Universidad Gerardo Barrios

Facultad de Ciencia y Tecnología

Ingeniería en Sistemas y Redes Informáticas

Asignatura: Programación Computacional III

Docente: William Alexis Montes Girón

Título: Laboratorio 1 – tercer computo – función principal proyecto final

Alumno:

Oscar René Palacios Franco Código: SMSS065523

Nelson Oswaldo Alvarenga Cuadra Código: SMSS127921

Gerson Manases Flores Quinteros Código: SMSS040923

Kilmar Vladimir Bonilla Alfaro Código: SMSS093723

Planteamiento del problema

En la actualidad, la seguridad en línea es una preocupación creciente debido al aumento de ataques cibernéticos y violaciones de datos. Muchas personas tienden a utilizar contraseñas débiles o repetidas en múltiples cuentas, lo que aumenta el riesgo de que sus datos personales y financieros sean vulnerados en caso de un ataque. Además, recordar una gran cantidad de contraseñas seguras y complejas puede ser complicado para los usuarios, así como también, pensar en contraseñas "seguras" puede ser algo que genere dudas como ¿Qué es una contraseña segura?, ¿Cuántos dígitos debe de llevar? ¿Qué caracteres debe incluir?, etc.

El objetivo de este proyecto es desarrollar un gestor de contraseñas que permita a los usuarios generar y almacenar contraseñas seguras de manera fácil y organizada. Para garantizar la protección de las contraseñas almacenadas, van a pasar a ser encriptadas antes de guardarse en una base de datos local. De este modo, el gestor no solo facilita la creación y manejo de contraseñas fuertes, sino que también las protege contra accesos no autorizados en caso de que la base de datos sea comprometida.

Usando librerías como secrets ya que permite generar contraseñas seguras y aleatorias sin patrones que se puedan adivinar, usando pycryptodome para encriptar las contraseñas generadas, con una interfaz simple pero muy bien entendible para cualquier publico de cualquier edad todo gracias a la librería PyQt5 y PyQt Designer. También, el usuario podrá editar a su manera la contraseña generada para más personalización del usuario.

Todo esto incluido permitirá que el usuario pueda personalizar su contraseña o mantener nuestra contraseña generada de manera que tendrá un alto grado de nivel de confianza, usando las políticas ISO para la creación de contraseñas y al mismo tiempo tener un lugar seguro donde almacenar las contraseñas de manera encriptada y no tener que recordar cada contraseña diferente.

Avances del proyecto

El proyecto esta en fase de inicio aun, básicamente, la funcionalidad principal de nuestro proyecto esta realizada que es la creación de una contraseña completamente aleatoria usando la librería secrets básicamente con la librería Strings definimos que tipos de caracteres queremos que incluya en la generación de nuestra contraseña en nuestro caso letras, número y símbolos haciendo que la contraseña sea mas segura. Después usamos la librería secrets que con su modulo choice elige de todos esos caracteres según la longitud (en nuestro caso doce dígitos). Y muestra la contraseña generada en un LineEdit donde el usuario tiene la capacidad de poder editar esta contraseña generada pudiendo personalizarla mas o si en caso no es conveniente esa contraseña poder generar una nueva.

Funcionalidades implementadas:

- Generación de contraseña segura usando Secret y String.

Objetivos Faltantes

Los componentes faltantes de nuestro proyecto son básicamente dos la encriptación de la contraseña generada y el guardado de esta en la base de datos. El porcentaje aproximado avanzado de nuestro proyecto es del 40% debido a que la funcionalidad principal esta lista. Para la parte de encriptar la contraseña generada pensamos utilizar pycryptodome que es una librería de python la cual contiene muchos métodos de poder encriptarla a nuestro criterio es la librería más apta para este tipo de usos y para guardar nuestra contraseña generada en MySQL pensamos usar la librería mysql-connector-python es de las librerías mas usadas para este tipo de uso y muy sencilla de utilizar.

Estos elementos complementaran a que nuestro usuario pueda almacenar de una manera muy segura su contraseña en nuestros servidores para luego poder visualizarla en la misma aplicación y evitar la molestia de estar recordando cada contraseña.