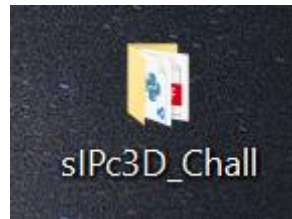
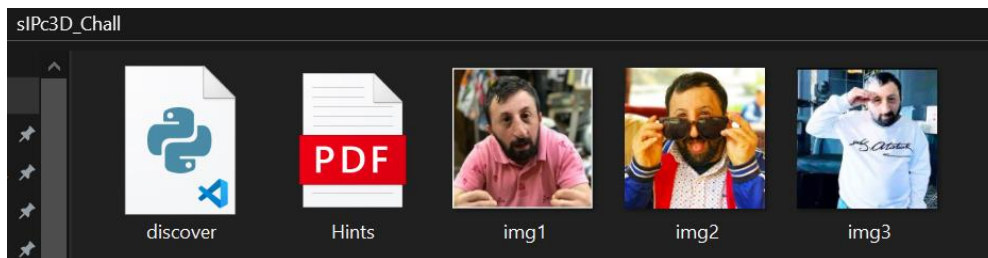


Write-up : sIPc3D_Chall / level:medium



Our challenge



sIPc3D_chall contains :

- **Discover script.**
- **3 images contain a hidden keys encrypted.**
- **Hints.**

Step1: using discover script to extract hidden keys :

```
(kali㉿kali)-[~/Desktop]
$ cd sIPc3D_Chall

(kali㉿kali)-[~/Desktop/sIPc3D_Chall]
$ python3 discover.py
img1.png
the secret key is : y1oo_jklz

(kali㉿kali)-[~/Desktop/sIPc3D_Chall]
$ python3 discover.py
img3.png
the secret key is : AS@GqAS@G

(kali㉿kali)-[~/Desktop/sIPc3D_Chall]
$ python3 discover.py
img2.png
the secret key is : ppwqq$(>@

(kali㉿kali)-[~/Desktop/sIPc3D_Chall]
$
```

After reading the hints file we now know that:

- The key1 hidden in the first image is encrypted by a substitution cipher with a text cipher and numbers (12.....90) + letters of a keyboard type (qwerty).
- The key2 hidden in the 2sd image is encrypted using a XOR cipher / $pass2 = pass(i) \oplus C2$.
- The key3 hidden in the 3rd image is encrypted using a XOR cipher / $pass2 = pass(i) \oplus C3$.

Step2: decrypt the hidden keys using the right combinations:

pass1 -----> pass2 -----> pass3 (maybe is the flag)

pass3 -----> pass2 -----> pass1 (maybe is the flag)

pass1 -----> pass3 -----> pass2 (maybe is the flag) (the right one)

pass3 -----> pass1 -----> pass2 (maybe is the flag)

pass2 -----> pass3 -----> pass1 (maybe is the flag)

key1:

Recipe

Substitute

Plaintext
1234567890qwertyuiopasdfghjklzxcvbnm

Ciphertext
y1oo_jklz

☒ Ignore case

Output
pass_1234

Key3:

Recipe

XOR

Key
pass_1234

Scheme
UTF8

Standard

☐ Null preserving

Input
AS@GqAS@G

Output
1234.pass

Key2 = the flag:

The screenshot shows the 'Recipe' configuration window in Burp Suite. The 'Recipe' tab is selected, and the operation is 'XOR'. The 'Key' field is set to '1234.pass', and the 'Scheme' is 'UTF8'. The 'Input' field contains the string 'ppwqq\$(>@'. The 'Output' field contains the string 'ABDE_TIM3'. A red arrow points from the top of the image to the 'Key' field.

Recipe	Input
XOR Key: 1234.pass Scheme: UTF8 <input type="checkbox"/> Null preserving	ppwqq\$(>@

Output
ABDE_TIM3

The flag is DEFENSYS{ABDE_TIM3}