

PRÁCTICA 2022/2023

SEGURIDAD EN EL DISEÑO DEL SOFTWARE (V1.0)

CONDICIONES GENERALES

- El desarrollo se realizará en [Go](#).
- Se realizará por parejas (salvo excepciones justificadas).
- Se evitarán interfaces de usuario complejas, utilizando esencialmente el terminal y concentrando el esfuerzo en el problema y la seguridad.
- El programa irá acompañado de una documentación (se publicará una guía específica más adelante) que explique el diseño, la funcionalidad implementada, el proceso de desarrollo, así como las decisiones tomadas y las expectativas de seguridad del proyecto.

GESTOR DE CREDENCIALES

El objetivo consistirá en la creación de un gestor de contraseñas y/o credenciales (al estilo de PasswordSafe, Password Gorilla, 1Password, KeePass, LastPass, etc.) con almacenaje en servidor que permita su acceso desde distintos clientes remotos.

Las características mínimas que se deben incluir en el diseño para aprobar son:

- Arquitectura cliente/servidor realizándose ambos en Go.
- Cada entrada incluirá, como mínimo, un identificador, un usuario y una contraseña.
- Cifrado apropiado de la base de datos de contraseñas en el servidor.
- Mecanismo de autenticación seguro (gestión de contraseñas e identidades).
- Transporte de red seguro entre cliente y servidor (se puede emplear algún protocolo existente como TLS o HTTPS).

Algunos desafíos adicionales (aspectos extra u opcionales para subir nota) podrían ser:

- Optimización de la privacidad (conocimiento cero: el servidor sólo recibe datos cifrados por el cliente).
- Generación de contraseñas aleatorias y por perfiles (longitud, grupos de caracteres, facilidad de recordar o pronunciar, etc.)
- Incorporación de datos adicionales (notas de texto, ficheros, etc.) en cada entrada.
- Capacidad de generar/almacenar credenciales de clave pública o certificados como entrada.
- Incorporación de clave pública en la autenticación de usuarios.
- Incorporación de firma digital para garantizar el origen de los datos.
- Posibilidad de compartir credenciales entre distintos usuarios.
- Otros a consensuar con el profesorado.