ISO 27001 Reporte de Incidente - Vulnerabilidad de SQL Injection

Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de SQL injection en una aplicación web de prueba. La evaluación 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 de la aplicación web, se descubrió una vulnerabilidad de SQL injection en el módulo de "Búsqueda de Usuarios". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.

Método de SQL Injection Utilizado

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga útil SQL en el campo de entrada:

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

Esta carga útil explota la vulnerabilidad al modificar la consulta SQL original de tal manera que siempre devuelve un resultado verdadero. Al ejecutar esta inyección SQL, se obtuvieron los siguientes resultados:

```
ID: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

Impacto del Incidente

La explotación de esta vulnerabilidad permitió acceder a información confidencial de la base de datos, incluyendo nombres y apellidos de varios usuarios. Esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por la aplicación.

Recomendaciones

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

1. **Validación de Entrada**: Implementar validaciones estrictas de entrada para todos los datos proporcionados por el usuario, utilizando parámetros seguros en las consultas SQL para prevenir inyecciones SQL.
2. **Pruebas de Penetración**: Realizar auditorías de seguridad regulares, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades de seguridad antes de que sean explotadas por atacantes.
3. **Educación y Concienciación**: Capacitar al personal técnico y no técnico sobre prácticas de desarrollo de aplicaciones seguras y aumentar la concienciación sobre los riesgos asociados con las vulnerabilidades de seguridad.

Conclusiones

La identificación y explotación exitosa de la vulnerabilidad de SQL injection en la aplicación web subraya la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web. Implementar controles de seguridad robustos y seguir las mejores prácticas de ciberseguridad son esenciales para proteger activos críticos y garantizar la continuidad del negocio.