




# BUUCTF: 喵喵喵

原创

末初  于 2020-10-29 20:57:03 发布  2200  收藏 4

分类专栏: [CTF\\_MISC\\_Writeup](#)

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/mochu7777777/article/details/109368451>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges/#%E5%96%B5%E5%96%B5%E5%96%B5>

Challenge

390 Solves

×

# 喵喵喵

## 1

喵喵喵，扫一扫注意：得到的flag请包上flag{}提交

📄 3057c969-4...

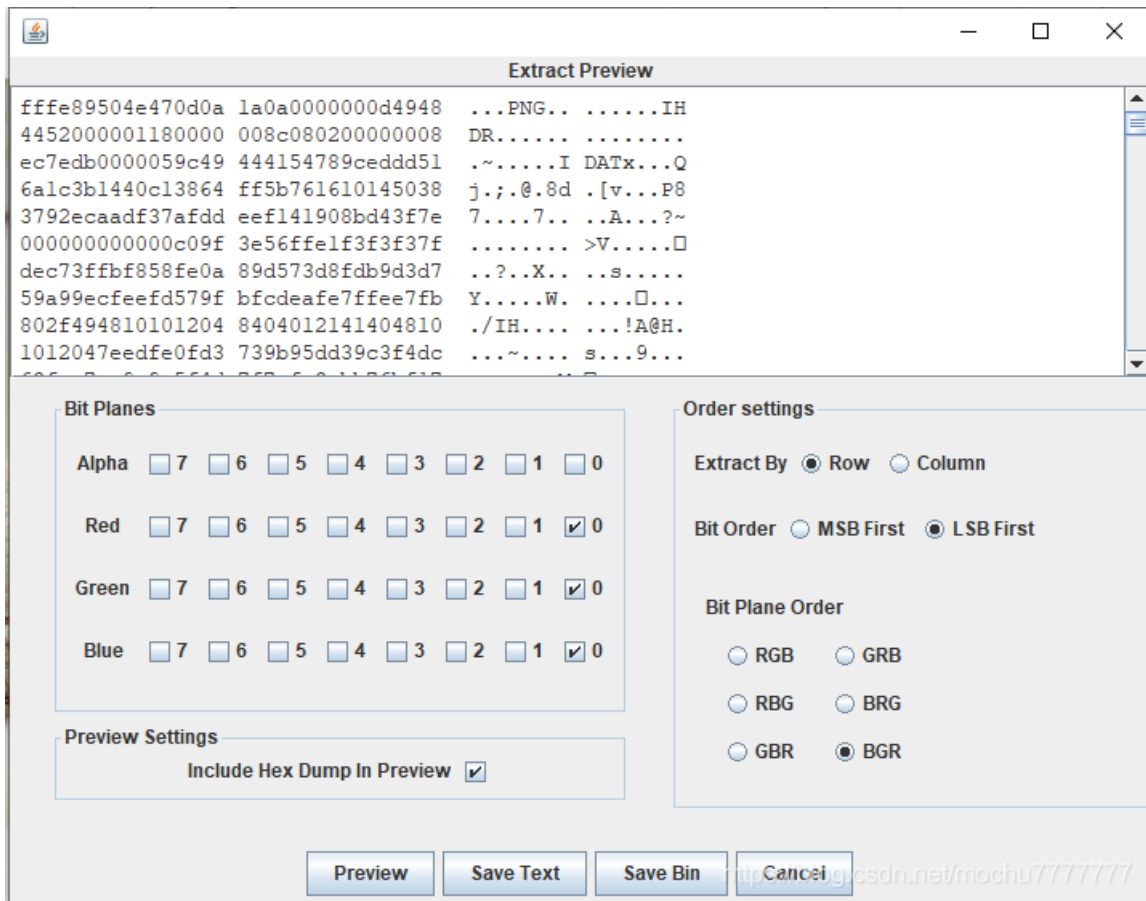
Flag

Submit

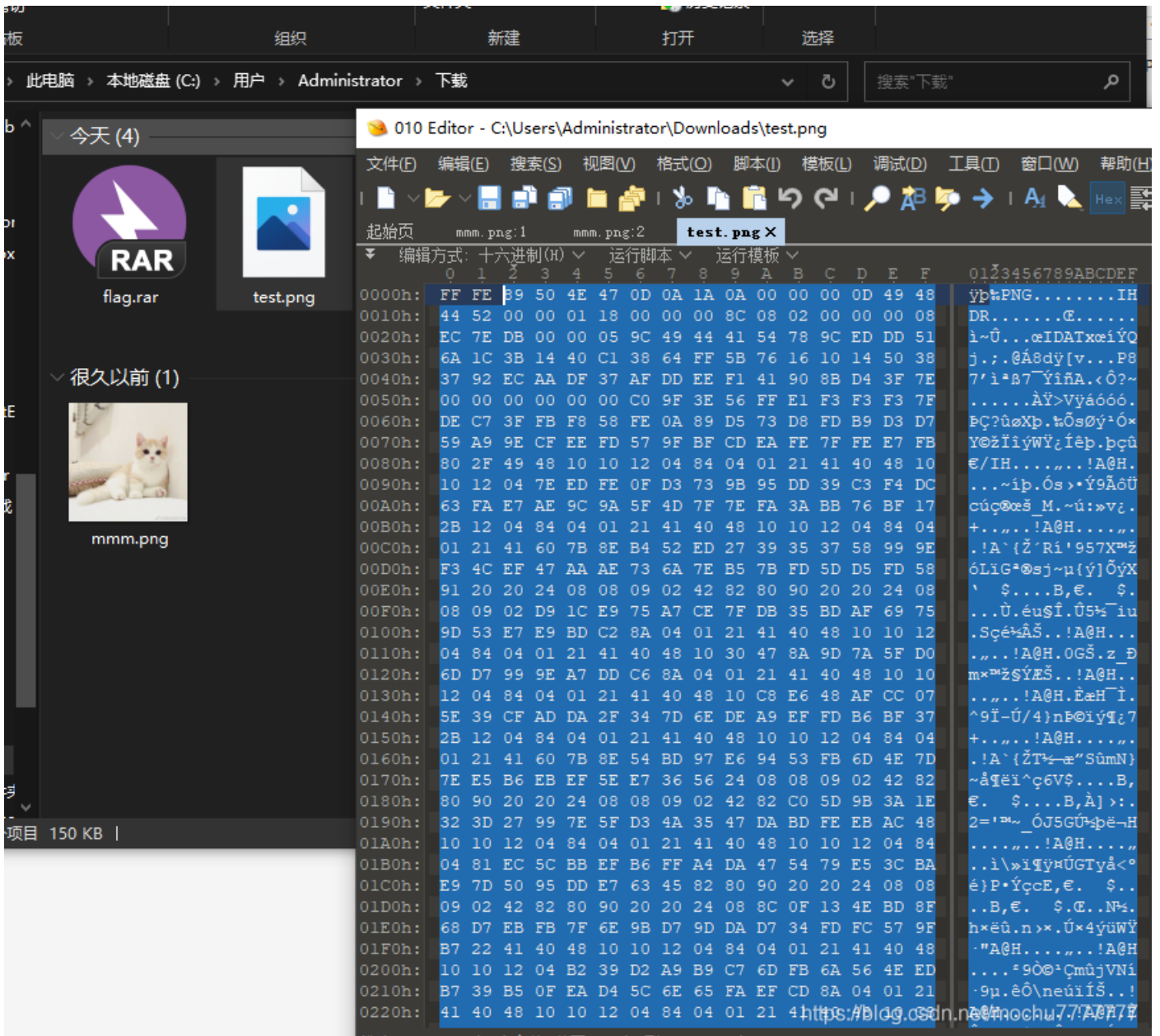
<https://blog.csdn.net/mochu7777777>



stegslove 打开，发现 RGB 的 0通道 存在异常，LSB隐写 发现 png



保存为 `test.png`，无法正常显示的，因为文件头前面多了些东西导致无法识别为PNF，另存从 `PNG` 文件头开始到 `IEND` 结束的数据即可



保存得到半张二维码，用 010 Editor 打开出现CRC不匹配，明显修改了宽高

复制路径 粘贴快捷方式 移动

test\_2h\_5EFh.png X

编辑方式: 十六进制(H) 运行脚本 运行模板: PNG.bt

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
0010h:	00	00	01	18	00	00	00	8C	08	02	00	00	00	08	EC	7E	.....E.....i~
0020h:	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	0...eIDATxœiYQj.
0030h:	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	;.@Á8dy[v...P87'
0040h:	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	i^B7`YiñA.<Ô?~..
0050h:	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	...Äÿ>Vÿá666.ËÇ
0060h:	3F	FB	F8	58	FE	0A	89	D5	73	D8	FD	B9	D3	D7	59	A9	?ûæXp.%ôs0ý^ó*Yø
0070h:	9E	CF	EE	FD	57	9F	BF	CD	EA	FE	7F	FE	E7	FB	80	2F	žIiyWÿ;Iêp.þçú€/
0080h:	49	48	10	10	12	04	84	04	01	21	41	40	48	10	10	12	IH.....!A@H...
0090h:	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	63	FA	~ip.ôs)*Ý9ÃóÜcú
00A0h:	F7	AF	9C	9A	5E	4D	7E	7E	FA	3A	BB	76	BF	17	2B	12	çœë M<ú~ÿ; +

输出

执行模板 'C:\Users\Administrator\Documents\SweetScape\010 Templates\Repository\PNG.bt' 于  
 \*ERROR: CRC Mismatch @ chunk[0]; in data: 08ec7edb; expected: 286c213a  
 \*ERROR Line 332: 声明中的数组大小无效。

输出 查找结果 多文件中查找 比较 直方图 校验和 进程

\*ERROR: CRC Mismatch @ chunk[0]; in data: 08ec7edb; expected: 286c213a 行 33

<https://blog.csdn.net/mochu777777>

test\_2h\_5EFh.png\* X

编辑方式: 十六进制(H) 运行脚本 运行模板: PNG.bt

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
0010h:	00	00	01	18	00	00	01	8C	08	02	00	00	00	08	EC	7E	.....E.....i~
0020h:	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	0...eIDATxœiYQj.
0030h:	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	;.@Á8dy[v...P87'
0040h:	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	i^B7`YiñA.<Ô?~..
0050h:	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	...Äÿ>Vÿá666.ËÇ
0060h:	3F	FB	F8	58	FE	0A	89	D5	73	D8	FD	B9	D3	D7	59	A9	?ûæXp.%ôs0ý^ó*Yø

得到完整的二维码，扫描得到信息

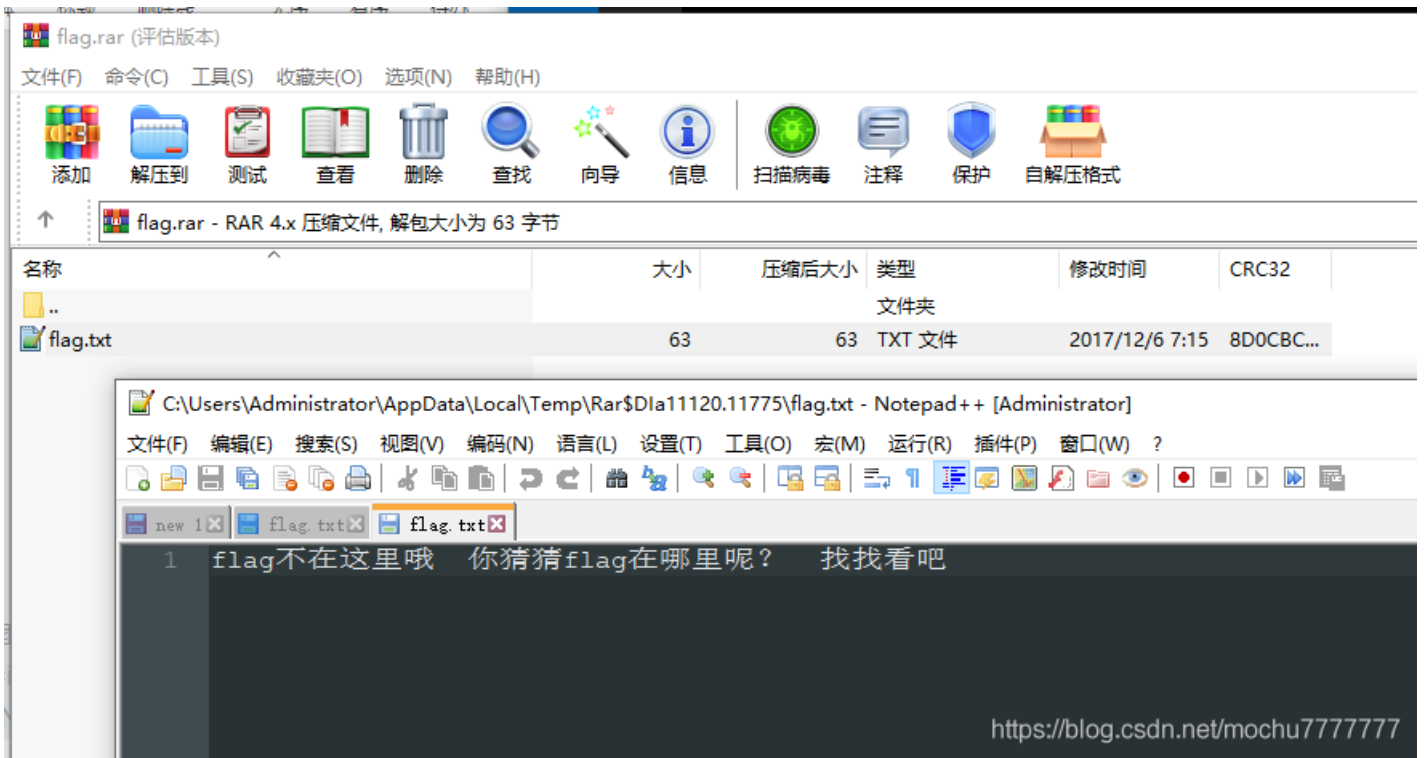
<https://pan.baidu.com/s/1pLT2J4f>



下载 [flag.rar](#)



[flag.txt](#) 打开没有发现flag



这里猜测有 NTFS 文件流隐写，将 flag.txt 解压到一个新建的文件夹内，利用 NtfsStreamsEditor



果然藏了东西，导出 flag.pyc

利用 Pyc反编译 在线网站进行反编译: <https://tool.lu/pyc/>

得到如下代码

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import base64

def encode():
    flag = '*****'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]

ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']
```

写个脚本把 `ciphertext` 解出来



```
#Author: mochu7
def decode(arg1):
    ciphertext = arg1[::-1]
    flag = ''
    for i in range(len(ciphertext)):
        if i % 2 == 0:
            s = int(ciphertext[i]) - 10
        else:
            s = int(ciphertext[i]) + 10
        s = s ^ i
        flag += chr(s)
    print(flag)

if __name__ == '__main__':
    ciphertext = [
        '96',
        '65',
        '93',
        '123',
        '91',
        '97',
        '22',
        '93',
        '70',
        '102',
        '94',
        '132',
        '46',
        '112',
        '64',
        '97',
        '88',
        '80',
        '82',
        '137',
        '90',
        '109',
        '99',
        '112']
    decode(ciphertext)
```

```
PS C:\Users\Administrator\Downloads\新建文件夹> python .\decode.py
flag{Y@e_C13veR_C1Ever!}
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)