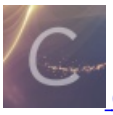
CTF-Misc-[BJDCTF2020]一叶障目

原创

归子莫 于 2020-05-14 11:02:56 发布 2263 收藏 6

分类专栏： CTF 文章标签： ctf

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/106115563
版权



CTF 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

CTF-Misc-[BJDCTF2020]一叶障目

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，[BJDCTF2020]一叶障目

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

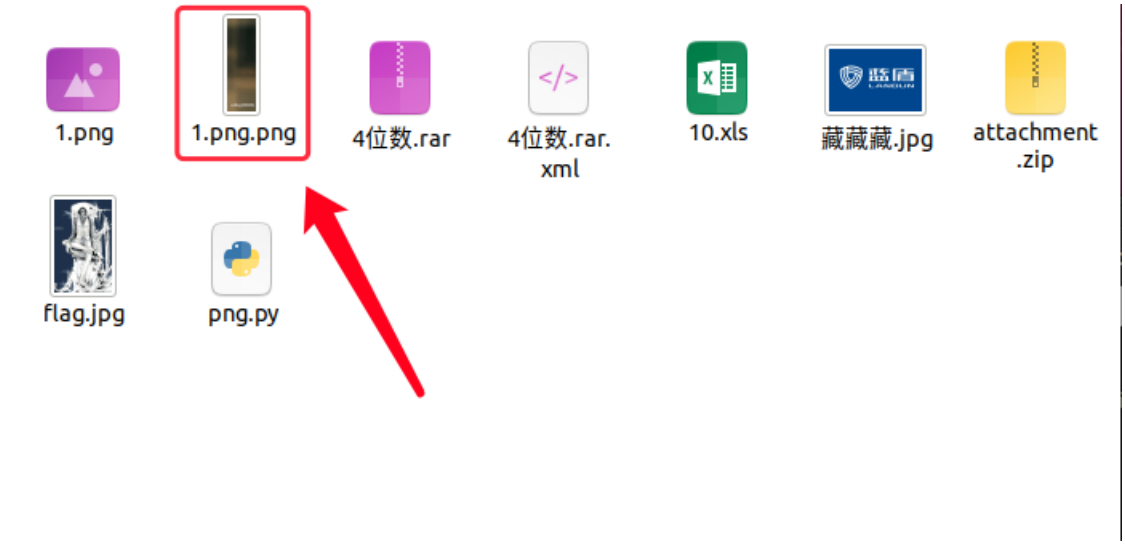
在网上找到了大佬关于png修复CRC错误的脚本

```python
#coding=utf-8
import zlib
import struct
#读文件
file = '1.png'  #注意，1.png图片要和脚本在同一个文件夹下哦~
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
#crc32key = 0xCBD6DF8A #补上0x，copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x00\x01\xF1\x08\x06\x00\x00\x00')  #hex下copy grep hex
n = 4095 #理论上0xffffffff,但考虑到屏幕实际，0x0fff就差不多了
for w in range(n):#高和宽一起爆破
    width = bytearray(struct.pack('>i', w))#q为8字节，i为4字节，h为2字节
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            #写文件
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png','wb')#保存副本
            fw.write(newpic)
            fw.close
```

```
python3 png.py
```

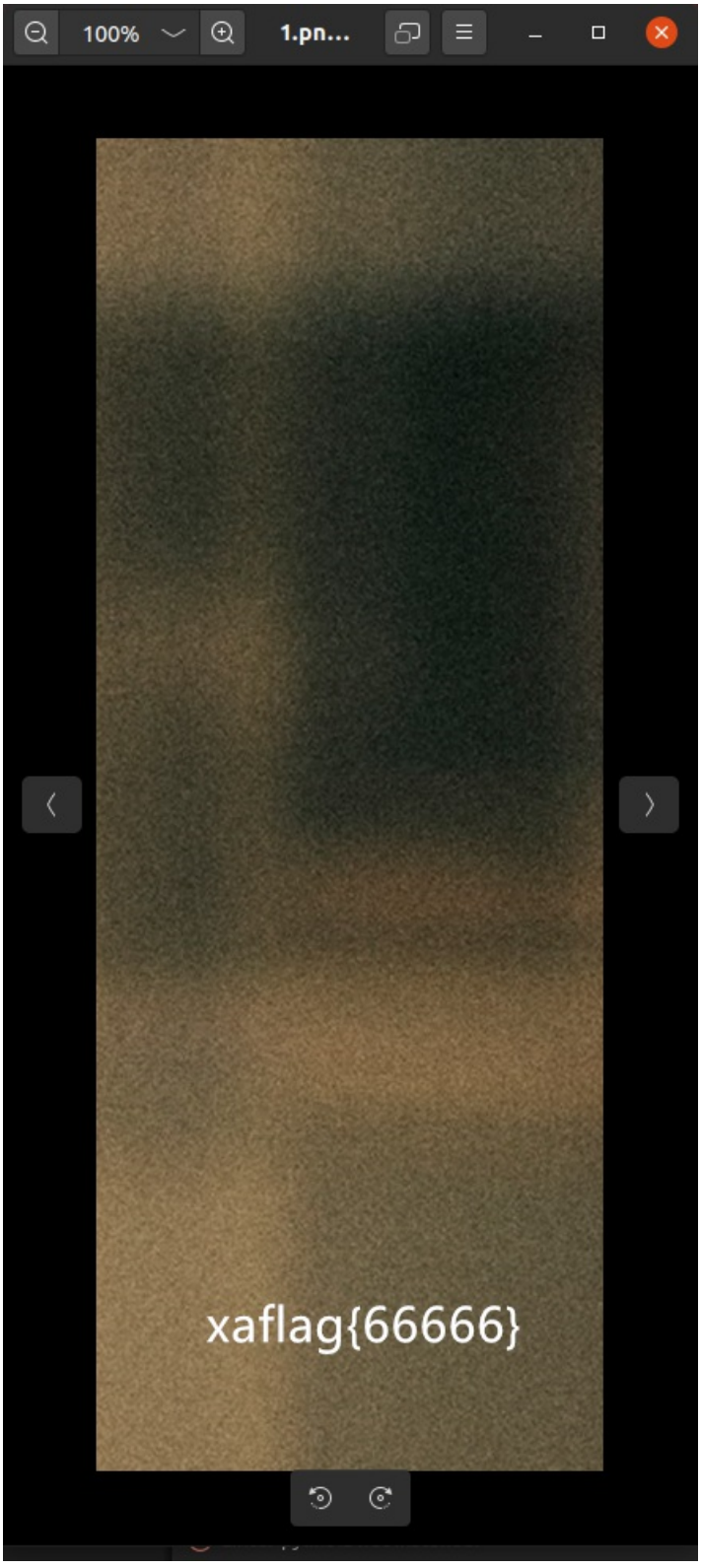
```
tanglei@ubuntu:~/Desktop/ctf/misc$ python3 png.py
bytearray(b'\x00\x00\x01A') bytearray(b'\x00\x00\x03L')
```

然后会发现多出来了一个png文件



这个就是修复好了的

打开修复好了的png，找到flag



感谢

> BUUCTF
> 以及勤劳的自己