XCTF MISC 高手区 Dift

原创

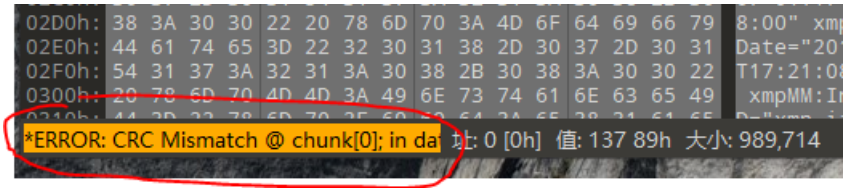
T0m0rrow 于 2021-01-06 22:21:58 发布 22 收藏

分类专栏： CTF

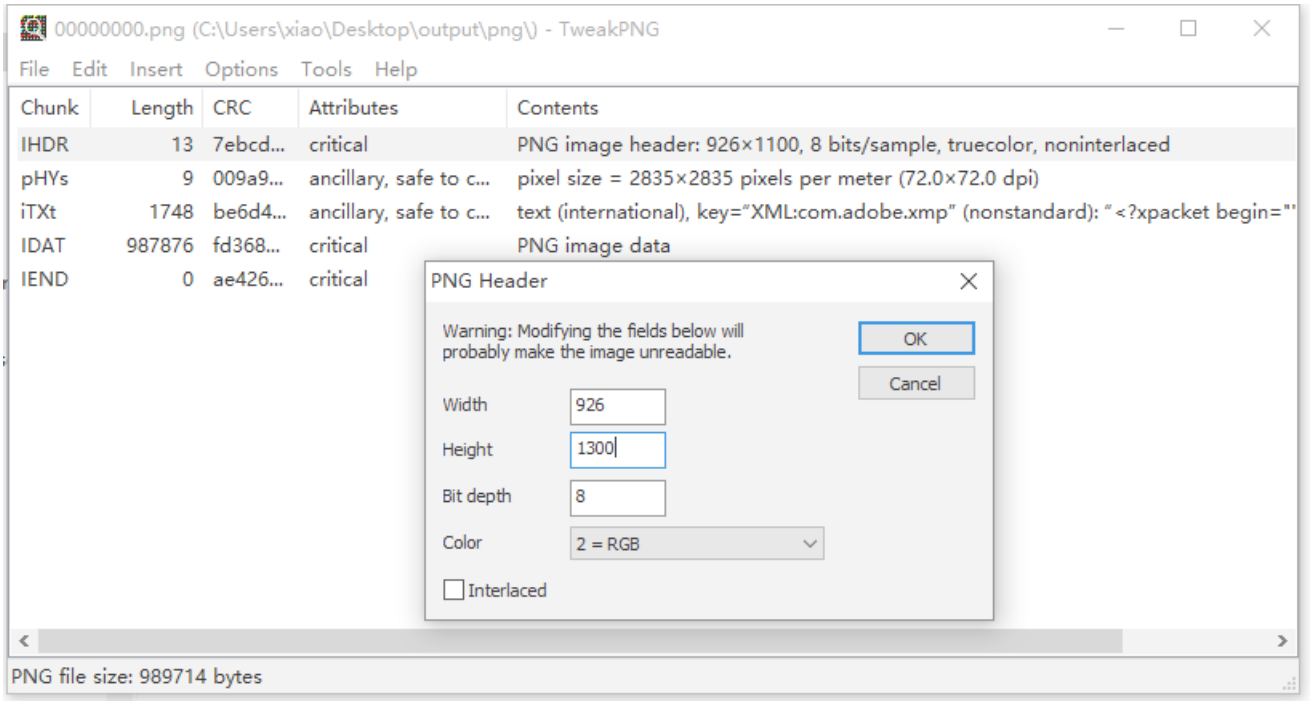
本文链接：https://blog.csdn.net/duwanglai/article/details/112298458

Dift

- 附件是一张png图片，用foremost分离得到png和一个加密的rar文件，用`ARCHPR`暴力破解失败。
- 没有其它可用的信息，压缩包应该是和png图片有关
- 用010editor打开分离后的png图片



- 显示CRC校验出错，很显然图片被修改过，因为windows系统会忽略CRC校验，所以图片能正常打开，而在linux系统上则会报错。详细分析：https://www.cnblogs.com/cxjchen/p/12611792.html
- 最简单快速的方法就是用`tweakpng`修改图片的宽高，以看到被隐藏起来的信息
- 我们这里适当增加图片高度，将1100改到1300



- 发现隐藏的一串字符，应该就是解压密码

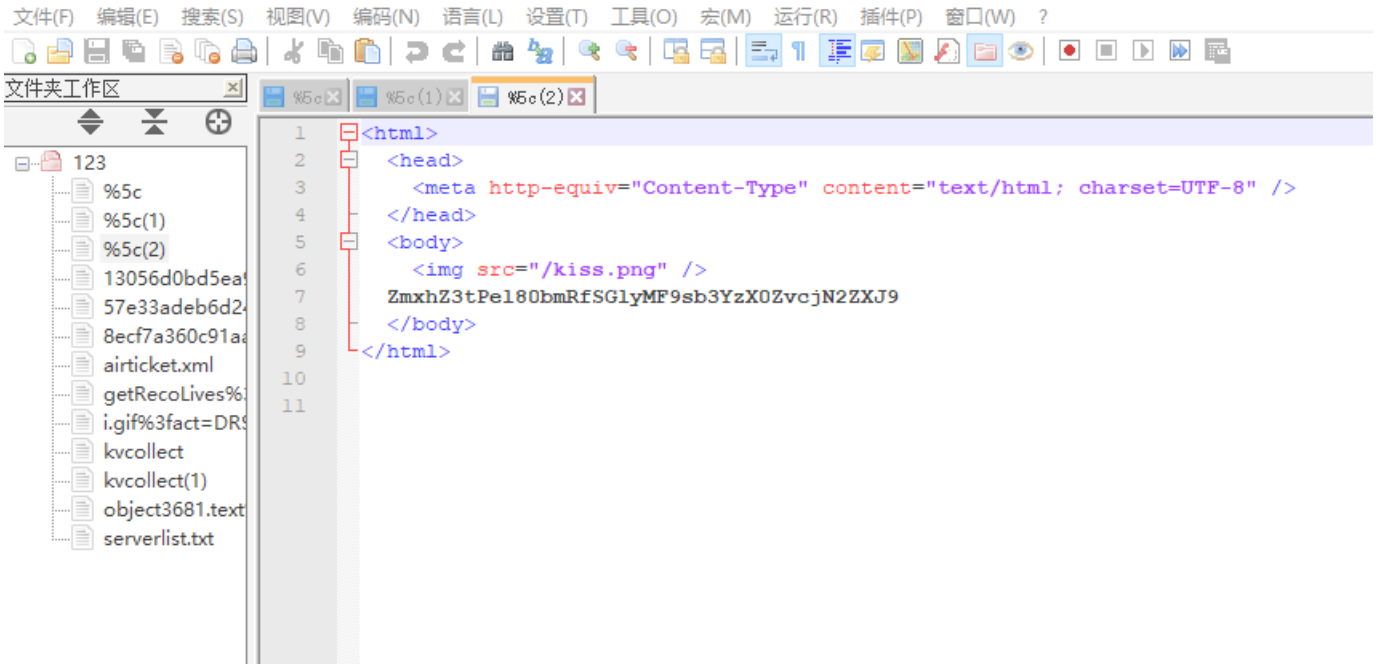
> StRe1izia

StRe1izia

这里也可以通过CRC32碰撞的方式获取准确的宽高，从网上搜集的代码如下：

```
#!/usr/bin/env python
# -*- encoding: utf-8 -*-
import zlib
import struct
#读文件
file = '00000000.png' #文件路径
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = int('0x' + fr[29:33].hex(),16)
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
```

- 解压缩得到**Dift.pcapng**流量包文件foremost分离没有结果，用wireshark打开，导出所有HTTP对象
- 在%5c(2)这个文件中发现一串base64编码



- 解码可得flag

flag{Oz_4nd_Hir0_lov3_For3ver}