Reporte de Incidente de Seguridad inyeccion sql

Hicimos una inyeccion SQL en DVWA, se identificó una vulnerabilidad crítica de SQL Injection (SQLi) en el módulo de consulta de usuarios, esta vulnerabilidad permite a un atacante interactuar directamente con la base de datos sin autorización previa. La aplicación no funciona correctamente la entrada del usuario en el campo User ID al introducir caracteres especiales y operadores lógicos de SQL, el motor de la base de datos interpreta estos datos como parte de la consulta legítima, permitiendo la extracción de información sensible.

SQL Injection de DVWA.Inserción en el campo de texto: 1' OR '1'='1, la aplicación devolvió el nombre y apellido de todos los usuarios registrados en la base de datos (admin, Gordon, Hack, Pablo, Bob)

Confidencialidad: Acceso no autorizado a toda la base de datos de usuarios.
Integridad: Un atacante avanzado podría modificar o eliminar registros.
Autenticación: Permite saltarse procesos de login (bypass) al manipular las consultas de validación.

Restringir el campo User ID para que solo acepte caracteres numéricos. Principio de Mínimo Privilegio, asegurar que el usuario de la base de datos no tenga privilegios de administrador (root).

CONCLUSION:

La vulnerabilidad confirmada representa un riesgo alto para la organización. La implementación de consultas preparadas es la solución más efectiva para neutralizar este vector de ataque de forma definitiva.