《Make Steg Great Again》 WriteUp

查看题目图片源码,可以在最下方看到 Key:

2059 円次X.製tUr/6**E2D**U3 (SEASTEM **ECONO**12**E2D**U **EASIN ECON ECON**

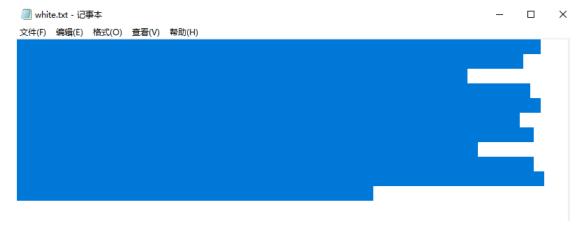
根据图片名称 Steg.jpg 猜测图片存在隐写,利用 StegHide 工具和获得的 Key(P@SsW00000)可以从图片中提取到 hacker.rar 压缩包:

root@iZnseq7e9mf5gcZ:~# steghide extract -sf /root/Steg.jpg
Enter passphrase:
wrote extracted data to "hacker.zip".

打开 hacker.rar 压缩包可以看到 GitHacker.pyc 和 white.txt 两个文件:

			文件夹
B GitHacker.pyc	4,981		Compiled Pyth
white.txt	507	98	文本文档

其中 white.txt 中有隐藏内容:



猜测是 snow 隐写,snow 隐写需要 key,因此重点转移到 GitHacker.pyc 文件上,从 pyc 文件很容易想到 pyc 字节码隐写,利用工具 Stegosaurus (https://bitbucket.org/jherron/stegosaurus/src)可以获取到 pyc 字节码隐写的内容

vaala@VAALA-SORFACE > -\..\stegosaurus > python -m stegosaurus C:\Users\huidc\Desktop\stegosaurus__pycache__\GitHacker .cpython-36-stegosaurus.pyc -x

Extracted payload: Your_key_is:'PPPPasword'_And_do_you_love_winter

隐写内容中的"And_do_you_love_winter"也是一个 Hint 提示 Snow 隐写 得到 Snow 隐写密钥 PPPasword 之后在 http://fog.misty.com/perry/ccs/snow/snow/snow.html 直接解密:

Decryption URL containing concealed message: http://39 161/white.bt Password: PPPPasword Decrypt

得到 Flag:

DASCTF {2741590dbe55ead7f2bfc50abb2d73e3}