

# Lab 4: Edge Services - Web Application Firewall Workshop

---

## Objectives of the workshop

1. Host the JuiceShop application on OCI VM
2. Domain name setup and DNS configuration in freenom.com.
3. Setup a Web Application Firewall (WAF) Policy on OCI for a Web app to clearly demonstrate the role of a WAF.
4. Setup Access Control Rules to detect, log and block access to the Web Application using invalid URL and HTTP Headers.
5. Test the Access Rules.
6. Setup Protection Rules in the WAF policy to protect Web Application from targeted attacks like Cross-site scripting, SQL Injection etc.
7. Test the protection rules.
8. Setup JavaScript Challenge in Bot Management Policies
9. Test JavaScript Challenge using cURL utility and the browser.

## Workshop Prerequisites

1. A OCI VCN with public subnet and access to Internet
2. OCI Account with access to manage WAF Policies.
3. Google Chrome browser – required to test Header based Access Rule for the web application.
4. One Different Browser to test the use cases for the unprotected web application (i.e. when we directly access the web application we setup using the compute instance's public IP address) – recommended but not required as we can use incognito mode/Add People feature in Google Chrome.
5. cURL utility or Postman client.

## Sections

- [Host the JuiceShop application on OCI VM](#)
- [Domain name setup and DNS configuration in Freenom](#)
- [Setup Web Application Firewall Policy on OCI](#)
- [Setup Access Control Rules](#)
- [Test the Access Rules](#)
- [Setup Protection Rules](#)
- [Test Protection Rules](#)
- [Setup JavaScript Challenge in Bot Management](#)
- [Test JavaScript Challenge](#)

## Host the JuiceShop application on OCI VM

Let us first create a Virtual Machine in a public subnet of your VCN. Log in to OCI console and navigate to Compute --> Instance

The screenshot shows the Oracle Cloud Applications Console interface. The left sidebar is titled "Core Infrastructure" and contains several categories: Compute, Block Storage, Object Storage, File Storage, Networking, Database, Autonomous Data Warehouse, Autonomous Transaction Processing, Bare Metal, VM, and Exadata, and Data Safe. Under the "Compute" category, the "Instances" option is selected, which is highlighted with a blue background. To the right of the sidebar, there are three main sections: "TRANSACTION database" (with a database icon), "AUTONOMOUS DATA WAREHOUSE Create an ADW database" (with a database icon), and "RESOURCE MANAGER Create a stack" (with a stack icon). Each section includes a short description and a time estimate (e.g., "3-5 mins" or "2-6 mins"). At the bottom right of the sidebar, there is a "Collapse" button.

Click *Create Instance* and select Oracle Linux with any available shape. Select your VCN, the corresponding public subnet, pass your SSH public key, and click *Create*

The screenshot shows the "Create Compute Instance" page. The "NAME" field is filled with "JuiceShopVm". Below it, the "Image or operating system" section shows "ORACLE Linux" selected, with "Oracle Linux 7.8" and "Image Build: 2020.04.17-0" listed. A "Change Image" button is also present. Further down, there are sections for "Availability domain" (with options AD 1, AD 2, and AD 3), "Shape" (with a dropdown menu), and buttons for "Create" and "Cancel".

SSH into the VM and run the following commands to install docker

```
ssh -i <private-key> opc@<public-ip-of-vm>
```

```
sudo yum install docker-engine  
sudo systemctl start docker  
sudo systemctl enable docker
```

Run the following command to pull the [JuiceShop](#) docker image and run the application on port 80

```
docker run -d -p 80:3000 bkimminich/juice-shop
```

Now navigate to the public subnet of your VCN, select its security list and add stateful ingress port 80 for it be accessible over the internet

Screenshot of Oracle Cloud Networking interface showing a Regional Public Subnet named "S". The subnet is available and has the following details:

- OCID:** ...7lb47q [Show](#) [Copy](#)
- CIDR Block:** 172.16.0.0/19
- Virtual Router Mac Address:** 00:00:17:77:A1:DC
- Subnet Type:** Regional
- Compartment:** AllTeamSharedCompartment
- DNS Domain Name:** regionpublic... [Show](#) [Copy](#)
- Subnet Access:** Public Subnet
- DHCP Options:** Default DHCP Options for StaticVCN
- Route Table:** Default Route Table for StaticVCN

**Resources**

**Security Lists**

Name	State	Compartment	Created
Default Security List for StaticVCN	Available	AllTeamSharedCompartment	Mon, Apr 6, 2020, 19:09:07 UTC

Showing 1 Item < Page 1 >

**Edit Ingress Rule**

**Ingress Rule 1**

**TCP traffic for ports: 80**

**STATELESS** *(i)*

**SOURCE TYPE** **SOURCE CIDR** **IP PROTOCOL** *(i)*

CIDR	0.0.0.0/0	TCP
------	-----------	-----

Specified IP addresses: 0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

**SOURCE PORT RANGE** *OPTIONAL* *(i)* **DESTINATION PORT RANGE** *OPTIONAL* *(i)*

All	80
-----	----

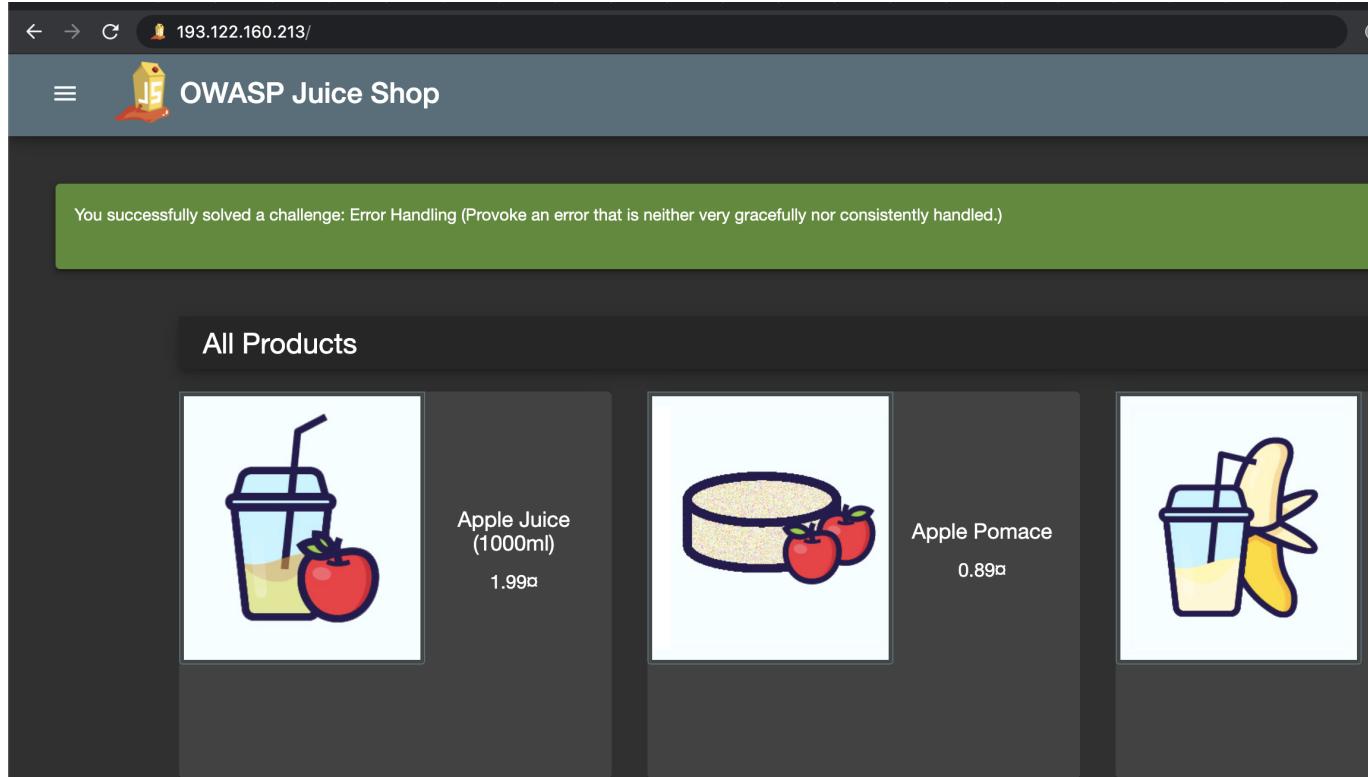
Examples: 80, 20-22 Examples: 80, 20-22

**DESCRIPTION** *OPTIONAL*

Maximum 255 characters

**Save Changes** **Cancel**

The application should be accessible if you open a browser and enter the IP of the host machine.



## Domain name setup and DNS configuration in Freenom

Let visit freenom.com and register a free domain (usually .tk, .gq, .cf etc) and also use their own DNS service to add a DNS A Record and CNAME Record for the registered domain. If you have the domain name setup and mapped to the origin hosting the Web application, then you can move onto next section.

Create an account, login and search if the domain you wish to register is available. In this workshop, I will be using the domain [networkinglab.tk](#) which is registered with freenom. In this workshop when we are testing out the WAF Policies, replace the [networkinglab.tk](#) with the domain name that you create with freenom

The screenshot shows the Freenom website at <https://www.freenom.com/en/index.html?lang=en>. A search bar at the top contains the name "umeshtanna". Below it, a blue header bar features the Freenom logo and navigation links for "Services", "Partners", "About Freenom", "Support", "Sign in", and "English". A large blue button labeled "Check Availability" is prominent.

A message at the top says "Get one of these domains. They are free!" followed by a list of five free domain options:

Domain Name	Status	Price	Action
umeshtanna.tk	FREE	USD 0.00	Selected
umeshtanna.ml	FREE	USD 0.00	Get it now
umeshtanna.ga	FREE	USD 0.00	Get it now
umeshtanna.cf	FREE	USD 0.00	Get it now
umeshtanna.gq	FREE	USD 0.00	Get it now

Below this, another section titled "Cost Price Domains cannot be found cheaper elsewhere!" lists three cost-priced domain options:

Domain Name	Status	Price	Action
umeshtanna.com	COST PRICE	USD 8.38	Select
umeshtanna.net	COST PRICE	USD 6.71	Select
umeshtanna.org	COST PRICE	USD 9.38	Select

Select the time period depending on how long you wish to keep the domain name and then click on continue

The screenshot shows the Freenom website at <https://my.freenom.com/cart.php?a=confdomains&language=english>. The top navigation bar includes "Services", "Partners", "About Freenom", "Support", "Sign in", and "English". A large blue button labeled "Check Availability" is visible.

A central box displays the message "Find a new FREE domain" and a "Check Availability" button.

Below this, a table allows configuration of the domain "umeshtanna.tk".

Domain	IDSHIELD	Use your new domain	Period
umeshtanna.tk		Forward this domain or Use DNS	12 Months @ FREE

A "Continue" button is located at the bottom right of the configuration area.

We can use Freenom's DNS service to direct any traffic for your domain to the IP address of your web application. Essentially it is mapping your domain name to the IP address of the machine hosting the Web Application

This mapping is called a DNS A Record and this record can be added on freenom's DNS Management console or your DNS providers management console

Below screenshot shows creation of A records while we are registering the domain. Enter the public IP of the VM we just created under both the IP address fields.

The screenshot shows the Freenom domain registration interface. At the top, there is a navigation bar with links for Apps, Oracle, Learning, Personal, Services, Partners, About Freenom, Support, Sign in, and English. Below the navigation bar, there is a search bar with the placeholder "Find a new FREE domain" and a large blue button labeled "Check Availability".

The main area is titled "Domain" and shows the registered domain "umeshtanna.tk". There are two options for DNS management: "Forward this domain" and "Use DNS". The "Use DNS" option is selected, indicated by a green checkmark icon. Below this, there are two sets of input fields for creating A records:

Hostname	IP address
umeshtanna.tk	[Empty]
www.umeshtanna.tk	[Empty]

At the bottom right of the main area, there is a "Period" dropdown set to "12 Months @ FREE".

Once you complete the process, the domain should be active in a few minutes. If you've used the DNS Service by Freenom then you can check the DNS settings under Manage Domain -> Manage Freenom DNS.

Below screenshot shows the configured A records for the registered domain. Make sure you have two records, if not, you can edit and save changes.

**DNS MANAGEMENT for trywaf.tk**

+ Back to domain details

Modify Records

Name	Type	TTL	Target	Action
	A	300	130.61.93.185	Delete
WWW	A	300	130.61.93.185	Delete

Save Changes

Add Records

Name	Type	TTL	Target
	A	3600	

+ More Records Save Changes

The domain is now setup and ready to be used to setup a WAF Policy on OCI

Visit your domain with [www.<your-domain-name>.tk](http://www.<your-domain-name>.tk) and it should point to your juice shop application

## Setup Web Application Firewall Policy on OCI

On the OCI console, navigate to WAF Policy by clicking on the hamburger menu -> Security -> WAF Policies

The screenshot shows the OCI console interface. The left sidebar has a navigation menu with various services like Analytics, Resource Manager, Email Delivery, Application Integration, Monitoring, Logging, Developer Services, Marketplace, More Oracle Cloud Services, Platform Services, Classic Data Management Services, Classic Infrastructure Services, Governance and Administration, Account Management, Identity, Security (which is selected), Governance, and Administration. The main content area is titled "Ingress Rules" and shows a table with one row. The table columns are "Stateless", "Source", and "IP Protocol". The row contains: "No", "0.0.0.0/0", and "TCP". Below the table, there are buttons for "Add Ingress Rules", "Edit", and "Remove". The "WAF Policies" section is highlighted in the navigation bar.

Stateless	Source	IP Protocol
No	0.0.0.0/0	TCP

**Ingress Rules**

Add Ingress Rules Edit Remove

Stateless	Source	IP Protocol
No	0.0.0.0/0	TCP

0 Selected

Click on Create WAF Policy. Enter the domain name and URI for the web application

Create WAF Policy [Help](#) [Cancel](#)

POLICY NAME OPTIONAL [\(i\)](#)

Domains

PRIMARY DOMAIN [\(i\)](#)

ADDITIONAL DOMAINS OPTIONAL [\(i\)](#)

[X](#)

[+ Additional Domain](#)

WAF Origin

ORIGIN NAME

Must be a unique identifier.

URI [\(i\)](#)

IPv4 address or FQDN.

[Show Advanced Origin Options](#)

Once WAF policy is created a property called CNAME target gets created. It consists of a hyphenated version of the domain name

Use this CNAME target and modify the DNS Settings in DNS Service Provider management console. If you are using the domain registered and DNS managed by freenom, the screenshot below shows the changes to be made.

Under target column for the www A Record, remove the IP address of the host and add the CNAME Target of the WAF Policy to route incoming traffic through the WAF for the Web application

The screenshot shows the Freenom DNS Management interface. At the top, there's a navigation bar with links for Services, Partners, About Freenom, Support, Hello Raj, and English. The main title is "DNS MANAGEMENT for networkinglab.tk". Below the title, there's a message "Record added successfully". The "Modify Records" section shows two entries: one for "A" type with target "193.122.160.213" and another for "CNAME" type with target "www-networkinglab-tk.o.waas.oci.oraclecloud.net". Both entries have "Delete" buttons. A "Save Changes" button is located at the bottom right of this section. Below it, the "Add Records" section is partially visible.

## Add Records

Name	Type	TTL	Target
	A	300	193.122.160.213
WWW	CNAME	300	www-networkinglab-tk.o.waas.oci.oraclecloud.net

[Save Changes](#)

[+ More Records](#) [Save Changes](#)

Before we move to the protection rules, let us take a look at the Access Control Rules to have a restricted access to the web application

## Setup Access Control Rules

For this, we can use a simple webpage and use a simple Webserver like Apache to host the sample web page

Click on the created WAF Policy to view more information about it and to configure Access Control rules. Click on Access Rules from the options menu on the left side of the OCI WAF console

The screenshot shows the Oracle Cloud WAF Policy Overview page. At the top, there's a header with "ORACLE Cloud" and a search bar. The main content area has tabs for "Policy Information" and "Tags", with "Policy Information" selected. It displays details about the WAF Policy: Name (SHJuiceShop), Primary Domain (www.shjuiceshop.tk), Additional Domains (No Value), OCID (...75njqq), CNAME Target (www.shjuiceshop-tk.b.waas.oci.oraclecloud.net), and Date Created (Thu, May 30, 2019, 9:07:21 PM UTC). Below this, there's an "ACTIVE" status indicator. The "WAF Policy" section has a sidebar with "Overview", "Origin Management", "Settings", "Access Control" (which is highlighted with a red box), "Bot Management", "Logs", and "Unpublished Changes". The "Overview" section contains boxes for "Origin Management", "Protection Rules", "Settings", and "Access Control". The "Origin Management" box describes defining ports and URLs for origin servers. The "Protection Rules" box describes predefined security rules. The "Settings" box describes managing domain keys and SSL certificates. The "Access Control" box describes defining explicit actions for requests based on conditions. At the bottom, there are links for "Terms of Use and Privacy" and "Cookie Preferences", and a copyright notice: "Copyright © 2019, Oracle and/or its affiliates. All rights reserved."

Click on Add Access Rule. Let us add an Access Rule that blocks users trying to access the web-application with unwanted parameters in the URL by showing an error page with appropriate message and description

The screenshot shows the Oracle Cloud WAF Policy configuration for the domain 'SHJuiceShop'. The 'Access Control' tab is active, displaying the 'Access Rules' section. A red box highlights the 'Add Access Rule' button, which is located at the top of the rule list table.

Give a name to the Access Rule. Under Conditions, from the rule conditions dropdown select URL is option and specify /foo under URL Address. This is going to block any access to you web application origin with the URL <http://www.<your-domain-name>/foo>

## Edit Access Rule

[Help](#)

**NAME**  
Invalid\_URL

**Conditions**

All conditions must match for set action to be taken.

CONDITION <i>i</i>	URL ADDRESS <i>i</i>
URL is	/foo

A total of 1 condition(s) must match for action to be taken.  
[+ Additional Condition](#)

**Action**

LOG AND ALLOW    DETECT ONLY    BLOCK    REDIRECT    BYPASS    SHOW CAPTCHA

Block request with just setting the response code and showing the browser page for selected response code.

BLOCK ACTION *i*

Show Error Page

Under Actions select Block as Rule Action. From the Block Action Dropdown select Set Error Page. Enter the appropriate values for the Error Page that should be displayed when this rule is triggered. Click on Add Access Rule

### Action

**RULE ACTION**

**LOG AND ALLOW**  
Log all matched requests and take no further action.

**DETECT ONLY**  
Create a detection for all matched requests and take no further action.

**BLOCK**  
Block request with just setting the response code and showing the browser page for selected response code.

**BLOCK ACTION** (i)

Show Error Page

**BLOCK ERROR PAGE MESSAGE** (i)

Access is blocked.

**BLOCK ERROR PAGE DESCRIPTION** (i)

Access blocked by website owner. Please contact support. Unsupported Path Parameter

**BLOCK ERROR PAGE CODE** (i)

Access Rules-403

**Add Access Rule** Cancel

Let's add another Access Rule. Click on Add Access Rule and give the name `HTTPHeaderAccessRule`. We will block access to the web application for any request with the header key **`name`** and value **`blockme`**. We can use MOD Header browser extension for Google Chrome to test this one out. For Rule Action, we select Block, same as previously created Action Rule. For Block Action select Show Error Page and enter appropriate Error message and description. Click on Add Access Rule

### Add Access Rule

[help](#) [cancel](#)

**NAME**

**RULE CONDITION *i***

HTTP Header contains  X

[+ Additional Condition](#)

### Conditions

**RULE ACTION**

**LOG AND ALLOW**  
Log all matched requests and take no further action.

**DETECT ONLY**  
Create a detection for all matched requests and take no further action.

**BLOCK**  
Block request with just setting the response code and showing the browser page for selected response code.

### Action

**BLOCK ACTION *i***

Show Error Page

**BLOCK ERROR PAGE MESSAGE *i***

Access is blocked.

**BLOCK ERROR PAGE DESCRIPTION *i***

Access blocked by website owner. Please contact support.

**BLOCK ERROR PAGE CODE *i***

Access Rules-403

**Add Access Rule** X

Now we have to publish the changes to the WAF policy. Navigate to Unpublished Changes. Click on the Publish All Button.

The screenshot shows the Oracle Cloud WAF Policy Management interface. At the top, there's a navigation bar with the Oracle Cloud logo and various icons. Below it, a sidebar on the left lists categories like Overview, Origin Management, Settings, Protection Rules, Access Control, Bot Management, and Logs. The 'Unpublished Changes' tab is selected. The main content area displays 'Unpublished Changes' with two buttons at the top: 'Publish All' (highlighted with a red box) and 'Discard All'. A table below shows two items under 'Access Control': 'Access Rule URLPathAccessRule has been added.' and 'Access Rule HTTPHeaderAccessRule has been added.'. Both rows have a checked checkbox next to them. The bottom right of the table says 'Showing 2 item(s)'.

Publishing of these changes takes around 10 mins. Once the changes are published we can test the Access Rules in action.

## Test the Access Rules

We can test the first access rule of the URL path by opening a browser to visit [www.<domain>/foo](http://www.<domain>/foo). This should take you to an error page as shown in the screenshot below

The screenshot shows a browser window with the address bar displaying '<http://www.networkinglab.tk/fo>'. The main content area shows an error message: 'www.networkinglab.tk' with the subtext 'Access is blocked.' Below this, a table provides details about the incident:

Incident ID	2020-06-01T22:54:33Z e24e1e2828 209.17.40.43 wfNLPm8wG
Your IP address	209.17.40.43
Server IP	XXX.XXX.XXX.183
Code	Access Rules-403
Description	Access blocked by website owner. Invalid Path

To test the HeaderAccessRule, we can use a Google Chrome browser extension called ModHeader. Once added to Google Chrome, open the extension and enter name for Name and blockme as Value as the

request headers. This will append name:blockme as the header for our next request when we open [www.<your-domain-name>](#)

The screenshot shows two parts of the ModHeader extension. The top part is the extension's page on the Chrome Web Store, showing a 4.92-star rating and over 300,000 users. The bottom part is a configuration interface for Profile 2, where a 'Request headers' rule named 'name' has been added with the value 'blockme'.

**ModHeader**  
Offered by: <https://bewisse.com>  
★★★★★ 492 | [Developer Tools](#) | 300,000+ users

[Remove from Chrome](#)

Overview    Reviews    Support    Related

**Import and export profiles with ease**

Profile 2

- + Request headers
- 1 Name
- 2 Response headers
- 3 Redirect URLs
- Filters

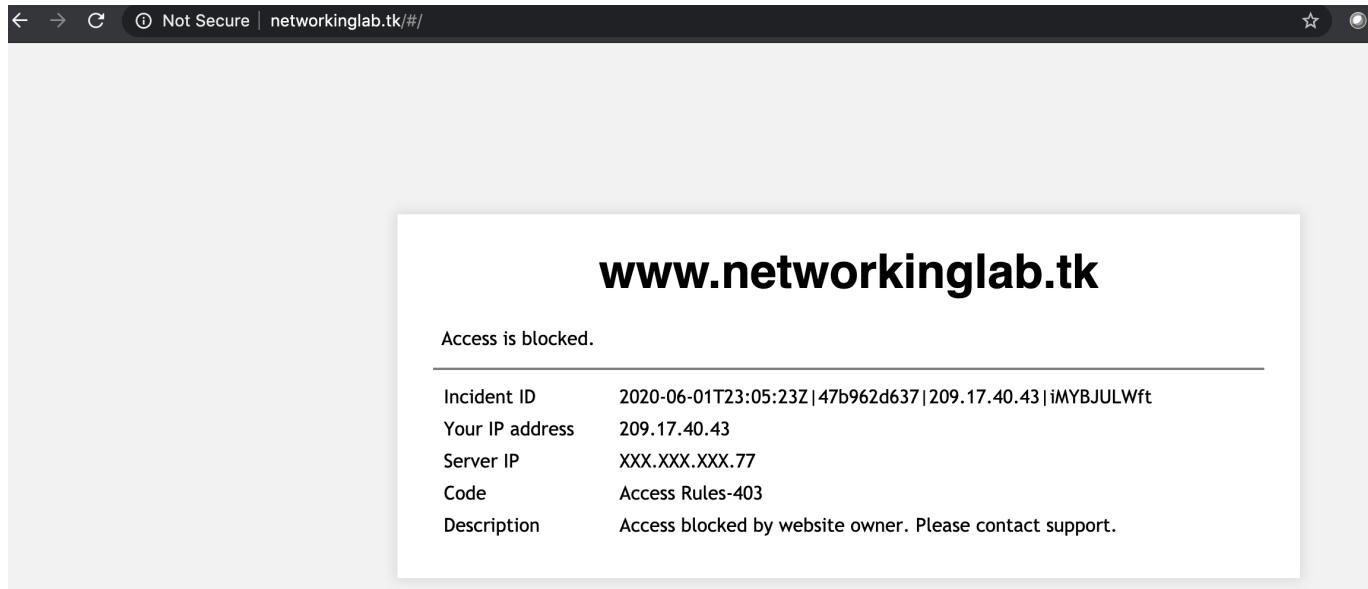
Show comment column  
Lock to tab  
Delete profile  
Clone profile  
Export / share profile(s)  
Import profile(s)  
Restore from cloud backup

① Profile 1

+ Request headers

1 name ▼ blockme

When we try to open the web application by hitting the domain name we'll be shown an error page because of the HeaderAccessRule we created



## Setup Protection Rules

Now let's setup protection rules in the WAF policy to protect Web Application from targeted attacks like Cross-site scripting and SQL Injection

Setup Protection Rules for Cross-Site Scripting attacks and manually test the rules in action by running the web application in 2 different browsers (one accessing web application directly using the instance IP and the other accessing the web application through the WAF Policy)

Go into the WAF policy that was created in Section 2. Navigate to Protection Rules from the panel on the lower left side of the WAF policy detail page

Actions	Rule ID	Protection Rule	Action
<input type="checkbox"/>	9320000	Remote Code Execution (RCE) Collaborative Group - Unix RCE Filter Categories Remote Code Execution (RCE) Attempt: RCE Filters for Unix.	Off
<input type="checkbox"/>	9321000	OWASP OWASP-2017 CRS3 A1 A1-2017 RCE REMOTE CODE EXECUTION UNIX	
<input type="checkbox"/>	9321050	WASCTC PCI COLLABORATIVE	

Under the Rule ID Filters look up for rules with the following ID's – 950006, 941140, 950907, 981242(981243), 981272, 950007, then use the check box under Actions button to select all filtered results and change status to Block

The screenshot shows the Oracle Cloud WAF Policy Protection Rules interface. On the left, a sidebar lists various policy sections like Overview, Origin Management, Settings, Protection Rules (which is selected and highlighted in blue), Access Control, Bot Management, Logs, and Unpublished Changes. Below this is a 'Filters' section with a 'clear' button. The main content area is titled 'Protection Rules' and contains a 'Rules' tab. Under the 'Actions' dropdown, 'Block' is selected. A specific rule for 'Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4' is highlighted with a red box. This rule has an 'Off' status and is categorized under OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A3, A3-2017, and XSS. Below this are sections for 'Injection for common system commands', 'OS Command Injection', and 'Classic SQL injection probings', each with their own set of rules and statuses. At the bottom, there are 'Terms of Use and Privacy' and 'Cookie Preferences' links, along with a copyright notice: 'Copyright © 2019, Oracle and/or its affiliates. All rights reserved.'

Navigate to Unpublished changes. Check box under Publish All button and click on the Publish All button. It will take a few minutes to publish these changes. Once the WAF policy status is active, we can test the Protection Rules manually

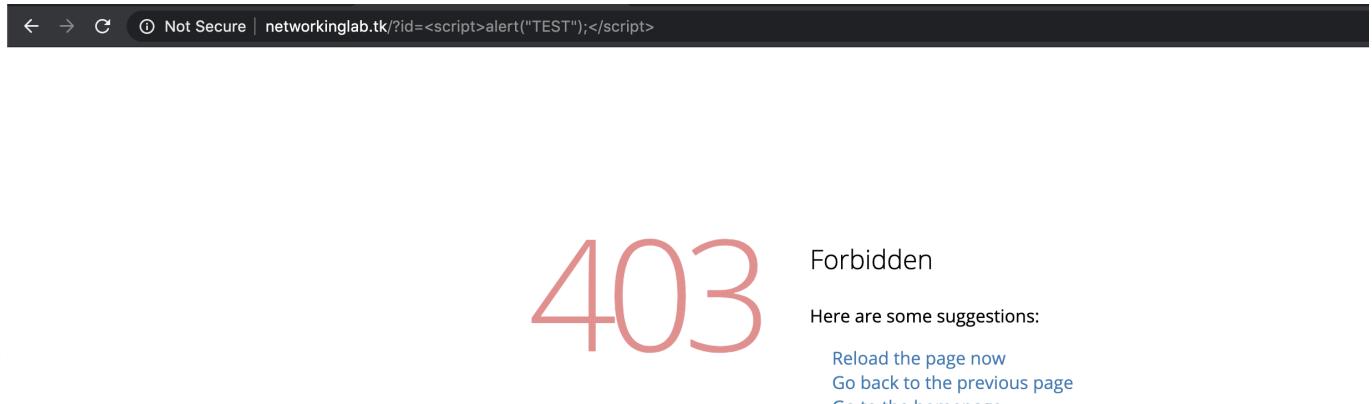
## Test Protection Rules

To test the Cross-Site Scripting Protection Rule with No WAF, enter URL of the web application with the IP Address instead of the domain name – [http://193.122.160.213?id=<script>alert\("TEST"\);</script>](http://193.122.160.213?id=<script>alert('TEST');</script>). The application opens which is not a desired outcome as there was an unchecked script passed into the browser

The screenshot shows the OWASP Juice Shop website. The URL in the address bar is 'Not Secure | 193.122.160.213/?id=<script>alert("TEST");</script>#/'. The page title is 'OWASP Juice Shop'. The main content is a grid of products under the heading 'All Products'. The products shown are Apple Juice (1000ml) at 1.99€, Apple Pomace at 0.89€, Banana Juice (1000ml) at 1.99€, Carrot Juice (1000ml) at 2.99€, Eggfruit Juice (500ml) at 8.99€, and a barrel with a tap. A tooltip on the right side of the screen says: 'This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!'. There is also a 'Me want it!' button.

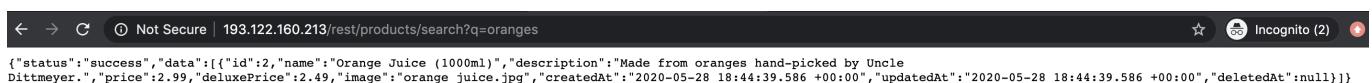
Now try to access the web application using the domain name - [http://www.networkinglab.tk?id=<script>alert\("TEST"\);</script>](http://www.networkinglab.tk?id=<script>alert('TEST');</script>). As the traffic is redirected to the WAF Policy CNAME target on OCI, which recognizes the script injected into the URL because of the rules we setup for protection against Cross-site scripting attacks in the previous section. We are redirected to an error page as shown in the screenshot below

Make sure you have removed the MODHeader that was added to test Access Rule in the previous section. Or else we'll be shown the error page for the HeaderAccessRule we setup instead of the 403 Forbidden Error page shown in the screenshot below



Next, we can check the Protection Rules for a SQL Injection attack. We can perform a similar test where we access both protected and unprotected Web applications

In a browser tab open the URL of web app with IP Address followed by /rest/products/search?q=oranges. <http://193.122.160.213/rest/products/search?q=oranges>. When we open this URL we can see from the screenshot below that a result is being shown thus meaning the SQL was passed and successfully run



Now this was a valid input and we got the result for it from both but now instead of a valid input, when we change the search parameter to a random string '; <http://193.122.160.213/rest/products/search?q='>; we get a SQLITE Error which is suggestive of the possibility of an SQL Injection Attack



## OWASP Juice Shop (Express ^4.17.1)

```
500 SequelizeDatabaseError: SQLITE_ERROR: near "%": syntax error
at Query.formatError (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:422:16)
at Query._handleQueryResponse (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:73:18)
at afterExecute (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:250:31)
at replacement (/juice-shop/node_modules/sqlite3/lib/trace.js:19:31)
at Statement.errBack (/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)
```

By fixing the query parameter to ')-- and running the URL on a browser again

[http://193.122.160.213/rest/products/search?q='\)--](http://193.122.160.213/rest/products/search?q=')--) will display all the results thus showing the SQL

Injection attack is done

```
← → C ⓘ Not Secure | 193.122.160.213(rest/products/search?q=%27))-- Incognito (2)

{"status": "success", "data": [{"id": 1, "name": "Apple Juice (1000ml)", "description": "The all-time classic.", "price": 1.99, "deluxePrice": 0.99, "image": "apple_juice.jpg", "createdAt": "2020-05-28 18:44:39.586 +00:00", "updatedAt": "2020-05-28 18:44:39.586 +00:00", "deletedAt": null}, {"id": 2, "name": "Orange Juice (1000ml)", "description": "Made from oranges hand-picked by Uncle Dittmeyer.", "price": 2.99, "deluxePrice": 2.49, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.586 +00:00", "updatedAt": "2020-05-28 18:44:39.586 +00:00", "deletedAt": null}, {"id": 3, "name": "Eggfruit Juice (500ml)", "description": "Now with even more exotic flavours.", "price": 8.99, "deluxePrice": 8.99, "image": "eggfruit_juice.jpg", "createdAt": "2020-05-28 18:44:39.586 +00:00", "updatedAt": "2020-05-28 18:44:39.586 +00:00", "deletedAt": null}, {"id": 4, "name": "Raspberry Juice (1000ml)", "description": "Made from blended Raspberry Pi, water and sugar.", "price": 14.99, "deluxePrice": 14.99, "image": "raspberry_juice.jpg", "createdAt": "2020-05-28 18:44:39.586 +00:00", "updatedAt": "2020-05-28 18:44:39.586 +00:00", "deletedAt": null}, {"id": 5, "name": "Lemon Juice (500ml)", "description": "Sour but full of vitamins.", "price": 2.99, "deluxePrice": 1.99, "image": "lemon_juice.jpg", "createdAt": "2020-05-28 18:44:39.587 +00:00", "updatedAt": "2020-05-28 18:44:39.587 +00:00", "deletedAt": null}, {"id": 6, "name": "Banana Juice (1000ml)", "description": "Monkeys love it the most.", "price": 1.99, "deluxePrice": 1.99, "image": "banana_juice.jpg", "createdAt": "2020-05-28 18:44:39.587 +00:00", "updatedAt": "2020-05-28 18:44:39.587 +00:00", "deletedAt": null}, {"id": 7, "name": "OWASP Juice Shop T-Shirt", "description": "Real fans wear it 24/7!", "price": 22.49, "deluxePrice": 22.49, "image": "fan_shirt.jpg", "createdAt": "2020-05-28 18:44:39.587 +00:00", "updatedAt": "2020-05-28 18:44:39.587 +00:00", "deletedAt": null}, {"id": 8, "name": "OWASP Juice Shop CTF Girly-Shirt", "description": "For serious Capture-the-Flag heroines only!", "price": 22.49, "deluxePrice": 22.49, "image": "fan_girly.jpg", "createdAt": "2020-05-28 18:44:39.587 +00:00", "updatedAt": "2020-05-28 18:44:39.587 +00:00", "deletedAt": null}, {"id": 9, "name": "OWASP SSL Advanced Forensic Tool (O-Saft)", "description": "O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. <a href=\"https://www.owasp.org/index.php/O-Saft\" target=\"_blank\">More...</a> ", "price": 0.01, "deluxePrice": 0.01, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.590 +00:00", "updatedAt": "2020-05-28 18:44:39.590 +00:00", "deletedAt": null}, {"id": 10, "name": "Christmas Super-Surprise Box (2014 Edition)", "description": "Contain a random selection of 10 bottles (each 500ml) of our tastiest juices and an extra fan shirt for an unbeatable price! <br>Seasonal special offer (limited availability)!", "price": 29.99, "deluxePrice": 29.99, "image": "undefined.jpg", "createdAt": "2020-05-28 18:44:39.590 +00:00", "updatedAt": "2020-05-28 18:44:39.590 +00:00", "deletedAt": null}, {"id": 11, "name": "Ripperpert Special Juice", "description": "Contains a magical collection of the rarest fruits gathered from all around the world, like Cheryomoya Annona cherimolia, Jaboticaba Myrciaria cauliflora, Bael Aegle marmelos... and others, at an unbelievable price! <br>This item has been made unavailable because of lack of safety standards. (This product is unsafe! We plan to remove it from the stock!) ", "price": 16.99, "deluxePrice": 16.99, "image": "undefined.jpg", "createdAt": "2020-05-28 18:44:39.591 +00:00", "updatedAt": "2020-05-28 18:44:39.591 +00:00", "deletedAt": "2019-02-01 00:00:00.000 +00:00"}, {"id": 12, "name": "OWASP Juice Shop Sticker (2015/2016 design)", "description": "Die-cut sticker with the official 2015/2016 logo. By now this is a rare collectors item. <em>Out of stock!</em>", "price": 999.99, "deluxePrice": 999.99, "image": "sticker.png", "createdAt": "2020-05-28 18:44:39.592 +00:00", "updatedAt": "2020-05-28 18:44:39.592 +00:00", "deletedAt": "2017-04-28 00:00:00.000 +00:00"}, {"id": 13, "name": "OWASP Juice Shop Iron-Ons (16pcs)", "description": "Upgrade your clothes with washer safe <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">iron-on</a> of the OWASP Juice Shop or CTF Extension logo!", "price": 14.99, "deluxePrice": 14.99, "image": "iron-on.jpg", "createdAt": "2020-05-28 18:44:39.592 +00:00", "updatedAt": "2020-05-28 18:44:39.592 +00:00", "deletedAt": null}, {"id": 14, "name": "OWASP Juice Shop Magnets (16pcs)", "description": "Your fridge will be even cooler with these OWASP Juice Shop or CTF Extension logo <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">magnets</a>", "price": 15.99, "deluxePrice": 15.99, "image": "magnets.jpg", "createdAt": "2020-05-28 18:44:39.593 +00:00", "updatedAt": "2020-05-28 18:44:39.593 +00:00", "deletedAt": null}, {"id": 15, "name": "OWASP Juice Shop Sticker Page", "description": "Massive decoration opportunities with these OWASP Juice Shop or CTF Extension magnets <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">sticker pages</a>! Each page has 16 stickers on it.", "price": 9.99, "deluxePrice": 9.99, "image": "sticker_page.jpg", "createdAt": "2020-05-28 18:44:39.593 +00:00", "updatedAt": "2020-05-28 18:44:39.593 +00:00", "deletedAt": null}, {"id": 16, "name": "OWASP Juice Shop Sticker Single", "description": "Super high-quality vinyl <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">sticker single</a> with the OWASP Juice Shop or CTF Extension logo! The ultimate laptop decal!", "price": 14.99, "deluxePrice": 14.99, "image": "sticker_single.jpg", "createdAt": "2020-05-28 18:44:39.594 +00:00", "updatedAt": "2020-05-28 18:44:39.594 +00:00", "deletedAt": null}, {"id": 17, "name": "OWASP Juice Shop Temporary Tattoos (16pcs)", "description": "Get one of these <a href=\"https://www.stickeryou.com/products/owasp-juice-shop/794\" target=\"_blank\">temporary tattoos</a> to proudly wear the OWASP Juice Shop or CTF Extension logo on your skin! If you tweet a photo of yourself with the tattoo, you get a couple of our stickers for free! Please mention <a href=\"https://twitter.com/owasp_juiceshop\" target=\"_blank\">@owasp_juiceshop</a> in your tweet!", "price": 14.99, "deluxePrice": 14.99, "image": "tattoo.jpg", "createdAt": "2020-05-28 18:44:39.594 +00:00", "updatedAt": "2020-05-28 18:44:39.594 +00:00", "deletedAt": null}, {"id": 18, "name": "OWASP Juice Shop Mug", "description": "Black mug with regular logo on one side and CTF logo on the other! Your colleagues will envy you!", "price": 21.99, "deluxePrice": 21.99, "image": "fan_mug.jpg", "createdAt": "2020-05-28 18:44:39.595 +00:00", "updatedAt": "2020-05-28 18:44:39.595 +00:00", "deletedAt": null}, {"id": 19, "name": "OWASP Juice Shop Hoodie", "description": "Mr. Robot-style apparel. But in black. And with logo.", "price": 49.99, "deluxePrice": 49.99, "image": "fan_hoodie.jpg", "createdAt": "2020-05-28 18:44:39.595 +00:00", "updatedAt": "2020-05-28 18:44:39.595 +00:00", "deletedAt": null}, {"id": 20, "name": "OWASP Juice Shop CTF Velcro Patch", "description": "4x3.5\" embroidered patch with velcro backside. The ultimate decal for every tactical bag or backpack!", "price": 2.92, "deluxePrice": 2.92, "image": "velcro_patch.jpg", "createdAt": "2020-05-28 18:44:39.595 +00:00", "updatedAt": "2020-05-28 18:44:39.595 +00:00", "deletedAt": null}, {"id": 21, "name": "Woodruff Syrup X-Treme", "description": "Harvested and manufactured in the Black Forest, Germany. Can cause hyperactive behavior in children. Can cause permanent green tongue when consumed undiluted.", "price": 16.99, "deluxePrice": 16.99, "image": "woodruff_syrup.jpg", "createdAt": "2020-05-28 18:44:39.595 +00:00", "updatedAt": "2020-05-28 18:44:39.595 +00:00", "deletedAt": null}, {"id": 22, "name": "Green Smoothie", "description": "Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.", "price": 1.99, "deluxePrice": 1.99, "image": "green_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 23, "name": "Quince Juice (1000ml)", "description": "Juice of the <em>Cydonia oblonga</em> fruit. Not exactly sweet but rich in Vitamin C.", "price": 4.99, "deluxePrice": 4.99, "image": "quince.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 24, "name": "Apple Pomace", "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 25, "name": "Orange Pressings", "description": "Finest pressings of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 26, "name": "Lemon Pressings", "description": "Finest pressings of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 27, "name": "Banana Pressings", "description": "Finest pressings of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 28, "name": "Apple Smoothie", "description": "Finest smoothie of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 29, "name": "Orange Smoothie", "description": "Finest smoothie of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 30, "name": "Lemon Smoothie", "description": "Finest smoothie of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 31, "name": "Banana Smoothie", "description": "Finest smoothie of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 32, "name": "Orange Juice", "description": "Finest juice of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 33, "name": "Lemon Juice", "description": "Finest juice of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 34, "name": "Banana Juice", "description": "Finest juice of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 35, "name": "Apple Pomace", "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_pomace.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 36, "name": "Orange Pressings", "description": "Finest pressings of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 37, "name": "Lemon Pressings", "description": "Finest pressings of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 38, "name": "Banana Pressings", "description": "Finest pressings of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 39, "name": "Apple Smoothie", "description": "Finest smoothie of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 40, "name": "Orange Smoothie", "description": "Finest smoothie of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 41, "name": "Lemon Smoothie", "description": "Finest smoothie of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 42, "name": "Banana Smoothie", "description": "Finest smoothie of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 43, "name": "Orange Juice", "description": "Finest juice of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 44, "name": "Lemon Juice", "description": "Finest juice of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 45, "name": "Banana Juice", "description": "Finest juice of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 46, "name": "Apple Pomace", "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_pomace.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 47, "name": "Orange Pressings", "description": "Finest pressings of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 48, "name": "Lemon Pressings", "description": "Finest pressings of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 49, "name": "Banana Pressings", "description": "Finest pressings of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 50, "name": "Apple Smoothie", "description": "Finest smoothie of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 51, "name": "Orange Smoothie", "description": "Finest smoothie of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 52, "name": "Lemon Smoothie", "description": "Finest smoothie of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 53, "name": "Banana Smoothie", "description": "Finest smoothie of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 54, "name": "Orange Juice", "description": "Finest juice of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 55, "name": "Lemon Juice", "description": "Finest juice of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 56, "name": "Banana Juice", "description": "Finest juice of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 57, "name": "Apple Pomace", "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_pomace.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 58, "name": "Orange Pressings", "description": "Finest pressings of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 59, "name": "Lemon Pressings", "description": "Finest pressings of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 60, "name": "Banana Pressings", "description": "Finest pressings of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_pressings.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 61, "name": "Apple Smoothie", "description": "Finest smoothie of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "apple_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 62, "name": "Orange Smoothie", "description": "Finest smoothie of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 63, "name": "Lemon Smoothie", "description": "Finest smoothie of lemons. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "lemon_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 64, "name": "Banana Smoothie", "description": "Finest smoothie of bananas. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "banana_smoothie.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 65, "name": "Orange Juice", "description": "Finest juice of oranges. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.", "price": 0.89, "deluxePrice": 0.89, "image": "orange_juice.jpg", "createdAt": "2020-05-28 18:44:39.596 +00:00", "updatedAt": "2020-05-28 18:44:39.596 +00:00", "deletedAt": null}, {"id": 66, "name": "Lemon Juice", "description": "Finest juice of lemons. Allergy disclaimer: Might contain traces of worms
```

☰ ORACLE Cloud

OCID: ...75njqq [Show](#) [Copy](#)

CNAME Target: www-shjuiceshop-tk.b.waas.oci.oraclecloud.net

Date Created: Thu, May 30, 2019, 9:07:21 PM UTC

## WAF Policy

Overview

Origin Management

Settings

Protection Rules

Access Control

Bot Management

**Logs**

Unpublished Changes

Filters [clear](#)

START DATE  [calendar icon](#)

START TIME

## Logs

Showing logs from Mon, Jun 17, 2019, 3:33:15 AM UTC to Mon, Jun 17, 2019, 3:33:47 AM UTC

Request URL	Client IP Address	Action	Log Type	Timestamp
/favicon.ico	73.134.175.202		Access	Mon, Jun 17, 2019, 3:33:47 AM UTC
/rest/product/search?q=%27)--	73.134.175.202	● Block	Protection Rules	Mon, Jun 17, 2019, 3:33:15 AM UTC
/rest/product/search?q=%27)--	73.134.175.202		Access	Mon, Jun 17, 2019, 3:33:15 AM UTC

Showing 3 Item(s) [Page 1](#) [next page icon](#)

From the above JSON we can see the protection rules that was triggered which blocked the access of the web application as its action. The search parameters and the matched attack string were also captured in the logs

# Setup JavaScript Challenge in Bot Management

From the left panel on the WAF policy page on OCI, select Bot Management. Click on Edit JavaScript Challenge

The screenshot shows the Oracle Cloud WAF Policy interface. On the left, a sidebar lists navigation options: Overview, Origin Management, Settings, Protection Rules, Access Control, **Bot Management** (which is selected and highlighted with a red box), and Logs. The main content area displays "Policy Information" for a policy named "SHJuiceShop". It shows the Primary Domain as "www.shjuiceshop.tk", Additional Domains as "No Value", OCID as "...75njqq", and CNAME Target as "www-shjuiceshop-tk.b.waas.oci.oraclecloud.net". The Date Created is listed as "Thu, May 30, 2019, 9:07:21 PM UTC". Below this, the "Bot Management" section is expanded, showing three tabs: JavaScript Challenge (selected and highlighted with a red box), CAPTCHA Challenge, and Good Bot Whitelist. Under the JavaScript Challenge tab, there is a button labeled "Edit JavaScript Challenge" and a setting "Enable JavaScript Challenge: No".

Check on the box Enable JavaScript challenge

The screenshot shows the Oracle Cloud WAF Policy interface with the "Bot Management" section expanded. In the "JavaScript Challenge" dialog box, the "ENABLE JAVASCRIPT CHALLENGE" checkbox is checked (highlighted with a red box). A tooltip provides information about how the challenge works: "When an EDGE server receives the first connection request from a client, instead of instantly reporting with the requested content, a small calculation written in JavaScript is injected. The second request is used to compare the result and, if the calculation is accurate, the EDGE server will return the requested content along with a cookie to ensure that subsequent connections from that client are not challenged." Below the dialog, the "Save" button is visible.

Change Action to Block and change Block Action Show Error Page

**JavaScript Challenge**

[help](#) [cancel](#)

Manage the settings that detect and filter abnormal and malicious bot traffic.

**ENABLE JAVASCRIPT CHALLENGE** [\(i\)](#)

**JS CHALLENGE ACTION** [\(i\)](#)

**DETECT ONLY**  
Create a detection for all matched requests and take no further action.

**BLOCK**  
Block all matched requests and return the specified response code, error page or CAPTCHA.

**BLOCK ACTION** [\(i\)](#)

Show Error Page [\(i\)](#)

**BLOCK RESPONSE CODE** [\(i\)](#)

403 Forbidden [\(i\)](#)

403 Forbidden is the default response. 503 Service Unavailable sends back the Service Unavailable response code.

Scroll down and edit the Error page message and description and change Action Threshold to 6 requests.  
Click on Save

**BLOCK ERROR PAGE MESSAGE** *(i)*

Access to the website is blocked.

**BLOCK ERROR PAGE DESCRIPTION** *(i)*

Access blocked by website owner. Please contact support. JavaScript Challenge.

**BLOCK ERROR PAGE CODE** *(i)*

JSC-403

**ACTION THRESHOLD** *(i)*

6 Requests

Due to the asynchronous request from the browser during page loading, it's recommended to set a threshold of 10 for web applications with basic ajax usage, and 100 for apps with heavy ajax usage.

**ACTION EXPIRE TIME** *(i)*

60 Seconds

Due to client IP address changes, it's recommended that the expiry time is set to 120 seconds for apps with mobile users and 3600 seconds for apps with desktop users only.

**Save**

**Cancel**

Publish the changes

## Test JavaScript Challenge

Once the JavaScript challenge is published and WAF Policy is back to active, open a terminal window and enter the command. Use the public IP of the instance running the web application

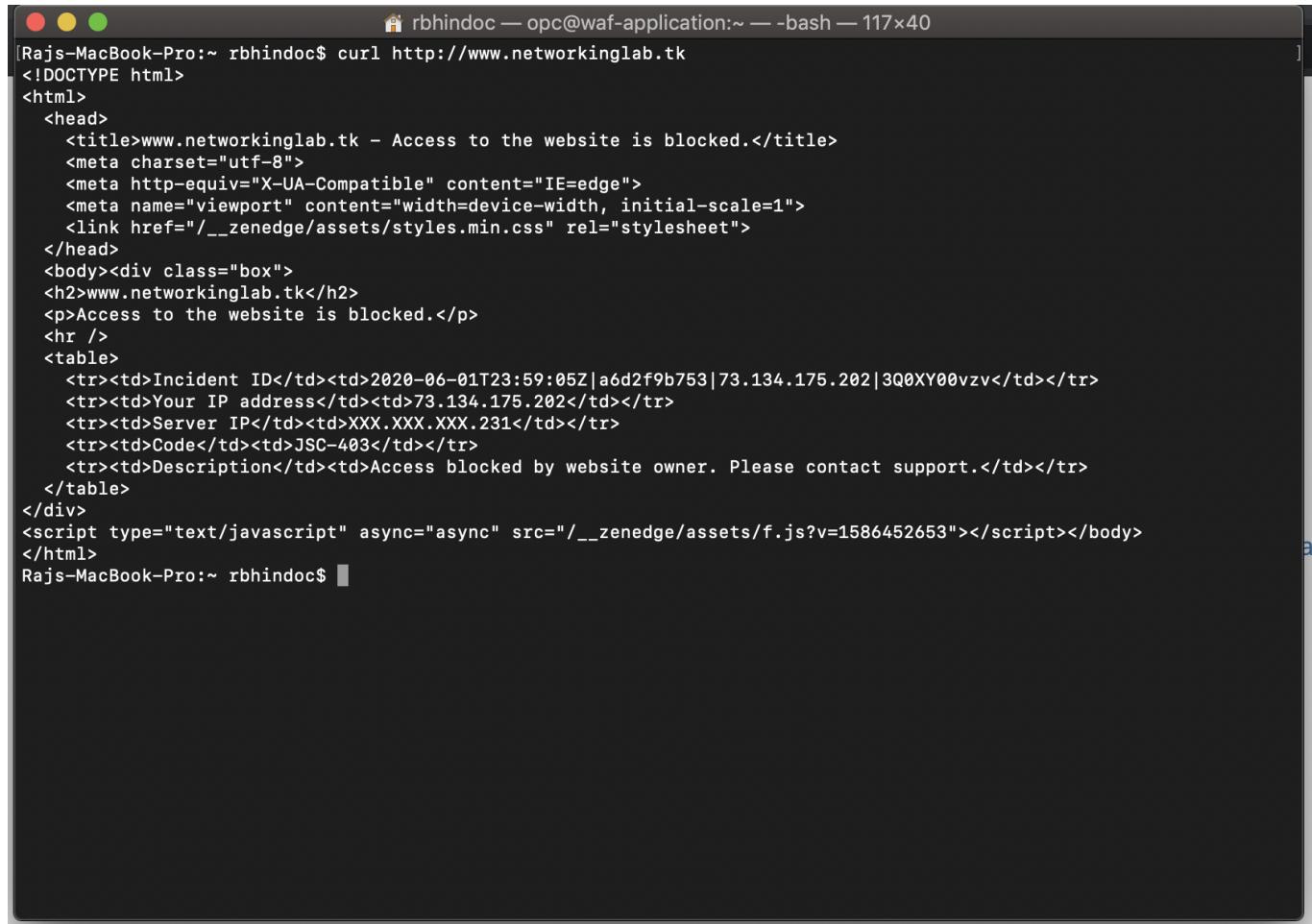
```
curl http://<your-ip-address>
ex.
curl http://193.122.160.213
```

Execute the above command in a quick succession 8-9 times. We can still see the response returned is index.html for the Web application

Now execute the following command in quick succession for 8-9 times

```
curl http://www.<your-domain-name>  
ex.  
curl http://www.networkinglab.tk/
```

We can see the JavaScript challenge that was enforced by the WAF Policy. Beyond 6 requests (threshold) we can see that we are being returned a 403 Forbidden Error.



```
Rajs-MacBook-Pro:~ rbhindoc$ curl http://www.networkinglab.tk
[...]
```

The terminal window shows the output of a curl command to the URL http://www.networkinglab.tk. The response is an HTML page indicating that access to the website is blocked. The page contains meta-information, a title, and a table with four rows. The table rows are:

Incident ID	2020-06-01T23:59:05Z a6d2f9b753 73.134.175.202 3Q0XY00vzv
Your IP address	73.134.175.202
Server IP	XXX.XXX.XXX.231
Code	JSC-403

The last row of the table contains the description "Access blocked by website owner. Please contact support". The entire page is wrapped in a script tag that includes a JavaScript file reference.

```
<html>
<head>
<title>www.networkinglab.tk - Access to the website is blocked.</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="/__zenedge/assets/styles.min.css" rel="stylesheet">
</head>
<body><div class="box">
<h2>www.networkinglab.tk</h2>
<p>Access to the website is blocked.</p>
<hr />
<table>
<tr><td>Incident ID</td><td>2020-06-01T23:59:05Z|a6d2f9b753|73.134.175.202|3Q0XY00vzv</td></tr>
<tr><td>Your IP address</td><td>73.134.175.202</td></tr>
<tr><td>Server IP</td><td>XXX.XXX.XXX.231</td></tr>
<tr><td>Code</td><td>JSC-403</td></tr>
<tr><td>Description</td><td>Access blocked by website owner. Please contact support.</td></tr>
</table>
</div>
<script type="text/javascript" async="async" src="/__zenedge/assets/f.js?v=1586452653"></script></body>
</html>
Rajs-MacBook-Pro:~ rbhindoc$
```

We can check the logs for the JavaScript challenge from the Logs section on the left side panel as well.

To learn more about Oracle WAF click [here](#)