

Inyección SQL

INTRODUCCIÓN

Se encontró un agujero de seguridad que permite a cualquiera ver datos que no debería al manipular una casilla en la página web.

DESCRIPCIÓN DEL INCIDENTE

Un atacante pudo saltarse la seguridad de la aplicación al introducir un código malicioso en el campo de "User ID". Esto obligó al sistema a mostrar todos los usuarios de la base de datos, en lugar de buscar solo un ID específico.

PROCESO DE REPRODUCCIÓN

- 1) Se fue a la vulnerabilidad (SQL Injection)
- 2) En la casilla "User ID" , metió : 1'OR='1
- 3) Al presionar "Submit" , el sistema mostró una lista completa de usuarios

IMPACTO DEL INCIDENTE

Este fallo permite robar información de usuarios y podría usarse para hacerse pasar por el administrador o acceder a otras áreas privadas del sistema

RECOMENDACIONES

- 1) Usar "preguntas seguras" : El código que habla con la base de datos debe ser cambiado para usar Consultas Parametrizadas. Es la forma más importante para bloquear este tipo de ataque
- 2) Validación de entradas : La casilla de "User ID" debe ser configurada para solo aceptar números y rechazar cualquier letra o símbolo

CONCLUSIÓN

Es un problema crítico de seguridad y se debe corregir implementando preguntas seguras para proteger los datos de los usuarios y la integridad del sistema