# Informe de Incidente de Seguridad: Vulnerabilidad de Inyección SQL en DVWA

## Introducción

Este informe documenta la identificación, reproducción y análisis de una vulnerabilidad de inyección SQL en la plataforma DVWA (Damn Vulnerable Web Application). El ejercicio se realizó en un entorno controlado con una máquina virtual Linux (Debian) en VirtualBox, con el objetivo de aprender a detectar y reportar este tipo de vulnerabilidad siguiendo las políticas de seguridad de la información según la norma ISO 27001. El propósito final es comprender los riesgos, la metodología de explotación y presentar recomendaciones para mitigar y gestionar incidentes similares en entornos reales.

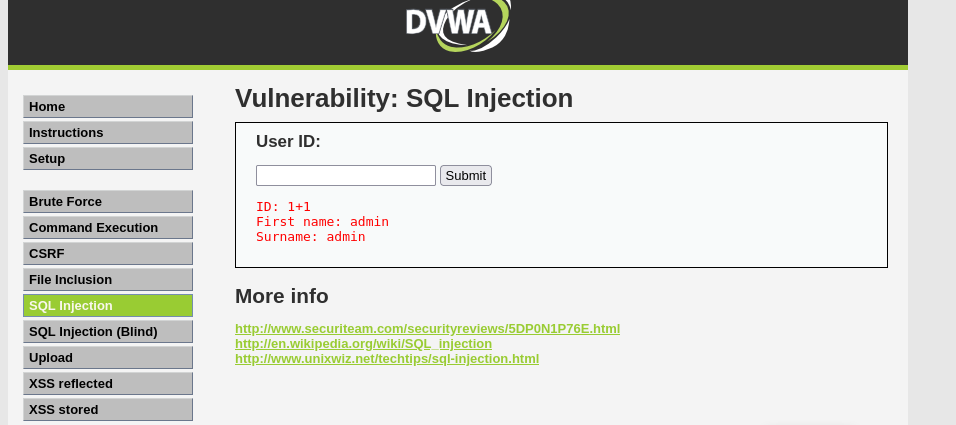
## Descripción del Incidente

Se detectó que la aplicación web DVWA presenta una vulnerabilidad de inyección SQL en su sección de "SQL Injection", lo que permite a un atacante ejecutar comandos SQL arbitrarios en la base de datos subyacente, comprometiendo la confidencialidad de los datos y pudiendo escalar la vulnerabilidad para obtener privilegios en el sistema o manipular la información.

## Impacto del Incidente

La vulnerabilidad de inyección SQL permite a un atacante:

* Acceder y modificar información confidencial almacenada en la base de datos.
* Realizar consultas no autorizadas y extraer datos personales.
* Posible escalada para obtener control total sobre la base de datos.
* Vulnerabilidad potencial a ataques futuros de mayor gravedad, afectando la confidencialidad, integridad y disponibilidad del sistema.

Este incidente, en un entorno real, representaría un riesgo alto de pérdida de datos, incumplimiento legal, y daño a la reputación de la organización.

Recomendaciones

### Medidas inmediatas

* **Aplicar validación y sanitización de entradas en todas las entradas de usuario**.
* **Utilizar consultas parametrizadas (prepared statements)** en la codificación.
* **Aumentar el nivel de seguridad en DVWA y entornos reales**, configurando filtro y control adicional.

### Políticas y gestión

* **Implementar auditorías periódicas en las aplicaciones web** para detectar vulnerabilidades.