crackme-py

Medium Reverse Engineering picoCTF 2021

AUTHOR: SYREAL

Description

crackme_gen.py

Hints

(None)

Setelah didownload, buka program pythonnya dan muncul seperti ini :

```
bezos_cc_secret = "A:4@r%uL`>0c0Abc?FE0g`_47fgaagg6ffN"

# Reference alphabet
alphabet = "!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ"+ \
           "[\\]^_`abcdefghijklmnopqrstuvwxyz{|}~"



def decode_secret(secret):
    """ROT47 decode

    NOTE: encode and decode are the same operation in the ROT cipher family.
    """

    # Encryption key
    rotate_const = 47

    # Storage for decoded secret
    decoded = ""

    # decode loop
    for c in secret:
        index = alphabet.find(c)
        original_index = (index + rotate_const) % len(alphabet)
        decoded = decoded + alphabet[original_index]

    print(decoded)



def choose_greatest():
    """Echo the largest of the two numbers given by the user to the program

    Warning: this function was written quickly and needs proper error handling
    """

    user_value_1 = input("What's your first number? ")
    user_value_2 = input("What's your second number? ")
    greatest_value = user_value_1 # need a value to return if 1 & 2 are equal

    if user_value_1 > user_value_2:
        greatest_value = user_value_1
    elif user_value_1 < user_value_2:
        greatest_value = user_value_2

    print( "The number with largest positive magnitude is "
        + str(greatest_value) )



choose_greatest()
```

Kita fokus ke function decode_secret() nya yang mungkin merupakan fungsi untuk mendekode. Lalu kita bisa bikin fungsi untuk mereverse decodernya seperti berikut :

```
def reversing_secret(chiper):

   plaintext = ""
   for c in chiper:
       index_in_alphabet = alphabet.find(c) # 4
       temp_original_index = index_in_alphabet + len(alphabet) # 98
       reversed_original_index = (temp_original_index - 47) %
len(alphabet) #51
       reversed_char = alphabet[reversed_original_index]

       plaintext+=reversed_char

   return plaintext
```

Hasil fullnya seperti ini

```
alphabet =
"!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ"+ \
          "[\\]^_`abcdefghijklmnopqrstuvwxyz{|}~"

chipertext = "A:4@r%uL`>0c0Abc?FE0g`_47fgaagg6ffN"

def reversing_secret(chiper):

   plaintext = ""
   for c in chiper:
       index_in_alphabet = alphabet.find(c) # 4
       temp_original_index = index_in_alphabet + len(alphabet) # 98
       reversed_original_index = (temp_original_index - 47) %
len(alphabet) #51
       reversed_char = alphabet[reversed_original_index]

       plaintext+=reversed_char

   return plaintext
```

```
plaintext = reversing_secret(chipertext)
print(plaintext)
```

kita bisa run untuk mendapatkan flagnya.

Flag : picoCTF{1m_4_p34nut_810cf782288e77}