Seguridad e inyección en SQL

Administración y Diseño de Bases de Datos

Cheuk Kelly Ng Pante, Javier González de la Barreda Arimany y Samuel Toledo Hernández

14 de noviembre de 2023

Índice general

1. Introducción a la seguridad de bases de datos

1.1. Introducción a las bases de datos

Una base de datos consiste en una colección de datos interrelacionados que representan información sobre una organización o área en particular. Estas bases de datos están organizadas según modelos de datos que definen la estructura, almacenamiento y manipulación de la información. El modelo principal es un modelo relacional que representa datos a través de tablas y crea relaciones entre ellos.

Los sistemas de gestión de bases de datos (DBMS) son programas informáticos que gestionan, modifican, consultan y crean bases de datos. Entre sus ventajas importantes se incluyen la independencia de los datos con respecto a la aplicación respectiva, la garantía de integridad mediante reglas de validación; seguridad de la información mediante control de acceso; y optimización del rendimiento a través de índices/vistas.

En el diseño de bases de datos intervienen una variedad de etapas, incluido el análisis de requisitos, el diseño conceptual, el diseño lógico y el diseño físico. Los modelos de entidad, atributos y relaciones se utilizan en el modelo de relación de entidad para representar datos en el diseño conceptual. El modelo relacional es la base del diseño lógico, ya que presenta datos a través de tablas, claves y restricciones.

El lenguaje utilizado para consultar la base de datos es un conjunto de instrucciones que permiten a los usuarios seleccionar, insertar, actualizar y eliminar datos. La mayoría de los DBMS pueden ser compatibles con SQL, qué es el lenguaje de consulta más utilizado.

En el ámbito de la programación de bases de datos, se emplean subrutinas, que son bloques de código encargados de llevar a cabo tareas específicas relacionadas con los datos. Estas subrutinas pueden manifestarse como procedimientos almacenados o funciones, diferenciándose en que los procedimientos almacenados pueden retornar varios valores o ninguno, mientras que las funciones solo pueden devolver un valor. La ejecución de estas subrutinas dentro del Sistema de Gestión de Bases de Datos (SGBD) contribuye a mejorar tanto la eficiencia como la seguridad de las bases de datos

1.2. Seguridad de bases de datos

La seguridad de la base de datos abarca un conjunto de herramientas, medidas y controles diseñados para proteger la integridad, confidencialidad y disponibilidad de los datos almacenados en una base de datos. Estas “copias” están implementadas para evitar el acceso no autorizado, modificaciones inapropiadas o pérdidas accidentales. En este contexto, se cubrirán aspectos técnicos y organizativos, incluidas actividades como autenticación, auditoría, cumplimiento normativo, gestión de riesgos, educación, etc.

La importancia de la seguridad de las bases de datos reside en su función esencial para asegurar el funcionamiento adecuado de las organizaciones y la salvaguardia de la privacidad de las personas. Para preservar la integridad del sistema, resulta crucial hacer frente a amenazas como ataques internos, errores humanos, vulnerabilidades de software, ataques de inyección SQL, ataques de denegación de servicio y la presencia de malware.

Ante las amenazas mencionadas, se sugiere adoptar las mejores prácticas de ciberseguridad, que incluyen medidas como salvaguardar la integridad física, aplicar controles administrativos y de acceso a la red, asegurar dispositivos y cuentas de usuarios finales, proteger el software de bases de datos, garantizar la seguridad de servidores de aplicaciones y web, así como implementar precauciones en las copias de respaldo y llevar a cabo auditorías periódicas.

La seguridad de las bases de datos emerge como un tema de gran importancia y complejidad. En este contexto, se busca resguardar la información almacenada en dichas bases contra accesos no autorizados, alteraciones indebidas y pérdidas accidentales o maliciosas. La protección de la base de datos involucra diversos elementos críticos como:

- **Datos de la base de datos:** Esta información, que abarca desde nombres y contraseñas hasta números de tarjetas de crédito y debe mantenerse confidencial, íntegra y accesible únicamente para usuarios autorizados.
- **Sistema de gestión de bases de datos (DBMS):** Desempeña un papel fundamental al crear, administrar y manipular las bases de datos. Es esencial que el DBMS esté actualizado, configurado y protegido de manera adecuada para prevenir vulnerabilidades y ataques.
- **Aplicaciones asociadas:** Los programas que interactúan con la base de datos para realizar diversas operaciones deben validar y filtrar las entradas de los usuarios. Además, es crucial que utilicen consultas parametrizadas o procedimientos almacenados, y limiten los permisos y privilegios de los usuarios y las bases de datos.
- **Servidor de base de datos físico y/o virtual y hardware subyacente:** Estos dispositivos, ya sean físicos o virtuales, donde residen la base de datos y el DBMS, deben contar con protección física, sistemas de copia de seguridad y recuperación, así como medidas de seguridad de red, como firewalls, antivirus y cifrado.
- **Infraestructura informática y/o de red para acceder a la base de datos:** Los medios a través de los cuales usuarios y aplicaciones se comunican con la base de datos, como ordenadores, dispositivos móviles e internet, deben garantizar la seguridad y privacidad de las comunicaciones. Esto implica el uso de protocolos seguros, contraseñas robustas, certificados de seguridad, entre otras medidas.

La importancia de asegurar las bases de datos radica en la necesidad de prevenir o reducir al mínimo los riesgos y las consecuencias asociadas a los ciberataques. Estos eventos pueden resultar en daños irreparables tanto para los datos almacenados como para las organizaciones y los usuarios involucrados. Algunos de los ciberataques más comunes y peligrosos pueden ser:

- **La inyección SQL:** Implica la introducción de código SQL malicioso en las entradas de los usuarios para alterar o acceder a la información de la base de datos. Este tipo de ataque puede ocasionar la pérdida o el robo de datos sensibles, la modificación o eliminación de información crucial, la ejecución de comandos arbitrarios en el servidor, o la revelación de datos internos o confidenciales de una organización.
- **El robo de credenciales:** Se refiere a la obtención de contraseñas o nombres de usuario de usuarios o aplicaciones que acceden a la base de datos. El propósito de este ataque es suplantar identidades o llevar a cabo acciones no autorizadas, lo que puede resultar en acceso no autorizado a los datos, alteración o borrado de información, o la propagación de malware o virus.
- **El ransomware:** Implica cifrar los datos de la base de datos o bloquear su acceso, con el objetivo de exigir un rescate a cambio de su liberación. Este tipo de ataque puede conducir a la inaccesibilidad de los datos, interrupciones en el funcionamiento del negocio o el pago de grandes sumas de dinero

La seguridad de las bases de datos exige la implementación de un conjunto integral de medidas técnicas, organizativas y legales destinadas a resguardar los datos de posibles amenazas, tanto internas como

externas, como hackers, empleados deshonestos, errores humanos, fallas de hardware o software, desastres naturales y violaciones normativas. Diversas prácticas, políticas y tecnologías pueden ser adoptadas para fortalecer la seguridad de las bases de datos, entre las que se encuentran:

- Diseñar una arquitectura de base de datos segura que separe los datos sensibles de los no sensibles, que minimice los puntos de acceso y que aplique el principio de mínimo privilegio.
- Implementar un sistema de gestión de bases de datos (DBMS) actualizado y configurado adecuadamente, que ofrezca funciones integradas de seguridad, tales como cifrado, control de acceso, registro de eventos y detección de anomalías.
- Desarrollar una aplicación segura que utilice métodos de conexión seguros, que evite la inyección de código malicioso, valide los datos de entrada y cifre la información en tránsito y en reposo.
- Llevar a cabo pruebas de seguridad periódicas que evalúen la vulnerabilidad de la base de datos e identifiquen y corrijan posibles debilidades o brechas.
- Impartir formación y concienciación a los usuarios y administradores de la base de datos acerca de las mejores prácticas de seguridad, como la utilización de contraseñas sólidas, el cambio regular de credenciales, el bloqueo de sesiones inactivas y la notificación de cualquier incidente sospechoso

2. Riesgos y consecuencias de la inyección SQL

2.1. Introducción a SQL