La Plateforme

Password

be2c41f44354eb8f5b15de515065e224f35f743de5e315039ae5372e1e1d9433

Contexte

Découvrez comment utiliser les fonctionnalités de la bibliothèque “**random**” pour créer des mots de passe aléatoires et forts, et comment utiliser des algorithmes de hachage pour stocker et vérifier ces mots de passe de manière sécurisée.

Ce sujet vous permettra d'aborder différentes techniques pour générer et sécuriser des mots de passe en Python, en utilisant notamment les modules “**random**” et “**hashlib**”. Vous pourrez ainsi apprendre à créer des mots de **passe aléatoires** et **forts** en utilisant des caractères spéciaux, des chiffres et des lettres, et à stocker ces mots de passe de manière sécurisée en utilisant des algorithmes de hachage tels que SHA-256 ou bcrypt.

Descriptif

Écrivez un programme Python qui demande à l'utilisateur de choisir un mot de passe, puis vérifie si ce mot de passe répond à certaines exigences de sécurité.

```
Veuillez entrer votre mot de passe :
```

Votre programme devra afficher un message d'erreur si le mot de passe choisi ne respecte pas ces exigences, et demander à l'utilisateur de choisir un nouveau mot de passe jusqu'à ce qu'il en choisisse un qui soit valide.

Voici les exigences de sécurité à respecter pour le mot de passe :

- Il doit contenir au moins 8 caractères.
- Il doit contenir au moins une lettre majuscule.
- Il doit contenir au moins une lettre minuscule.
- Il doit contenir au moins un chiffre.
- Il doit contenir au moins un caractère spécial (!, @, #, $, %, ^, &, *).
- Voici comment votre programme devrait fonctionner :

1. Demandez à l'utilisateur de choisir un mot de passe.
2. Vérifiez si le mot de passe choisi respecte les exigences de sécurité.
3. Si le mot de passe est valide, affichez un message de confirmation et quittez le programme.
4. Si le mot de passe n'est pas valide, affichez un message d'erreur et demandez à l'utilisateur de choisir un nouveau mot de passe.
5. Répétez les étapes 2 à 4 jusqu'à ce que l'utilisateur choisisse un mot de passe valide.

Maintenant, à l'aide de la librairie "Hashlib" et en utilisant l'algorithme de hachage SHA-256, écrire un programme qui crypte le mot de passe que l'utilisateur a entré précédemment.

... pour aller plus loin

Créer un programme qui permet de gérer les mots de passe renseigné par l'utilisateur en enregistrant les mots de passe hachés dans un fichier.

Le programme doit pouvoir permettre à l'utilisateur d'ajouter de nouveaux mots de passe ou d'afficher ces derniers.

Pour ce bonus, il est nécessaire d'utiliser la bibliothèque "**Json**" de python.

... pour encore aller plus loin

Comparer les mots de passe afin de ne pas avoir 2 fois le même mot de passe enregistré dans le fichier.

Rendu

Le projet est à rendre sur **https://github.com/prenom-nom/Password**.
Pensez à mettre votre repository en public !

Compétences visées

- Maîtriser les bases de python
- Implémenter un algorithme de chiffrement

Base de connaissances

- Sha 256