# Appointment

## Task1

What does the acronym SQL stand for?

`Structured Query Language`

## Task 2

What is one of the most common type of SQL vulnerabilities?

`SQL Injection`

## Task 3

What does PII stand for?

`Personally Identifiable Information`

## Task 4

What does the OWASP Top 10 list name the classification for this vulnerability?

- Hint: Consult the OWASP Top 10 on the OWASP website.

`A03:2021-Injection`

## Task 5

What service and version are running on port 80 of the target?

- Hint: Simply run `sudo nmap -sC -sV -v YourBoxIP`

`Apache httpd 2.4.38 ((Debian))`

## Task 6

What is the standard port used for the HTTPS protocol?

`443`

## Task 7

What is one luck-based method of exploiting login pages?

`brute-forcing`

## Task 8

What is a folder called in web-application terminology?

`directory`

## Task 9

What response code is given for "Not Found" errors?

`404`

## Task 10

What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?
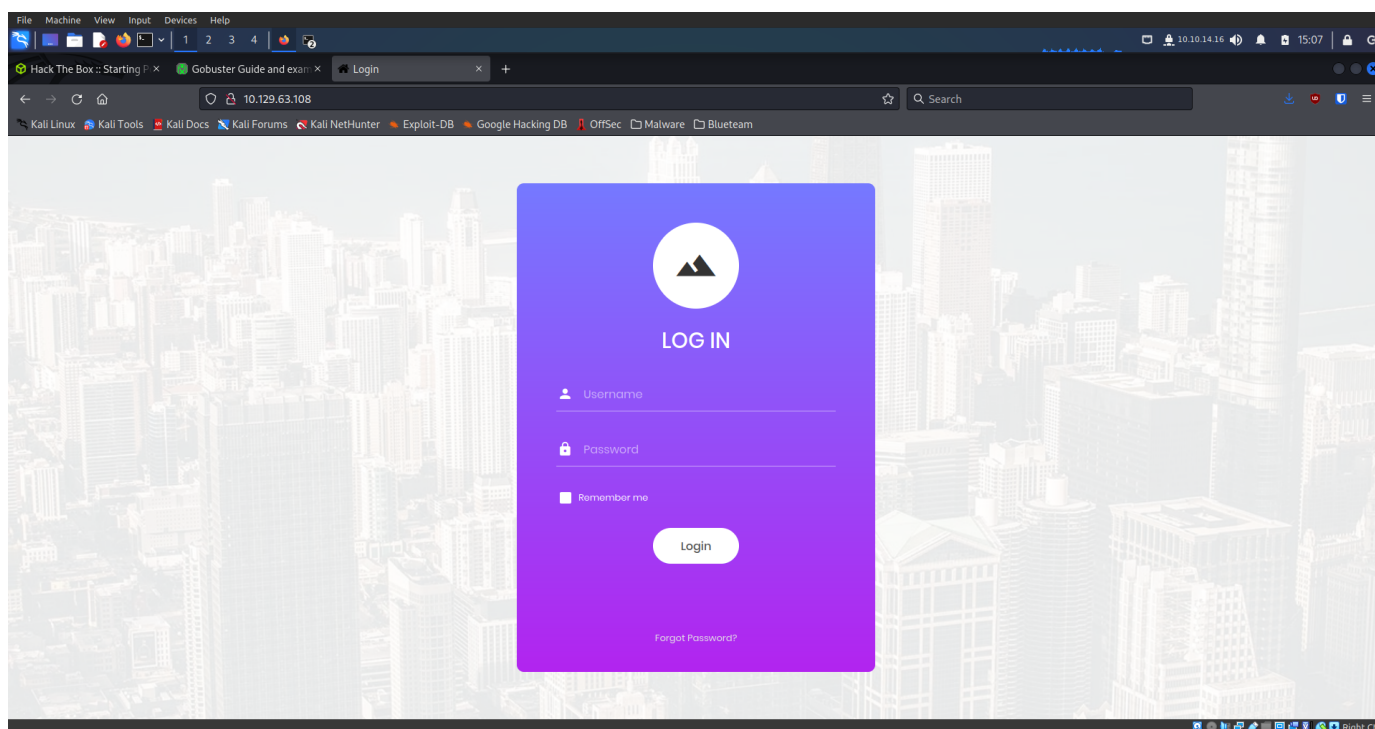
`dir`

## Task 11

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

`#`

## Task 12

Submit root flag

To find the root flag we must first paste the target IP into Firefox. It should bring to a page like this:



We can then do a Ctrl+U to inspect the elements of the page. We can examine it to see if it can give us any usernames or passwords:

Since we can't find any, we will attempt a SQL Injection. I will be attempting it with some common usernames such as admin, adminstrator and root.

- Example syntax for SQL Injection: `admin'#`



The single `'` is used as a character limiter. The `#` is used to close our syntax. The reason for this gibberish is to cancel out any queries for the password. Meaning we can put whatever we want for the password on this page. So, let's see if this will work:

Congratulations!

Your flag is: e3d0796d002a446c0e622226f42e9672