TP - Vérifier la fiabilité des mots de passe

Le site Have I Been Pwned? (HIBP - https://haveibeenpwned.com/) est un site web que les internautes peuvent consulter dans le but de vérifier si leurs données personnelles ont été compromises à la suite de violations de données. Le service recueille et analyse régulièrement des centaines d'exports de bases de données et de données texte, lesquelles comprennent des informations sur des milliards de comptes compromis.
Les internautes peuvent s'enregistrer pour recevoir une alerte en cas de compromission future. Le site a été largement loué pour sa pertinence pour les internautes qui souhaitent protéger leurs données en ligne ainsi que leur vie privée.

https://fr.wikipedia.org/wiki/Have_I_Been_Pwned%3F

Je vous encourage à vous inscrire sur ce site si ce n'est déjà fait.

Ce site haveibeenpwned permet également de vérifier si un mot de passe a été compromis, bien que le site semble fiable, il n'est pas conseillé de saisir son mot de passe sur un site internet, on ne sait pas ce que le propriétaire du site peut en faire (l'ajouter à la liste des mots de passe ? Tentez de vous pirater ?). Voici tout de même le lien, vous pouvez tester des mots de passe du genre : P@ssw0Rd, admin, 123456 …

https://haveibeenpwned.com/Passwords

Le créateur du site permet toutefois de vérifier son mot de passe sans devoir le saisir, comment ? En utilisant une empreinte (hash) du mot de passe en sha1.

Etape 1 : Générer un hash sha1 des mots de passe (ici "root")

-linux :

```
printf "root" |sha1sum
                ou
echo -n "root"|sha1sum  //-n permet de supprimer le saut de ligne final sans quoi le hash serait différent (/n)
```

-Windows powershell :

```
$stringAsStream = [System.IO.MemoryStream]::new()
$writer = [System.IO.StreamWriter]::new($stringAsStream)
$writer.write("root")
$writer.Flush()
$stringAsStream.Position = 0
Get-FileHash -InputStream $stringAsStream -Algorithm SHA1| Select-Object Hash
```

⇨ On obtient : dc76e9f0c0006e8f919e0c515c66dbba3982f785

Etape 2 : Recherche de notre empreinte dans la liste des empreinte

Là encore par sécurité, le site ne permet pas de chercher une emprunte directement, mais les 5 premiers caractères de l'emprunte (ainsi le site ne sait pas précisément quelle emprunte nous cherchons).

Adaptez l'url suivante en adaptant les 5 derniers caractères en fonction de votre empreinte :

https://api.pwnedpasswords.com/range/dc76e

Il ne vous reste plus qu'à rechercher sur la page votre empreinte complète et espérer ne pas la trouver ;-) Ici avec le mot de passe root vous allez forcément trouver votre empreinte.

Conclusion

Le mot de passe "root" a été trouvé 12 398 fois (au 25 novembre 2021) dans la base de données. Essayer avec un autre mot de passe pour voir la sécurité de celui-ci.