Reporte de Gestión de Incidentes conforme a ISO 27001

Vulnerabilidad: Inyección SQL (SQL Injection)

Introducción

Este informe documenta la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA). Las pruebas se realizaron en un entorno controlado para demostrar una vulnerabilidad común y su impacto potencial 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 así la integridad y confidencialidad de los datos almacenados.

Método de Inyección Utilizado

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

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

Esta inyección aprovecha la vulnerabilidad para modificar la consulta SQL, haciendo que se devuelvan todos los registros de usuarios, sin necesidad de un ID válido. El resultado muestra nombres y apellidos de todos los usuarios.

Impacto del Incidente

La explotación de esta vulnerabilidad permite a un atacante:

- Obtener acceso no autorizado a datos sensibles como nombres de usuarios.

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

Recomendaciones

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

2. Principio de privilegios mínimos: Limitar los permisos de la cuenta de base de datos utilizada por la aplicación.

3. 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.

4. Educación y concienciación: Formar al personal técnico y no técnico en prácticas de desarrollo
   desarrollo de aplicaciones seguras y sensibilizar sobre los riesgos asociados a las vulnerabilidades de seguridad.

Conclusión

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 del negocio.