

原创

noisy_wind 于 2021-10-23 11:00:40 发布 38 收藏

分类专栏: #CTF养成计划-MISC 文章标签: 网络安全

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/noisy_wind/article/details/120918078

版权



[CTF养成计划-MISC 专栏收录该内容](#)

10 篇文章 1 订阅

订阅专栏

一、分析

- 1. 压缩包可以正常解压
- 2. 图片可以正常打开
- 3. 查看PNG图片的宽高是否被修改了

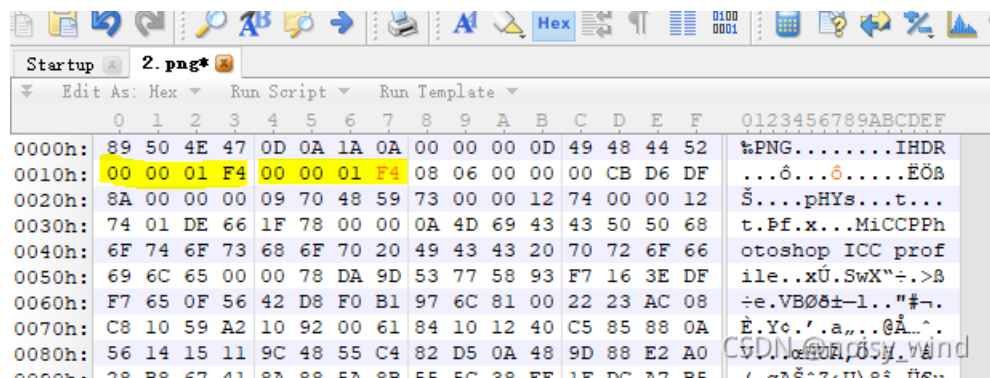
```
PNG_Heigh_Width x
F:\Anaconda\install\python.exe E:/CTF-Python/PNG_Heigh_Width.py
500 500
hex 0x1f4 0x1f4
Process finished with exit code 0
CSDN @noisy_wind
```

010Editor打开PNG后, 宽高在如图标黄处。

010Editor															
Startup 2.png															
Edit As: Hex Run Script Run Template															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44
0010h:	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6
0020h:	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00
0030h:	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50
0040h:	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F
0050h:	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E
0060h:	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC
0070h:	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88
0080h:	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	F2

发现还真是被修改了, 相当于图片下面被截断了, 所以隐藏了信息。

4. 修复



修改为01f4 后，保存，查看已经被修改的图片

5. 获取flag



BUGKU{a1e5aSA}

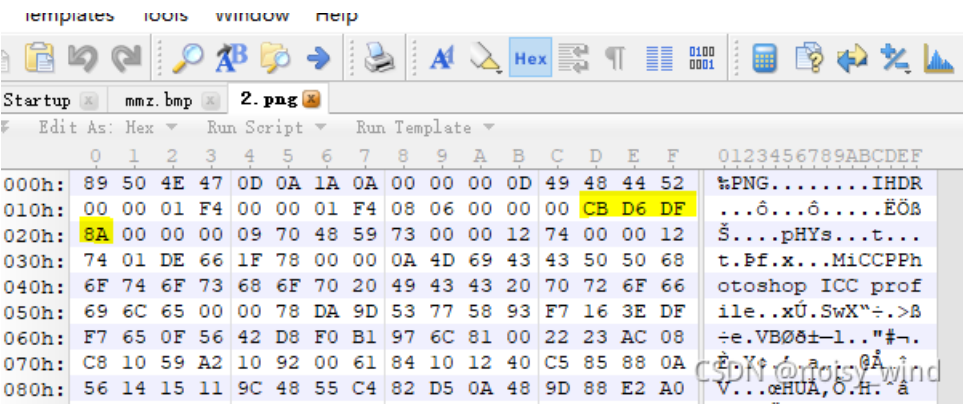
6. 分享一下python代码

```
import binascii
import struct

crcbp = open(r'C:\Users\peng\Desktop\file\2.png', 'rb').read()

for i in range(1024):
    for j in range(1024):
        data = crcbp[12:16] + struct.pack('>i', i) + struct.pack('>i', j) + crcbp[24:29]
        crc32 = binascii.crc32(data) & 0xffffffff
        if crc32 == 0xCRC值:
            print(i, j)
            print('hex', hex(i), hex(j))
```

010Editor打开PNG后，CRC值在如图标黄处。



二、感想

PNG图片常有这个宽高的修改。

MISC的题还是要多积累解题的技巧，不然这种简单的隐写方式，可能会让人在使用图片隐写工具的过程中浪费大量时间。