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 Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno controlado para demostrar una vulnerabilidad común y su posible impacto en la seguridad de las aplicaciones.

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 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 "User ID":

sql

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

Este payload explota la vulnerabilidad modificando la consulta SQL original para devolver todos los datos correspondientes a cada ID. Al ejecutar exitosamente esta inyección SQL, se obtienen las credenciales del usuario objetivo sin autorización.

Gestión del incidente

Explotar esta vulnerabilidad podría permitir a un atacante:

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

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

Recomendaciones

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

Validación de entradas: Implementar validaciones estrictas para todos los datos proporcionados por los usuarios, utilizando parámetros seguros en las consultas SQL para prevenir inyecciones SQL.

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

Conclusiones

El descubrimiento y la explotación exitosa de la vulnerabilidad de inyección SQL en DVWA subraya la necesidad crítica de adoptar medidas de seguridad proactivas en el desarrollo y mantenimiento de aplicaciones web. Fortalecer los controles de seguridad y adherirse a las mejores prácticas de ciberseguridad es esencial para proteger los activos clave y garantizar la continuidad de las operaciones empresariales.