ISO 27001 Reporte de gestión de incidentes de conformidad – Vulnerabilidad SQL Injection

Introducción

Este reporte detalla la identificación y explotación de una vulnerabilidad a nivel aplicación web en el servicio de la empresa. Las pruebas fueron realizadas en un ambiente controlado para demostrar la vulnerabilidad en común y su impacto potencial en la seguridad de la aplicación web.

Descripción del incidente

Durante las pruebas de seguridad en la aplicación web de la empresa se descubrió una vulnerabilidad de tipo “SQL INJECTION” en la página principal del servicio web, siendo más específicos, en el formulario de USER ID. Esta vulnerabilidad permite a los atacantes inyectar código malicioso a través de queries SQL en los campos de ingreso de datos de la aplicación web logrando, de esta forma, comprometer la integridad y confidencialidad de los datos almacenados en la base de datos.

Método de SQL Injection usado

Para replica la vulnerabilidad demostrada, solo es necesario introducir el siguiente texto en el campo “User ID”:

```
1' OR '1'='1
```

Al ingresar este texto en el campo y presionar el botón “submit” se explota la vulnerabilidad para modificar la consulta original en SQL de forma que muestra de regreso los nombres de usuarios y apellidos almacenados en la base de datos. Una vez se explota esta vulnerabilidad, el atacante puede obtener los nombres y apellidos de los usuarios contenidos sin autorización.

Impacto del incidente

Al explotar esta vulnerabilidad un atacante es possible que logre:

- Accesar y extraer información confidencial de la base de datos, incluidos los nombres y apellidos.

Lo anterior representa un gran riesgo para la confidencialidad e integridad de la información confiada a nosotros por parte de los usuarios lo que, a su vez, compromete su integridad, disponibilidad y confidencialidad.

Recomendaciones

Basados en la vulnerabilidad encontrada en esta prueba, se recomienda encarecidamente implementar inmediatamente las siguientes acciones:

1. **Validación de entradas:** Implementar reglas más estrictas de validación de datos de entrada tomando muy en cuenta la prohibición de ingreso de parámetros de consultas SQL.
2. **Penetration Testing:** Realizar continuamente (al menos tres veces al mes) pruebas de penetración y explotación de vulnerabilidades del servicio web para detectar con anticipación las vulnerabilidad y corregirlas antes de que se conviertan en una amenaza usada por los atacantes.
3. **Training de empleados:** Realizar cursos y talleres para todos los empleados de la empresa del área de desarrollo web y ciberseguridad acerca de la importancia de las prácticas de seguridad al momento de llevar a cabo cambios y nuevos desarrollos web con el objetivo de evitar vulnerabilidades antes de salir a producción.

Conclusiones

La identificación a tiempo de la vulnerabilidad con SQL Injection resalta la importancia de realizar pruebas de penetración y explotación continuas oara detectar a tiempo posibles amenazas y no exponer la información y servicios antes posibles ataques.