APPOINTMENT

Hack the Box

Appointment

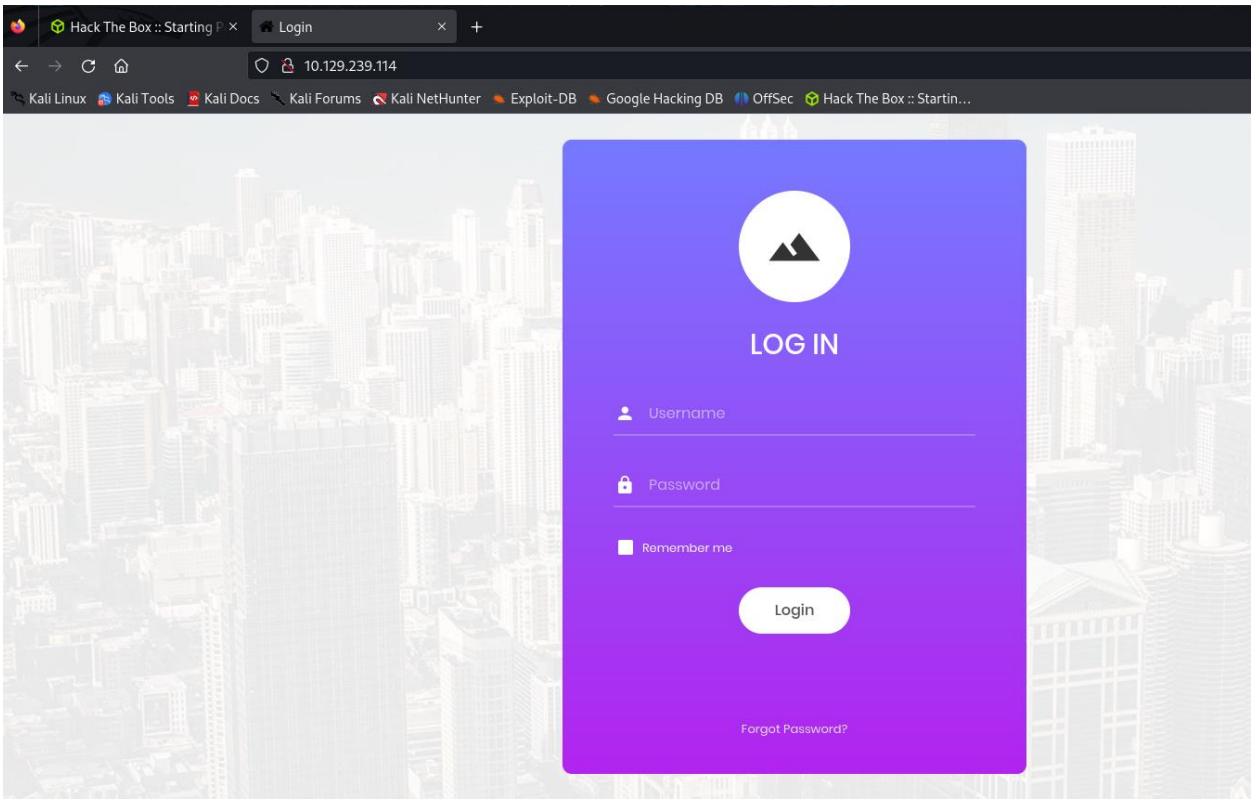
Target Ip=10.129.239.114

With the given IP of the machine, I ran nmap scan in order to know about running services

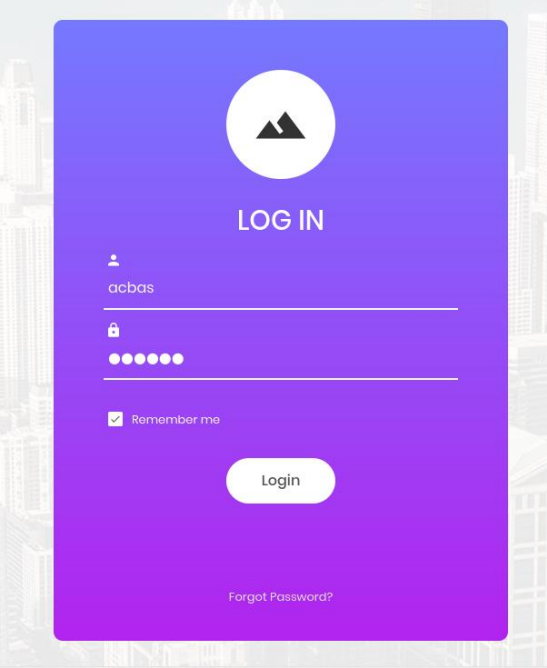
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sV 10.129.239.114
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 16:22 PKT
Nmap scan report for 10.129.239.114
Host is up (0.33s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.78 seconds
```

So I found port 80 open running some services of http obviously, on reaching the given ip I was welcomed with a log in page



After this I tried some random inputs so that I can analyze the response and the act accordingly,



Or providing the wrong credentials I was again directed to the same page without any message or any change in the url and if I switch to forgot password then again I am directed to the same page with new url http://10.129.239.114/#

As I was not getting any luck so I decided to use dirb in order to further enumerate.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ dirb http://10.129.239.114/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jan 15 16:32:40 2024
URL_BASE: http://10.129.239.114/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.129.239.114/ ----
==> DIRECTORY: http://10.129.239.114/css/
```

After this dirb scan I found some new pages such as

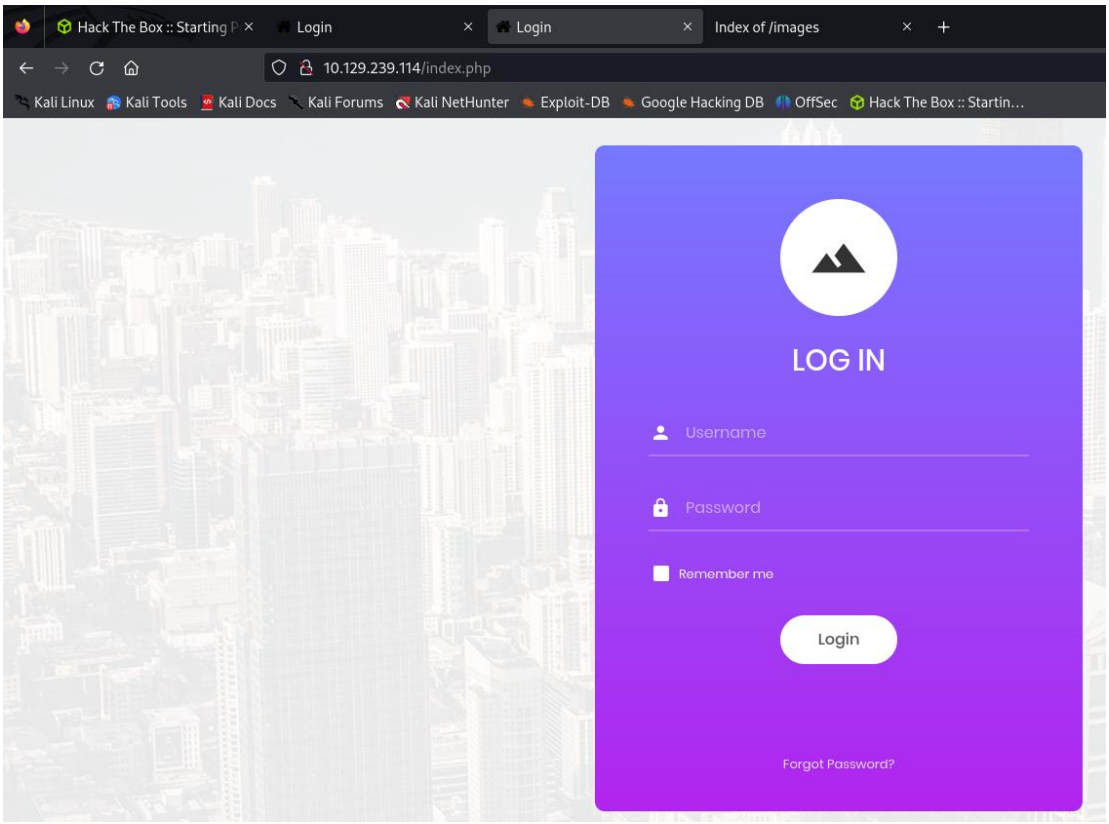
http://10.129.239.114/fonts

http://10.129.239.114/images

http://10.129.239.114/css

http://10.129.239.114/index.php

fonts images css all these just contained some css files some images and some fonts being used, index.php seemed really interesting at first but as I pinged to it I was again directed to the same initial login page.



So after all this I tried to manually brute force this by adding

admin:admin

admin:123

User:123

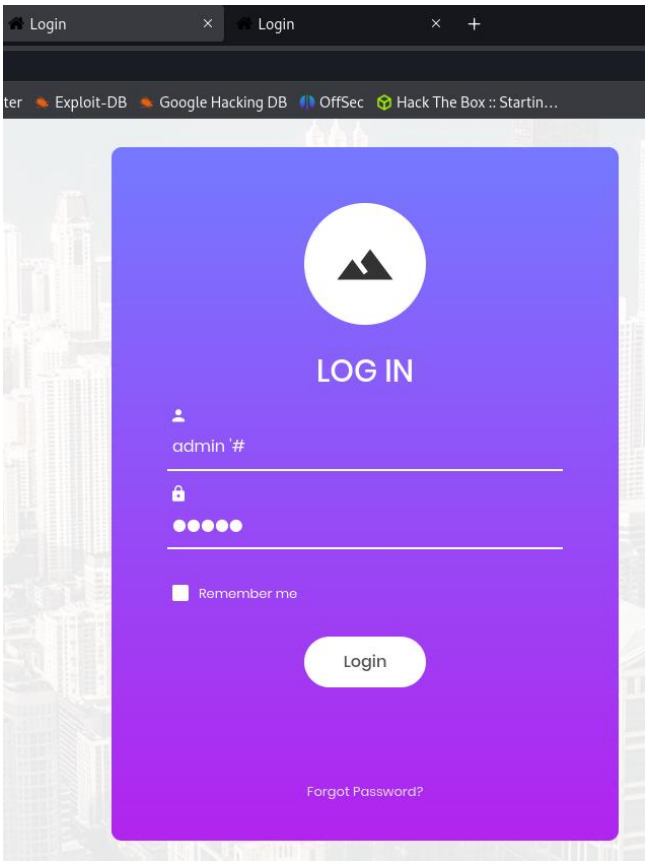
Root:root

Admin:1234@Abcd

And some others that I may gain luck but no luck

So then I decided to perform sql injection on this page so I added admin'# in the username field,

What I did was it infected the query



single quote in the admin'# told the query to search and select from admin and # commented the remaining query which was validating that the provided credentials are correct so by running this malicious query I bypassed the log in page and got the flag