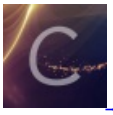
ctf-misc PNG(文件头IHEDR)图片隐写

原创

go_to_hacker 于 2018-02-26 11:21:35 发布
分类专栏： ctf 文章标签： ctf png misc



爆破crc校验所需要了解到的PNG文件头知识

- （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。

例题：
WDCTF-FINALS-2017¶

观察文件可以发现,文件头及宽度异常

```
00000000  80 59 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.YNG........IHDR|
00000010  00 00 00 00 00 00 02 f8  08 06 00 00 00 93 2f 8a  |................/.|
00000020  6b 00 00 00 04 67 41 4d  41 00 00 9c 40 20 0d e4  |k....gAMA...@ ..|
00000030  cb 00 00 00 20 63 48 52  4d 00 00 87 0f 00 00 8c  |.... cHRM.......|
00000040  0f 00 00 fd 52 00 00 81  40 00 00 7d 79 00 00 e9  |....R...@..}y...|
...
```

这里需要注意的是，文件宽度不能任意修改，需要根据 IHDR 块的 CRC 值爆破得到宽度,否则图片显示错误不能得到 flag。

```
import os
import binascii
import struct


misc = open("misc4.png","rb").read()

for i in range(1024):
    data = misc[12:16] + struct.pack('>i',i)+ misc[20:29]
    crc32 = binascii.crc32(data) & 0xffffffff
    if crc32 == 0x932f8a6b://CRS校验
        print i
```

得到宽度值为 709 后，恢复图片得到 flag。

2、宽度问题

图片地址：

题目链接：http://pan.baidu.com/s/1qY8sxZl 密码：5xam

图片尺寸为500x420(宽x高)

00 00 00 0D 说明IHDR头块长为13

49 48 44 52 IHDR标识

00 00 01 F4 图像的宽，500像素

00 00 01 A4 图像的高，420像素

最后四位CB　D6　DF　8 A为CRC校验

将图片的高改为500像素就拿到flag了