

# xctf攻防世界 MISC高手进阶区 2-1

原创

18947943 于 2022-02-02 21:45:11 发布 10474 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

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/18947943/article/details/122772030>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

## 1. 进入环境, 下载附件

给的一张png尾缀的文件, 尝试双击打开, 提示文件已损坏。猜测可能是文件头有问题, 因此丢入winhex中, 如图:

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII	^
00000000	80	59	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	€YNG IHDR	
00000016	00	00	00	00	00	00	02	F8	08	06	00	00	00	93	2F	8A	ø "/š	
00000032	6B	00	00	00	04	67	41	4D	41	00	00	9C	40	20	0D	E4	k gAMA α@ ä	
00000048	CB	00	00	00	20	63	48	52	4D	00	00	87	0F	00	00	8C	Ë cHRM ‡ Œ	
00000064	0F	00	00	FD	52	00	00	81	40	00	00	7D	79	00	00	E9	ýR @ }y é	
00000080	8B	00	00	3C	E5	00	00	19	CC	73	3C	85	77	00	00	0A	< <á ïs<...w	
00000096	39	69	43	43	50	50	68	6F	74	6F	73	68	6F	70	20	49	9iCCPPhotoshop I	
00000112	43	43	20	70	72	6F	66	69	6C	65	00	00	48	C7	9D	96	CC profile HÇ -	
00000128	77	54	54	D7	16	87	CF	BD	77	7A	A1	CD	30	D2	19	7A	wTT* †İ:wz;í0ò z	
00000144	93	2E	30	80	F4	2E	20	1D	04	51	18	66	06	18	CA	00	".0eó. Q f ê	
00000160	C3	0C	4D	6C	88	A8	40	44	11	11	01	45	90	A0	80	01	Ã Ml^~@D E €	
00000176	A3	A1	48	AC	88	62	21	28	A8	60	0F	48	10	50	62	30	€# [h/ /E 7b0	
00000192	8A	A8	A8	64	46	D6	4A	7C	79	79	EF	E5	E5	F7	C7	BD	S dF0J vviää=C4	

发现png文件头不对, 去搜搜文件格式, 进行修改。

## 2. 问题分析

查阅相关png图片的数据标识, [https://blog.csdn.net/zz\\_Caleb/article/details/89927673](https://blog.csdn.net/zz_Caleb/article/details/89927673):

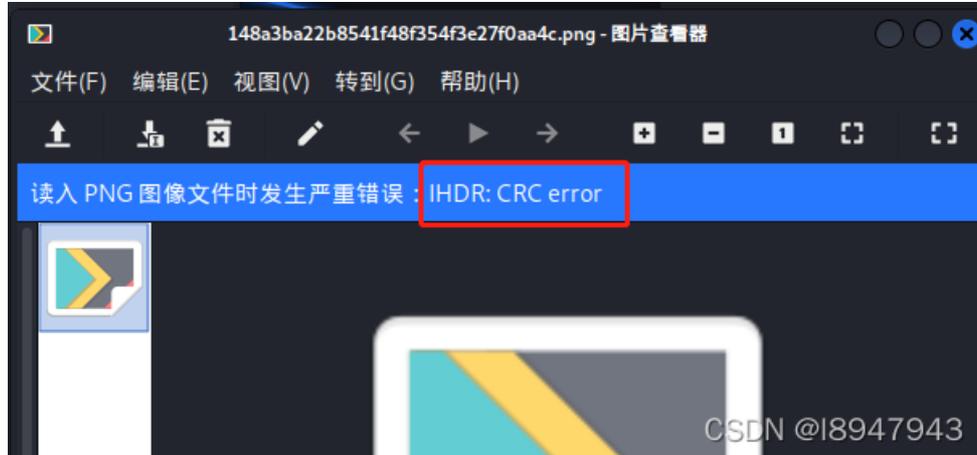
先详细解释一下png的文件头:

- (固定) 八个字节89 50 4E 47 0D 0A 1A 0A为png的文件头
- (固定) 四个字节00 00 00 0D (即为十进制的13) 代表数据块的长度为13
- (固定) 四个字节49 48 44 52 (即为ASCII码的IHDR) 是文件头数据块的标示 (IDCH)
- (可变) 13位数据块 (IHDR)
  - 前四个字节代表该图片的宽
  - 后四个字节代表该图片的高
  - 后五个字节依次为:  
Bit depth、ColorType、Compression method、Filter method、Interlace method
- (可变) 剩余四字节为该png的CRC检验码, 由从IDCH到IHDR的十七位字节进行crc计算得到。  
也就是说我们可以通过爆破来得到高度和宽度

修改相关的头后，如图：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR
00	00	00	00	00	00	02	F8	08	06	00	00	00	93	2F	8A	ø	"/Š
6B	00	00	00	04	67	41	4D	41	00	00	9C	40	20	0D	E4	k	gAMA α@ ä
CB	00	00	00	20	63	48	52	4D	00	00	87	0F	00	00	8C	È	cHRM ‡ Œ
0F	00	00	FD	52	00	00	81	40	00	00	7D	79	00	00	E9	ýR	@ }y é
8B	00	00	3C	E5	00	00	19	CC	73	3C	85	77	00	00	0A	<	<Å ìs<...w

使用kali打开提示CRC错误，如图：



写到这里，无从下手，参考网上的脚本，提示png图片crc宽度爆破，搜了一下，看了看相关博客：

<https://h3110w0r1d.com/archives/128/>

根据提示，使用脚本进行宽度遍历

```
import binascii
import struct

with open('./pic/148a3ba22b8541f48f354f3e27f0aa4c.png', 'rb') as file:
    # 得到文件的16进制数据
    data = file.read()
    for i in range(1024):
        # 找到数据的12到16位 (IHDR)
        # struct.pack('>i', i)中>表示大端模式, i表示integer数据类型, 将i为4位宽度进行表示
        # data[20 : 29]表示IHDR中的后9位
        # c表示IDCH和IHDR数据, 用于后续crc校验
        c = data[12:16] + struct.pack('>i', i) + data[20 : 29]
        # 如果校验结果是符合winhex中图片的第13到16位的crc值, 则爆破成功宽度
        crc = binascii.crc32(c) & 0xffffffff
        if crc == 0x932f8a6b:
            print(i)
```

跑出的图片宽度为709，对应16进制为 `0x2c5`，我们在winhex中修改对应的宽度值，如图：

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR
16	00	00	02	C5	00	00	02	F8	08	06	00	00	00	93	2F	8A	À	ø"/Š
32	6B	00	00	00	04	67	41	4D	41	00	00	9C	40	20	0D	E4	k	gAMA α@ ä
48	CB	00	00	00	20	63	48	52	4D	00	00	87	0F	00	00	8C	Ë	cHRM ‡ Œ
64	0F	00	00	FD	52	00	00	81	40	00	00	7D	79	00	00	E9	ýR	@ }y é
80	8B	00	00	3C	E5	00	00	19	CC	73	3C	85	77	00	00	0A	<	<À Ìs<...w
96	39	69	43	43	50	50	68	6F	74	6F	73	68	6F	70	20	49	9iCCP	Photoshop I
112	43	43	20	70	72	6F	66	69	6C	65	00	00	48	C7	9D	96	CC	profile HÇ -
128	77	54	54	D7	16	87	CF	BD	77	7A	A1	CD	30	D2	19	7A	wTT*	†Ï:wz;ÍÒ z
144	93	2E	30	80	F4	2E	20	1D	04	51	18	66	06	18	CA	00	".0eó.	Q f Ê
160	C3	0C	4D	6C	88	A8	40	44	11	11	01	45	90	A0	80	01	Ã Ml^`@D	E €
176	A3	A1	48	AC	88	62	21	28	A8	60	0F	48	10	50	62	30	z;H~^b!(```	H Pb0
192	8A	A8	A8	64	46	D6	4A	7C	79	79	EF	E5	E5	F7	C7	BD	Š	""dFÖJlyyiaã+Çz
208	DF	DA	67	EF	73	F7	D9	7B	9F	B5	2E	00	24	4F	1F	2E	Š	""dFÖJlyyiaã+Çz

得到最终的可打开图片：

`flag is wdflag{Png_`

`C2c_u_kn0W}`

CSDN @18947943

最终答案为：`wdflag{Png_C2c_u_kn0W}`