GESTOR DE CONTRASEÑAS

SEGURIDAD EN DISEÑO DEL SOFTWARE

Pedro Giménez Aldeguer y Melanie Mariam Cruz Morgado

16.04.2019

Objetivos de desarrollos marcados

Creación de un gestor de contraseñas con arquitectura cliente/servidor cuyo almacenaje sea en el servidor y que permita su acceso desde distintos clientes remotos.

Características que debe cumplir:

- [ ] El mecanismo de autentificación debe ser seguro.
- [ ] Usar un transporte de red seguro entre cliente y servidor.
- [ ] Conocimiento Cero.

Descripción de implementación

Mecanismo de autenticación seguro

Hash:

El cliente tras escribir la contraseña le realiza un hash con SHA 512, a continuación coge los primeros 256 bits de dicho hash y, por último, lo envía al servidor para utilizarlos como clave de autenticación.

Función de derivación:

Esos bits enviados al servidor más el añadido de la “sal” los utiliza en una función de derivación de clave (Scrypt) para aumentar la seguridad.

Creación de un gestor de contraseñas con arquitectura cliente/servidor cuyo almacenaje sea en el servidor y que permita su acceso desde distintos clientes remotos.

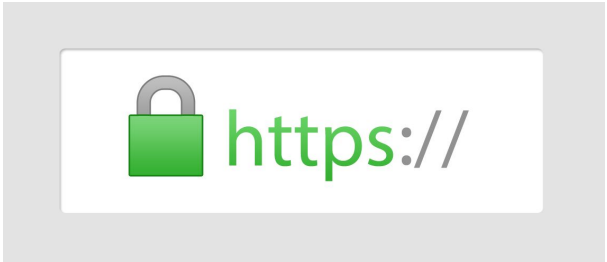
Características que debe cumplir:

- [x] El mecanismo de autentificación debe ser seguro.
- [ ] Usar un transporte de red seguro entre cliente y servidor.
- [ ] Conocimiento Cero.

Transporte de red seguro Cliente/Servidor

HTTPS:

Para el envío seguro de los datos hemos utilizado *Https*, es necesario generar un certificado no firmado con *Openssl*. Añadiendolo a la conexión hemos conseguido que esta sea segura y privada.



Creación de un gestor de contraseñas con arquitectura cliente/servidor cuyo almacenaje sea en el servidor y que permita su acceso desde distintos clientes remotos.

Características que debe cumplir:

- [x] El mecanismo de autentificación debe ser seguro.
- [x] Usar un transporte de red seguro entre cliente y servidor.
- [ ] Conocimiento Cero.

Conocimiento Cero

A la hora del envío de la contraseña

El cliente realiza el hash a la contraseña y a continuación el envío de una parte de este y de esta forma, el servidor en ningún momento conoce nuestra contraseña.

* Próximamente realizaremos conocimiento cero, para los siguientes objetivos a desarrollar.

Creación de un gestor de contraseñas con arquitectura cliente/servidor cuyo almacenaje sea en el servidor y que permita su acceso desde distintos clientes remotos.

Características que debe cumplir:

- El mecanismo de autentificación debe ser seguro.
- Usar un transporte de red seguro entre cliente y servidor.
- Conocimiento Cero.

Estado actual de la implementación

Gestor de contraseñas

- Cliente
  - Registro
  - Inicio sesión
  - ~~Guardar contraseñas~~
  - ~~Hacer consultas~~
- Servidor
  - Guardar usuario y contraseña del cliente
  - Realizar la autentificación
  - ~~Guardar el archivo de contraseñas y devolverlo cuando el cliente haga una consulta~~

Objetivos a desarrollar

Objetivos a desarrollar...

- Generación de contraseñas aleatorias y por perfiles.
- Incorporación de datos adicionales.
- Cifrado del fichero de contraseñas en el servidor.
- Optimización de la privacidad.

¡GRACIAS POR VUESTRA ATENCIÓN!

¿PREGUNTAS?