

Título del Reporte

Informe de incidente — Inyección SQL en DVWA

Introducción

Durante esta práctica se usó la aplicación **DVWA** en una máquina virtual Debian para aprender cómo funciona una **inyección SQL** y cómo se debe reportar según la norma **ISO 27001**.

El objetivo fue identificar una vulnerabilidad y documentar el proceso de forma sencilla, tal como se haría en un entorno real.

Descripción del Incidente

En el módulo *SQL Injection* de DVWA, el campo *User ID* no valida lo que se escribe. Al introducir una cadena manipulada, la aplicación devuelve todos los usuarios de la base de datos, lo que demuestra que es vulnerable a ataques de inyección SQL.

Proceso de Reproducción

1. Entré a <http://localhost/DVWA> con usuario **admin** y contraseña **password**.
2. En la pestaña *DVWA Security*, seleccioné **Low**.

En *SQL Injection*, escribí:

`1' OR '1'='1`

- 3.
 4. Al enviar, aparecieron todos los registros de usuarios, confirmando la vulnerabilidad.
 [Aregar captura con el resultado]
-

Impacto del Incidente

Si esta vulnerabilidad existiera en una web real, alguien podría ver, cambiar o borrar datos importantes de la base de datos.

Afecta sobre todo la **confidencialidad** y la **integridad** de la información.

Recomendaciones

- Usar **consultas preparadas** en lugar de concatenar texto.
 - Validar los datos que introduce el usuario.
 - No usar el usuario **root** de la base de datos.
 - Realizar pruebas de seguridad periódicas.
-

Conclusión

Esta práctica demuestra lo fácil que puede ser explotar una app sin medidas básicas de seguridad.

Aprendí la importancia de validar entradas y proteger la base de datos, ya que una inyección SQL puede poner en riesgo toda la información del sistema.