

```

(root@kali)-[/home/alvadelg]
# nmap -sV -O -sS -A -p- 10.129.72.166 -6=n/a
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 15:32 CET
Nmap scan report for 10.129.72.166
Host is up (0.046s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS
1 43.40 ms 10.10.14.1
2 44.71 ms 10.129.72.166
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 50.55 seconds

```

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

Apache httpd 2.4.38 ((Debian))

What does the acronym SQL stand for?

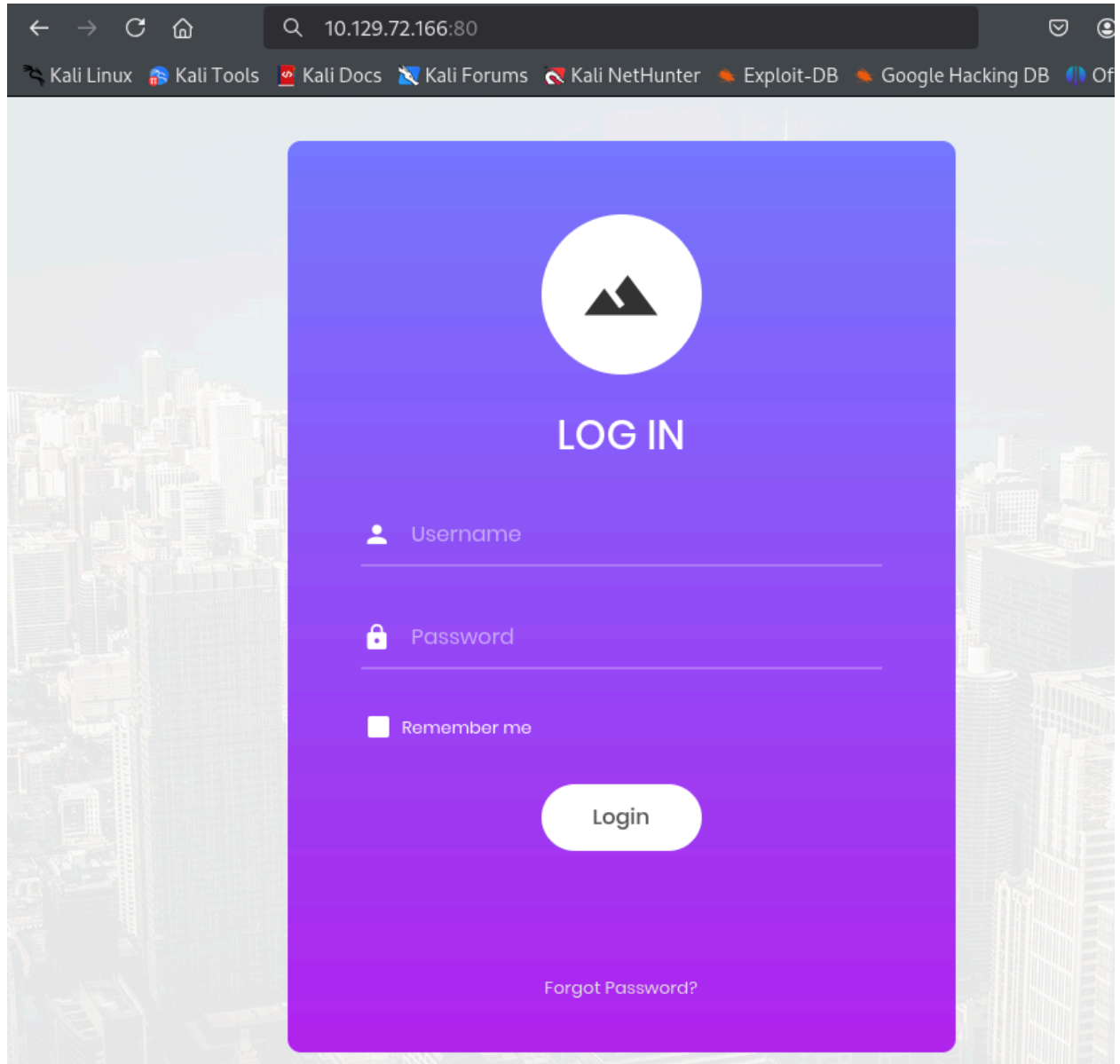
SQL stands for Structured Query Language. It's a standardized programming language used for managing and manipulating relational databases. With SQL, you can create, read, update, and delete data in a database, among other operations.

What is the standard port used for the HTTPS protocol?

The standard port used for the HTTPS protocol is **port 443**. This port is used for secure web traffic, ensuring that the data transmitted between your browser and the web server is encrypted and secure.

What is a folder called in web-application terminology?

Directory



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

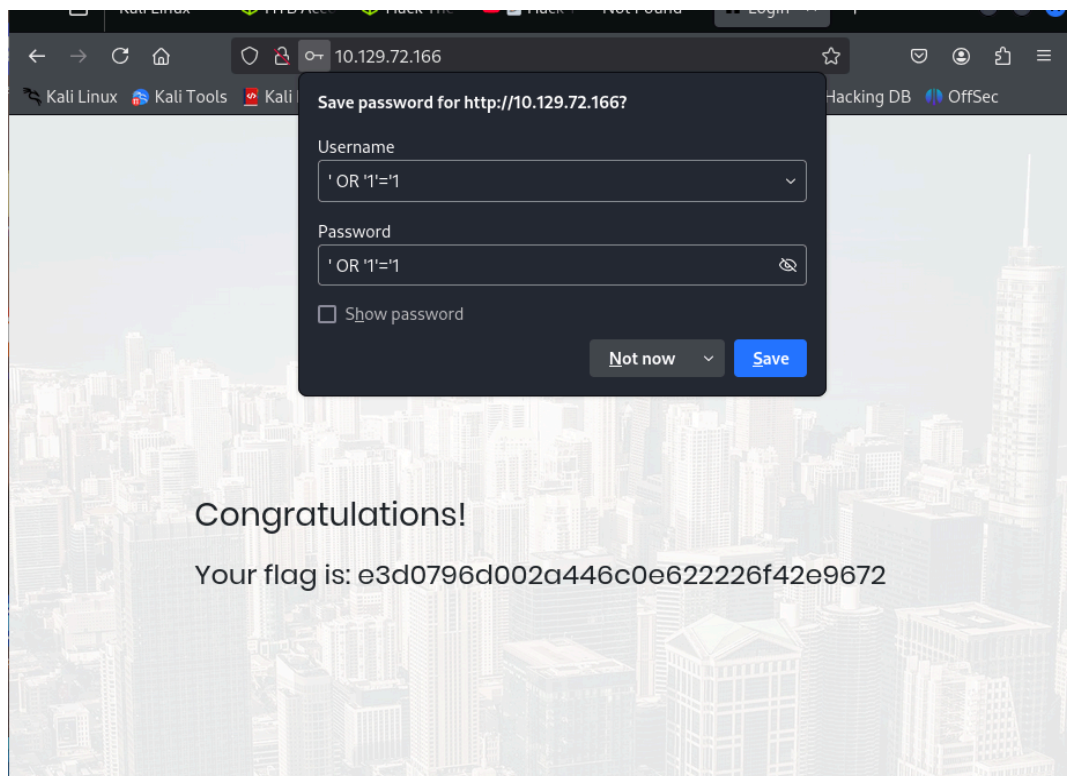
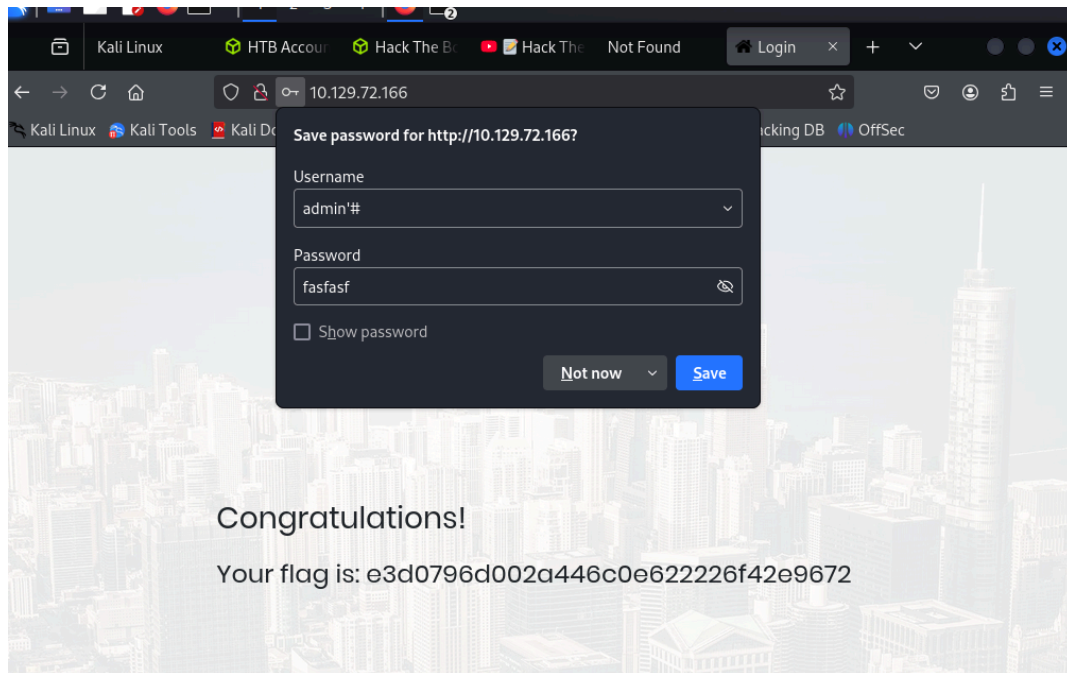
One of the most common types of SQL vulnerabilities is SQL Injection (SQLi). SQL Injection occurs when an attacker inserts or "injects" malicious SQL code into an application's input fields, which can then be executed by the database

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

A03:2021-Injection

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

#



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?

Congratulations