

The background of the cover is a complex digital-themed illustration. It features a large, metallic, 3D padlock in the center, which is slightly open. The padlock is surrounded by swirling patterns of binary code (0s and 1s) in various colors like blue, red, and orange. The overall aesthetic is high-tech and futuristic, with sharp geometric shapes and a sense of motion.

# radware CloudWAF

Lab Manual – July 2025



# TABLE OF CONTENTS

## Contents

➞ INTRODUCTION .....	3
➞ LAB ENVIRONMENT .....	3
➞ GET YOUR CLOUD ACCESS .....	4
➞ INITIAL CLOUD WAF LOGIN .....	4
➞ CREATE YOUR APPLICATION .....	7
➞ ENABLE BLOCKING ON THE APPLICATION.....	9
➞ CONFIGURE KALI TO ACCESS APPLICATION VIA CLOUDWAF .....	10
➞ RUN ATTACKS .....	12
➞ MONITORING AND REPORTING WITH OWASP-ZAP .....	16
➞ CONFIGURE NOTIFICATIONS (ALERTS) .....	21
➞ CONFIGURE REPORTS.....	23
➞ API PROTECTION .....	24

## ➔ INTRODUCTION

The **CloudWAF** lab is comprised of several activity flows that you will be asked to perform in the CloudWAF service while reviewing the online course. It covers basic configurations and reporting in CloudWAF installations.

The features and functions of Radware CloudWAF discussed in this document are based on SW version from June 202. In case you use a newer version of the CloudWAF service, the information provided can be different from the elements we discuss in this document.

Use an online lab and the CloudWAF portal, together with this manual to perform lab activities.

For technical assistance, please contact Radware lab support at [radwarevirtuallab@radware.com](mailto:radwarevirtuallab@radware.com) or [training@radware.com](mailto:training@radware.com).

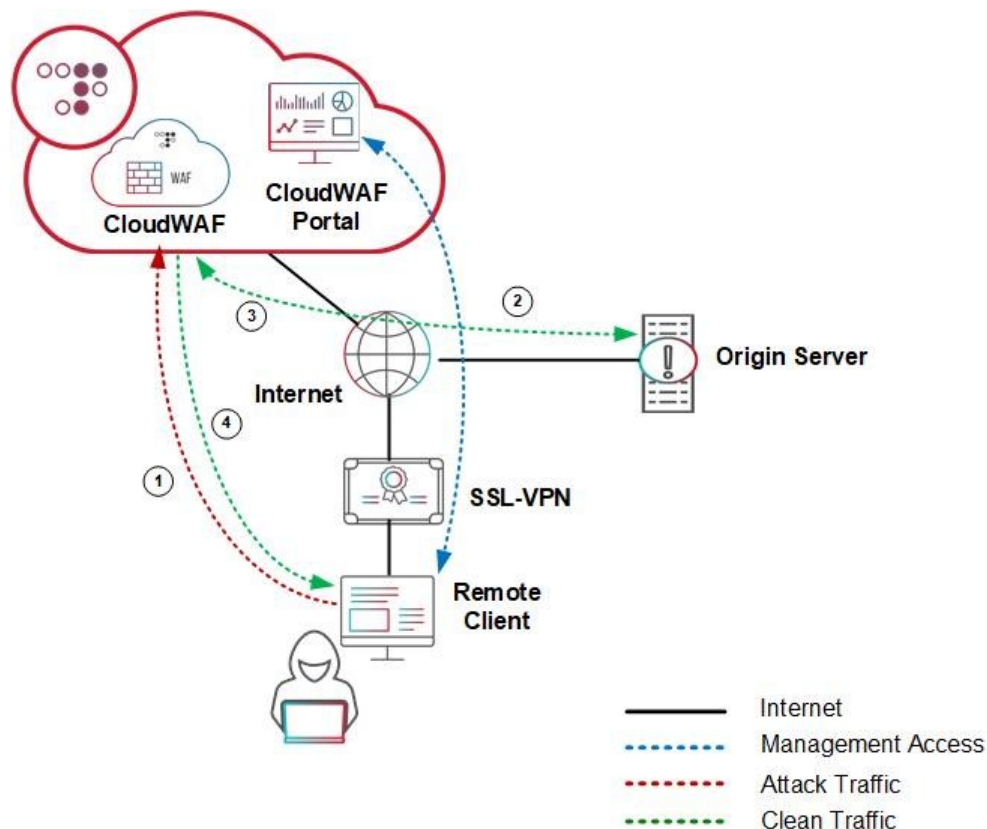
## ➔ LAB ENVIRONMENT

This lab kit consists of:

- Radware Training CloudWAF account
- Attacker Machine
- Protected Server

<b>Local Workstation or Laptop</b>	Capable of running a web browser with internet access
------------------------------------	---

All machines are preconfigured. You will receive as assignment access information for you to use.



## ➔ GET YOUR CLOUD ACCESS


Before you can start the lab you need to send an email to [RadwareVirtualLAB@Radware.com](mailto:RadwareVirtualLAB@Radware.com) to get lab assigned, in case you didn't get it assigned by your trainer already.

Our labs are reserved, in advance, for a week (Monday – Friday) per availability. Please provide us with three different weeks that you are available to complete your labs (for example the week of May 3-7). We will add your reservation on one of your selected dates or earliest available.

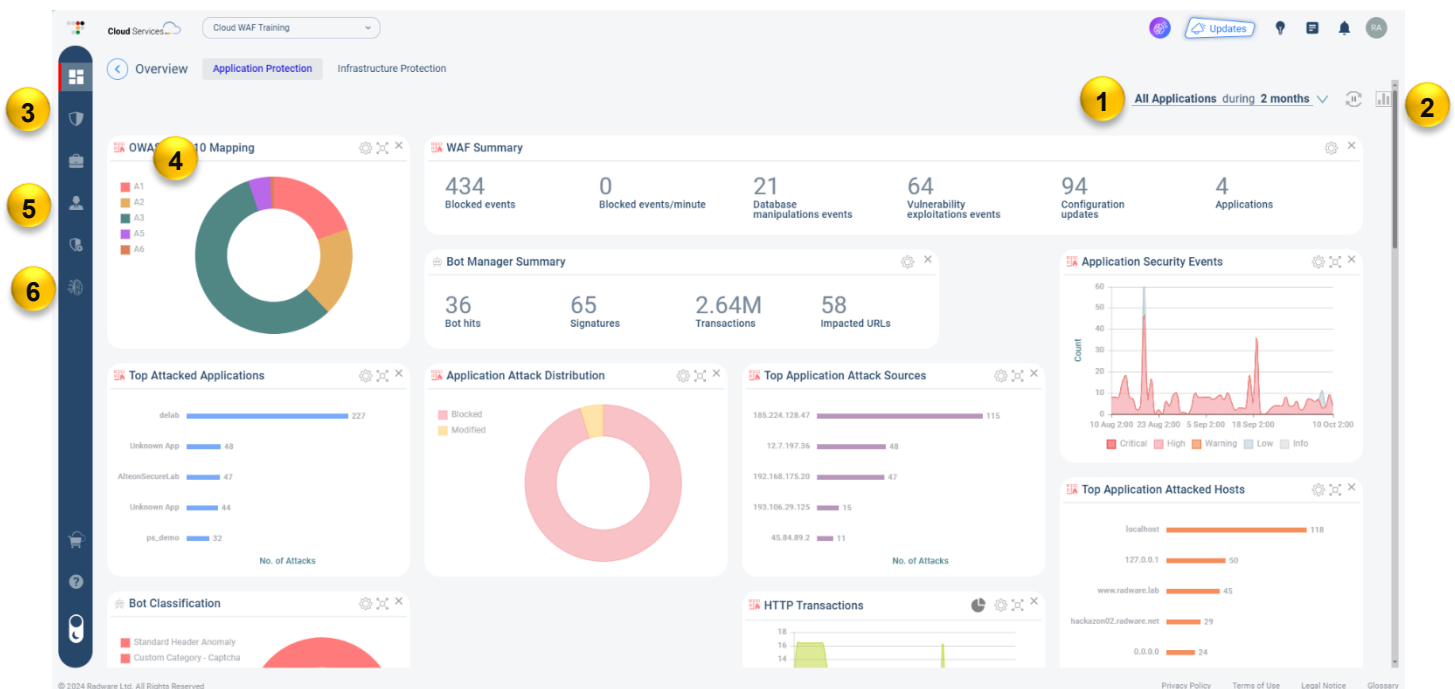
Your reservation confirmation and further instructions will be emailed separately.

## ➔ INITIAL CLOUD WAF LOGIN

**You can login to the CloudWAF portal only from within the remote lab!** Open the browser  on the remote machine and connect to <https://console.radwarecloud.com>

The landing page of the portal is the **Dashboard**, that displays details on the currently selected application. You can always return to this screen by clicking the dashboard icon .

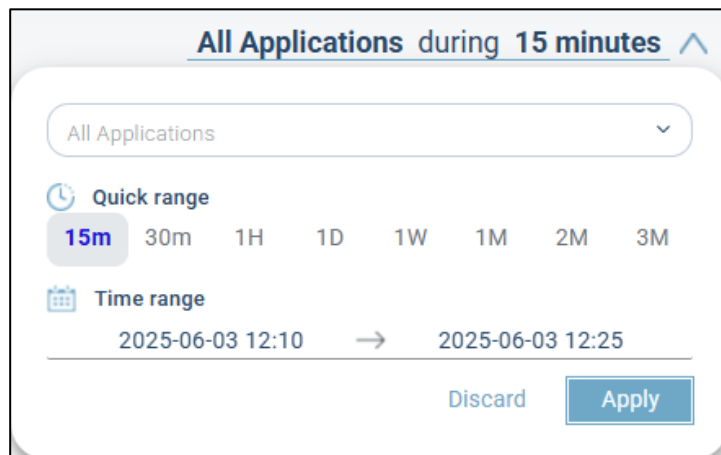
You did not yet create an application in this lab, but you may see applications that others created from the virtual company called “Cloud WAF Training”.




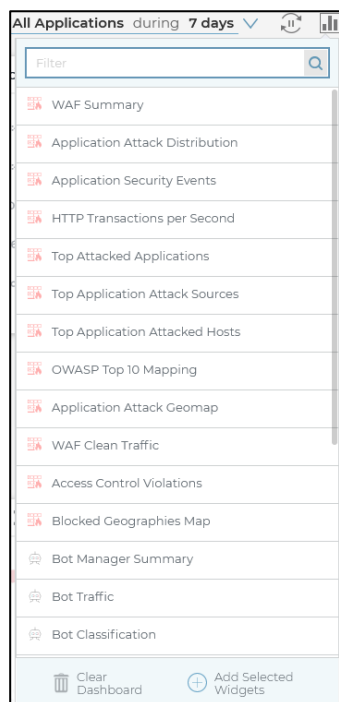
## CloudWAF Dashboard


Use the  to expand the sidebar menu to see the menu labels and use  to collapse the sidebar menu.

You can use the dropdown menu (1) to change the time range and the application on which you want to see data. To see data from all applications, leave this field empty...




Using the **Widgets Repository**  icon (2), you can add /remove additional widgets.



Under the **Monitor**  menu (3) you can select the following sections:


- **Security Events** showing the details about the recorded security events
- **Operational Events** showing the details about operational events for the Cloud DDoS protection
- **Analytics** showing correlated security events
- **Notifications** add/remove/change notifications (alerts)
- **Reports** add/remove/change/run reports

In the **Assets**  menu (4) you have the following options:

- **Security Policies** a new way of managing multiple applications security settings
- **Assets** add/delete/change applications and the relevant settings
- **DNS** configures the DNS as a service add-on settings
- **Integrations** configuration of BOT manager software integrations (server & client)
- **Sites** part of Infrastructure protection (CloudDDoS)
- **Certificates** import/export/delete SSL certificates
- **Templates & Policies** allows to configure Security Templates, IP Groups and Geo Blocking Policies

The **Account**  menu (5) contains the following options



- **Accounts** see the Service Overview of the bought services and select SSL settings
- **Users** you can see the users of your organization  
and if you have permissions - add/delete/change users
- **API Keys** you can configure access keys for the API access
- **Audit Logs** show you activities on the account

The **Threat Intelligence Center**  (5) allows you to get more insight information on an IP address.






## CREATE YOUR APPLICATION

You will now create an application that you are going to protect.

1. In the cloud portal go to  > **Assets (Applications)**. You should see applications that were already created.
2. Click  to add a new application.
3. In the **New Application** windows fill in the following information:

<b>Application Type</b>	Standard
<b>Display Name</b>	hackazon## (like hackazon03 if you are team 3)
<b>Application Domain</b>	hackazon##.radware.net
<b>Keep</b>	HTTP/HTTPS application supporting up to 2 ports
<b>Application Protocol</b>	only HTTPS
<b>Certificate</b>	*.radware.net
<b>Origin Server IPv4</b>	12.7.197.40
<b>Region</b>	Europe (Frankfurt (Amsterdam))
<b>Security Hardening</b>	Standard

3. Click **Save** to complete the application creation dialog.  
Your application will go into *Provisioning*.

Type	Name	Domain	Origin	Created ↕	Region	Events (Last 7 days)	
 	hackazon01	hackazon01.radware.net		June 3, 2025, 12:32	Europe – Frankfurt (Amsterdam)	0	<a href="#">Details</a> 

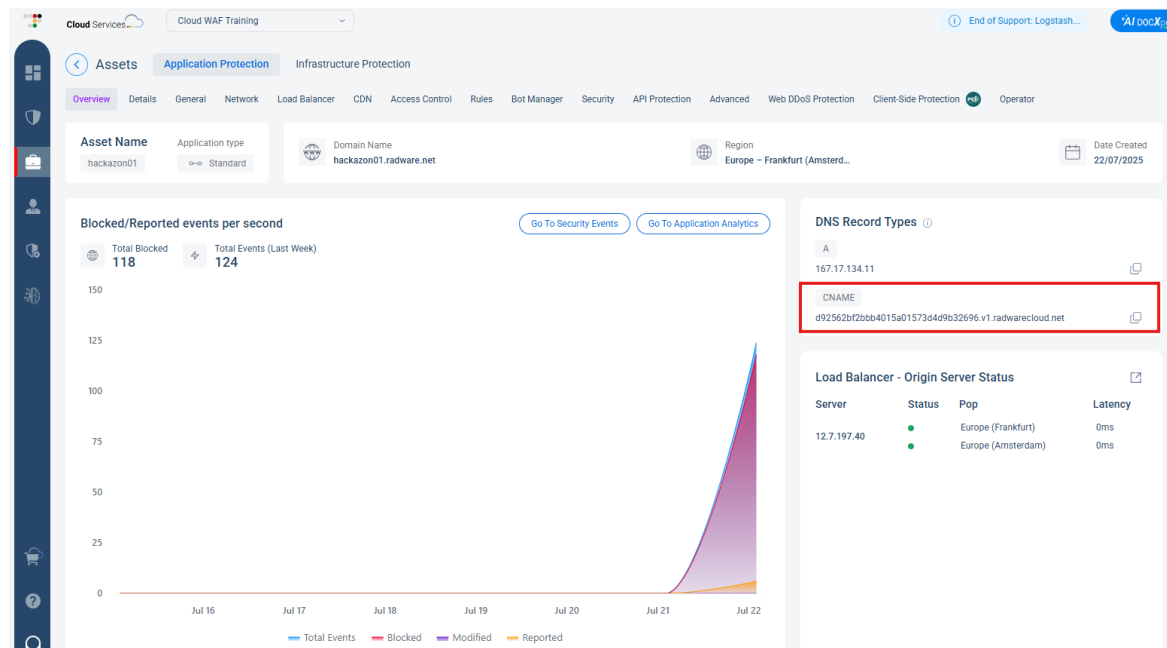
When *Provisioning* is completed, the application is ready to protect.



**This process typically takes a few minutes to complete.**

After the application is successfully created an email with the application details will be send to the account created it. In the lab the email will be send to [radwarevirtuallab@radware.com](mailto:radwarevirtuallab@radware.com) , ask your instructor to receive it or directly the lab administration.

But you don't need to wait to receive the email, the application details like the CNAME can be found on the application itself.



4. Change the TCP port used for the origin server to 21045, since the application is using this port for the web service.

In the CloudWAF Portal go to **Assets** and click on your application to change its settings. Some settings are in *read only* while the application is in *Learning* mode.

Select **Network > Application Services** and change the **Back-End Port** to 21045.

Front-End Port	Back-End Port	Type	Description
443	21045	HTTPS	

Certificate: \*.radware.net (5931...)  
Type: Regular Valid To: 2025/09/10

Redirect Port 80 To Port: N/A

HTTP Health-Check Success Criteria: N/A

HTTPS Health-Check Success Criteria: 443 -> 21045

TCP ☒ HTTP ☐

Cancel Save

Click **Save** to store the change.



## ➔ ENABLE BLOCKING ON THE APPLICATION

To make sure the CloudWAF is blocking all critical requests to the application, you will enable blocking.

**i** In a production environment you should start with a *report-only* period to learn potential issues!

1. In the CloudWAF Portal go to **Assets** and click on your application to change its settings.
2. Select **Security** and change all the security options to *Block and Report* instead of *Report only*.

The screenshot shows the 'Security' tab for the application 'TestNewOrigin' (www2.radware.net, Standard). A red box highlights the right-hand column of settings, where each security feature has a dropdown menu to select the action. The features and their current settings are:

Security Feature	Current Setting
RFC Violation Protection	Block and Report
Anonymous Proxy Blocking	Disabled
Signature based Protection	Block and Report
Custom Signature	Block and Report
SQL Injection Protection	Block and Report
Path Access Protection	Block and Report
JSON Validation Protection	Block and Report
Source Blocking	Disabled (indicated by a red 'x' icon)
DDoS Protection	Block and Report

3. Now you are set to block attacks towards the application via the CloudWAF service.


The **Details** section of your application should show something like this:

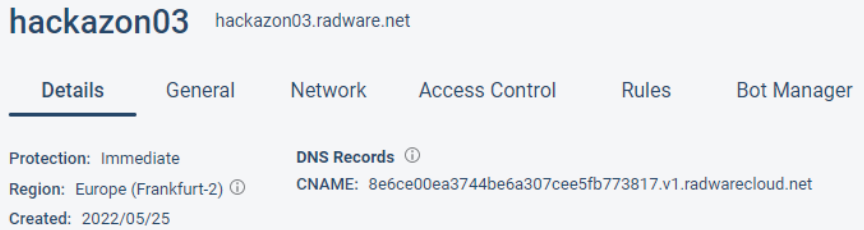
The screenshot shows the 'Details' section of the application, organized into three categories:

- Network Protection**
  - DDoS Protection: Blocking
  - Web DDoS Protection: Disabled
  - Geo-Blocking: Disabled
  - Access Control List: Disabled
  - EAAF Blocking: Blocking
  - Rate Limiting: Disabled
  - Source Blocking: Disabled
- Bot Management**
  - Bot Manager: Disabled
- Application Protection**
  - RFC Violation Protection: Blocking
  - Anonymous Proxy Blocking: Disabled
  - Signature based Protection: Blocking - Analyzing Traffic
  - SQL Injection Protection: Blocking - Analyzing Traffic
  - Path Access Protection: Blocking - Analyzing Traffic
  - API Protection - OpenAPI: Disabled
  - API Protection - GraphQL: Disabled

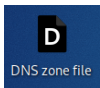
## ➡ CONFIGURE KALI TO ACCESS APPLICATION VIA CLOUDWAF

To access the application you created, let's update the DNS zone file of radware.net to add the CNAME entry of hackazon##.radware.net to point to the CloudWAF.

1. Use the SSLVPN connection received by your trainer or [RadareVirtualLab@radware.com](mailto:RadareVirtualLab@radware.com). If the machine gets locked or you need to provide authentication for sudo commands, use **kali** as **username** and **password**.
2. Open the  browser and connect to <https://console.radwarecloud.com/login>.
3. Go to your application and copy the CNAME under the details for the next step



4. On the desktop of the remote Kali client you will see an icon called "DNS zone file".



Double-Click it to open a text editor

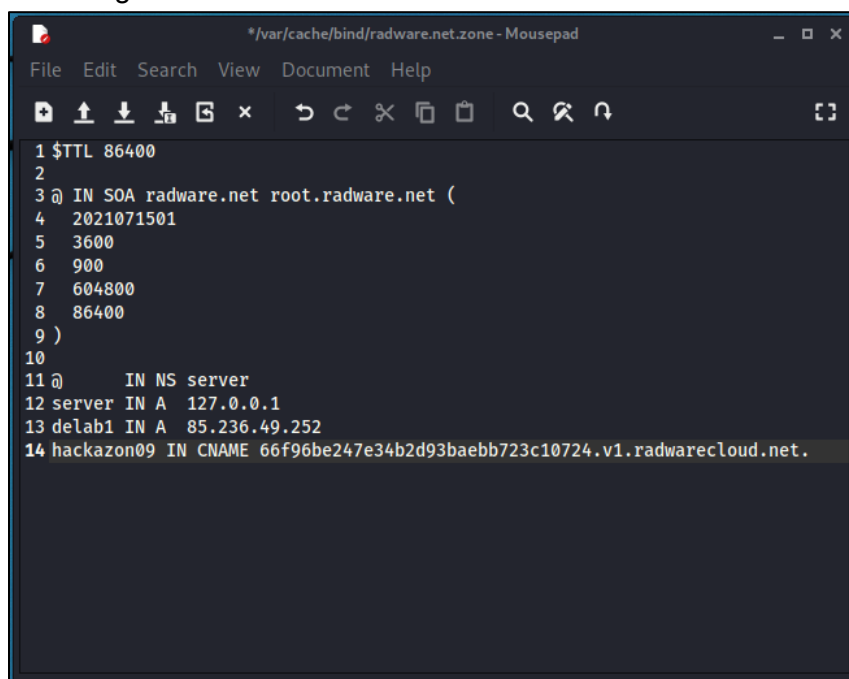
5. Change the value in line 4 to the current date and add 01 at the end like 2024071501
6. Add a line after 13 like the following:

*<application name> IN CNAME <cname string from CloudWAF>.*

for example:

Hackazon09. IN CNAME **66f96be247e34b2d93baebb723c10724.v1.radwarecloud.net.**

Don't forget the **.** at the end of the line!



```
*/var/cache/bind/radware.net.zone - Mousepad
File Edit Search View Document Help
1 $TTL 86400
2
3 @ IN SOA radware.net root.radware.net (
4 2021071501
5 3600
6 900
7 604800
8 86400
9 )
10
11 @ IN NS server
12 server IN A 127.0.0.1
13 delab1 IN A 85.236.49.252
14 hackazon09 IN CNAME 66f96be247e34b2d93baebb723c10724.v1.radwarecloud.net.
```

Click on **File > Save**

**Close the Mousepad**

7. Open a command prompt  and run the following command:

**sudo systemctl reload bind9**



The password for the user kali is kali !

8. If you continue with step 9 and it is not working and you get “connection refused” message, wait a few more minutes and retry. The bind service need time to restart.
9. On the same command prompt check if the config was done successfully using the following command:

**dig hackazon##.radware.net**


```
dig hackazon09.radware.net

; <<>> DiG 9.16.15-Debian <<>> hackazon09.radware.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 13898
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

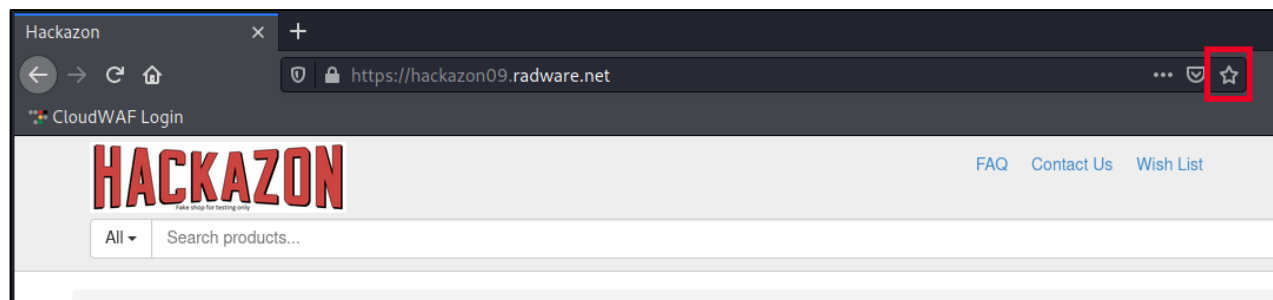
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 522550eec0cb26760100000060f0578090682c43523f9ff1 (good)
;; QUESTION SECTION:
;hackazon09.radware.net.                IN      A

;; ANSWER SECTION:
hackazon09.radware.net. 86400 IN      CNAME  66f96be247e34b2d93baebb723c10724.v1.radwarecloud.net.
66f96be247e34b2d93baebb723c10724.v1.radwarecloud.net. 30 IN A 20.80.57.231

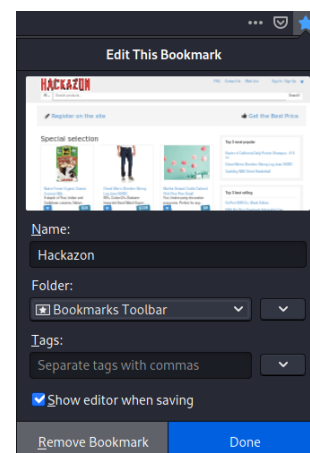
;; Query time: 44 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jul 15 11:42:56 EDT 2021
;; MSG SIZE rcvd: 161
```

10. click on  the firefox browser and try to surf to the host you just added to the DNS configuration.

Like <https://hackazon09.radware.net>



For your convenience you can create a bookmark which is called **Hackazon** to point to your application using the star symbol.



## RUN ATTACKS

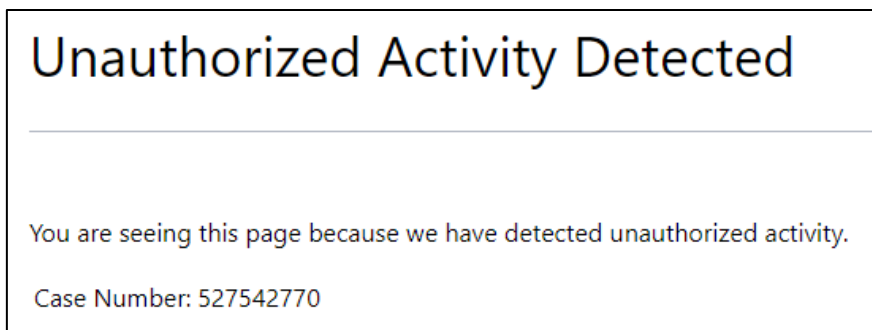
Now you will run some attacks to see security events in the CloudWAF portal.


You'll start with some SQL Injections.

1. In the remote client, type the following string in the **Search** products text box of the Hackazon web site, and click on **Search**:

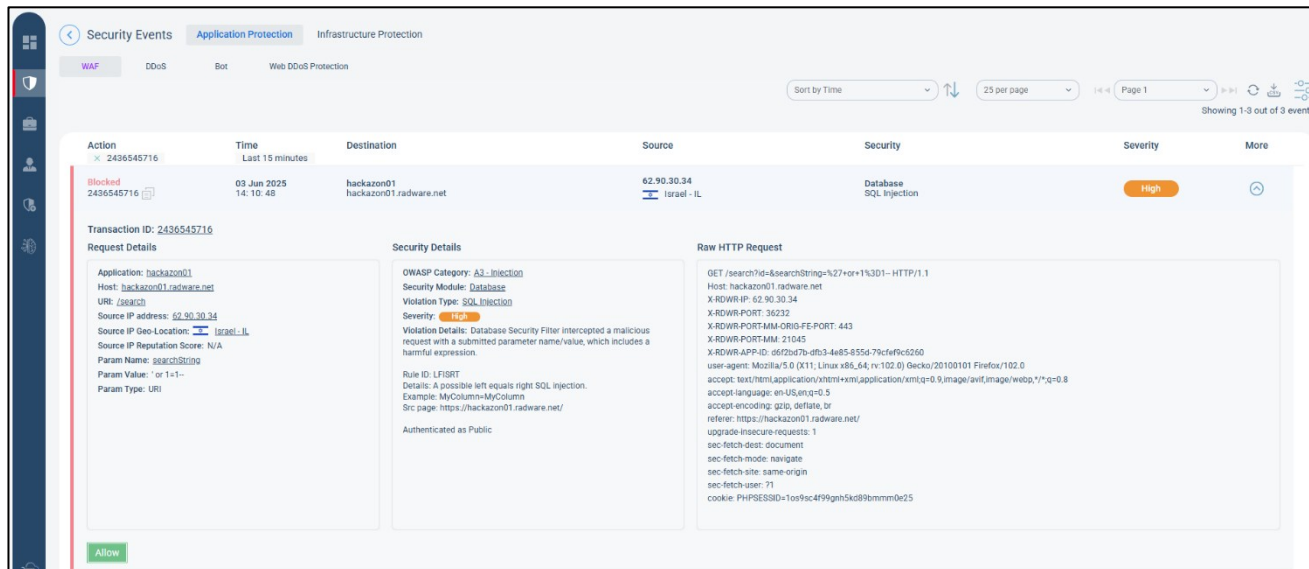
**' or 1=1--**

Since the CloudWAF is in *block* mode, you will see the following message:




2. Open the CloudWAF portal and go to **Monitor > Security Events**
3. You should see an *SQL Injection Database* security event. Click on the event or the  icon to see the details. You should see the string you typed in the search field in the **Param Value** part of the event details.

The security event also shows you the OWASP category, here A3 and other attack details.



The screenshot shows the CloudWAF Security Events portal. The top navigation bar includes 'Security Events', 'Application Protection', and 'Infrastructure Protection'. The 'Security Events' tab is active, showing a table of events. The first event is highlighted, showing details for a blocked request.

Action	Time	Destination	Source	Security	Severity	More
Blocked 2436545716	03 Jun 2025 14:10:48	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Database SQL Injection	High	

Transaction ID: 2436545716

**Request Details**

- Application: hackazon01
- Host: hackazon01.radware.net
- URI: /search
- Source IP address: 62.90.30.34
- Source IP Geo-Location: Israel - IL
- Source IP Reputation Score: N/A
- Param Name: searchString
- Param Value: ' or 1=1--
- Param Type: URI

**Security Details**

- OWASP Category: A3 - Injection
- Security Module: Database
- Violation Type: SQL Injection
- Severity: High
- Violation Details: Database Security Filter intercepted a malicious request with a submitted parameter name/value, which includes a harmful expression.
- Rule ID: LFI00T
- Details: A possible left equals right SQL injection. Example: MyColumn=MyColumn
- Src page: https://hackazon01.radware.net/
- Authenticated as Public

**Raw HTTP Request**

```
GET /search?id=searchString=%27+or+1%3D1-- HTTP/1.1
Host: hackazon01.radware.net
X-RDWR-IP: 62.90.30.34
X-RDWR-PORT: 36232
X-RDWR-PORT-MM-ORIG-FE-PORT: 443
X-RDWR-PORT-MM: 21045
X-RDWR-APP-ID: d6/2bd7b-dfb3-4e85-855d-79cfe9c6260
User-agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
accept-encoding: gzip, deflate, br
referer: https://hackazon01.radware.net/
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: same-origin
sec-fetch-user: ?1
cookie: PHPSESSID=10a9sc4f99gh5k8@bmm0e25
```

If a security event is a false positive, you can click on **Allow** so Cloud WAF will allow it in the future.

- Click on **Allow** for this event. This question will appear.

Modify the policy to allow this file extension to be requested for your Application (applies in all URIs)? Allow Cancel

- Click on **Allow** again. The status of your request will be *in progress*.

Allow request was sent. Status: In Progress

When the processing of your request is completed, the request status changes to *Succeeded*.

Allow request was sent. Status: Succeeded

If you run the same attack again, CloudWAF will not trigger a security event.

As a second event, we are going to force a **Server Information Leakage** event.

- Try to access the admin area of php installations on your web server by using a similar URL with you application's name:

<https://hackazon09.radware.net/phpmyadmin/scripts/setup.php>

You will see again the unauthorized activity detected page.

- Copy the **Case Number** from within the error message so you can search for this event.
- In the CloudWAF portal, go to **Monitor > Security Events** and click on Filter button.

Security Events Application Protection Infrastructure Protection

WAF DDoS Bot Web DDoS Protection

Sort by Time 25 per page Page 1

- Paste the **Case Number** you copied in the **Transaction ID** field and click **Apply**.

Filters Clear All Apply

Transaction ID

☐ Modified ☐ Reported ☐ Blocked

You should see only this security event:

Action	Time	Destination	Source	Security	Severity	More
Blocked 190382986	03 Jun 2025 14:15:41	hackazon01 hackazon01.radware.net	77.137.31.132 Israel - IL	Vulnerabilities Predictable Resource Location	High	
Transaction ID: 190382986						
Request Details		Security Details		Raw HTTP Request		
<div>Application: <code>hackazon01</code> Host: <code>hackazon01.radware.net</code> URI: <code>/phpmyadmin/scripts/setup.php</code> Source IP address: <code>77.137.31.132</code> Source IP Geo-Location: <code>Israel - IL</code> Source IP Reputation Score: <code>N/A</code></div>		<div>OWASP Category: <a href="#">A1 - Broken Access Control</a> Security Module: <a href="#">Vulnerabilities</a> Violation Type: <a href="#">Predictable Resource Location</a> Severity: <span>High</span> Pattern: <code>/phpmyadmin</code> Violation Details: Vulnerabilities Security Filter intercepted a malicious request, which includes a blocked pattern. 9238 Description: PHPMyAdmin Interface (Severity: High)  No Src Page: might be manual hacking attempt! Authenticated as Public</div>		<div>GET /phpmyadmin/scripts/setup.php HTTP/1.1 Host: hackazon01.radware.net X-RDWR-IP: 77.137.31.132 X-RDWR-PORT: 57442 X-RDWR-PORT-MM-ORIG-FE-PORT: 443 X-RDWR-PORT-MM: 21045 X-RDWR-APP-ID: 65f2bd7b-dfb3-4e85-855a-79cfe7f6c260 user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 accept-language: en-US,en;q=0.5 accept-encoding: gzip, deflate, br upgrade-insecure-requests: 1 sec-fetch-dest: document sec-fetch-mode: navigate sec-fetch-site: none sec-fetch-user: ?1 cookie: PHPSESSID=10e95c4f99gnh5kd9bmnm0e25</div>		
Allow						

As the third attack you will misuse the application behavior and try to view files from the file system of the server via the application.

1. Login to the application. Click on **Sign-In** and use the following credentials:

<b>User Name</b>	test_user
<b>Password</b>	123456

2. Open this page like:  
[https://hackazon09.radware.net/account/help\\_articles?page=/etc/passwd](https://hackazon09.radware.net/account/help_articles?page=/etc/passwd)

You should see the security page again.

3. Copy the case number from the security page and search for this event.
4. Review the security event in the CloudWAF portal.

It is showing A5 – *Security Misconfiguration* and a message about the `/etc/passwd`.

**Action:** Blocked  
**Transaction ID:** 2452463484  
**Time:** 03 Jun 2025 14:23:44  
**Destination:** hackazon01.radware.net  
**Source:** 62.90.30.34 Israel - IL  
**Security:** Vulnerabilities Security Misconfiguration  
**Severity:** High

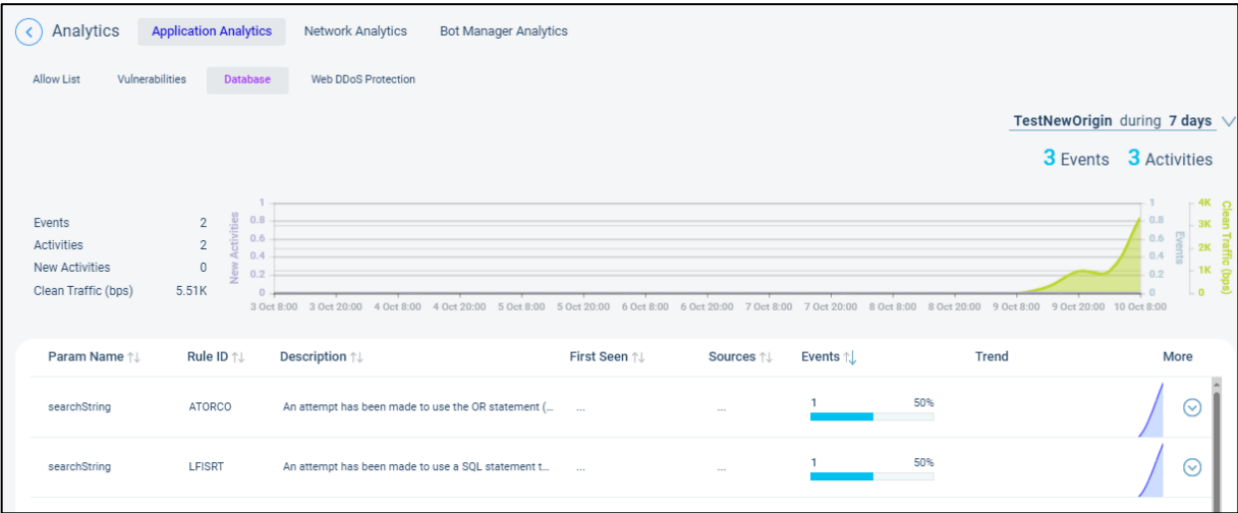
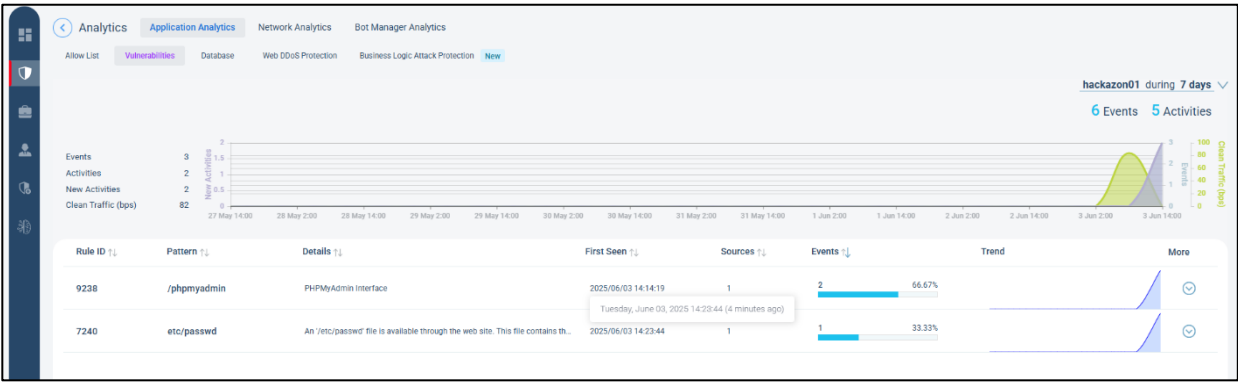
**Request Details:**  
Application: hackazon01  
Host: hackazon01.radware.net  
URI: /account/help\_articles  
Source IP address: 62.90.30.34  
Source IP Geo-Location: Israel - IL  
Source IP Reputation Score: N/A

**Security Details:**  
OWASP Category: A5 - Security Misconfiguration  
Security Module: Vulnerabilities  
Violation Type: Security Misconfiguration  
Severity: High  
Pattern: /etc/passwd  
Violation Details: Vulnerabilities Security Filter intercepted a malicious request, which includes a blocked pattern.  
Description: An '/etc/passwd' file is available through the web site. This file contains the systems users and passwords. (Severity: Medium)  
No Src Page: might be manual hacking attempt!  
Authenticated as Public

**Raw HTTP Request:**  
GET /account/help\_articles?page=/etc/passwd HTTP/1.1  
Host: hackazon01.radware.net  
X-RDWR-IP: 62.90.30.34  
X-RDWR-PORT: 45648  
X-RDWR-PORT-M4-ORIG-PORT: 443  
X-RDWR-PORT-M4: 21045  
X-RDWR-APP-ID: d6f2bd7b-dfb3-4e85-8556-79cfe9c6260  
user-agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
accept-language: en-US,en;q=0.5  
accept-encoding: gzip, deflate, br  
upgrade-insecure-requests: 1  
sec-fetch-dest: document  
sec-fetch-mode: navigate  
sec-fetch-site: none  
sec-fetch-user: ?1  
cookie: PHPSESSID=1os9sc4f99ghn5kd99mmmm0e25

**Allow**


5. Go to **Monitor > Analytics**. Make sure your application is selected (like hackazon03 in the screen capture) and look for the attacks you just performed under *Vulnerabilities* and *Database*.





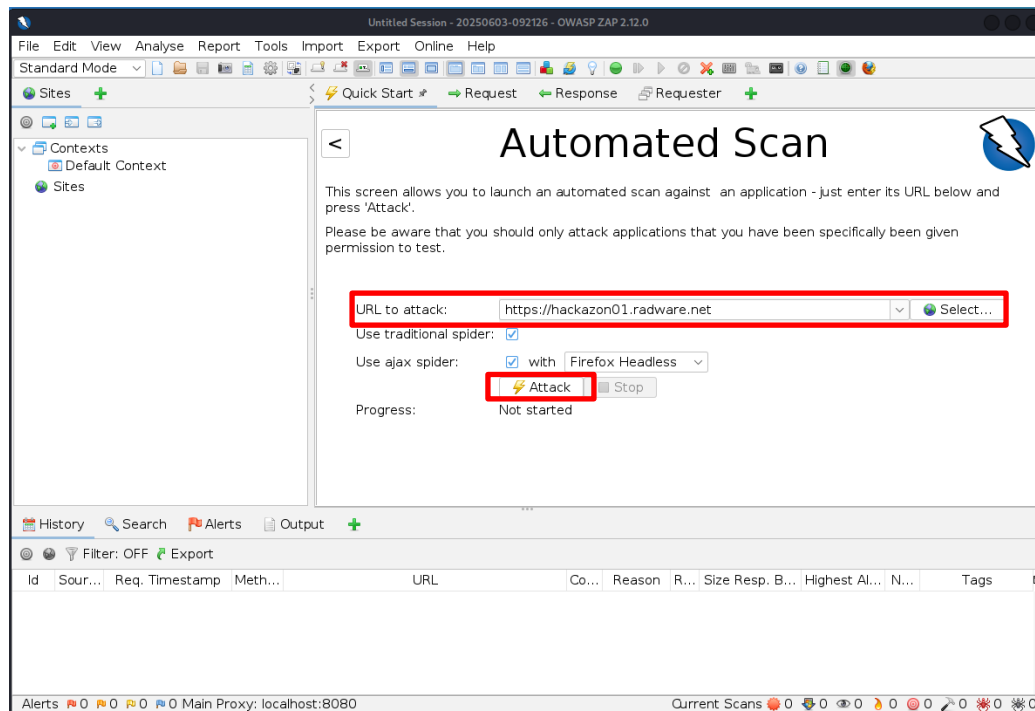
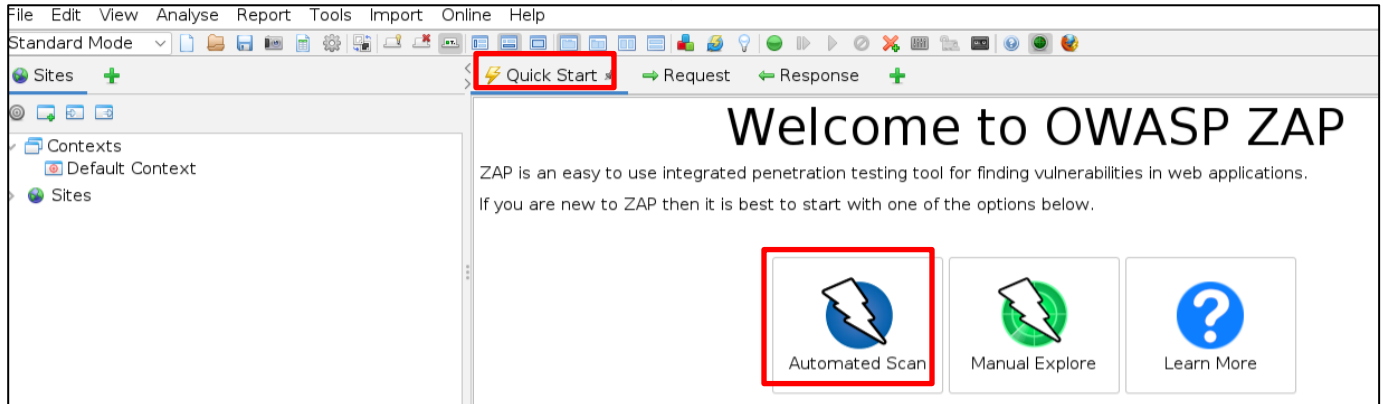
## ➡ MONITORING AND REPORTING WITH OWASP-ZAP


To generate some more traffic and events, we use the OWASP-ZAP tool which is installed on the Kali machine.

1. Click the **OWASP-ZAP** tool icon  on the top menu bar and wait a few moments until it starts.



2. In the ZAP tool select the **Quick Start** window, *click on Automated Scan*.



3. In the **URL to Attack** field, type the URL of your CloudWAF application, like in this example: <https://hackazon01.radware.net>
4. Click the  button.

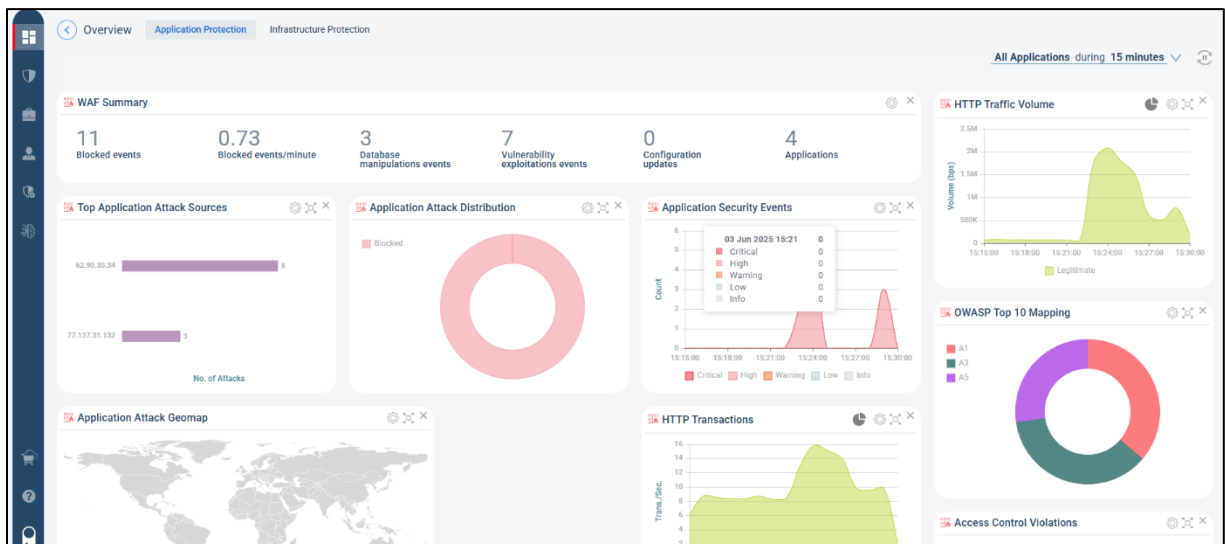
The tool will systematically browse the application to learn its structure; you can track its progress in the window below the quick start.

Let the tool run and return to the CloudWAF portal; remember, you need to wait several minutes until the portal displays the events.

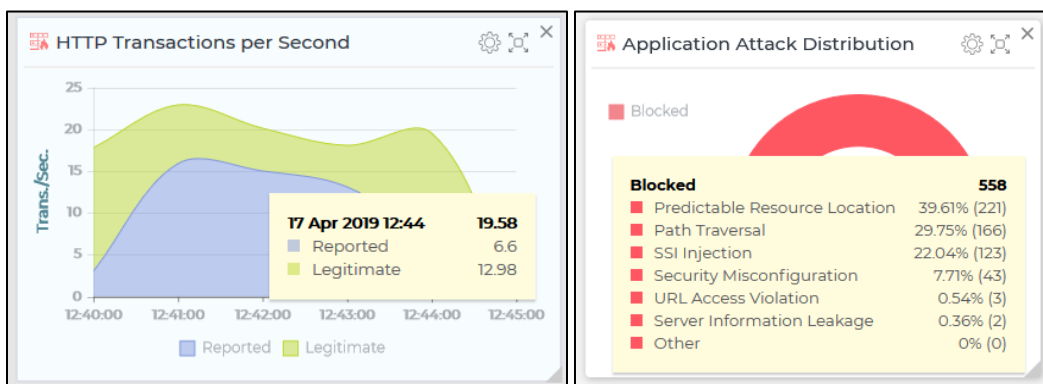
5. On the Cloud portal go to the **Dashboard** and set the time frame to the last 15 minutes; make sure your application is selected.

The screenshot shows the configuration interface for the Cloud portal dashboard. At the top, there is a dropdown menu with the application name "hackazon01". Below this, there are two sections: "Quick range" and "Time range". The "Quick range" section has buttons for "15m", "30m", "1H", "1D", "1W", "1M", "2M", and "3M", with "15m" selected. The "Time range" section shows a date and time range from "2025-06-03 15:10" to "2025-06-03 15:25". At the bottom, there are "Discard" and "Apply" buttons.

6. Wait a few minutes until you see some activity generated by the ZAP \*.



7. Review each of the widgets to see more details; hover over the graphs.



8. Go to **Monitoring > Security Events** and review the numerous events that accumulated there.

Security Events							
Application Protection							
Infrastructure Protection							
WAF DDoS Bot Web DDoS Protection							
Sort by Time 25 per page Page 1 Showing 1-11 out of 11 events							
Action	Time Last 15 minutes	Destination	Source	Security	Severity	More	
Blocked 2452463650	03 Jun 2025 15:29:36	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Database SQL Injection	High		
Blocked 2452463650	03 Jun 2025 15:29:36	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Database SQL Injection	High		
Blocked 2452463650	03 Jun 2025 15:29:36	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Database SQL Injection	High		
Blocked 207485535	03 Jun 2025 15:24:44	hackazon01 hackazon01.radware.net	77.137.31.132 Israel - IL	Vulnerabilities Predictable Resource Location	High		
Blocked 2452463639	03 Jun 2025 15:24:42	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Vulnerabilities Security Misconfiguration	High		
Blocked 190383092	03 Jun 2025 15:24:30	hackazon01 hackazon01.radware.net	77.137.31.132 Israel - IL	Vulnerabilities Security Misconfiguration	High		
Blocked 2452463638	03 Jun 2025 15:24:29	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Vulnerabilities Security Misconfiguration	High		
Blocked 2452463637	03 Jun 2025 15:24:28	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Vulnerabilities Predictable Resource Location	High		
Blocked 2436629429	03 Jun 2025 15:24:28	hackazon01 hackazon01.radware.net	62.90.30.34 Israel - IL	Vulnerabilities Predictable Resource Location	High		
Blocked 9024984629	03 Jun 2025 15:24:26	hackazon01 hackazon01.radware.net	77.137.31.132 Israel - IL	Allowed File Extension URL Access Violation	High		

9. To see what the tool is testing, you can click on an event and view its details, like in this example:

Back to Dashboard

Security Events

WAF DDoS

Sort by Time 25 per page Page 1 Showing 1-25 out of 245 events

Action	Time Last 5 minutes	Destination hackazon01	Source	Security	Severity	More
Blocked 180621005	08 Jul 2021 17:52:39	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Tunnel Module Server Information Leakage	Low	

Transaction ID: 180621005

Request Details

Security Details

Raw HTTP Request

Event can't be allowed

Host: hackazon01.radware.net

URI: /product/view

Source IP: 188.193.133.250

Source IP Geo-Location: Germany - DE

Source IP Reputation Score: N/A

OWASP Category: A3 - Sensitive Data Exposure

Security Module: Tunnel Module

Violation Type: Server Information Leakage

Severity: Low

Violation Details: This message is a response that matches a request on an event. You can get the event using the evtid

GET /product/view?id=%27%22%00%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0

Pragma: no-cache

Cache-Control: no-cache

Content-Length: 0

Referer: https://hackazon01.radware.net/category/view?id=3

Cookie: PHPSESSID=3dvhpaov657pttq0rmmmbckk3;

visited\_products=%2C101%2C1%2C24%2C152%2C95%2C176%2C28%2C105%2C33%2C67%2C30%2C194%2C51%2C72%2C99%2C44%2C195%2C13%2C13%2C98%2C54%2C102%2C93%2C143%2C43%2C200%2C202%2C197%2C208%2C210%2C203%2C206%2C199%2C196%2C185%2C191%2C193%2C187%2C189%2C175%2C160%2C182%2C184%2C177%2C179%2C171%2C174%2C167%2C169%2C162%2C164%2C150%2C140%2C135%2C157%2C158%2C151%2C147%2C149%2C141%2C144%2C137%2C139%2C130%2C120%2C110%2C132%2C134%2C127%2C128%2C122%2C124%2C116%2C119%2C112%2C114%2C90%2C106%2C107%2C96%2C97%2C92%2C86%2C88%2C89%2C66%2C77%2C79%2C82%2C84%2C69%2C71%2C74%2C62%2C75%2C65%2C37%2C40%2C42%2C48%2C50%2C55%2C31%2C35%2C27%2C11%2C6%2C23%2C17%2C19%2C20%2C15%2C7%2C9%2C10%2C3%2C

Host: hackazon01.radware.net

X-RDWR-CWAF: 188.193.133.250

X-RDWR-IP: 188.193.133.250

X-RDWR-PORT: 55479

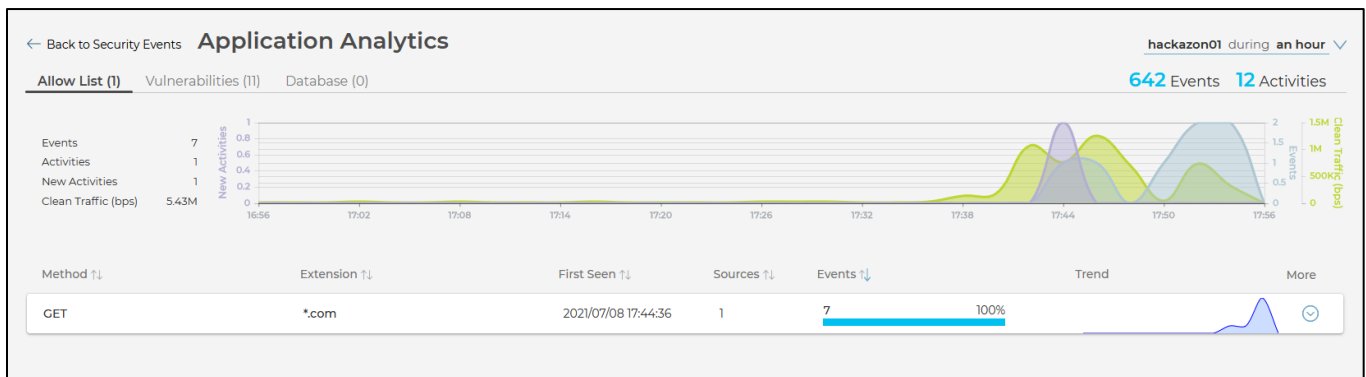
Now you'll review the **Application Analytics**, which aggregates security events to make the management easier.

1. Go to **Monitor > Analytics**.
2. Select your application, as time frame - the last hour (1H) and click **Apply**.

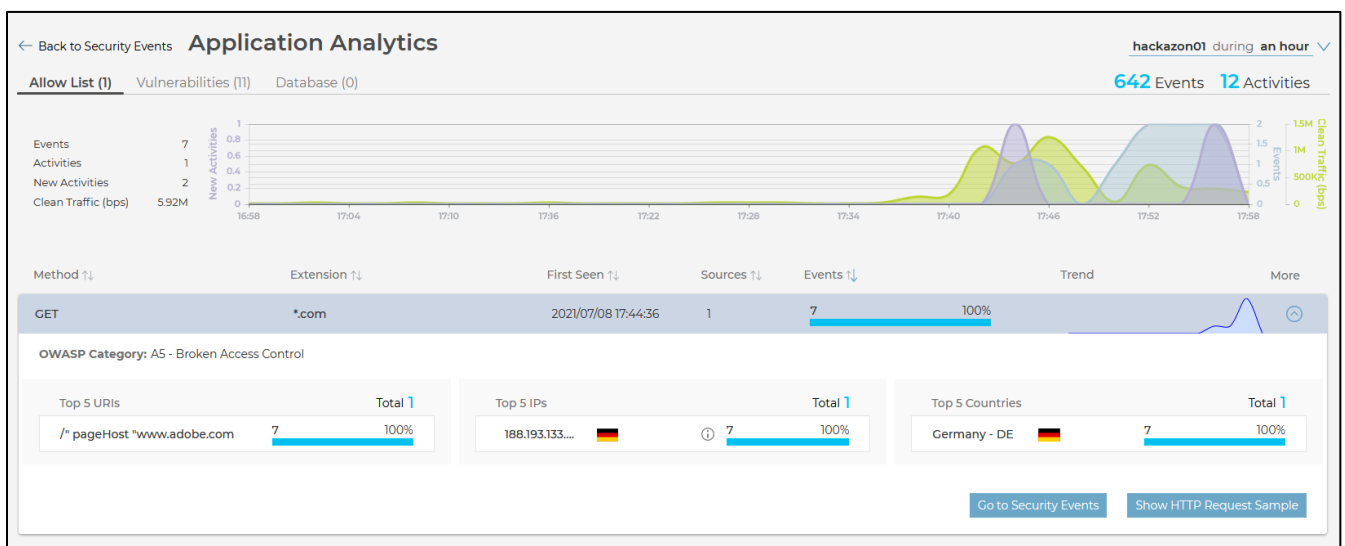
A filter dialog box titled "No Application during 7 days". It contains a dropdown menu with "hackazon01" selected. Below it is a "Filter by IP" input field. A "Quick range" section has buttons for "1H", "1D", "1W", "2W", and "1M", with "1H" selected. A "Time range" section shows "Jul 08, 2021 16:55" to "Jul 08, 2021 17:55". There are checkboxes for "Blocked" and "Reported". At the bottom is a "All countries" dropdown. Buttons for "Clear Filter", "Discard", and "Apply" are at the bottom.

3. Review the items in the **Allow List**, **Vulnerabilities** and **Database** section.

Click on each to see the relevant information.



To see an event's details, click on the event line and a summary will be presented:



4. Click on **Go to Security Events** button to see the related events.

← Back to Application Analytics **Security Events**

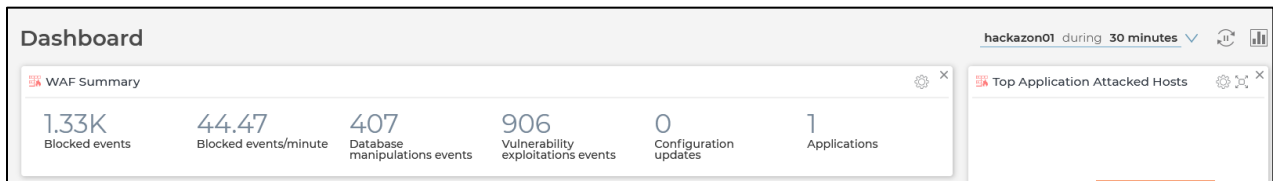
WAF DDoS

Sort by Time 25 per page Page 1

Showing 1-7 out of 7 events

Action	Time	Destination	Source	Security	Severity	More
Blocked 180621021	08 Jul 2021 17: 54: 40	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180621020	08 Jul 2021 17: 54: 39	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180621017	08 Jul 2021 17: 53: 38	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180620996	08 Jul 2021 17: 52: 25	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180620850	08 Jul 2021 17: 50: 59	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180620750	08 Jul 2021 17: 47: 12	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More
Blocked 180620568	08 Jul 2021 17: 44: 36	hackazon01 hackazon01.radware.net	188.193.133.250 Germany - DE	Allowed File Extension URL Access Violation	High	More

5. Change the timeframe to a longer period to see more events generated by the ZAP tool that is still running.



## ➔ CONFIGURE NOTIFICATIONS (ALERTS)

1. Go to **Security Events > Notifications** in the CloudWAF portal and click on the plus (+) sign to create a new notification.
2. Fill in the **New Alert** screen with the following parameters.

Parameter	Value
<b>Name</b>	SQL-Injections
<b>Type</b>	Select "Events Count"
<b>Description</b>	
<b>When</b>	Event count
<b>Is</b>	> 5
<b>For at least ...</b>	1
<b>Applications</b>	Choose your application
<b>Event Action</b>	Select Blocked
<b>Event Type</b>	SQL-Injection
<b>Send alerts by email to</b>	Type your email address
<b>Limit notifications to ...</b>	10

**Add New Notification**

SQL-Injection

Service \*

Application Protection

Type \*

Traffic Events Count Transactions Web DDoS

Description

Notification Description

For at least 1 consecutive periods of 5 minutes.

Application/s \*

TestNewOrigin

Event Action

Blocked Reported Modified

Event Type \*

SQL Injection

Method

Email SMS

Recipients \*

myemail@gmail.com

Limit notifications to 10 e-mails a day

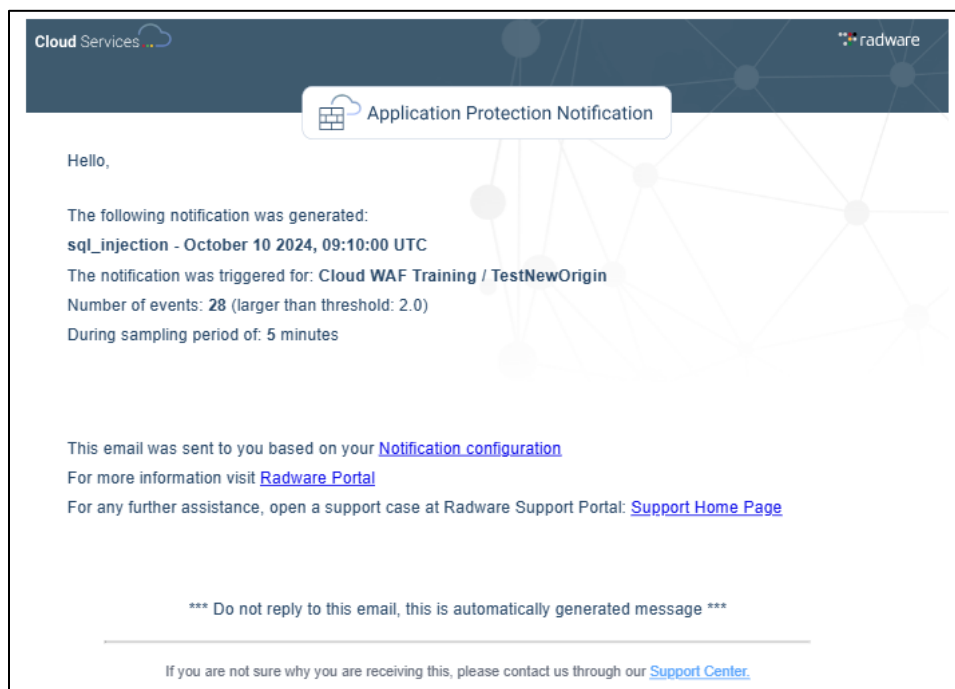
Cancel Save

3. Click **Save** to save your Alert.

Since ZAP is still running, you should get emails soon, but remember the silent period of 1 hour.

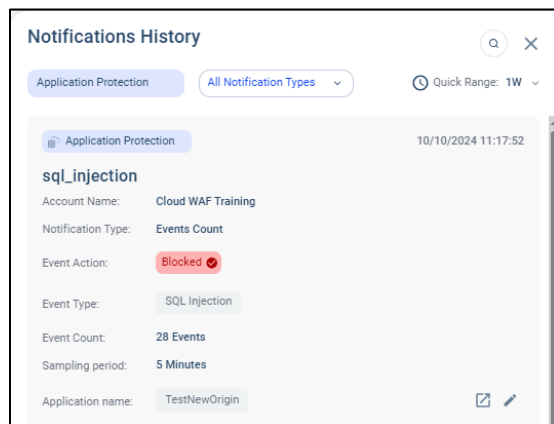
4. If you don't receive an email, check if ZAP is running and if it is, consider lowering the threshold.



Here is an example for an alert email:



If an alert is being triggered, the **Bell** symbol will turn yellow.

Click on the bell symbol to see the Notifications history.



Use the  symbol to see the security event details or use the  symbol to see the notification settings.

5. After you receive the email and you view the notification, remove the alert to make sure you are not flooded with emails!



## ➔ CONFIGURE REPORTS

1. Go to **Monitor > Reports** in the CloudWAF portal and click on the **plus (+)** sign to create a new alert.
2. Type your application name in the **Name** field
3. Select Service: **Application Protection**
4. Select your application
5. Add your email address to the Recipients.
6. Set the report to retrieve the report via email periodically
7. Select the **Report Period** to be Week.
8. Click **Save** to save your report
9. To force the report to be send now, open the report and click on **"Send"**, or you can download the pdf.

The screenshot shows the 'Add New Report' form with the following fields and options:

- Test** (Title)
- Overview** (Tab)
- Entity** (Dropdown menu)
- Applications** (Dropdown menu)
- Application/s \*** (Text field with 'TestNewOrigin' selected)
- Description** (Text field with 'Description' placeholder)
- Report Properties**
  - Date Range \*** (Dropdown menu)
  - 1D 1W 1M 3M** (Radio buttons, '1W' is selected)
- Report Schedule**
  - Frequency \*** (Dropdown menu)
  - Daily Weekly Monthly** (Radio buttons, 'Daily' is selected)
  - Every \*** (Text field with '1' selected)
  - day(s) at \*** (Text field with '11:15:00' selected)
- Recipients \*** (Text field with 'rainers@radware.com' entered)
- Cancel** and **Save** buttons

10. You should receive an email with the report you generated (only partial visible below).

The screenshot shows the 'Application Protection Report' with the following details:

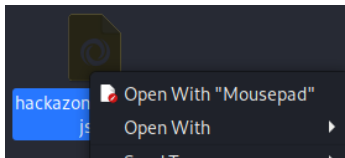
- Cloud Services** (Header)
- radware** (Header)
- Start** 03/10/2024 09:15 UTC
- End** 10/10/2024 09:15 UTC
- Application Protection Report** (Title)
- Test** (Section)
  - Account Name:** Cloud WAF Training
  - Application Name:** TestNewOrigin
  - Date Range:** 1W
- Table of Contents**
  - WAF Summary** 2
  - OWASP Top 10 Mapping** 2
  - Application Attack Distribution** 3
  - Application Security Events** 4
  - Top Application Attack Sources** 5
  - Top Application Attacked Hosts** 6

## ➔ API PROTECTION

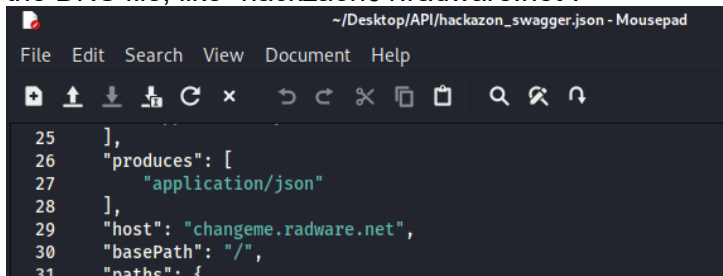
Application development and delivery environments are more amorphic and elastic than ever before, bringing together independent components that interoperate and facilitate secure application delivery. The cement of these emerging architectures are APIs that allow data exchange, integration and automation. APIs are in use for back-end systems, microservices, mobile apps, serverless architectures and event-driven processes. As a result, it's critical to safeguard exposed APIs from an array of cyberthreats, such as data theft, data manipulation, account takeover attacks, and more.

Let's now see how we can protect APIs with the CloudWAF

1. On the remote Client open the API folder located on the desktop and right-click on the "hackazon\_swagger.json" file and select "Open With Mousepad".

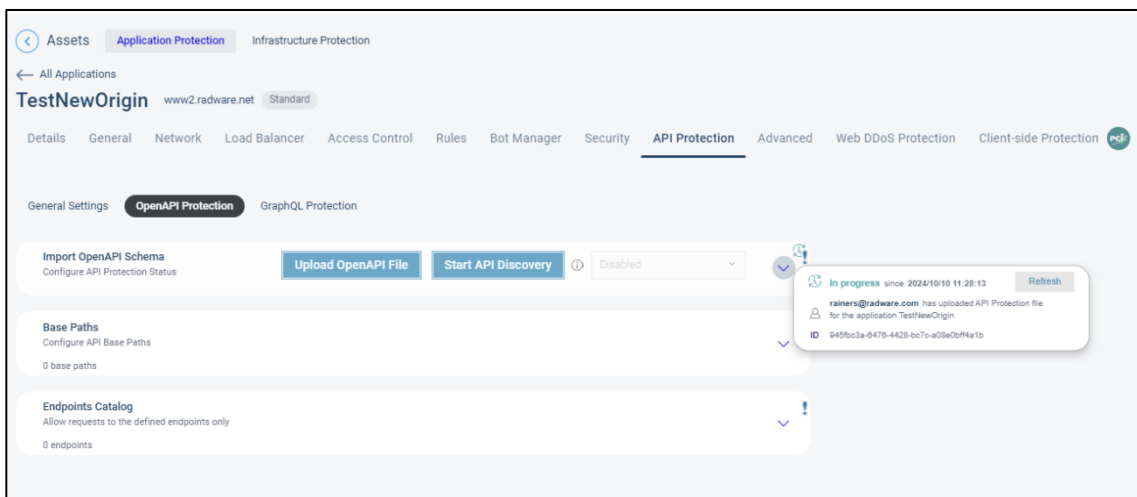


2. At line 29 change the "host" value from "changeme.radware.net" to your domain you entered in the DNS file, like "hackzaon01.radware.net".

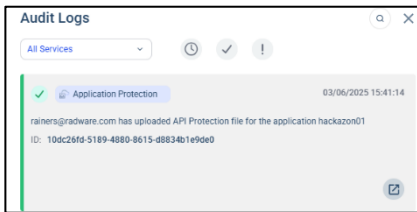


NOTE: Make sure it is the same name used on the CloudWAF portal for the application, otherwise the upload will fail!

3. Save the file.
4. On the CloudWAF portal go to **Assets > Applications** click on your application and go to **API Protection > OpenAPI Protection**.
5. Click on Upload OpenAPI File and upload the changed swagger file.
6. After the upload you should see a successful message and as sign that the file handling is in progress



7. After a short while you should see a new message at the "Activity Logs". It should indicate that the file was successfully uploaded and handled



8. After it is uploaded and processed you should see one base path (/) at **Base Paths** and 15 endpoints at **Endpoints Catalog**

Details General Network Load Balancer Access Control Rules Bot Manager Security **API Protection** Advanced

General Settings **OpenAPI Protection** GraphQL Protection

Import OpenAPI Schema  
Configure API Protection Status

Upload OpenAPI File Start API Discovery ⓘ Report Only

**Base Paths**  
Configure API Base Paths  
1 base paths

**Endpoints Catalog**  
Allow requests to the defined endpoints only  
15 endpoints

Showing 15 out of 15 The filtered results have changed

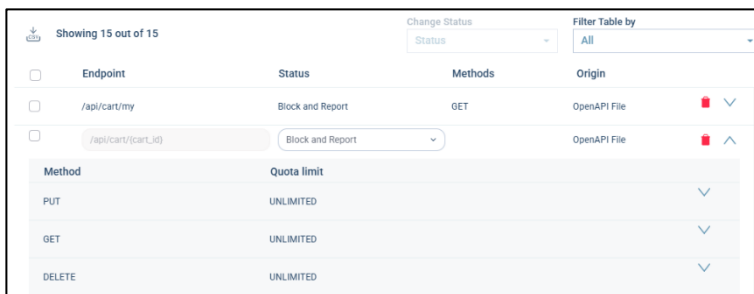
Change Status  
Status

Filter Table by  
All

<input type="checkbox"/>	Endpoint	Status	Methods	Origin	
<input type="checkbox"/>	/api/auth	Block and Report	GET	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/category	Block and Report	GET	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/user/me	Block and Report	GET	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/product	Block and Report	GET	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/product/{product_id}	Block and Report	GET	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/cartItems	Block and Report	POST	OpenAPI File	<input type="checkbox"/> ✓
<input type="checkbox"/>	/api/customerAddress	Block and Report	POST, GET	OpenAPI File	<input type="checkbox"/> ✓

Cancel Submit

9. For each endpoint you can see the details like the path, status and allowed methods. For example view the `/api/cart/{cart_id}` endpoint.

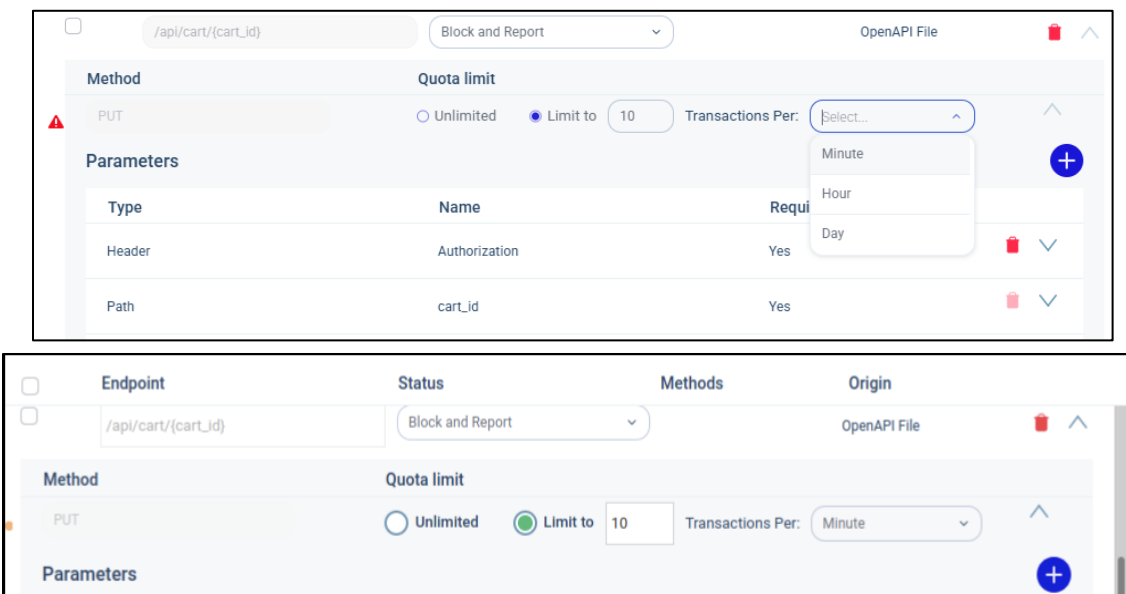


Endpoint	Status	Methods	Origin
/api/cart/my	Block and Report	GET	OpenAPI File
/api/cart/{cart_id}	Block and Report		OpenAPI File

Method	Quota limit
PUT	UNLIMITED
GET	UNLIMITED
DELETE	UNLIMITED

10. For each endpoint you can also configure a quota on how many transactions per timeframe (Minute/Hour/Day) can be performed.



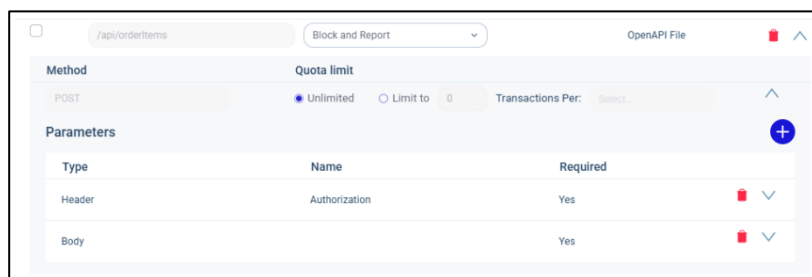
Endpoint: `/api/cart/{cart_id}` Status: Block and Report Methods: PUT Origin: OpenAPI File

Method: PUT Quota limit: ☐ Unlimited ☒ Limit to 10 Transactions Per:

Parameters

Type	Name	Required
Header	Authorization	Yes
Path	cart_id	Yes

11. Parameter are also visible, which needs to be present for an API request.

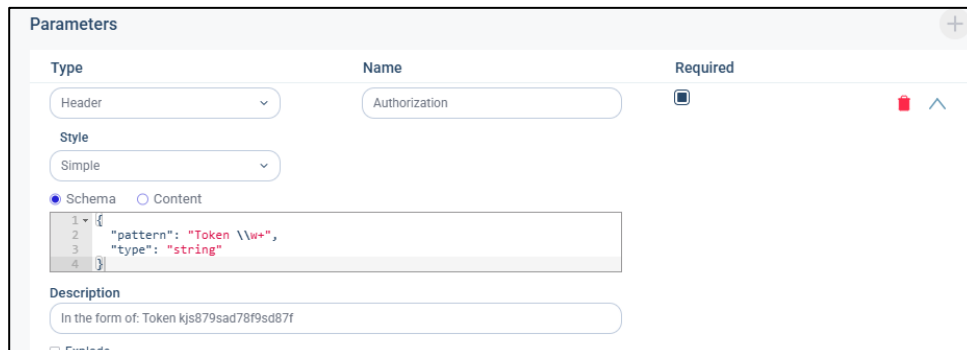


Endpoint: `/api/orderItems` Status: Block and Report Methods: POST Origin: OpenAPI File

Method: POST Quota limit: ☒ Unlimited ☐ Limit to 0 Transactions Per:

Parameters

Type	Name	Required
Header	Authorization	Yes
Body		Yes



Parameters

Type	Name	Required
Header	Authorization	<input checked="" type="checkbox"/>

Style: Simple

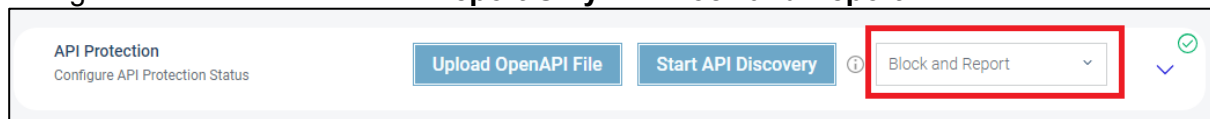
☒ Schema ☐ Content

```
1 {
2   "pattern": "Token \\w+",
3   "type": "string"
4 }
```

Description: In the form of: Token kjs879sad78f9sd87f

☐ Explode

12. You can also add new parameters in case the application has changed after the OpenAPI file was created.
13. Since we want to block all requests violating the OpenAPI file definition, make sure that you change the API Protection form “**Report Only**” to “**Block and Report**”.

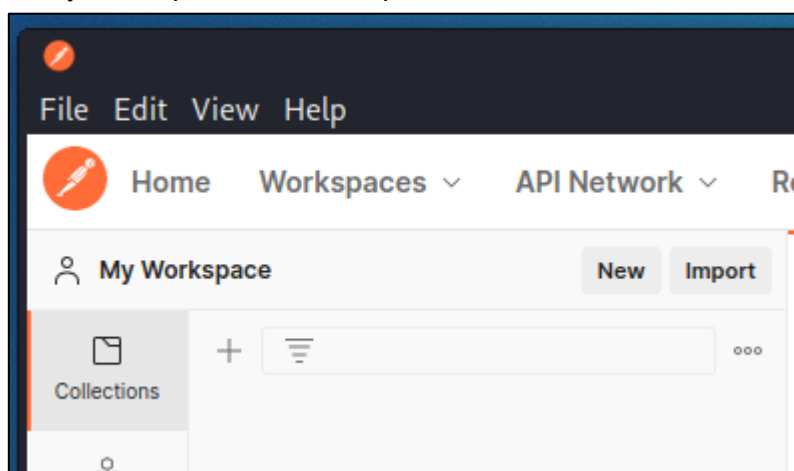


14. To create an API based attack, open on the remote client the Postman application from the desktop. In case Postman complains about the login, click on logout and login using the following credentials:



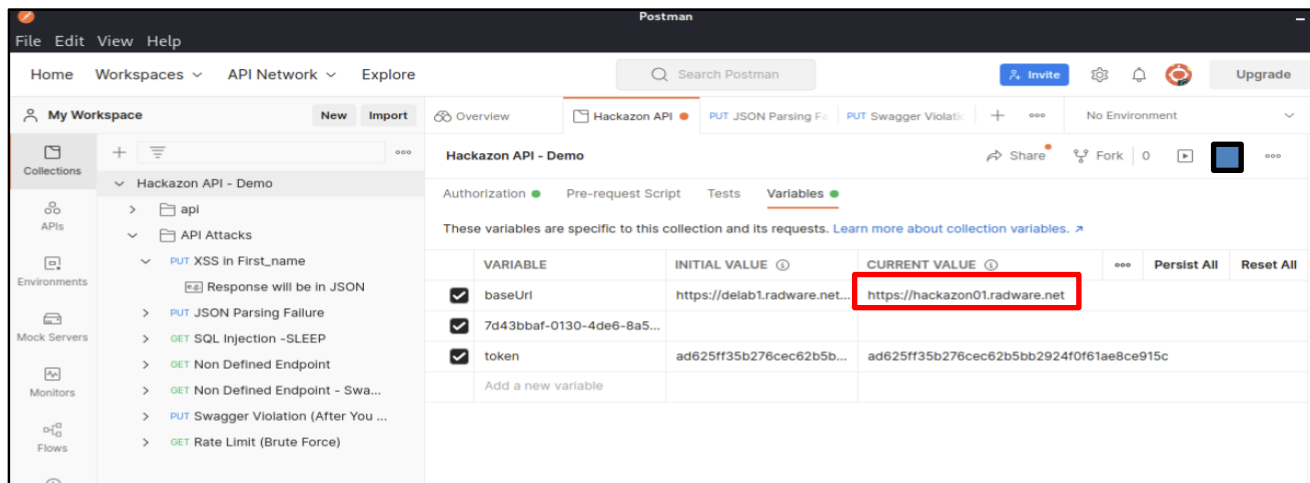
username: radwarevirtuallab@radware.com  
password: radware24!

15. At My Workspace click on Import

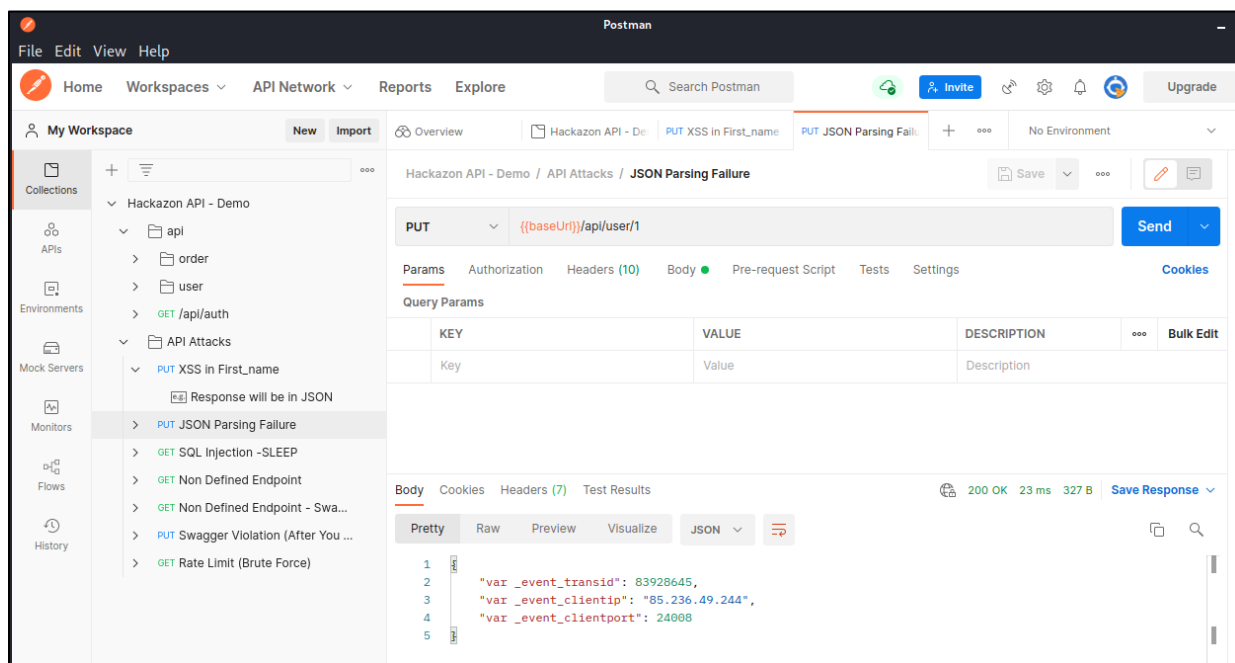


16. Click on “Uploaded Files” and navigate to the desktop/API folder and select “Hackazon API – postman\_collection.json” and click on import

17. After the collection is imported select “Hackazon API – Demo” and select on the right side the “Variables”. Change the baseUrl > Current Value from <https://delab1.radware.net:1234/> to the URL you use like <https://hackazon01.radware.net> and click Save (disk icon).



18. In the collection expand the “API Attacks” section and select “Json Parsing Failure”. On the right side click on send. In the Response you should see that it was blocked, since the \_event\_transid and is visible. As you can see for API protections, the response is in JSON format not the regular security page.



19. Check the Security Events on the cloud portal you should see the corresponding event.

Security Events

Application Protection

Infrastructure Protection

WAF

DDoS

Bot

Web DDoS Protection

Sort by Time

25 per page

Page 1

Showing 1-1 out of 1 events

Action	Time Last 15 minutes	Destination	Source	Security	Severity	More
Blocked 207925542	03 Jun 2025 15:55:47	hackazon01 hackazon01.radware.net	77.137.31.132 Israel - IL	API Security Module API Security - Violation	High	

Transaction ID: 207925542

Request Details

Security Details

Raw HTTP Request

Application: hackazon01

Host: hackazon01.radware.net

URL: /api/user/1

Source IP address: 77.137.31.132

Source IP Geo-Location: Israel - IL

Source IP Reputation Score: N/A

Security Module: API Security Module

Violation Type: API Security Violation

Severity: High

Violation Details: A request to an API endpoint included one or more parameters that failed validation.

Description: API Security Violation Detected.  
Endpoint: /api/user/{user\_id}  
Method: PUT  
Violation: Request Body Validation Failure:  
Parameter: application/json - Error: the string is not a valid json or xml and cannot be parsed

Suggestion: Review API Security settings if needed

Module: API Security

Error Number: -216

Authenticated as Public

PUT /api/user/1 HTTP/1.1

Host: hackazon01.radware.net

X-RDWR-IP: 77.137.31.132

X-RDWR-PORT: 48744

X-RDWR-PORT-MM-2065-PE-PORT: 443

X-RDWR-PORT-MM-21045

X-RDWR-APP-ID: d6f2d2b7-dfb3-4e85-8556-79cfe9c6260

Content-Length: 324

Content-Type: application/json

Authorization: Basic d0VzdF91c2VvOjEYmzQ1Ng==

User-Agent: PostmanRuntime/7.37.3

Accept: \*/\*

Cache-Control: no-cache

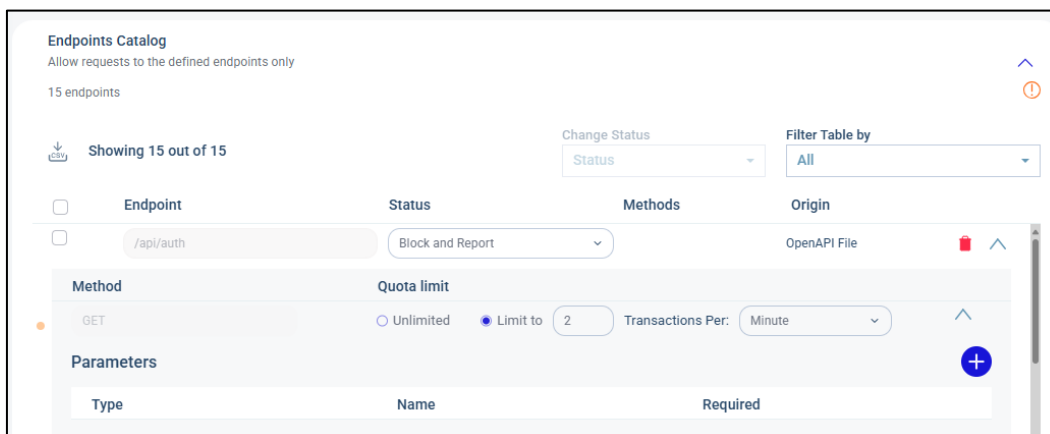
Postman-Token: 572f35f7-f027-44aa-8ad1-856d3b8a813b

Accept-Encoding: gzip, deflate, br

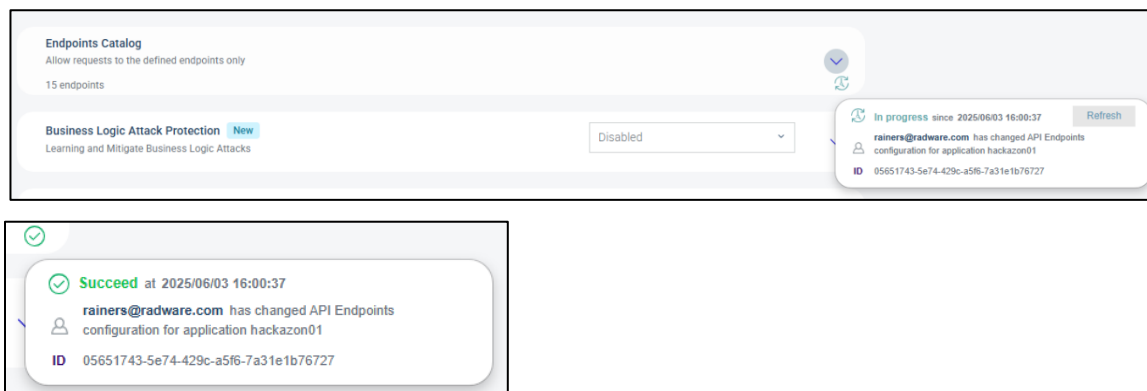
Go to API Protection Configuration



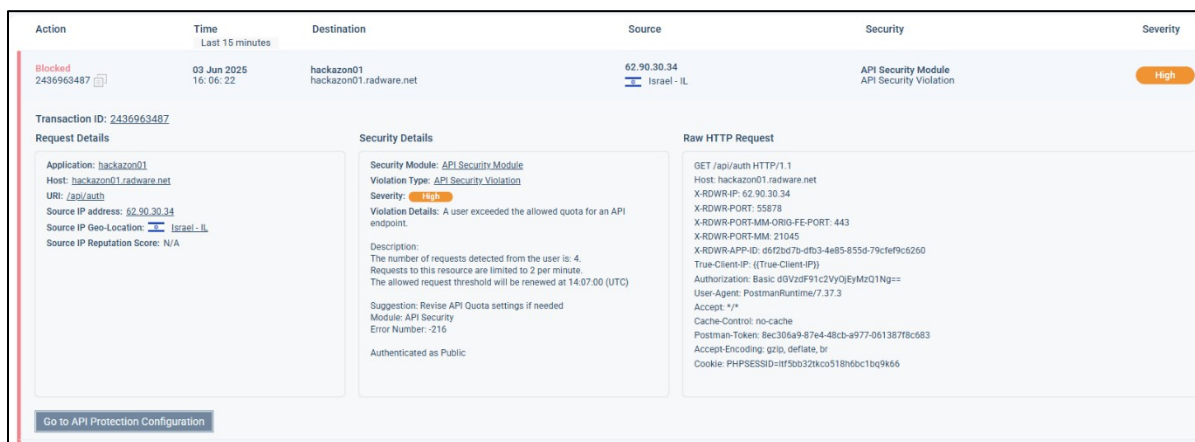
20. Try also the other attacks: XSS in First\_name, SQL Injection, Swagger Violation and you should see the corresponding events.
21. Let us configure a Quota limit how often the authentication via the API can be performed. On the Application go to API Protection and at Endpoints Catalog select the path `/api/auth`. Add a quota limit of 2 transactions per Minute. Scroll down and click Submit.



22. Make sure that the change was processed. After it was successful processed you should see the green tick instead of the clock



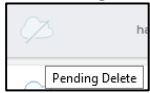
23. Now use the "Rate Limit (Brute Force) attack in the Postman and run it a couple of times, after a few requests (>2 per minute) the Quota limit should be triggered, and you should see the blocking information.
24. See the corresponding security event on the Cloud portal



25. This is the end of the inline lab manual.

26. Before you close the lab you can delete your application if you don't want to continue practicing.

At **Assets > Applications** use the trash can icon at your application. You should see an icon showing that your application is pending delete:



27. If you finished with the lab, please send an email to [radwarevirtuallab@radware.com](mailto:radwarevirtuallab@radware.com), so your account can be deleted.

*This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.*

©2025 Radware Ltd. All rights reserved. Radware and all other Radware product and service names are registered trademarks or trademarks of Radware in the U.S. and other countries. All other trademarks and names are property of their respective owners. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications. For more details please see: <https://www.radware.com/LegalNotice/>

