ISO 27001 Informe de gestión de incidentes de cumplimiento - Vulnerabilidad de inyección SQL

Introducción

Este reporte detalla la identificación y explotación de una vulnerabilidad de inyección SQL en el Damn Vulnerable Web Application (DVWA). Este test fue realizado en un ambiente controlado para demostrar una vulnerabilidad común y su potencial impacto en la seguridad de aplicaciones.

Descripción del incidente

Durante la evaluación de seguridad de DVWA, una vulnerabilidad de inyección SQL fue descubierta en el módulo de “Inyección SQL”. 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 inyección SQL utilizado

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

Sql

```
SELECT * FROM users WHERE username = 'username' AND password = '1' OR '1'='1';
```

Cuando una aplicación web construye una consulta SQL utilizando la concatenación de cadenas con la entrada del usuario, esta carga manipula la estructura de la consulta para eludir la autenticación o extraer datos no autorizados.

Impacto del incidente

Aprovechar esta vulnerabilidad podría permitir a un atacante:

● Acceder y extraer información confidencial de la base de datos, incluidas las credenciales de usuario.

● Modificar, eliminar o comprometer datos confidenciales almacenados en la aplicación.

Esto representa un riesgo significativo a la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

Recomendaciones.

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

1. Validación de entrada: Implementar validaciones de entrada estrictas para todos los datos proporcionados por el usuario, utilizando parámetros seguros en las consultas SQL para evitar la inyección de SQL.

2. Pruebas de penetración: Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar las vulnerabilidades de seguridad antes de que sean explotadas por atacantes.

3. Educación y concientización: Capacitar al personal técnico y no técnico en prácticas seguras de desarrollo de aplicaciones y concientizar sobre los riesgos asociados con las vulnerabilidades de seguridad.

Conclusiones

La identificación y explotación exitosa de la vulnerabilidad de inyección SQL en DVWA 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 es esencial para proteger activos críticos y garantizar la continuidad del negocio.