攻防世界 Misc高手进阶区 3分题 2-1

原创

思源湖的鱼 于 2020-11-14 13:56:01 发布 275 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 misc png文件头

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109689926

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

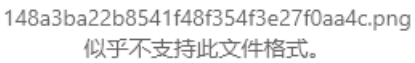
本篇是2-1的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个png文件



扔进winhex

```
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  œ@  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  ‹  <å    Ìs<…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× ‡Ï½wz¡Í0Ò z
00000144  93 2E 30 80 F4 2E 20 1D  04 51 18 66 06 18 CA 00  "."0€ô.   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¬^b!(¨` H Pb0
00000192  8A A8 A8 64 46 D6 4A 7C  79 79 EF E5 E5 F7 C7 BD  Š¨¨dFÖJ|yyïåå÷Ç½
00000208  DF DA 67 EF 73 F7 D9 7B  9F B5 2E 00 24 4F 1F 2E  ßÚgïs÷Ù{Ÿµ. $O .
```

文件头不对

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

可以看到

- 59要改为50，80要改为89
- 宽度要改为符合crc的宽度

```
import os
import binascii
import struct

misc = open("2-1.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:
        print (i)
```

得到宽度709
转为16进制为02C5

最终改为

```
00000000  89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  ‰PNG        IHDR
00000016  00 00 02 C5 00 00 02 F8  08 06 00 00 00 93 2F 8A     Å    ø      "/Š
00000032  6B 00 00 00 04 67 41 4D  41 00 00 9C 40 20 0D E4  k    gAMA  œ@  ä
00000048  CB 00 00 00 20 63 48 52  4D 00 00 87 0F 00 00 8C  Ë    cHRM  ‡   Œ
```

得到png文件如下

flag is wdflag{Png_

C2c_u_kn0W}

得到flag

结语

就是png文件头
回头整理下各文件的文件头