ISO 27001 – Reporte de Gestión de Incidentes
Vulnerabilidad de Inyección SQL

1. Introducción

Este reporte documenta la identificación y explotación controlada de una vulnerabilidad de Inyección SQL detectada en la aplicación Damn Vulnerable Web Application (DVWA). El análisis se realizó en un entorno controlado con fines educativos, con el objetivo de comprender cómo una validación inadecuada de entradas puede comprometer la seguridad de una aplicación web y la integridad de su base de datos.

2. Descripción del Incidente

Durante la evaluación de seguridad de la plataforma DVWA, se identificó una vulnerabilidad en el módulo de Inyección SQL. La aplicación no valida correctamente los datos ingresados por el usuario antes de integrarlos en las consultas SQL del backend. Esta deficiencia permite alterar la lógica original de la consulta, facilitando el acceso no autorizado a la información almacenada en la base de datos.

3. Proceso de Reproducción

La vulnerabilidad fue reproducida siguiendo los siguientes pasos dentro del entorno controlado:

1. Acceder a la aplicación DVWA utilizando credenciales válidas.
2. Configurar el nivel de seguridad de la aplicación en "Low".
3. Navegar al módulo de Inyección SQL.
4. Introducir un valor manipulado en el campo "User ID" con el fin de modificar la consulta SQL original.
5. Enviar la solicitud y analizar la respuesta generada por la aplicación.

Como resultado, la aplicación devolvió registros de la base de datos que no deberían ser accesibles bajo condiciones normales.

4. Impacto del Incidente

Si esta vulnerabilidad fuera explotada en un entorno productivo, podría generar consecuencias críticas, tales como:

- Acceso no autorizado a información confidencial.
- Exposición de credenciales de usuarios.
- Modificación o eliminación de datos sensibles.
- Riesgo elevado para la confidencialidad, integridad y disponibilidad de la información.

5. Recomendaciones

Para mitigar este tipo de vulnerabilidades y prevenir incidentes similares, se recomiendan las siguientes acciones:

1. Implementar consultas preparadas y parametrizadas.

2. Validar y sanitizar estrictamente todas las entradas del usuario.
3. Aplicar el principio de mínimo privilegio en las cuentas de base de datos.
4. Realizar pruebas de seguridad periódicas y auditorías técnicas.
5. Capacitar al personal técnico en prácticas de desarrollo seguro.

6. Conclusión

La identificación y explotación controlada de esta vulnerabilidad demuestra la importancia de aplicar controles de seguridad desde las primeras etapas del desarrollo. La adopción de buenas prácticas alineadas con ISO 27001 permite reducir significativamente la superficie de ataque y fortalecer la postura de seguridad de las aplicaciones web.