

week2 0yster's writeup

这周做得很水，好多题都是一路做到最后就是卡住没出结果。菜是原罪不多说，不过端正态度想想题目虽然没做出来，但是期间学到了许多姿势和知识，至少也不是一无所获。



re

Pro的Python教室(二)

下下来的pyc拿去在线反编译得到代码：

```
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'io0avquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue

enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You 're Right!"
else:
    print "You're Wrong!"
```

分析代码可知：输入流奇数位的字符的ASCII码加1，偶数位的加2。然后隔了3位重组字符串。

那对应写解密脚本，就是先三位三位取出然后重组得到字符ASCII码改变的字符串，然后字符串每个字符按奇偶位对ASCII码进行操作反推出flag。

```
#coding=utf-8
aaa = 'io0avquaDb}x2ha4[~ifqZaujQ#'
enc1=[]
flag=[]

for i in range(9):
    enc1.append(aaa[i])
    enc1.append(aaa[i+18])
    enc1.append(aaa[i + 9])

for j in range(len(enc1)):
    if j % 2 == 0:
        flag.append(chr(ord(enc1[j])-1))
        continue
    flag.append(chr(ord(enc1[j]) - 2))
print ''.join(flag)
```

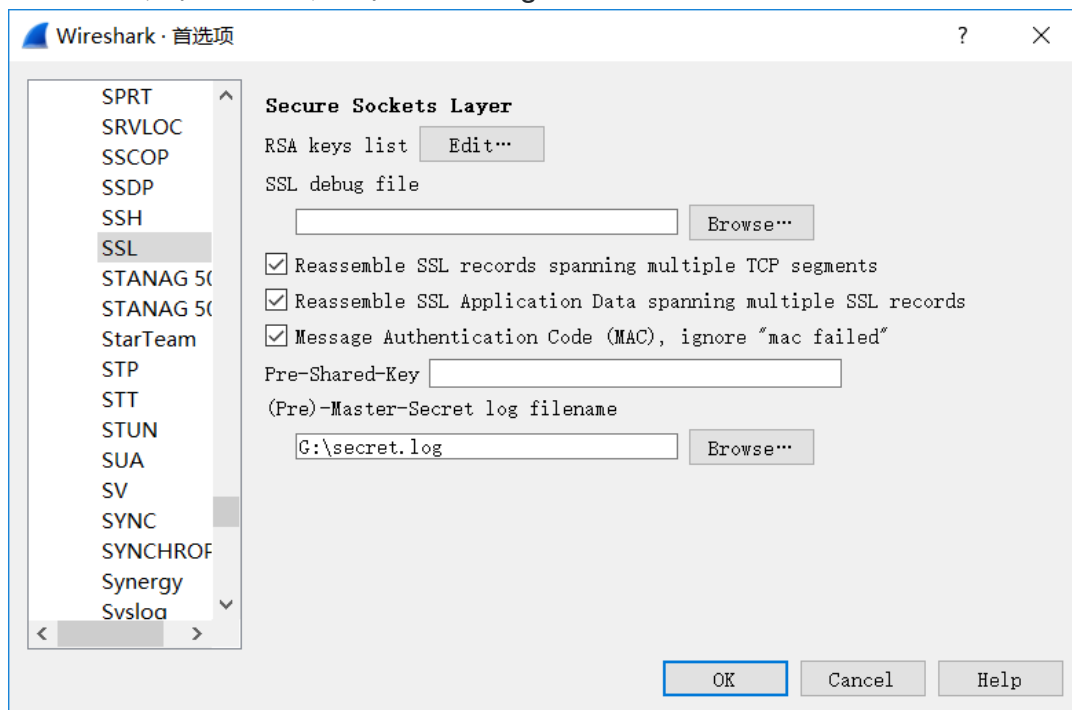
跑出来结果hgame{Now_Y0u_got_th3_PYC!}

misc

找得到我嘛？小火汁

下载得到的流量包打开，先导出对象无果。于是按16进制搜索zip特征头，找到一个压缩包。提取出来，里面的文件是secret.log。经谷歌，猜测是解密https的密钥。

编辑首选项，在ssl协议出将secret.log导入



此时尝试导出对象，发现多出1.tar这个文件

分组	主机名	内容类型	大小	文件名
16	192.168.61.135	text/html	41 bytes	\
22	192.168.61.135	text/html	3650 bytes	favicon.ico
25	192.168.61.135	text/html	41 bytes	index.html
58	192.168.61.135	text/html	41 bytes	\
64	192.168.61.135	text/html	3650 bytes	favicon.ico
194	192.168.61.135	application/octet-stream	116 kB	1.tar

里面的文件在winhex下打开找到flag

crypto

Vigener~

打开复制，直接找个解密网站

这里真的是没有比较，没有伤害。vigener在线无密钥解密的网站，百度找死没找到，谷歌一查就出。

<https://www.kidclark.com/vigener/>

维吉尼亚密码在线解密

请输入要加密的明文

The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the nineth century and so acquired its present name. flag is gfyuytukariyydfjlpwxsdbzwvqt

加密

无密钥解密

密钥: guess

密钥长度(选填)

有密钥解密

密钥

请输入要解密的密文

Zbi Namyrwjk wmhzk cw s eknlqv uz ifuxstlata edhnufwlow xwpz vc mkohk s kklmwk uz mflklagnkh Gswyuv uavbjik, huwvv uh xzw rylwmxm sx s qycogxx. Ml ay u jgis ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnyv ak kuwg lu orvwmxsfj urv asjpwekhx, tmz cx jwycwlw upd szniehzm xg txyec az zsj lnlw ukhxmjoyw, ozowl wxshiv az nlw vkmgiavnmgf ry qzazlw atxiuzozijshfi. Ests twgvfi zsby xjaks xg asjpwekhx wflchloir kunyqwk zbel sxy ikkhhxasrfc Namyrwjk wmhzkwl. Af kckzkyr kadnc lzxyi, Xjoyhjaib Oskomoa ogm xzw lcvkl zi tmtrowz s myrwjgf qwlnih gx jygahnyvafm Pmywtvww uojlwiy. Nlw Noaifwxy gahnyv osy ivayohedde xikuxcfwv hs Kagbur Tsznmklg Viddqms af ncw gfk nlgyurv xopi zmtxvww ghx xaln- gfk vsgc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek qek dgnij eomellxcfmkx xg Trumkw jy Zaykhijw oh xzw tcrwln wifalc sfj ms suwomijw csk hxywvzf heew. Ifey ay ajgmenycpqlmqajzndhrqwpvhtaniz