Password Checker Tool

Introduction:

password checker tool is the tool used to check the user passwords on the internet either it is breached or not. If breached found then it will notify. It also generate SHA1 and MD5 of given password.

Project Objective:

Most of the users uses common password or their password may be breached and stored on online. So this tool checks the users password .At first it converts user password into encrypted form and checks the encrypted password is available in internet or not if password exists then it will notify and also suggest strong password .

Code:

import requests

import hashlib

import sys

import time

import random

from sqlalchemy import null

def request\_api\_data(query\_char):

url = 'https://api.pwnedpasswords.com/range/' + query\_char

print("Searching on web...")

time.sleep(5)

print("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*")

res = requests.get(url)

if res.status\_code != 200:

raise RuntimeError(

f'Request failed : {res.status\_code}. Please try again with different charater string')

else:

return res

def get\_hash\_leak\_count(hashes, hash):

hashes = (line.split(':') for line in hashes.text.splitlines())

for val, count in hashes:

if(hash == val):

return count

return 0

def pwned\_api\_check(password):

sha1password = hashlib.sha1(password.encode('utf-8')).hexdigest().upper()

md5password=hashlib.md5(password.encode('utf-8')).hexdigest().upper()

print("Encryption on process:")

time.sleep(5)

print("SHA1:",sha1password)

print("MD5:",md5password)

first\_5\_char, tail = sha1password[:5], sha1password[5:]

res = request\_api\_data(first\_5\_char)

return get\_hash\_leak\_count(res, tail)

def main(passwords):

count = pwned\_api\_check(passwords)

if(count):

print(

f'Alert entered password:{passwords} is already breached. It was found used {count} times...')

print("Suggestions:")

symbo=["@", "#", "$", "\_", "%", "&"]

charl = ["1", "2", "3", "4", "5", "6"]

charl2 = ["7", "8", "9", "0", "1", "2"]

char=random.choice(charl)

char2=random.choice(charl2)

sugges=char + random.choice(symbo) + passwords + char2

print("password: ",sugges)

else:

print(f'Sucess! This password not found in database !!You can use this password')

print("For Better Security we suggest:")

symbo=["@", "#", "$", "\_", "%", "&"]

charl = ["1", "2", "3", "4", "5", "6"]

charl2 = ["7", "8", "9", "0", "1", "2"]

char=random.choice(charl)

char2=random.choice(charl2)

sugges=char + random.choice(symbo) + passwords + char2

print("password: ",sugges)

if(\_\_name\_\_ == '\_\_main\_\_'):

print("Note: The password entered here is not saved in any server.")

passwords = input("Enter your password to check: ")

if(passwords==""):

print("Empty input is not accepted")

exit()

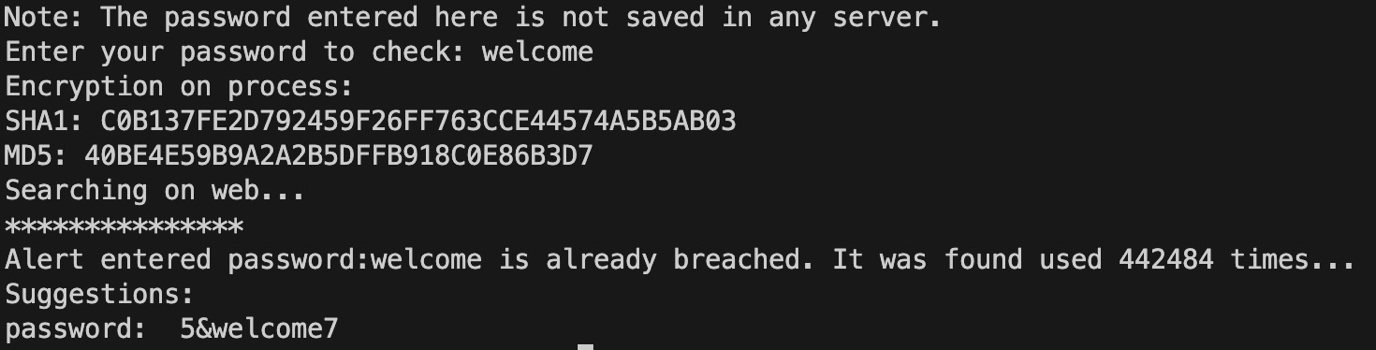
sys.exit(main(passwords))

OUTPUT:

Checking with custom easy password:



Checking with common password:



Checking with strong password:

