PROYECTO

“Instalación de DVWA en una Máquina Virtual para Prácticas de Inyección SQL“

Alumno: Miguel A. Acosta DNI 77478992L
Curso: Ciberseguridad
Instructor: Sergio D. Ballen
Ciudad: Madrid
Fecha: 20 de Diciembre 2025

Reporte de Incidente de Seguridad. Norma ISO 27001 SQL Injection vulnerability

Introducción

En este reporte se documenta la explotación como la identificación realizada con fines académicos de las vulnerabilidades de inyección SQL en una web.

Este análisis cumple con los principios de la norma ISO 27001, en lo relativo a la protección de los activos de información.

Método Utilizado

La inyección SQL es una de las vulnerabilidades más críticas en aplicaciones web, ya que permite a un atacante manipular consultas a la base de datos, comprometiendo información sensible y la integridad del sistema.

Durante la interacción con el módulo SQL Injection, se observó que la aplicación arroja como datos los nombres de usuarios y contraseñas.

Como consecuencia, una entrada manipulada fue interpretada directamente como parte de la consulta SQL ejecutada por el servidor, permitiendo:

Extraer información completa de la base de datos de usuarios.

Impacto del Incidente

Impacto Directo: Seguridad de la Información

Pilar CIA	Impacto
Confidencialidad	ALTO
Integridad	MEDIO
Disponibilidad	BAJO

Impactos Técnico: Acceso NO autorizado a base de datos y divulgación de nombres, apellidos y datos de usuarios.

Impacto Organizativo: Fuga de la información y Incumplimiento de principios básicos de seguridad.

Recomendaciones

Basado en los análisis realizados y lo incidentes, las recomendaciones serán:

1.- Validar las entradas del usuario.

2.- Evitar concatenación directa de entradas en consultas SQL.

3.- Aplicar el principio de mínimo privilegio a los usuarios de la base de datos.

4.- Evitar el uso de usuarios con permisos elevados para aplicaciones web.

5.- Implementar controles del Anexo A norma ISO 27001:

A.8 – Gestión de activos de información.

A.12 – Seguridad en operaciones.

A.14 – Seguridad en el desarrollo y mantenimiento de sistemas.

6.- Realizar pruebas de seguridad periódicas (pentesting).

7. Conclusión

La vulnerabilidad de Inyección SQL realizada demuestra que puede comprometer gravemente la seguridad de una aplicación web. Este es una de las principales

causas de brechas de seguridad a nivel mundial. La correcta implementación de controles técnicos y organizativos es esencial para prevenir este tipo de ataques.