REPORTE DE INCIDENCIA POR INYECCIÓN SQL

INTRODUCCIÓN

En este documento se especifica la detección de una posible vulnerabilidad introducida por una inyección SQL en Damn Vulnerable Web Application (DVWA) y su explotación. El objetivo de este reporte es, como consecuencia, la concienciación de la existencia de vulnerabilidades y cómo evitar que se vuelvan amenazas para la seguridad del sistema.

DESCRIPCIÓN DEL INCIDENTE

El incidente por inyección SQL detectado se encuentra en el formulario login de la página web. Esto indica que el posible atacante tenga el permiso de acceder y consultar la base de datos de manera no autorizada, de convertirse esta vulnerabilidad en una amenaza.

IMPACTO DEL INCIDENTE

La inyección SQL permite acceso no autorizado a la base de datos, eso significa dar permiso a un atacante a poder modificar, eliminar, robar o exponer información y datos vulnerables. Esto además de generar riesgo reputacional y legal, afecta la integridad de la empresa y la disponibilidad de sus datos.

RECOMENDACIONES

Para evitar futuras vulnerabilidades y/o amenazas, se recomienda:
1. **REALIZAR PRUEBAS DE SEGURIDAD PERIÓDICAS**: De esta manera, se detectan vulnerabilidades antes de que lleguen a ser explotadas por atacantes.
2. **REVISAR Y RESTRINGIR PERMISOS INNECESARIOS AL USUARIO**: Asignar solo permisos altamente necesarios para que al atacante se le dificulte modificar datos.
3. **CONCIENCIACIÓN DEL PERSONAL**: Correcta educación sobre amenazas y vulnerabilidades y cómo evadirlas para una seguridad reforzada.

CONCLUSIÓN

Es necesario llevar a cabo un buen monitoreo de los movimientos y permisos con el objetivo de aumentar la seguridad de información sensible en la base de datos. Amenazas como la inyección SQL comprometen esta información y su corrección resulta prioritaria para el beneficio reputacional y legal de la empresa.