Informe de gestión de incidentes conforme a la norma ISO 27001: Vulnerabilidad de inyección SQL

Introducción:

Este documento detalla el descubrimiento análisis de una vulnerabilidad de seguridad por Inyección SQL usando como banco de pruebas DVWA. La práctica se llevó a cabo en un entorno controlado.

Descripción del incidente.

Durante la evaluación de seguridad de DVWA se descubrio una vulnerabilidad de inyeccion SQL.
Esta vulnerabilidad permite a los atacantes obtener datos desde el campo “user ID” y la información del mismo.

Proceso de reproducción.

Accedimos a la plataforma DVWA, se realizó una autenticación con credenciales de admin.
Navegamos hasta el apartado SQL Injection.
En el campo “ID User” introdujimos un payload malicioso “1’ OR ‘1’=’1’” lo que se traduce como “TRUE” y proporcionará todos los valores correspondientes a los usuarios.

Impacto del incidente.

Tiene un impacto crítico pues es una vulnerabilidad capaz de extraer datos de mucha importancia.
Pérdida de confidencialidad ya que un atacante puede acceder a toda la información sensible de la tabla de usuarios.
Pérdida de integridad ya que podría modificar el payload para ejecutar sentencias SQL como UPDATE o DELETE que es peor aún
Pérdida de disponibilidad ya que podría usarse comandos como “DROP TABLE USERS” perdiendo así información muy importante de nuestros clientes o empleados.

Recomendaciones.

Realizar auditorías regularmente, para identificar y mitigar las vulnerabilidades.
Usar herramientas IDs/IPs como Snort o WAF.
Usar el principio del mínimo privilegio.
Usar validación de entradas rechazando cualquier entrada que no se ajuste al formato.

Conclusión.

Esta vulnerabilidad identificada es un riesgo crítico que expone todos los datos de usuarios al demostrarse su explotación. Se recomendó la adopción de medidas como usar herramientas IDS/IPS o WAF.