

Laboratorio #12

Roberto GonzalezFerrer

Descargamos la herramienta xampp

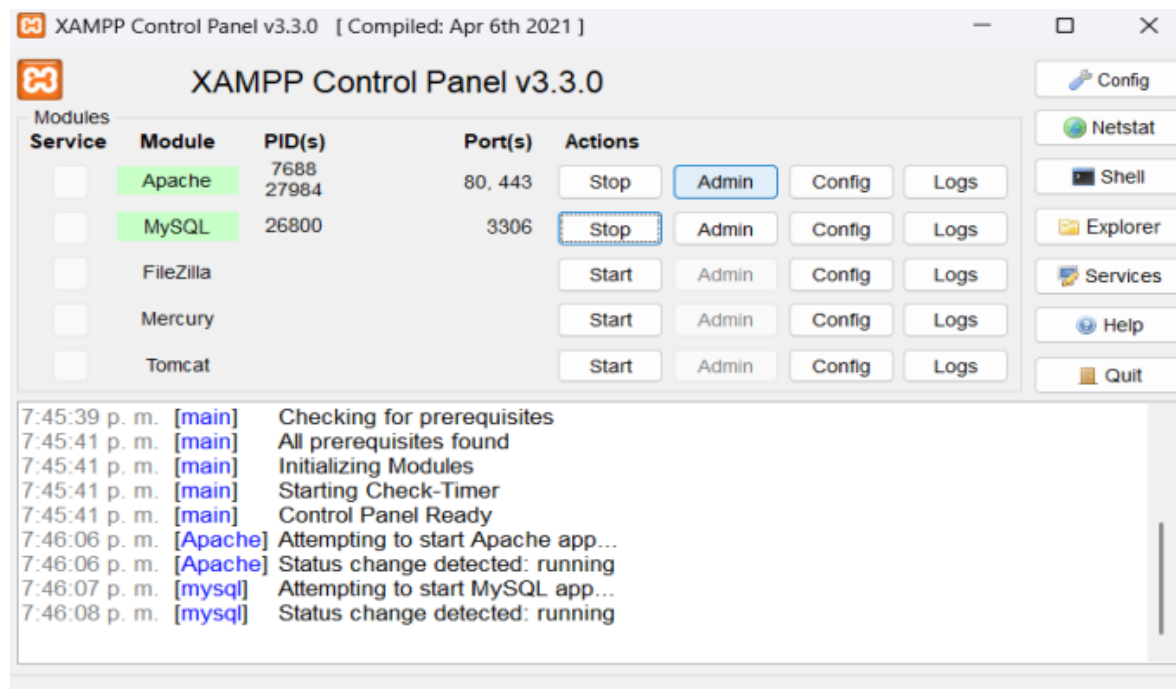


Versión	Suma de comprobación	Tamaño
8.0.30 / PHP 8.0.30	md5 sha1	144 Mb
8.1.25 / PHP 8.1.25	md5 sha1	148 Mb
8.2.12 / PHP 8.2.12	md5 sha1	149 Mb

[Requisitos](#) [Más Descargas »](#)

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#).

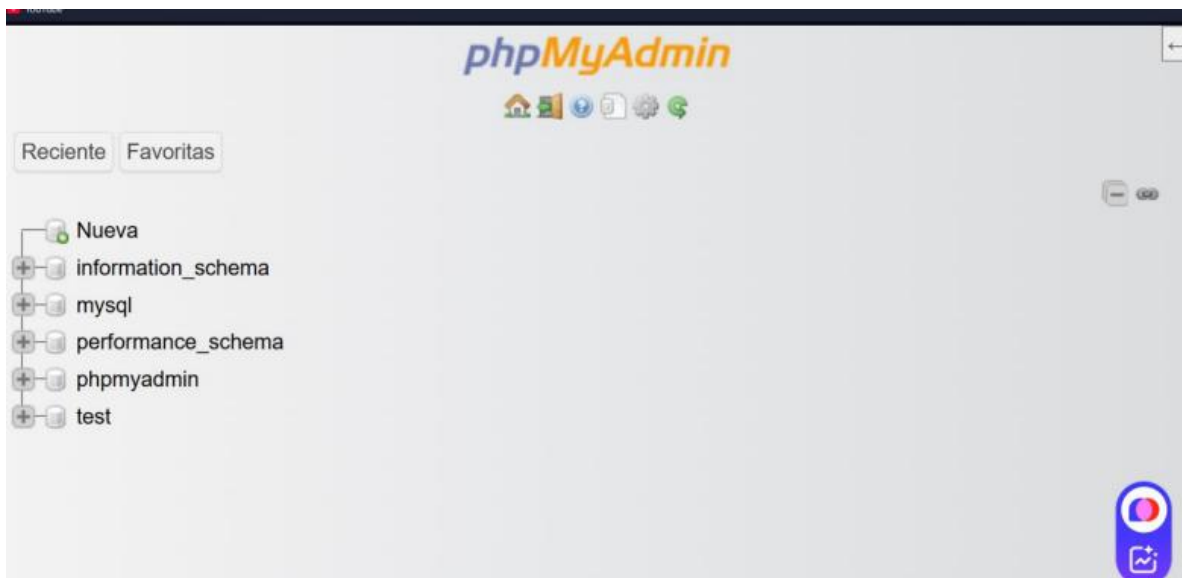
Iniciamos servidor



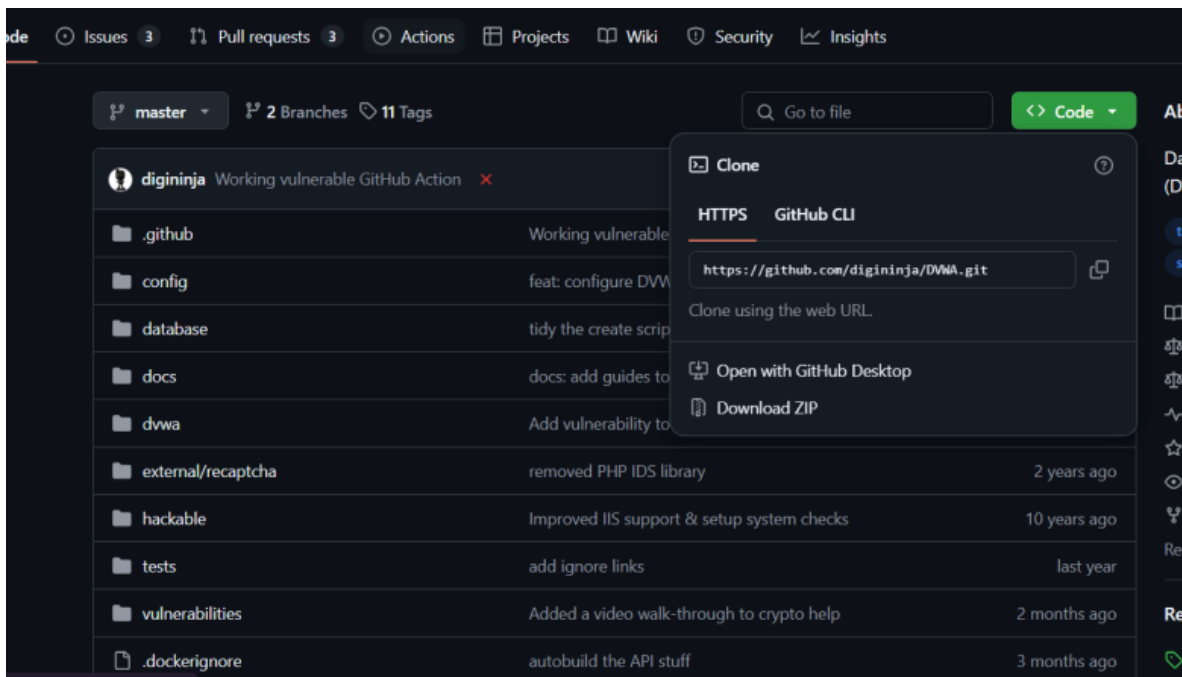
Service	Module	PID(s)	Port(s)	Actions
<input type="checkbox"/>	Apache	7688 27984	80, 443	Stop Admin Config Logs
<input type="checkbox"/>	MySQL	26800	3306	Stop Admin Config Logs
<input type="checkbox"/>	FileZilla			Start Admin Config Logs
<input type="checkbox"/>	Mercury			Start Admin Config Logs
<input type="checkbox"/>	Tomcat			Start Admin Config Logs

7:45:39 p. m. [main] Checking for prerequisites
7:45:41 p. m. [main] All prerequisites found
7:45:41 p. m. [main] Initializing Modules
7:45:41 p. m. [main] Starting Check-Timer
7:45:41 p. m. [main] Control Panel Ready
7:46:06 p. m. [Apache] Attempting to start Apache app...
7:46:06 p. m. [Apache] Status change detected: running
7:46:07 p. m. [mysql] Attempting to start MySQL app...
7:46:08 p. m. [mysql] Status change detected: running

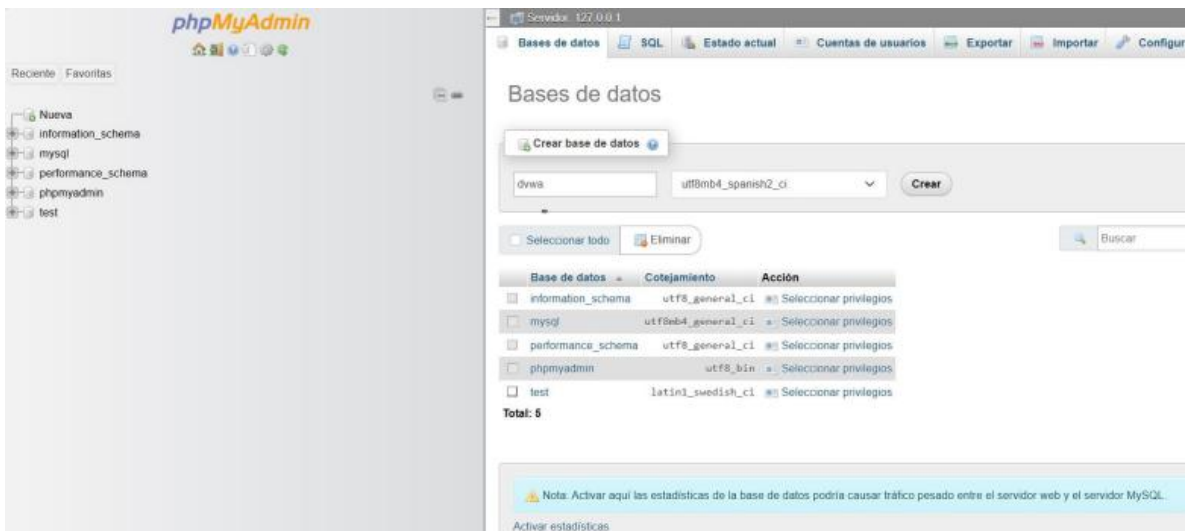
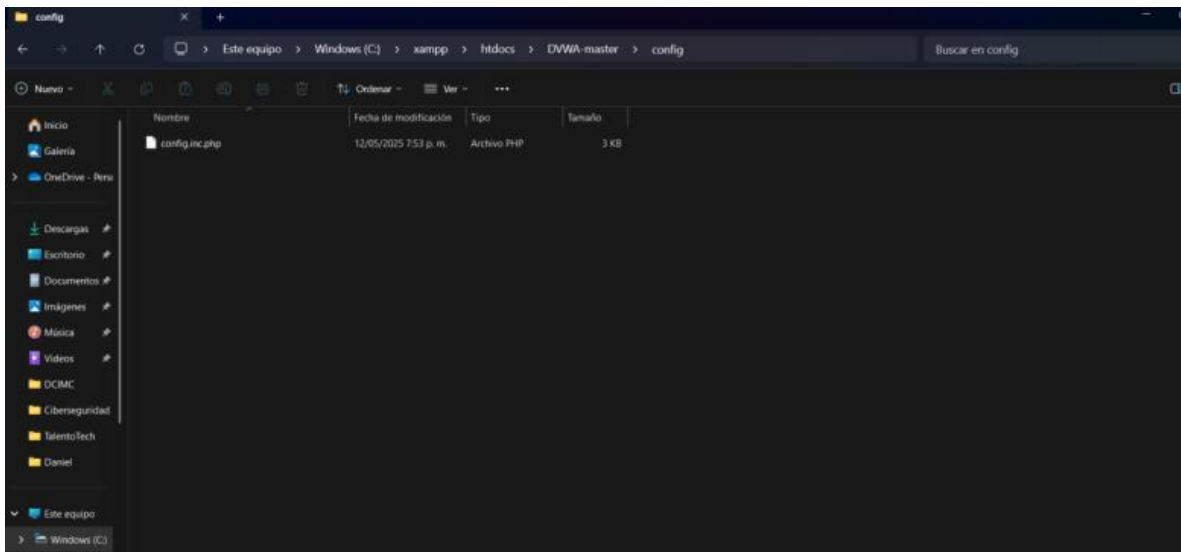
Creamos servidor

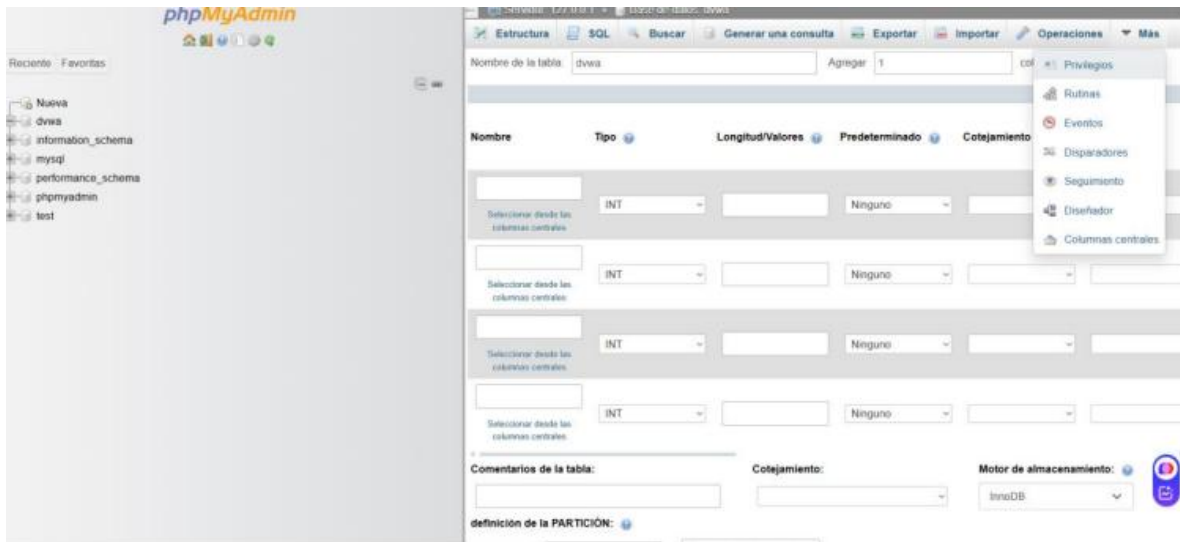


Se instala la herramienta



Configuramos servidor





```
# 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') ? : 'p@ssw0rd';
$_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
# Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = getenv('DISABLE_AUTHENTICATION') ? : false;
```

Agregar cuenta de usuario

Información de la cuenta

Nombre de usuario:	Use el campo de text ▾	<input type="text" value="dvwa"/>
Nombre de Host:	Cualquier servidor ▾	<input type="text" value="%"/> ⓘ
Contraseña:	Use el campo de text ▾	<input type="password" value="*****"/> Fuerza: <div><div></div></div> Débil
Debe volver a escribir:		<input type="password" value="*****"/>
plugin de autenticación		<input type="text" value="Autenticación de MySQL nativo"/> ▾
Generar contraseña:	<input type="button" value="Generar"/>	<input type="text"/>

Base de datos para la cuenta de usuario

- ☐ Crear base de datos con el mismo nombre y otorgar todos los privilegios.
- ☐ Otorgar todos los privilegios al nombre que contiene comodín (username_%).
- ☒ Otorgar todos los privilegios para la base de datos dvwa.

YouTube

phpMyAdmin

usuario Favoritas

Nueva
dvwa
information_schema
mysql
performance_schema
phpmyadmin
test

Servidor: 127.0.0.1

Bases de datos SQL Estado actual Cuentas de usuarios Exportar Importar Más

Base de datos Tabla Rutina Información de la cuenta

Editar los privilegios: Cuenta de usuario 'dvwa'@'%' - Base de datos c

Privilegios específicos para la base de datos ☒ Seleccionar todo

Nota: Los nombres de los privilegios de MySQL están expresados en inglés.

<input checked="" type="checkbox"/> Datos	<input checked="" type="checkbox"/> Estructura	<input checked="" type="checkbox"/> Administración
<input checked="" type="checkbox"/> SELECT	<input checked="" type="checkbox"/> CREATE	<input type="checkbox"/> GRANT
<input checked="" type="checkbox"/> INSERT	<input checked="" type="checkbox"/> ALTER	<input checked="" type="checkbox"/> LOCK TABLES
<input checked="" type="checkbox"/> UPDATE	<input checked="" type="checkbox"/> INDEX	<input checked="" type="checkbox"/> REFERENCES
<input checked="" type="checkbox"/> DELETE	<input checked="" type="checkbox"/> DROP	
	<input checked="" type="checkbox"/> CREATE TEMPORARY TABLES	
	<input checked="" type="checkbox"/> SHOW VIEW	
	<input checked="" type="checkbox"/> CREATE ROUTINE	
	<input checked="" type="checkbox"/> ALTER ROUTINE	
	<input checked="" type="checkbox"/> EXECUTE	
	<input checked="" type="checkbox"/> CREATE VIEW	
	<input checked="" type="checkbox"/> EVENT	
	<input checked="" type="checkbox"/> TRIGGER	

Usuario "ADMIN", contraseña PASSWORD



Username

Password

PHP function display_errors: **Enabled**
PHP function display_startup_errors: **Enabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

Database
Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: *********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

API
This section is only important if you want to use the API module.
Vendor files installed: **Not installed**

For information on how to install these, see the [README](#).

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

First time using DVWA.
Need to run 'setup.php'.

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
First name: admin
Surname: admin

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/>

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
First name: admin
Surname: admin

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/>

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

DVWA Security

DVWA

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

Desencriptamos la clave incryptada

Encrypter

Decrypter

Md5 Hash

5f4dcc3b5aa765d61d8327deb882cf99

>>

Text

password

Elapsed Time: 0.312s

Trial Count: 4