XCTF攻防世界：MISC新手题解（7~12）

原创

CNwanku 于 2019-12-18 11:29:34 发布 953 收藏 2

文章标签： 信息安全 反编译 jar 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。

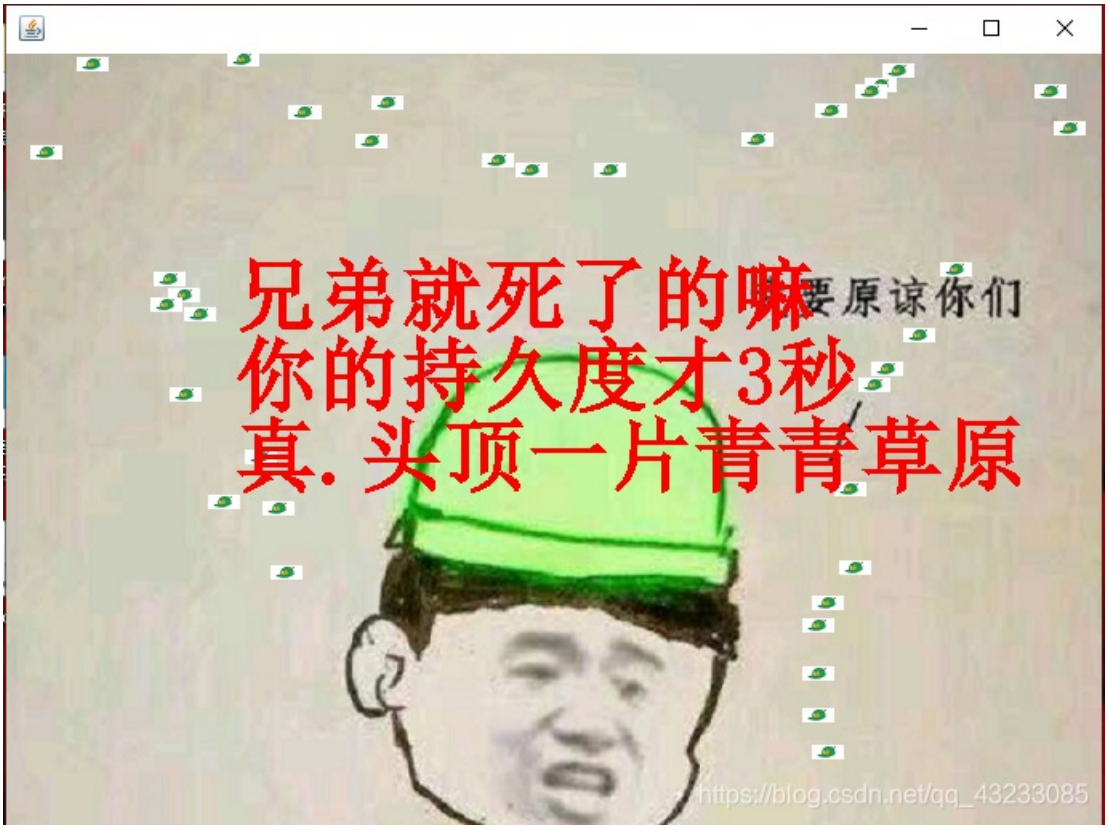
本文链接：https://blog.csdn.net/qq_43233085/article/details/103594407

版权

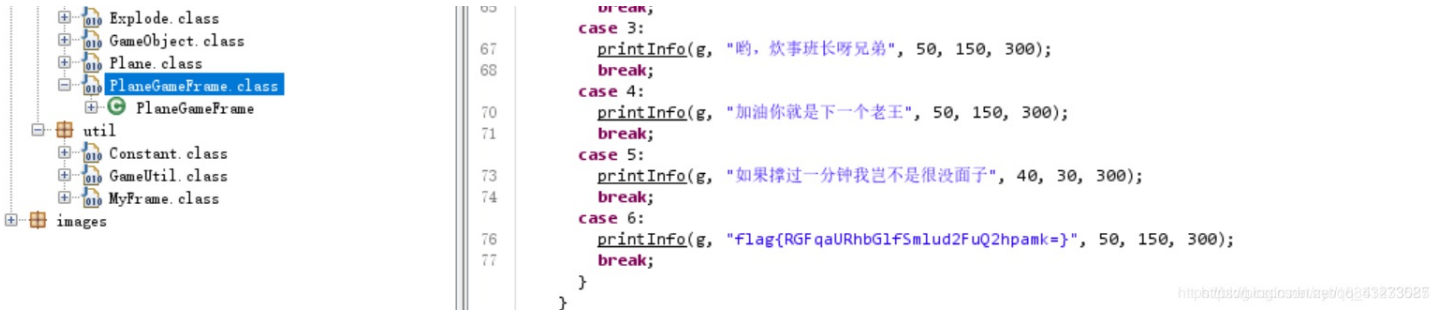
XCTF攻防世界：MISC新手题解（7~12）

坚持60s

下载是个打包的java程序，打开是一个游戏文件



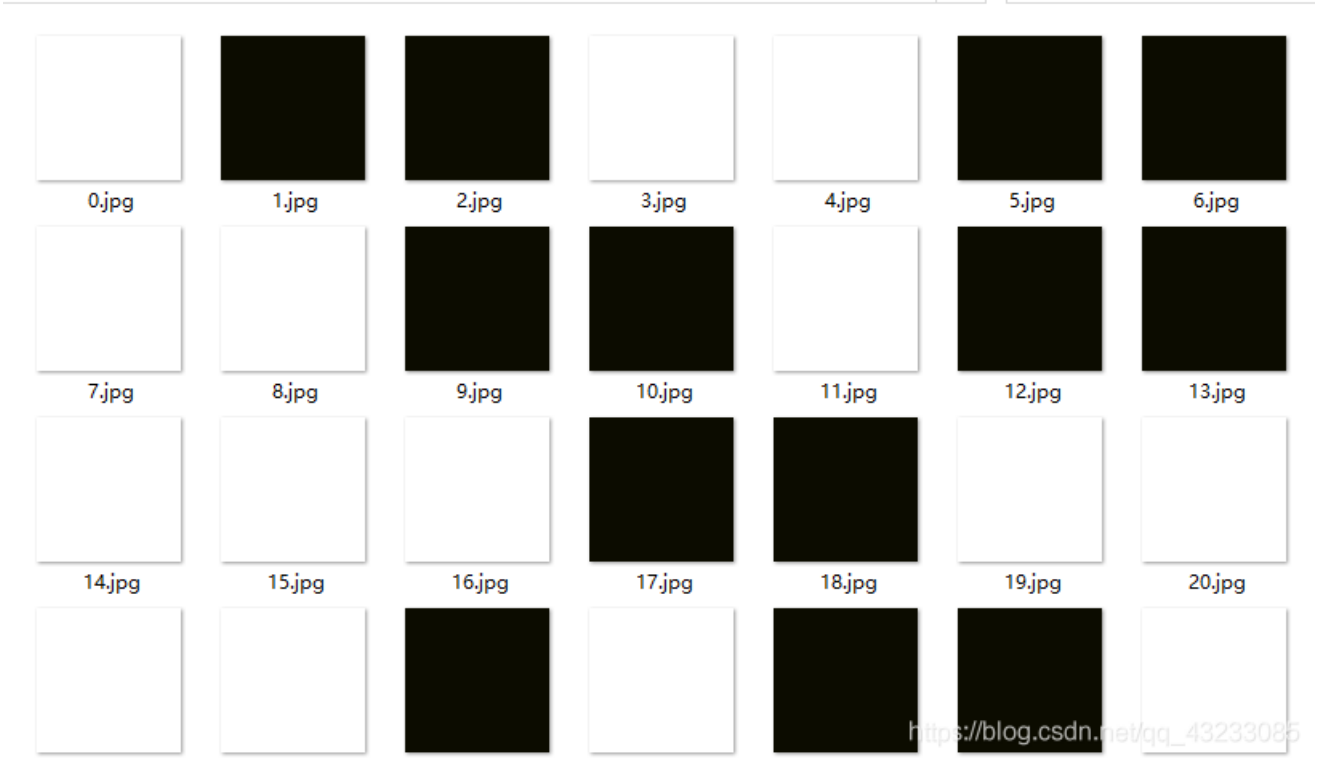
既然是程序会给出flag，那么flag就在源代码中了，用java反编译工具反编译，在文件中可以找到PlaneGameFrame.class中找到flag(大括号中base64需要解码)。



得到 flag{DajiDali_JinwanChiji}

gif

打开压缩包发现许多张黑白颜色的图片



将黑白图片分别记为1,0，得到

```
01100110011011000110000101100111011111011010001100111010101001110010111111011001110110100101000110011111101
```

转化为字符串形式即可

```
import re
a = '01100110011011000110000101100111011111011010001100111010101001110010111111011001110110100101000110011111101'
b = re.findall(r'.{8}', a)
flag = ''
for i in b : flag += chr(int(i, 2))
print(flag)
```

得到flag{FuN_giF}

掀桌子

现题目中的字符串由0-9、a-f组成，我们知道2位十六进制可表示1个字节，写脚本将该字符串两两分组转换成字节，发现所有字节均大于128，我们又知道ASCII码表示范围是0-127，于是每一个字节都减去128，再转换成字符串，得到flag

```
cc = '\xc8\xe9\xac\xa0\xc6\xf2\xe5\xf3\xe8\x
cd = ''
for i in cc:
    cd+=chr(ord(i) - 128)
print(cd)
```

```
C:\WINDOWS\system32\cmd.exe
Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr
请按任意键继续. . .
```

https://blog.csdn.net/qq_43233085

得到flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

如来十三掌

下载后发现为一串看不懂的文字，网上搜索发现有一个“与佛论禅”的网站，应该可以解密
网站地址：http://www.keyfc.net/bbs/tools/tudoucode.aspx
开始直接粘贴进去，好像解不了…

发现格式要在前面加上佛曰：

第一反应将其进行BASE64解密，但是解码失败，据题意，十三…ROT13编码。
将其先ROT13再加密一次即解密，之后再进行BASE64解码
得到flag值，flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

base64stego

本来以为又要与佛论禅了，结果发现它的加密是假的，用WinRAR的修复功能直接修复解压，发现了一个txt文件。
打开文件，进行base64解码，结果如下：

> Steganography is the art and science of writing hidden messages in such a way that no one

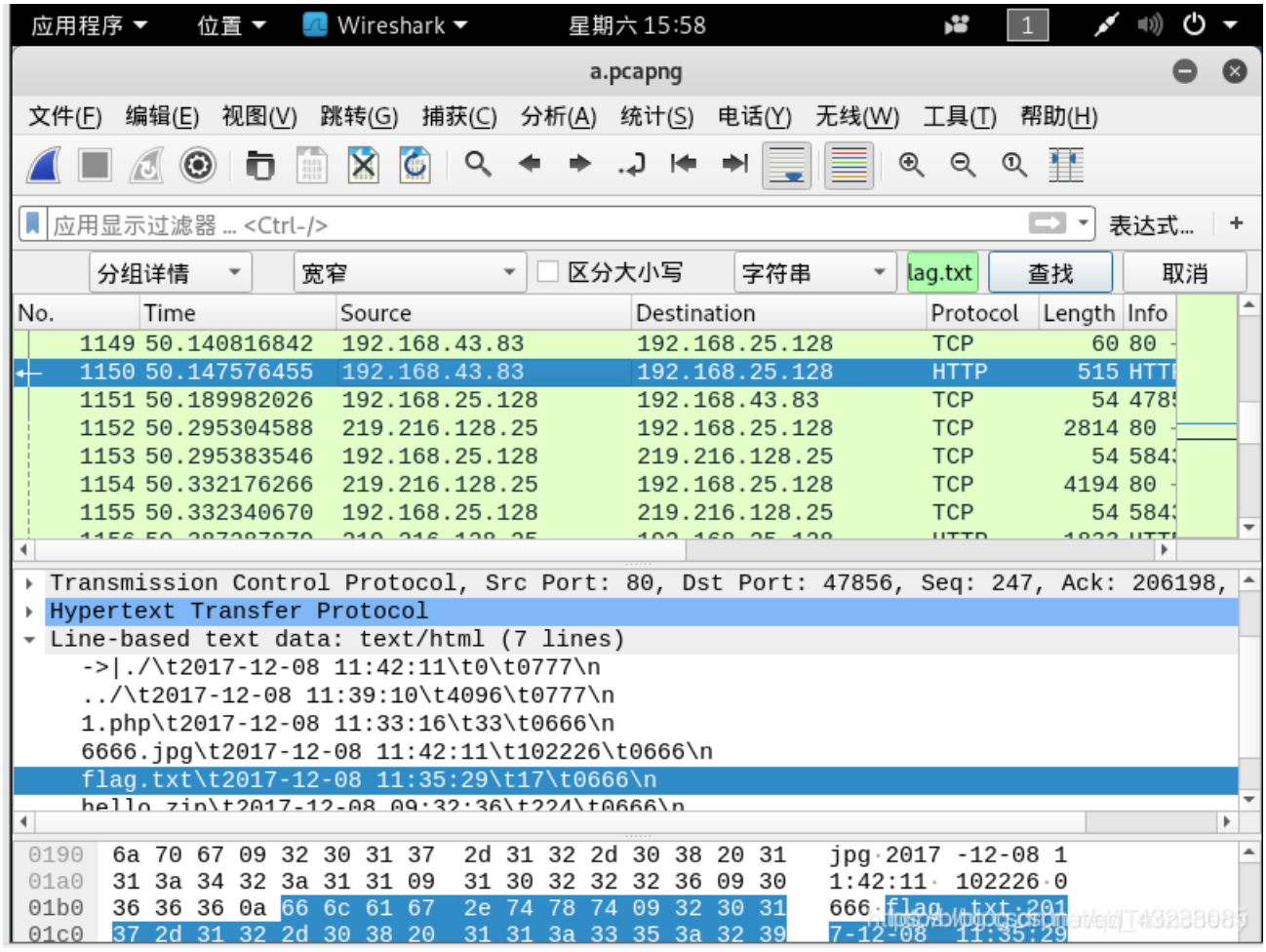
意思是说，隐写是个很好的解决方法
马上上网查了查，发现base64可以隐写的，并发现了大佬们的脚本代码

```
#coding=utf-8
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res
def solve_stego():
    with open('D:\\火狐下载\\1.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)
def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str
if __name__ == '__main__':
    solve_stego()
```

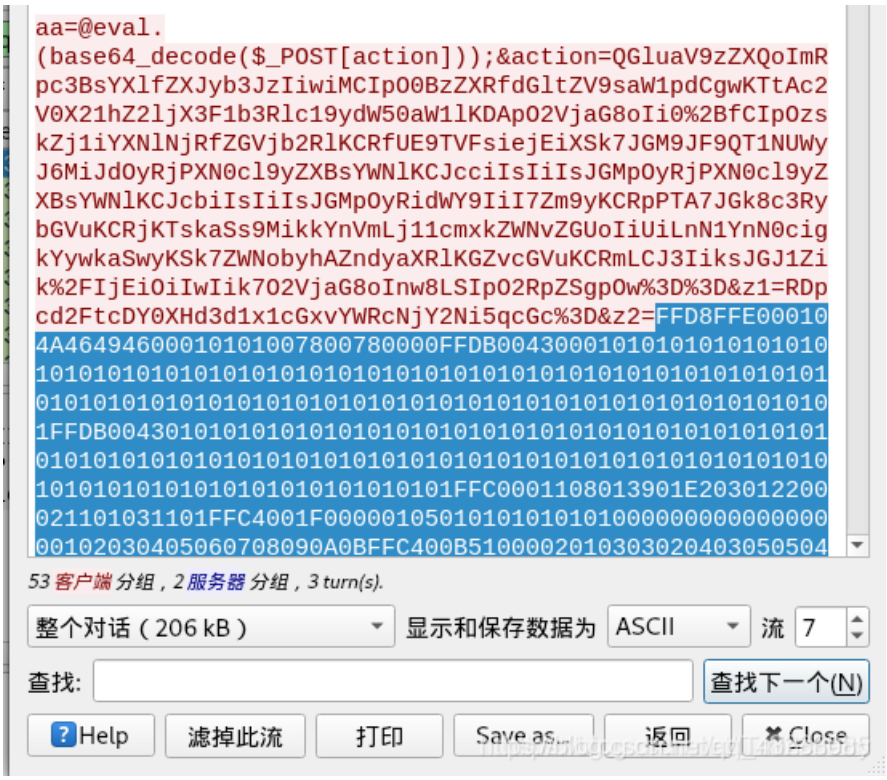
这个是python2的脚本，所以运行要用python2来运行，否则出错这里无法解决，编码符设置我为ANSI
跑下脚本，得到flag，flag{Base_sixty_four_point_five}

功夫再高也怕菜刀

下载附件，用foremost进行pcapng文件的分离，得到一个zip，打开zip，得到一份加密的flag.txt文件。然后用wireshark打开pcapng文件，查找flag.txt关键字



发现有个6666.jpg，右键第1150个数据包，追踪TCP流，复制从FFD8开始到FFD9的内容，到winHex里新建文件粘贴，注意粘贴格式是ASCII Hex。

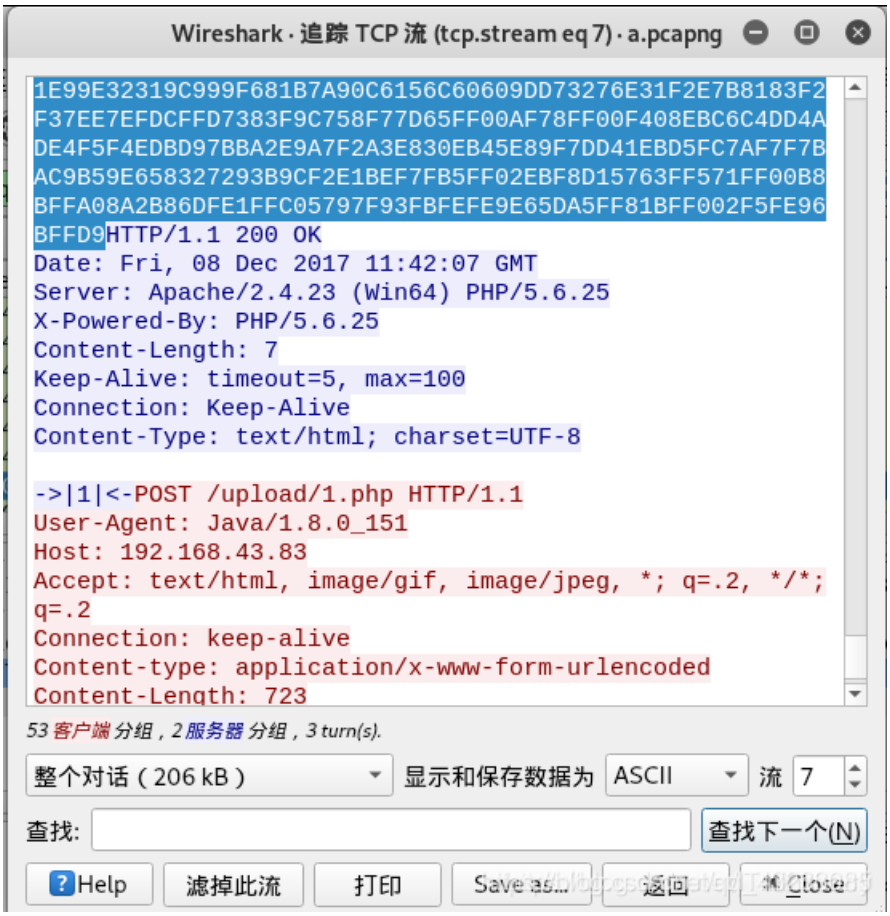


53 客户端 分组，2 服务器 分组，3 turn(s).

整个对话（206 kB） 显示和保存数据为 ASCII 流 7

查找: 查找下一个(N)

Help 滤掉此流 打印 Save as... 返回 Close



保存为jpg格式，可以得到图片，

图片里的文字就是密码，输入密码，得到flag。
flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}