

Buuctf 一叶障目

原创

Dexret 于 2021-11-26 10:41:00 发布 66 收藏

分类专栏: [Buuctf Misc](#) 文章标签: [Buuctf misc python](#)

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/Dexret/article/details/121554427>

版权



[Buuctf Misc 专栏收录该内容](#)

47 篇文章 0 订阅

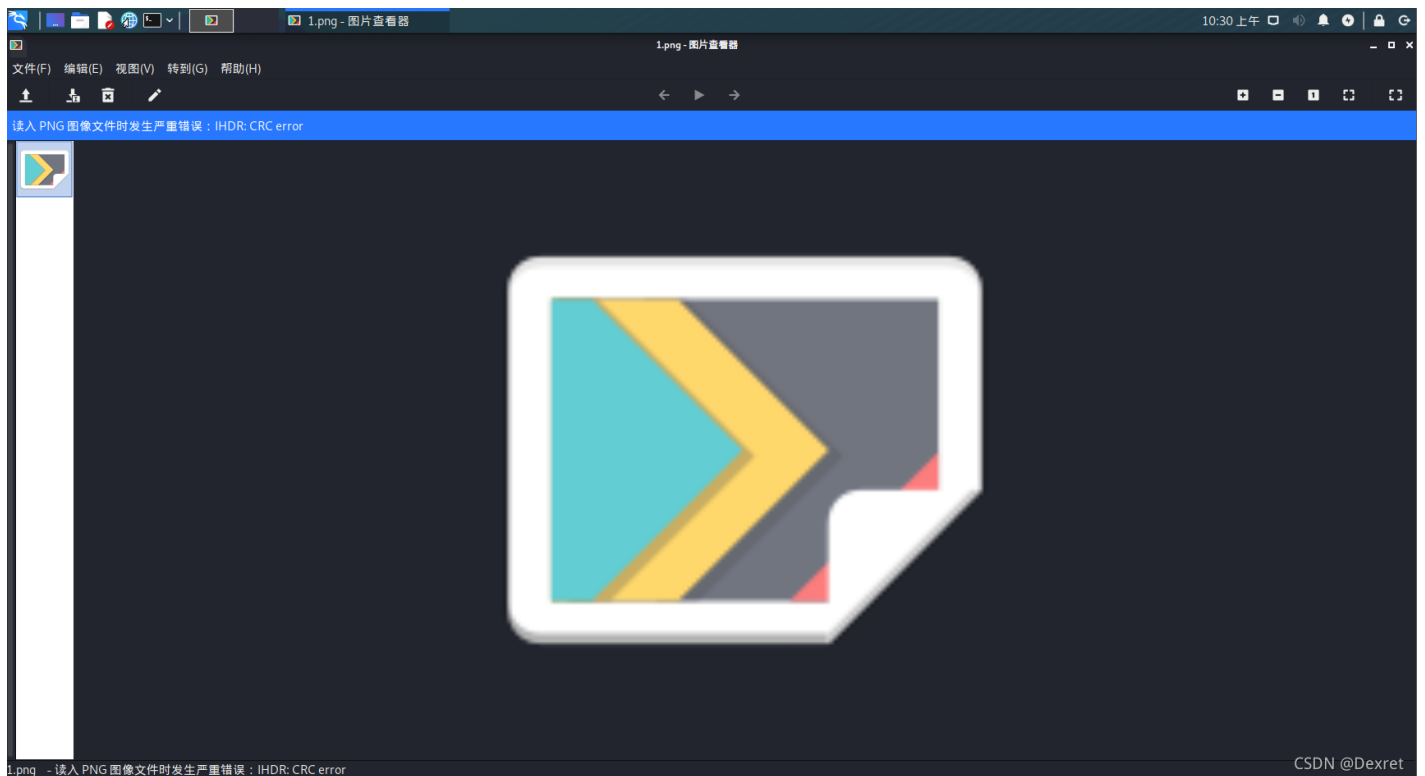
订阅专栏

下载该文件, 发现该文件为一张照片

利用UltraEdit和StegSlove对该图片进行检测, 没有发现任何有用信息

但当我准备将该图片放到kail中测试时, 发现该图片无法打开

提示CRC错误



查了一下资料应是CRC的校验出现了问题

在网上找了一下大佬修复图片CRC校验错误的python脚本

```

#coding=utf-8
import zlib
import struct
#读文件
file = '1.png' #注意, 1.png图片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
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

```

运行一下该脚本

The screenshot shows a Python IDE with the following code in the editor:

```

1 #coding=utf-8
2 import zlib
3 import struct
4 #读文件
5 file = '1.png' #注意, 1.png图片和脚本在同一个文件夹下哦~
6 fr = open(file,'rb').read()
7 data = bytearray(fr[12:29])
8 crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
9 #crc32key = 0xCBD6DF8A #补上0x, copy hex value
10 #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
11 n = 4095 #理论上0xffffffff,但考虑到屏幕实际, 0x0fff就差不多了
12 for w in range(n):#高和宽一起爆破
13     width = bytearray(struct.pack('>i', w))#q为8字节, i为4字节, h为2字节
14     for h in range(n):
15         height = bytearray(struct.pack('>i', h))
16         for x in range(4):
17             data[x+4] = width[x]
18             data[x+8] = height[x]
19             #print(data)
20         crc32result = zlib.crc32(data)
21         if crc32result == crc32key:
22             print(width,height)
23             #写文件
24             newpic = bytearray(fr)
25             for x in range(4):
26                 newpic[x+16] = width[x]
27                 newpic[x+20] = height[x]
28             fw = open(file+'.png', 'wb')#保存副本
29             fw.write(newpic)
30             fw.close

```

The console output shows the following:

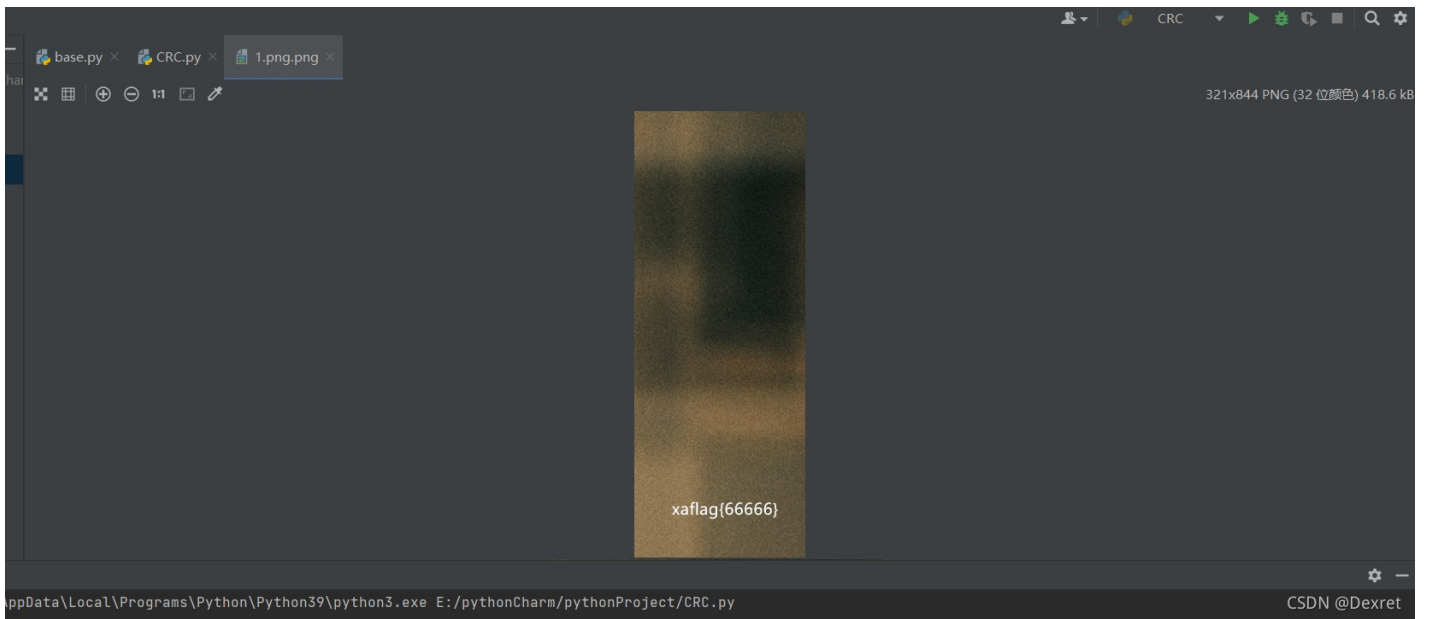
```

运行: CRC
C:\Users\13631\AppData\Local\Programs\Python\Python39\python3.exe E:/pythonCharm/pythonProject/CRC.py
bytearray(b'\x00\x00\x01A') bytearray(b'\x00\x00\x03L')
进程已结束, 退出代码为 0

```

运行成功后得到一个1.png.png的图像

打开该图像得到该题的flag



flag{66666}