Desarrollo de un sistema seguro para el acceso y almacenamiento de historiales médicos en formato digital

Seguridad y Confidencialidad 2025

Práctica de programación

- **Fecha de entrega: 11 de junio de 2025**
- Se realizará por grupos y en lenguaje Go utilizando el proyecto base “prac”.
- La evaluación consistirá en la entrega del código fuente de la práctica junto con una memoria explicativa de la implementación.
- Durante el desarrollo de la práctica, se darán ejemplos de implementación de las funcionalidades necesarias. El nivel de conocimiento sobre estos códigos fuentes se evaluará mediante **dos test evaluables** en las sesiones de prácticas.
- Se realizarán **dos seguimientos presenciales evaluables** de la consecución de objetivos de la práctica (aproximadamente el 01/04 y del 06/05)
- En la última sesión de prácticas se realizará **un test evaluable** de conocimiento del código general de la práctica.

Descripción

En esta práctica se va a desarrollar un sistema seguro para el acceso y almacenamiento de historiales médicos en formato digital. Se proporciona un proyecto base en Go, denominado “prac”, que ya provee la funcionalidad básica de registro, login, almacenamiento en base de datos, etc. Sin embargo, además de la funcionalidad necesaria para completar la aplicación, faltan componentes esenciales de seguridad que constituyen el enfoque principal de la práctica.

El objetivo es que, partiendo del proyecto base (donde el cliente y el servidor se comunican mediante HTTP sin seguridad y se guardan los datos en una base de datos embebida no relacional), se implemente la funcionalidad oportuna, así como los distintos aspectos de seguridad necesarios y que se ven en la asignatura:

- Comunicación segura (HTTPS) entre cliente y servidor.
- Autenticación segura de usuarios (hash de contraseñas, verificación robusta, etc.).
- Cifrado de la información almacenada en la base de datos (evitando que cualquiera con acceso al fichero .db pueda ver los datos en claro).
- Gestión segura de la clave de cifrado (evitando claves fijas en el código).
- Cualquier mejora adicional de seguridad que se estime oportuna para mejorar la seguridad y resiliencia del sistema (doble factor, roles, firma digital, etc.)

Para simplificar el proceso de implementación y prueba, la aplicación proporcionada arranca tanto el cliente como el servidor en un único paso. El proyecto está muy documentado con comentarios y se organiza en varios paquetes y ficheros Go:

- Main. Inicia tanto el servidor como el cliente en paralelo.
- Server. Implementa la lógica de servidor.
- Client. Implementa el cliente interactivo por terminal. Muestra un menú y manda peticiones al servidor.
- API. Define los tipos de mensajes (Request, Response) y constantes de acciones; es común tanto al servidor como al cliente.
- Store. Gestiona la persistencia de la información en una base de datos no relacional (boltDB).
- UI. Maneja la interfaz de texto para el usuario (limpiar pantalla, leer inputs, menús, etc.).

Desarrollo

Además de ampliar la funcionalidad de acuerdo con el objetivo de la práctica, se deberán implementar las siguientes medidas de seguridad ausentes en el proyecto proporcionado.

- Autentificación segura mediante contraseñas.
- Compresión y cifrado de la base de datos del sistema.
- Gestión de la clave maestra para el cifrado de la base de datos.
- Propuesta e implementación de posibles mejoras.

Detallemos a continuación los diferentes elementos a implementar.

Autentificación segura

Actualmente se realiza autentificación por contraseña, pero se almacenan en abierto. Se deberá modificar el servidor para emplear el método más seguro posible, así como incorporar los campos necesarios en la BD e indicar en la memoria cómo mejora esto la seguridad de la aplicación. Se debe tener en cuenta tanto el registro de nuevos usuarios como la comprobación de las credenciales de usuarios ya existentes (login).

Cifrado de la base de datos del sistema

El sistema utiliza una base de datos no relacional embebida (boltDB, ficheros store.go y bbolt.go) para almacenar la estructura de datos del sistema. Se ha de modificar el proyecto para añadir compresión y cifrado a la información almacenada en la BD, así como descifrado y descompresión en el proceso inverso. De esta forma, aunque se robara el fichero de la base de datos, la información no quedaría desprotegida.

Gestión de la clave maestra de cifrado

Al incorporar cifrado de datos al sistema, resulta necesario tener una clave para dicho cifrado. Se ha de evitar una clave fija y que, por lo tanto, reside en el código de la aplicación. Este método no es el ideal, ya que cualquiera con acceso al código fuente (o al ejecutable utilizando ingeniería inversa) puede obtener dicha clave y descifrar la base de datos. Se ha de añadir la funcionalidad necesaria al servidor para que dicha clave dependa de factores externos (como, por ejemplo, que el administrador introduzca una contraseña de la que se deriva una clave al arrancar el servidor).

Funcionalidad adicional

Se podrán implementar o diseñar medidas de seguridad extra para aumentar la nota de la práctica, siempre documentándolas debidamente en la memoria y adaptándolas al contexto de la práctica como se estime oportuno. Entre otras:

- Autentificación con doble factor (email, pin, tarjeta de coordenadas, etc.)
- Extender la funcionalidad del sistema con seguridad adicional, uso de firma digital, acceso por roles a la información, etc.
- Mejora de la interfaz de usuario o extensión a otros paradigmas (web, etc.).
- Otras mejoras a propuesta del alumnado.

Evaluación

La evaluación de prácticas se realizará conforme a los siguientes apartados:

- **0,25 puntos –** Test sobre el tour de Go.
- **0,75 puntos –** Práctica 0.
- **1 puntos –** Cumplir con hitos en fechas de revisión.
- **2 puntos –** Funcionalidades de almacenamiento de historiales médicos en formato digital.
- **1 puntos –** Memoria.
- **2 puntos –** Implementación de los elementos de seguridad obligatorios.
- **1 punto –** Test sobre interpretación de códigos de ejemplo.
- **0,5 puntos –** Test final sobre conocimientos de la práctica.
- **1,5 puntos –** Funcionalidades de ampliación de seguridad.
- *Hasta 2 puntos extras por más funcionalidades de ampliación*.