2-1 攻防世界

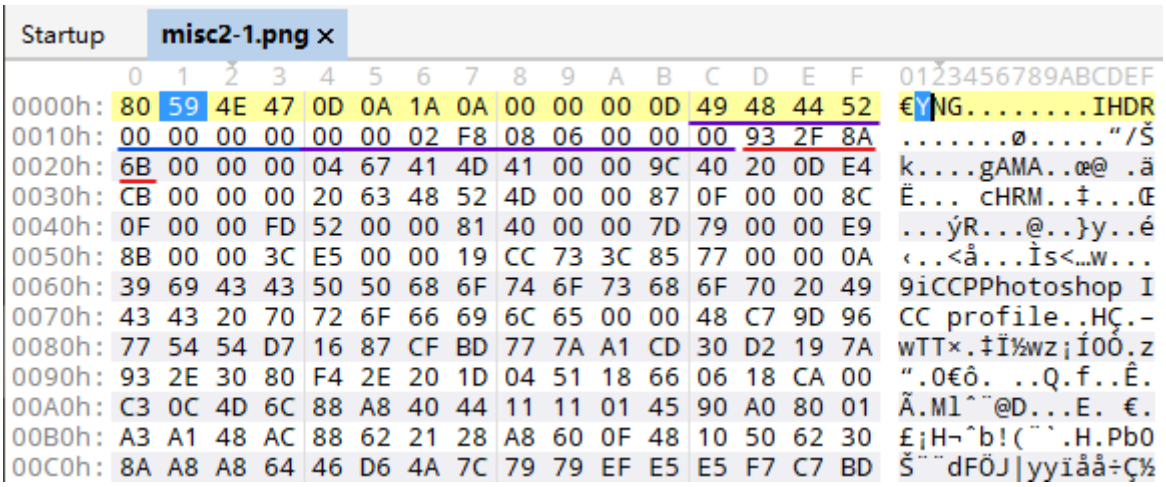
🐫 3分

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



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

```python
import os
import binascii
from pwn import *
misc = open("misc2-1.png","rb").read()

for i in range(1024):
    data = misc[12:16] + p32(i,endian="big")+ misc[20:29]
    crc32 = binascii.crc32(data)&0xffffffff
    if crc32 == 0x932f8a6b:
        print (hex(i))
```

可得到宽度为`0x2c5`

修复后的图片可以看到flag