Gestionnaire de mots de passes

Description

Un gestionnaire de mots de passe est une application qui permet aux utilisateurs de stocker de manière sécurisée leurs identifiants de connexion, mots de passe et autres informations sensibles. Voici quelques fonctionnalités à intégrer à un gestionnaire de mots de passe :

1. **Stockage sécurisé :** Les mots de passe doivent être stockés de manière sécurisée, généralement chiffrés, pour garantir la confidentialité des informations.
2. **Génération de mots de passe :** Ajoutez une fonctionnalité qui permet aux utilisateurs de générer des mots de passe forts et aléatoires.
3. **Organisation par catégories :** Permettez aux utilisateurs de regrouper leurs mots de passe par catégories (par exemple, sites Web, applications, services bancaires) pour une meilleure organisation.
4. **Recherche :** Intégrez une fonction de recherche pour permettre aux utilisateurs de trouver rapidement un mot de passe spécifique parmi leurs enregistrements.
5. **Modification sécurisée :** Assurez-vous que les utilisateurs peuvent modifier leurs informations en toute sécurité, avec des mécanismes pour confirmer leur identité avant de pouvoir effectuer des modifications.
6. **Synchronisation et sauvegarde :** Proposez une fonctionnalité de sauvegarde et de synchronisation pour permettre aux utilisateurs d'accéder à leurs mots de passe depuis différents appareils.
7. **Gestion des notes :** En plus des identifiants de connexion, donnez aux utilisateurs la possibilité de stocker des notes sécurisées ou d'autres informations sensibles.
8. **Gestion des comptes multiples :** Permettez aux utilisateurs de gérer plusieurs comptes, chacun avec ses propres enregistrements de mots de passe.
9. **Sécurité renforcée :** Intégrez des mesures de sécurité telles que la déconnexion automatique après une période d'inactivité, la protection par mot de passe principal, etc.
10. **Journal d'activité :** Tenez un journal d'activité qui enregistre les modifications apportées aux mots de passe et les connexions récentes pour la sécurité et la traçabilité.

Itérations

Itération 1 - Fonctionnalités de base :

1. Interface en ligne de commande.
2. Ajout, modification et suppression de mots de passe.
3. Stockage local des mots de passe (non chiffré pour le moment).

Itération 2 - Sécurité de base :

1. Création d'une interface simple avec tkinter.
2. Chiffrement des mots de passe stockés.
3. Ajout d'une fonction de génération de mots de passe forts.
4. Implémentation d'une protection par mot de passe principal pour accéder à l'application.

Itération 3 - Organisation et Recherche :

1. Ajout de catégories pour organiser les mots de passe.
2. Possibilité de rechercher des mots de passe.
3. Amélioration de l'interface utilisateur pour une meilleure convivialité.

Itération 4 - Fonctionnalités avancées de sécurité :

1. Mise en place d'une déconnexion automatique après une période d'inactivité.
2. Enregistrement des actions de l'utilisateur dans un journal d'activité.
3. Possibilité de générer et enregistrer des notes sécurisées.

Itération 5 - Synchronisation et Sauvegarde :

1. Ajout de fonctionnalités de sauvegarde et de restauration.
2. Possibilité de synchroniser les données entre plusieurs appareils.
3. Amélioration de la sécurité des processus de sauvegarde et de synchronisation.

Itération 6 - Gestion avancée des comptes :

1. Prise en charge de plusieurs profils ou comptes d'utilisateur.
2. Possibilité de personnaliser les paramètres de sécurité pour chaque compte.
3. Améliorations de l'interface utilisateur pour la gestion des comptes multiples.

Itération 7 - Améliorations de l'interface utilisateur :

1. Modernisation de l'interface graphique avec des éléments visuels plus attrayants.
2. Améliorations ergonomiques basées sur les retours des utilisateurs.
3. Ajout de fonctionnalités de tri et de filtrage des mots de passe.

Itération 8 - Journal d'activité avancé :

1. Amélioration du journal d'activité avec des détails supplémentaires.
2. Ajout d'options de filtrage et de recherche dans le journal.
3. Intégration de notifications pour les activités importantes.

Itération 9 - Sécurité avancée :

1. Mise en place d'une vérification en deux étapes pour l'accès à l'application.
2. Améliorations continues de la sécurité en suivant les dernières pratiques.
3. Possibilité de régénérer des mots de passe pour renforcer la sécurité.

Itération 10 - Finalisation et Tests approfondis :

1. Tests approfondis de l'application pour détecter et résoudre les éventuels problèmes de sécurité.
2. Correction des bogues signalés par les utilisateurs et identification des dernières améliorations possibles.
3. Documentation complète de l'application et préparation pour le déploiement.