ISO 27001 Compliant Incident Management Report - SQL Injection Vulnerability

Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de inyección SQL en la Aplicación Web Damn Vulnerable (DVWA). La prueba se realizó 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 DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo «SQL Injection». 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 usado para SQL Injection

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

sql

```
select first_name as 'First name:',last_name as 'Surname:' from users where user_id=1 or '1'=1;
```

Este payload aprovecha la vulnerabilidad para modificar la consulta SQL original de forma que devuelva los nombres de usuario y contraseñas almacenados en la tabla users, concretamente para el usuario con id = 2. Al ejecutar con éxito esta inyección SQL, se obtienen las credenciales del usuario objetivo sin autorización.

Impacto del incidente

La explotación de 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 para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

Recomendaciones

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

1. Validación de entradas: Implemente validaciones de entrada estrictas para todos los datos suministrados por el usuario, utilizando parámetros seguros en las consultas SQL para evitar la inyección SQL.
2. Pruebas de penetración: Realice auditorías de seguridad periódicas, incluidas pruebas de penetración, para identificar y mitigar las vulnerabilidades de seguridad antes de que sean explotadas por los atacantes.
3. Educación y concienciación: Formar al personal técnico y no técnico en prácticas seguras de desarrollo de aplicaciones y concienciar sobre los riesgos asociados a las vulnerabilidades de seguridad.

Conclusiones

La identificación y explotación con éxito de la vulnerabilidad de inyección SQL en DVWA subraya la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web. Implantar controles de seguridad sólidos y seguir las mejores prácticas de ciberseguridad son esenciales para proteger los activos críticos y garantizar la continuidad de la actividad.