Rapport du devoir maison de Sécurité

BASUALDO Lautaro et LOI Léo

10 avril 2024

Table des matières

1 Exercice 1 :

Avant de pouvoir décrypter les deux mots de passes, nous devons déjà les identifier.
Or, nous savons que la fonction SHA-256 génèrera toujours le même haché pour un mot de passe donné.
Ainsi, nous pouvons détecter deux hachés différents :

- 068be8be83f9bfafd1545d357fd3cd132f8c659effd11e635a698811b796c880 (utilisé par Bart, Homer, Lisa et March)
- 15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225 (utilisé par Bob, Carlton, John et William)

Pour le premier haché, grâce aux différents indices, nous pouvons deviner que le mot de passe utilisé est le 74ème élément du tableau périodique des élements. A savoir le "tungstène" appelé en anglais "tungsten"
Afin de s'assurer de nos résultats, nous avons haché le mot "tungsten" avec la fonction de hachage SHA-256 ce qui donne le résultat suivant :

```
moi@moi-HP-245-G7-Notebook-PC:~$ echo -n 'tungsten' | openssl sha256
(stdin)= 068be8be83f9bfafd1545d357fd3cd132f8c659effd11e635a698811b796c880
```

Nous pouvons constater que les deux hachés sont similaire, le mot de passe utilisé par Bart, Homer, Lisa et March est donc bien "tungsten"

Pour le second haché, grâce aux différents indices, nous pouvons deviner que le mot de passe utilisé est la suite de chiffres "123456789"
Afin de s'assurer de nos résultats, nous avons haché le mot "123456789" avec la fonction de hachage SHA-256 ce qui donne le résultat suivant :

```
moi@moi-HP-245-G7-Notebook-PC:~$ echo -n '123456789' | openssl sha256
(stdin)= 15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225
```

Nous pouvons constater que les deux hachés sont similaire, le mot de passe utilisé par Bob, Carlton, John et William est donc bien "123456789"

2 Exercice 2 :

2.1 Question 1 :

Ci-dessous, une fonction python qui ajoute un utilisateur à une base de donnée grâce à un identifiant et un mot de passe qu'il fournit

```
def AjoutUtilisateur():
  connection = sqlite3.connect("donnees.db")
  curseur = connection.cursor()
  is_id_incorrect = True
  #tant que le login est deja utilise,
  #on demande a l'utilisateur de re-rentrer un login
  while is_id_incorrect:
    print("Choississez votre identitfiant :")
    id = input()
    res = curseur.execute("SELECT name FROM
       utilisateurs WHERE name = '"+id+"'")
    #si on n'a trouve aucun resultat,
    #le login n'existe pas dans la base de donnee
    if res.fetchone() is None:
      #on sort de la boucle
      is_id_incorrect = False
    else:
      #on redemande son identifiant a l'utilisateur
      print("L'identifiant est deja utilise, veuillez
         en saisir un autre")
  is_mdp_incorrect = True
  #tant que les deux entrees de l'utilisateurs ne
     correspondent pas,
  #on lui demande de re-rentrer un mot de passe et de
     le confirmer
  while is_mdp_incorrect:
    print("choisissez votre mot de passe :")
    mdp = input()
    print("Validez votre mot de passe :")
    mdp2 = input()
    #si les deux entrees correspondent
    if mdp == mdp2:
      #on sort de la boucle
      is_mdp_incorrect = False
    else:
      print("Vos entrees ne correspondent pas")
  #On ajoute l'utilisateur a la base de donnee
  curseur.execute("INSERT INTO utilisateurs VALUES('"+
     id+"','"+mdp+"')")
  connection.commit()
```

2.2 Question 2 :

Après plusieurs éxecutions du programme ci-dessus, les valeurs suivantes peuvent être récupérées dans la base de donnée

```
moi@moi-HP-245-G7-Notebook-PC:~$ python3 ajoutUtil.py
[('Leo', 'Motdepasse'), ('idRandom', 'mdpRandom')]
```

2.3 Question 3 :

```
def Verification():
  connection = sqlite3.connect("donnees.db")
  curseur = connection.cursor()
  print("Connexion :")
  is_not_connected = True
  #tant que le login et le mot de passe ne
     correspondent a aucune entree de la base de
     donnee, on demande a l'utilisateur d'en re-
     rentrer
  while is_not_connected:
    print("Entrez votre identifiant")
    id = input()
    print("Entrez votre mot de passe")
    mdp = input()
    res = curseur.execute("SELECT name FROM
       utilisateurs WHERE name = '" + id + "' AND
       password ='" + mdp +"'")
    if res.fetchone() is None:
      print("Mot de passe ou identifiant incorrect")
    #le login et le mot de passe correspondent a une
       entree de la base de donnee
    else:
      is_not_connected = False
  print("Bravo ! Vous etes connecte")
```

2.4 Question 4 :