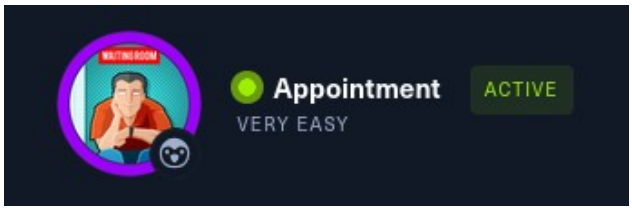
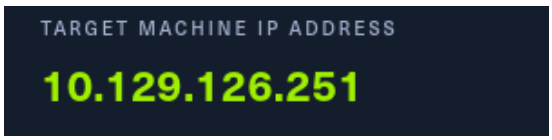




1. What does the acronym SQL stand for?
   Answer: Structured Query Language

2. What is one of the most common types of SQL vulnerabilities?
   Answer: SQL Injection

3. What is the 2021 OWASP Top 10 classification for this vulnerability?
   Answer: A03:2021-Injection

4. What does Nmap report as the service and version that are running on port 80 of the target?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV -p 80 10.129.126.251
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 11:00 EDT
Nmap scan report for 10.129.126.251
Host is up (0.069s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
```

   Answer: Apache httpd 2.4.38 ((Debian))

5. What is the standard port used for the HTTPS protocol?
   Answer: 443

6. What is a folder called in web-application terminology?
   Answer: directory

7. What is the HTTP response code is given for 'Not Found' errors?
   Answer: 404

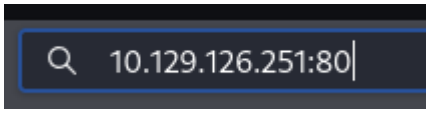
8. Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ gobuster --help | grep -i 'directory'
  dir         Uses directory/file enumeration mode
```

   Answer: dir

9. What single character can be used to comment out the rest of a line in MySQL?
   Answer: #

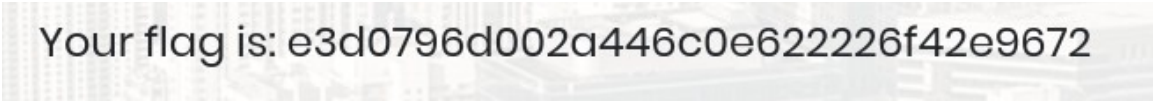
10. If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?



Login: admin' --
Password: 123

Answer: Congratulations

11. Submit root flag.



Answer: e3d0796d002a446c0e622226f42e9672