

2-1 攻防世界

🐪 3分

题目描述

题目给了一张图片，但是不能正常打开

解题

010 Editor 查看文件

Startup	misc2-1.png x																															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF															
0000h:	80	59	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	€NG.....IHDR															
0010h:	00	00	00	00	00	00	02	F8	08	06	00	00	00	93	2F	8Aø....."/Š															
0020h:	6B	00	00	00	04	67	41	4D	41	00	00	9C	40	20	0D	E4	k....gAMA...æ@.ä															
0030h:	CB	00	00	00	20	63	48	52	4D	00	00	87	0F	00	00	8C	Ë... cHRM...‡...Æ															
0040h:	0F	00	00	FD	52	00	00	81	40	00	00	7D	79	00	00	E9	...ÿR...@...}y...é															
0050h:	8B	00	00	3C	E5	00	00	19	CC	73	3C	85	77	00	00	0A	<...<ä...İs<...w...ı															
0060h:	39	69	43	43	50	50	68	6F	74	6F	73	68	6F	70	20	49	9iCCPPtoshop I															
0070h:	43	43	20	70	72	6F	66	69	6C	65	00	00	48	C7	9D	96	CC profile..HÇ.-															
0080h:	77	54	54	D7	16	87	CF	BD	77	7A	A1	CD	30	D2	19	7A	wTT×.‡İwzjİ00.z															
0090h:	93	2E	30	80	F4	2E	20	1D	04	51	18	66	06	18	CA	00	".0€ô. ..Q.f..Ê.															
00A0h:	C3	0C	4D	6C	88	A8	40	44	11	11	01	45	90	A0	80	01	Ã.Ml~^@D...E. €.															
00B0h:	A3	A1	48	AC	88	62	21	28	A8	60	0F	48	10	50	62	30	£jH~^b!(``.H.Pb0															
00C0h:	8A	A8	A8	64	46	D6	4A	7C	79	79	EF	E5	E5	F7	C7	BD	Š~`dFÖJ yyiää÷Ç¥															

发现文件头损坏，将 80 59 改为 89 50。

另外图片的宽度值为 00 00 00 00

通过CRC32爆破来获取图片宽度。

Python

```
1 import os
2 import binascii
3 from pwn import *
4 misc = open("misc2-1.png", "rb").read()
5
6 for i in range(1024):
7     data = misc[12:16] + p32(i, endian="big") + misc[20:29]
8     crc32 = binascii.crc32(data) & 0xffffffff
9     if crc32 == 0x932f8a6b:
10         print(hex(i))
```

可得到宽度为 `0x2c5`

修复后的图片可以看到flag

flag is wdflag{Png_

C2c_u_kn0W}