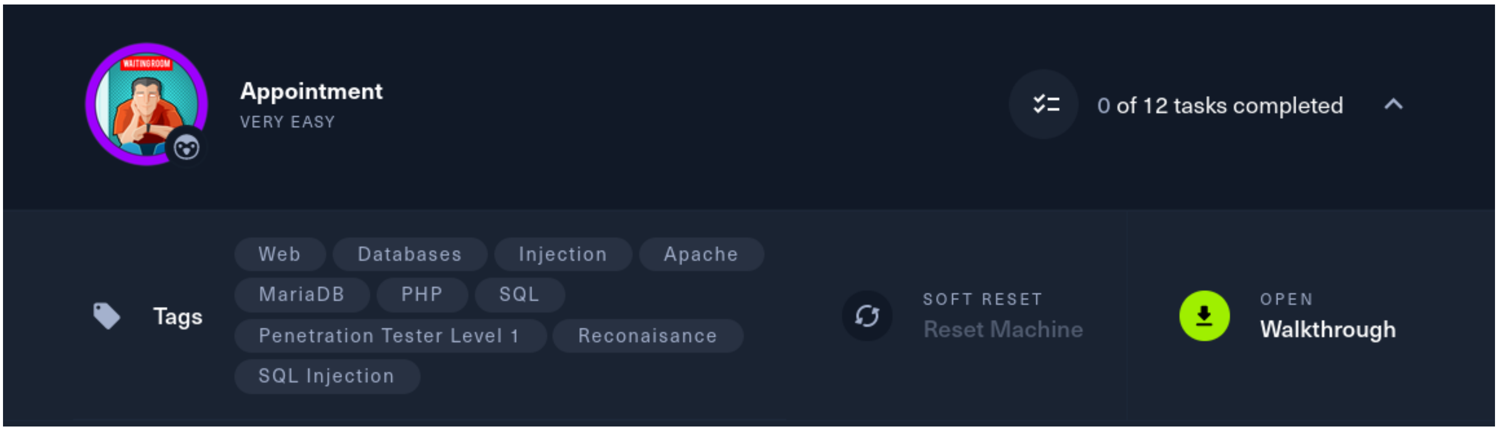
Appointment | TIER 1

TIER 1 BEGINS

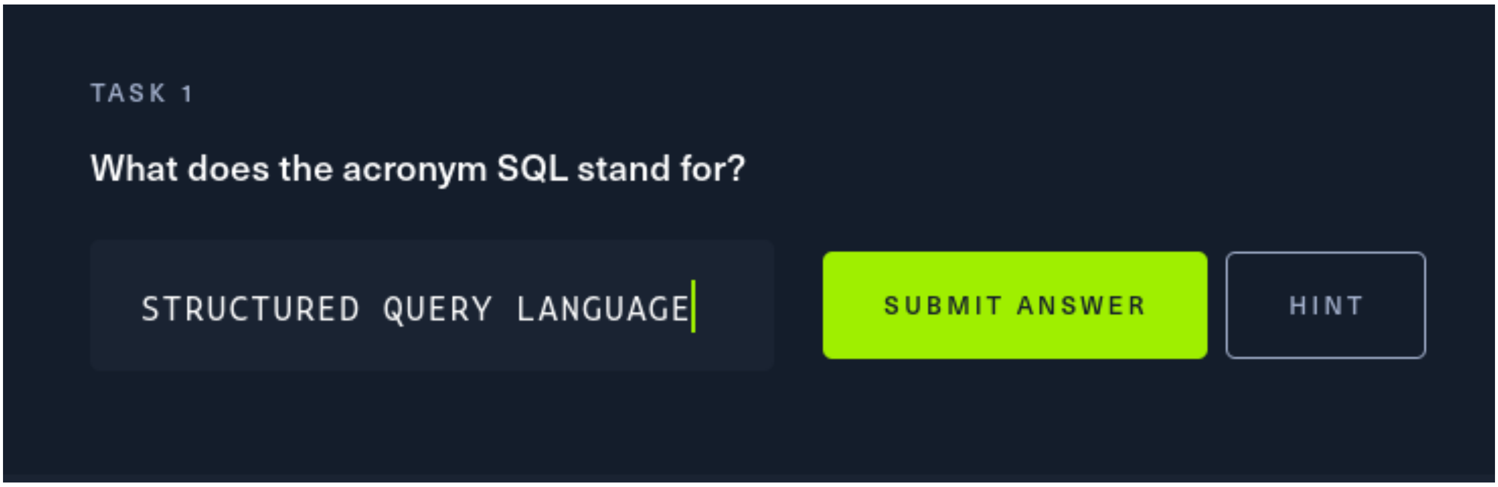


10.129.88.43

Q/A SECTION

1)

SQL (pronounced "ess-que-el") stands for **Structured Query Language**. SQL is used to communicate with a database. According to ANSI (American National Standards Institute), it is the standard language for relational database management systems.

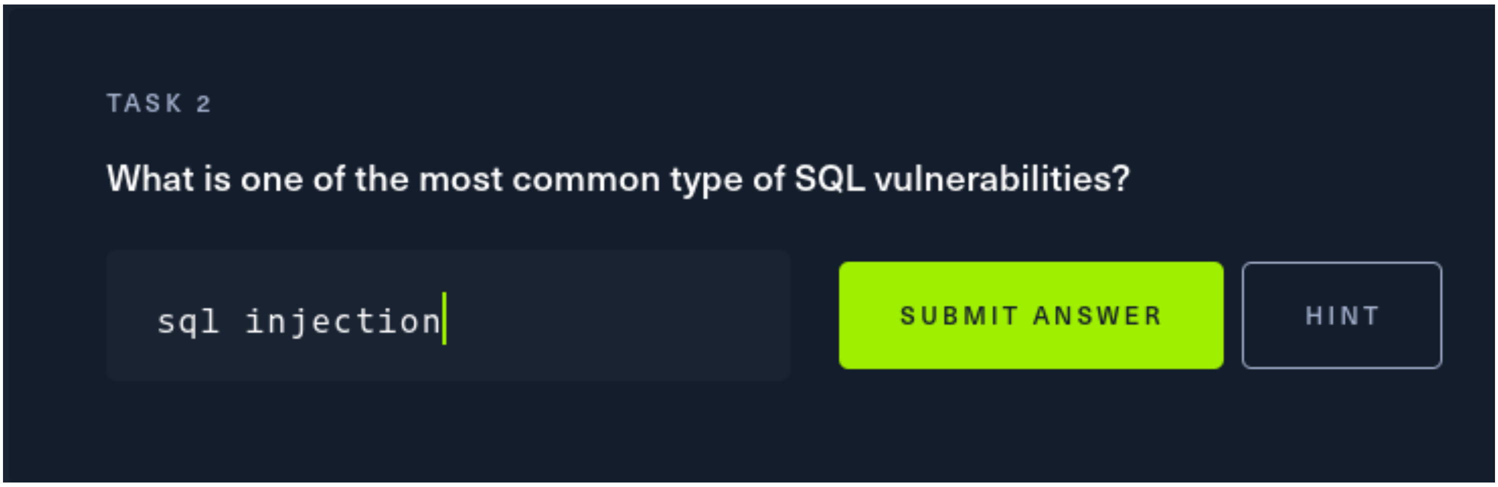


TASK 1

What does the acronym SQL stand for?

STRUCTURED QUERY LANGUAGE

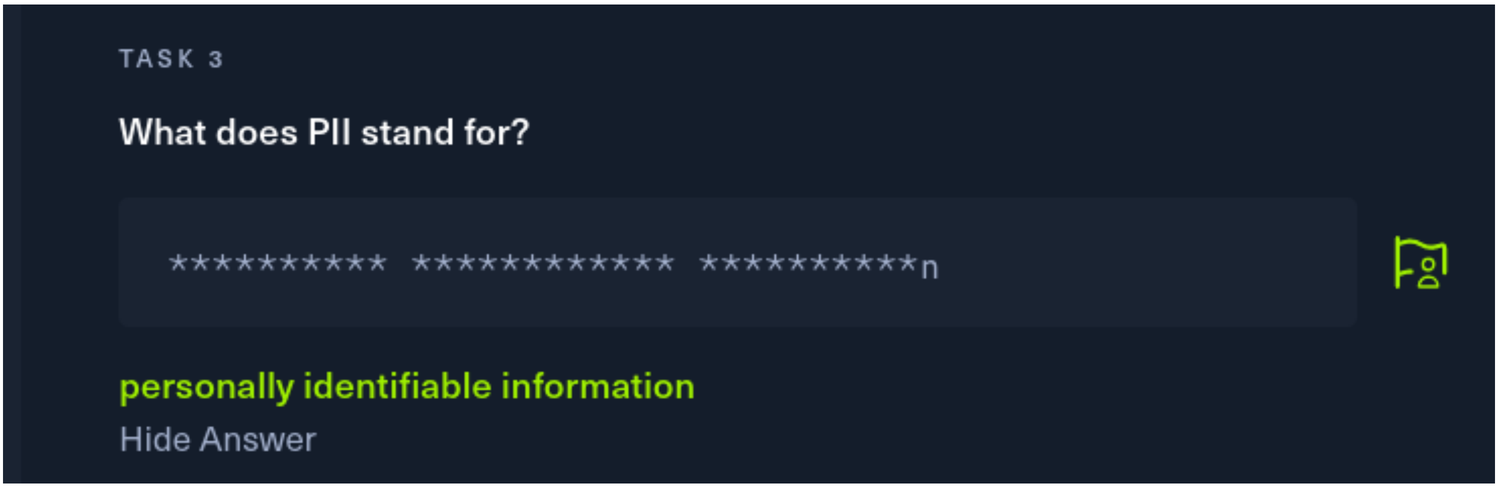
2)


TASK 2

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

```
sql injection
```

3) **Personal Identifiable Information** (PII) is defined as: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

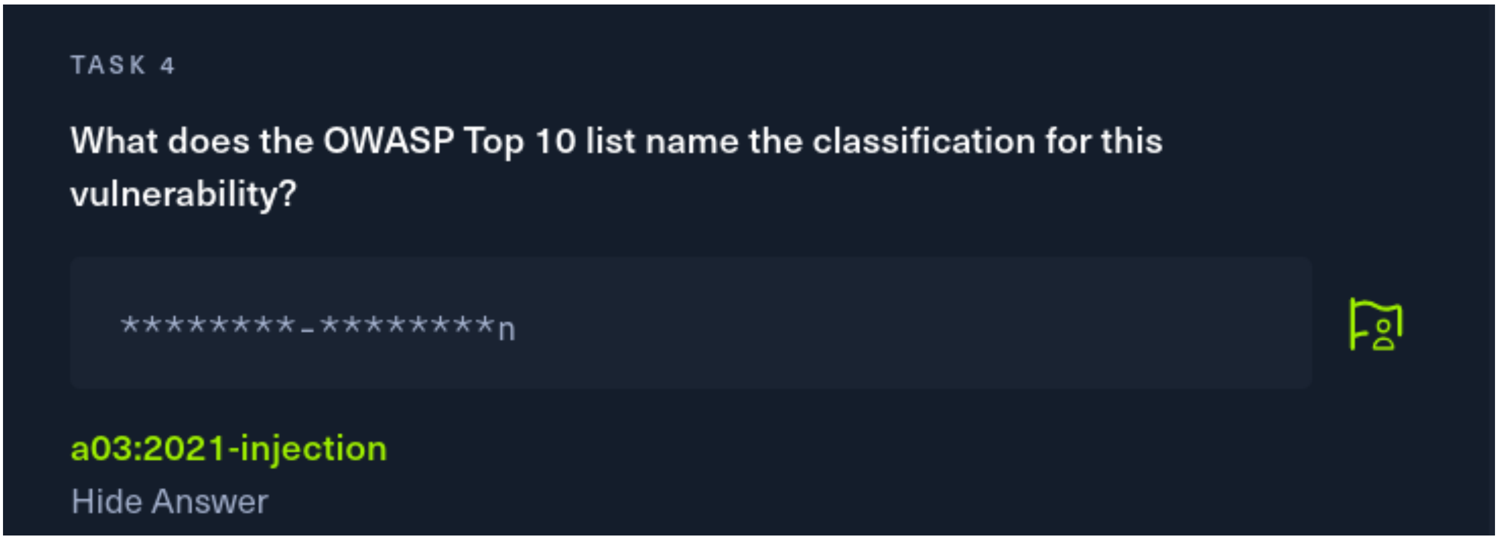

TASK 3

What does PII stand for?

```
********** *********** **********n
```

personally identifiable information

4)

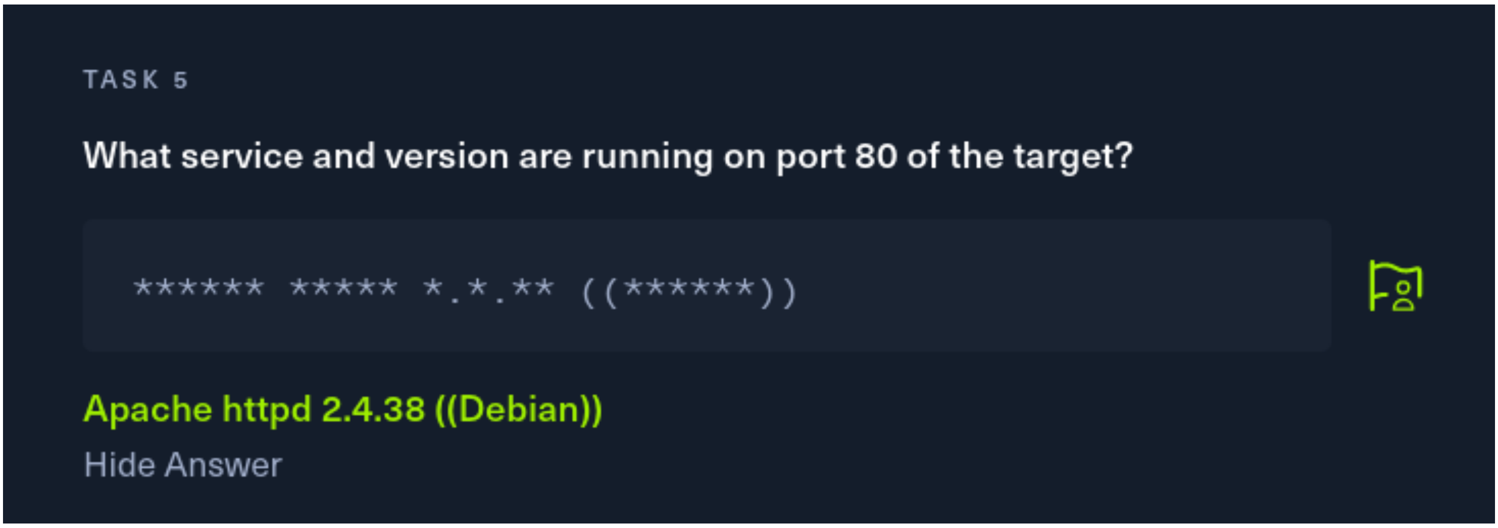

TASK 4

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

```
********_********n
```

a03:2021-injection

5)



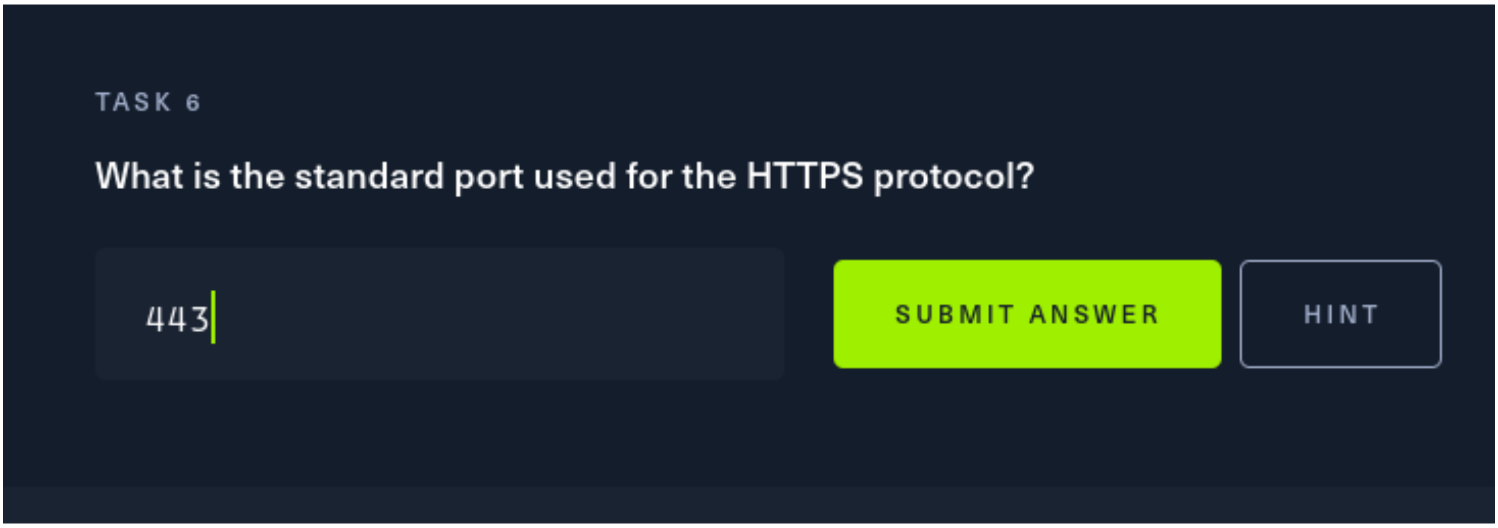
TASK 5

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

```
****** ***** *.*.** ((******))
```

Apache httpd 2.4.38 ((Debian))

6) By default, these two protocols are on their standard port number of 80 for HTTP and **443** for HTTPS.

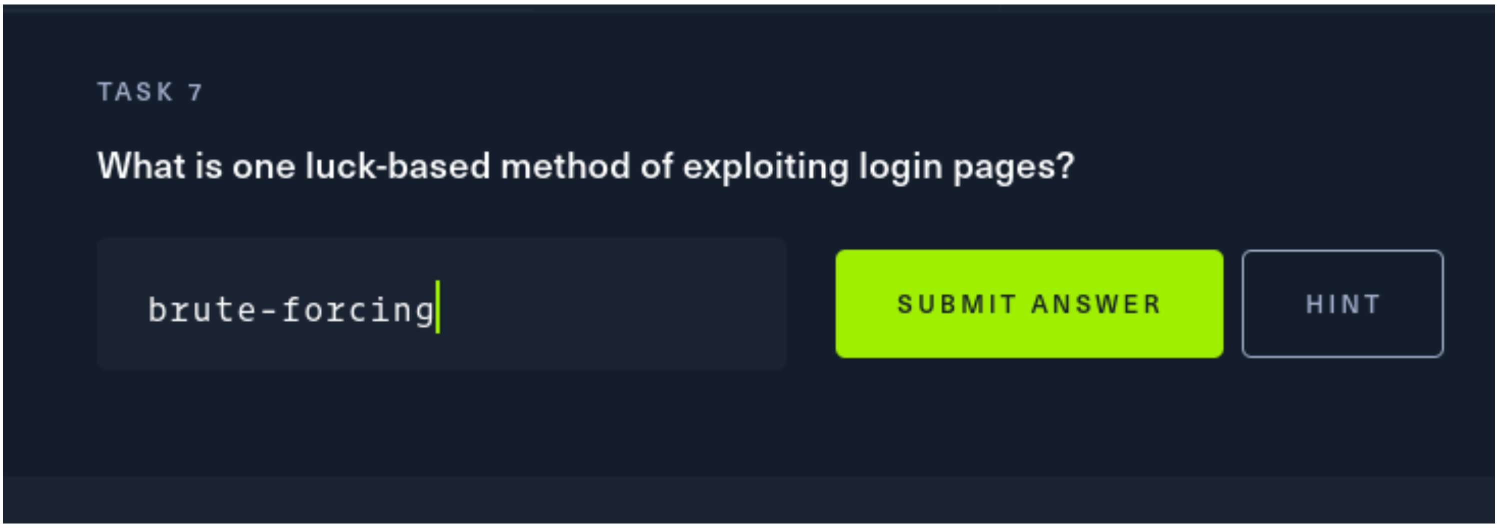


TASK 6

What is the standard port used for the HTTPS protocol?

443

7)

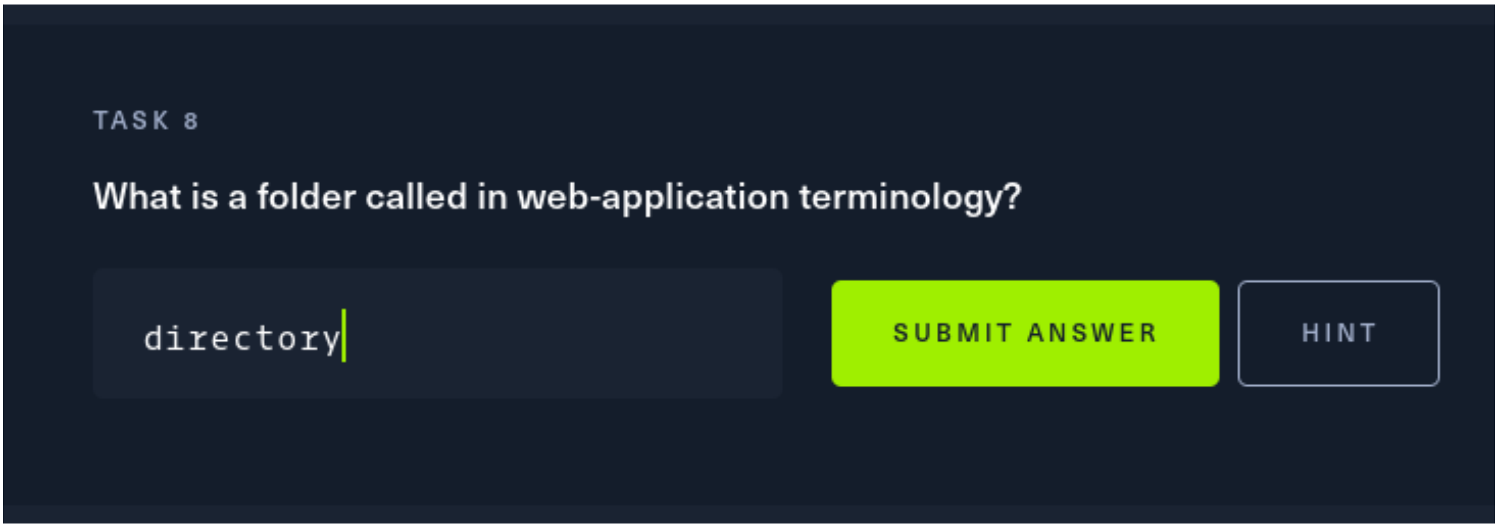


TASK 7

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

brute-forcing

8)

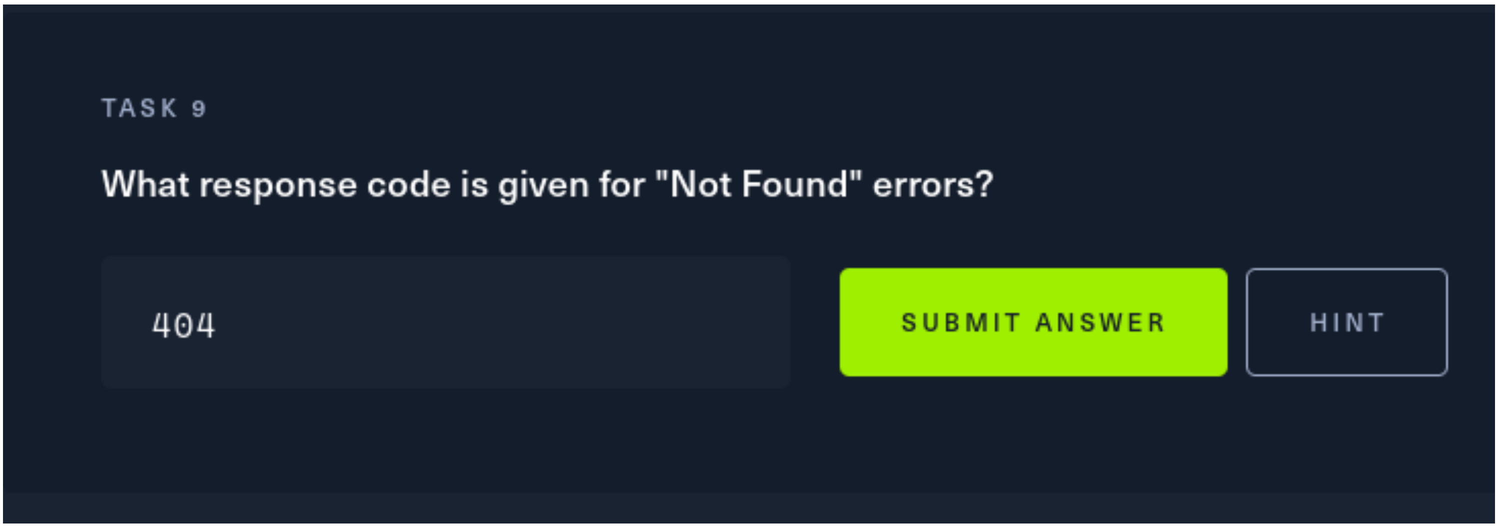


TASK 8

What is a folder called in web-application terminology?

directory

9)

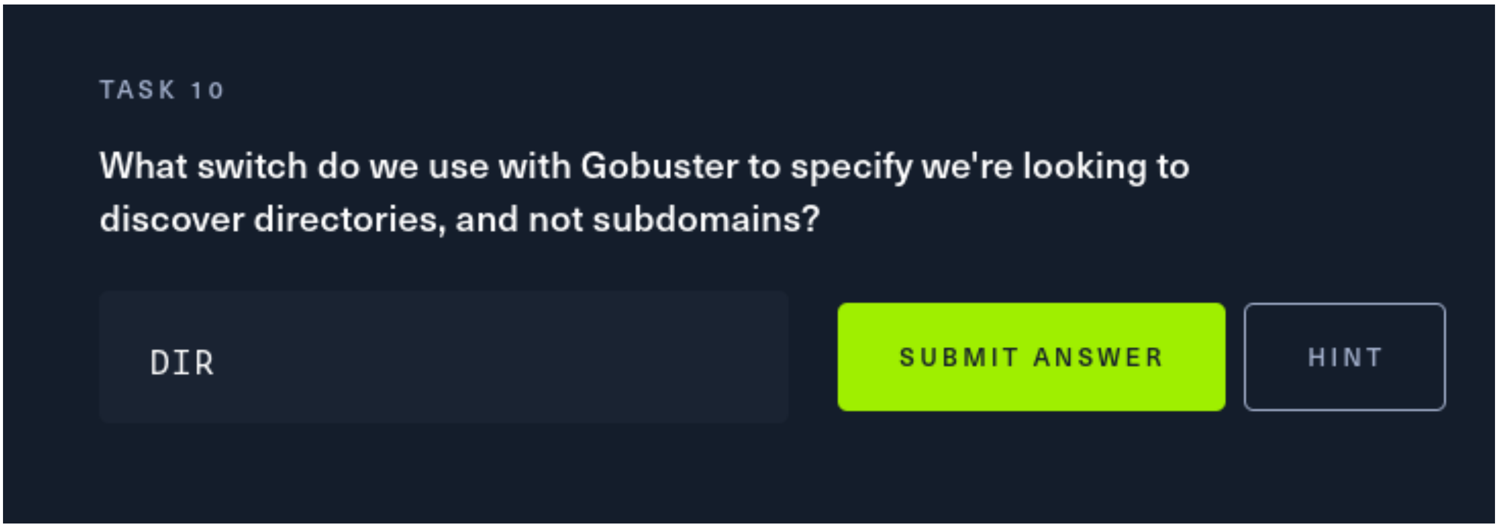


TASK 9

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

404

10)

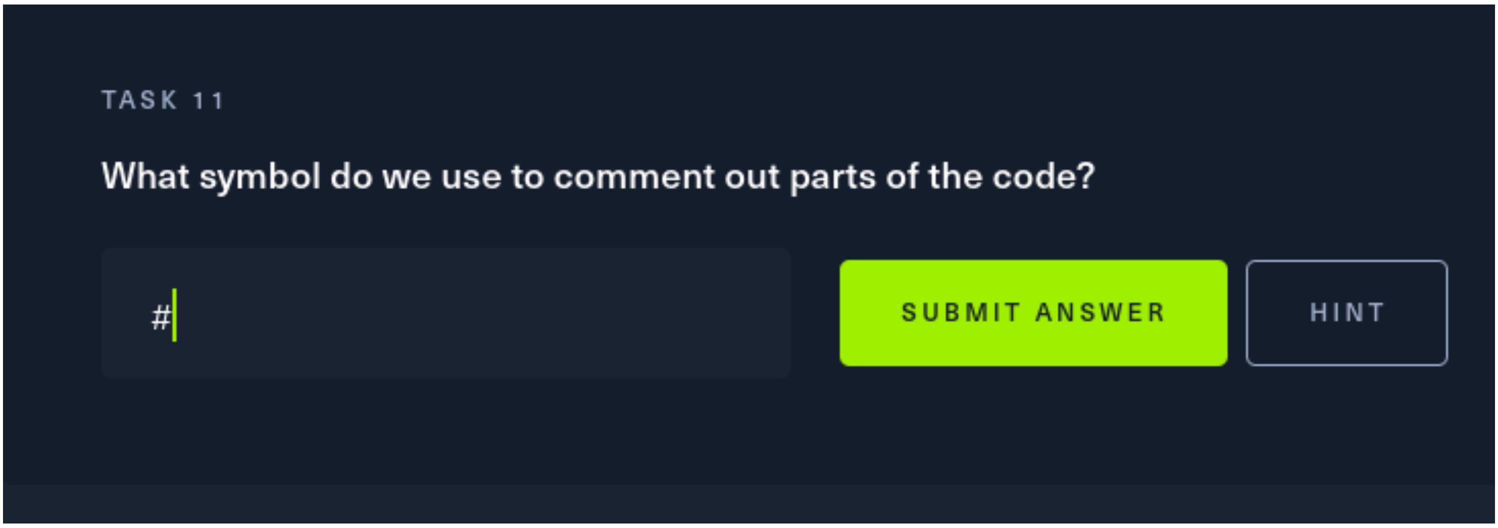


TASK 10

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

DIR

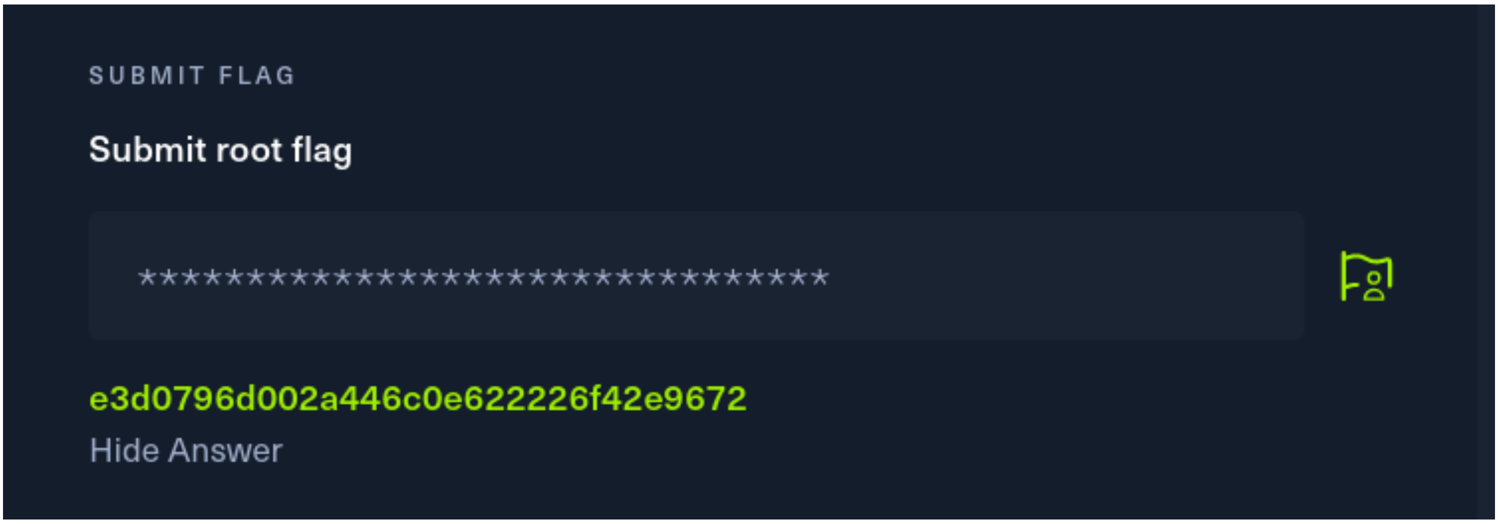
11)


TASK 11

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

#

12)


SUBMIT FLAG

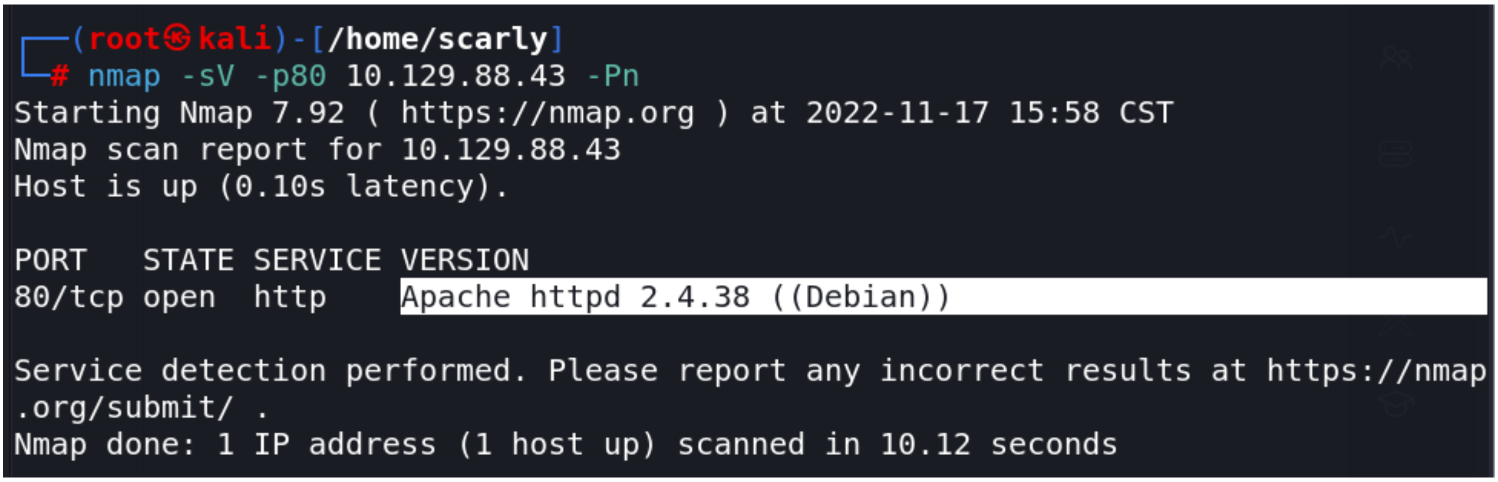
Submit root flag

****

e3d0796d002a446c0e622226f42e9672

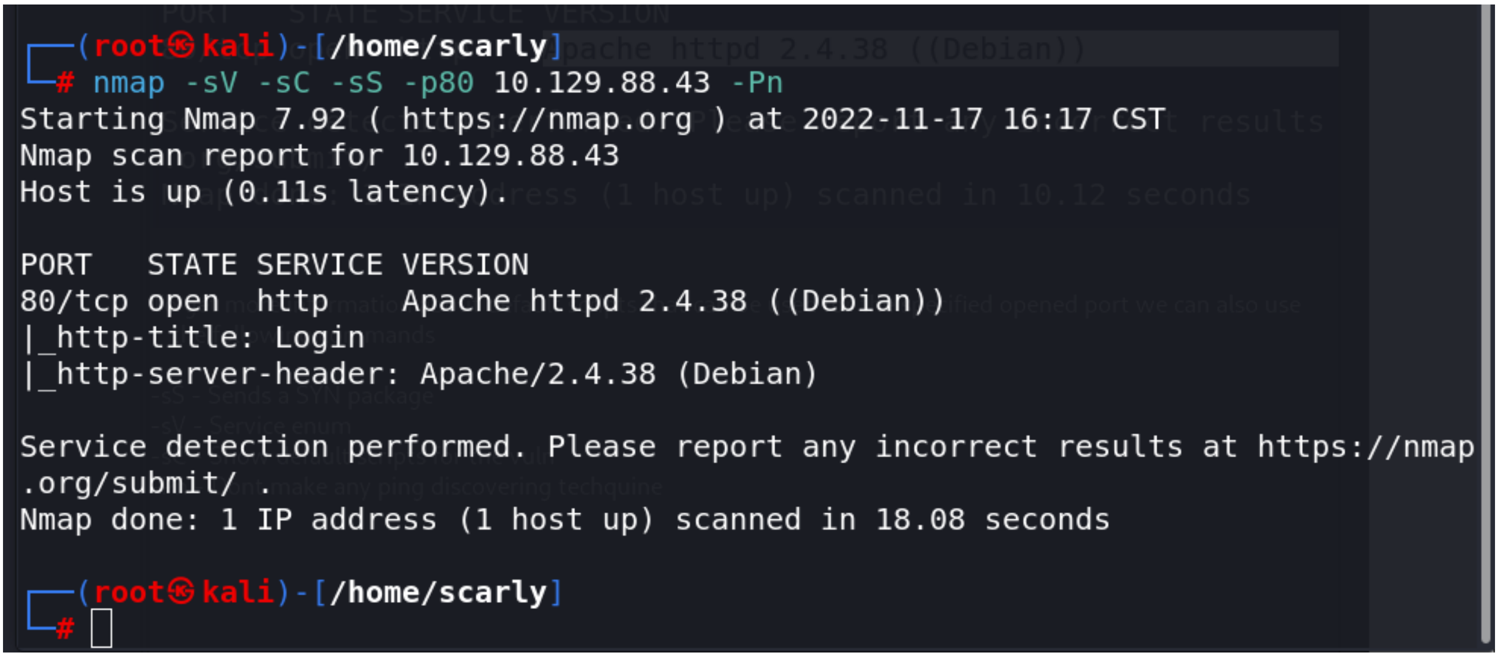
NMAP enumeration

We just have to check for both service and version running on port 80 so lets do it.


```
┌──(root㉿kali)-[/home/scarly]
└─# nmap -sV -p80 10.129.88.43 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 15:58 CST
Nmap scan report for 10.129.88.43
Host is up (0.10s latency).

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 10.12 seconds
```

To get more information about default scripts that can be used for the specified opened port we can also use the following commands

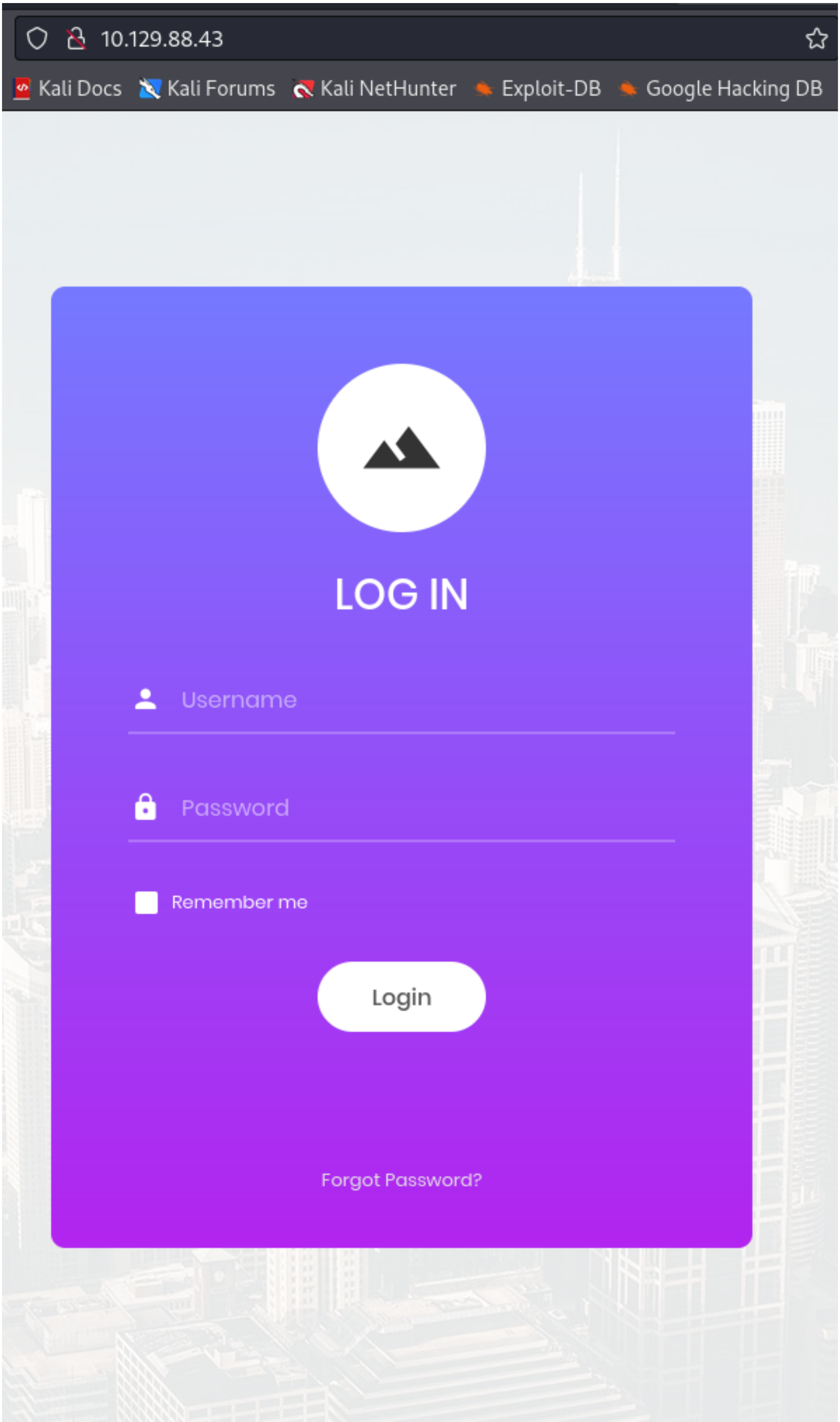
-sS - Sends a SYN package
-sV - Service enum
-sC - Show default scripts for the vuln
-Pn - Dont make any ping discovering techquine



```
┌──(root㉿kali)-[/home/scarly]
└─# nmap -sV -sC -sS -p80 10.129.88.43 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 16:17 CST
Nmap scan report for 10.129.88.43
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Login
|_http-server-header: Apache/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 18.08 seconds

┌──(root㉿kali)-[/home/scarly]
└─# 
```

CTF

10.129.88.43:80 on our browser

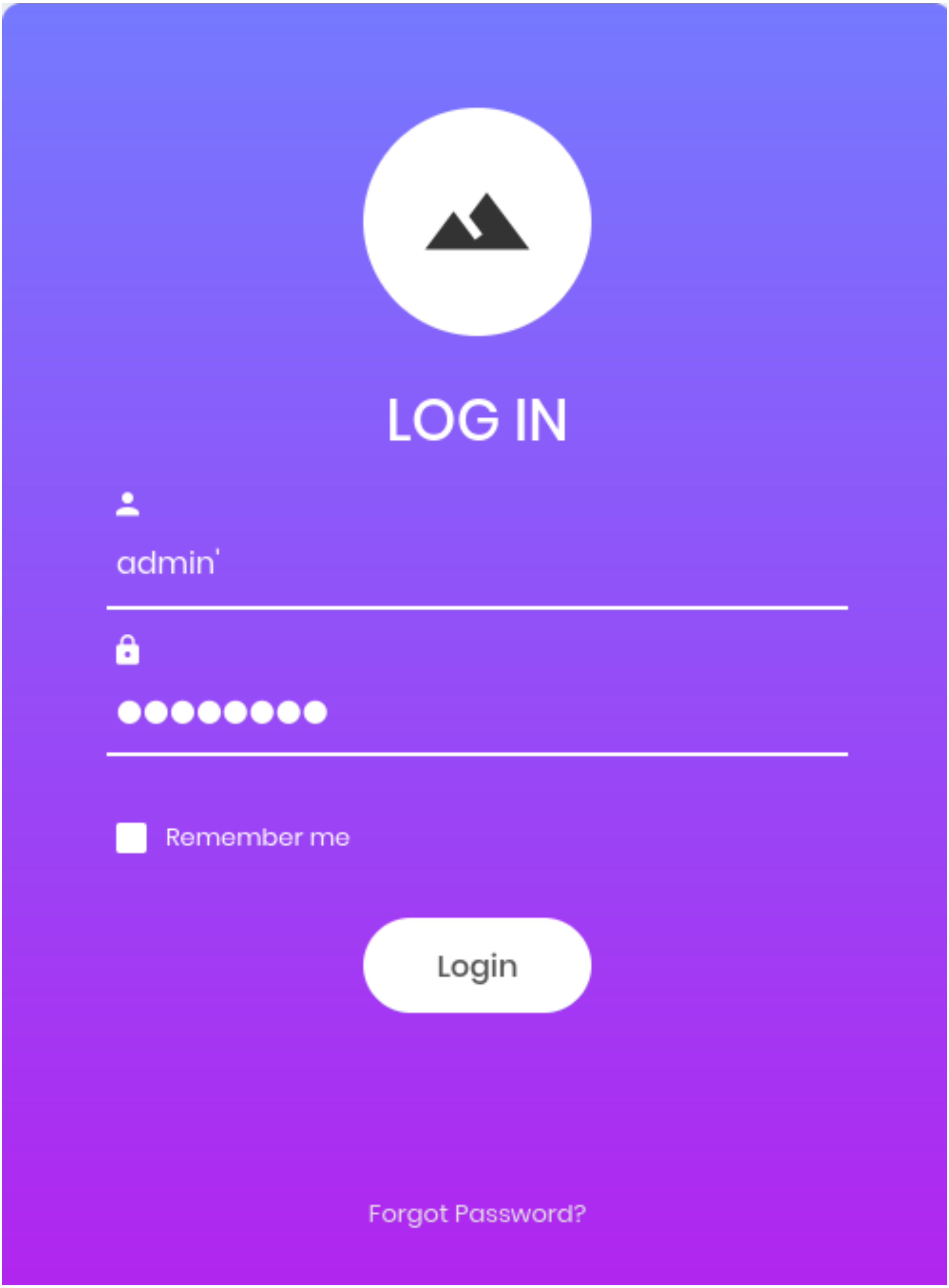


10.129.88.43
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
LOG IN
Username
Password
Remember me
Login
Forgot Password?

Tenemos que hacer una inyección SQL, probando solo con el nombre de usuario porque la contraseña en algunos casos es solo un campo de front-end requerido pero no en el backend

We'll add the ' simple quotation since we are assuming that its selecting a username and password directly from the database. So this is going to select the username we want to

So we have admin' ant in password field we can literally put whatever



Although it would work in some cases, this aint.

We'll add a pound # sign.
# is how you comment out

Th final result is the following:

admin'#

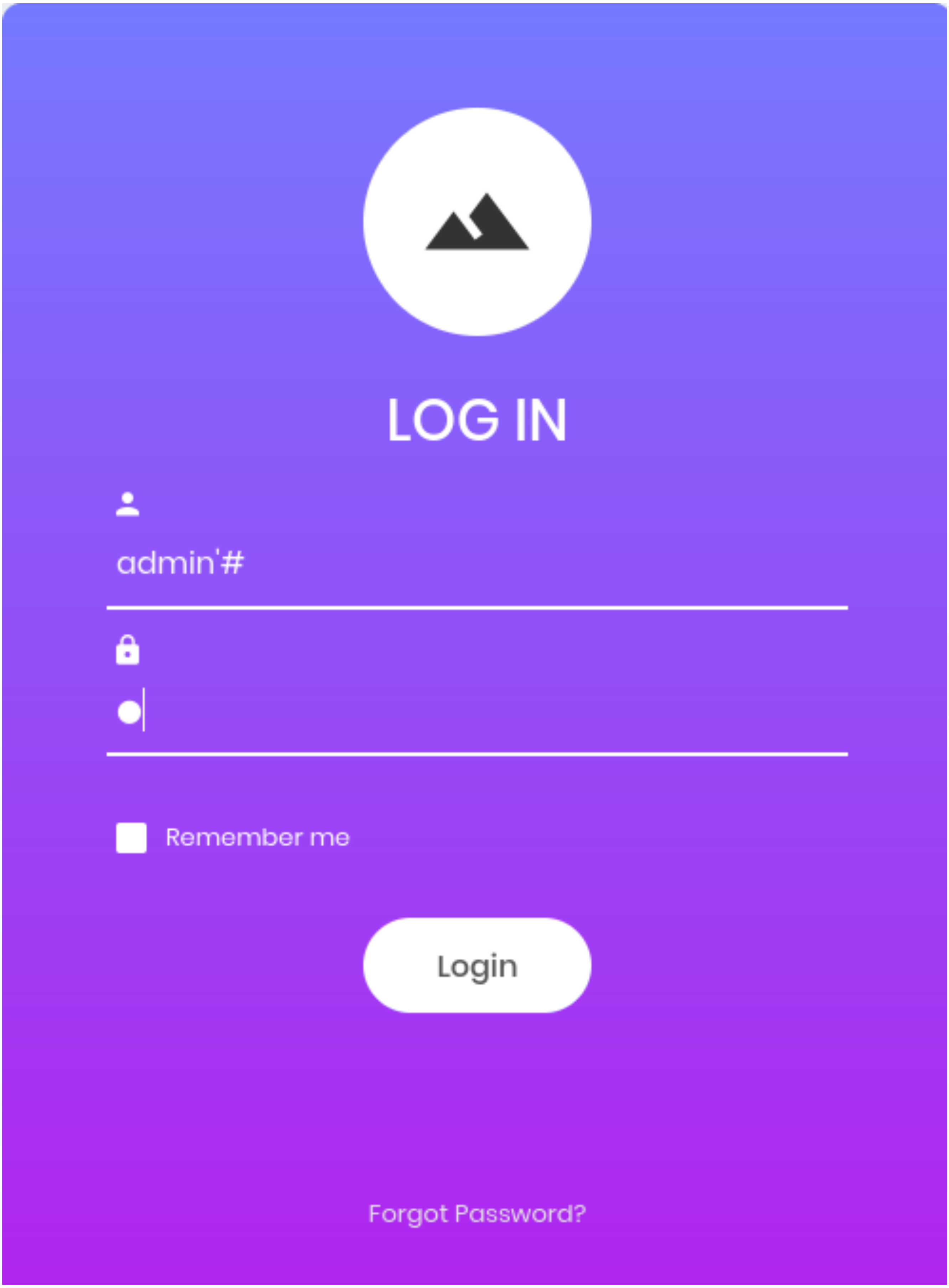
What are we doind here?

We're going to inject the username admin
Weŕe going to close off the username

And when it's looking to ask for the password you can assume there's a very similar query on the backend to openning the bracket and it's going to look for that password as well

So we'll use this pound sign to comment out the query for tha password entirely so this is the logic.

Our main goal was to comment out the password and with this,its done.



LOG IN

admin'#

●

□ Remember me

Congratulations!

Your flag is: e3d0796d002a446c0e622226f42e9672