Informe de Gestión de Incidentes Conforme a ISO 27001

Introducción

Este informe documenta la identificación y explotación de una vulnerabilidad de inyección SQL observada en una aplicación web vulnerable. La prueba fue realizada en un entorno controlado con el objetivo de demostrar cómo una inyección SQL básica puede comprometer la seguridad de los datos almacenados.

Descripción del Incidente

Durante el análisis de seguridad, se detectó una vulnerabilidad de inyección SQL en el módulo de "User ID" de la aplicación. La vulnerabilidad permite a un atacante manipular la consulta SQL utilizando entradas maliciosas, lo que resulta en la exposición no autorizada de múltiples registros de usuarios almacenados en la base de datos.

Proceso de Reproducción

Para reproducir y demostrar la vulnerabilidad, se utilizó el siguiente payload en el campo de entrada "User ID":

1' OR '1'='1

Este payload modifica la consulta SQL original, provocando que la condición siempre sea verdadera ('1'='1'). Como resultado, el sistema devuelve todos los registros de usuarios en la base de datos en lugar de un único usuario.

Resultados observados en la explotación:
- admin
- Gordon Brown
- Hack Me
- Pablo Picasso
- Bob Smith

Esto demuestra que la aplicación no filtra ni valida adecuadamente los datos de entrada proporcionados por

el usuario.

Impacto del Incidente

La explotación de esta vulnerabilidad podría permitir a un atacante:

- Acceder y extraer datos confidenciales de la base de datos.
- Realizar ataques posteriores basados en la información obtenida.
- Alterar o eliminar datos almacenados.

Esto compromete gravemente los principios de confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

Con base en los hallazgos, se recomiendan las siguientes acciones:

1. Validación de Entradas: Implementar validaciones estrictas y consultas parametrizadas.
2. Uso de ORM: Utilizar frameworks que gestionen consultas de forma segura.
3. Pruebas de Penetración Regulares: Realizar auditorías de seguridad periódicas.
4. Capacitación en Seguridad: Formar al personal de desarrollo en prácticas de codificación segura.

Conclusión

La explotación exitosa de la vulnerabilidad identificada demuestra la importancia de aplicar controles de seguridad robustos en el desarrollo de aplicaciones web. La validación adecuada de las entradas de usuario es fundamental para proteger la integridad de los datos y evitar brechas de seguridad.