# PROYECTO 2026/02/20 - INFORME VULNERABILIDAD INYECCIÓN SQL - CONFORME A LA NORMA ISO 27001

En este informe trataremos la inyección y explotación de una vulnerabilidad de inyección SQL. Se realiza mediante la aplicación DVWA (Damn Vulnerable Web Application) que será el sistema afectado. El proyecto se llevó a cabo en Virtualbox en Linux en este caso en distribución Debian, un entorno de pruebas.

**Descripción del incidente:** Durante la revisión del ejercicio realizado se descubrió una vulnerabilidad, en este caso una inyección SQL en DVWA. Este ataque consiste en que un atacante introduce código SQL malicioso en un formulario o URL para que la base de datos ejecute algo que no estaba previsto. En resumen, un engaño a la BBDD para que ejecute y saque toda la información.

**Método utilizado para la explotación:** En el campo USER ID se utilizó la siguiente carga para replicar y demostrar la vulnerabilidad.

```
1' OR '1'='1
```

La BBDD lo representa como SELECT * FROM users WHERE id = '1' OR '1'='1'; y '1'='1' es siempre verdadero, por lo que la consulta devuelve todos los registros, no solo el que corresponde.

### Impacto del incidente:

Los riesgos afectan principalmente a la confidencialidad, integridad y disponibilidad. Datos sensibles expuestos, filtración de datos personales, modificación de BBDD, alterar resultados e incluso corromper la disponibilidad de la BBDD, aparte de un impacto a la organización a nivel de daños de reputación y costos adicionales para la recuperación de esos datos.

### Recomendaciones:

- Validación y filtrado de entradas
- Privilegios mínimos
- Consultas parametrizadas
- Monitorización y registros
- Configuración de seguridad y actualizaciones de la aplicación
- Capacitación a los usuarios a nivel de seguridad

### Conclusiones:

El proyecto nos permitió comprender cómo funciona un ataque SQL Injection y su impacto en la seguridad de la información.

Es muy importante  implementar controles de seguridad desde el principio y mantener procesos de gestión de incidentes alineados con ISO 27001 para proteger la confidencialidad, integridad y disponibilidad de los datos.