Re

maze

用ida打开，f5 分析程序
发现一串奇怪的字符串\

```
"1111111111111111111111111111111111111111111111111111111111111111..............111111111111111..............111"
"111111111111.1111111111111.11111111111111.1111111111111.11111111111111.1111111111111.11111111111111.1111111111111"
".11111111111111.111111111111.11111111111111.111111111111.11111111111111.111111111111s11111111111111.111111111"
"1111s11111111111111.1111111111111111111111111111.1111111111111111111111111111.1111111111111111111111111111.11111"
"11111111111111111111111.11111111111111111111111111111.1111.11111111111111111111111.1t...........11111111111111.1"
"t...........11111111111111.111111111111.11111111111111.111111111111.11111111111111.111111111111.111111111111"
"11.1111111111111.11111111111111.111111111111.11111111111111.111111111111.11111111111111.111111111111.111111111"
"111111.111111111111.11111111111111.111111111111.11111111111111.111111111111.11111111111111.111111111111.11111"
"111111111.111111111111.11111111111111..............11111111111111..............11111111111111111111111111111"
"1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111"
```

下面是不死的情况

```
v2 == 46
v2 == 115
if(i==v4-1) v2 == 116

a1 == 100 && y_2973<=17
a1==115 && x_2974 <=58
a1==119 && y_2973>0
a1==97 && x_2974>0
```

查了一下Ascii。嗯？不就是打游戏么，'a'后退一格，'d'前进一格，'w'向前跳跃60格，'s'向后跳跃60格\
打游戏是不可能打游戏的，那就开挂吧（主要是当时觉得挺复杂的，总不能用生命打游戏吧）\
于是乎，脚本如下：

```
#maze.py

str='1111111111111111111111111111111111111111111111111111111111111111..............111111111111111..............111111111111111.1111111111111.11111111111111.1111111111111.1111111
y_2973 = 5
x_2974 = 22
a1=['d','s','a','w']
a2='d'*12
def jianyan(a2,y_2973,x_2974,str):
        flag=True
        for n in range(len(a2)):
            i=a2[n]
            if i=='d' and  y_2973<=17:
                resoult = str[60*y_2973+x_2974+1]
                if resoult == '.' or resoult=='s':
                    x_2974+=1
                else:
                    flag=False
                    break
            if i=='s' and x_2974<=58:
                resoult = str[60*(y_2973+1) + x_2974]
                if resoult == '.' or resoult=='s':
                    y_2973+=1
                else:
                    flag=False
                    break
            if i=='w' and y_2973>0:
                resoult = str[60*(y_2973-1) + x_2974]
                if resoult == '.' or resoult=='s':
                    y_2973-=1
                else:
                    flag=False
                    break
            if i=='a' and x_2974>0:
                resoult = str[60*y_2973 + x_2974-1]
                if resoult == '.' or resoult=='s':
                    x_2974-=1
                else:
                    flag=False
                    break
        if resoult =='t':
            print(a2)
            print("end")
            return [True,True]
        elif not flag:
            return [False,False]
        else:
            return [True,False]

str_box_old=['w']
str_box_new=[]
while True:
    for a2 in str_box_old:
        for m in a1:
            a2=a2+m
            print(len(a2),end=' ')
            print(a2)
            [is_OK,is_end] = jianyan(a2,y_2973,x_2974,str)
            if is_OK and not (a2[-2:] in ['sw','ws','da','ad']):
                str_box_new.append(a2)
                if is_end:
                    print(a2)
                    print("END!")
                    break
            a2=a2[:-1]
    str_box_old=str_box_new
```

```
    str_box_new=[]
    if is_end:
        break
```

这是最终版本。前几个版本由于没有意识到无意义的移动，跑了很久很久很久。。。
就加了

```
and not (a2[-2:] in ['sw','ws','da','ad'])
```

分分钟End！

brainfxxker's revenge

一开始想爆破来着（还是太天真了），于是不怀好意地py出题人去了。\
知道了位数正确会输出'w rongansw er!'或'congratulations!'\
一开始美滋滋，后来一想就觉得不对，我问之前自己也乱输了好多字符没啥动静啊。
一测，72个字符。。。~~我爆你个锤子呦~~\
后来盯着'代码'看就久了也知道要化简，怎么化简呢？（1+1-1型的已经化简了）\

```
#brainfucker's revenge
str1='>,>++++++[<------------------>-][+<]<--[<+>[-]][.>[<.[<-<[+>-<]-<.]][<[,>.[[->][,[-,.[,[,[,---<]-]-<[>[>>+[[--,+>][.,>>>].>]++<]]<[<[,,<]+,,].>]-<]][-<,..[,-<--]+].]+<]<-,],>++++++
str2=str1.replace('+-','')
str2=str1.replace('-+','')
str2=str1.replace('><','')
str2=str1.replace('<>','')
print(str2)
```

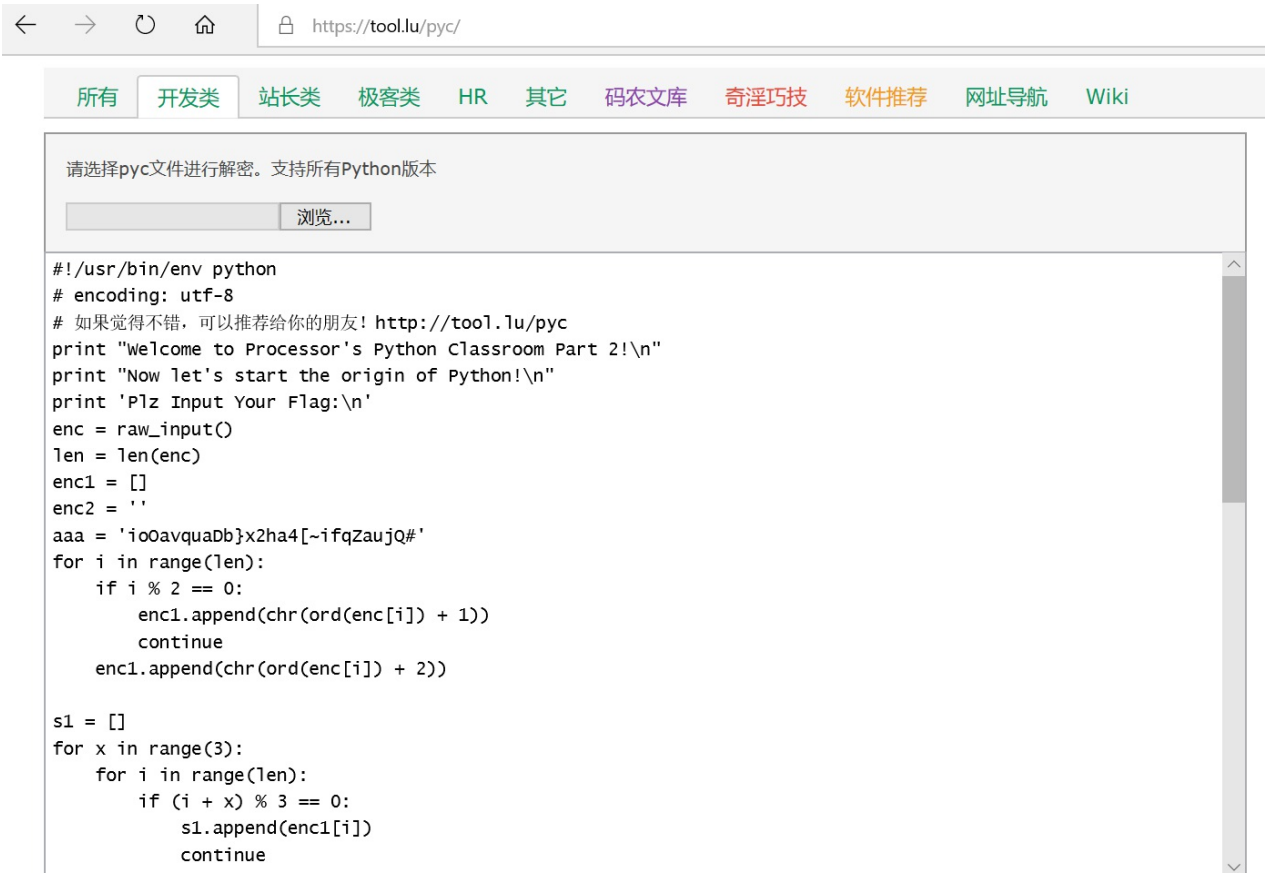
我想到了在72个字符输入完成之前，没有任何字符输出，这说明'.'没有被执行。\
于是乎，我就去消'.'了。于是乎，完蛋了。\
代码确实变干净了，但就是消不干净（这哪是两个脚本能解决的事情？！）\
不过在这个过程中，我发现还有一种可以化简代码的情况:\
']['能够从']'里出来的~~都是真男人~~都是0，当0遇上'['，简直完美！
于是乎，代码如下：

```
#brainfucker's revenge
str='>,>++++++[<------------------>-][+<]<--[<+>[-]][.>[<.[<-<[+>-<]-<.]][<[,>.[[->][,[-,.[,[,[,---<]-]-<[>[>>+[[--,+>][.,>>>].>]++<]]<[<[,,<]+,,].>]-<]][-<,..[,-<--]+].]+<]<-,],>++++++[

def huajian(i,str):
    unmatched=0
    for n in range(i+1,len(str)):
        if str[n]=='[':
            unmatched+=1
        if str[n]==']':
            unmatched-=1
            box=n
        if unmatched==0:
            break
    a='0'*(box-i)   #加'0'看看到底是哪些地方被删掉了
    str=str[:i+1]+a+str[box+1:]
    return[str]

for i in range(len(str)-1):
    if str[i]==']' and str[i+1]=='[':
        str=''.join(huajian(i,str))

str2=''
for i in range(len(str)):
    if str[i]!='0':
        str2=str2+str[i]
print(str2)

#以','为标志，分条打印
count=0;n=0
for i in range(len(str2)):
    if str2[i]==',':
        count+=1
        str3=str2[n:i]
        print(str3[1:])
        n=i-1
print(str2[n+1:])
print(count+1)
```

最后是放到bf1的代码里跑出flag

Pro的Python教室(二)

在线反编译



话不多说，上脚本：

```
a1 = 'ioOavquaD'
a2 = 'b}x2ha4[~'
a3 = 'ifqZaujQ#'
s1=[]
s2=''
for i in range(len(a1)):
    s1.append(a1[i])
    s1.append(a3[i])
    s1.append(a2[i])
s2=''.join(s1)

for i in range(len(s1)):
    if i %2 ==0:
        s1[i]=chr(ord(s1[i])-1)
        continue
    s1[i]=chr(ord(s1[i])-2)
s2=''.join(s1)
print(s2)
```

其实有个问题\

```
>>> s = "Alex aab"
>>> ret = "aa" in s
>>> print(ret)
True
>>> ret = "ab" in s
>>> printf(ret)
Traceback (most recent call last):
  File "<pyshell#6>", line 1, in <module>
    printf(ret)
NameError: name 'printf' is not defined
>>> print(ret)
True
>>> ret = "ab"in s
>>> print(ret)
True
>>> ret = "sds" in s
>>> print(ret)
False
```

```
enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You 're Right!"
else:
    print "You're Wrong!"
    exit(0)
```

所以并不需要enc2==aaa吧。

CRYPTO

Vigener

~~这才是真正的song-fen-ti啊~~