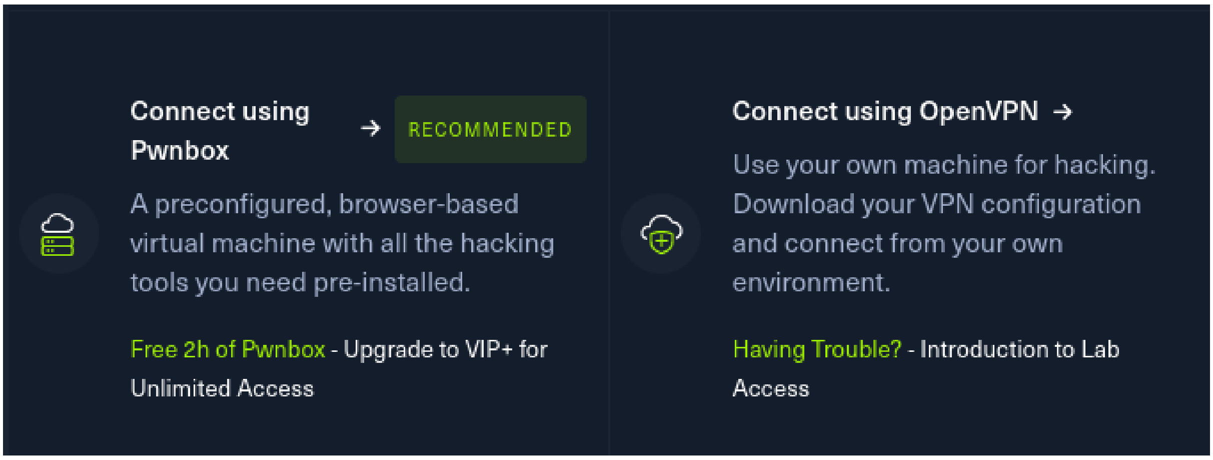
Hack The Box Tier 1 Lab 1 “Appointment” Writeup

Connect To Starting Point VPN:

You must connect yourself to the starting point VPN before answering the question. You can choose one way to connect to the VPN from the following two ways shown below 👇.



Connect using Pwnbox → RECOMMENDED

A preconfigured, browser-based virtual machine with all the hacking tools you need pre-installed.

Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access

Connect using OpenVPN →

Use your own machine for hacking. Download your VPN configuration and connect from your own environment.

Having Trouble? - Introduction to Lab Access

Once you’re connected to the Starting Point VPN now spawn your machine by clicking on the SPAWN MACHINE button shown in the image below 👇 .

SPAWN MACHINE

Spawn the target machine and the IP will show here

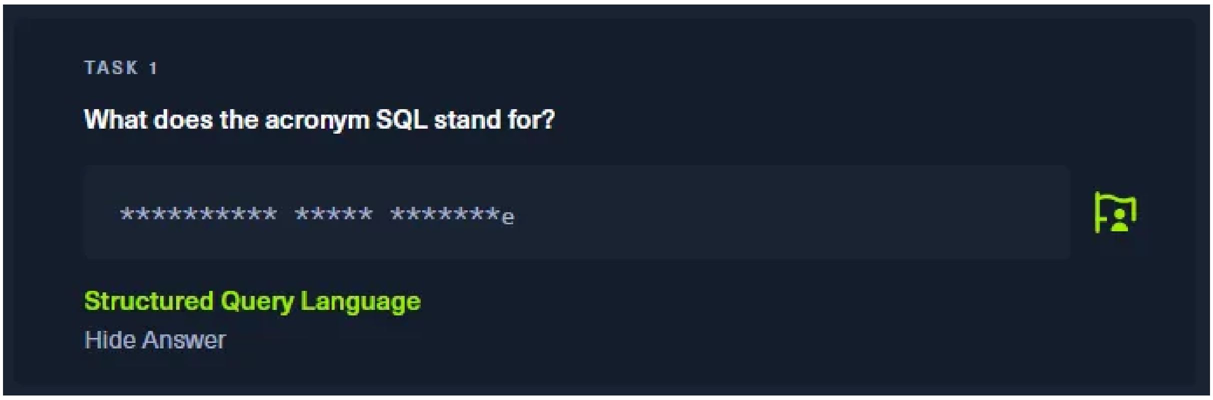
Now Let’s start answering the questions.

Task No 01:

What does the acronym SQL stand for?

Answer:

Structured Query Language



TASK 1

What does the acronym SQL stand for?

********** ***** *******e

Structured Query Language

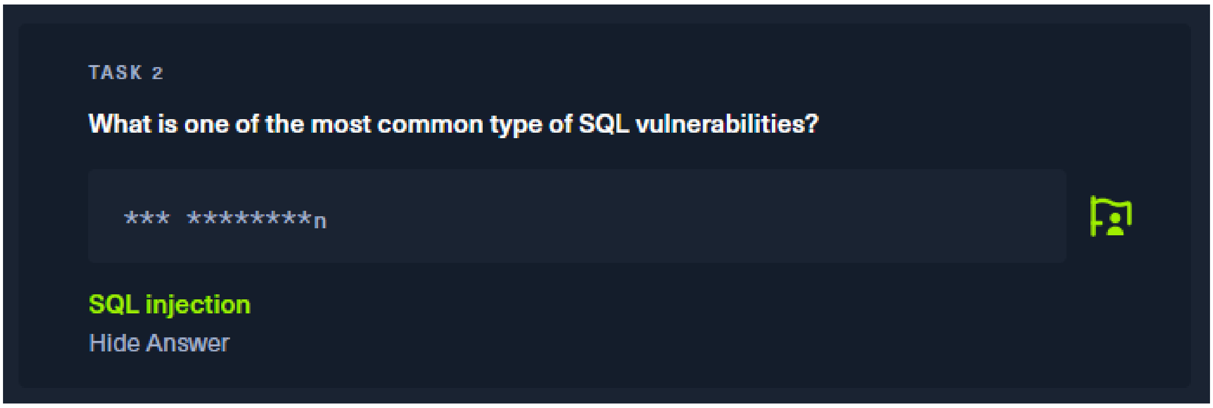
Hide Answer

Task No 02:

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

Answer:

SQL Injection



TASK 2

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

*** ********n

SQL injection

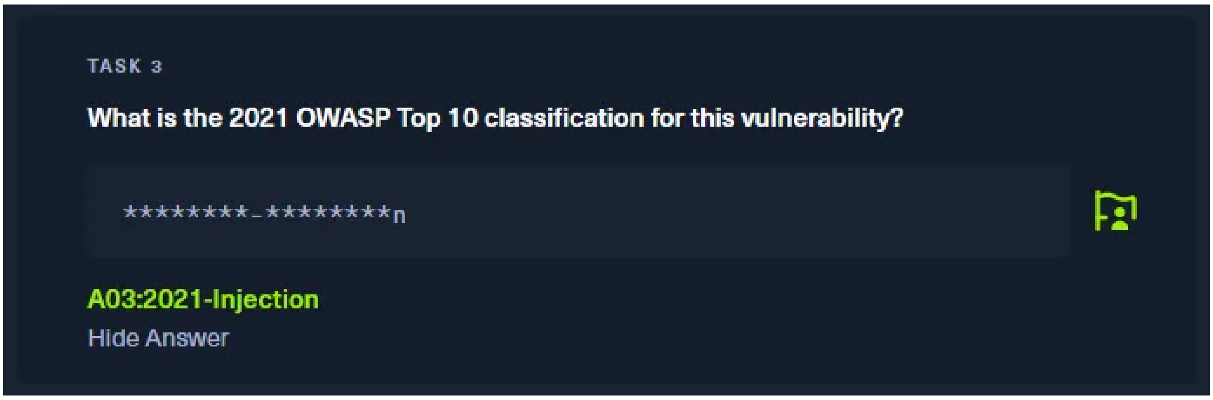
Hide Answer

Task No 03:

What is the 2021 OWASP Top 10 classification for this vulnerability?

Answer:

A03:2021-Injection



TASK 3

What is the 2021 OWASP Top 10 classification for this vulnerability?

********_********n

A03:2021-Injection

Hide Answer

Task No 04:

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

Answer:

Apache httpd 2.4.38 ((Debian))

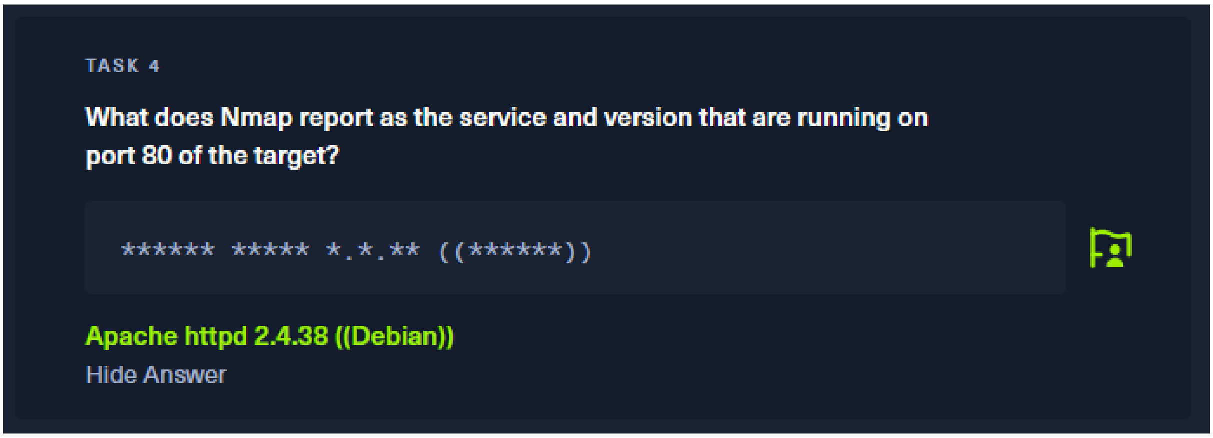
To find out the service and version running on port 80 use the following 👇 command.

```
nmap -sV target-ip -p 80
```

Command Explanation:

Let’s now understand what the above command is doing:

- ***nmap:*** used for scanning
- ***sv:*** used to give details about version used on the target-ip
- ***p:*** used to specify port
- ***80:*** http port



TASK 4

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

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

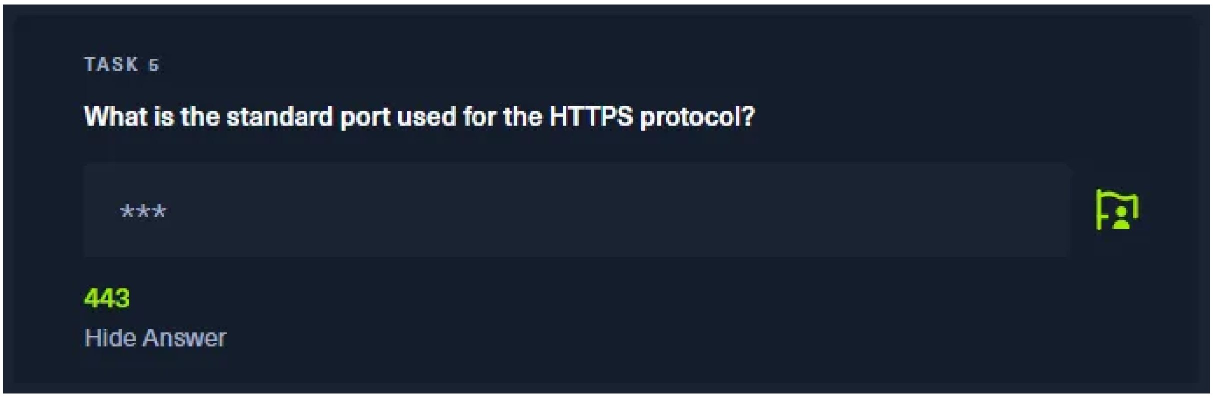
Apache httpd 2.4.38 ((Debian))

Task No 05:

What is the standard port used for the HTTPS protocol?

Answer:

443



TASK 5

What is the standard port used for the HTTPS protocol?

```
***
```

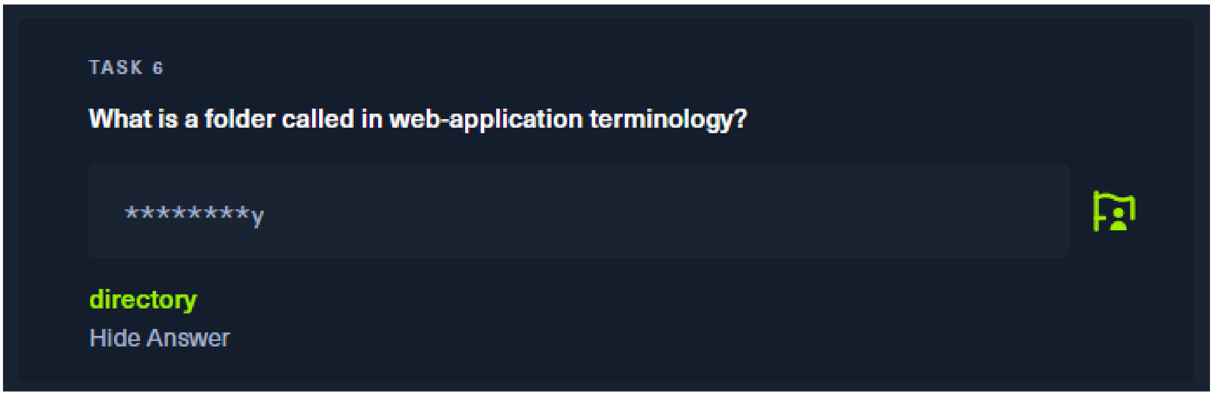
443

Task No 06:

What is a folder called in web-application terminology?

Answer:

Directory



TASK 6

What is a folder called in web-application terminology?

********y

directory

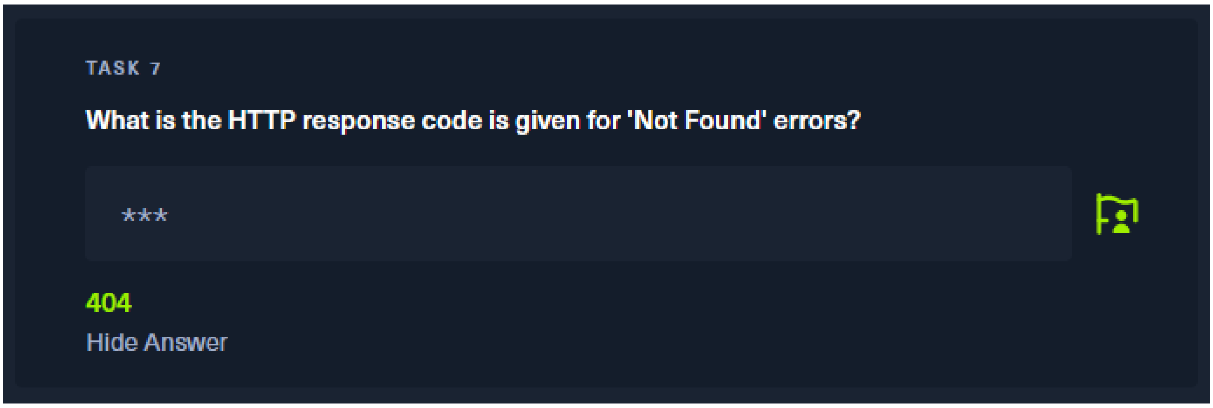
Hide Answer

Task No 07:

What is the HTTP response code is given for ‘Not Found’ errors?

Answer:

404



TASK 7

What is the HTTP response code is given for 'Not Found' errors?

***

404

Hide Answer

Task No 08:

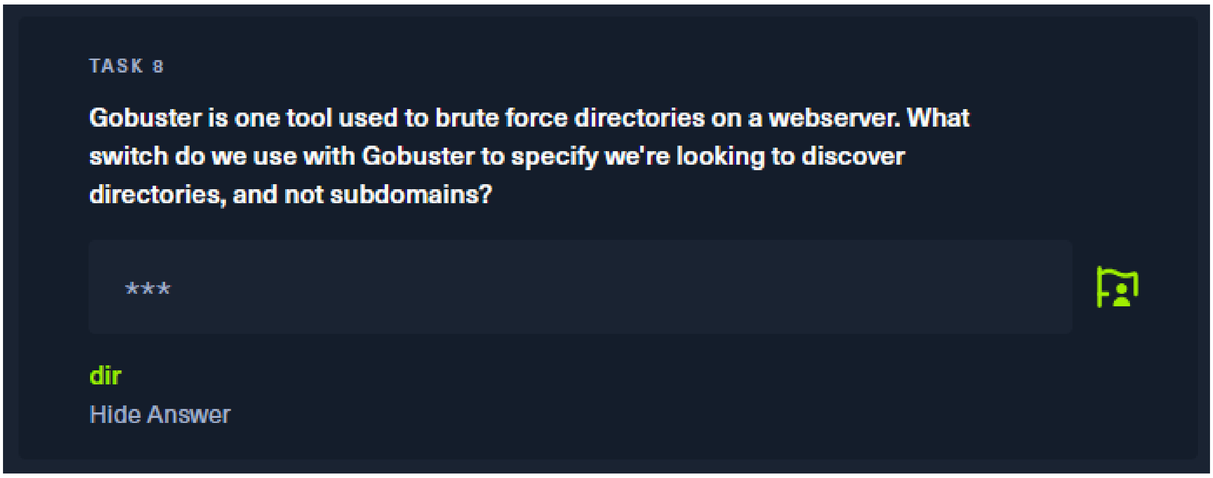
Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we’re looking to discover directories, and not subdomains?

Answer:

dir

Check out the manual page of gobuster using this 👇 command.

```
man gobuster
```



TASK 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?

***

dir

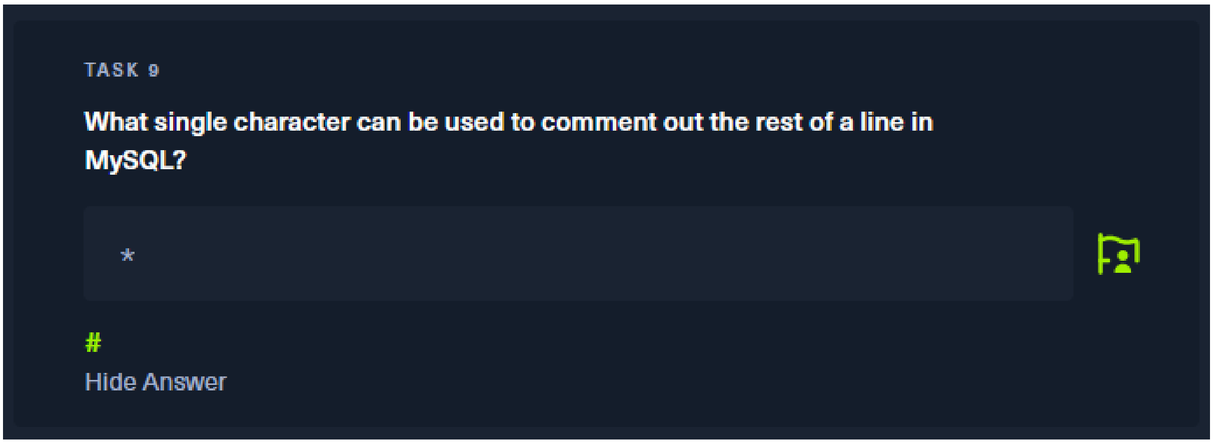
Hide Answer

Task No 09:

What single character can be used to comment out the rest of a line in MySQL?

Answer:

#



TASK 9

What single character can be used to comment out the rest of a line in MySQL?

*

#

Hide Answer

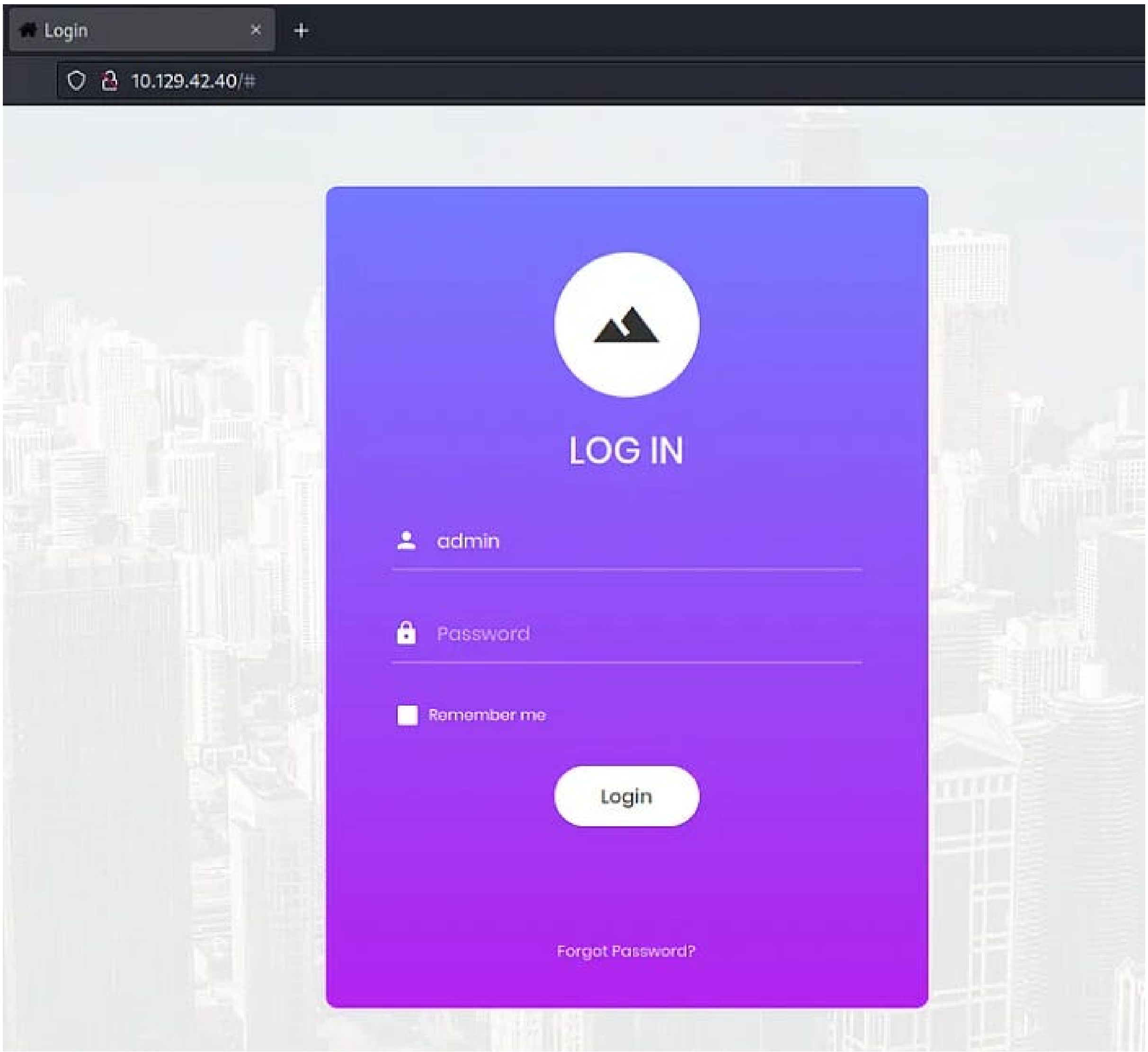
Task No 10:

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?

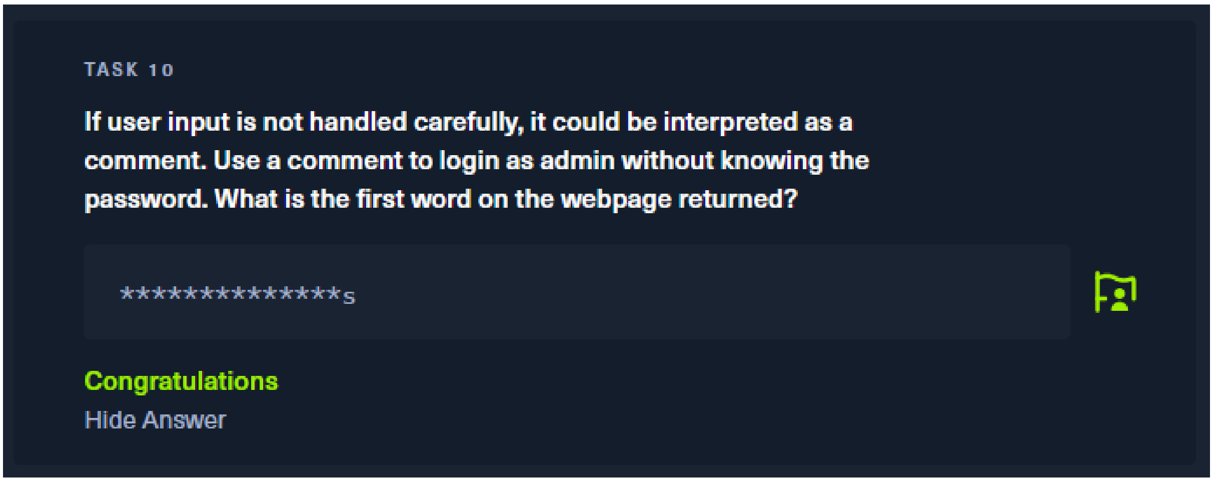
Answer:

Congratulations

To get the answer to task 10 first you would need to access the admin page. You can do it by entering the target-ip into your browser’s search bar. When done you will have a screen like this 👇.



Enter admin# as user and password. You will get the flag and answer to task 10.


TASK 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?

**************s

Congratulations

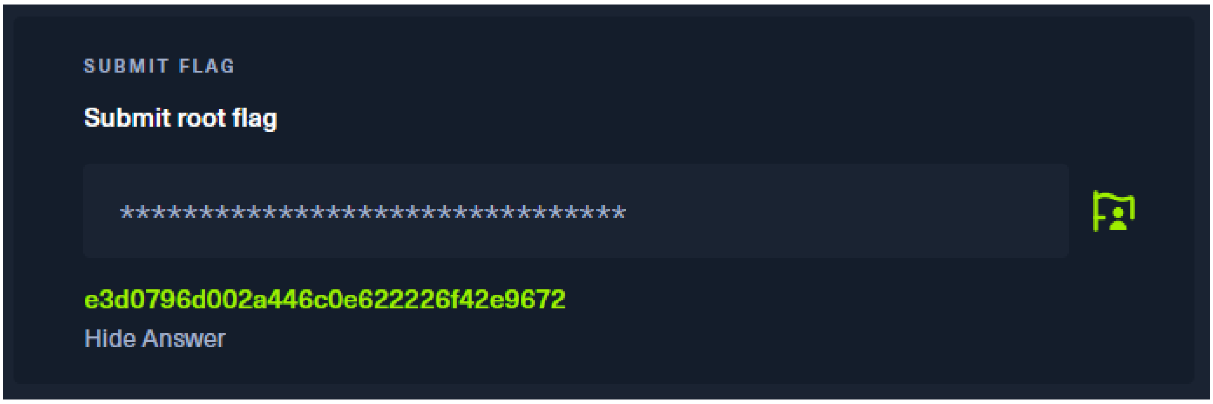
Hide Answer

Task No 11:

Submit root flag

Answer:

e3d0796d002a446c0e622226f42e9672


SUBMIT FLAG

Submit root flag

****

e3d0796d002a446c0e622226f42e9672

Hide Answer

Congratulation 🎉🎊 you've successfully completed your first lab of Tier 1 in hack the box Learning The Basics Of Penetration Testing Module.

Appointment

VERY EASY

Machine Pwned