

# Reporte de Incidente de Seguridad - Inyección SQL en DVWA

## 1. Introducción

Este reporte documenta una vulnerabilidad de inyección SQL identificada en la aplicación Damn Vulnerable Web Application (DVWA).

El incidente se analiza conforme a las normas ISO 27001 para la gestión de incidentes de seguridad de la información.

## 2. Descripción del Incidente

La inyección SQL es una vulnerabilidad que permite a un atacante manipular consultas SQL de una aplicación para acceder o modificar datos no autorizados en una base de datos. En este caso, se detectó una falla en el módulo "SQL Injection" de DVWA, permitiendo extraer información de usuarios mediante una consulta maliciosa.

## 3. Procedimiento de Explotación

### 3.1. Entorno de Pruebas

- Sistema Operativo: Debian en VirtualBox
- Servidor Web: Apache 2
- Base de Datos: MariaDB
- Aplicación: DVWA (Damn Vulnerable Web Application)

### 3.2. Pasos para Reproducir la Inyección SQL

1. Acceder a DVWA a través de <http://192.168.1.116/DVWA>
2. Iniciar sesión con:
  - Usuario: admin
  - Contraseña: password

3. Navegar a "Vulnerability > SQL Injection".

4. Ingresar la siguiente consulta en el campo de entrada:

1' OR '1'='1

5. Presionar "Submit".

6. El servidor devuelve una lista de todos los usuarios almacenados en la base de datos, indicando que la inyección fue exitosa.

#### 4. Impacto del Incidente

Esta vulnerabilidad podría permitir a un atacante:

- Obtener información confidencial de usuarios.
- Modificar datos en la base de datos.
- Eliminar registros de manera maliciosa.
- Obtener acceso privilegiado al sistema.



#### 5. Recomendaciones y Mitigaciones

Para evitar este tipo de ataques, se recomienda:

- Usar consultas parametrizadas en SQL en lugar de concatenación de strings.
- Validar y sanitizar todas las entradas del usuario.
- Aplicar el principio de menor privilegio en la base de datos.
- Actualizar y parchar regularmente el software y la base de datos.

#### 6. Conclusión

Se ha identificado y explotado una vulnerabilidad de inyección SQL en DVWA, demostrando el impacto que este tipo de fallas puede tener

en la seguridad de la información. Se recomienda implementar las medidas de mitigación mencionadas para proteger la integridad de la base de datos y la confidencialidad de los usuarios.

---

#### Anexo: Captura de Pantalla

(Si es requerido, se pueden adjuntar más imágenes que muestren la explotación de la vulnerabilidad).