Informe de Gestión de Incidentes (Conforme a ISO 27001) - Vulnerabilidad de Inyección SQL.

Se encuentra detallada la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web de prueba Damn Vulnerable Web Application (DVWA). La prueba se llevó a cabo en un entorno controlado para demostrar una vulnerabilidad común y su impacto potencial en la seguridad de la aplicación.

Descripción del incidente:

Durante la evaluación de seguridad, se descubrió una vulnerabilidad de inyección SQL en el módulo "SQL Injection". Esta vulnerabilidad permite a el atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación, evidenciando una brecha a la integridad y confidencialidad de los datos almacenados en la base de datos.

Método Utilizado:

Inyeccion de SQL con Payload en el campo de “User ID” :
'1' OR '1'='1'
Este Payload explota la vulnerabilidad modificando la consulta SQL original modificando las variables “WHERE” para que todo siempre sea “TRUE” y devuelva en vez de un solo Usuario, arroje todo el directorio de usuario que posee en su base de datos.

Impacto del incidente:

Permite al atacante extraer información confidencial de la base de datos, incluido modificaciones, esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por la aplicación.

Recomendaciones:

Basados en los hallazgos de esta evaluación de seguridad se recomiendan las siguientes medidas:

- Implementar parámetros más estrictos para proteger los datos de los usuarios y así evitar un ataque de inyección de SQL.
- Realizar Auditorías de seguridad periódicas incluyendo pentesting para así evitar futuras brechas de seguridad.
- Formar al personal técnico sobre prácticas de desarrollo de aplicaciones seguras y concienciar sobre los riesgos asociados a las vulnerabilidades de seguridad.

Conclusiones:

Identificar la vulnerabilidad de tu sistema a través de inyección SQL en DVWA indica la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web y así mismo implementar controles de seguridad robustos y seguir las mejores prácticas de ciberseguridad es esencial para proteger los activos críticos y garantizar tanto la seguridad como el uso confiable de tu sistema.