Universidad
Carlos III de Madrid

Criptografía y seguridad informática

G24 - Reporte 1

Javier Martín Pizarro

Alberto Pascau Sáez

Raúl Armas Seriña

Índice general

Índice general **1**

1. Propósito de la aplicación. Estructura interna **2**
1.1. Propósito de la aplicación 2
1.2. Estructura interna 2

Capítulo 1

Propósito de la aplicación. Estructura interna

1.1. Propósito de la aplicación

La aplicación simula una página web, levantada en local por el propio usuario, en la que se pueden crear una serie de desafíos (*challenges*) tanto privados como públicos. Dependiendo de qué tipo de sea cada desafío, el flujo interno (de código) será distinto.

- **Desafío público:** cualquier usuario registrado tiene acceso a ellos.
- **Desafío privado:** solamente pueden ser compartidos con un único usuario. El creador del desafío selecciona al otro usuario que será capaz de verlo.

El propósito de esta aplicación es generar un sistema informático que cumpla unos requisitos mínimos. Nótese que a medida que la práctica avance, esta lista podrá verse modificada.:

1. El sistema debe de ser capaz de registrar usuarios y que su información confidencial quede correctamente cifrada.
2. El sistema debe ser capaz de permitir un inicio de sesión fluido donde se sea capaz de obtener y comparar los datos cifrados de los usuarios de la base de datos con los proporcionados por el cliente.
3. El sistema debe de ser capaz de crear y recuperar desafíos cuya información pueda o no estar cifrada.
4. El sistema debe de ser capaz de permitir a un usuario A leer el desafío creado por el usuario B si este se lo ha compartido.

1.2. Estructura interna

Esta aplicación consta de tres partes fundamentales:

- Frontend: esencial para la experiencia de usuario. Actua como interfaz entre el cliente y el backend.

- Backend: donde se encuentra la API. Todos los mecanismos de cifrado, autenticación, *hasheo* se encuentran en este directorio.
- Base de datos: creada usando MariaDB SQL debido a su simplicidad. La base de datos tiene únicamente dos tablas, *users* y *challenges*.