ATTACK DEFENSE

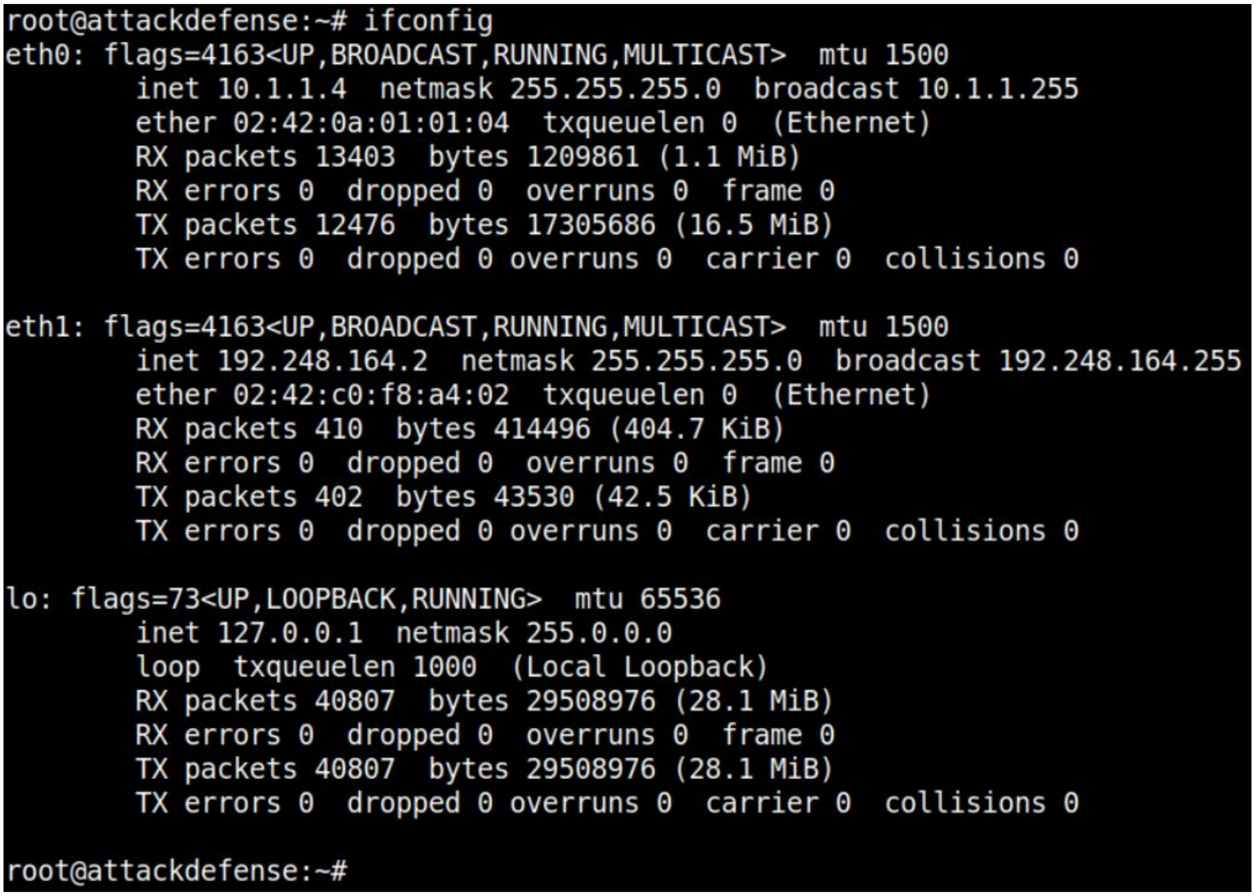
by PentesterAcademy

Name	Excessive Data Exposure I
URL	https://attackdefense.com/challengedetails?cid=1919
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:~#
```

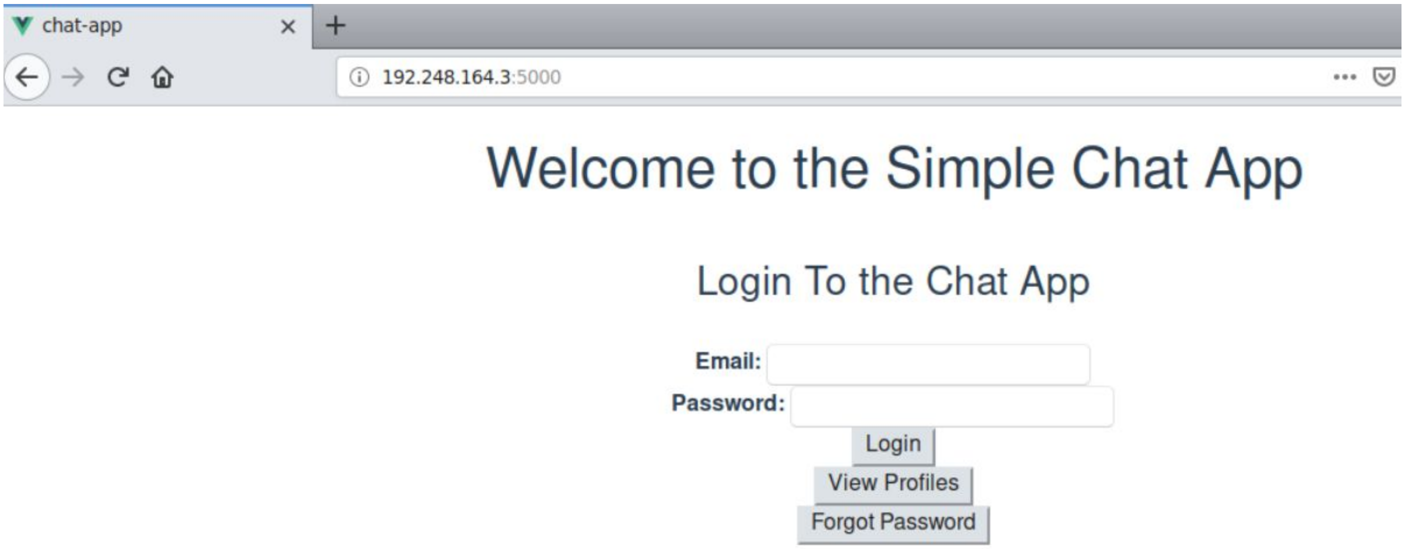
The IP address of the machine is 192.248.164.2.

Therefore, the Chat WebApp is running on 192.248.164.3, at port 5000.

Step 2: Viewing the Chat WebApp.

Open the following URL in firefox.

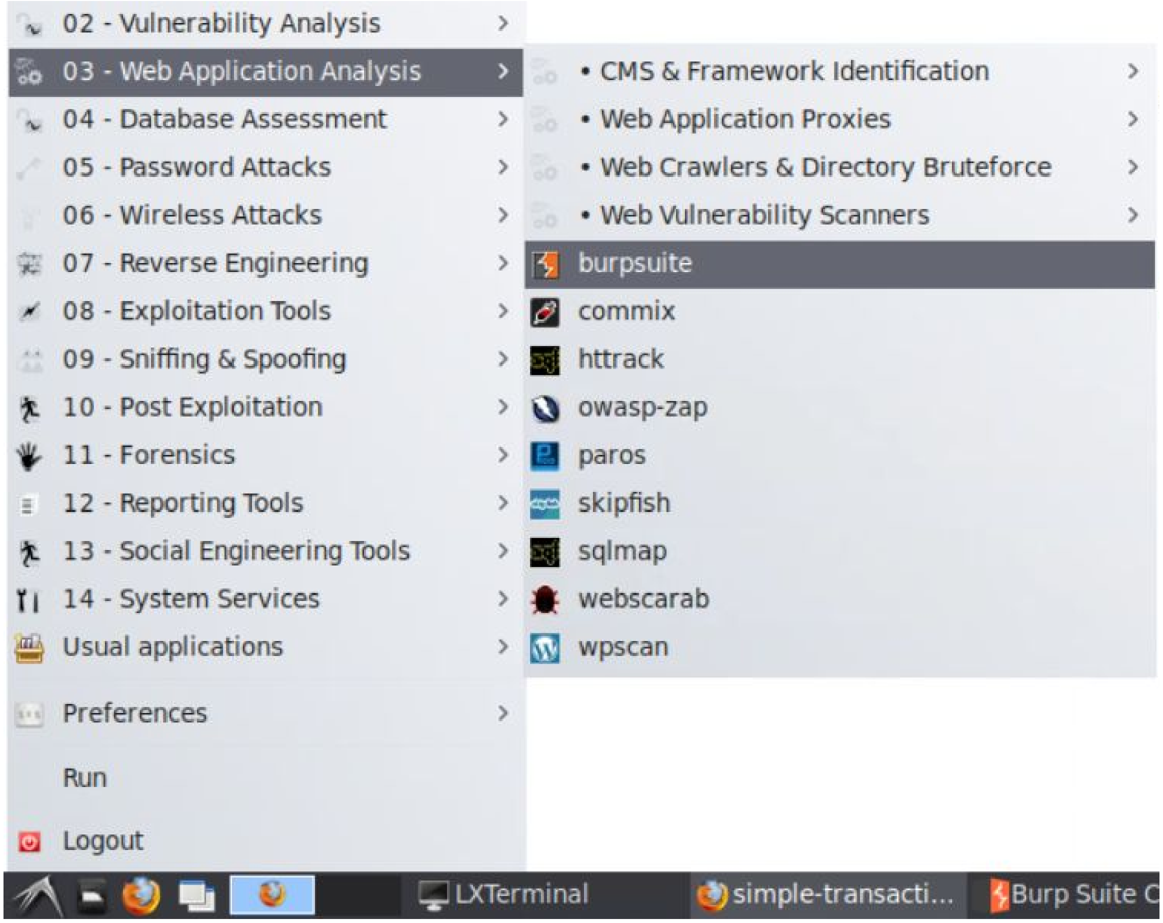
URL: http://192.248.164.3:5000



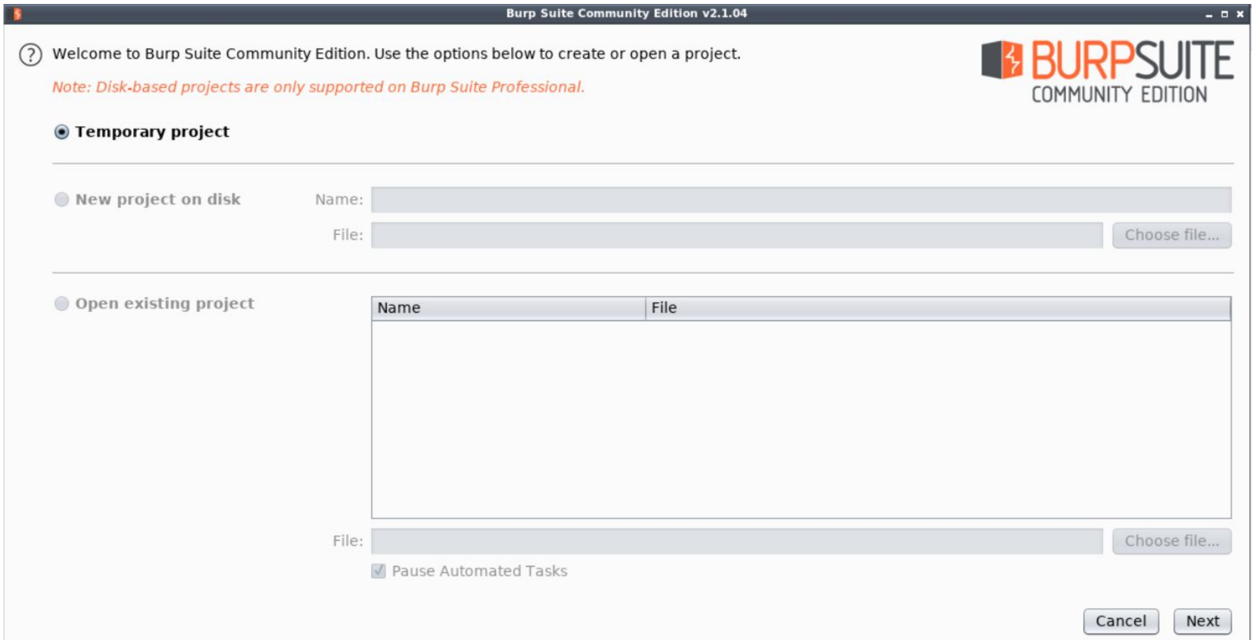
Step 3: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite



The following window will appear:



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**

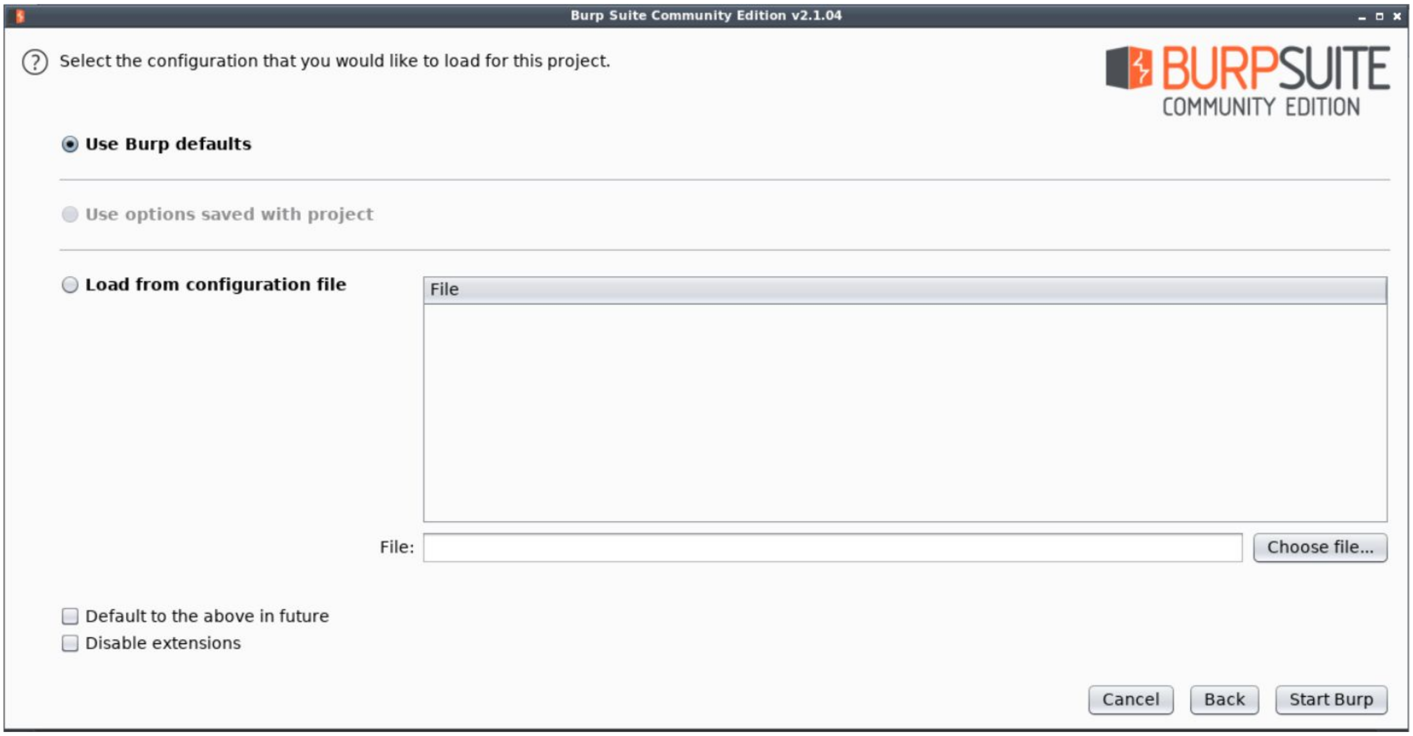
Name	File

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**

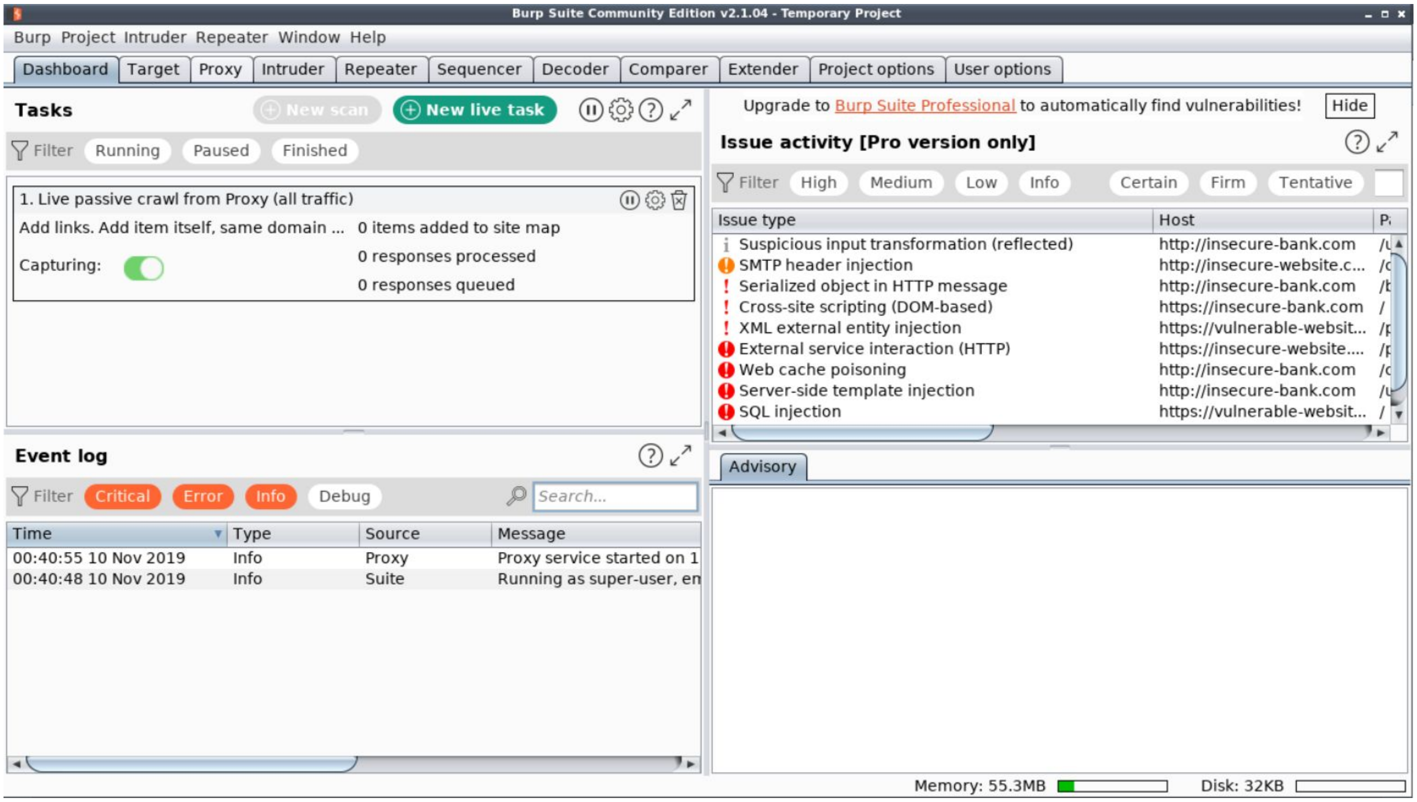
File

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
Memory: 55.3MB
Disk: 32KB

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

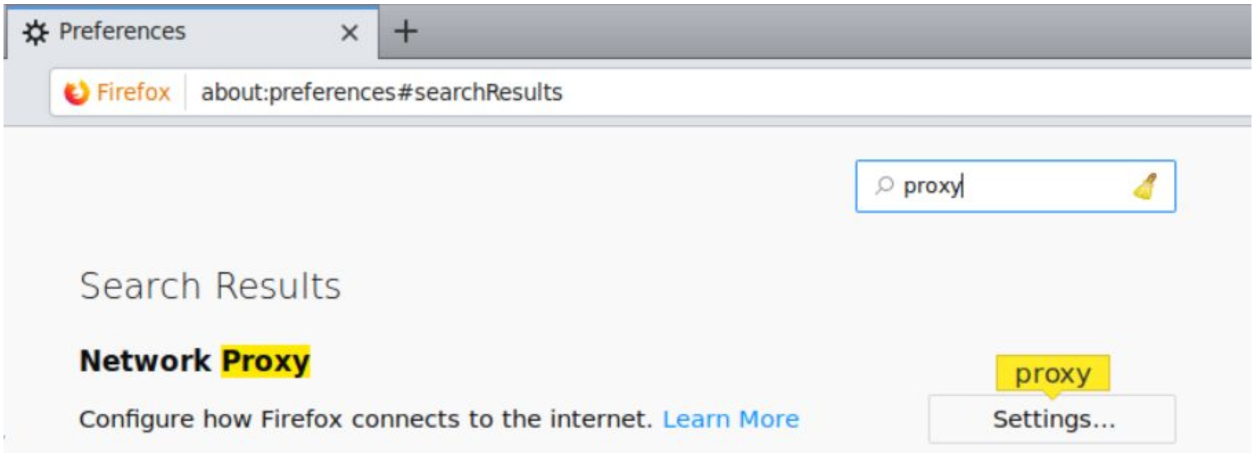
0 responses queued

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

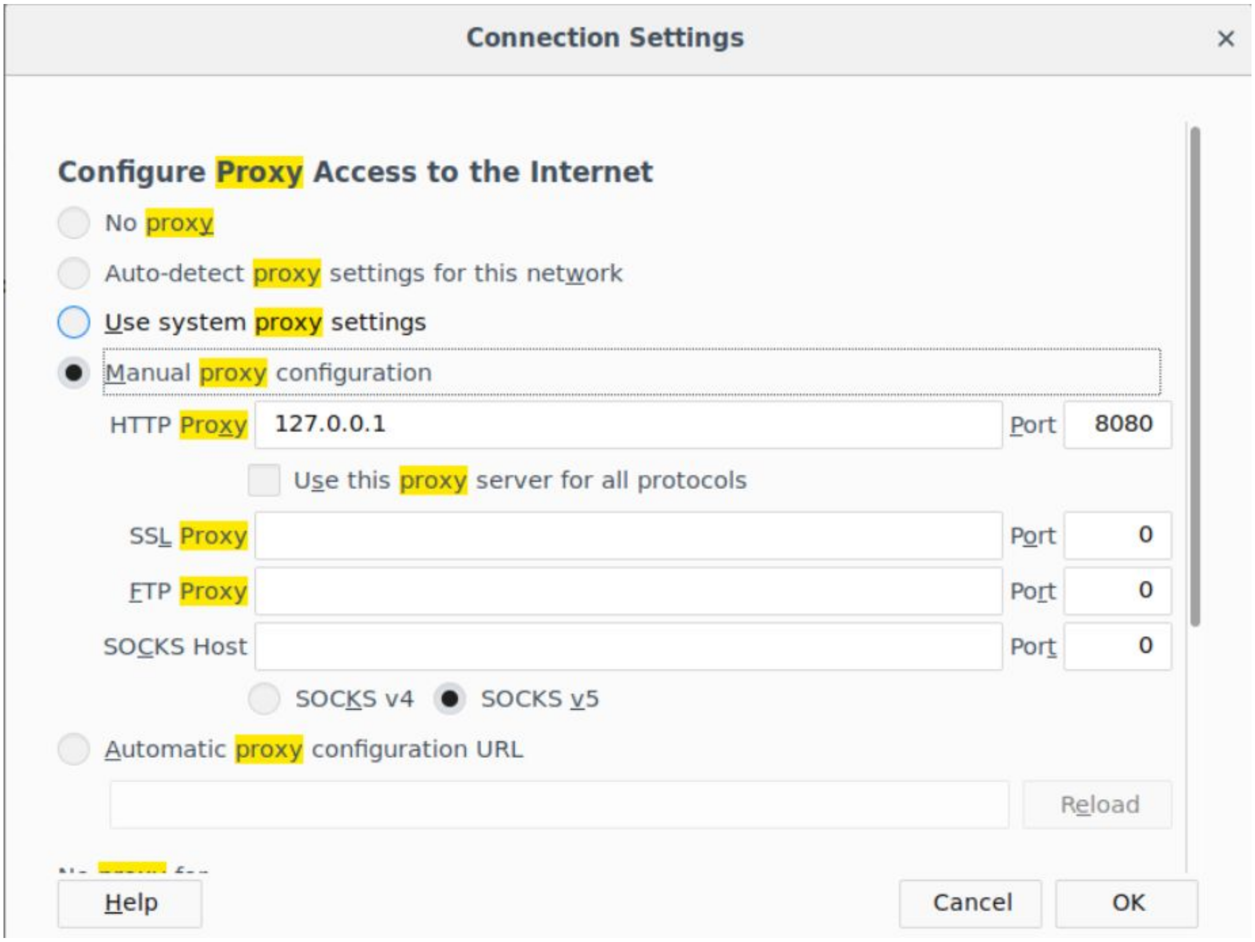
Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

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



Preferences
Firefox about:preferences#searchResults
proxy
Search Results
Network Proxy
Configure how Firefox connects to the internet. Learn More
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 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

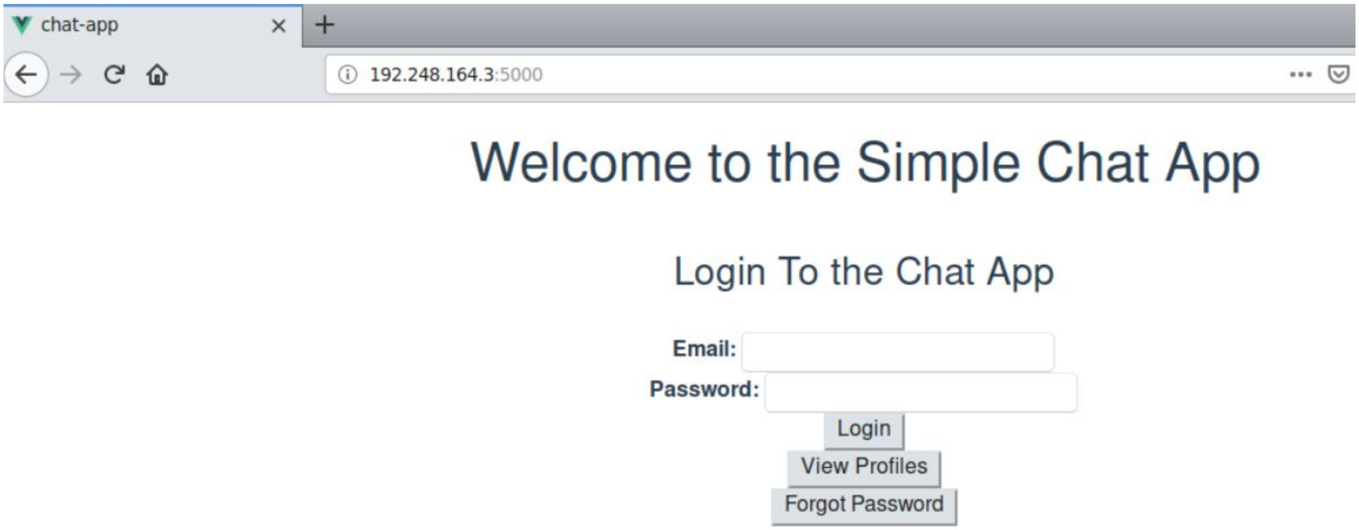
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Click OK.

Everything required to intercept the requests has been setup.

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



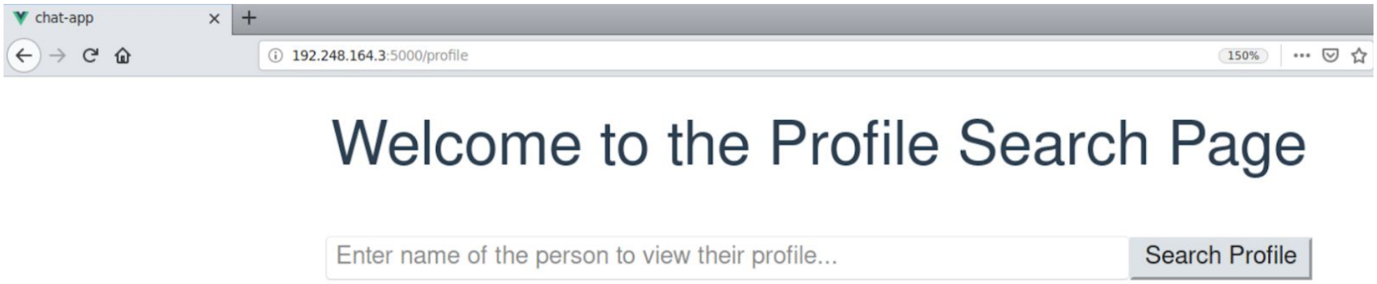
Welcome to the Simple Chat App

Login To the Chat App

Email:

Password:

Click on the View Profiles button to view the profiles for different users.



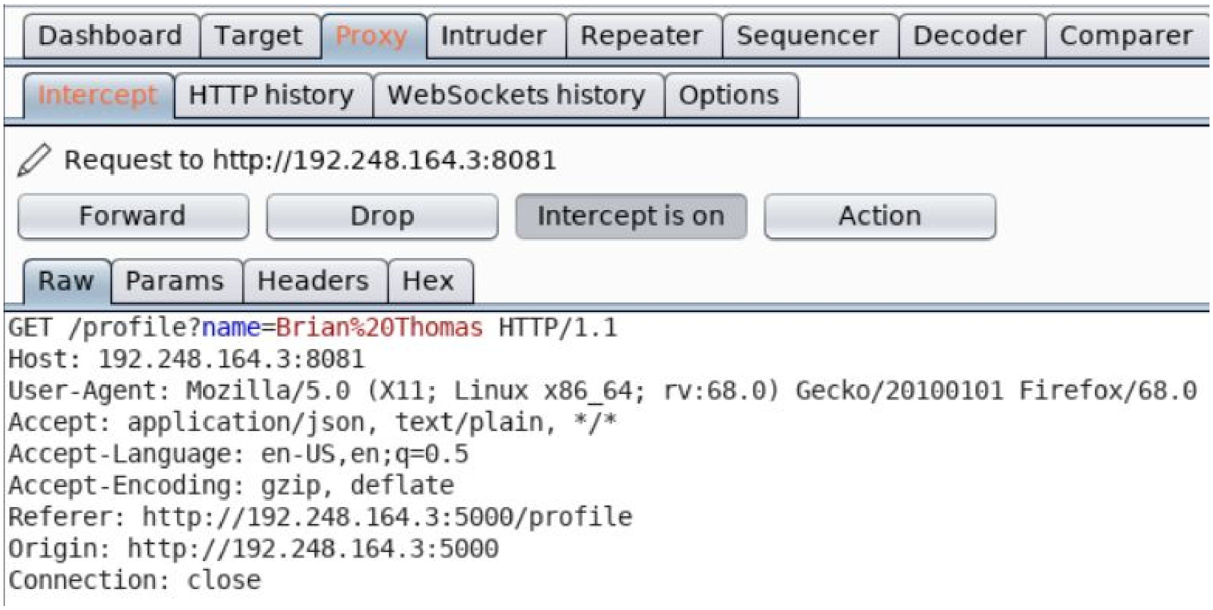
chat-app
192.248.164.3:5000/profile
150%

Welcome to the Profile Search Page

Enter name of the person to view their profile...
Search Profile

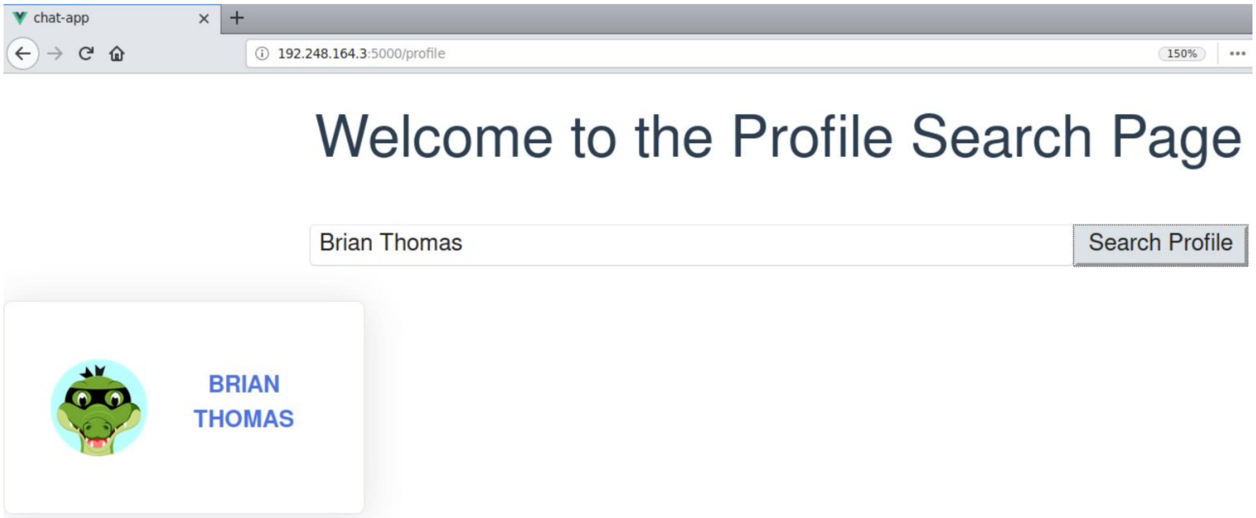
Note: Make sure that intercept is on in BurpSuite

Enter the name "Brian Thomas" to search for that user’s profile and click on the Search Profile button.



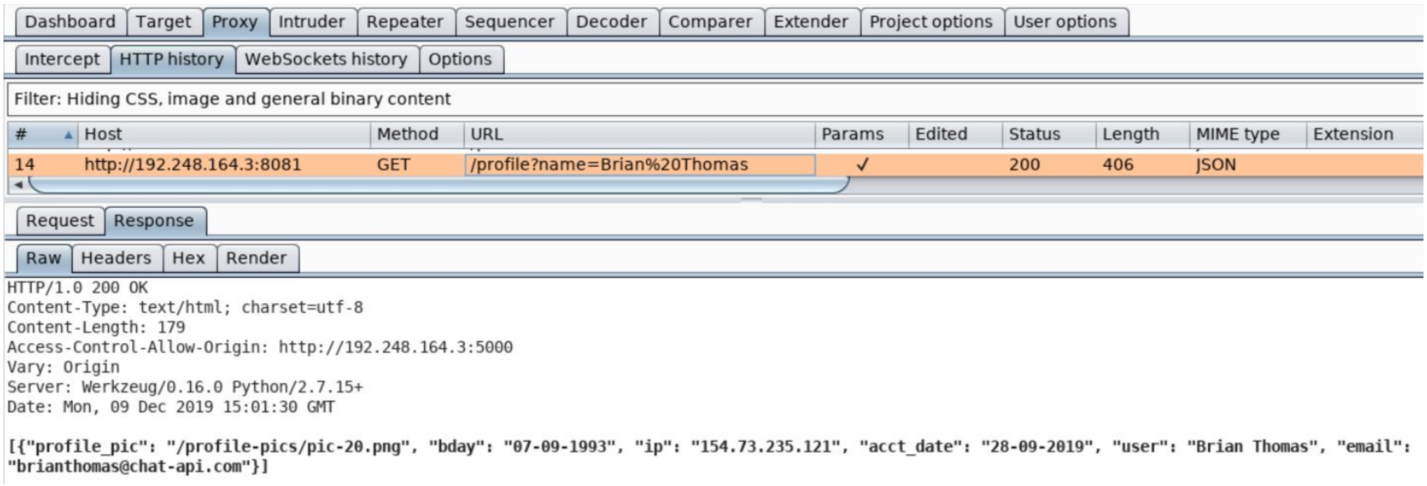
```
GET /profile?name=Brian%20Thomas HTTP/1.1
Host: 192.248.164.3:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.248.164.3:5000/profile
Origin: http://192.248.164.3:5000
Connection: close
```

Forward the above request.


chat-app
192.248.164.3:5000/profile
150%
Welcome to the Profile Search Page
Brian Thomas
Search Profile
BRIAN
THOMAS

The response on the web page shows the user avatar and their name.

Check the raw response returned by the Chat API in HTTP History tab of BurpSuite.



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
14	http://192.248.164.3:8081	GET	/profile?name=Brian%20Thomas	✓		200	406	JSON	

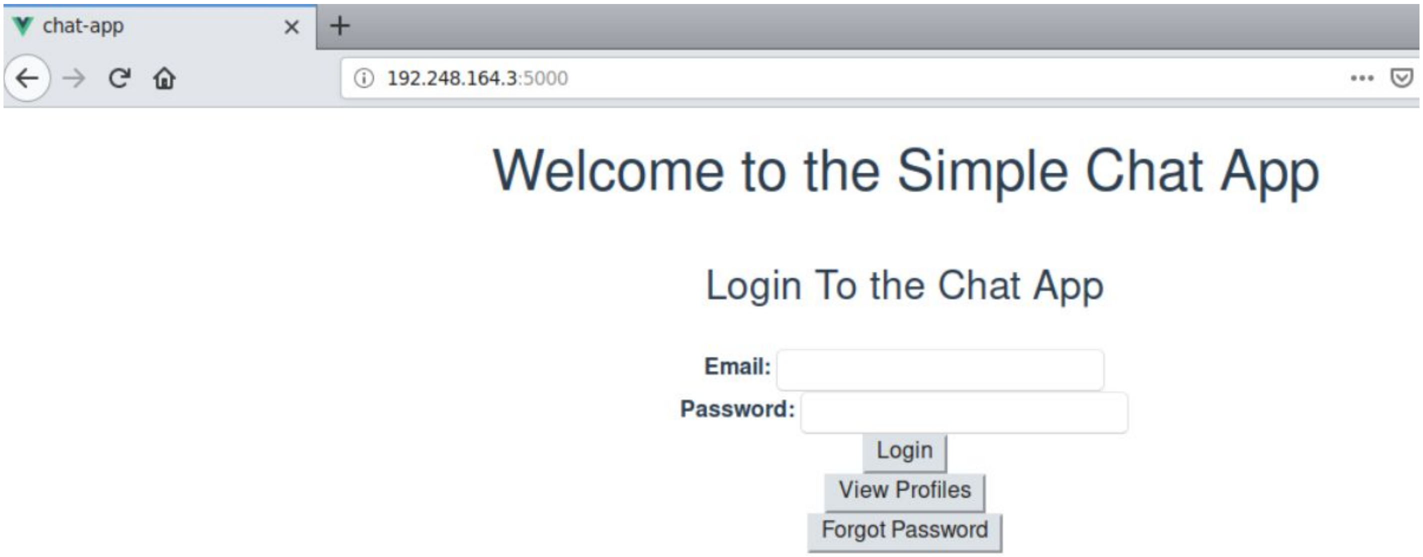
```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 179
Access-Control-Allow-Origin: http://192.248.164.3:5000
Vary: Origin
Server: Werkzeug/0.16.0 Python/2.7.15+
Date: Mon, 09 Dec 2019 15:01:30 GMT

[{"profile_pic": "/profile-pics/pic-20.png", "bday": "07-09-1993", "ip": "154.73.235.121", "acct_date": "28-09-2019", "user": "Brian Thomas", "email":
"brianthomas@chat-api.com"}]
```

Notice that the response contains a lot more information that it is displayed on the web page.

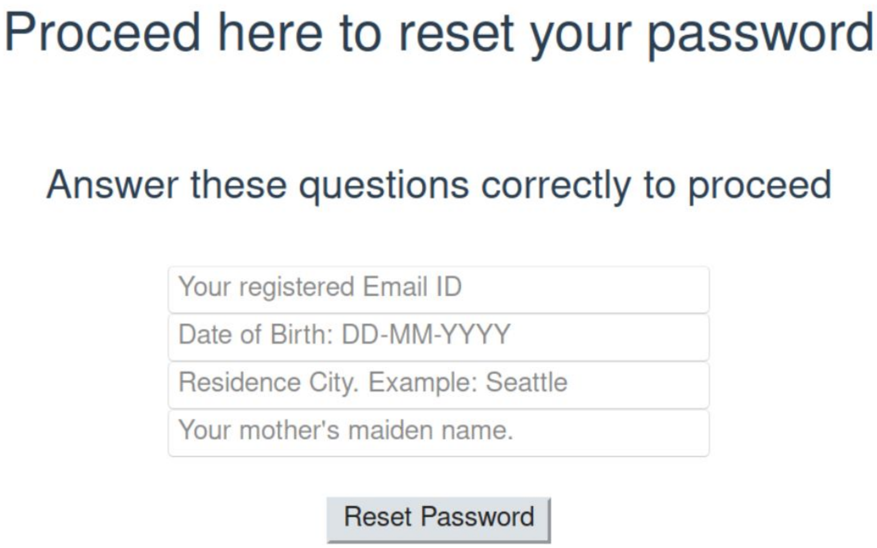
The returned data contains the birth date, IP address, email and account creation date for the specified user. This information is sensitive and could lead to account compromise.

Return back to the starting page.



Note: Turn off the intercept mode in Burp Proxy for all future requests.

Click on Forgot Password button.



Proceed here to reset your password

Answer these questions correctly to proceed

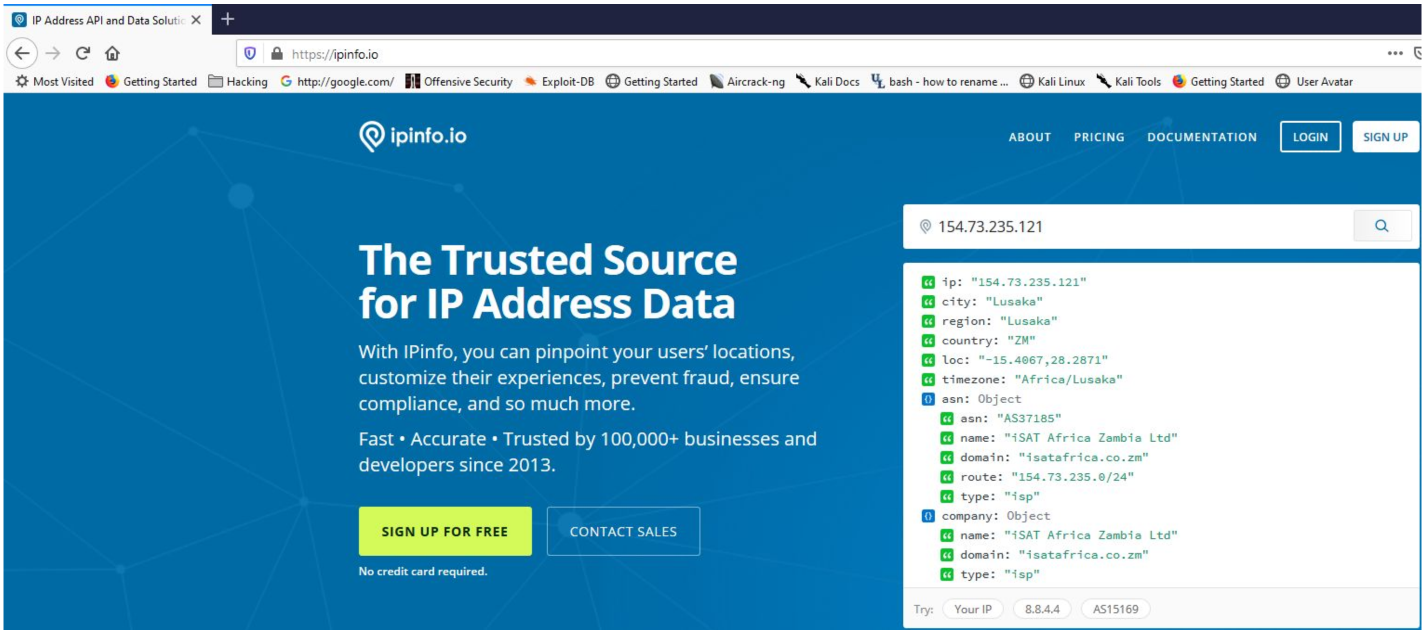
Your registered Email ID
Date of Birth: DD-MM-YYYY
Residence City. Example: Seattle
Your mother's maiden name.
Reset Password

This page contains a set of questions to be answered before proceeding forward to change the password.

Since some of the information was revealed by the API when the user profile was requested, using that here.

To figure out the city of residence, use any Geolocation API to get the city corresponding to the IP address of the user revealed from the API response.

Using https://ipinfo.io to determine the city using the IP address of the user:



IP Address API and Data Solutic

https://ipinfo.io

Most Visited · Getting Started · Hacking · http://google.com/ · Offensive Security · Exploit-DB · Getting Started · Aircrack-ng · Kali Docs · bash - how to rename ... · Kali Linux · Kali Tools · Getting Started · User Avatar

ipinfo.io — ABOUT · PRICING · DOCUMENTATION · LOGIN · SIGN UP

The Trusted Source for IP Address Data

With IPinfo, you can pinpoint your users' locations, customize their experiences, prevent fraud, ensure compliance, and so much more.

Fast • Accurate • Trusted by 100,000+ businesses and developers since 2013.

SIGN UP FOR FREE · CONTACT SALES

No credit card required.

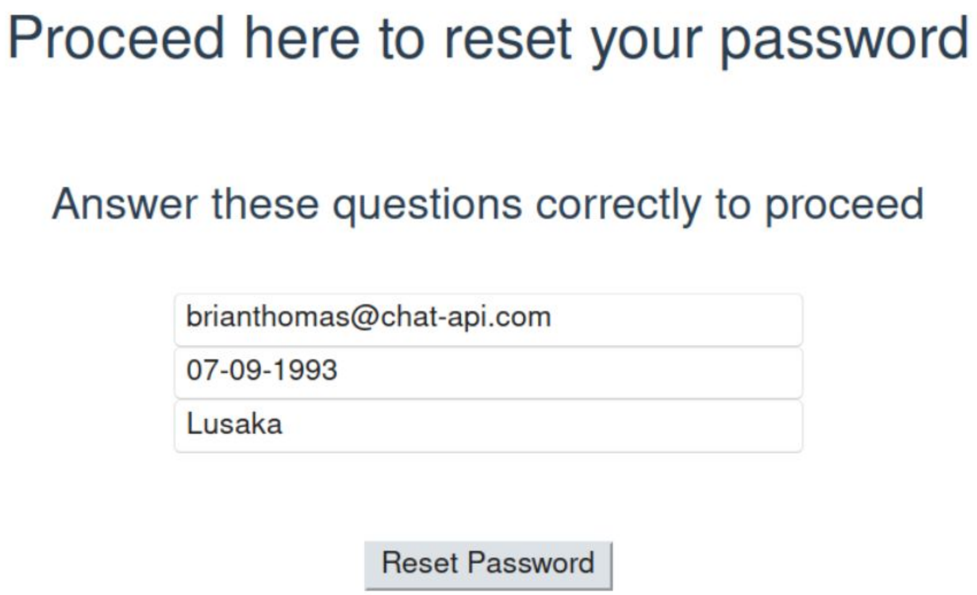
154.73.235.121

```
ip: "154.73.235.121"
city: "Lusaka"
region: "Lusaka"
country: "ZM"
loc: "-15.4067,28.2871"
timezone: "Africa/Lusaka"
asn: Object
  asn: "AS37185"
  name: "iSAT Africa Zambia Ltd"
  domain: "isatafrica.co.zm"
  route: "154.73.235.0/24"
  type: "isp"
company: Object
  name: "iSAT Africa Zambia Ltd"
  domain: "isatafrica.co.zm"
  type: "isp"
```

Try: Your IP · 8.8.4.4 · AS15169

Source: https://ipinfo.io

As revealed from the IP address, the corresponding city is Lusaka.



Proceed here to reset your password

Answer these questions correctly to proceed

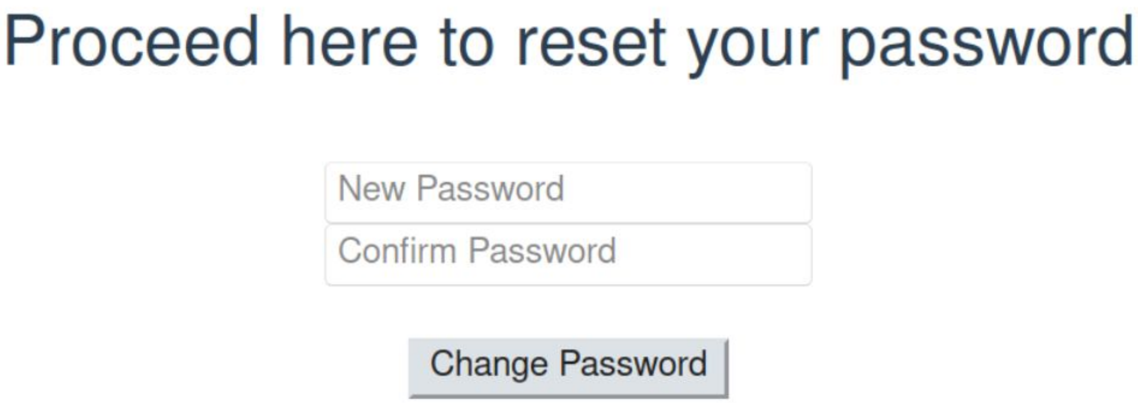
brianthomas@chat-api.com

07-09-1993

Lusaka

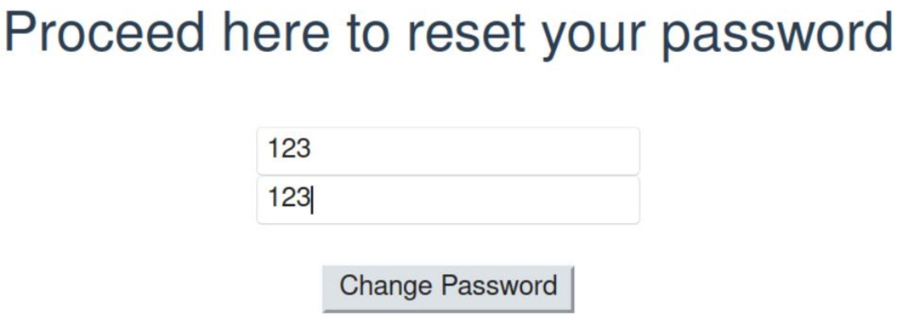
Reset Password

Click on Reset Password button.



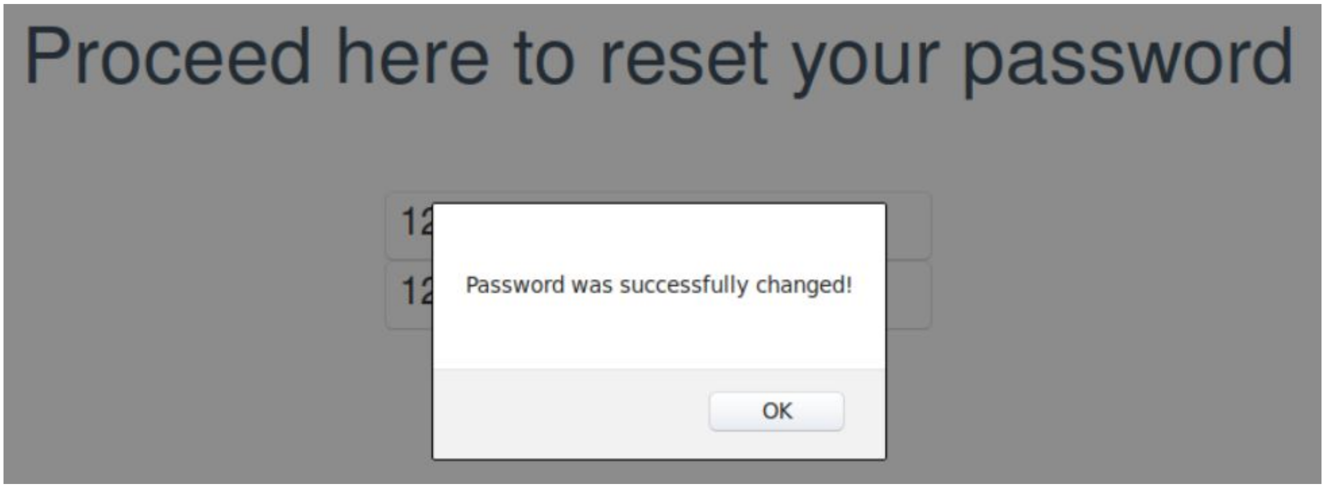
Proceed here to reset your password

Change the password to 123.



Proceed here to reset your password

123
123



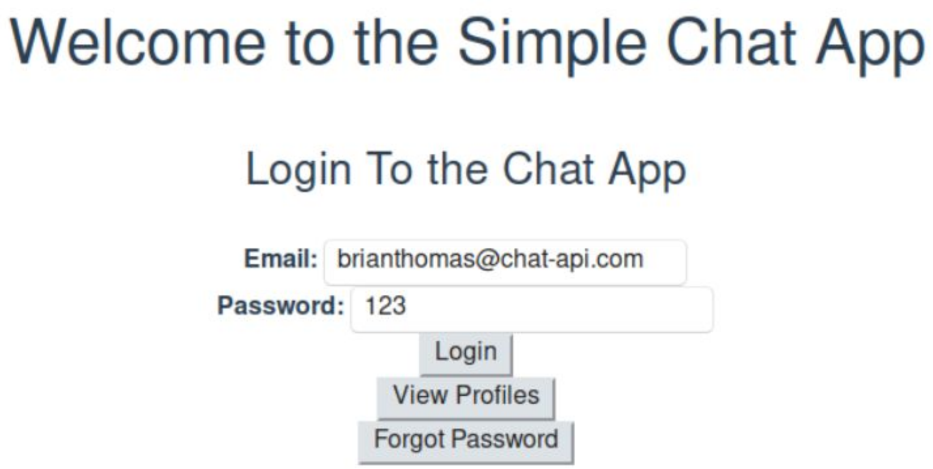
Proceed here to reset your password

Password was successfully changed!

The password was changed successfully.

Login to the web app using the modified credentials:

Username: Brian Thomas
Password: 123

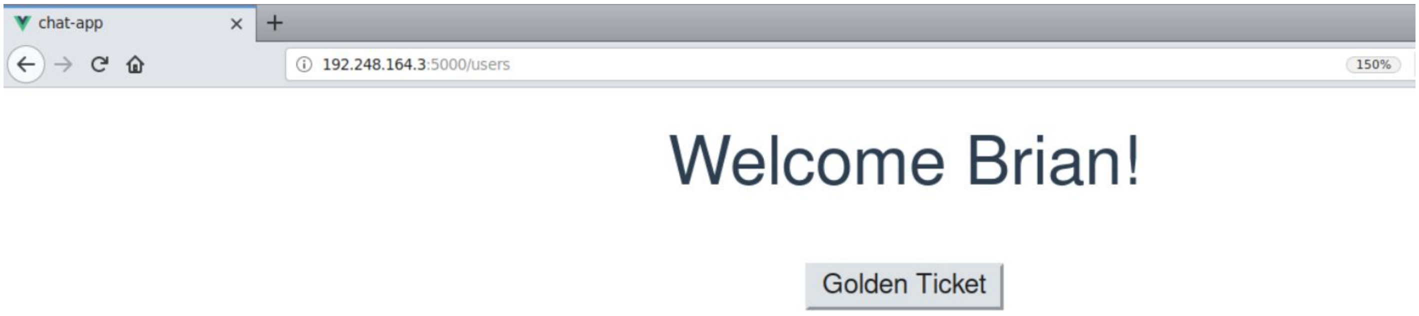


Welcome to the Simple Chat App

Login To the Chat App

Email: brianthomas@chat-api.com
Password: 123

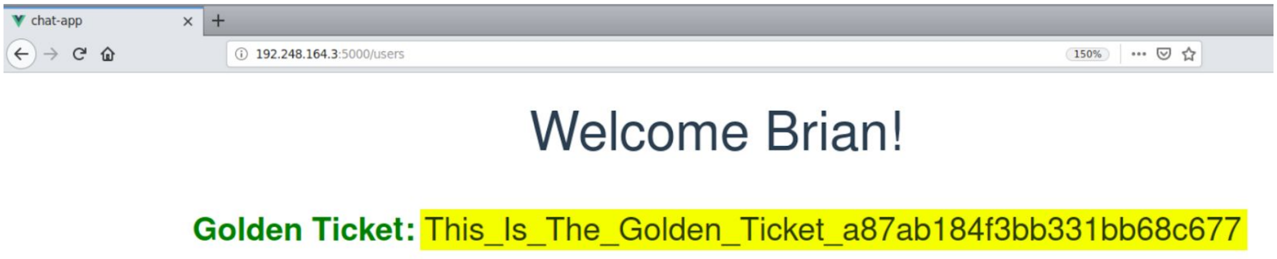
Step 5: Retrieving the Golden Ticket.



192.248.164.3:5000/users

Welcome Brian!

Click on Golden Ticket button to get the Golden Ticket.



Welcome Brian!

Golden Ticket: This_Is_The_Golden_Ticket_a87ab184f3bb331bb68c677

Golden Ticket: This_Is_The_Golden_Ticket_a87ab184f3bb331bb68c677

References:

1. OWASP API Security (https://www.owasp.org/index.php/OWASP_API_Security_Project)