Empresa BM
SOLUTIONS

MANUAL TÉCNICO DE SOFTWARE DE GENERADOR DE CONTRASEÑAS

Fecha: Noviembre 2024

Autor: Departamento de Ingeniería de Software

Contenido

1. Introducción

Objetivo

Este manual técnico tiene como objetivo proporcionar instrucciones detalladas para la instalación, configuración y uso del Programa de Generador de Contraseñas SecurePass, a fin de garantizar una implementación adecuada que optimice la seguridad de las contraseñas almacenadas. A lo largo de este documento, el usuario encontrará guías paso a paso para cifrar contraseñas de forma efectiva, asegurando que permanezcan inaccesibles a personas no autorizadas y cumplan con los estándares de seguridad de la información.

Alcance

Este manual abarca el proceso completo de instalación, configuración inicial y resolución de problemas básicos del Programa de Generado de Contraseñas SecurePass. No incluye configuraciones avanzadas ni personalizaciones específicas.

Público Objetivo:

Este manual está dirigido a usuarios con conocimientos básicos de informática, así como a técnicos de soporte que requieran asegurar la protección y gestión de contraseñas de manera eficiente.

Advertencias

Este software debe instalarse exclusivamente en sistemas que cumplan con los requisitos mínimos especificados en este manual. La instalación en entornos no compatibles puede comprometer el funcionamiento y la seguridad del programa.

2. Descripción General del Sistema

El Programa de Generador de Contraseñas SecurePass es una herramienta diseñada para gestionar de manera segura las contraseñas de los usuarios mediante la creación y cifrado avanzado de contraseñas. Además, proporciona funcionalidades colaborativas y análisis de seguridad para asegurar una óptima protección de los datos sensibles. Sus principales características incluyen:

- **Gestión de Tareas:** Permite la creación, almacenamiento y cifrado seguro de contraseñas, asegurando que cada contraseña esté protegida mediante algoritmos de alta seguridad.
- **Colaboración:** Facilita la creación de contraseñas seguras en distintos entornos, brindando recomendaciones y ayudando a los usuarios a mantener contraseñas robustas allí donde las necesiten, optimizando la seguridad de las cuentas y accesos.
- **Análisis de Datos:** Proporciona sugerencias de mejora y frecuencia de cambios recomendados para mantener un entorno seguro.

3. Requisitos Previos

Requisitos de Hardware:

- **Procesador**: Intel Core i3 de novena generación o superior; AMD Ryzen 3 o superior.
- **Memoria RAM:** 4 GB o más.
- **Espacio en disco:** 500 MB disponibles para la instalación del programa.

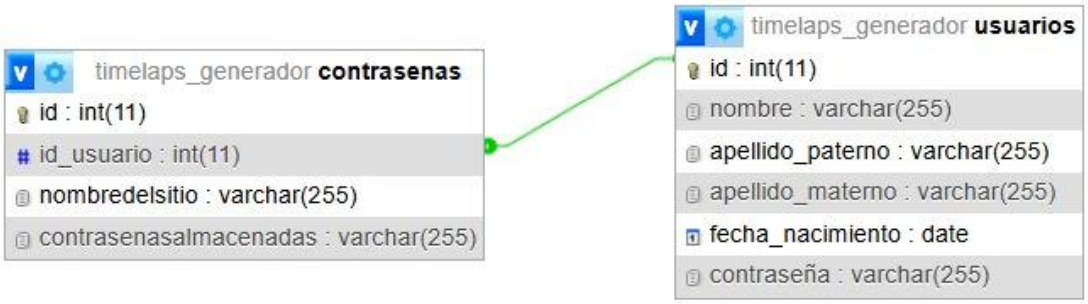
Requisitos de Software:

- **Sistema Operativo:** Windows 10 o versiones superiores.
- **Conexión a Internet**

  Necesaria para la instalación, actualización y funcionamiento del programa en tiempo real

3.1. Base de Datos de Almacenamiento de Contraseñas

Descripción de la Base de Datos



1. **usuarios**: Almacena la información de los usuarios registrados en el sistema. Incluye datos personales y la contraseña encriptada usando el algoritmo Argon2, reconocido por su robustez y seguridad frente a ataques. La estructura de la tabla es la siguiente:
    - **id** (INT, Primary Key): Identificador único de cada usuario.
    - **nombre** (VARCHAR): Nombre del usuario.
    - **apellido_paterno** (VARCHAR): Apellido paterno del usuario.
    - **apellido_materno** (VARCHAR): Apellido materno del usuario.
    - **fecha_nacimiento** (DATE): Fecha de nacimiento del usuario.
    - **contraseña** (VARCHAR): Contraseña encriptada del usuario. Se usa Argon2 para asegurar un almacenamiento seguro de la contraseña.
2. **contrasenas**: Gestiona las contraseñas almacenadas de distintos sitios web asociados al usuario. Esta tabla permite que cada usuario guarde sus contraseñas cifradas de diferentes sitios, facilitando la recuperación segura de información cuando sea necesario.
    - **id** (INT, Primary Key): Identificador único de cada contraseña almacenada.

- **id_usuario** (INT, Foreign Key): Referencia al usuario dueño de esta contraseña.
- **nombredelsitio** (VARCHAR): Nombre del sitio o servicio para el cual se almacena la contraseña.
- **contrasenasalmacenadas** (VARCHAR): Contraseña cifrada correspondiente al sitio especificado.

3.2. Elección del Sistema de Base de Datos

Para gestionar el almacenamiento de contraseñas de manera centralizada y segura, *SecurePass* utiliza **phpMyAdmin** como interfaz para administrar la base de datos. phpMyAdmin facilita la administración de bases de datos MySQL o MariaDB, permitiendo al equipo técnico realizar configuraciones, respaldos y mantenimientos de forma eficiente a través de una interfaz gráfica intuitiva.

Esta elección de sistema permite a *SecurePass* una administración robusta y segura de los datos, y también ofrece flexibilidad para realizar ajustes y consultas avanzadas.

Funcionalidad

- **Login Seguro**: Utiliza la tabla usuarios para autenticar a los usuarios mediante una contraseña encriptada.
- **Gestor de Contraseñas**: Permite a los usuarios almacenar y recuperar contraseñas seguras de múltiples sitios.

3.3. Seguridad de la Base de Datos

1. **Cifrado de datos**: Todos los datos en la base de datos están cifrados mediante **Argon2**, asegurando que las contraseñas y otros datos sensibles no puedan ser accedidos sin la clave de descifrado.
2. **Protección de integridad**: Se realizan verificaciones de integridad periódicas para prevenir la corrupción de datos y asegurar que los registros de contraseñas se mantienen intactos.

3. **Autenticación de acceso**: Para acceder a la base de datos a través de phpMyAdmin, se requiere autenticación mediante credenciales seguras. Además, para acceder a las contraseñas almacenadas, es necesaria una **contraseña maestra**, lo que garantiza que solo usuarios autorizados puedan ver la información sensible.

3.4. Ubicación y Respaldo de la Base de Datos

- **Ubicación**: La base de datos se almacena en un servidor seguro gestionado a través de phpMyAdmin. El servidor está configurado para limitar accesos externos y proteger los datos almacenados.

- **Respaldo**: Es fundamental realizar copias de seguridad de la base de datos semanalmente a través de phpMyAdmin. Estas copias de seguridad también estarán cifradas, protegiendo los datos incluso en caso de pérdida o acceso no autorizado.

4. Instrucciones de Instalación

1. Se le proporcionara un archivo ejecutable a el usuario

2. Ejecutar el archivo Generador de contraseñas.exe.

3. Seguir las instrucciones en pantalla para seleccionar el directorio de instalación**.**

4. Completar la instalación y reiniciar el sistema si es necesario.

5. Código

Generador de 500 palabras

Paso 1: Importación de módulos

- **random**: Se utiliza para realizar selecciones aleatorias, como la longitud de las cadenas y los caracteres individuales dentro de ellas.

- **string**: Contiene constantes útiles como ascii_letters (que incluye todas las letras del alfabeto, tanto mayúsculas como minúsculas) y punctuation (una lista de caracteres de puntuación estándar).

Paso 2: Estructura de la lista

El objetivo es crear una lista de 500 cadenas aleatorias, donde cada cadena tiene una longitud variable y consiste en caracteres seleccionados al azar. Esto se logra utilizando una **comprensión de listas**, que permite crear listas en una sola línea de código de forma eficiente y concisa.

```
# 500 palabras tipo XKCD generadas aleatoriamente
xkcd_palabras = [
    ''.join(random.choice(string.ascii_letters + string.punctuation)
            for _ in range(random.randint(5, 10)))
    for _ in range(500)
]
```

Generar contraseña por medio de los campos

- **Validación Inicial**: Se verifica que todos los campos requeridos estén completos. Si no lo están, se muestra un mensaje de error y se termina la función.
- **Longitud de Contraseña**: El usuario selecciona la longitud deseada desde un menú desplegable.
- **Entradas Utilizadas**: Se toman datos ingresados (nombre, apellidos, fecha de nacimiento, canción favorita, nombre de mascota) como base para generar la contraseña.
- **Proceso de Generación**:

- Se seleccionan caracteres aleatorios de los campos ingresados.
- Se mezclan mayúsculas, minúsculas y símbolos.
- Se repite hasta alcanzar la longitud deseada.
- **Salida**: La contraseña generada se muestra en la interfaz y se ofrece al usuario la opción de guardarla.
- **Evaluación**: Se analiza la seguridad de la contraseña generada.

```
def generate_password(self):
        """Genera una contraseña segura basada en los campos ingresados."""
        if not self.validate_fields():
            self.show_error("Debes completar todos los campos.")
            return

        length = int(self.password_length.currentText())
        all_fields = [
            self.name_input.text(), self.paternal_lastname_input.text(),
            self.maternal_lastname_input.text(),
self.birthdate_input.text(),
            self.song_input.text(), self.pet_input.text()
        ]

        # Generar contraseña a partir de los campos ingresados
        password = ''
        while len(password) < length:
            random_field = random.choice(all_fields)
            random_char = random.choice(random_field)
            password += random_char.upper() if random.random() > 0.5 else
random_char.lower()
            if len(password) < length and random.random() > 0.7:
                password += random.choice(string.punctuation)

        self.password_result.setText(password[:length])
        self.evaluate_security(length)
        self.ask_to_save_password(password[:length])
```

Generador de contraseñas XKCD

- **Longitud de Contraseña**: El usuario selecciona la longitud deseada mediante un menú desplegable.
- **Palabras Fuente**: Se utiliza una lista predefinida (xkcd_palabras) que contiene palabras generadas previamente.
- **Proceso de Generación**:

- Se seleccionan palabras aleatorias de xkcd_palabras.
- Las palabras se concatenan hasta que la longitud total de la contraseña cumpla o exceda la longitud especificada.

- **Ajuste Final**:

- La contraseña se recorta a la longitud exacta seleccionada por el usuario.
- Se muestra la contraseña en la interfaz.

- **Evaluación y Almacenamiento**:

- Se evalúa la seguridad de la contraseña generada.
- Se ofrece la opción de guardar la contraseña.

```
def generate_xkcd_password(self):
        """Genera una contraseña tipo XKCD respetando la longitud
seleccionada."""
        length = int(self.password_length.currentText())
        words = []
        while len(''.join(words)) < length:
            words.append(random.choice(xkcd_palabras))

        password = ''.join(words)[:length]
        self.password_result.setText(password)
        self.evaluate_security(length)
        self.ask_to_save_password(password)
```

PHP asegurando el encryptado en Argon 2

- **Cifrado de Contraseña**:

  Utiliza el algoritmo Argon2ID para cifrar la contraseña ingresada, garantizando un almacenamiento seguro.

- **Inserción en Base de Datos**:

  Realiza una consulta SQL para insertar los datos en la tabla usuarios con los campos: nombre, apellido_paterno, apellido_materno, fecha_nacimiento, y contraseña.

  Usa consultas preparadas para evitar inyecciones SQL.

```php
        // Hash de la contraseña usando Argon2
        $contraseña_hashed = password_hash($contraseña, PASSWORD_ARGON2ID);

        // Consulta SQL para insertar los datos del usuario
        $sql = "INSERT INTO usuarios (nombre, apellido_paterno,
apellido_materno, fecha_nacimiento, contraseña)
                VALUES (?, ?, ?, ?, ?)";

        log_error("Ejecutando consulta: $sql", [
            'nombre' => $nombre,
            'apellido_paterno' => $apellido_paterno,
            'apellido_materno' => $apellido_materno,
            'fecha_nacimiento' => $fecha_nacimiento,
            'contraseña' => $contraseña_hashed
        ]);

        // Preparar la consulta y ejecutarla
        $stmt = $conn->prepare($sql);
        $stmt->execute([
            $nombre,
            $apellido_paterno,
            $apellido_materno,
            $fecha_nacimiento,
            $contraseña_hashed
        ]);

        echo "Usuario registrado exitosamente.";

    } catch (PDOException $e) {
        log_error("Error en el registro: " . $e->getMessage(), $_POST);
        echo "Error en el registro: " . $e->getMessage();
    }
}
```

6. Configuración Inicial

1. Abrir el software y seleccionar “ejecutar”.
2. Tiene una instalación automática

7. Guía de Uso

Creación de Contraseñas Cifradas:

1. Iniciar sesión.
2. Genera tu contraseña de manera aleatoria o con unos campos específicos dentro de la aplicación.
3. Especificar el nivel de seguridad deseado (longitud de la contraseña).
4. Hacer clic en "Generar". El programa creará una contraseña con los datos especificados, contiene otro botón de “Generar” pero este es una contraseña aleatoria.
5. Guardar la contraseña para que se almacene en la base de datos segura del programa.

8. Mantenimiento y Actualización

Actualización:

Las actualizaciones que se hagan respecto a esta aplicación serán notificadas por nuestro equipo de software a el usuario.

Mantenimiento:

1. **Verificar integridad del sistema**: Cada seis meses, revisa la integridad del sistema. Esto incluye asegurarte de que todas las contraseñas se sincronicen correctamente y que no haya datos corruptos.

9. Solución de Problemas

Error al iniciar el software:

1. **Requisitos del sistema**: Asegúrate de que el dispositivo cumpla con los requisitos mínimos de hardware y software especificados en la documentación del producto.
2. **Reinstalación**: Si el problema persiste, desinstala el software y vuelve a instalarlo desde la fuente oficial.
3. **Permisos de acceso a internet**: Verifica que la aplicación tenga los permisos necesarios para acceder a Internet en la configuración de tu dispositivo.

10. Anexos

Glosario:

- **Cifrado**: Proceso de convertir información en un código para proteger su contenido.
- **Contraseña maestra**: Contraseña principal que permite acceder a todas las contraseñas almacenadas.
- **Autenticación de dos factores (2FA)**: Método de seguridad que requiere dos formas de identificación antes de acceder a la cuenta.

Documentos de referencia:

- **Manual de usuario**: Instrucciones detalladas sobre cómo usar la aplicación.
- **Especificaciones técnicas**: Detalles sobre los requisitos del sistema y capacidades del software.

11. Elección del Algoritmo y Pruebas de Seguridad

Elección del Algoritmo de Cifrado

Para el programa *SecurePass*, se ha seleccionado el **algoritmo de derivación de claves Argon2** debido a su alta seguridad y eficiencia. Argon2 es actualmente uno de los algoritmos de hash más seguros y recomendados para el almacenamiento de contraseñas, diseñado específicamente para resistir ataques de fuerza bruta y de diccionario. Su estructura optimiza el uso de memoria y procesamiento, haciendo que sea difícil de vulnerar incluso en sistemas con recursos avanzados, cumpliendo así con los estándares de seguridad requeridos.

Pruebas de Seguridad Realizadas

1. **Verificación de la seguridad de las contraseñas generadas**: Se revisó que las contraseñas generadas automáticamente por el sistema cumplen con los criterios de seguridad más estrictos, incluyendo longitud mínima, combinación de caracteres especiales, números y letras mayúsculas/minúsculas. Estas características aseguran que las contraseñas sean seguras y confiables, con alta resistencia a ataques de fuerza bruta.

2. **Prueba de resistencia a ataques de fuerza bruta**: Aunque Argon2 está diseñado para dificultar ataques de fuerza bruta, se realizaron simulaciones adicionales para confirmar su efectividad en entornos de prueba, asegurando que sin la clave adecuada el descifrado sea inviable.

3. **Prueba de cifrado y descifrado**: Se verificó que los datos cifrados con Argon2 puedan ser descifrados correctamente solo con la clave adecuada, asegurando la integridad del proceso de cifrado.

4. **Simulaciones de ataques de intermediario (Man-in-the-Middle)**: Se realizaron pruebas para confirmar que la información protegida por el cifrado Argon2 se mantiene segura durante su transmisión y almacenamiento, impidiendo el acceso no autorizado.

Este análisis y las pruebas de seguridad realizadas aseguran que el software *SecurePass* cumple con los estándares necesarios para proteger la información sensible de los usuarios y ofrece contraseñas seguras y confiables.

12. Contactos y Soporte Técnico

- **Correo de soporte**: bmsolutions2024@gmail.com
- **Teléfono**: +52 7752539970
- **Horario de soporte**: Lunes a Viernes de 9:00 a 20:00