




# BUUCTF 刷新过的图片 writeup

原创

碧羽o(\*/▽/\*)づ回雪  已于 2022-03-19 22:08:38 修改  99  收藏

分类专栏: [CTF writeup](#) 文章标签: [python](#)

于 2021-10-15 13:17:15 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zhangzhaolin12/article/details/120781402>

版权



[CTF writeup 专栏收录该内容](#)

16 篇文章 0 订阅

订阅专栏

下载后是一张图片, 但是这张图片实在有点。。。

这里题目是刷新过的图片, 刷新是F5键呀, 这就是一个提示, 图片是F5加密, 这里如果不知道这种加密就比较难办。

kali: 在F5-steganography路径下, 执行下面指令。解密后就多了一个output.txt文件。看一下, 发现是乱码。用010看一下, 发现是压缩包(文件头是50400102)。改一下后缀, 解压, 这里我忘记解压时有没有输入密码的弹窗, 如果有的话应该是伪加密(找到504b后面的14 00后面的两组十六进制数, 这就是加密的标记位)。解压后就是flag。

```
(root@kali)~/F5-steganography# java Extract Misc.jpg
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used

(root@kali)~/F5-steganography# ls
2.jpg bin.noise crypt d d.bat e e.bat Embed.class Embed.java Extract.class Extract.java gpl.txt image james java license.txt Makefile Misc.jpg ms_d.bat ms_e.bat ortega output.txt readme.md

(root@kali)~/F5-steganography# cat output.txt
PFDLcFrEY(flag.txtkIL4KMK1H4206010K361L424047HMHMF4LcFrEY($ flag.txt
PKZN
```

CSDN @几味^少年