ISO 27001 Compliant Incident Management Report - SQL Injection Vulnerability

Introdución:

La prueba se realizó en un entorno controlado para demostrar una vulnerabilidad común y su impacto potencial en la seguridad de la aplicación, siguiendo los lineamientos de la norma ISO 27001.

Descripción del incidente:

Durante una evaluación de seguridad de DVWA con el nivel de seguridad configurado en "Low", se descubrió una vulnerabilidad de inyección SQL. Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación, comprometiendo la integridad y confidencialidad de los datos almacenados en la base de datos MariaDB.

Usado el método SQL Injection:

Para replicar y demostrar la vulnerabilidad, se utilizó el siguiente payload SQL en el campo "User ID":
1' OR '1'='1
Este payload explota la falta de validación de entrada para modificar la consulta SQL original. Al ser la condición '1'='1' siempre verdadera, la base de datos devuelve todos los registros de la tabla de usuarios en lugar de un solo ID, exponiendo nombres y apellidos de todos los usuarios registrados.

Impacto del incidente:

La explotación de esta vulnerabilidad podría permitir a un atacante:
• Acceder y extraer información confidencial de la base de datos, incluyendo credenciales de usuario.
• Modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.
• Obtener una enumeración completa de la estructura de la base de datos.
Esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por la plataforma.

Recomendaciones:

Basado en los hallazgos de esta evaluación, se recomiendan las siguientes medidas correctivas y preventivas:

1. Input Validation: Implementar validaciones de entrada estrictas para todos los datos suministrados por el usuario, utilizando consultas preparadas (Prepared Statements) y parametrización para evitar que el código SQL sea ejecutado como comando.
2. Penetration Testing: Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades antes de que sean explotadas.

3. Education and Awareness: Capacitar al personal técnico en prácticas de desarrollo seguro y concienciar sobre los riesgos asociados a las vulnerabilidades web.

Conclusión:

La identificación y explotación exitosa de la vulnerabilidad de inyección SQL subraya la importancia de la seguridad en el desarrollo y mantenimiento de aplicaciones web. Implementar controles de seguridad robustos y seguir las mejores prácticas de ciberseguridad es esencial para proteger los activos críticos y garantizar la continuidad del negocio.