【BugKu-CTF论坛writeup(杂项)】俄罗斯套娃



Kingyo12 ● 于 2018-03-07 16:03:22 发布 ● 160 ℃ 收藏
 分类专栏: BugKu-CTF论坛writeup(杂项) 未完成
 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/preserphy/article/details/79470821
 版权

BugKu-CTF论坛writeup(杂项)同时被2个专栏收录 28篇文章1订阅



10

1篇文章0订阅

订阅专栏

zip压缩包,破解似乎需要密码,先考虑是不是伪加密。用HxD打开,将文件目录区(504B0102)的3个伪加 密标志位09依次修改为00

保存解压,得到三个文件



key.txt

lock.cap

接下来一个一个来看——



很多01,而且有换行,很奇怪。观察了一会儿之后发现离远了看,会有依稀可见的纹理。又重新仔细观察了一下,发现0的数量似乎有点太多了。就想到了计原里面学的曼彻斯特编码,是用01代表0,10代表1。网上搜了一下曼彻斯特编码的解码脚本,在这里贴一下,说不定以后还能用到

```
#!/usr/bin/env python
f = open('key.txt','r')#原文件
f1 = open('con.txt','w')#解码后的文件
for line in f.readlines():
    content = ''
    for i in range(0,len(line),2):
        if line[i:i+2] == '10':
            content += '1'
        if line[i:i+2] == '01':
            content += '0'
    f1.write(content+'\n')
f.close()
f1.close()
```

可以看到解码后的文件组成了一个类似二维码的东西



再次进行脚本处理,将01字符转化成图像,0表示黑,1表示白。

```
#!/usr/bin/env python
from PIL import Image
im = Image.new('RGB',(100,100),0xffffff)
im.save('blank.png','PNG')
img = Image.open('blank.png')
with open('con.txt') as f:
    con = f.read()
x,y,i = 0,0,0
length = len(con)
while i<length:
    if con[i] == '\n':
        v+=1
        x=0
        i+=1
        continue
    elif con[i]== '0':
        img.putpixel((x,y),(255,255,255))
    elif con[i]== '1':
        img.putpixel((x,y),(0,0,0))
    i+=1
    x+=1
img.save('result.png')
```



扫描得到http://47.93.205.124/d39ed8ea9184468644ed90dd20b10cc5.html

但是这个网址打不开打不开打不开......

所以,又卡住了.....