

**Karolina Gucko, 20/10/2024**

## **Informe de Gestión de Incidentes según ISO 27001 - Vulnerabilidad de Inyección SQL**

**Introducción:** Este informe describe la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA), que fue configurada con un nivel de seguridad bajo (Low). La vulnerabilidad fue detectada en el módulo "SQL Injection", y la prueba se realizó en un entorno controlado, con el objetivo de demostrar cómo identificar y reportar este tipo de vulnerabilidad.

**Descripción del incidente:** Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL en el campo "User ID". Esta vulnerabilidad permitió la ejecución de una consulta SQL maliciosa que comprometió la confidencialidad de los datos almacenados en la base de datos.

**Método de inyección SQL utilizado:** El payload utilizado para la explotación de la vulnerabilidad fue el siguiente:

ID: **1' OR '1'='1**


Este comando permitió obtener información sensible, mostrando en pantalla los registros almacenados en la base de datos, incluyendo los nombres y apellidos de varios usuarios. El comando logró engañar al sistema al hacer que siempre se cumpla la condición de la consulta SQL, devolviendo todos los registros existentes.

**Impacto del incidente:** La explotación de esta vulnerabilidad tuvo los siguientes impactos potenciales:

- Acceso no autorizado a la base de datos, revelando información confidencial de los usuarios.
- Posible modificación o eliminación de datos sensibles.
- Compromiso de la integridad y disponibilidad de los datos de la aplicación.

**Usuarios afectados:** La explotación del ataque reveló información de los siguientes usuarios:

- **admin:** Nombre y apellido: admin
- **Gordon Brown:** Nombre: Gordon, Apellido: Brown
- **Hack Me:** Nombre: Hack, Apellido: Me
- **Pablo Picasso:** Nombre: Pablo, Apellido: Picasso
- **Bob Smith:** Nombre: Bob, Apellido: Smith



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

DVWA Security

PHP Info

About

## Vulnerability: SQL Injection

User ID:

Submit

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://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://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

### Medidas correctivas recomendadas:

- Validación de entradas:** Se recomienda implementar validaciones estrictas en los campos de entrada para prevenir inyecciones SQL. Utilizar consultas preparadas o parámetros para garantizar la seguridad de las consultas SQL.
- Auditorías de seguridad regulares:** Realizar pruebas de penetración y auditorías de seguridad periódicas para identificar posibles vulnerabilidades antes de que sean explotadas.
- Capacitación en seguridad:** Capacitar al personal de desarrollo en las mejores prácticas de seguridad web, enfocándose en cómo prevenir ataques de inyección SQL y otros tipos de vulnerabilidades.

**Conclusión:** La identificación y explotación de la vulnerabilidad de inyección SQL en DVWA demuestra los riesgos que este tipo de vulnerabilidad representa para las aplicaciones web. Se debe priorizar la implementación de controles de seguridad sólidos, especialmente en lo que respecta a la validación de entradas y auditorías regulares de seguridad, para proteger los sistemas y la información sensible.