




CTF-Misc-大白

原创

归子莫  于 2020-05-14 19:48:09 发布  2637  收藏 3

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/qq_45163122/article/details/106127243

版权

CTF-Misc-大白

博客说明

文章所涉及的资料来自互联网整理和个人总结，意在于个人学习和经验汇总，如有什么地方侵权，请联系本人删除，谢谢！本文仅用于学习与交流，不得用于非法用途！

CTP平台

网址

<https://buuoj.cn/challenges>

题目

Misc类，大白

思路

这类题目首先把文件下载下来，然后打不开，环境是在linux下



报了CRC的错误，是png的CRC校验错误

在网上找到了大佬关于png修复CRC错误的脚本

```
#coding=utf-8
import os
import binascii
import struct

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

for i in range(1024):
    data = misc[12:20] + struct.pack('>i', i) + misc[24:29]
    crc32 = binascii.crc32(data) & 0xffffffff
    if crc32 == 0x6d7c7135:
        print i
```

python3 png.py

得出高为479，转化为十六进制1df

打开bless

在00000010开始前四位为宽，后四位为高

00000000 | 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 | .PI
00000012 | 02 A7 00 00 01 00 08 06 00 00 00 6D 7C 71 35 00 00 | ..
00000024 | 01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67 41 4D 41 | .sl
00000036 | 00 00 B1 8F 0B FC 61 05 00 00 00 09 70 48 59 73 00 00 | ..
00000048 | 0E C4 00 00 0E C4 01 95 2B 0E 1B 00 00 FF A5 49 44 41 | ..
0000005a | 54 78 5E EC BD 07 A0 A5 57 59 EE FF EE BE 4F 9B DE 93 | Tx'
0000006c | 4C 7A 0F 84 24 24 60 0C 04 A5 2B 20 45 10 10 BB 88 8A | Lz
0000007e | A8 57 BD FC EF BD 7A F5 5A AE 7A BD 5E CB BD 2A 62 05 | .W

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 | .PNG.....IHDR..
02 A7 00 00 01 DF 08 06 00 00 00 6D 7C 71 35 00 00 | .....m|q5...
01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67 41 4D 41 | .sRGB.....gAMA
00 00 B1 8F 0B FC 61 05 00 00 00 09 70 48 59 73 00 00 | .....a.....pHYs..
0E C4 00 00 0E C4 01 95 2B 0E 1B 00 00 FF A5 49 44 41 | .....+.....IDA
54 78 5E EC BD 07 A0 A5 57 59 EE FF EE BE 4F 9B DE 93 | Tx^.....WY....O...
4C 7A 0F 84 24 24 60 0C 04 A5 2B 20 45 10 10 BB 88 8A | Lz..$$`. . . + E.....
A8 57 BD FC EF BD 7A F5 5A AE 7A BD 5E CB BD 2A 62 05 | .W.....z.Z.z.^...*b.
04 69 52 04 E9 01 42 48 48 42 7A EF 7D 52 A6 CF 9C 7E | .iR...BHHBz.)R...~
76 FD 3F BF F7 DB EF 39 6B 76 F6 4C 26 C9 4C 32 E5 7B | v.?. . . . 9kv.L&.L2.{
CE 59 7B F5 DE 9E 6F 7D 6B AD AF D0 15 2C 47 8E 1C 39 | .Y{...o}k....,G..9
72 1C 90 6C 88 2E 14 0A 3D DD DE 63 6F FD A5 53 C0 93 | r..`.....=.co..S..
```

打开修复好了的png，找到flag



感谢

BUUCTF
以及勤劳的自己