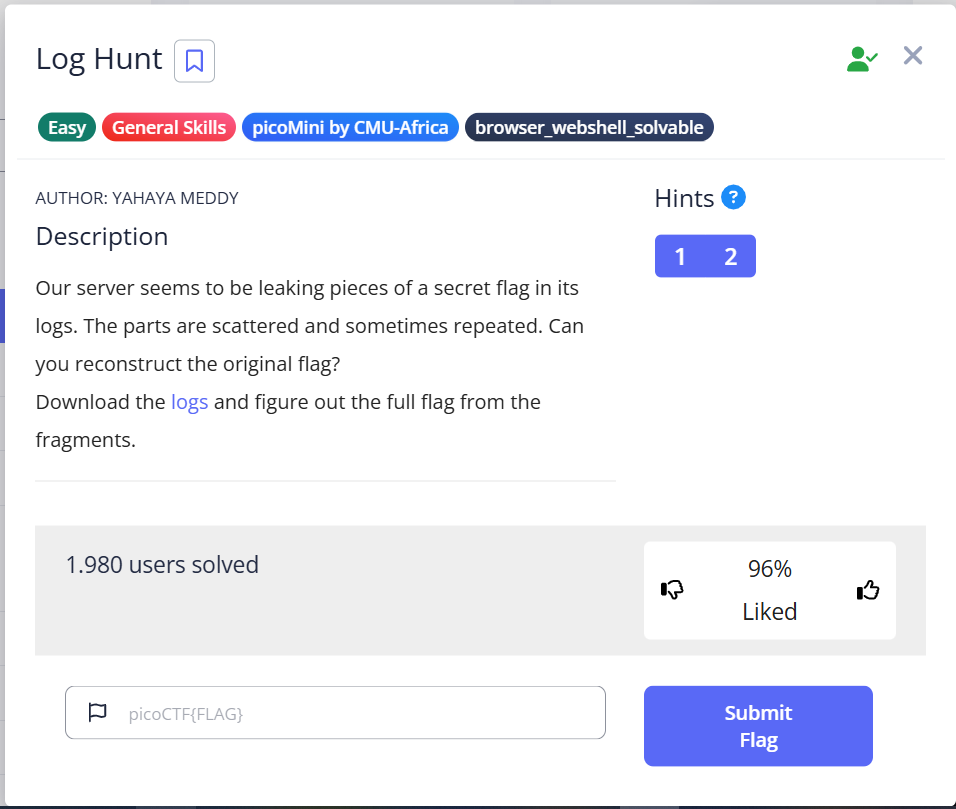
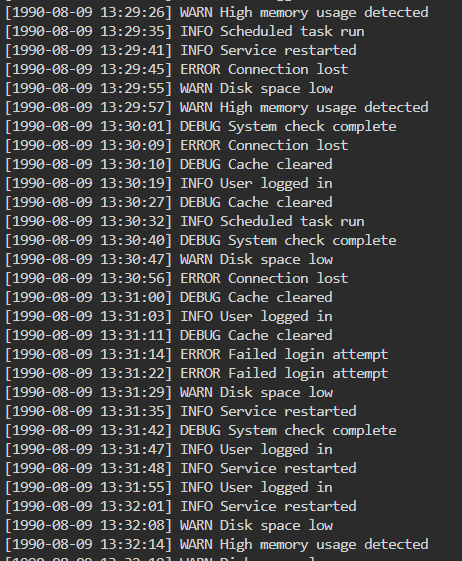
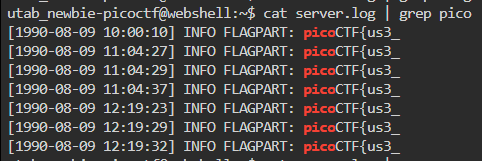
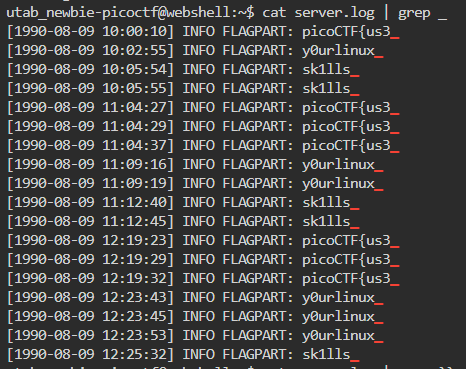
1. Log Hunt

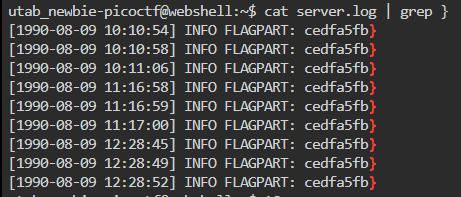


Diberikan sebuah file log yang dapat kita baca

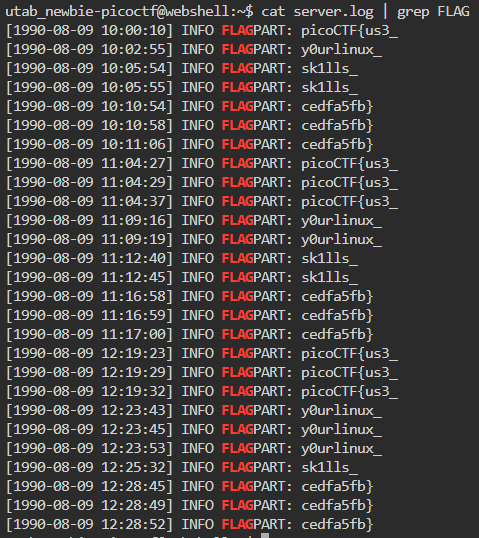


Langsung saja kita cari ciri khas sebuah flag dengan grep, dan flagnya pun didapatkan

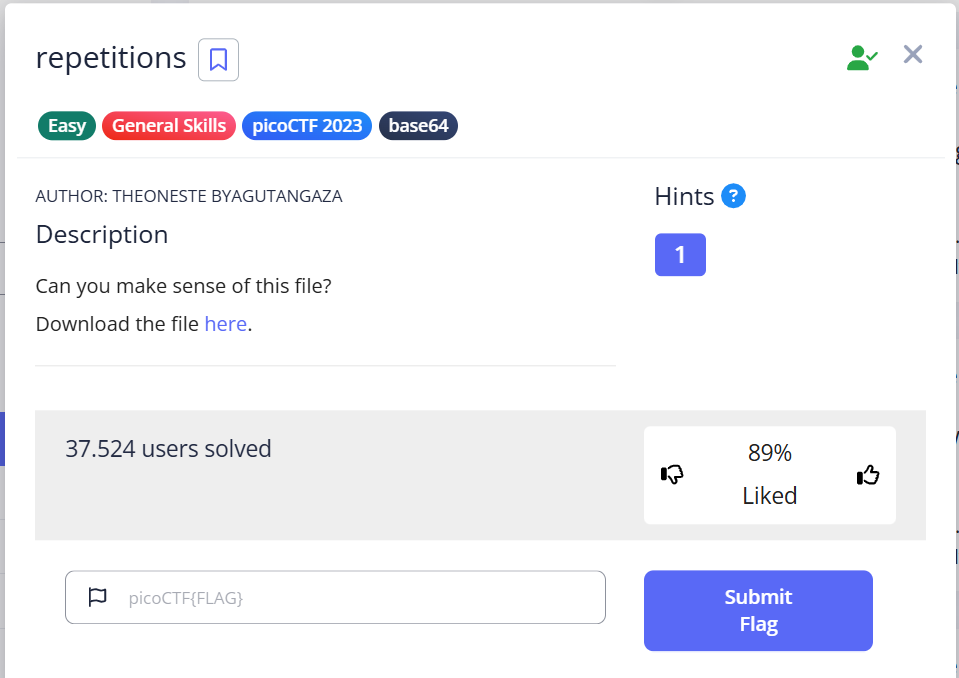


atau

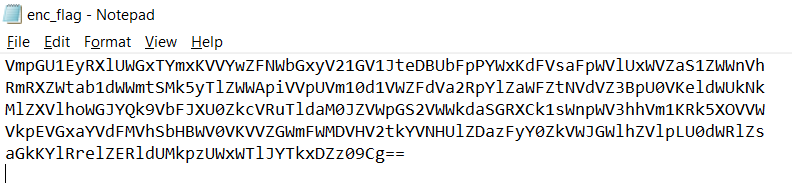


**Flag: picoCTF{us3\_y0urlinux\_sk1lls\_cedfa5fb}**

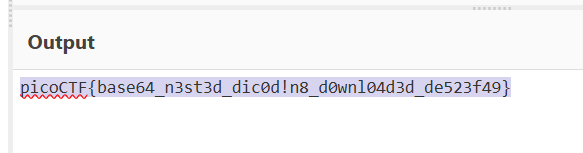
1. repetitions



Diberikan sebuah file yang isinya memiliki format base64

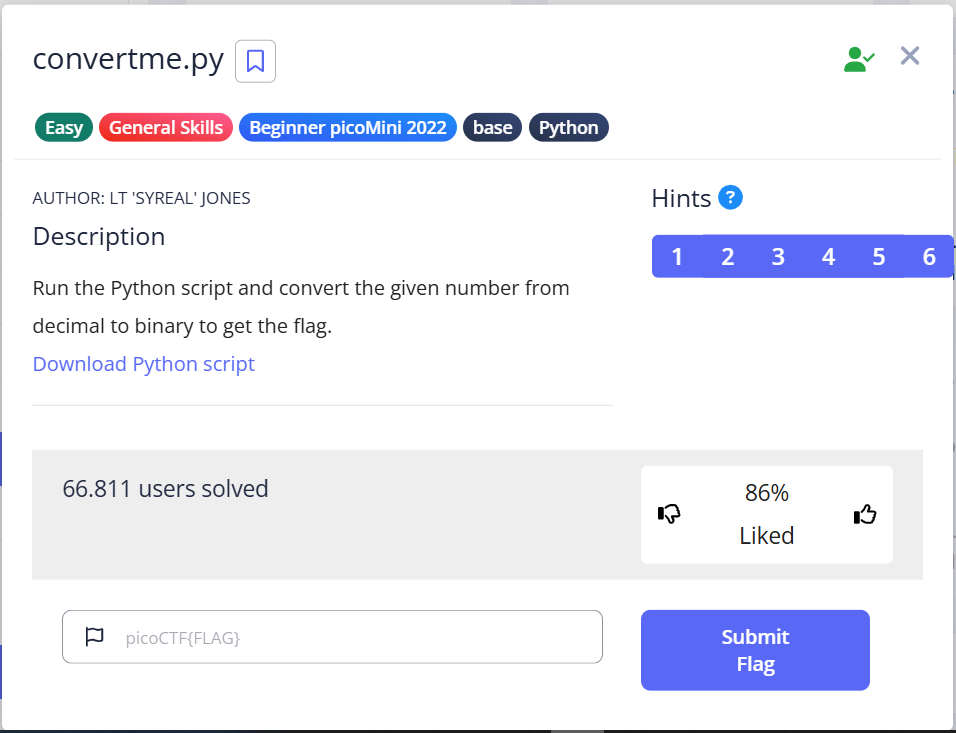


Langsung saja kita lakukan decode dengan base64 berulang kali dan didapatkanlah hasilnya

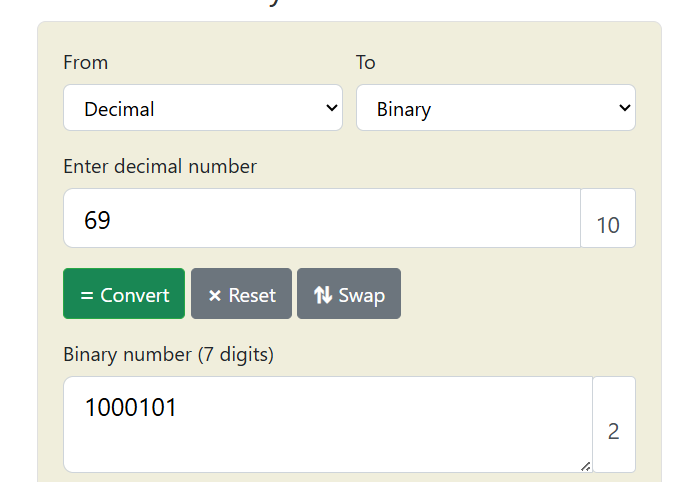


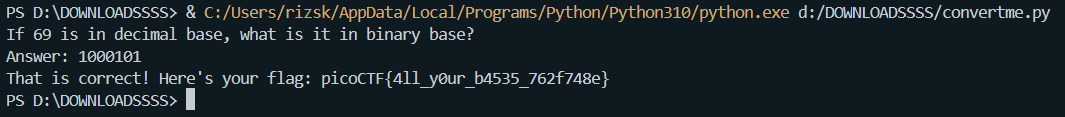
**Flag: picoCTF{base64\_n3st3d\_dic0d!n8\_d0wnl04d3d\_de523f49}**

1. convertme.py



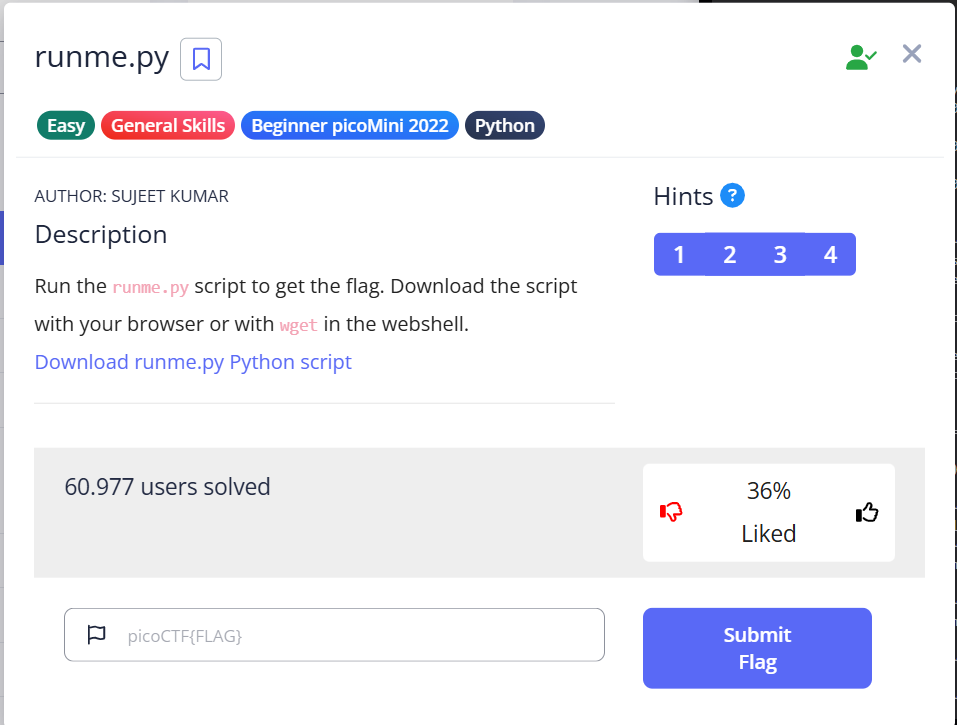
Diberikan sebuah file .py yang akan memberi pertanyaan/ perintah untuk mengubah sebuah bilangan decimal ke binary. Langsung saja kita gunakan tool online yang mengubah dari decimal ke binary, hehe

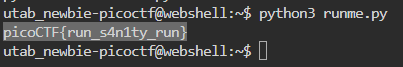




**Flag: picoCTF{4ll\_y0ur\_b4535\_762f748e}**

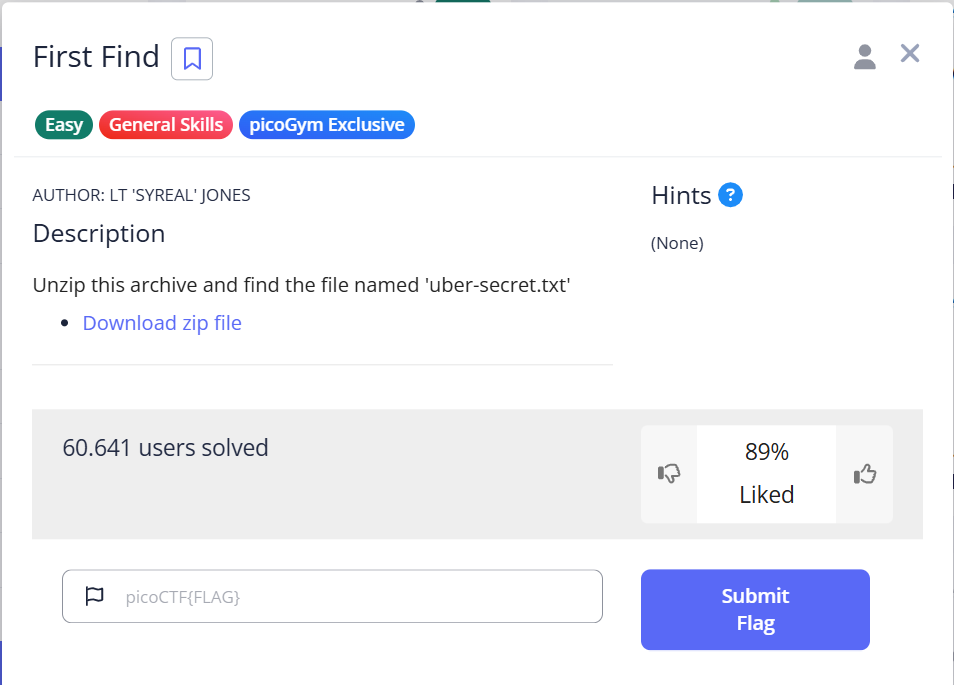
1. runme.py



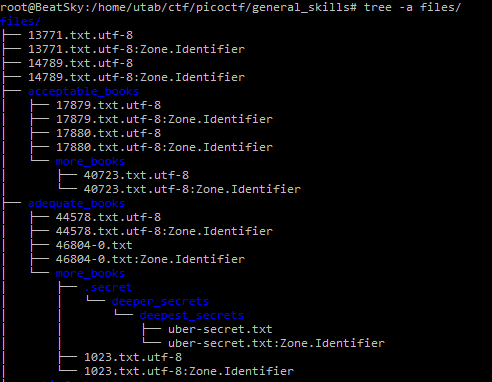
Diberikan sebuah chall... ini cuman disuruh running saja jirrr  


**Flag: picoCTF{t1m3m@ch1n3\_b476ca06}**

1. First find



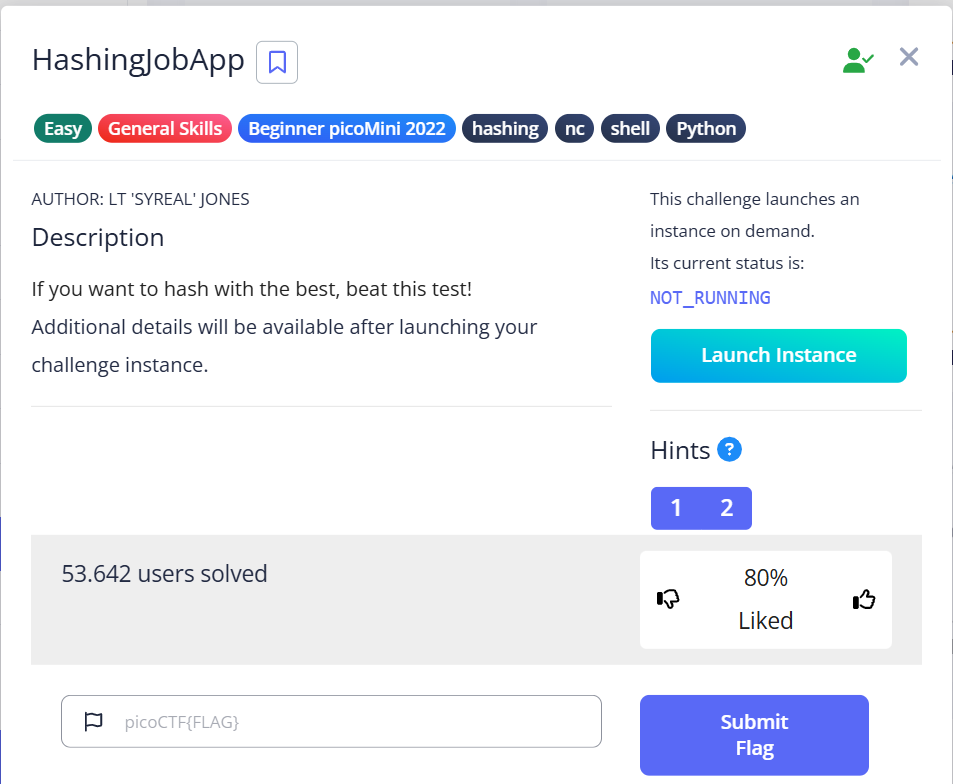
Diberikan sebuah file zip dan disuruh untuk mencari file bernama 'uber-secret.txt', langsung saja kita tree kan, dan ketemu hasilnya

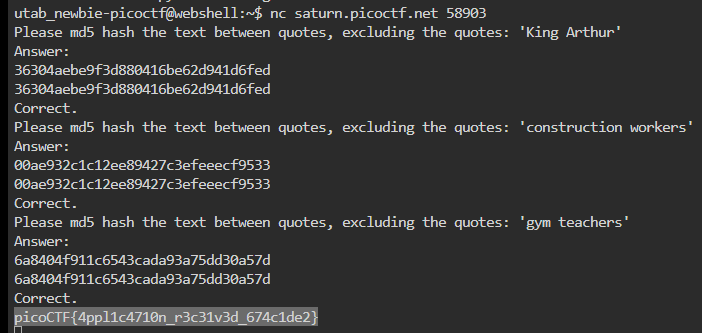




**Flag: picoCTF{f1nd\_15\_f457\_ab443fd1}**

1. HashingJobApp

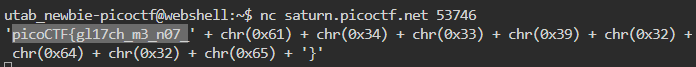


Diberikan sebuah chall, disini kita disuruh untuk melakukan md5 hashing beberapa text. Langsung saja kita lakukan dan dipatkan flagnya  


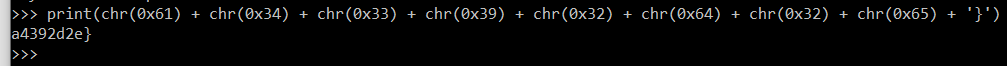
**Flag: picoCTF{4ppl1c4710n\_r3c31v3d\_674c1de2}**

1. Glitch Cat

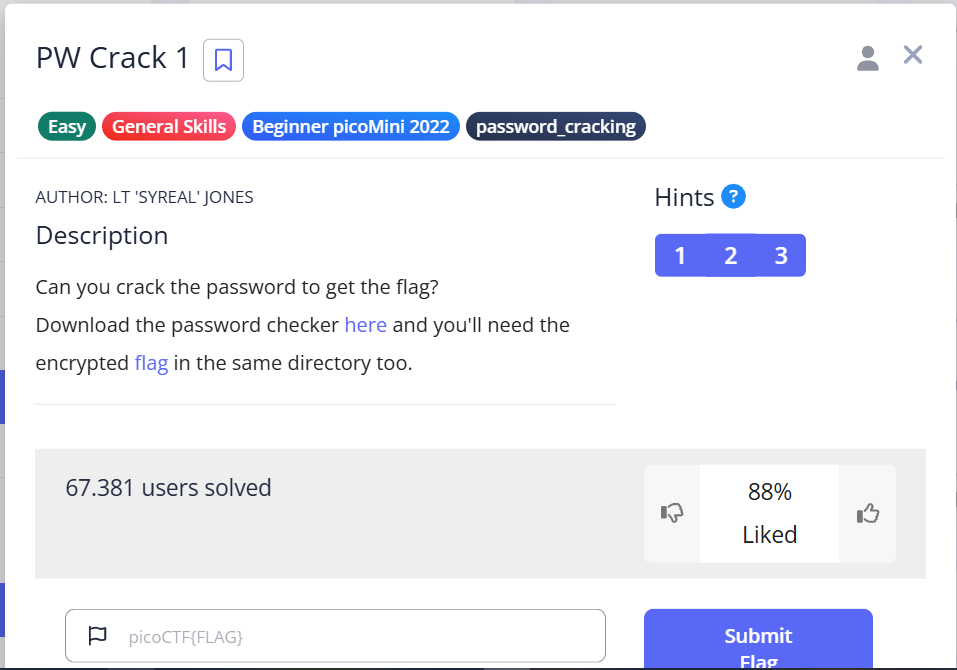
Diberikan sebuah koneksi yang mengirimkan semacam string human readable dan beberapa yang di ubah ke hexa.



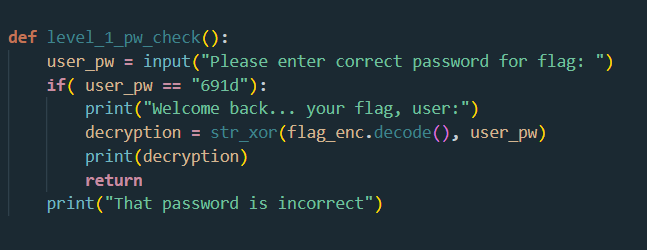
Langsung saja kita eksekusikan hex nya di python

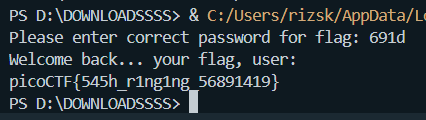


**Flag: picoCTF{gl17ch\_m3\_n07\_a4392d2e}**

1. PW crack 1  
   

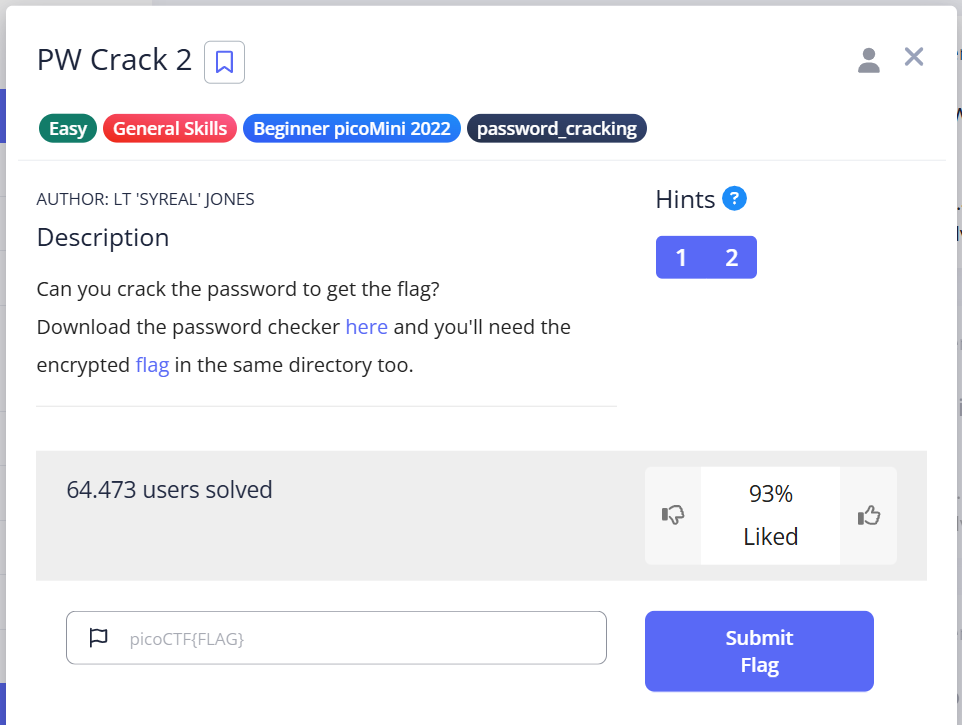
Diberikan sebuah chall dengan 2 file yakni script untuk membuka file nya dan flag yang terenkripsi.



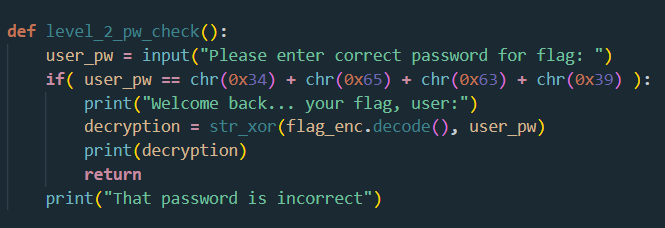
Saat dilihat codenya, ternyata password yang dibutuhin itu hardcoded, jadi langsung saja kita masukkan passwordnya  


**Flag: picoCTF{545h\_r1ng1ng\_56891419}**

1. PW crack 2



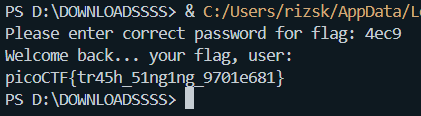
Sama kayak yang sebelumnya, masih di hard code si pw nya, tapi di obfuscate sedikit yak ges ya



Langsung saja kita ubah dengan python

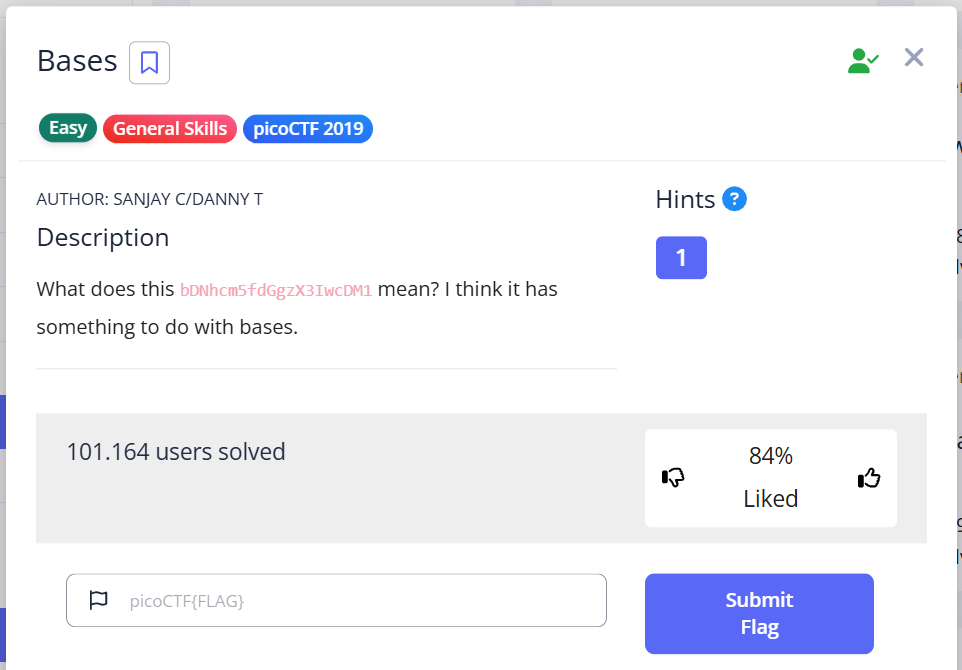


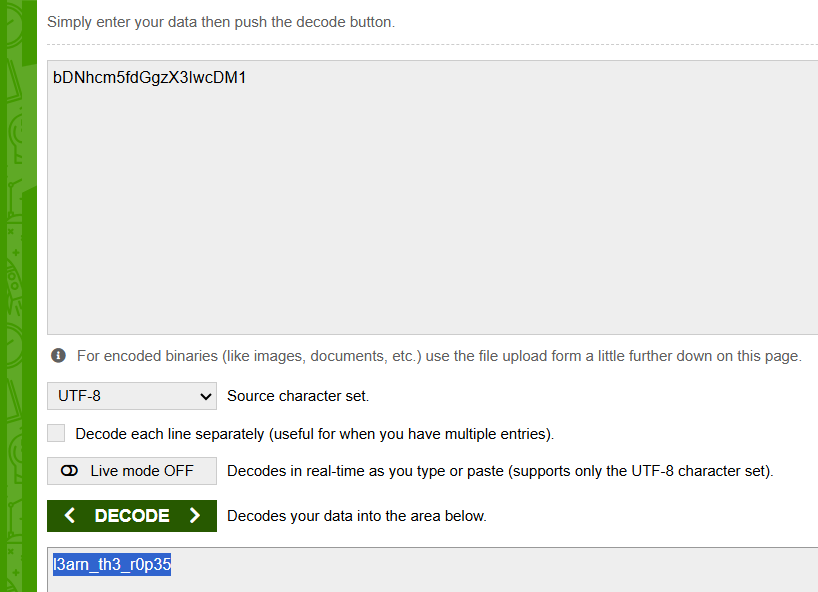
gasss



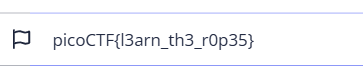
**Flag: picoCTF{tr45h\_51ng1ng\_9701e681}**

1. Bases



Yaaaa, intinya ini base64, jadi langsung saja di decode  


Baru di buat ke format “picoCTF{}”



**Flag: picoCTF{l3arn\_th3\_r0p35}**