

Preguntas

What does the acronym SQL stand for?

Structured Query Language

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

SQL injection

What does PII stand for?

Personally Identifiable Information

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

A03:2021-Injection

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

Apache httpd 2.4.38 ((Debian))

What is the standard port used for the HTTPS protocol?

443

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

brute-forcing

What is a folder called in web-application terminology?

directory

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

404

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

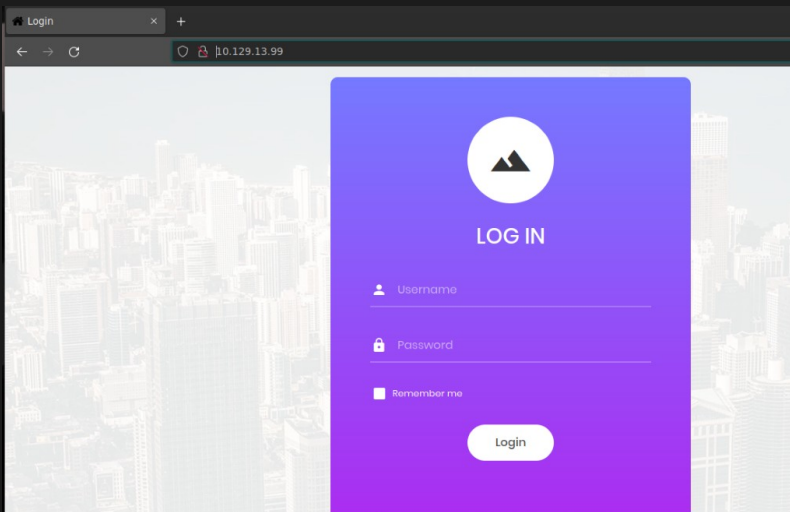
dir

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

#

Proceso

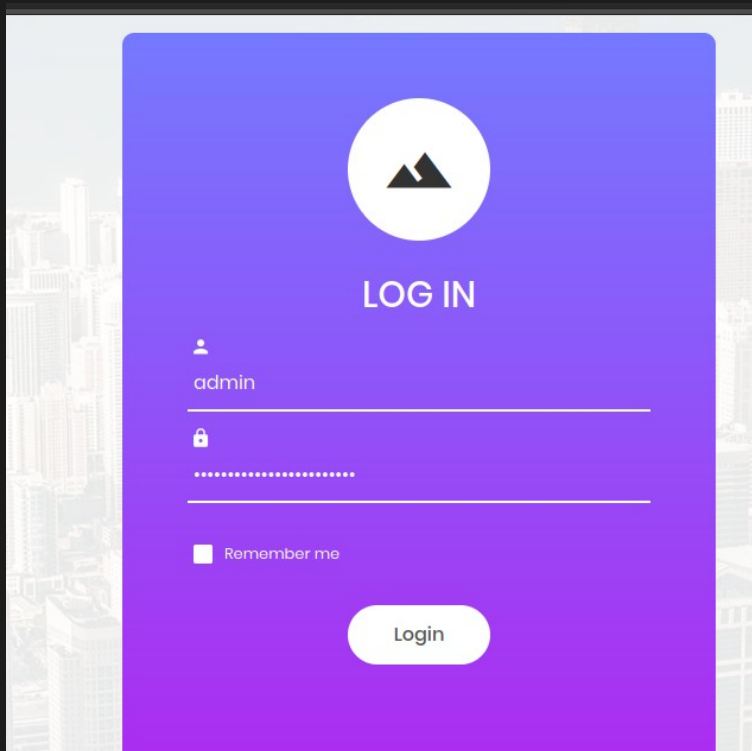
Entrar al sitio web desde el navegador poniendo la ip, aparecerá un login



Tratar de entrar mediante inyección de SQL del siguiente modo

Usuario= admin

Contraseña= wrongpassword' OR '1'='1



Dará acceso mostrando un mensaje con el flag

