Tier 1 Appointment Report

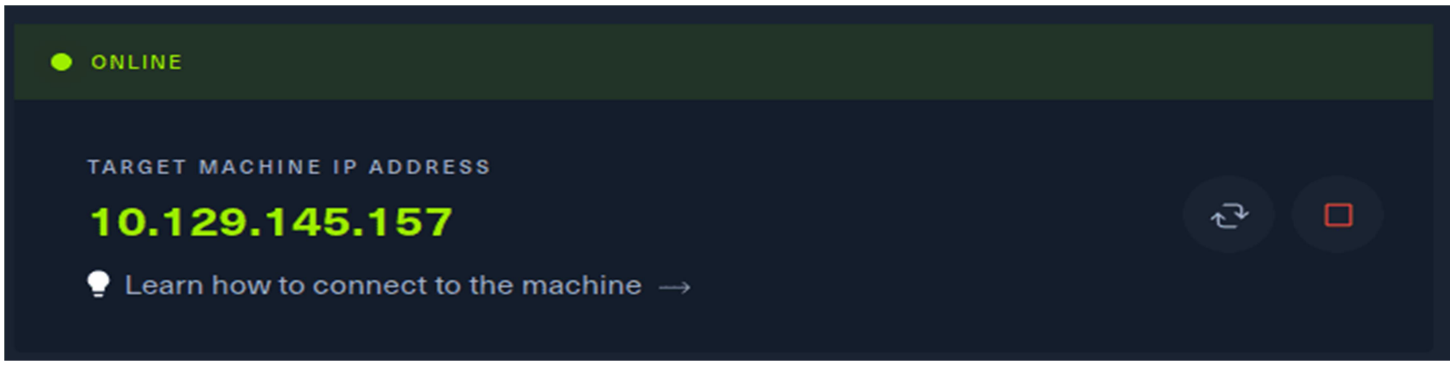
Prepared by: **Chanpreet Kaur**

Tools Used

- NMAP
- SQL Injection

Procedure

I will cover solution steps of the "**Appointment**" machine, which is part of the '**Starting Point**' labs and has a difficulty rating of '***Very Easy***'.



The machine is now active and showing a target IP address **10.129.145.157**

Now, we have to solve all the available tasks by providing correct inputs, we can also use hints in case we are stuck.

- **What does the acronym SQL stand for?**
  Structured Query Language

- **What is one of the most common type of SQL vulnerabilities?**
  SQL injection

- **What service and version are running on port 80 of the target?**
  Apache httpd 2.4.38 ((Debian))

- **What is the standard port used for the HTTPS protocol?**
  443

Now we will run nmap scan on the [Target_IP] as shown below –

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.129.145.157
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-18 04:32 EST
Nmap scan report for 10.129.145.157
Host is up (0.24s latency).
Not shown: 994 closed ports
PORT      STATE    SERVICE      VERSION
42/tcp    filtered nameserver
80/tcp    open     http         Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login
```

After executing the command, I discovered the port 80 is open and it is running Apache http server with version 2.4.38

- **What is a folder called in web-application terminology?**
  directory

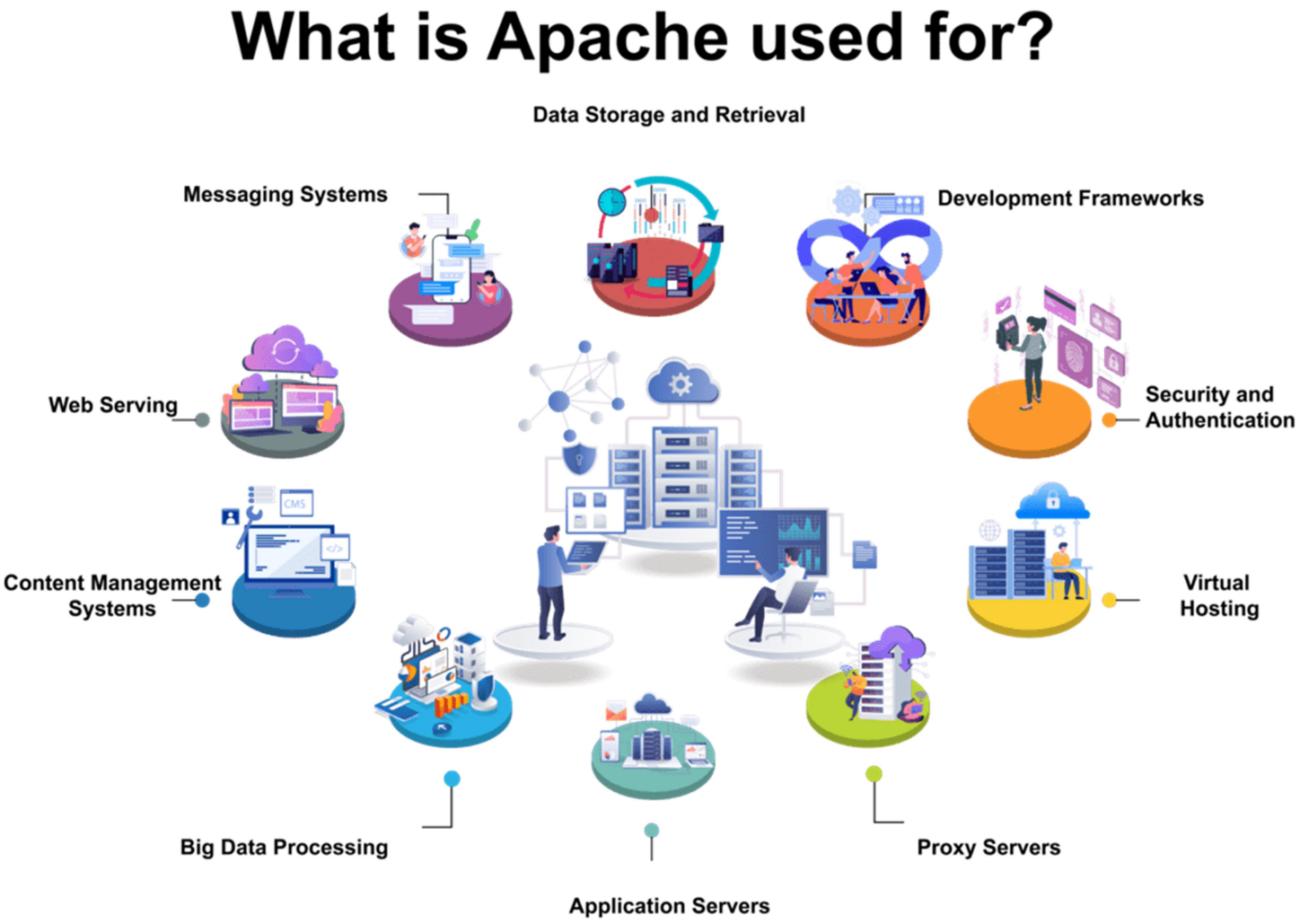
- **What response code is given for “Not Found” errors?**
  404

- **What switch do we use with Gobuster to specify we’re looking to discover directories, and not subdomains?**
  dir

- **What symbol do we use to comment out parts of the code?**
  #

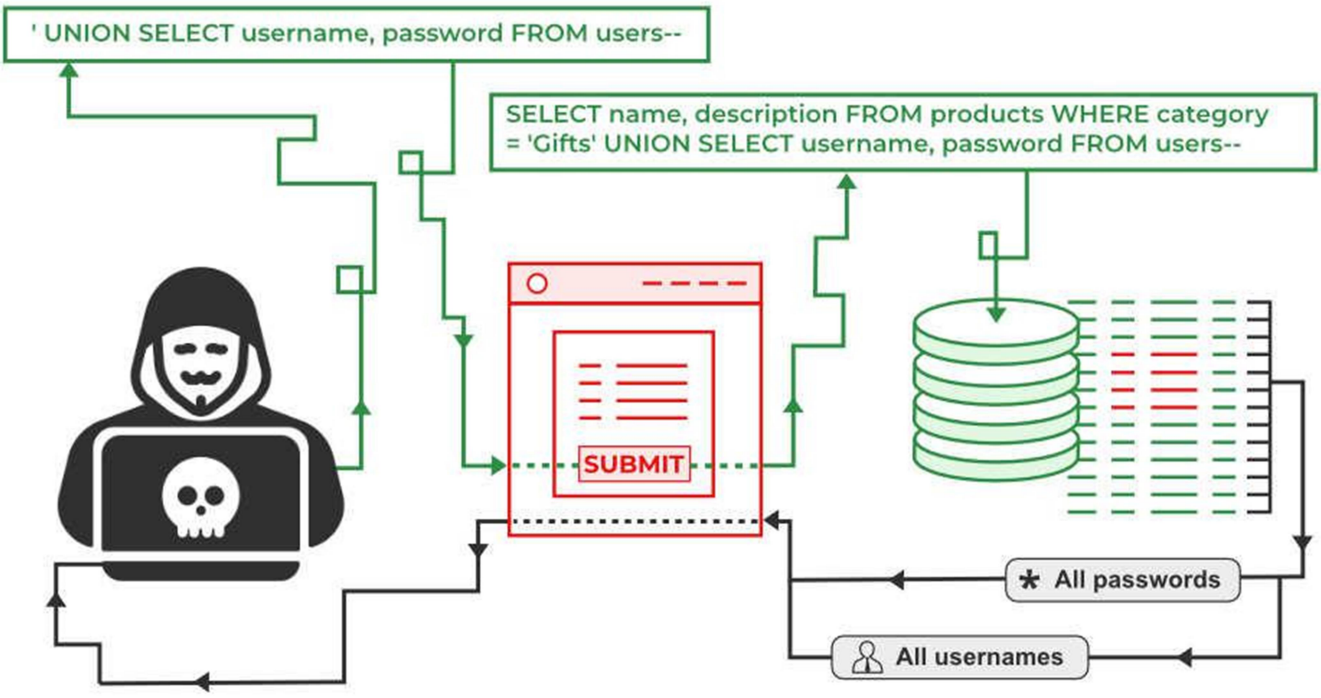
Apache Server .

Apache is free and open-source software of web server that is used by approx 40% of websites all over the world. Apache HTTP Server is its official name. It is developed and maintained by the Apache Software Foundation. Apache permits the owners of the websites for serving content over the web. It is the reason why it is known as a "web server." One of the most reliable and old versions of the Apache web server was published in 1995.



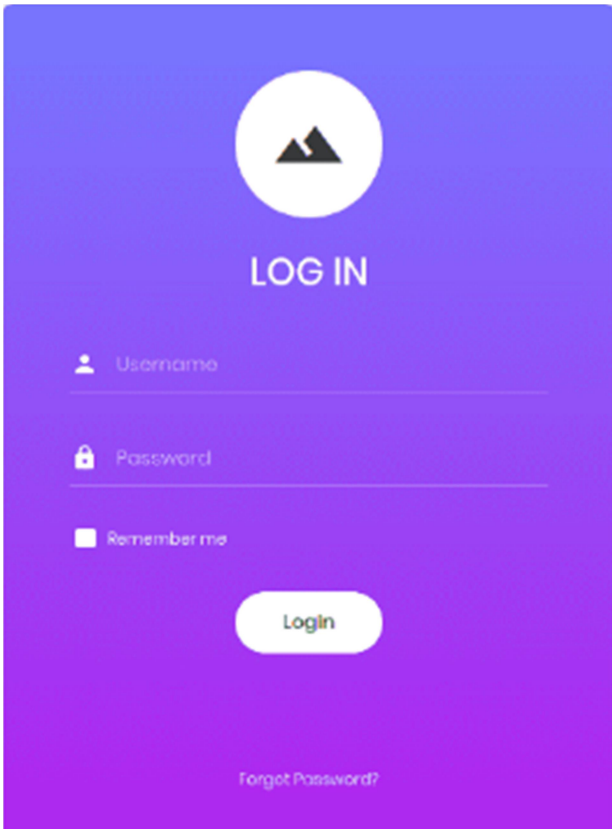
SQL Injection .

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.



Now, If I type the IP address of the device into the address bar of our browser, we can see a website with a login form.

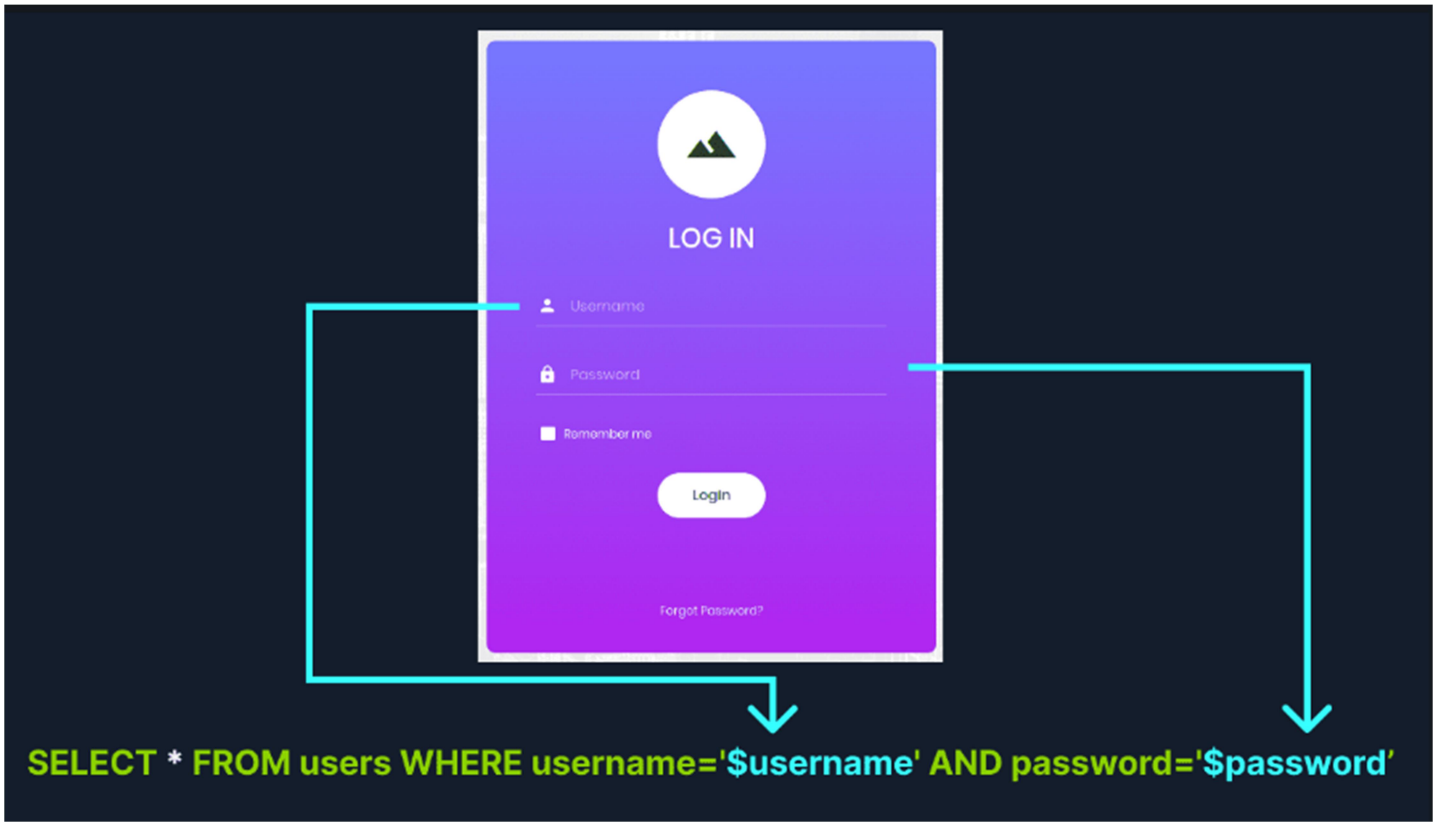
So let's start exploiting this.



Even after attempting default credential insertion or utilizing brute-force attacks to bypass the login system, I was still unable to gain access.

Now, We'll explore potential SQL injection vulnerabilities within the login form. Here's a sample SQL query responsible for authenticating usernames and passwords to grant access:

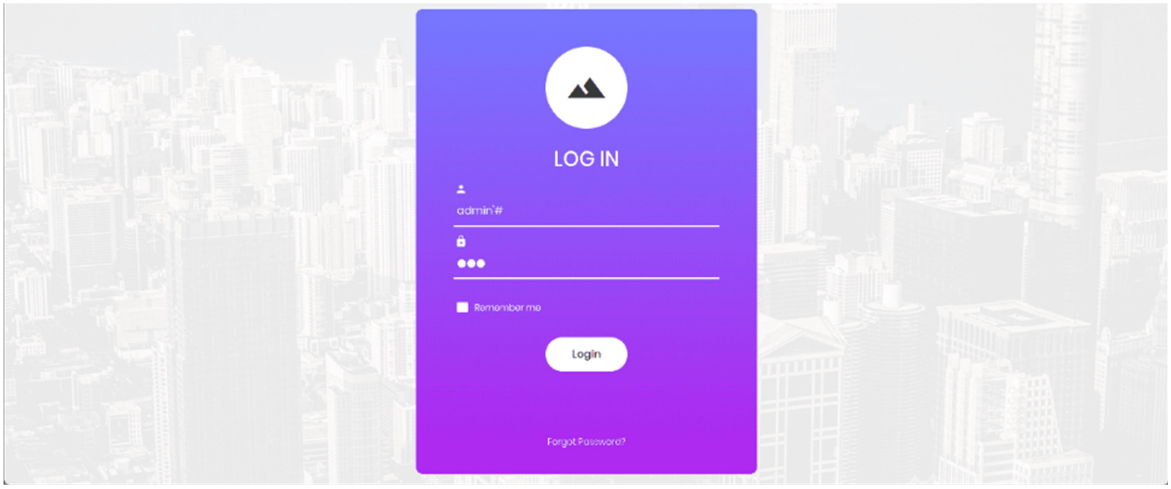
```
SELECT * FROM users WHERE username='$username' AND password='$password'
```



We can attempt SQL injection in the given login form because the values entered in the username and password fields replace **$username** and **$password**, respectively.

Additionally, in PHP, the **#** symbol comments out lines of code, granting us an opportunity to manipulate the SQL query.

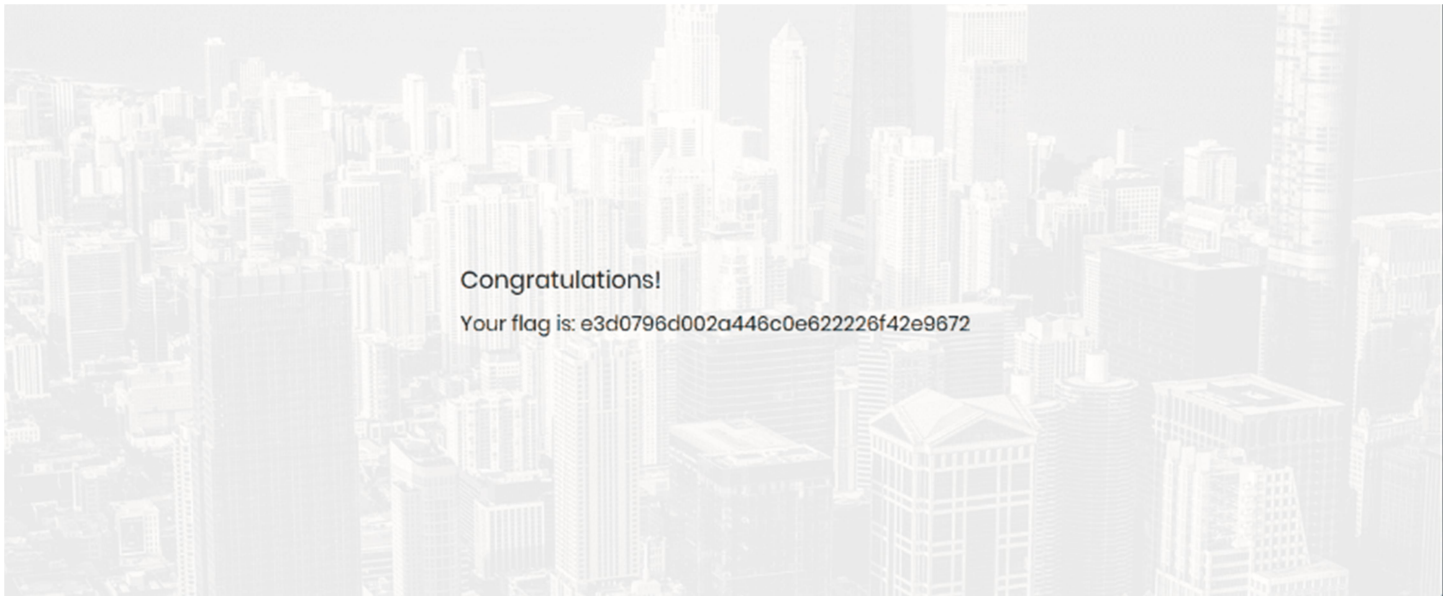
Let’s try this out,



By entering "admin'#" in the username field, the code processes it, setting the username as "admin." The trailing # comments out the rest of the line, essentially bypassing the password validation. Consequently, we can input any value in the password field to successfully log in.

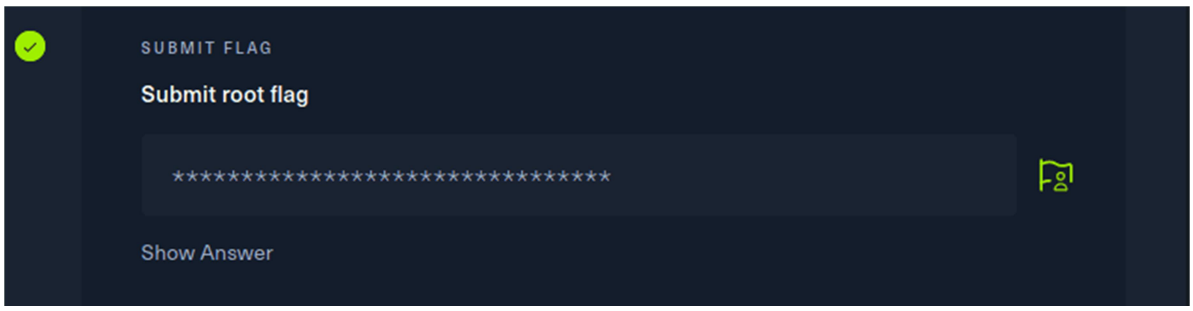
Query will look something like this…

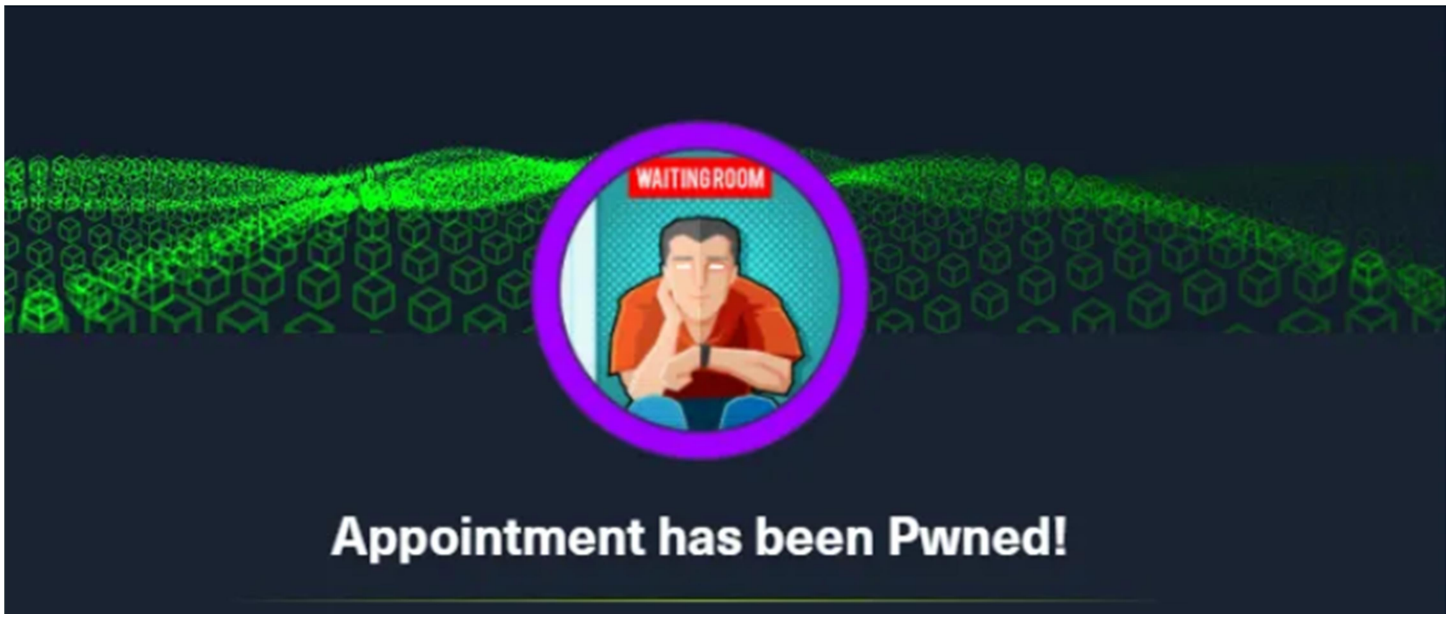
After the submission of the form, you will get the flag



Congratulations we have successfully exploited it

Copy the flag value and paste it into the Starting Point lab's page to complete your task




WAITING ROOM
Appointment has been Pwned!