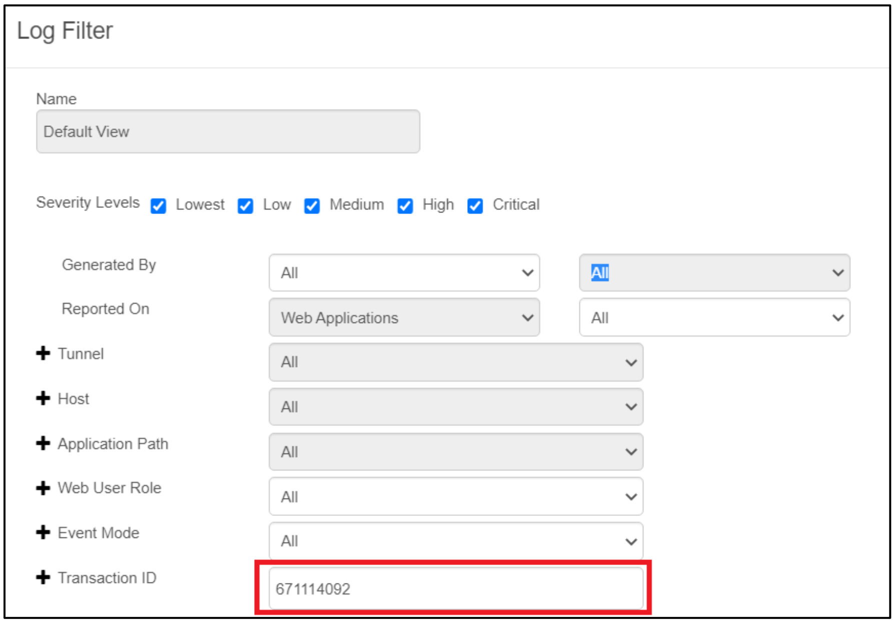
Events (1 to 17 of 17)

Refine	Severity	Passive	Date ↓
●	High		23-Apr-2023 07:52:03
●	High		23-Apr-2023 07:52:03
●	High		23-Apr-2023 07:52:03
●	High		23-Apr-2023 06:54:25
●	High		23-Apr-2023 06:54:25
●	High		23-Apr-2023 06:54:25
●	High		23-Apr-2023 06:54:25
	High		23-Apr-2023 05:05:27
	High		23-Apr-2023 05:05:27
	High		23-Apr-2023 05:05:21
	High		23-Apr-2023 05:05:20
●	High		23-Apr-2023 04:19:24

- Inside the "Transaction ID" field, type the case number and click **OK**.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Log Filter

Name: Default View

Severity Levels ☑ Lowest ☑ Low ☑ Medium ☑ High ☑ Critical

Generated By: All / All

Reported On: Web Applications / All

Tunnel: All

Host: All

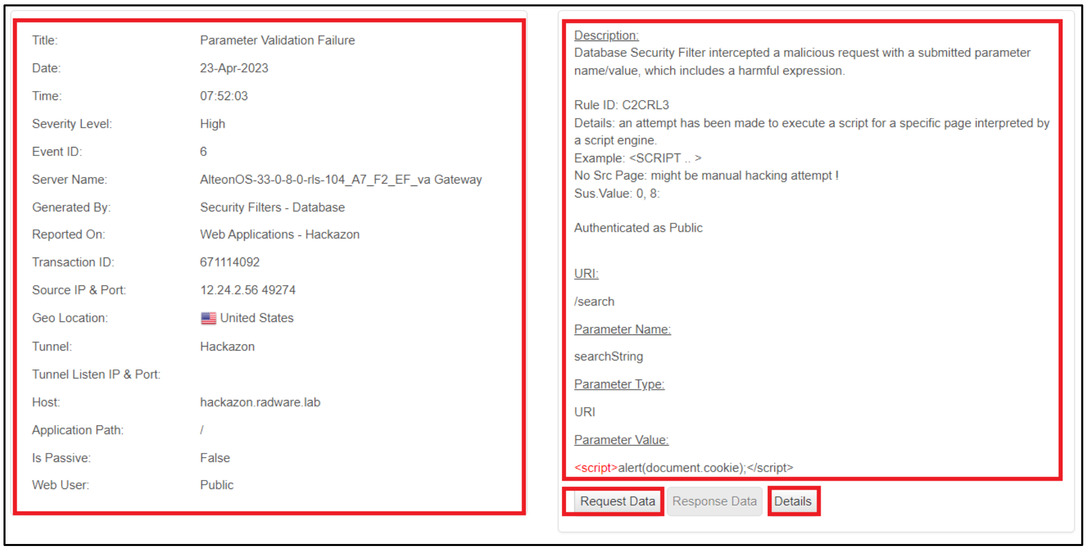
Application Path: All

Web User Role: All

Event Mode: All

Transaction ID: 671114092

- Review the **forensics event**:
  - Note that the attack has created three security events each based on different Rule ID's.
  - You can see what module intercepts the request (Database Filter).
  - **Source IP** address and **Geo Locatio**n.
  - Name of **Tunnel** (Hackazon).
  - **URI**, **Parameter name** and **Parameter value.**
  - Short Description about the attack and pattern number.



Title:	Parameter Validation Failure
Date:	23-Apr-2023
Time:	07:52:03
Severity Level:	High
Event ID:	6
Server Name:	AlteonOS-33-0-8-0-rls-104_A7_F2_EF_va Gateway
Generated By:	Security Filters - Database
Reported On:	Web Applications - Hackazon
Transaction ID:	671114092
Source IP & Port:	12.24.2.56 49274
Geo Location:	United States
Tunnel:	Hackazon
Tunnel Listen IP & Port:	
Host:	hackazon.radware.lab
Application Path:	/
Is Passive:	False
Web User:	Public

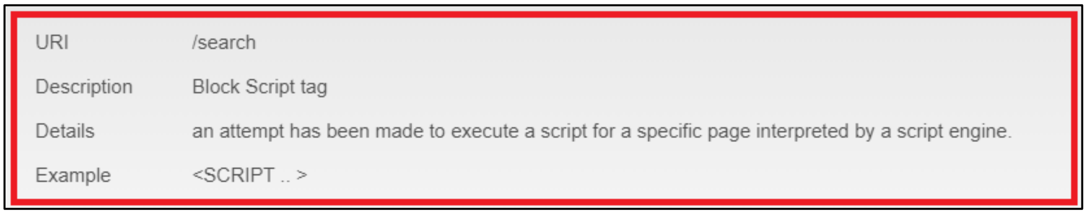
Description:
Database Security Filter intercepted a malicious request with a submitted parameter name/value, which includes a harmful expression.

Rule ID: C2CRL3
Details: an attempt has been made to execute a script for a specific page interpreted by a script engine.
Example: <SCRIPT .. >
No Src Page: might be manual hacking attempt !
Sus.Value: 0, 8:

Authenticated as Public

URI:
/search
Parameter Name:
searchString
Parameter Type:
URI
Parameter Value:
<script>alert(document.cookie);</script>

- Click on **Details** to get more information about the specific pattern that was blocked as well as the general attack type.



URI	/search
Description	Block Script tag
Details	an attempt has been made to execute a script for a specific page interpreted by a script engine.
Example	<SCRIPT .. >

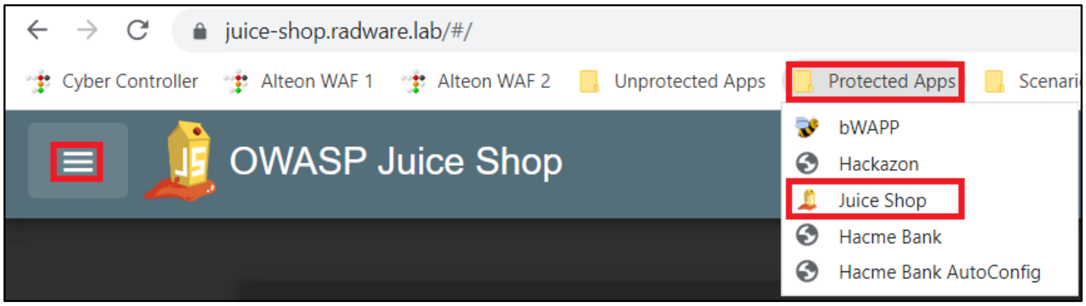
Scenario 4 – Quick Click Refinements

In this scenario, we'll demonstrate one of Alteon WAF's major advantages. One of the protected web applications has added a new static file to the website named legal.md. Since this file type or resource has not been explicitly permitted in the allow list, users trying to access it will get a security page along with a case number. The case number is used by the security administrator to locate the security event in forensics and quickly adjust the security policy to allow this new resource using Quick Click refinement.

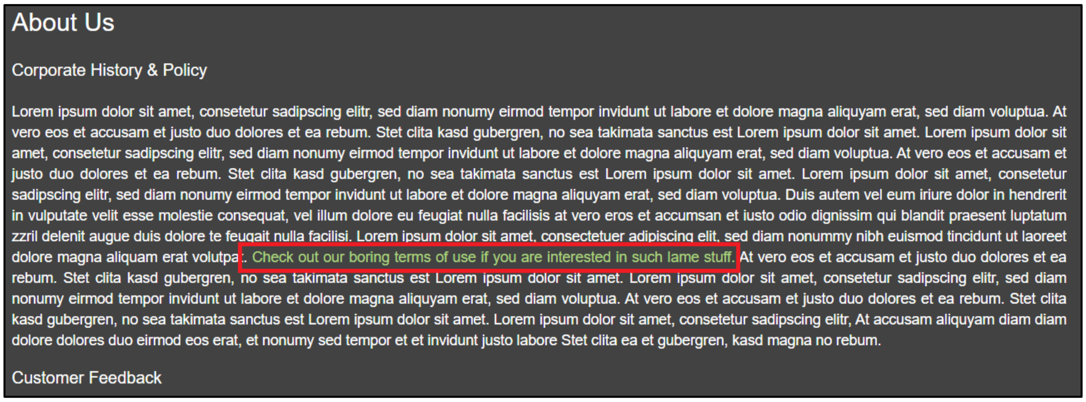
Example of Allow List filter false positive scenario :

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Open **Google Chrome**.
- Access the **Protected Apps** Folder in the **bookmark bar** and select **Juice-Shop**.
- Click the **three lines** icon in the **top-left corner** to **open the side menu**.



- Click **About Us.**
- On the **About Us page**, select the link saying, "***Check out our boring terms of use if you are interested in such lame stuff***."



About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

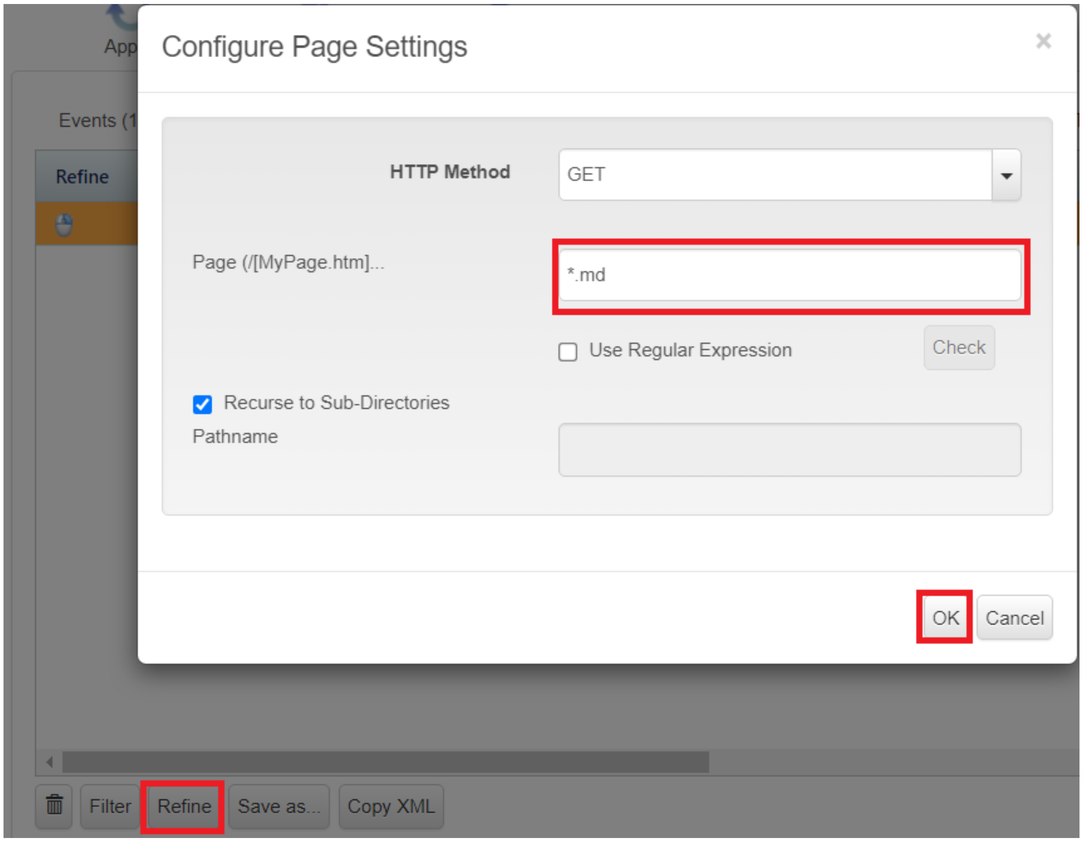
Customer Feedback

- The link tries to open the newly added **legal.md** file.
- **Copy** the **Case number** from the Security page.
- Go to the **Forensics** tab in the upper menu.
- Select **Default View** under the **Security folder** in the left bar.
- Press the **Filter** button.
- Input the **case number** in the "**Transaction ID**" field and click OK.
- Inspect the details in the security event:
  - Identify the module intercepting the request (Allow List Filter)
  - Note the Source IP address and Geo Location.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

  - Check the Name of Tunnel (Juice-Shop) and URI.
- Click "**Request Data**" to access further details and review the HTTP Request.
- Press the **Refine** button, followed by **OK**, and **Apply** to enable clients to open ***.md** resources.



Configure Page Settings

HTTP Method: GET

Page (/[MyPage.htm]...: *.md

☐ Use Regular Expression

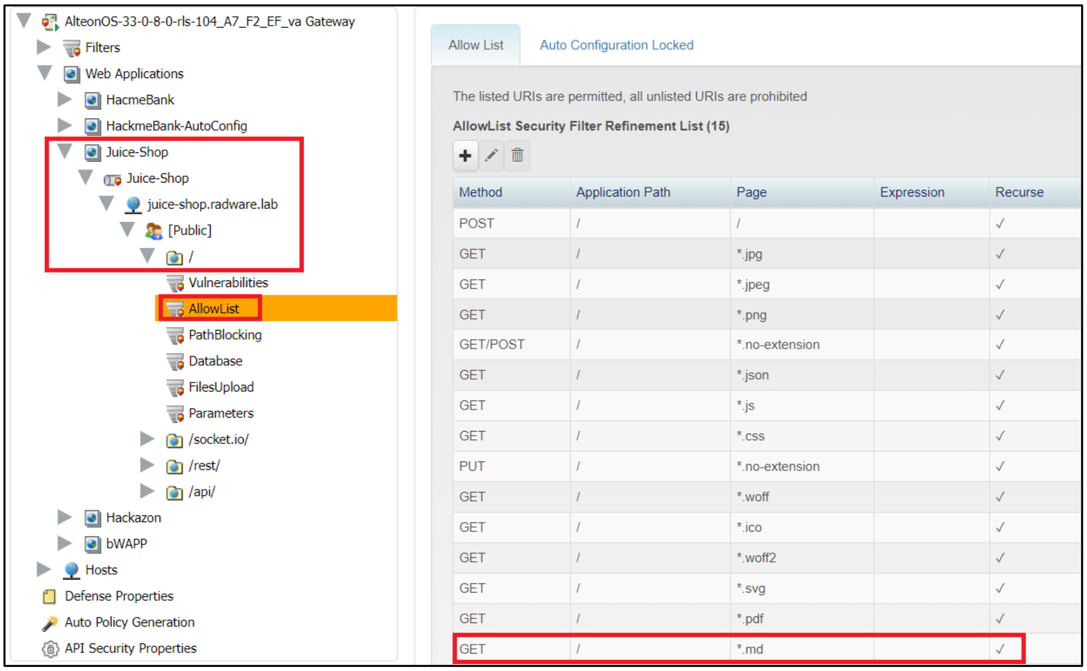
☑ Recurse to Sub-Directories

Pathname:

- To review the new refinement, go to the **Security Policy** tab, Juice-Shop, "juice-**shop.radware.lab**", Public, and click on **Allow List** under the " / " application path.b

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



The listed URIs are permitted, all unlisted URIs are prohibited

AllowList Security Filter Refinement List (15)

Method	Application Path	Page	Expression	Recurse
POST	/	/		✓
GET	/	*.jpg		✓
GET	/	*.jpeg		✓
GET	/	*.png		✓
GET/POST	/	*.no-extension		✓
GET	/	*.json		✓
GET	/	*.js		✓
GET	/	*.css		✓
PUT	/	*.no-extension		✓
GET	/	*.woff		✓
GET	/	*.ico		✓
GET	/	*.woff2		✓
GET	/	*.svg		✓
GET	/	*.pdf		✓
GET	/	*.md		✓

- Browse again to the following link https://juice-shop.radware.lab/ftp/legal.md or click on the ready link in the Bookmark bar under the **Scenario 4 Folder**.

Scenario 5 – Automatic Policy Generation

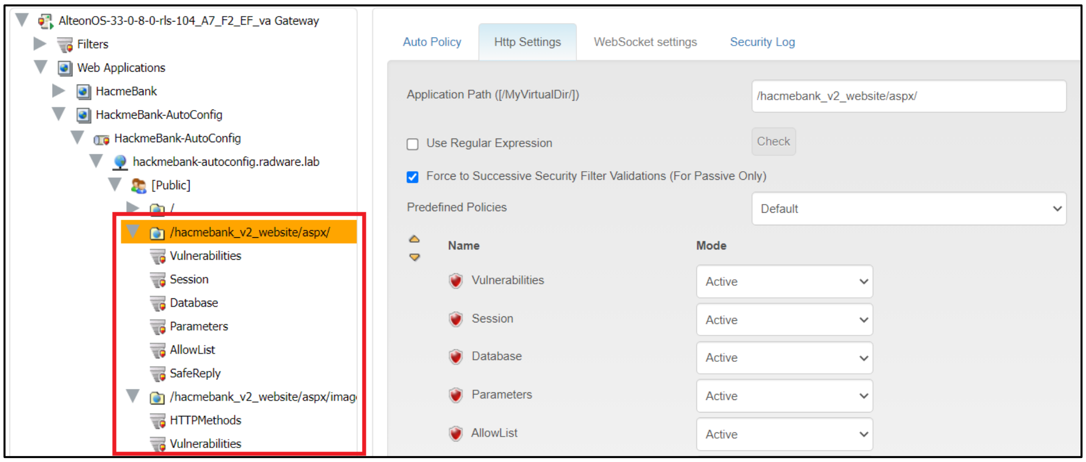
In this scenario, we'll examine the results of Automatic Configuration with a Positive Security Model. Alteon WAF's uses Automatic Policy generation to construct the application structure, apply relevant filters, configure settings for each security filter, refine false positives automatically, and indicate when Automatic Policy generation is complete.

Review Alteon WAF's learning:

- Display the **Application Tree**, showing different security filters based on content.
- Navigate to the **Security Policies** tab, select Web Applications, and click on the "HackmeBank-AutoConfig" web application. Click on Hackmebank-autoconfig.radware.lab, followed by Public.
- Expand both /Hackmebank_v2_website/aspx/ and /Hackmebank_v2_website/images/, showcasing the distinct security filters determined by auto-configuration based on risk.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



AlteonOS-33-0-8-0-rls-104_A7_F2_EF_va Gateway
- Filters
- Web Applications
  - HacmeBank
  - HackmeBank-AutoConfig
    - HackmeBank-AutoConfig
      - hackmebank-autoconfig.radware.lab
        - [Public]
          - /
          - /hacmebank_v2_website/aspx/
            - Vulnerabilities
            - Session
            - Database
            - Parameters
            - AllowList
            - SafeReply
          - /hacmebank_v2_website/aspx/imag
            - HTTPMethods
            - Vulnerabilities

Auto Policy | Http Settings | WebSocket settings | Security Log

Application Path ([/MyVirtualDir/]): /hacmebank_v2_website/aspx/

☐ Use Regular Expression — Check

☑ Force to Successive Security Filter Validations (For Passive Only)

Predefined Policies: Default

Name	Mode
Vulnerabilities	Active
Session	Active
Database	Active
Parameters	Active
AllowList	Active

In this scenario, we demonstrated how Automatic Policy generation enables Alteon WAF to build the application structure and fine-tune the security policy according to the content, risk level, and structure of the web application. This streamlines the process of securing web applications and minimizes the occurrence of false positives.

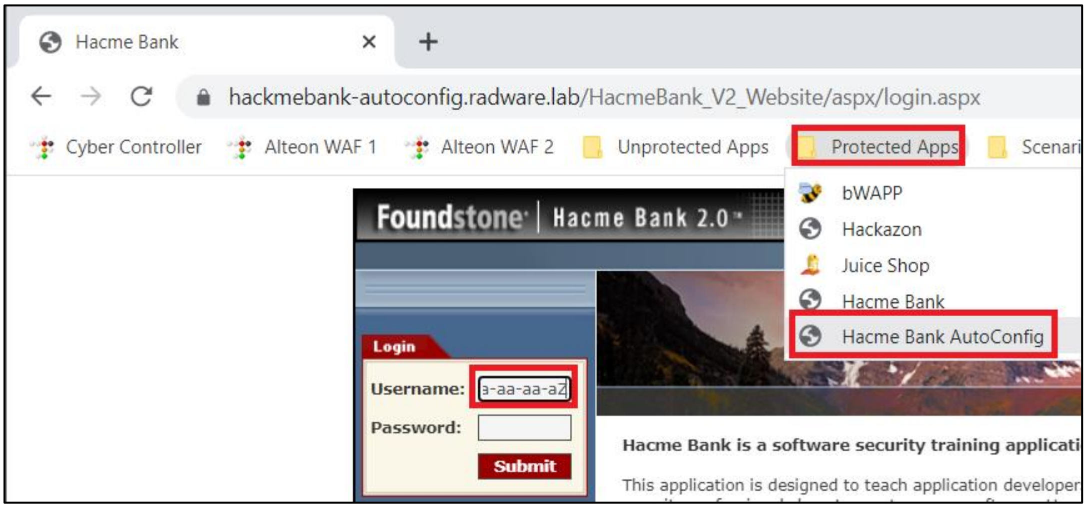
Scenario 6 – Buffer Overflow Attack

In this scenario, we will demonstrate Alteon WAF's Positive Security Model by showcasing parameter configuration after automatic configuration. Based on its learning, Alteon WAF knows that username lengths should range between two and seven characters. We will launch a Buffer Overflow attack by injecting an unexpectedly long value into the username field, typically attempting to overflow the database server buffers.

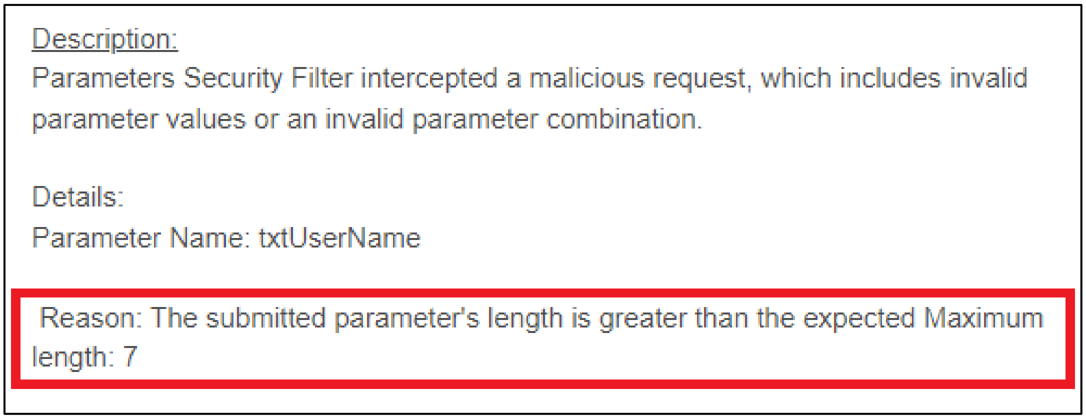
Example of Parameters Filter positive scenario:

- Open **Google Chrome**
- Open the **Protected Apps** Folder located in the **bookmark bar** and click on **Hackme Bank AutoConfig.**
- In the username field copy the following long string: *A123456789a-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aZ*

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.


Hacme Bank
hackmebank-autoconfig.radware.lab/HacmeBank_V2_Website/aspx/login.aspx
Cyber Controller
Alteon WAF 1
Alteon WAF 2
Unprotected Apps
Protected Apps
Scenari
bWAPP
Hackazon
Juice Shop
Hacme Bank
Hacme Bank AutoConfig
Foundstone | Hacme Bank 2.0
Login
Username:
a-aa-aa-aZ
Password:
Submit
Hacme Bank is a software security training applicati
This application is designed to teach application developer

- Click **Submit**, and a Security Page will appear.
- Copy the **Case number** from the Security page.
- Click on **Forensics** tab in the upper menu.
- On the left bar, click on **Default View** under **Security folder.**
- Click on the **Filter button.**
- Type the **case number** into the "**Transaction ID**" field and click **OK**.
- Review **Parameters** in the security event:
  The URI is login.aspx, inside 'txtusername' field, the value was longer than expected and not according to the expected maximum value (7 characters of type String).



Description:
Parameters Security Filter intercepted a malicious request, which includes invalid parameter values or an invalid parameter combination.

Details:
Parameter Name: txtUserName

Reason: The submitted parameter's length is greater than the expected Maximum length: 7

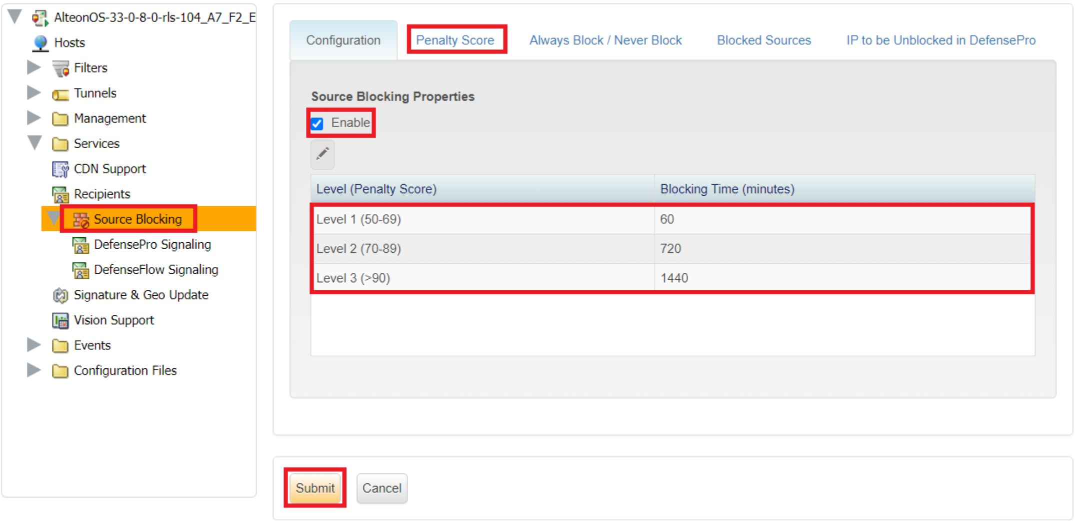
The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

In this scenario, we demonstrated how Alteon WAF's Positive Security Model, including automatic configuration, can detect and block a Buffer Overflow attack. The system identifies when the input value for a parameter exceeds the expected length, preventing potential harm to the application and its underlying database.

Scenario 7 – Source Blocking

In this scenario, we will attack the website with various types of attacks from multiple source IPs and demonstrate the Source Blocking mechanism.

- Under the Configuration tab, open Services and click on Source Blocking.
- In the **Source Blocking** settings, check "**Enable**" in the Configuration Tab, close the warning note, click **Submit**, click **Apply**, and click **Save**.
- Review the Levels and Blocking Times, which means that Alteon WAF blocks a source for 5 minutes when the source reaches a penalty score from 50-69. The score is per threat and found under the "**Penalty Score**" tab.



Source Blocking Properties

☑ Enable

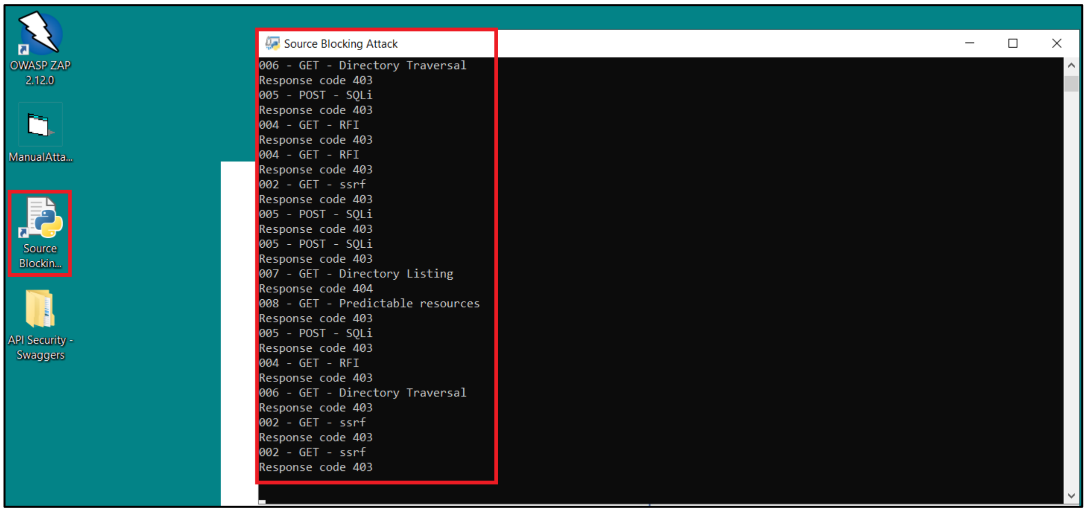
Level (Penalty Score)	Blocking Time (minutes)
Level 1 (50-69)	60
Level 2 (70-89)	720
Level 3 (>90)	1440

- Click on the **Penalty Score** tab to review the score for every threat that the source generates. When a source reaches a score of > 50 (e.g., due to 10 violations of Allow List with a score of 5 for each violation), it will be blocked by Level 1 blocking time for 5 minutes.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

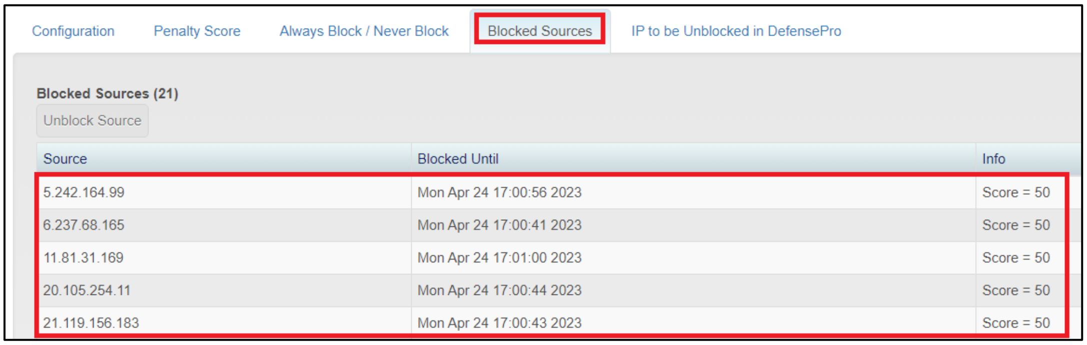
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- On the desktop, there is a shortcut named "**Source Blocking Attack**". Run it to start an attack on the protected website from multiple IP addresses.



```
006 - GET - Directory Traversal
Response code 403
005 - POST - SQLi
Response code 403
004 - GET - RFI
Response code 403
004 - GET - RFI
Response code 403
002 - GET - ssrf
Response code 403
005 - POST - SQLi
Response code 403
005 - POST - SQLi
Response code 403
007 - GET - Directory Listing
Response code 404
008 - GET - Predictable resources
Response code 403
005 - POST - SQLi
Response code 403
004 - GET - RFI
Response code 403
006 - GET - Directory Traversal
Response code 403
002 - GET - ssrf
Response code 403
002 - GET - ssrf
Response code 403
```

- Click on the **Blocked Sources** tab to review the current Blocked Source IP addresses.



Blocked Sources (21)

Source	Blocked Until	Info
5.242.164.99	Mon Apr 24 17:00:56 2023	Score = 50
6.237.68.165	Mon Apr 24 17:00:41 2023	Score = 50
11.81.31.169	Mon Apr 24 17:01:00 2023	Score = 50
20.105.254.11	Mon Apr 24 17:00:44 2023	Score = 50
21.119.156.183	Mon Apr 24 17:00:43 2023	Score = 50

- If you wish to investigate the attacks performed by the source, you can filter events in Forensics based on the IP address.

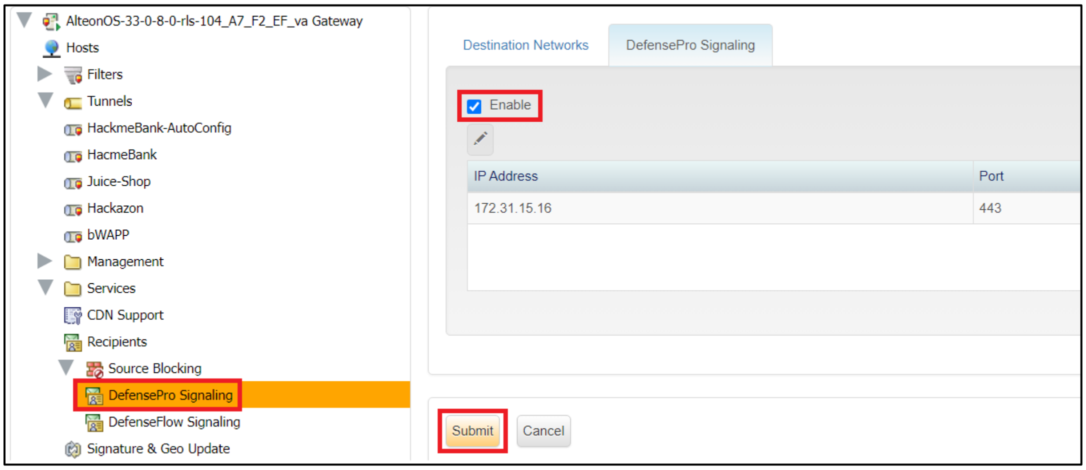
In this scenario, we demonstrated how the Alteon WAF Source Blocking mechanism can effectively block multiple source IPs that perform various types of attacks on the website. By monitoring penalty scores and applying appropriate blocking times, Alteon WAF helps protect the application from potential harm.

Scenario 8 – Defense Signaling

In this scenario, we will demonstrate Defense Signaling by sending the attacker's source IP to the DefensePro located on the network perimeter. Defense Signaling is based on the Source Blocking mechanism demonstrated in the previous scenario.

Activating Defense Signaling:

- In the Security Console, **navigate** to the **Configuration tab**, open **Services**, and click on **Source Blocking**.
- Click on **DefensePro Signaling**, then **click** on the **DefensePro Signaling tab**. Check the Enable box, and click **Submit**, **Apply**, and **Save**.



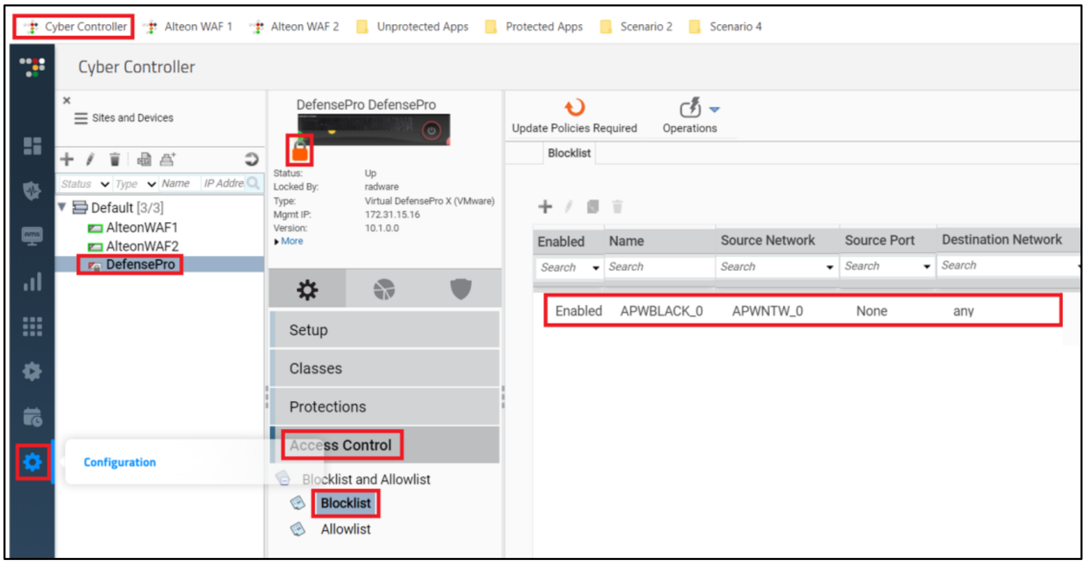
☑ Enable

IP Address	Port
172.31.15.16	443

Attacking the Web Site and Reviewing the DefensePro Blocklist:

- On the desktop, you have a shortcut named "**Source Blocking Attack**". Run it to start an attack on the protected website from multiple IP addresses.
- In **Google Chrome**, click on the **Cyber Controller** shortcut in the Bookmark Bar and log in with the credentials **radware/Radware1!**.
- Access **DefensePro X** and lock it.
- Click on the **Access Control** tab, select **Block List**, and **edit** the first item.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

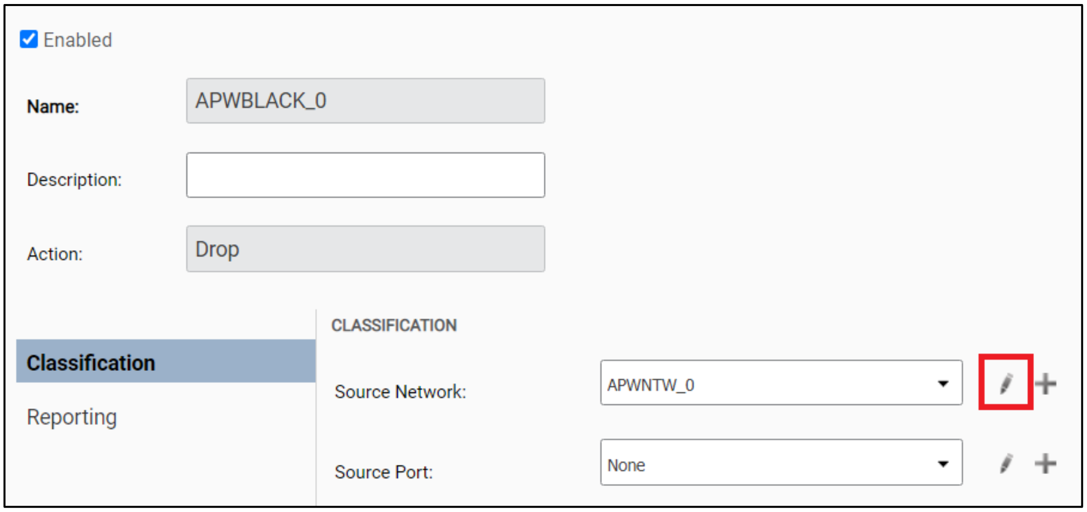


DefensePro DefensePro

Status: Up
Locked By: radware
Type: Virtual DefensePro X (VMware)
Mgmt IP: 172.31.15.16
Version: 10.1.0.0

Enabled	Name	Source Network	Source Port	Destination Network
Enabled	APWBLACK_0	APWNTW_0	None	any

- Edit the Source Network **APWNTW_0**.



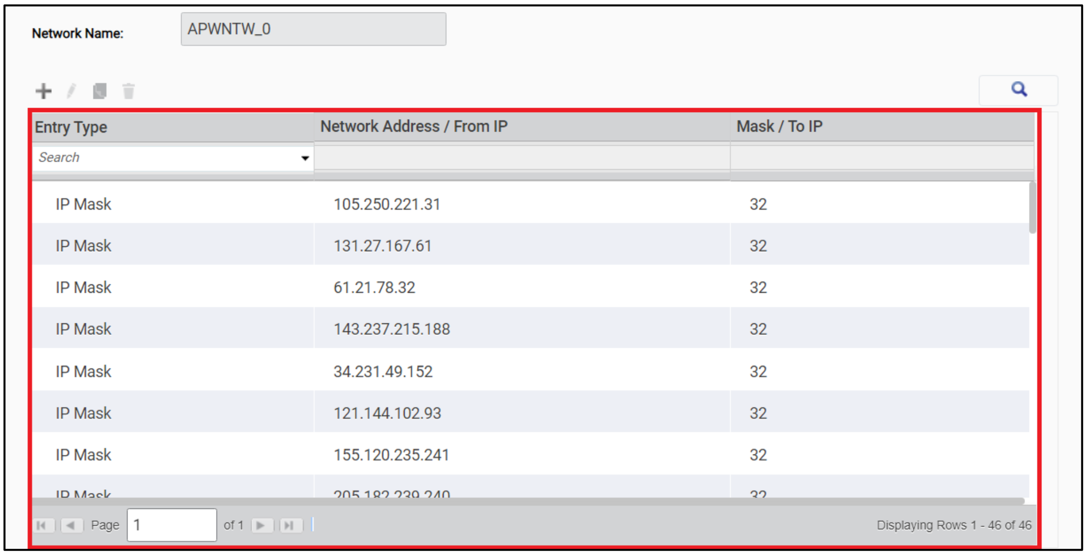
☑ Enabled

Name:	APWBLACK_0
Description:	
Action:	Drop
Source Network:	APWNTW_0
Source Port:	None

- Review the Blocked IP addresses in the DefensePro Blocklist.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Network Name: APWNTW_0

Entry Type	Network Address / From IP	Mask / To IP
IP Mask	105.250.221.31	32
IP Mask	131.27.167.61	32
IP Mask	61.21.78.32	32
IP Mask	143.237.215.188	32
IP Mask	34.231.49.152	32
IP Mask	121.144.102.93	32
IP Mask	155.120.235.241	32
IP Mask	205.182.239.240	32

Displaying Rows 1 - 46 of 46

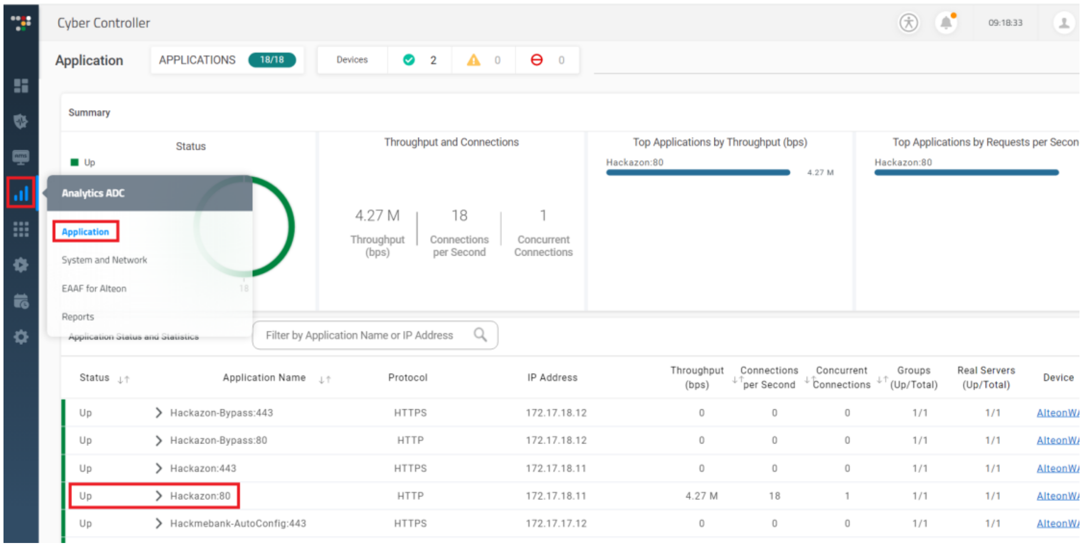
In this scenario, we demonstrated how the Alteon WAF Defense Signaling mechanism can effectively communicate with DefensePro to share attacker source IP information. This collaboration between Alteon WAF and DefensePro helps strengthen the overall security posture by blocking malicious traffic at the network perimeter before it reaches the protected web application.

Scenario 9 – ADC, Security and WAF AMS Analytics Page.

In this scenario, we will demonstrate Cyber Controller Analytics.

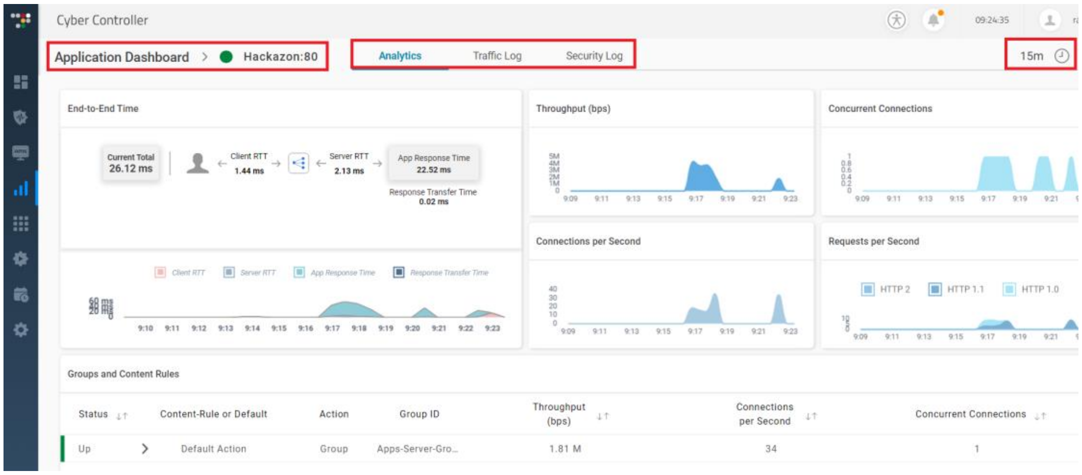
- Open **Google Chrome**.
- From the bookmark bar click on the **Cyber Controller** Shortcut.
- In the left panel, hover over **Analytics ADC**, click **Applications** and then select an application from the application list.

Note: Automatic Traffic is generator for Hackazon:80



Status	Application Name	Protocol	IP Address	Throughput (bps)	Connections per Second	Concurrent Connections	Groups (Up/Total)	Real Servers (Up/Total)	Device
Up	Hackazon-Bypass:443	HTTPS	172.17.18.12	0	0	0	1/1	1/1	AlteonW/
Up	Hackazon-Bypass:80	HTTP	172.17.18.12	0	0	0	1/1	1/1	AlteonW/
Up	Hackazon:443	HTTPS	172.17.18.11	0	0	0	1/1	1/1	AlteonW/
Up	Hackazon:80	HTTP	172.17.18.11	4.27 M	18	1	1/1	1/1	AlteonW/
Up	Hackmebank-AutoConfig:443	HTTPS	172.17.17.12	0	0	0	1/1	1/1	AlteonW/

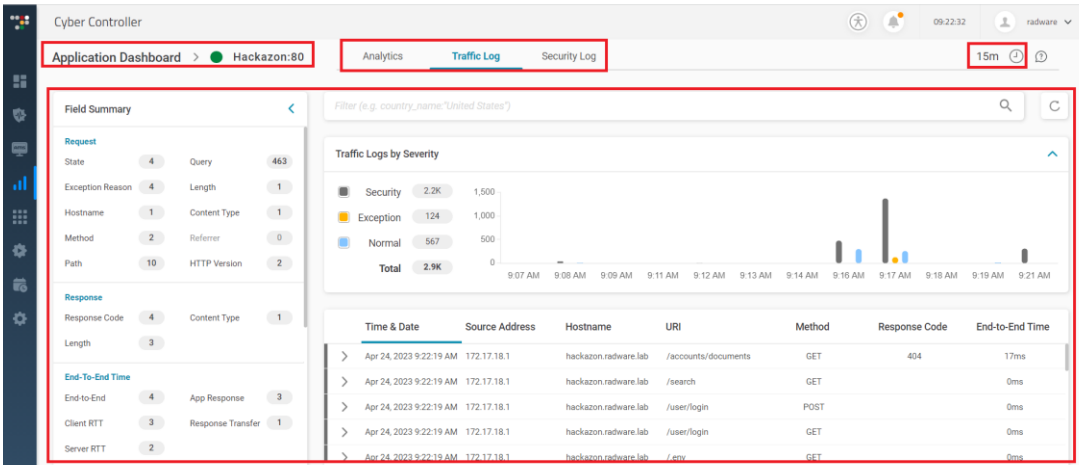
- Access an application that you have generated traffic/security events towards.



Status	Content-Rule or Default	Action	Group ID	Throughput (bps)	Connections per Second	Concurrent Connections
Up	Default Action	Group	Apps-Server-Gro…	1.81 M	34	1

- The analytics page presents various types of widgets displaying the overall traffic load and performance metrics of the application.
- To view detailed logs, click on the **Traffic Log** tab.
- In the Traffic Log section, you can view in depth detail regarding each transaction performed towards the application.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Field Summary

Request

State	4	Query	463
Exception Reason	4	Length	1
Hostname	1	Content Type	1
Method	2	Referrer	0
Path	10	HTTP Version	2

Response

Response Code	4	Content Type	1
Length	3		

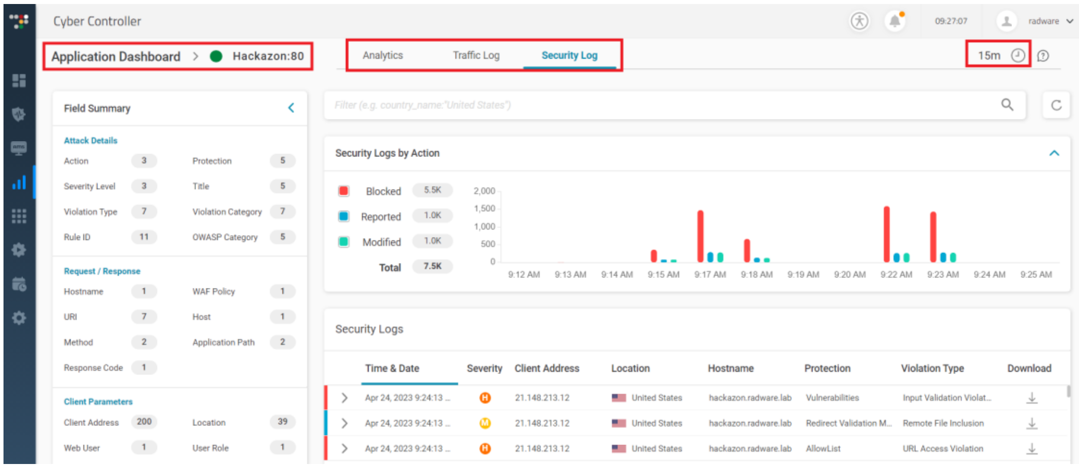
End-To-End Time

End-to-End	4	App Response	3
Client RTT	3	Response Transfer	1
Server RTT	2		

Security	2.2K
Exception	124
Normal	567
Total	2.9K

Time & Date	Source Address	Hostname	URI	Method	Response Code	End-to-End Time
Apr 24, 2023 9:22:19 AM	172.17.18.1	hackazon.radware.lab	/accounts/documents	GET	404	17ms
Apr 24, 2023 9:22:19 AM	172.17.18.1	hackazon.radware.lab	/search	GET		0ms
Apr 24, 2023 9:22:19 AM	172.17.18.1	hackazon.radware.lab	/user/login	POST		0ms
Apr 24, 2023 9:22:19 AM	172.17.18.1	hackazon.radware.lab	/user/login	GET		0ms
Apr 24, 2023 9:22:19 AM	172.17.18.1	hackazon.radware.lab	/.env	GET		0ms

- In the Security Log section, you can view in depth details regarding each Security Event related to the application. performed towards the application.



Field Summary

Attack Details

Action	3	Protection	5
Severity Level	3	Title	5
Violation Type	7	Violation Category	7
Rule ID	11	OWASP Category	5

Request / Response

Hostname	1	WAF Policy	1
URI	7	Host	1
Method	2	Application Path	2
Response Code	1		

Client Parameters

Client Address	200	Location	39
Web User	1	User Role	1

Blocked	5.5K
Reported	1.0K
Modified	1.0K
Total	7.5K

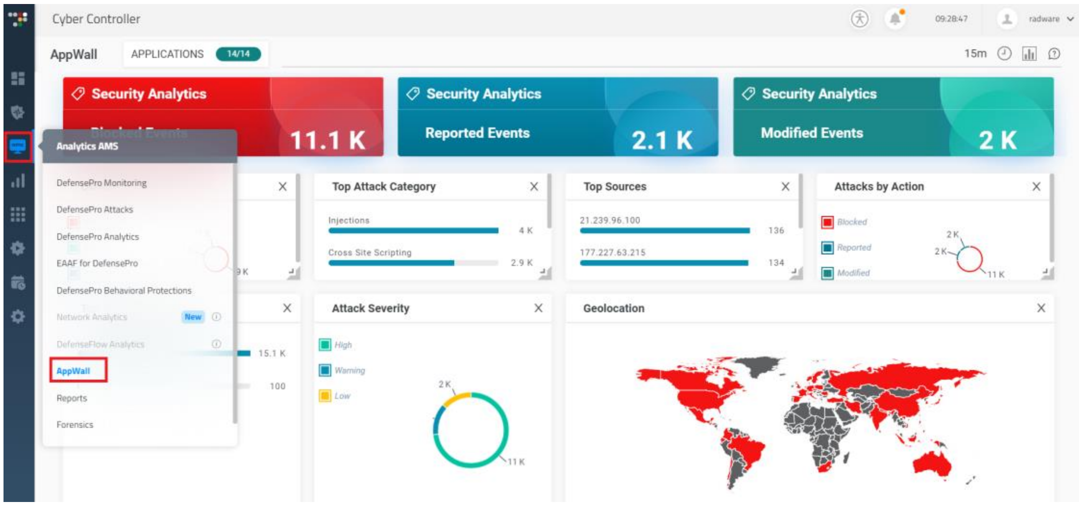
Security Logs

Time & Date	Severity	Client Address	Location	Hostname	Protection	Violation Type	Download
Apr 24, 2023 9:24:13 ...	H	21.148.213.12	United States	hackazon.radware.lab	Vulnerabilities	Input Validation Violat...	↓
Apr 24, 2023 9:24:13 ...	M	21.148.213.12	United States	hackazon.radware.lab	Redirect Validation M...	Remote File Inclusion	↓
Apr 24, 2023 9:24:13 ...	H	21.148.213.12	United States	hackazon.radware.lab	AllowList	URL Access Violation	↓

- To view the **AppWall AMS analytics** page, hover over **Analytics AMS** in the left side panel and click on **AppWall**.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



- Review the Analytics section:
  - OWASP top 10 attacks categories
  - Top Attack category (based on attack type)
  - Top Attackers' Source IPs
  - Top Attack Hosts (when your security policy is based on hosts)
  - Attackers' Geolocation (click on the red countries)

In this scenario, we showcased the Cyber Controller Analytics feature, which allows you to monitor and analyze application traffic and security events. The Analytics section provides valuable insights into various attack categories, attacker source IPs, attack hosts, and the geographical locations of attackers, helping you understand the security landscape and improve the overall protection of your web applications.

API Security Module

In this section, we will provide an overview of Alteon WAF's API Security module. Through the following scenarios, we will demonstrate various API-based requests using Postman, which has been preconfigured with requests related to these scenarios.

These requests include legitimate authorization, brute force, SQL injection, schema violation, and more, effectively demonstrating the value of API Protection. In the final scenario, we will explore the endpoint configuration within the Alteon WAF Security Console to examine the uploaded API schema file, upload a new version of a schema file, and use the Merge feature.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

Alteon WAF's API Security offers various ways to integrate with an application's API development life cycle. It provides additional API-focused positive security-based protection by allowing users to automate, define, upload, and merge the application API schema.

The API schema is a document that maps out the API catalog, consisting of endpoint paths and HTTP methods. For each endpoint, the document specifies related headers, parameters, authorization, and body-related elements. This gives Alteon WAF a map of what is "allowed" in terms of API requests and, consequently, what is "not allowed."

Once an initial schema is applied, schema enforcement can begin, enabling quota management, endpoint editing, and switching between report-only and block modes, as well as block-no-report for deprecated endpoints. The Merge options allow for customized continuous updating of the schema via the Security console or using Rest API for integration into the CI/CD pipeline.

Scenario 1 – Rate Limiting

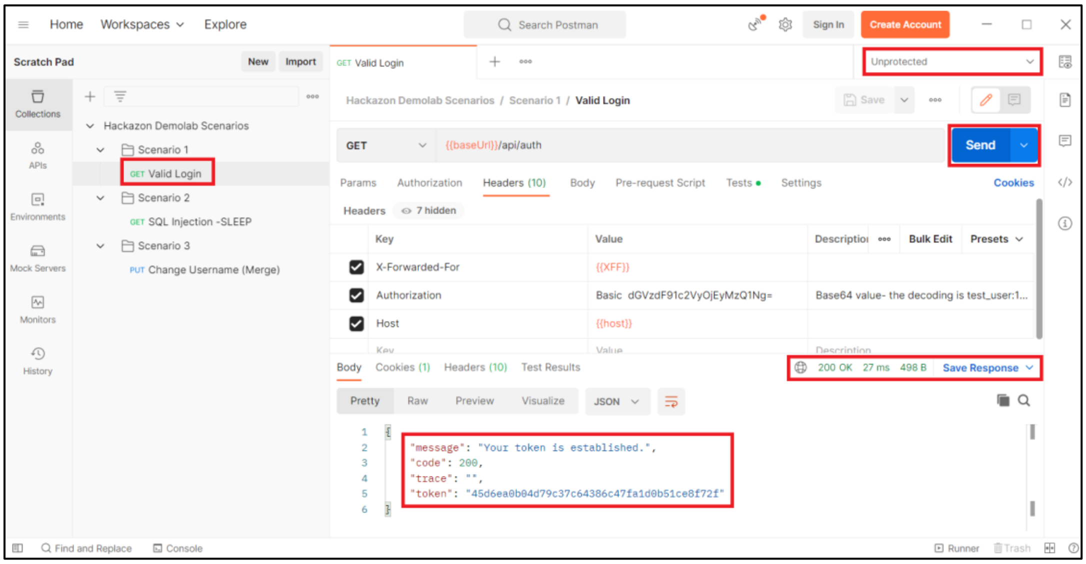
In this scenario, we'll showcase a quota limit for the authentication endpoint. The API Security configuration for the Hackazon website sets the quota limit for the authentication endpoint to 5 requests per minute. This means that when a sixth request is sent from the same source within a minute, it will be blocked.

APIs are more susceptible to automated attacks due to their constant exposure and lack of client-side, session, or other protective mechanisms. A best practice for API security is quota management, which enables customers to set a reasonable limit on the number of hits an endpoint can receive from a specific source within a specified time frame.

Testing multiple authentication requests on the unprotected version of the website:

- Launch the "**Postman**" application from the desktop.
- Open **Hackazon Demolab** Scenarios, then select **Scenario 1** and click on the "**Valid Login**" Request.
- Click the **Send** button.
- Observe the response at the bottom displaying the successful login and authorization token.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Unprotected

Hackazon Demolab Scenarios / Scenario 1 / Valid Login

GET {{baseUrl}}/api/auth

Headers 7 hidden

	Key	Value	Description
☑	X-Forwarded-For	{{XFF}}	
☑	Authorization	Basic dGVzdF91c2VyOjEyMzQ1Ng=	Base64 value- the decoding is test_user:1...
☑	Host	{{host}}	

200 OK 27 ms 498 B

```
{
"message": "Your token is established.",
"code": 200,
"trace": "",
"token": "45d6ea0b04d79c37c64386c47fa1d0b51ce8f72f"
}
```

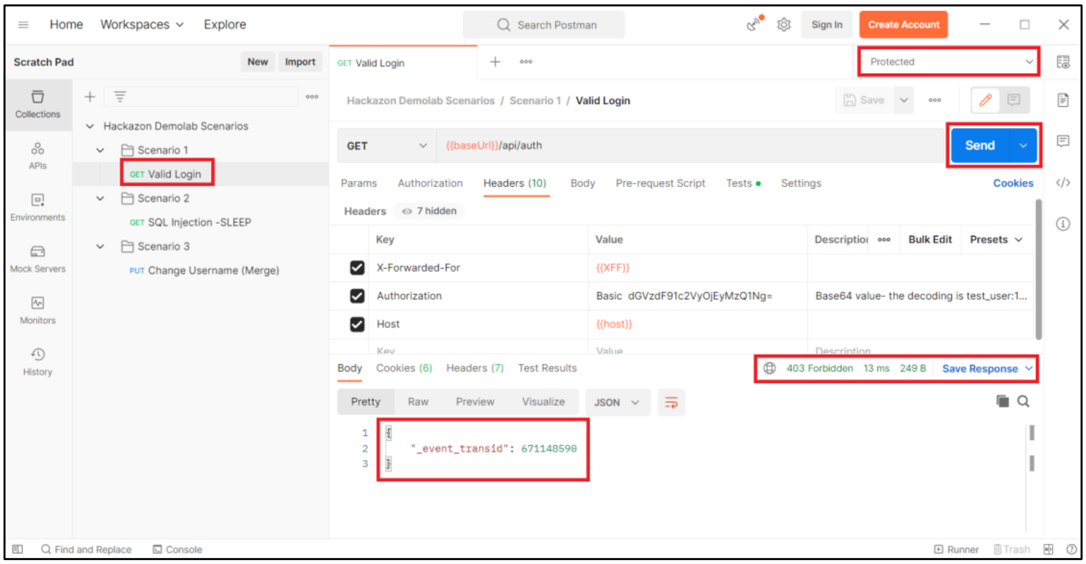
- Click **Send** 5 more times.
- Notice that nothing changes and the login function still works.

Testing multiple authentication requests on the protected version of the website:

- **Switch** to the **Protected** environment
- Click on the **Send** button.
- Observe the response at the bottom displaying the successful login and authorization token.
- Click **Send** 5 more times.
- Notice that the response switches from status code 200 to status code 403, displaying a security message with the transaction ID in JSON format

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



GET {{baseUrl}}/api/auth

	Key	Value	Description
☑	X-Forwarded-For	{{XFF}}	
☑	Authorization	Basic dGVzdF91c2VyOjEyMzQ1Ng=	Base64 value- the decoding is test_user:1...
☑	Host	{{host}}	

403 Forbidden 13 ms 249 B

```
{
    "_event_transid": 671148590
}
```

In this scenario, we demonstrated the effectiveness of quota management in API Security for safeguarding an authentication endpoint against abuse or automated attacks. By establishing a reasonable limit on the number of requests permitted from a specific source within a set time frame, the system helps maintain overall web application security. When the limit is surpassed, the response changes to a security message with a status code of 403, blocking further requests.

Scenario 2 – API Based Blind SQL injection.

In this scenario, we will showcase a blind SQL injection attack on an API. A blind SQL injection is an attack where the attacker cannot see the payload's response. In this case, the payload is an SQL Sleep command, which instructs the database to "Sleep" for 5 seconds. We can observe the attack's impact by measuring the response time.

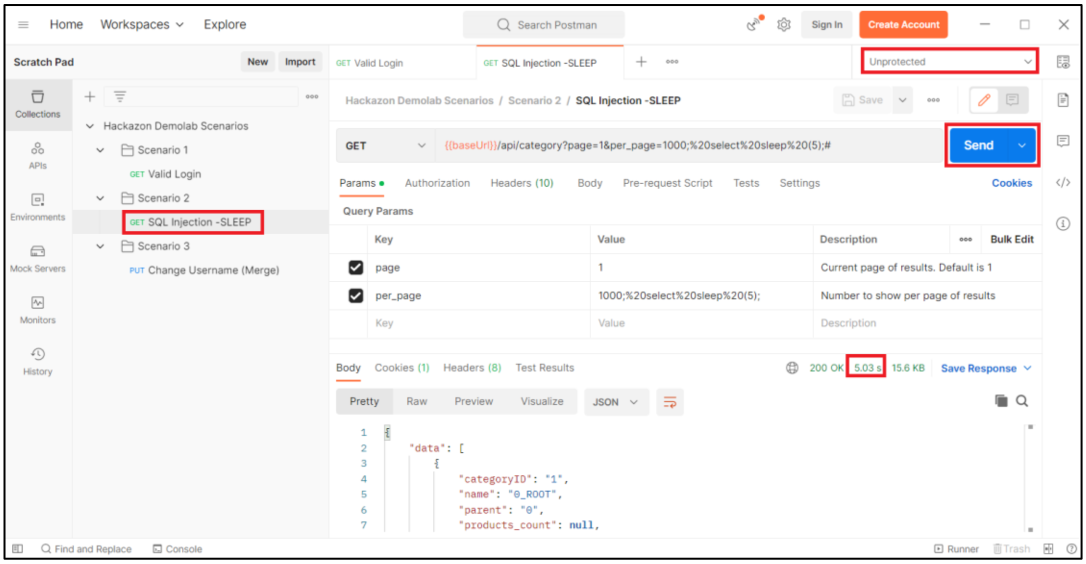
Attack Unprotected Web Application's API Endpoint:

- Open "**Postman**".
- Open **Hackazon Demolab** Scenarios, then select **Scenario 2**.
- Click on the "**SQL Injection - Sleep**" request.
- Ensure the **Environment** is set to **Unprotected**.
- Press the **Send** button.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Observe the 5-second response time.



Unprotected

GET {{baseUrl}}/api/category?page=1&per_page=1000;%20select%20sleep%20(5);#

Query Params

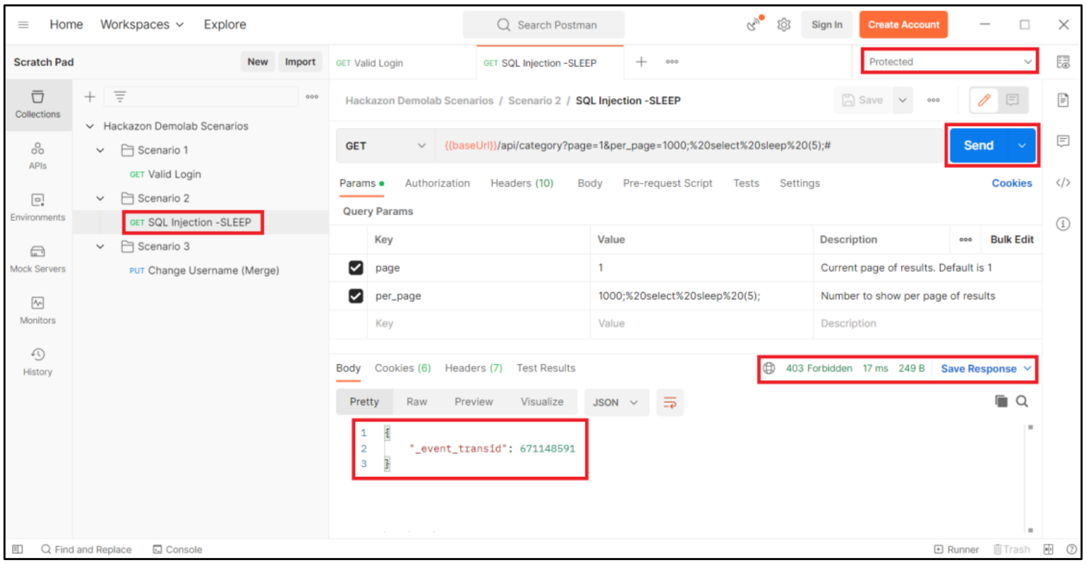
	Key	Value	Description
☑	page	1	Current page of results. Default is 1
☑	per_page	1000;%20select%20sleep%20(5);	Number to show per page of results
	Key	Value	Description

200 OK 5.03 s 15.6 KB

```
{
    "data": [
        {
            "categoryID": "1",
            "name": "0_ROOT",
            "parent": "0",
            "products_count": null,
```

Attack Protected Web Application's API Endpoint:

- Switch to the **Protected** Environment and press **Send**.
- Notice that the attack is blocked, and the response is the API Security page.



Protected

GET {{baseUrl}}/api/category?page=1&per_page=1000;%20select%20sleep%20(5);#

Query Params

	Key	Value	Description
☑	page	1	Current page of results. Default is 1
☑	per_page	1000;%20select%20sleep%20(5);	Number to show per page of results
	Key	Value	Description

403 Forbidden 17 ms 249 B

```
{
    "_event_transid": 671148591
}
```

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

Scenario 3 – Updating and Merging New Swagger Schema

In this scenario, we will demonstrate the process of updating and merging a new Swagger schema in Alteon WAF. The developers of the web application have issued an updated Swagger file that hardens the requirements for the username and email fields in the body of a PUT request for the /api/user/ endpoint. Instead of defining the parameters as strings, the developers have used regex patterns to define valid email addresses and usernames, allowing only those that match the patterns as values.

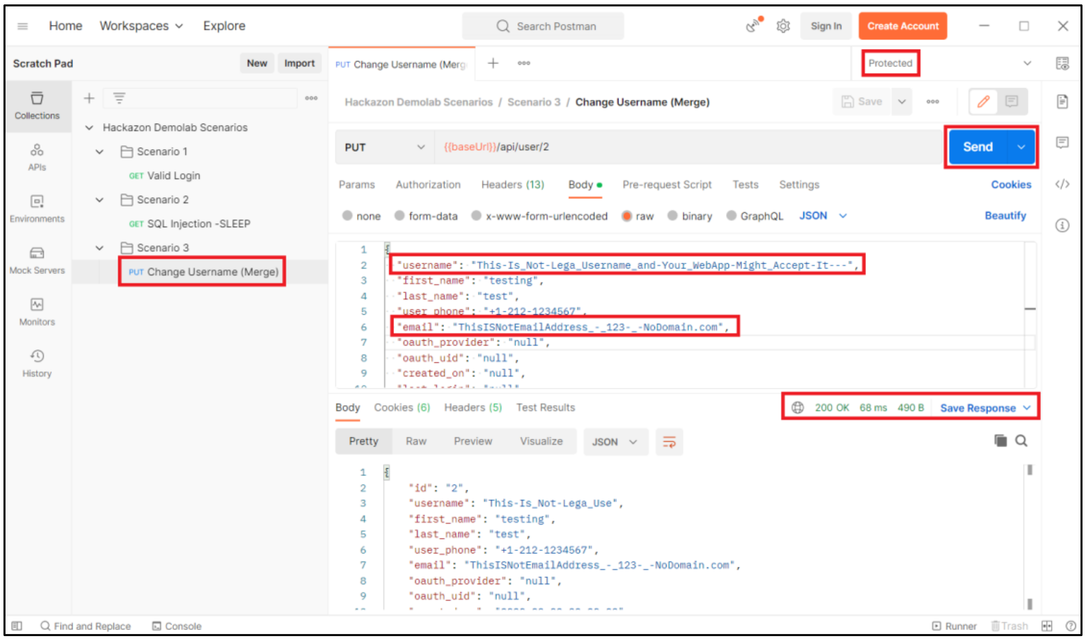
Note: Both Swagger files are located inside the API – Swagger folder on the desktop. To compare the two, you can use the compare tool in Notepad++.

When loading a new version of a Swagger file onto Alteon WAF, it is done through a process called "merge." This process allows control over which parts of the new Swagger file to adopt and whether to retain or merge parts of the old Swagger file.

Testing changes in the username and email before merging the new schema:

- Open "**Postman**".
- Open **Hackazon Demolab** Scenarios, then select **Scenario 3**.
- Click on the "**Change Username**" request.
- Observe that the body parameters (username and email address) do not conform to the usual format for those types of parameters.
- Ensure the **Environment** is set to **Protected**.
- Click "**Send**" and notice that the change is successful.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Hackazon Demolab Scenarios / Scenario 3 / Change Username (Merge)

PUT {{baseUrl}}/api/user/2

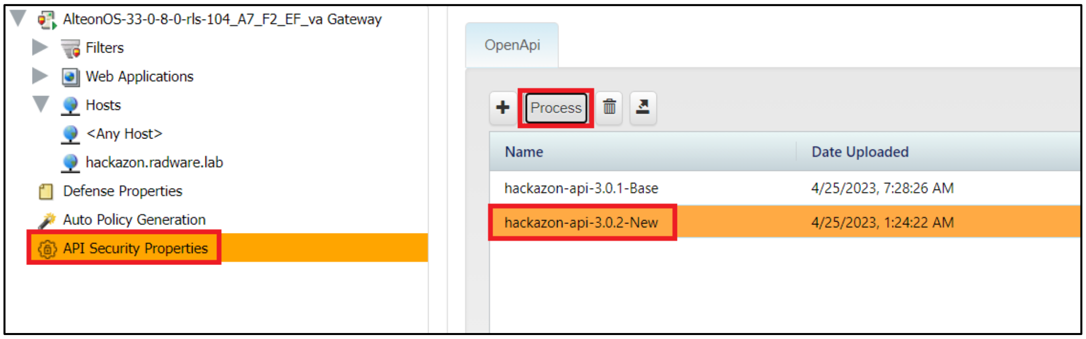
```
{
"username": "This-Is_Not-Lega_Username_and-Your_WebApp-Might_Accept-It---",
"first_name": "testing",
"last_name": "test",
"user_phone": "+1-212-1234567",
"email": "ThisISNotEmailAddress_-_123-_-NoDomain.com",
"oauth_provider": "null",
"oauth_uid": "null",
"created_on": "null",
```

200 OK 68 ms 490 B

```
{
    "id": "2",
    "username": "This-Is_Not-Lega_Use",
    "first_name": "testing",
    "last_name": "test",
    "user_phone": "+1-212-1234567",
    "email": "ThisISNotEmailAddress_-_123-_-NoDomain.com",
    "oauth_provider": "null",
    "oauth_uid": "null",
```

Uploading and merging the new Swagger schema:

- In **Google Chrome**, open Alteon WAF's **Security Console** and navigate to the **Security Policy** tab.
- Click on **API Security Properties**, where Swagger files are uploaded.
- Note that Hackazon-api-3.0.1-Base Schema has already been processed.
- Click on **Hackazon-api-3.0.2-New** and click "**Process**" to open the API Security – **Host Mapping** Window.



Name	Date Uploaded
hackazon-api-3.0.1-Base	4/25/2023, 7:28:26 AM
hackazon-api-3.0.2-New	4/25/2023, 1:24:22 AM

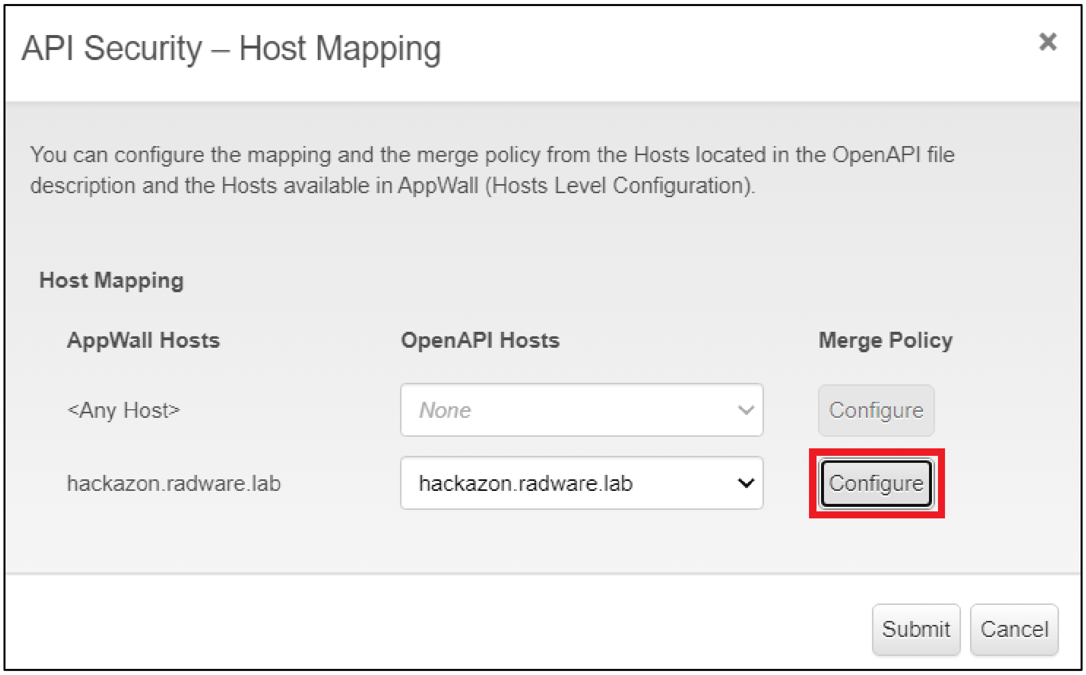
- Host Mapping allows you to assign the schema file to any host configured in Alteon WAF's Security Console, enabling merging to different hosts, such as pre-production.

Configuring the merge policy:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Click on the configure button beside the **Hackazon.radware.lab** host to set up the merge policy.



API Security – Host Mapping

You can configure the mapping and the merge policy from the Hosts located in the OpenAPI file description and the Hosts available in AppWall (Hosts Level Configuration).

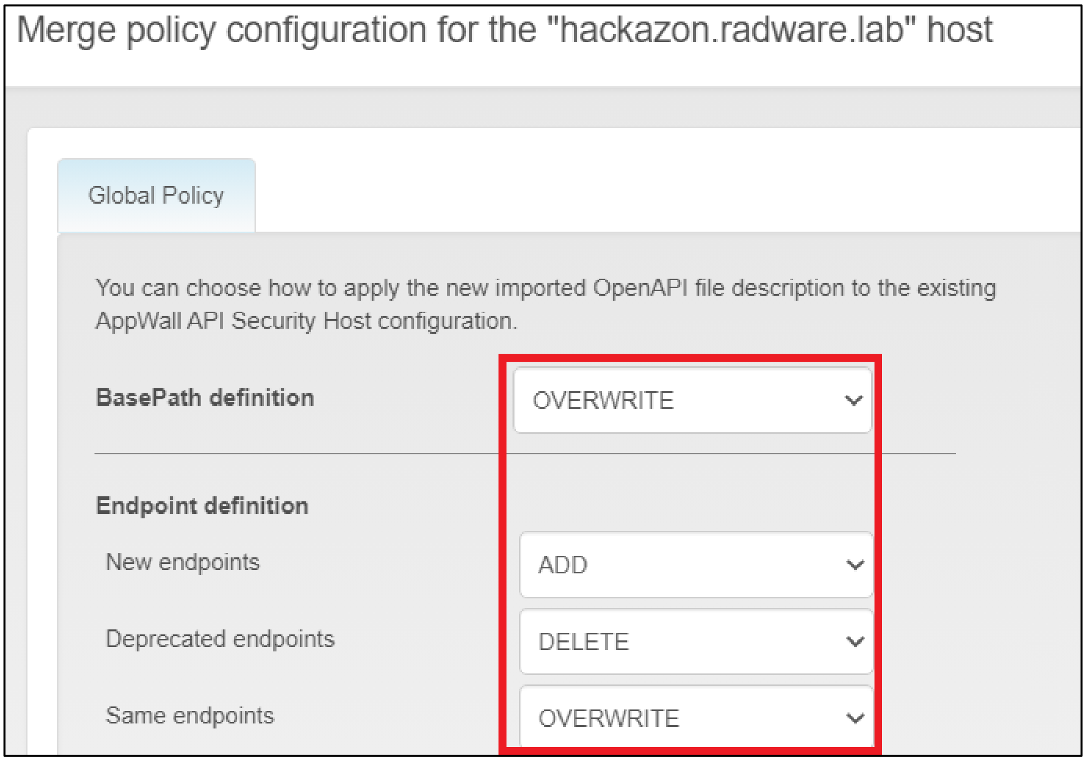
Host Mapping

AppWall Hosts	OpenAPI Hosts	Merge Policy
<Any Host>	None	Configure
hackazon.radware.lab	hackazon.radware.lab	Configure

- The merge flow starts with determining the most general aspects to merge, moving down to the most specific aspects.
- Set the following options for the **merge policy** in this scenario:
  - **BasePath definition**: OVERWRITE
  - **New endpoints**: ADD
  - **Deprecated endpoints**: DELETE
  - **Same endpoints**: OVERWRITE

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Merge policy configuration for the "hackazon.radware.lab" host

You can choose how to apply the new imported OpenAPI file description to the existing AppWall API Security Host configuration.

BasePath definition: OVERWRITE

Endpoint definition

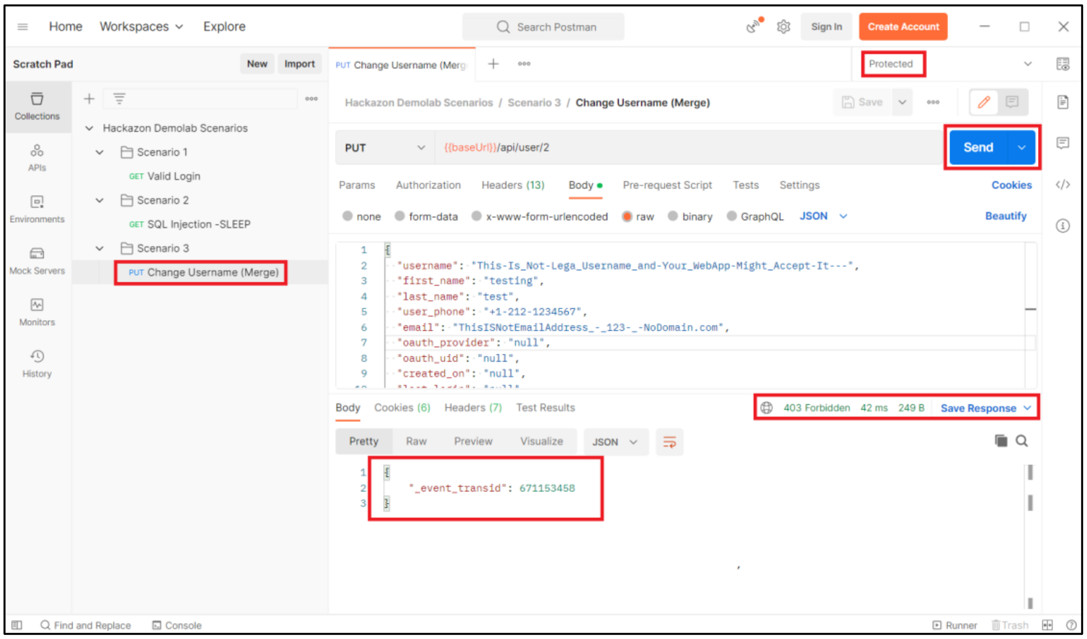
- New endpoints: ADD
- Deprecated endpoints: DELETE
- Same endpoints: OVERWRITE

- Click "**Save**," then "**Submit**" and "**Apply**."

Testing the updated schema:

- Open **Postman** after the merge process is complete.
- Resend the "**Change Username**" request to the **Protected Environment**.
- Observe that the response is now an API Security page, indicating that the change was unsuccessful due to the updated schema. This demonstrates that the new schema has taken effect and enforces stricter requirements for the username and email fields.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



```
PUT {{baseUrl}}/api/user/2
```

```
{
  "username": "This-Is_Not-Lega_Username_and-Your_WebApp-Might_Accept-It---",
  "first_name": "testing",
  "last_name": "test",
  "user_phone": "+1-212-1234567",
  "email": "ThisISNotEmailAddress_-_123-_-NoDomain.com",
  "oauth_provider": "null",
  "oauth_uid": "null",
  "created_on": "null",
```

```
{
   "_event_transid": 671153458
}
```

Scenario 4 – Show events

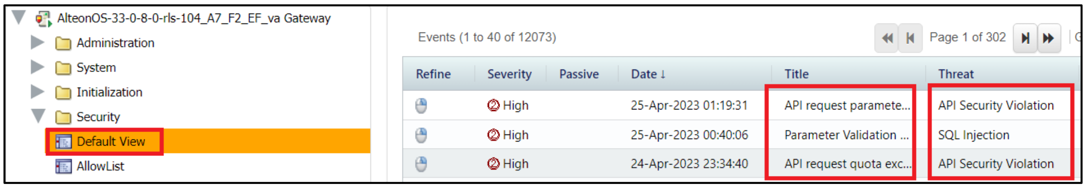
In this scenario, we will demonstrate the new API Security events within the Alteon WAF's Forensics tab.

Accessing the Forensics tab:

- In the Alteon WAF Security Console, click on the "**Forensics**" tab.
- Click on "**Security**" and then on "**API Security**."

Observing the API Security events:

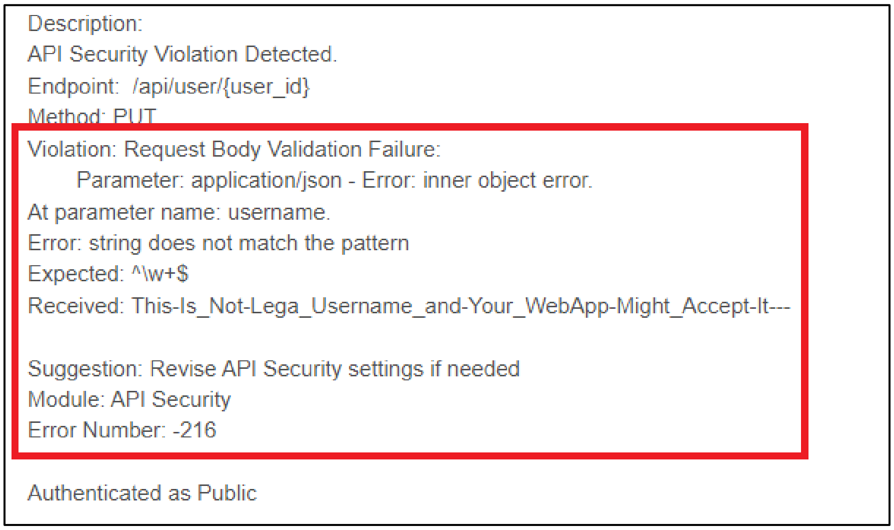
- Notice that both the "**Over Quota Event**" and the "**Schema Violation Event**" are of the type "**API Security Violation**," while the "**SQL Injection**" event remains the same.



Refine	Severity	Passive	Date ↓	Title	Threat
	High		25-Apr-2023 01:19:31	API request paramete...	API Security Violation
	High		25-Apr-2023 00:40:06	Parameter Validation ...	SQL Injection
	High		24-Apr-2023 23:34:40	API request quota exc...	API Security Violation

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Examining the "**Schema Violation Event**" reveals that the strings we have entered do not match the pattern enforced within the Open API schema.



```
Description:
API Security Violation Detected.
Endpoint:  /api/user/{user_id}
Method: PUT
Violation: Request Body Validation Failure:
       Parameter: application/json - Error: inner object error.
At parameter name: username.
Error: string does not match the pattern
Expected: ^\w+$
Received: This-Is_Not-Lega_Username_and-Your_WebApp-Might_Accept-It---

Suggestion: Revise API Security settings if needed
Module: API Security
Error Number: -216

Authenticated as Public
```

This scenario demonstrates how the Alteon WAF Forensics tab displays API Security events, providing users with valuable insights into security violations and helping them identify potential vulnerabilities and malicious activities.

Bot Manager Module

In this section we will provide a quick overview of Bot manager and then demonstrate three types of bot behaviors and bot attacks.

In this section, we will provide a comprehensive overview of the Bot Manager and demonstrate three different types of bot behaviors and bot attacks. Bot Management is essential for any publicly accessible web asset, as sophisticated bots today are capable of exploiting vulnerabilities, misusing features, and accessing data within a web application.

One of the main challenges in bot management is discerning between good bots, bad bots, and regular users. Bot Manager employs advanced techniques such as machine learning, signature analysis, behavioral analysis, and even blockchain technology to accurately differentiate between good bots, bad bots, and legitimate users.

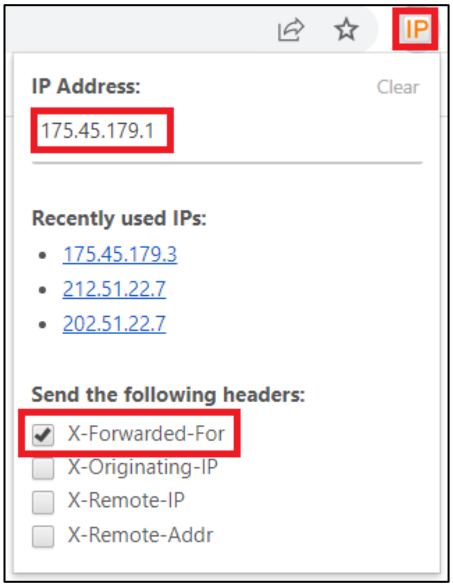
The protection offered by Bot Manager is crucial and complementary to any WAF-based protection system, as it possesses the capability to address attacks that traditional WAFs are not designed to defend against.

Scenario 1 – Browser Anomaly

In this scenario, we will demonstrate how Bot Manager can detect a fake user-agent by comparing the user-agent header with the browser driver's fingerprint. Bot Manager's fingerprinting identifies discrepancies between the browser drivers and the user-agent provided by the bot. We will use a Chrome plugin called User Agent Switcher to alter the user-agent value.

To attack the unprotected website:

- Open **Google Chrome.**
- Set **X-Forwarded-For** Header to IP **175.45.179.1**.



IP Address: 175.45.179.1

Clear

Recently used IPs:

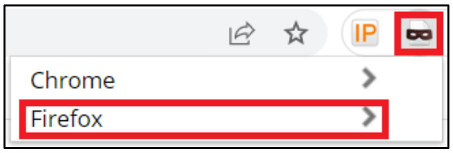
- 175.45.179.3
- 212.51.22.7
- 202.51.22.7

Send the following headers:

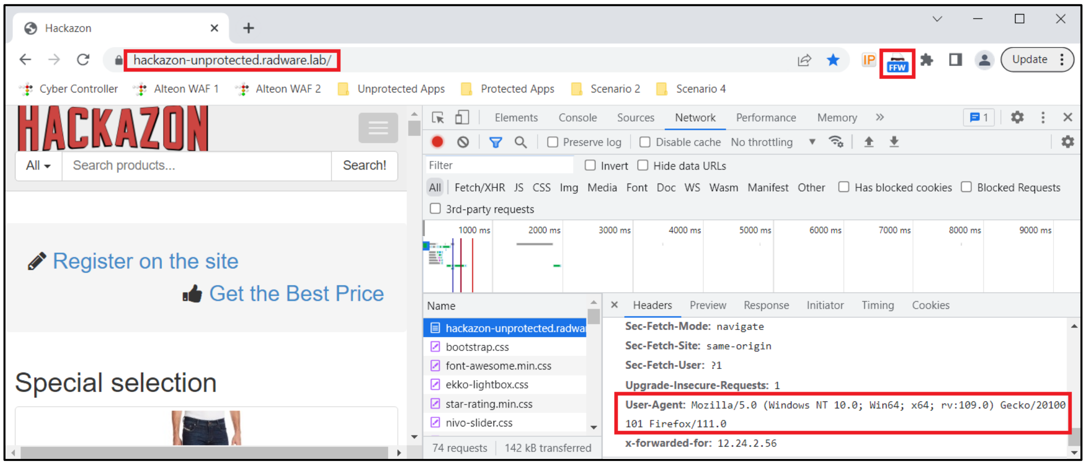
☑ X-Forwarded-For
□ X-Originating-IP
□ X-Remote-IP
□ X-Remote-Addr

- Set **Chrome UA Spoofer** to "**Windows Firefox 111**" Note that the letters "**FFW**" appear, indicating that the Firefox User-Agent is being used.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



- Open Developer Tools (Ctrl + Shift + I or F12 key) and switch to the Network tab.
- Open the **Unprotected Apps** Folder located in the **bookmark bar** and click on **Hackazon.**



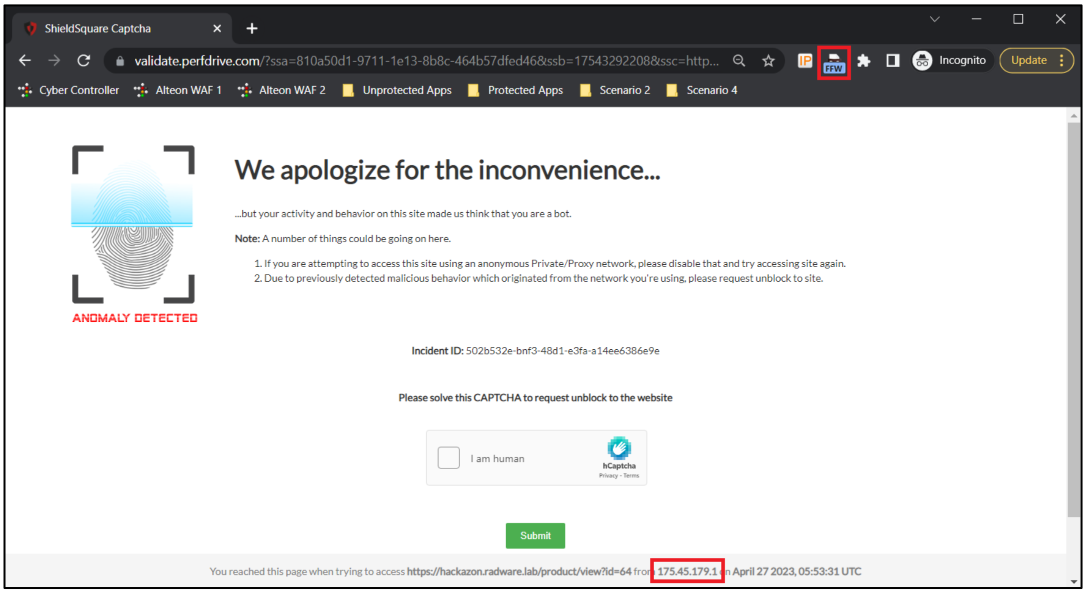
```
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100
101 Firefox/111.0
x-forwarded-for: 12.24.2.56
```

- Reset the User-Agent back to default by clicking on the plugin, selecting Chrome, and clicking on default.

Attack Protected Web Application:

- Close and reopen **Google Chrome** with an empty **Incognito tab**.
- Verify that X-Forwarded-For Header to IP 175.45.179.1.
- Verify that Chrome UA Spoofer is set to "Windows Firefox 111" Note that if the "FFW" letters appear on the extension icon this indicating that the Firefox User-Agent is being used.
- Open the **Protected Apps** Folder located in the **bookmark bar** and click on **Hackazon.**
- Click on a few links within the page until you encounter a **Captcha page**.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



We apologize for the inconvenience...

...but your activity and behavior on this site made us think that you are a bot.

Note: A number of things could be going on here.

1. If you are attempting to access this site using an anonymous Private/Proxy network, please disable that and try accessing site again.
2. Due to previously detected malicious behavior which originated from the network you're using, please request unblock to site.

Incident ID: 502b532e-bnf3-48d1-e3fa-a14ee6386e9e

Please solve this CAPTCHA to request unblock to the website

□ I am human

You reached this page when trying to access **https://hackazon.radware.lab/product/view?id=64** from **175.45.179.1** on **April 27 2023, 05:53:31 UTC**

After completing the scenario, open the Chrome Extension User-Agent Switcher and reset the User-Agent back to default. This scenario highlights Bot Manager's ability to detect browser anomalies.

Scenario 2 – Web Scraping

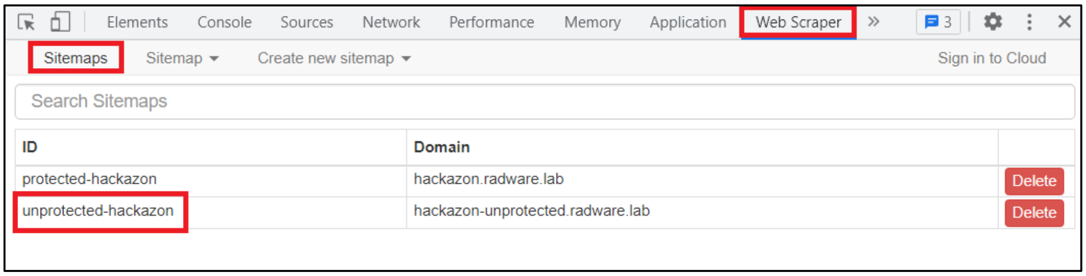
In this scenario, we will demonstrate how a bot can scrape an entire website and generate a database containing all product details and prices. The bot uses a browser plugin, enabling it to mimic user behavior, such as running JavaScript, downloading images and other referenced content, and following graphic links.

To attack the unprotected website:

- Open **Google Chrome.**
- Set **X-Forwarded-For** Header to IP **175.45.179.2.**
- Open **Developer Tools** (Ctrl + Shift + I or F12 key).
- Navigate to the **Web Scraper** tab.
- Click **Sitemaps**.
- Select the **unprotected-hackazon** sitemap.

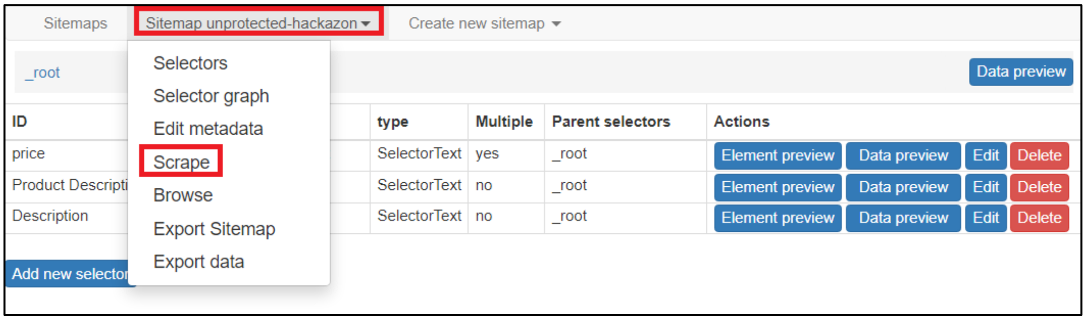
The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



ID	Domain	
protected-hackazon	hackazon.radware.lab	Delete
unprotected-hackazon	hackazon-unprotected.radware.lab	Delete

- In Web Scraper, click on **Sitemap unprotected-hackazon** and click **Scrape**.
- Click "**Start Scraping**."



ID	type	Multiple	Parent selectors	Actions
price	SelectorText	yes	_root	Element preview Data preview Edit Delete
Product Descripti	SelectorText	no	_root	Element preview Data preview Edit Delete
Description	SelectorText	no	_root	Element preview Data preview Edit Delete

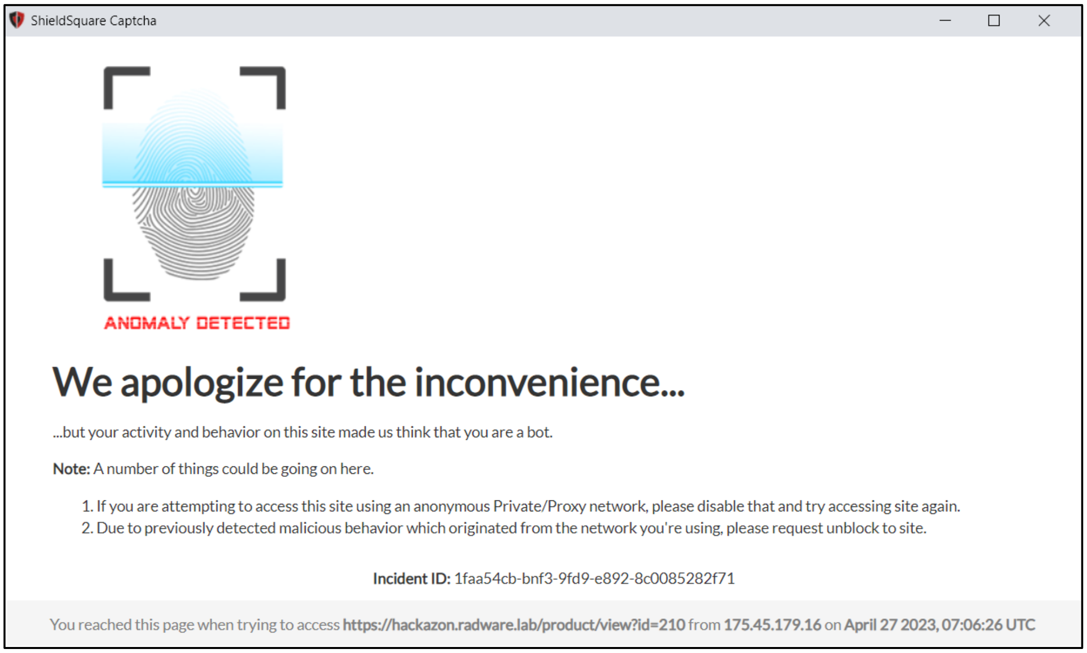
- A window appears, displaying each page being scraped.
- After a few moments, click on Sitemap **unprotected-hackazon** and click **Browse** to view all the scraped data.
- Note: You may close the scraping window at any time after at least 20 products have been scrapped.

Attack Protected Web Application:

- Close and reopen **Google Chrome** with an empty **Incognito** tab.
- Verify that **X-Forwarded-For** Header to IP **175.45.179.2**.
- Open Developer Tools (Ctrl + Shift + I or F12 key).
- Go to the **Web Scraper** tab.
- Click **Sitemaps**.
- Choose the **protected-hackazon** sitemap.
- In Web Scraper, click on **Sitemap protected-hackazon** and click **Scrape**.
- Click "**Start Scraping**."

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- A window appears, displaying each page being scraped which will quickly change to a recurring captcha page.
- After a few moments, click on **Sitemap protected-hackazon** and click **Browse** to view all the scraped data, observe that most of the data is null.
- Note: You may close the scraping window at any time after at least 20 products have been scrapped.



We apologize for the inconvenience...

...but your activity and behavior on this site made us think that you are a bot.

Note: A number of things could be going on here.

1. If you are attempting to access this site using an anonymous Private/Proxy network, please disable that and try accessing site again.
2. Due to previously detected malicious behavior which originated from the network you're using, please request unblock to site.

Incident ID: 1faa54cb-bnf3-9fd9-e892-8c0085282f71

You reached this page when trying to access **https://hackazon.radware.lab/product/view?id=210** from **175.45.179.16** on **April 27 2023, 07:06:26 UTC**

This scenario shows how web scraping bots can be stopped by implementing protective measures such as captchas on protected websites.

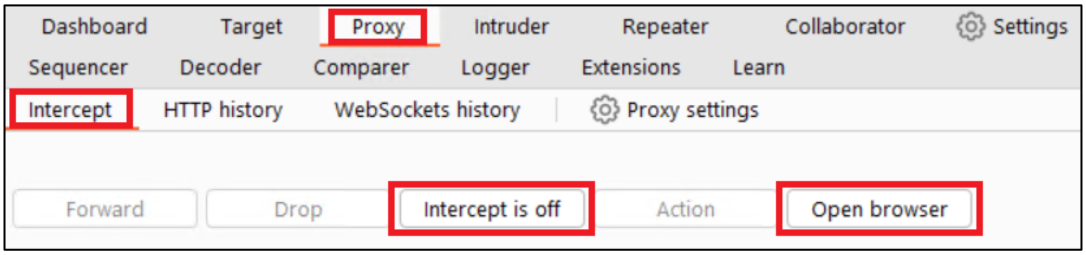
Scenario 3 – Account Takeover

In this scenario, we will demonstrate how bots can take over accounts using Credential Cracking and changing their source IP address almost with every request. We will use a known attacker tool to perform the attack.

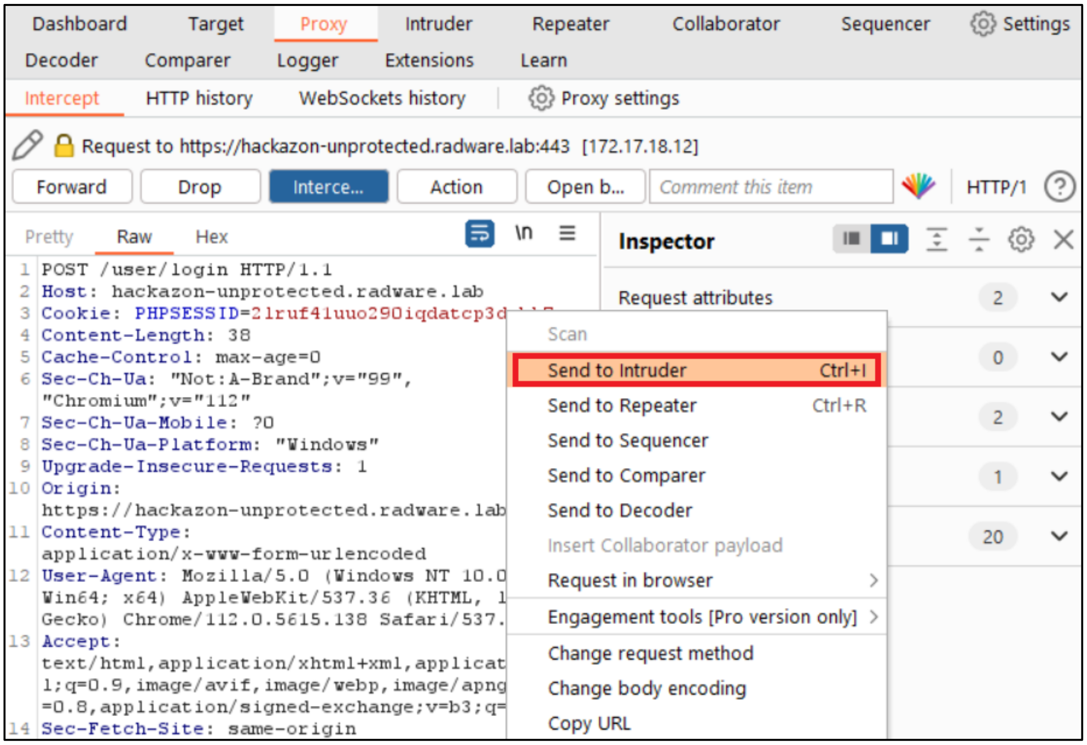
Attack the unprotected website:

- On the Desktop click on the icon named "**Burp Suite**" and click next.
- Switch to the Proxy tab and ensure Intercept is off.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



- Click on the **Open Browser** button. A special version of **Google Chrome** will open, preconfigured with the Burp Suite proxy.
- Inside this special version of Chrome, **enter** the URL **https://hackazon-unprotected.radware.lab/**
- Click the **Sign In/Sign Up button**, enter the username **'test_user'**, and input an incorrect password but **do not yet try to sign in**.
- Switch back to **Burp Suite** and set **Intercept** to **on**.
- Click the **Sign In** button. The request will be **intercepted** within **Burp Suite**.
- **Right-click** inside Burp Suite and select **Send to Intruder**.



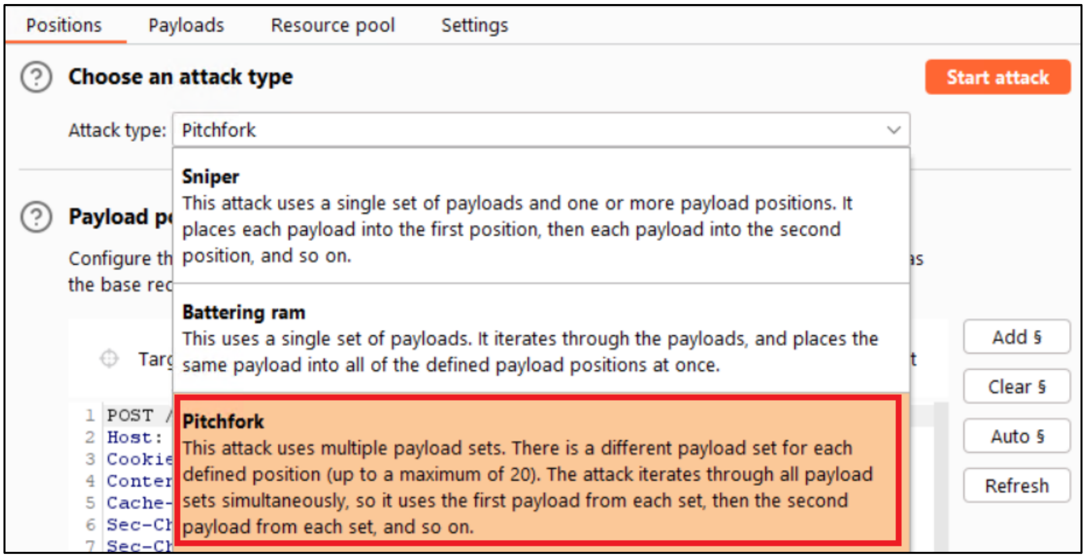
```
POST /user/login HTTP/1.1
Host: hackazon-unprotected.radware.lab
Cookie: PHPSESSID=21ruf41uuo290iqdatcp3d
Content-Length: 38
Cache-Control: max-age=0
Sec-Ch-Ua: "Not:A-Brand";v="99",
"Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin:
https://hackazon-unprotected.radware.lab
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0
Win64; x64) AppleWebKit/537.36 (KHTML, l
Gecko) Chrome/112.0.5615.138 Safari/537.
Accept:
text/html,application/xhtml+xml,applicat
l;q=0.9,image/avif,image/webp,image/apng
=0.8,application/signed-exchange;v=b3;q=
Sec-Fetch-Site: same-origin
```

- Set **Intercept** to **off**.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

- Switch to the **Intruder** tab, select **attack type Pitchfork**.



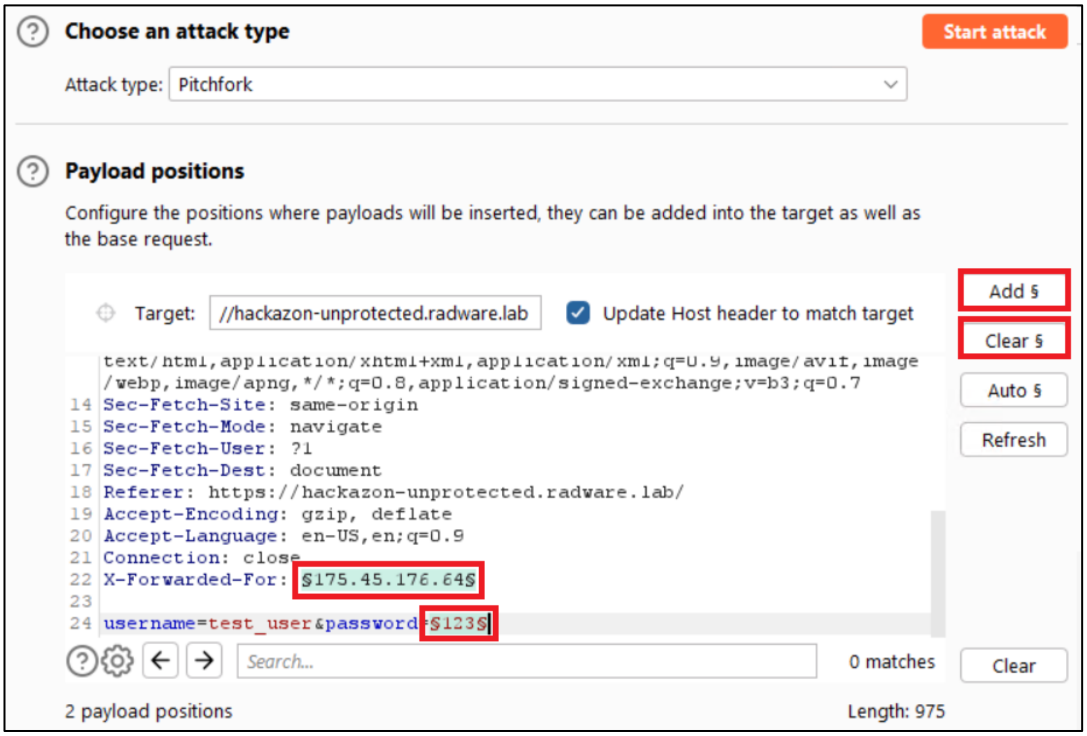
Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

- Click the **Clear §** button.
- Add the HTTP header "**X-Forwarded-For: 175.45.179.64**" to the request.
- **Highlight** the **IP value** and click **Add §**.
- **Highlight** the **password value** and click **Add §.**

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.



Choose an attack type

Attack type: Pitchfork

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: //hackazon-unprotected.radware.lab

☑ Update Host header to match target

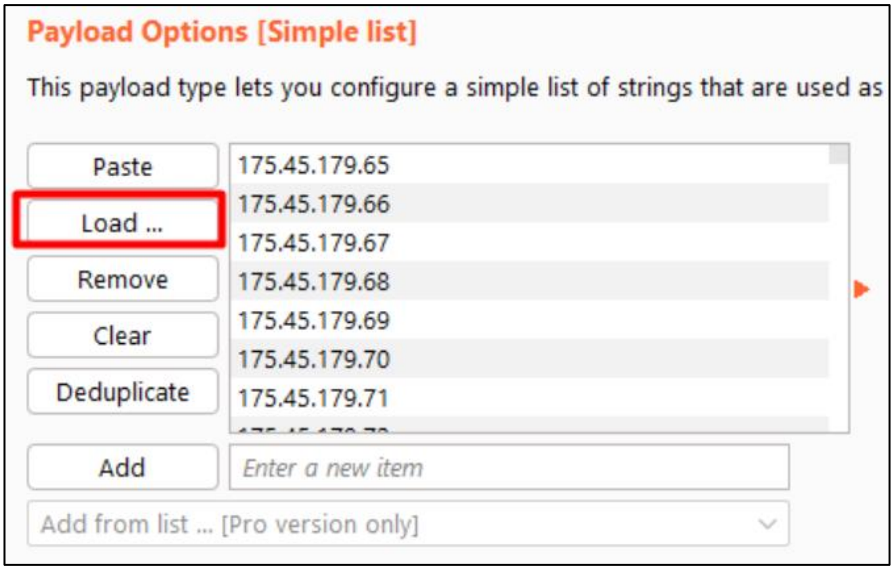
```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://hackazon-unprotected.radware.lab/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
X-Forwarded-For: §175.45.176.64§

username=test_user&password=§123§
```

0 matches

2 payload positions

Length: 975

- Switch to the **Payload** tab. In **Settings Option [Simple List]**, click **Load** and open the folder on the desktop named **Bot Scenario 3**. Open the file **IPs175.45.179.65-254.txt**.

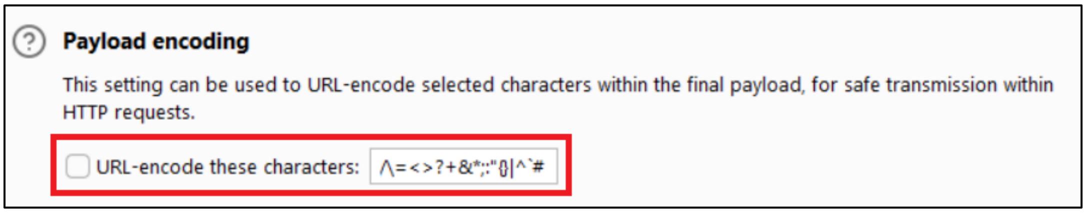


Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as

```
175.45.179.65
175.45.179.66
175.45.179.67
175.45.179.68
175.45.179.69
175.45.179.70
175.45.179.71
```

- Scroll to the bottom of the page and **uncheck** "**URL-encode these characters**".

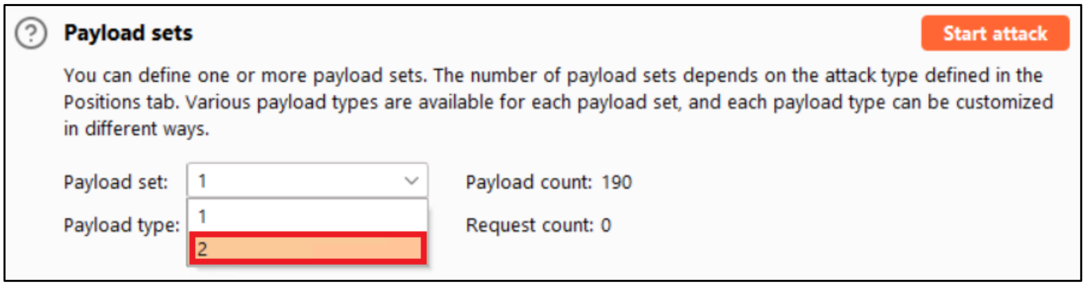


Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☐ URL-encode these characters: /\=<>?+&*;:"{}|^`#

- Scroll back to the top and **switch** to **Payload set number 2.**



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

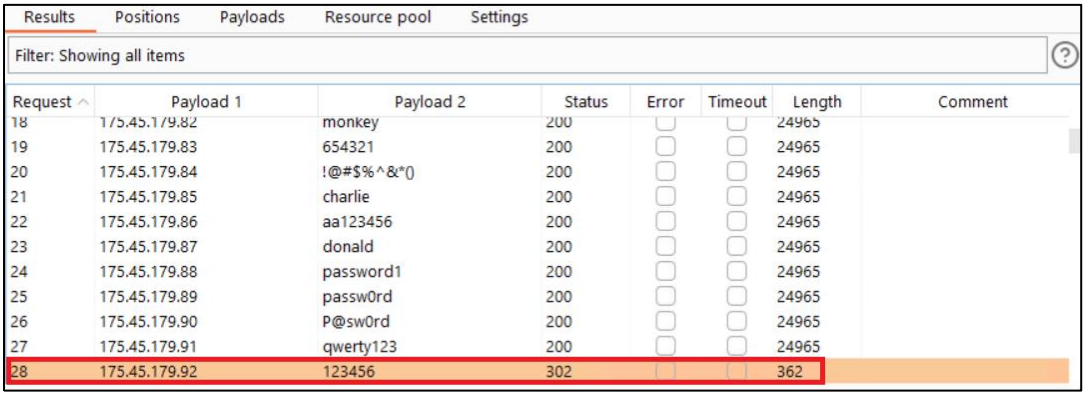
Payload set: 1

Payload count: 190

Payload type: 1 / 2

Request count: 0

- In the **Payload Settings [Simple list],** click **Load** and open the file **Top 1000 Dictionary Passwords.txt** from the same folder.
- Scroll to the bottom of the page and **uncheck** "**URL-encode these characters**".
- We have now instructed Burp Suite to repeat this request while changing the IP and password for each iteration of the request.
- Click **Start Attack** and then **OK**.
- A window will open, showing each request and its results. To find the correct password, look for the first response that is different from all the others.



Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
18	175.45.179.82	monkey	200	☐	☐	24965	
19	175.45.179.83	654321	200	☐	☐	24965	
20	175.45.179.84	!@#$%^&*()	200	☐	☐	24965	
21	175.45.179.85	charlie	200	☐	☐	24965	
22	175.45.179.86	aa123456	200	☐	☐	24965	
23	175.45.179.87	donald	200	☐	☐	24965	
24	175.45.179.88	password1	200	☐	☐	24965	
25	175.45.179.89	passw0rd	200	☐	☐	24965	
26	175.45.179.90	P@sw0rd	200	☐	☐	24965	
27	175.45.179.91	qwerty123	200	☐	☐	24965	
28	175.45.179.92	123456	302	☐	☐	362	

Attack the protected website:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

Repeat the steps from the previous section, but enter the following protected URL:

- https://hackazon.radware.lab

A window will open, showing each request and its results. However, this time, the SecurePath protected website's Bot Manager identifies the attack after a few requests and responds with a 302 redirect to a Captcha page.

This scenario shows how Account Takeover attacks can be mitigated by using Bot Manager, which identifies suspicious bot behavior and redirects them to Captcha pages, effectively preventing the attack.

Scenario OWASP Category Mapping

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. They provide a variety of resources, including the OWASP Top 10, which is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

The OWASP Top 10 for Web Application Security Risks includes categories like "A03:2021 - Injection" and "A05:2021 – Security Misconfiguration", which are relevant to several of the web scenarios in the Alteon WAF Demolab.

In addition to the Top 10 for web applications, OWASP also provides a Top 10 for API Security. This list focuses on the most critical risks to APIs, such as "API4:2019 - Lack of Resources & Rate Limiting" and "API8:2019 - Injection".

Finally, OWASP has defined a list of Automated Threats to Web Applications (OAT), which includes threats like "OAT-004 Fingerprinting", "OAT-011 Scraping", and "OAT-007 Credential Cracking". These threats are particularly relevant to scenarios involving bots.

The following table maps the scenarios in the Alteon WAF Demolab to the relevant categories from the OWASP Top 10 for web applications, the OWASP Top 10 for API security, and the OWASP Automated Threats list:

Scenario	OWASP Category
Web Scenario 1: SQL Injection	A03:2021 - Injection
Web Scenario 2: XSS Injection	A03:2021 - Injection
Web Scenario 6: Buffer Overflow	A05:2021 – Security Misconfiguration
Web Scenario 7: Source Blocking	A05:2021 – Security Misconfiguration
API Scenario 1: Rate Limiting	API4:2019 - Lack of Resources & Rate Limiting
API Scenario 2: SQL Injection	API8:2019 - Injection
Bot Scenario 1: Browser Anomaly	OAT-004 Fingerprinting
Bot Scenario 2: Web Scraping	OAT-011 Scraping
Bot Scenario 3: Account Takeover	OAT-007 Credential Cracking

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.