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 Web Application (DVWA). La prueba se llevó a cabo en un entorno controlado con el objetivo de 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 de "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 de Inyección SQL Utilizado

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

sql:

```
' UNION SELECT username, password FROM users WHERE id = 2 #
```

Este payload aprovecha la vulnerabilidad para modificar la consulta SQL original de manera que se devuelvan los nombres de usuario y contraseñas almacenados en la tabla de usuarios (`users`), específicamente el usuario con `id = 2`. Al ejecutar esta inyección SQL exitosamente, 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, incluyendo credenciales de usuario.
- Modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.

Esto representa un riesgo significativo para 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 recomienda implementar las siguientes medidas correctivas y preventivas:

1. **Validación de Entradas**: Implementar estrictas validaciones de entrada para todos los datos recibidos de los usuarios, utilizando parámetros seguros en las consultas SQL para prevenir inyecciones SQL.
2. **Pruebas de penetración**: Realizar auditorías regulares de seguridad, 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 en prácticas seguras de desarrollo de aplicaciones y concienciar 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 seguridad cibernética son fundamentales para proteger los activos críticos y garantizar la continuidad del negocio.