2017湖湘杯Writeup

转载

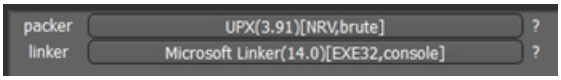
weixin_30642029 于 2017-11-26 13:31:00 发布 178 收藏
文章标签： php 移动开发
原文链接：http://www.cnblogs.com/L1B0/p/7898849.html

RE部分

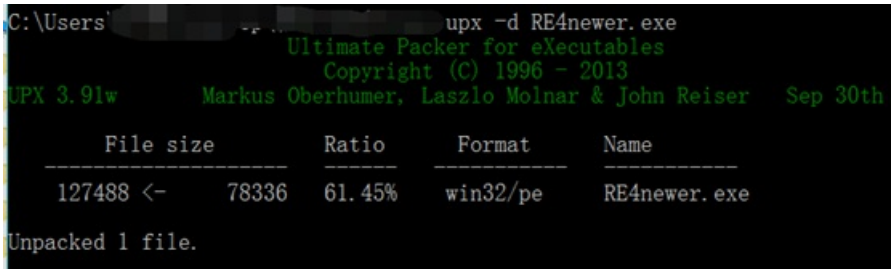
0x01 Re4newer

解题思路：

Step1：die打开，发现有upx壳。



Step2：脱壳，执行upx -d 文件名即可。



Step3：IDA打开，shift+F12看字符串。

点进去，F5看伪代码如图。

```
int sub_401160()
{
  int v0; // eax@1
  int v1; // ecx@1
  int v2; // ecx@3
  signed int v3; // eax@5
  char v5; // [sp+0h] [bp-3F4h]@1
  char v6; // [sp+8h] [bp-3ECh]@7

  sub_4087D0(&v5);
  v0 = sub_408A9C(&v5);
  v1 = *(_DWORD *)(v0 + 20) + 1900;
  if ( v1 > 2051 && v1 < 2053 )
  {
    v2 = *(_DWORD *)(v0 + 16) + 1;
    if ( v2 > 2 && v2 < 4 )
    {
      v3 = *(_DWORD *)(v0 + 12);
      if ( v3 > 13 && v3 < 15 )
      {
        sub_401020("Input your flag:", v5);
        sub_401050("%s", (unsigned int)&v6);
        sub_401080(&v6, strlen(&v6));
      }
    }
  }
  return 0;
}
```

Step4：逆算法。点进sub_401080可以看到关键函数的算法。

```
16  v4 = xmmword_41D740;
17  v5 = xmmword_41D730;
18  v6 = xmmword_41D7A0;
19  v7 = xmmword_41D760;
20  v8 = xmmword_41D7D0;
21  v9 = xmmword_41D750;
22  v10 = xmmword_41D790;
23  v11 = xmmword_41D780;
24  v12 = xmmword_41D7C0;
25  v13 = xmmword_41D7B0;
26  v14 = xmmword_41D770;
27  if ( a1 == 44 )
28  {
29    v3 = 0;
30    do
31    {
32      if ( (*(_BYTE *)(v3 + a2) ^ 0x22) != *((_DWORD *)&v4 + v3) )
33        break;
34      ++v3;
35    }
36    while ( v3 < 44 );
37    if ( v3 == 44 )
38      sub_401020("success!\n", a3);
39    else
40      sub_401020("wrong~\n", a3);
41  }
42 }
```

是简单的取字节异或，比较对象是v4-v14的值。

```
xmmword_41D730  xmmword 13000000A0000007600000059h
                                        ; DATA XREF: sub_401080+22↑r
xmmword_41D740  xmmword 450000004300000004E00000044h
                                        ; DATA XREF: sub_401080+13↑r
xmmword_41D750  xmmword 520000004F0000004B00000051h
                                        ; DATA XREF: sub_401080+59↑r
xmmword_41D760  xmmword 540000007D0000006300000007Dh
                                        ; DATA XREF: sub_401080+40↑r
xmmword_41D770  xmmword 5F0000005600000013000000 7Dh
                                        ; DATA XREF: sub_401080+90↑r
xmmword_41D780  xmmword 670000006700000070000000 70h
                                        ; DATA XREF: sub_401080+6F↑r
xmmword_41D790  xmmword 700000007D0000004700000004Eh
                                        ; DATA XREF: sub_401080+64↑r
xmmword_41D7A0  xmmword 710000004B0000007D00000051h
                                        ; DATA XREF: sub_401080+32↑r
xmmword_41D7B0  xmmword 710000005100000063000000 52h
                                        ; DATA XREF: sub_401080+85↑r
xmmword_41D7C0  xmmword 7D0000005700000007D00000067h
                                        ; DATA XREF: sub_401080+7A↑r
xmmword_41D7D0  xmmword 7D0000005B0000005000000011h
                                        ; DATA XREF: sub_401080+4E↑r
```

可以看到，这里可以分成44个两位16进制的数，并且顺序与箭头所指的数的大小有关。

Step4：得到flag。

pyhon脚本如下：

a = [0x45,0x43,0x4E,0x44,

0x13,0x4A,0x76,0x59,

0x71,0x4B,0x7D,0x51,

0x54,0x7D,0x63,0x7D,

0x7D,0x5B,0x50,0x11,

0x52,0x4F,0x4B,0x51,

0x70,0x7D,0x47,0x4E,

0x67,0x67,0x70,0x70,

0x7D,0x57,0x7D,0x67,

0x71,0x51,0x63,0x52,

0x5F,0x56,0x13,0x7D]

flag = ''

for i in range(11):

for j in [3,2,1,0]:

*flag += chr(a[i*4+j]^0x22)*

print(flag)

0x02 简单的android

解题思路：

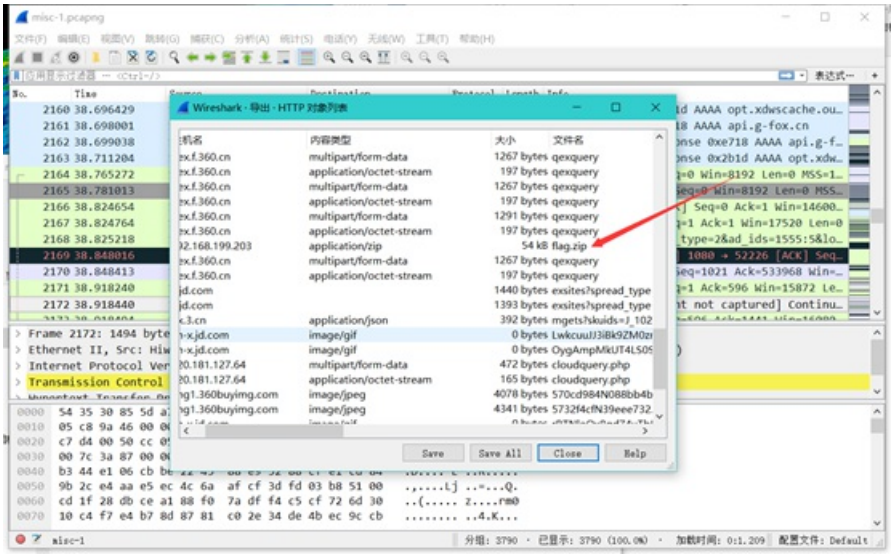
Step1：直接apk_tool打开，点jadx，得到flag。

MISC部分

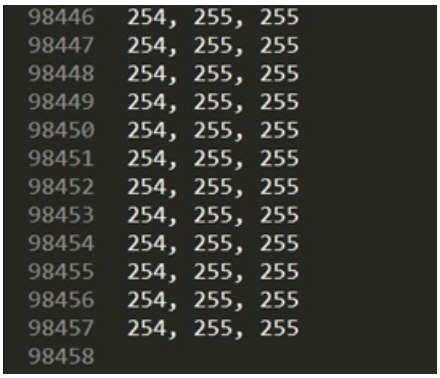
0x03 流量分析

解题思路:

Step1：直接打开，文件->导出对象->HTTP，可以看到flag.zip，保存下来。



Step2：flag.zip里面有很多数字，目测是RGB，于是写脚本形成图片。




```
>>> for i in range(2,1000):
        if int(98457/i) == 98457/i:
            print(i)


3
37
111
887
>>>
```

Step3：从上图可以猜想图片是宽为887，长为111。

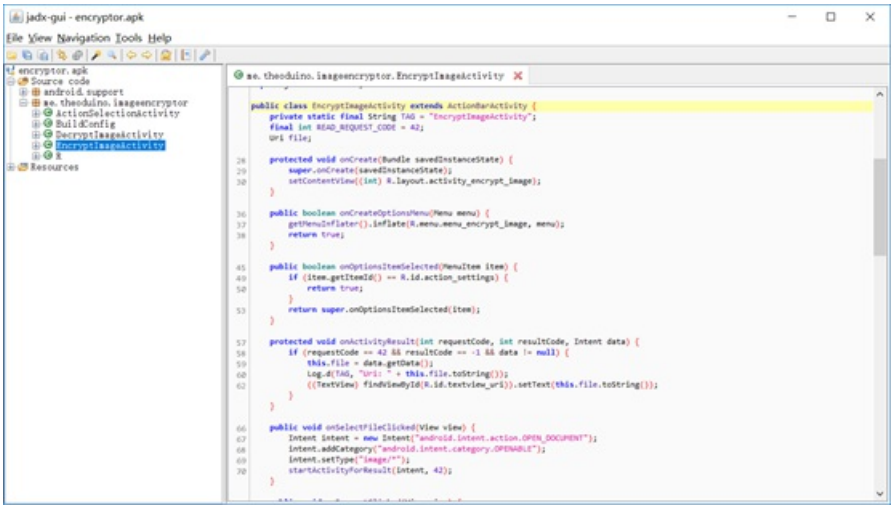
脚本如下：得到flag。

```
#-*- coding:utf-8 -*-
from PIL import Image
import re
x = 887 #x坐标  通过对txt里的行数进行整数分解
y = 111 #y坐标  x*y = 行数
im = Image.new("RGB",(x,y))#创建图片
file = open('ce.txt') #打开rbg值文件
#通过一个个rgb点生成图片
for i in range(0,x):
    for j in range(0,y):
        line = file.readline()#获取一行
        rgb = line.split(",")#分离rgb
        im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))#rgb转化为像素
im.show()
```

0x04 MISC200

解题思路：

压缩包里一个apk和一个疑似被加密的flag，先把apk拖到apktools里看下源码，



可以看到一个EncryptImageActivity，貌似有点用
可以看到很useful的函数

```
public void onEncryptClicked(View view) {
    String password = ((EditText) findViewById(R.id.text_password)).getText().toString();
    if (password.equals("")) {
        Toast.makeText(getApplicationContext(), "You must enter a password!", 0).show();
        return;
    }
    byte[] key = md5(password);
    if (this.file.toString().length() == 0) {
        Toast.makeText(getApplicationContext(), "You must select a file!", 0).show();
        return;
    }
    try {
        byte[] cipherText = encryptData(readUri(this.file), key);
        try {
            File outputFile = new File(getOutputPath(), generateRandomFilename(8) + ".encrypted");
            try {
                FileOutputStream fileOutputStream = new FileOutputStream(outputFile);
                fileOutputStream.write(cipherText);
                fileOutputStream.close();
                Toast.makeText(getApplicationContext(), "Successfully created file " + outputFile.getAbsolutePath(), 1).show();
            } catch (FileNotFoundException e) {
```

继续往下看

```
private byte[] encryptData(byte[] data, byte[] key) {
    byte keyLength = (byte) key.length;
    byte[] cipherText = new byte[data.length];
    for (int i = 0; i < data.length; i++) {
        cipherText[i] = (byte) (data[i] ^ key[i % keyLength]);
    }
    return cipherText;
}
```

这就是对文件进行加密的具体函数了，可以看到，使用key对文件逐位异或得到cipherText，联系上面的关键函数，可以得知，这个程序的工作流程：

1选择一个文件

2输入密码

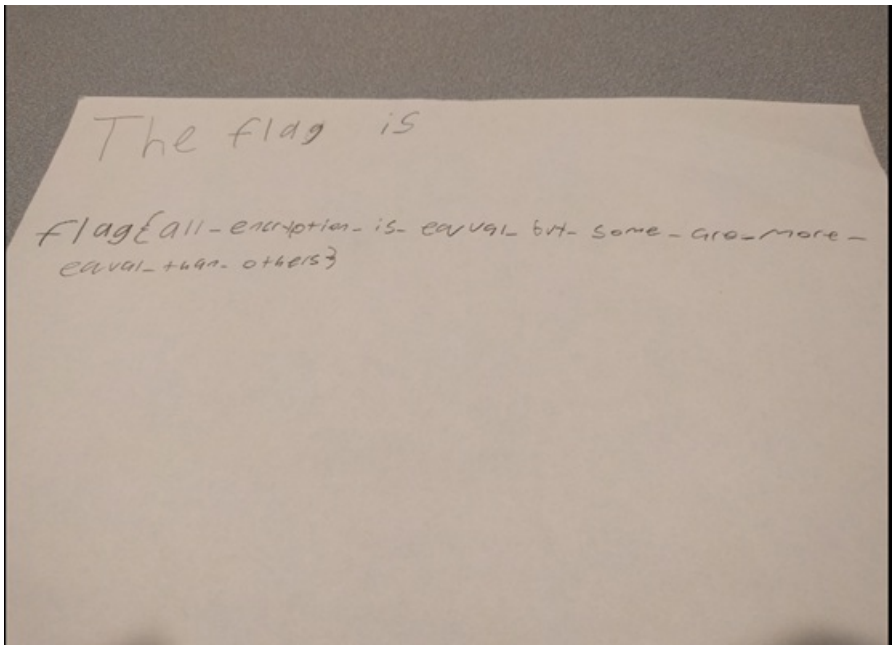
3使用密码的md5值对原始文件进行逐位异或

4将加密后的cipherText写入新文件并输出

由于异或的特性，使用password的md5值对已经加密的文件再次加密能够得到原来的文件，所以我们的任务就是逆向找到password了！！

上一句划掉

那么麻烦干嘛，扔到手机里运行一下（才不说我专心逆向找password，怕手机被加密另开了手机分身运行应用呢），发现密码已经是“记住”状态了，把flag.encrypted扔进去点击encrypt就会提示成功的创建了文件，只要提出来在Linux里直接能显示出图片了。



Flag：

出题人你出来，自己选砖头！神™字迹辨认

0x05 Misc300

解题思路：

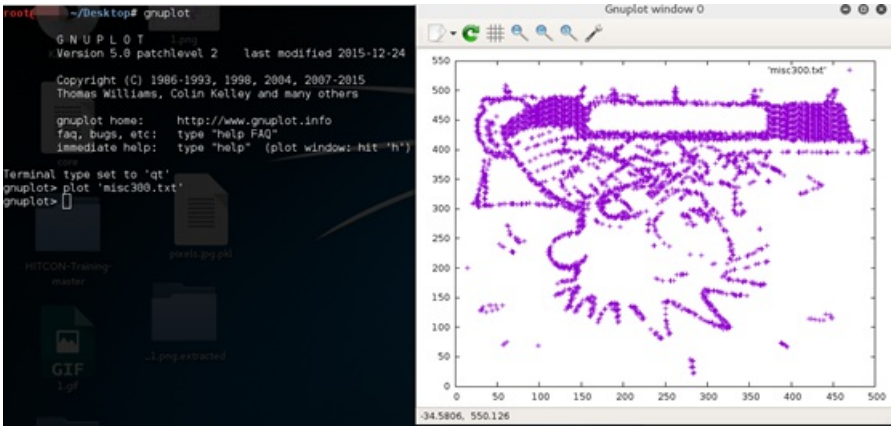
Step1：文件是pxl后缀，于是上网搜了一下。

```
>>> import pickle
>>> f = open('pixels.jpg.pkl')
>>> print(pickle.load(f))
```

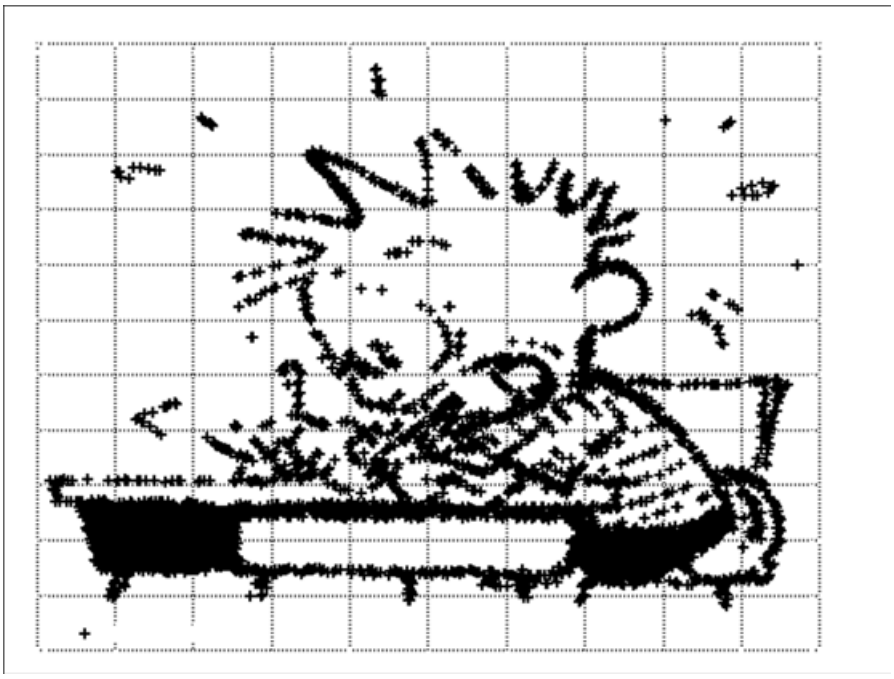
用这个脚本打开文件，发现是一堆坐标，联想到是黑白图片的坐标，出现的位置为1，否则为0。

Step2：将这堆数据处理成如图形式，执行第二张图片所示的代码，可以得到一张图片。

```
15 200
21 308
23 310
24 314
25 308
25 318
25 431
25 441
25 451
26 310
26 320
26 429
26 439
26 449
27 305
27 315
27 325
27 423
27 433
27 443
27 453
28 303
28 313
28 323
28 333
28 419
28 429
28 439
28 449
```



将所得图片倒置反色得到如图



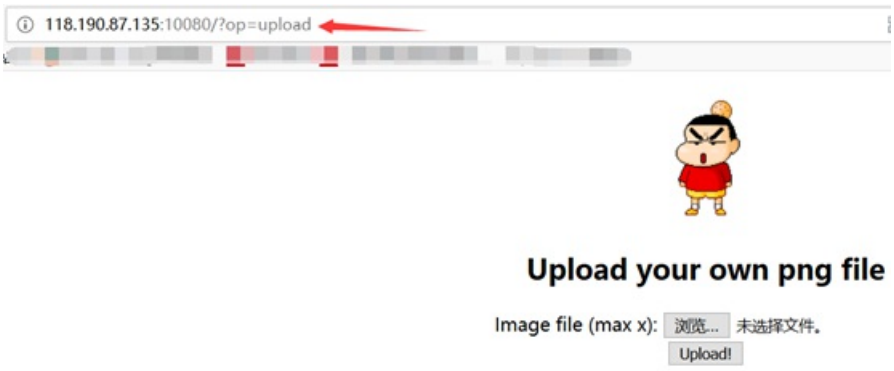
可知是一个卡通人物，是熟悉的*Bill Watterson*创造的，于是得到flag{小写名字}。

WEB部分

0x06 Web200

解题思路：

Step1：看到题目是文件上传，于是构造payload试试。



Step2：

http://118.190.87.135:10080/?op=php://filter/read=convert.base64-encode/resource=flag

得到flag的base64编码，解码得到flag。

总结

1.这次的Re主要就试了一下脱壳，最后那道400分的pyc怼不出来....

2.Misc部分第一次做流量包分析的题目，也算学习了一波，这次有两道题都是要用脚本或库形成图片的；

0x03是需要将所给的RGB值转换成图片，0x05是需要将坐标转换为黑白图片中RGB为0或1；这里附上M4x大佬的博客http://www.cnblogs.com/WangAoBo/p/6950547.html

3.Web部分太菜了就搞了一道，文件上传之前也看到过类似的题，在钿神的提示下拿flag.php的内容就A了。

Tips：

Re和Misc题目

链接：http://pan.baidu.com/s/1eSH9seY 密码：wc0x

Upx脱壳和Apktool工具

链接：http://pan.baidu.com/s/1eRA72le 密码：abch

作者： LB919
出处：http://www.cnblogs.com/L1B0/

转载于:https://www.cnblogs.com/L1B0/p/7898849.html