SQL Injection: como un pequeno erro pode comprometer unha base de datos

1. Introdución

Na actualidade, unha gran parte da información persoal e profesional almacénase en sistemas informáticos conectados a Internet. Isto fai que a seguridade das aplicacións web sexa un aspecto fundamental para protexer datos sensibles.

Unha das vulnerabilidades máis coñecidas na seguridade web é a chamada SQL Injection, que permite manipular consultas realizadas a unha base de datos cando unha aplicación non valida correctamente os datos introducidos polos usuarios.

Neste proxecto analizamos como funciona esta vulnerabilidade e demostramos, mediante un exemplo práctico, como pequenas decisións na programación poden comprometer a seguridade dun sistema ou, polo contrario, protexelo.

2. Fundamentos teóricos

As aplicacións web utilizan habitualmente bases de datos para almacenar información, como usuarios, contrasinais ou datos persoais. Para acceder a estes datos utilízase unha linguaxe chamada SQL (Structured Query Language).

Unha consulta SQL típica pode utilizarse para comprobar se un usuario e o seu contrasinal existen na base de datos durante un proceso de inicio de sesión.

O problema aparece cando unha aplicación non valida correctamente os datos introducidos polos usuarios. Neste caso, un atacante pode introducir código SQL dentro dun campo dun formulario web, modificando a consulta orixinal que realiza a aplicación.

Este tipo de ataque coñécese como SQL Injection e pode permitir, entre outras cousas:

- acceder a información privada
- modificar datos almacenados
- eliminar información da base de datos

Para evitar este problema existen diferentes técnicas de programación segura, como:

- validación e filtrado de datos introducidos polos usuarios
- uso de consultas parametrizadas

- control de permisos de acceso á base de datos

Estas medidas reducen significativamente o risco de explotación desta vulnerabilidade.

3. Materiais e métodos

Para estudar esta vulnerabilidade desenvolveuse unha páxina web de proba cun sistema de inicio de sesión vulnerable.

Este sistema simulaba o funcionamento básico dun formulario de autenticación no que o usuario introduce o seu nome de usuario e contrasinal. A aplicación realizaba unha consulta SQL para comprobar se os datos coincidían cos almacenados na base de datos.

Nun primeiro momento a aplicación non incluía mecanismos de protección, o que permitía manipular a consulta SQL introducindo determinadas cadeas de texto no formulario.

Posteriormente aplicáronse diferentes medidas de seguridade, como:

- validación dos datos introducidos polos usuarios
- uso de consultas parametrizadas
- control de entradas sospeitosas

Deste xeito foi posible comparar o comportamento da aplicación antes e despois da implementación das medidas de seguridade.

4. Resultados

Durante as probas observouse que a aplicación vulnerable permitía modificar a consulta SQL introducindo determinadas cadeas de texto no formulario de inicio de sesión.

Isto permitía acceder ao sistema sen coñecer os datos reais do usuario, demostrando como unha mala validación da información pode comprometer a seguridade dunha base de datos.

Cando se aplicaron as medidas de seguridade, o sistema deixou de aceptar estas manipulacións e o acceso non autorizado xa non foi posible.

Estes resultados demostran a importancia de aplicar técnicas de programación segura no desenvolvemento de aplicacións web.

5. Conclusións

A investigación realizada permite concluír que a vulnerabilidade SQL Injection representa un risco real para as aplicacións web que non implementan mecanismos adecuados de validación de datos.

Tamén se comprobou que mediante técnicas relativamente sinxelas, como o uso de consultas parametrizadas e validación de entradas, é posible evitar este tipo de ataques.

Este proxecto pon de manifesto a importancia da ciberseguridade no desenvolvemento de software e da formación dos programadores en boas prácticas de programación.