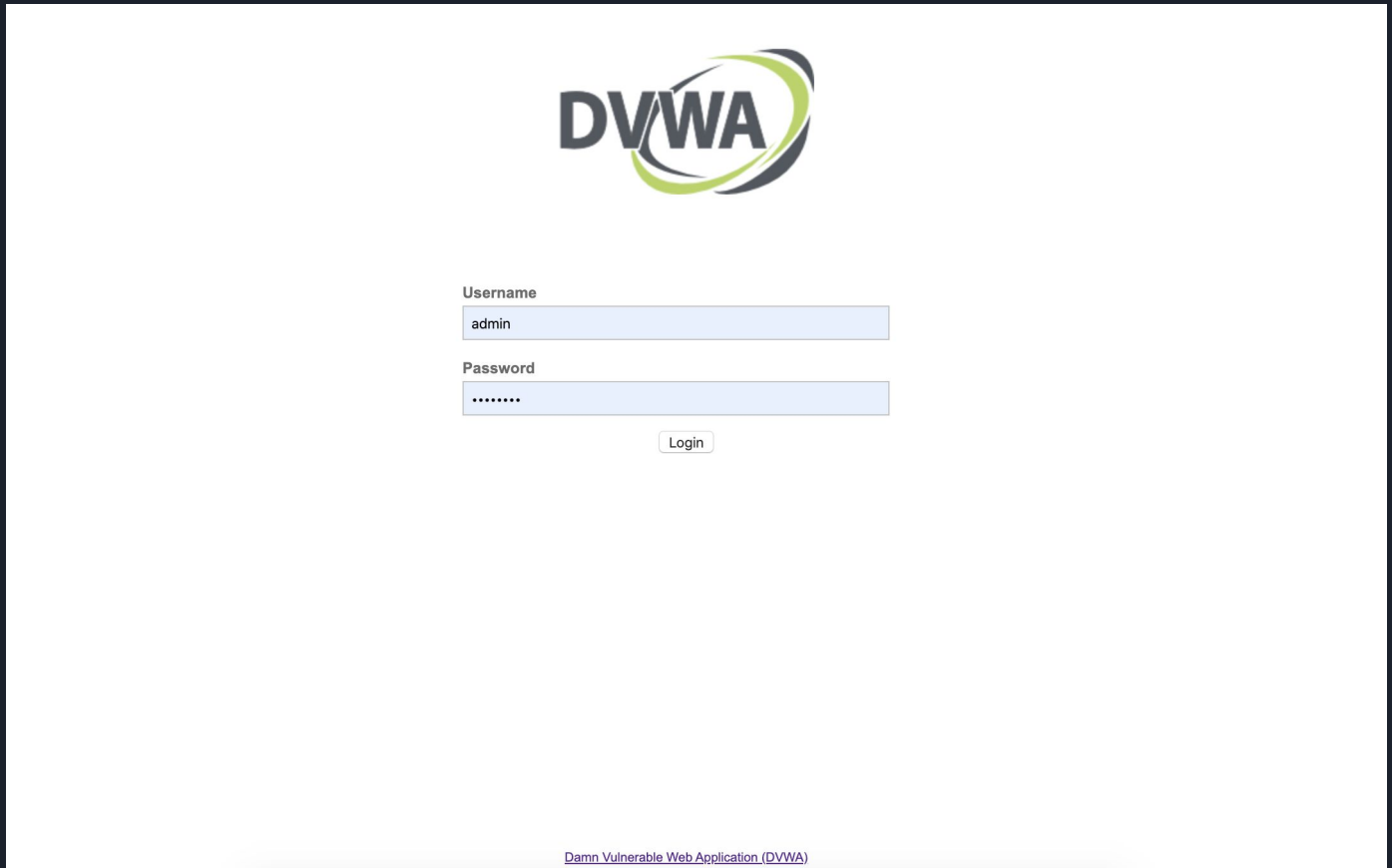
Damn Vulnerable Web App

Conocer y explotar vulnerabilidades web.

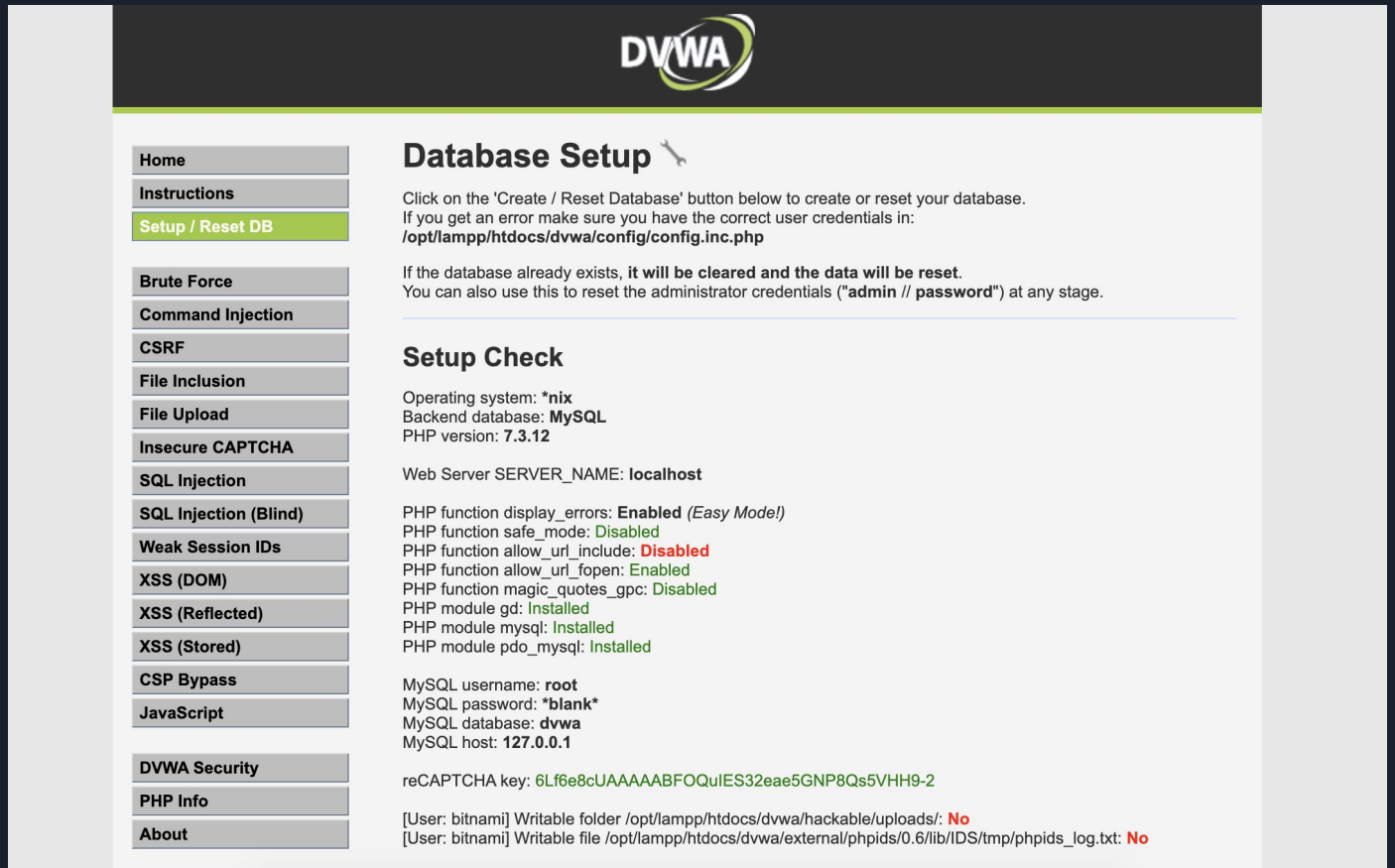
¿Qué es la DVWA? ¿Para qué sirve?

- Aplicación web vulnerable programada en PHP/MYSQL.
- Programación vulnerable para realizar pruebas de seguridad en un entorno legal.
- Entorno de entrenamiento en explotación de seguridad web.
- Distintos niveles de seguridad.

Log in


DVWA
Username
admin
Password
••••••••
Login
Damn Vulnerable Web Application (DVWA)

Set Up


DVWA
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
DVWA Security
PHP Info
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:
/opt/lampp/htdocs/dvwa/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
Operating system: *nix
Backend database: MySQL
PHP version: 7.3.12
Web Server SERVER_NAME: localhost
PHP function display_errors: Enabled (Easy Mode!)
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: root
MySQL password: *blank*
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: 6Lf6e8cUAAAAABFOQuIES32eae5GNP8Qs5VHH9-2
[User: bitnami] Writable folder /opt/lampp/htdocs/dvwa/hackable/uploads/: No
[User: bitnami] Writable file /opt/lampp/htdocs/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: No

Niveles de seguridad

Cada vulnerabilidad tiene cuatro niveles de seguridad diferentes, bajo, medio, alto e imposible. Los niveles de seguridad suponen un desafío para el “atacante” y también muestra cómo cada vulnerabilidad puede medirse mediante una programación segura.

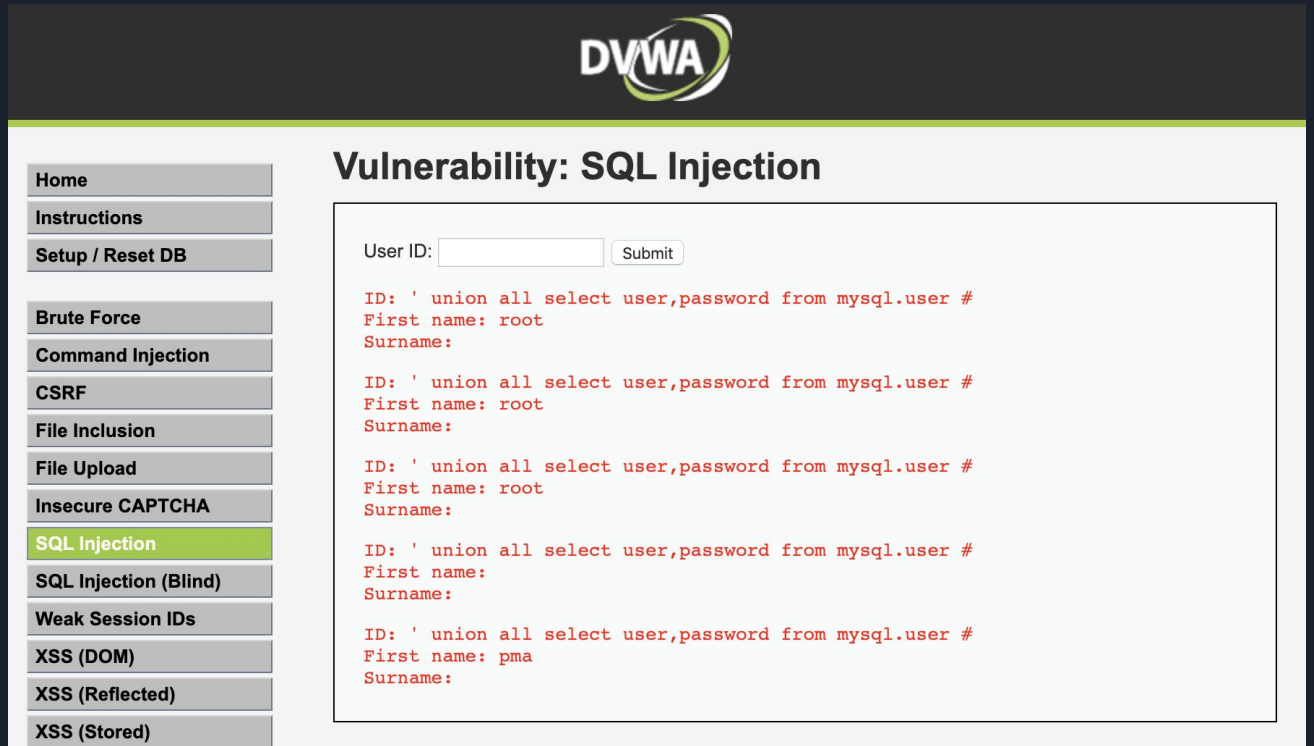
- Bajo: *este nivel de seguridad está destinado a simular un sitio web sin ningún tipo de seguridad implementada en su programación.*
- Medio: *el propósito de este nivel de seguridad es dar al ‘atacante’ un desafío en la explotación y también servir como un ejemplo de malas prácticas de programación/seguridad.*
- Alto: *Este nivel de vulnerabilidad brinda al usuario un ejemplo de cómo proteger la vulnerabilidad a través de métodos de programación seguros. Permite al usuario comprender cómo se puede medir la vulnerabilidad.*
- Imposible: *Este nivel da dificultades que enfrentamos en el mundo real.*

Vulnerabilidades

- Fuerza bruta.
- Inyección de comando.
- CSRF.
- Carga de archivos.
- Captcha inseguro.
- Inyección SQL / Blind.
- ID de sesión débil.
- XSS (DOM/Reflected/Stored).

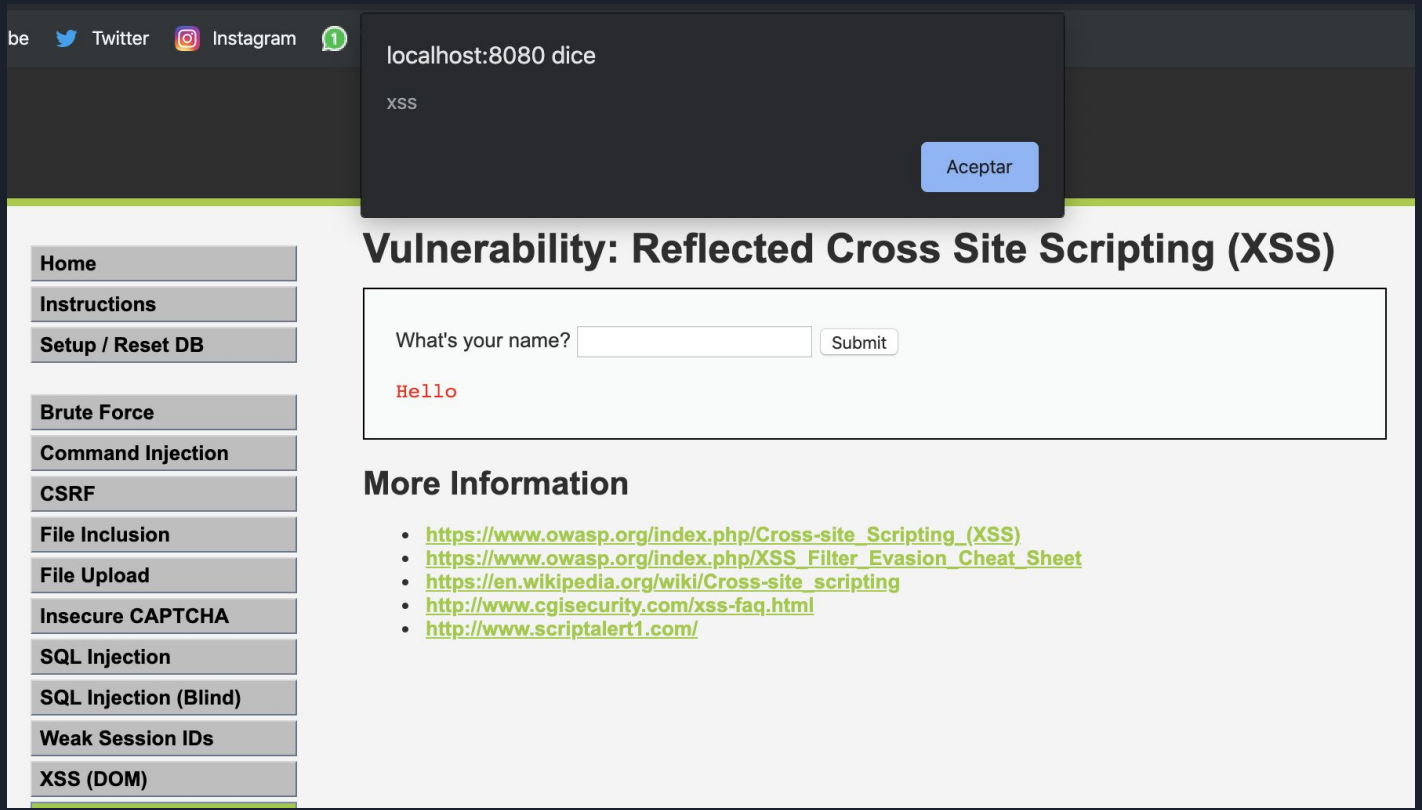
Inyección SQL

Usuarios del servicio:
>> ' union all select user,password from mysql.user #



XSS Reflected

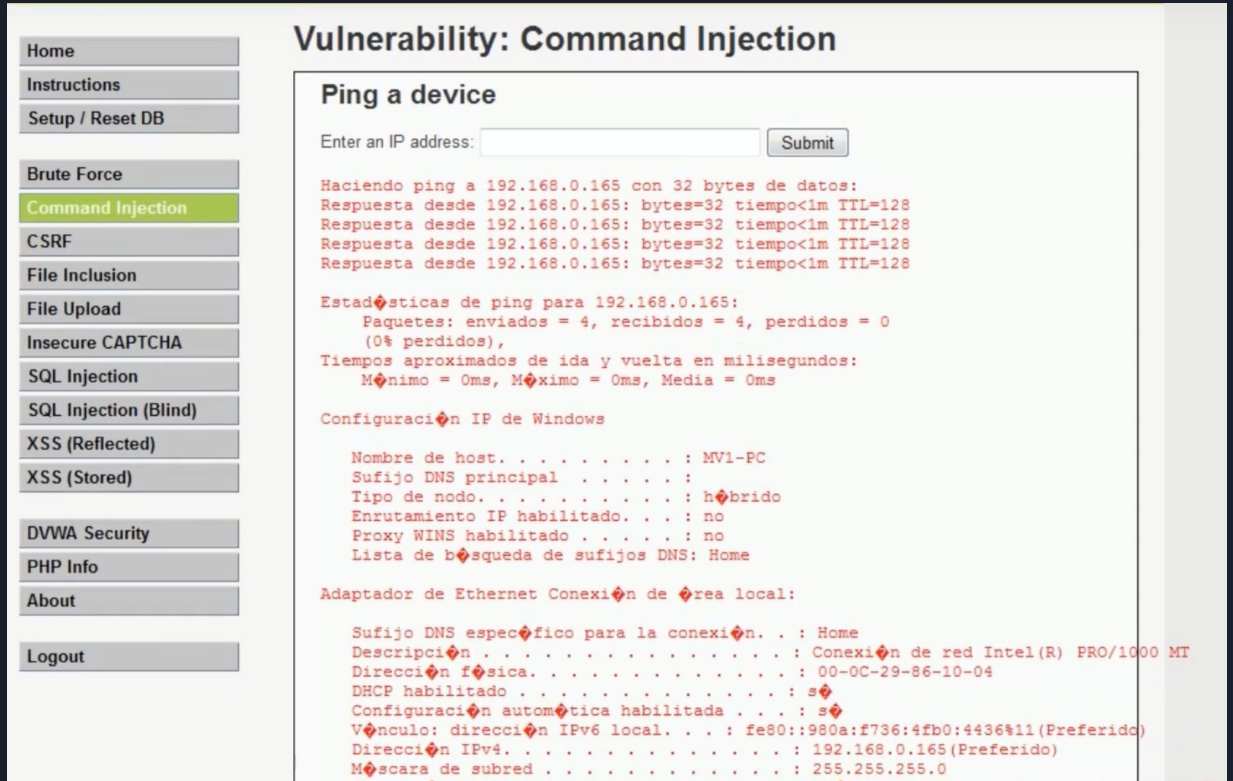
>> <script>alert("xss")</script>



Inyección de comando

Obtener la configuración de la red:

>> Número de IP && ipconfig /all



¿Cuáles son los beneficios de usar DVWA?

- Ayuda a comprender mejor los procesos de seguridad en el desarrollo de aplicaciones web.
- Sencillo de instalar.
- Entorno legal.
- Permite determinar su dificultad y así mejorar habilidades.
- Apps similares: bWAPP, Mutillidae, Metasploitable.