耗子尾汁

发表于 2021-03-05 更新于 2021-03-15 分类于 Challenge ， 2020 ， SWPU CTF 2020 ， Misc
Challenge | 2020 | SWPU CTF 2020 | Misc | 耗子尾汁

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *图片隐写*
- *仿射密码*

解题思路

2.9M的gif图

其中flag.txt当然是假的

2^4_2^5_2^6.mp4

再次binwalk分离得到有密码的压缩包

但没有提示密码相关信息，爆破可能性不大，所以逐帧看mp4文件得到`c2lnbl9pbg==`

base64解码后得到`sign_in`即为压缩包密码

19_20.txt

解压后看到一长串字符串 拿去解base64后还是一长串奇奇怪怪的东西

想到mp4文件的名字很奇怪"2^4_2^5_2^6" 可以猜到base64，base32，base16依次解开后即为txt文件内提示的最后一层单表替换密码

txt文件的名字"19_20" 为仿射加密的两个参数a，b的值，解开即为flag字符串

按题目要求的格式改为flag{you_have_signed_in_successfully} 即可

弱弱说一句，这道题的提示全在文件名

`2^4_2^5_2^6`对应`base16.32.64`编码，`19_20`对应仿射的两个参数

然后可以解得flag

Flag

```
flag{you_have_signed_in_successfully}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Misc/91XmWXmBaB5D14aojzR2TM.html*

 # Challenge # 2020 # Misc # SWPU CTF 2020
jailbreak
来猜谜了