CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

Seguridad

SECCIÓN D04

INTEGRANTES DE EQUIPO:
Gildo López Miguel Ángel

González Ramírez Alan Leonardo

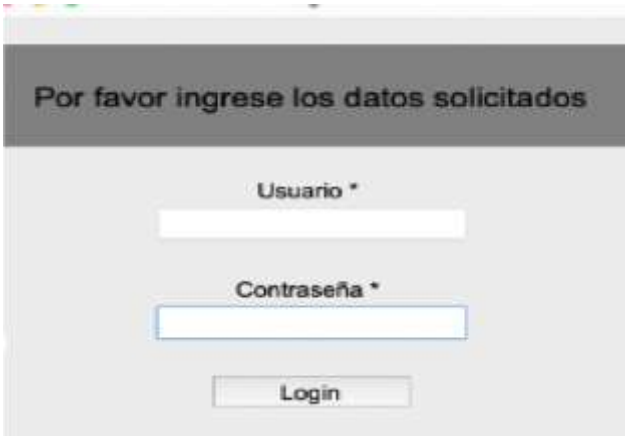
Montejano Paredes Diego Fernando

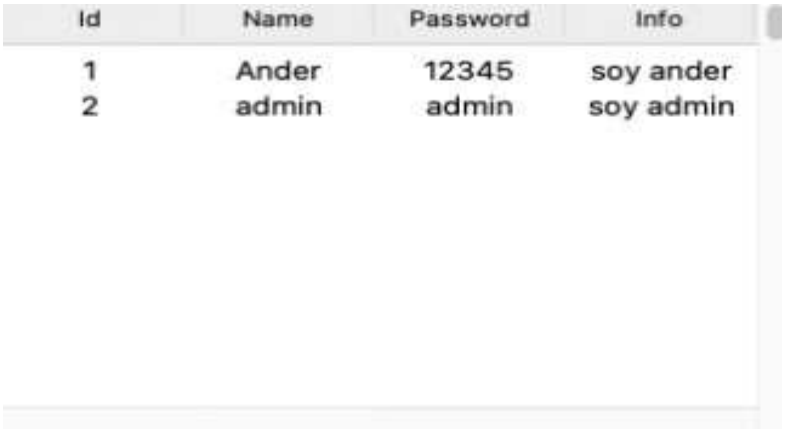
PROFESOR: Vazquez Curiel Armida Griselda
11/03/2024

Actividad 3.2 Seguridad en Base de Datos Defensa

Introducción

La seguridad informática es un aspecto crucial en la gestión de información valiosa o confidencial a través de bases de datos. En este contexto, SQLite se destaca como una base de datos relacional ampliamente utilizada debido a su simplicidad, eficiencia y versatilidad. A pesar de su sólida reputación, SQLite no está exento de posibles vulnerabilidades que podrían comprometer la integridad de la información almacenada. Este ensayo se enfoca en la importancia de la seguridad de las bases de datos SQLite y explora diversas medidas de protección y defensa que pueden implementarse para garantizar la integridad de los datos.





Id	Name	Password	Info
1	Ander	12345	soy ander
2	admin	admin	soy admin

Software implementado en SQLite

Medidas de Protección para Bases de Datos SQLite:

- **Encriptación de la Base de Datos:**
  La encriptación es una capa fundamental de protección para cualquier base de datos. Para SQLite, se recomienda encarecidamente utilizar extensiones como SQLCipher, que proporciona encriptación robusta a nivel de archivo y protege el contenido de la base de datos. Esto garantiza que incluso si un atacante obtiene acceso al archivo de la base de datos, no podrá descifrar su contenido sin la clave de desencriptación adecuada.

- **Autenticación y Control de Acceso:**
  Una autenticación sólida y la gestión adecuada de los permisos de usuario son componentes críticos de la seguridad de la base de datos. Es fundamental asegurarse de que solo los usuarios autorizados tengan acceso a la base de datos y de otorgar permisos de manera adecuada y específica, minimizando así el riesgo de acceso no autorizado.

- **Actualizaciones Regulares:**
  Mantener SQLite y sus dependencias actualizadas es esencial. Las actualizaciones periódicas suelen incluir correcciones de seguridad que abordan vulnerabilidades conocidas. Permanecer al día con las últimas versiones de SQLite y otras bibliotecas relacionadas es una forma efectiva de fortalecer la seguridad de la base de datos.

- **Respaldo y Recuperación de Datos:**
  La realización de copias de seguridad regulares de la base de datos es fundamental. En caso de una violación de seguridad o pérdida de datos, contar con un respaldo actualizado permite restaurar la información de manera eficiente y minimizar la pérdida.

- **Monitoreo Continuo:**
  Implementar un sistema de monitoreo de seguridad que registre y alerte sobre actividades inusuales o intentos de acceso no autorizado es una medida proactiva. Esto facilita la detección y respuesta temprana a posibles amenazas, protegiendo así la base de datos en tiempo real.

- **Actualización de Bibliotecas y Dependencias:**

Además de mantener actualizado SQLite, es importante mantener al día todas las bibliotecas y dependencias relacionadas con la aplicación que utiliza la base de datos. Las vulnerabilidades en otras partes de la aplicación pueden afectar la seguridad general de la base de datos.

Conclusión:

Una base de datos SQLite es esencial para salvaguardar la privacidad y la integridad de la información que contiene. Aunque la inyección de SQL es una vulnerabilidad crítica que merece atención, es igualmente importante implementar un enfoque integral de seguridad que incluya medidas como la encriptación, la autenticación sólida, la gestión de permisos, las actualizaciones regulares, el respaldo de datos y el monitoreo continuo.