enumeration

nmap -sC -sV -sT -oN /home/kali/machines/retired/popcorn/nmap_default.txt 10.10.10.6
Starting Nmap 7.91 (https://nmap.org) at 2021-02-16 08:46 EST
Nmap scan report for 10.10.10.6
Host is up (0.18s 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 41.17 seconds

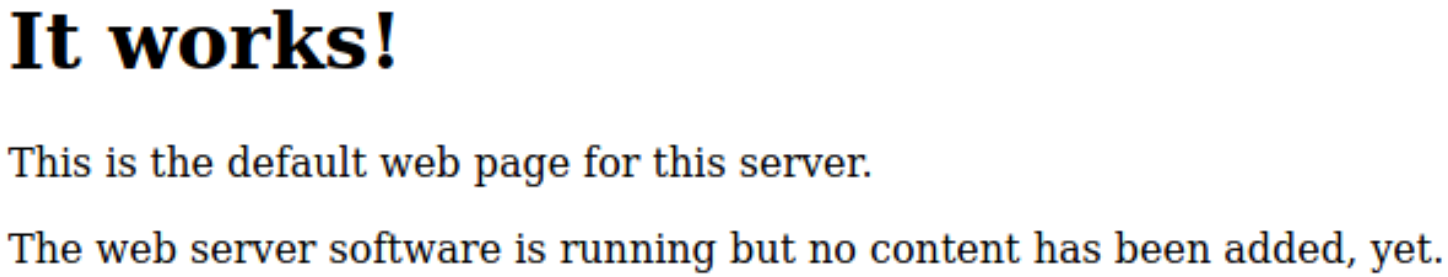
open ports are

22/tcp open ssh   OpenSSH 5.1p1 Debian 6ubuntu2

80/tcp open http   Apache httpd 2.2.12

and now we are running complete port scan to make sure no other ports are open which went unoticed

mean time lets go to http port 80



```
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>

```

so lets enumerate we will use nikto , searchsploit and gobuster

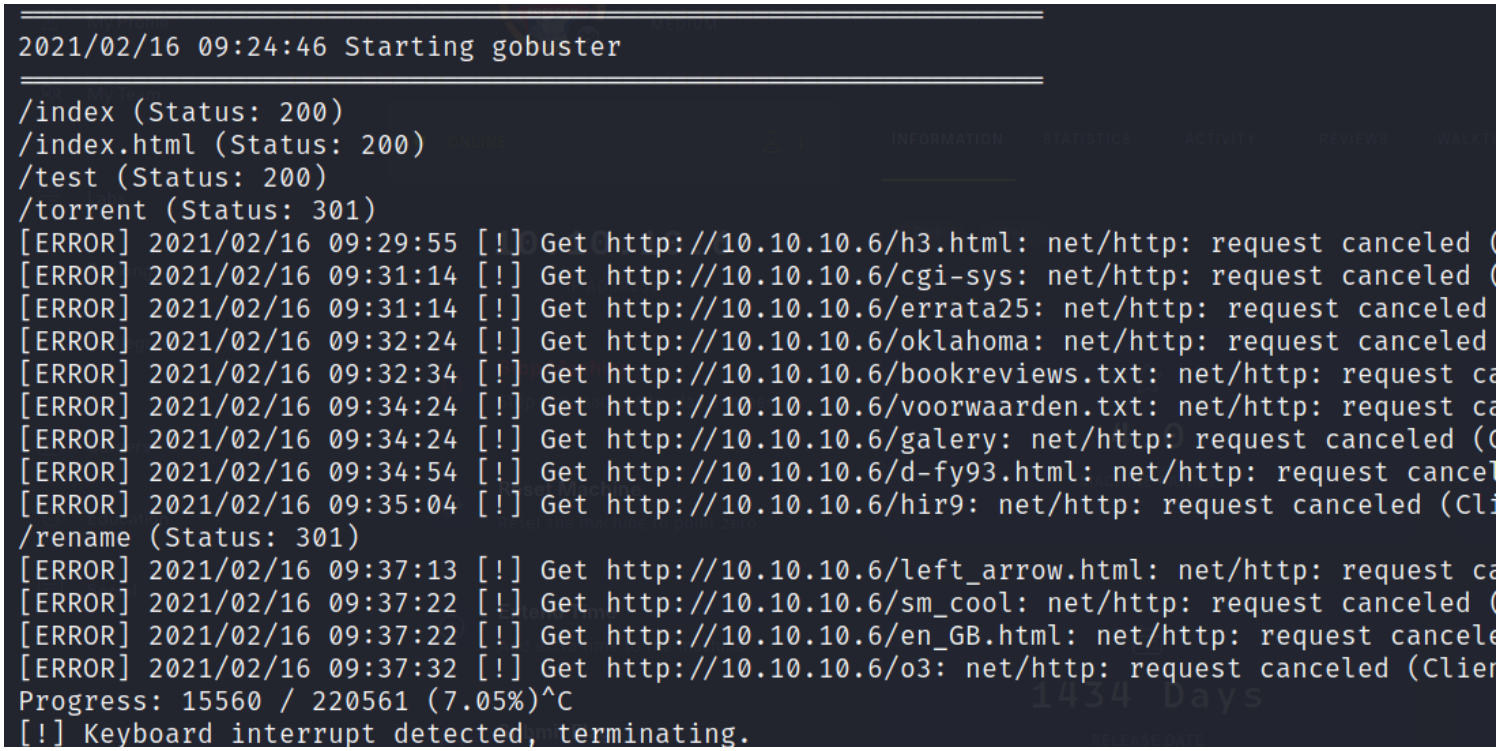
```
┌──(root💀kali)-[/home/kali]
└─# nikto -h 10.10.10.6
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.6
+ Target Hostname:    10.10.10.6
+ Target Port:        80
+ Start Time:         2021-02-16 09:09:53 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.12 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 43621, s
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
+ The X-Content-Type-Options header is not set. This could allow the user age
^C
```

nothing special

run searchsploit

nothing interesting

lets run go buster



we can see we have

- /index ----------html page
- /index.html----------html page
- /test ---------php info page
- /torrent
- /rename

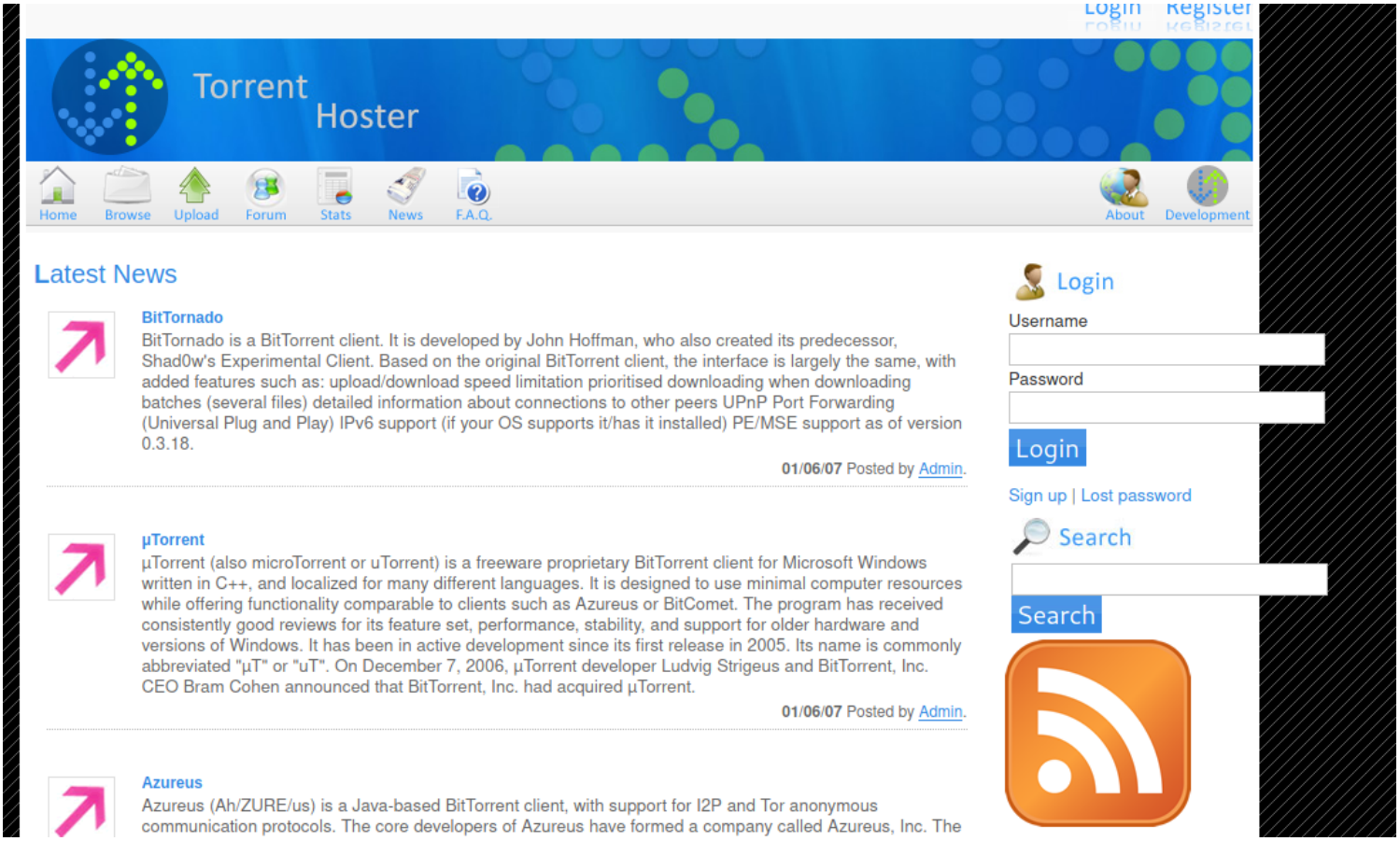
in which torrent and rename are 301 moved permanently

lets see these
/test

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

/torrent

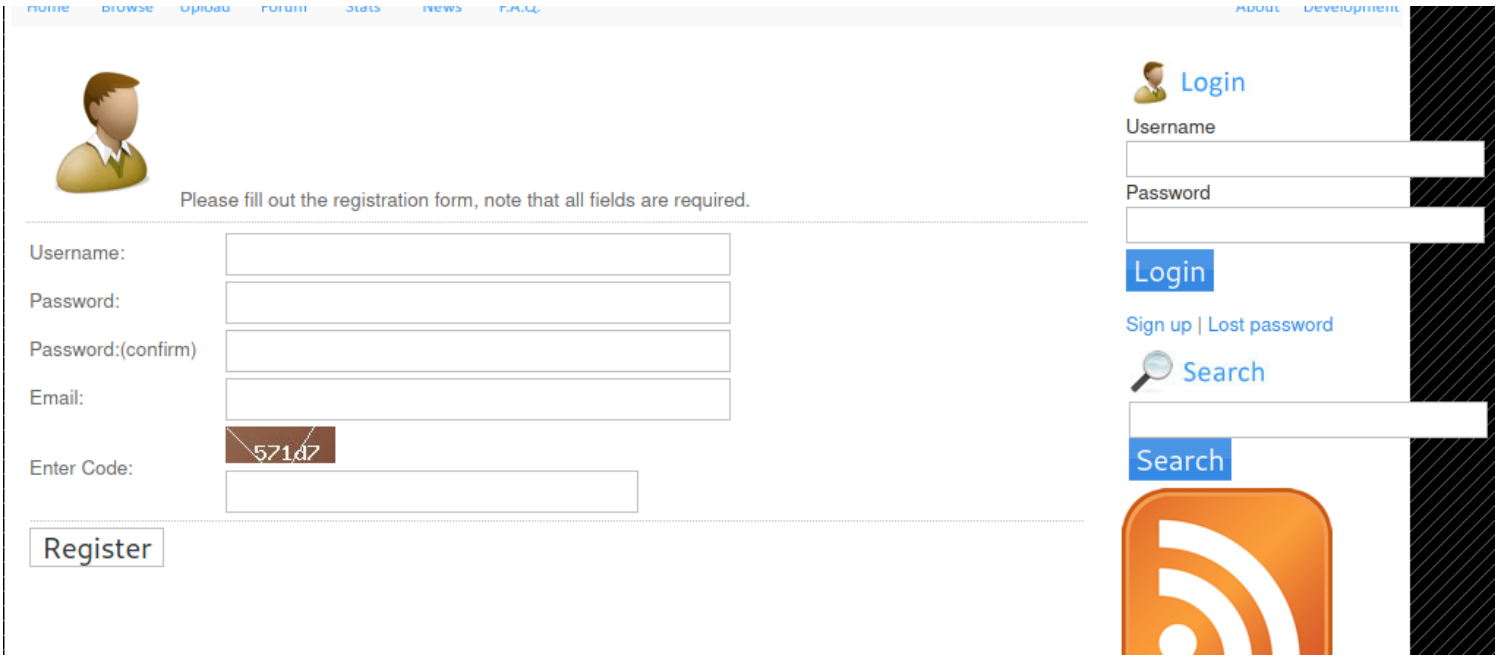


/rename

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

here we can see it is using a api which is use to rename something and this is the given format

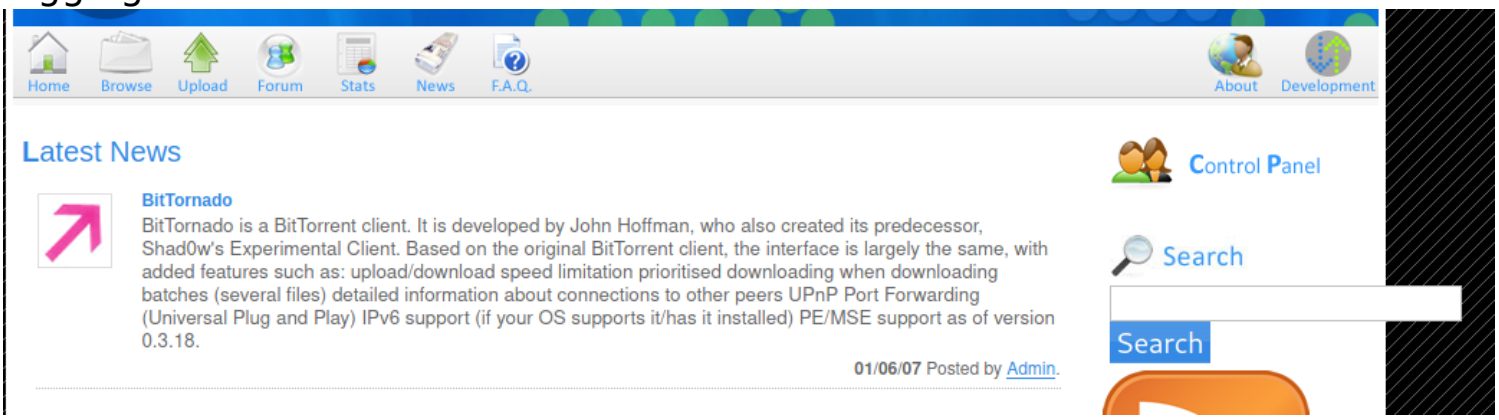
lets see the other 2 pages



lets register and see whats inside

> # Welcome
>
> Thank you for registering to Torrent Hoster Your account information is:
>
> Username: **hack**
> Password: **hack**
>
> Please write these down in a safe place and please do not give your password t
> reset it if you forget it on the login page.
>
> To continue using the system, please login now.

logging in we can see



here we have a upload button and also we can see that something is posted by admin so root name is admin or a username is admin which we can use

Torrent Hoster 2.0

Modified by DiEg0 based on webtorrent and t-xore.
visit to http://www.myanmartorrents.com/

Requirements:

- SQL
- php
- GD2

Installation

1. Create a new database for Torrent Hoster. Then, using phpmyadmin or any mysql administrator script, import /database/th_database.sql.

2. Open config.php and add the requirements.

4. Upload all the files from Torrent Hoster folder to your website.

5. CHMOD upload folder and torrents folder to 755. if u see error later, change it to 777.

6. go to the url where you uploaded the script and you are good to go. Admin username: admin; password : admin12

Update

No Update Yet.

Credit

Torrent Hoster script is based on webtorrents and t-xore. Full credits go to them. Other Credits to:

- Lokesh Dhakar http://www.huddletogether.com/ for image loading javascript
- Alexandre Moore http://www.iconsdesigns.com/ for lovely icons.

found this in /torrent/readme/readme.html

we have to upload a torrent file so lets download a kali torrent file and uplaod it

- 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-2020.4-installer-amd64.iso.torrent

Optional name: will use it to uplaod a picture

Category: Other

Subcategory: Other

Description: next we have to upload a picture with malicious code

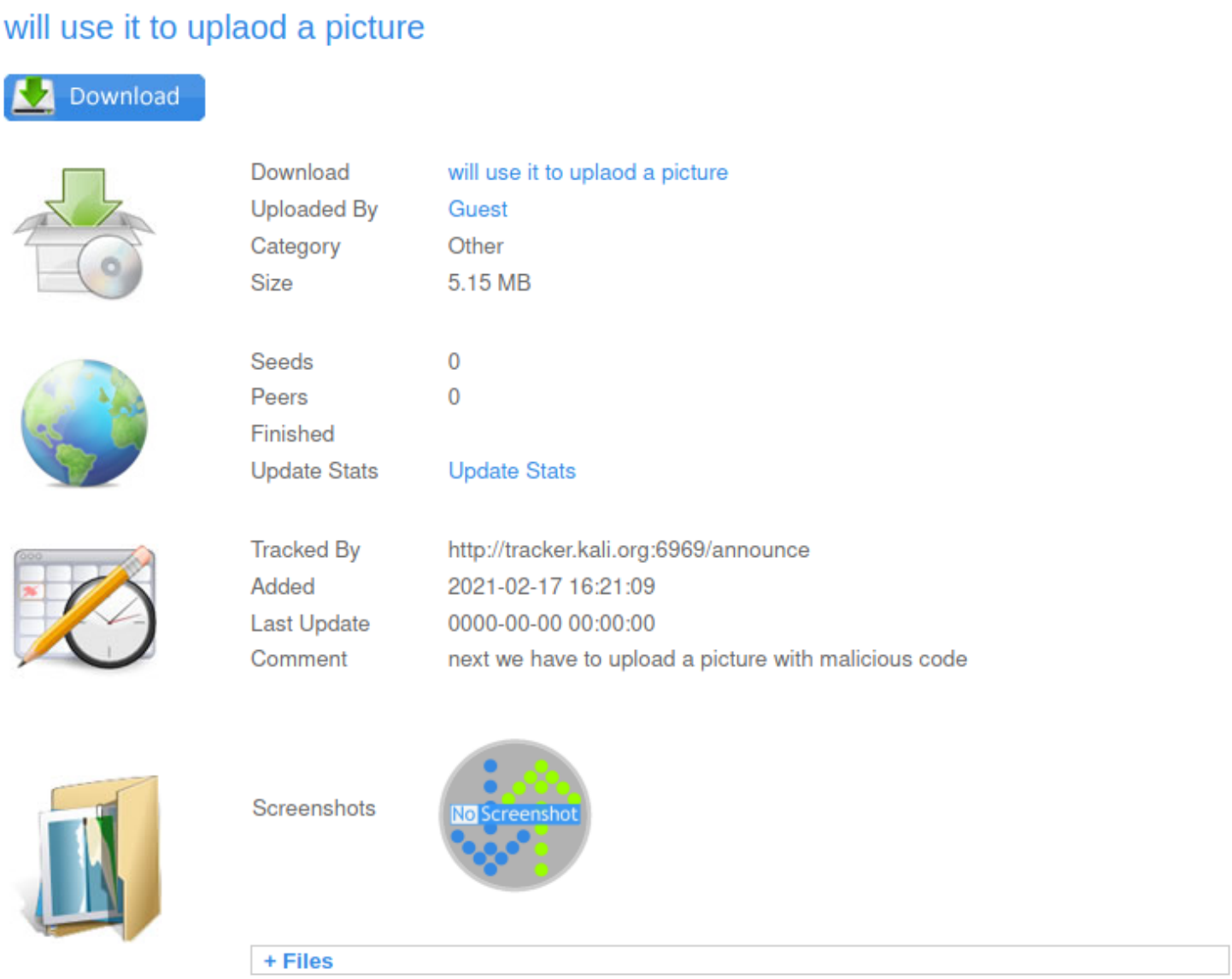
Tracker requires registration: Yes No

Post Annoymous: Yes No

Upload Torrent

we uplaoded a normal torrent file

so torrent file got uplaoded lets see



here we can see at the bottom we also have a option to uplaod a picture

and we have a directory in 10.10.10.6/torrent/upload/ in which the uplaoded picture goes and hence we can upload a php reverse shell and run it

but the problam is that we have to add a magic byte to out reverse file and intercept it with burp change it and uplaod id