TECNOLOGÍAS APLICADAS

Inacap

SQL Injection, ¿Qué son y cómo prevenirlas?

Lidia Moreno Farías

Inacap

TEMAS

PYTHON CHILE

1. ¿Qué es una inyección SQL
2. Riesgos de la vulnerabilidad
3. Inyecciones SQL más comunes
4. ¿Cómo evitar una inyección SQL
5. Ejemplo inyección SQL

inacap

¿Qué es una inyección SQL?

- Vulnerabilidad de seguridad que permite a los atacantes interferir con las consultas a la base de datos de una aplicación.
- Puede permitir: ver, modificar o eliminar datos a los que no se debiese tener acceso.

Riesgos de la Vulnerabilidad

DAÑOS AL SITIO WEB

ROBO O FILTRACIÓN DE DATOS

ESCALACIÓN DE PRIVILEGIOS.

PÉRDIDA DE REPUTACIÓN Y CONFIABILIDAD.

Inyecciones SQL más comunes

Inyección SQL mediante introducción de datos del usuario.

Inyección SQL mediante parámetros de una aplicación.

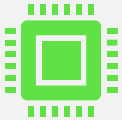
Inyección SQL mediante herramientas de hackeo automáticas

¿Cómo evitar una inyección SQL?

- Consultas parametrizadas
- Procedimientos almacenados
- Validación de entrada
- Principio del mínimo privilegio
- Firewall de Base de Datos
- Actualización y parches periódicos

Ejemplos de inyecciones SQL

Fornite, 2019: Fornite es un juego en línea con más de 350 millones de usuarios. En 2019, se descubrió una vulnerabilidad de inyección de SQL que les permitía a los atacantes acceder a las cuentas de los usuarios.



En 2018, se encontró una vulnerabilidad de inyección de SQL en **Cisco Prime License Manager.** La vulnerabilidad permitía que los atacantes tuvieran acceso shell a los sistemas en los que estaba implementado el administrador de licencias.

En 2014, investigadores de seguridad anunciaron que podían quebrantar el sitio web de **Tesla** con una inyección de SQL, lo que les permitiría obtener privilegios de administrador y robar datos de los usuarios en el proceso.

PYTHON CHILE

EJEMPLO INYECCIÓN SQL

Python, SQLite

inacap