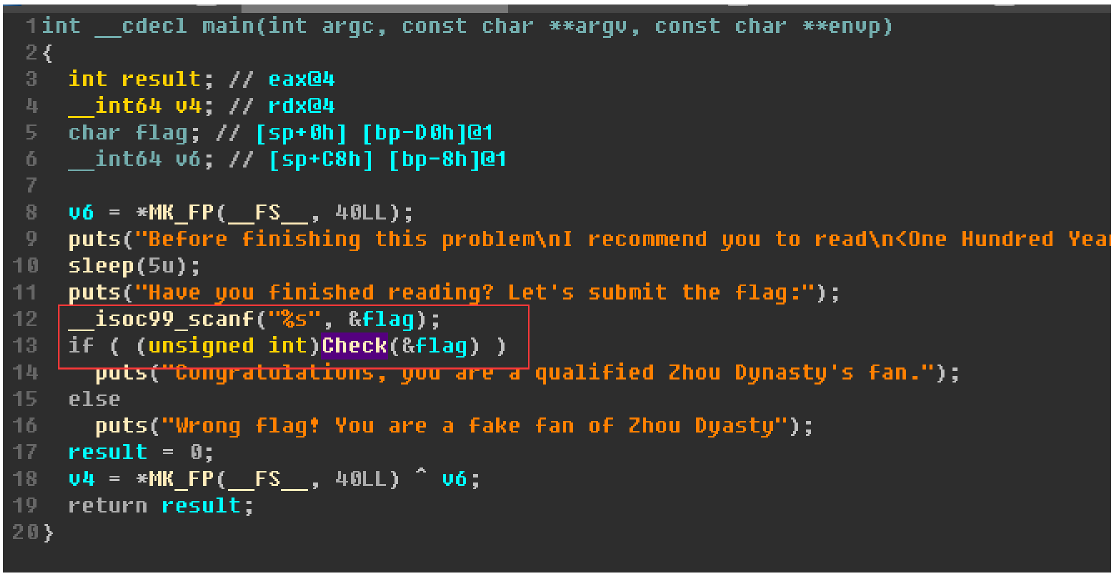
gonbe5 HGAME 2019 week-2 writeup

RE

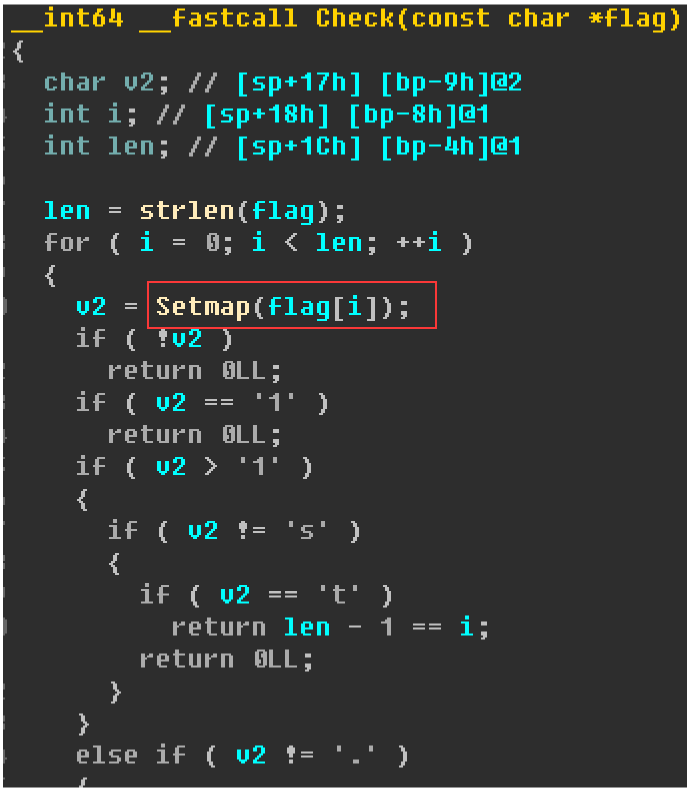
maze

打开 IDA 发现里面只有一个 Check



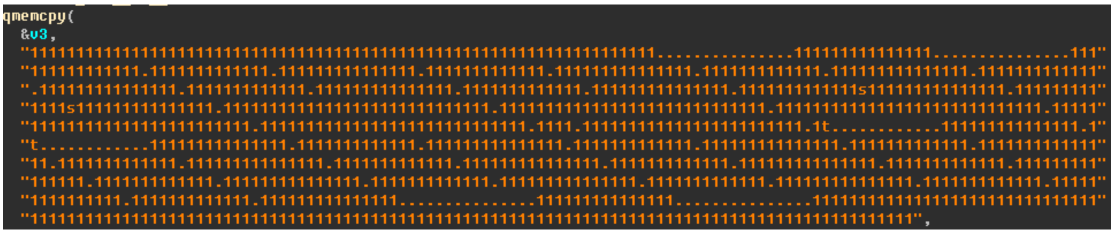
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax@4
  __int64 v4; // rdx@4
  char flag; // [sp+0h] [bp-D0h]@1
  __int64 v6; // [sp+C8h] [bp-8h]@1

  v6 = *MK_FP(__FS__, 40LL);
  puts("Before finishing this problem\nI recommend you to read\n<One Hundred Yea
  sleep(5u);
  puts("Have you finished reading? Let's submit the flag:");
  __isoc99_scanf("%s", &flag);
  if ( (unsigned int)Check(&flag) )
    puts("Congratulations, you are a qualified Zhou Dynasty's fan.");
  else
    puts("Wrong flag! You are a fake fan of Zhou Dyasty");
  result = 0;
  v4 = *MK_FP(__FS__, 40LL) ^ v6;
  return result;
}
```

是一些比较和跳转，Setmap 的地方进去看看



```
__int64 __fastcall Check(const char *flag)
{
  char v2; // [sp+17h] [bp-9h]@2
  int i; // [sp+18h] [bp-8h]@1
  int len; // [sp+1Ch] [bp-4h]@1

  len = strlen(flag);
  for ( i = 0; i < len; ++i )
  {
    v2 = Setmap(flag[i]);
    if ( !v2 )
      return 0LL;
    if ( v2 == '1' )
      return 0LL;
    if ( v2 > '1' )
    {
      if ( v2 != 's' )
      {
        if ( v2 == 't' )
          return len - 1 == i;
        return 0LL;
      }
    }
    else if ( v2 != '.' )
    {
```

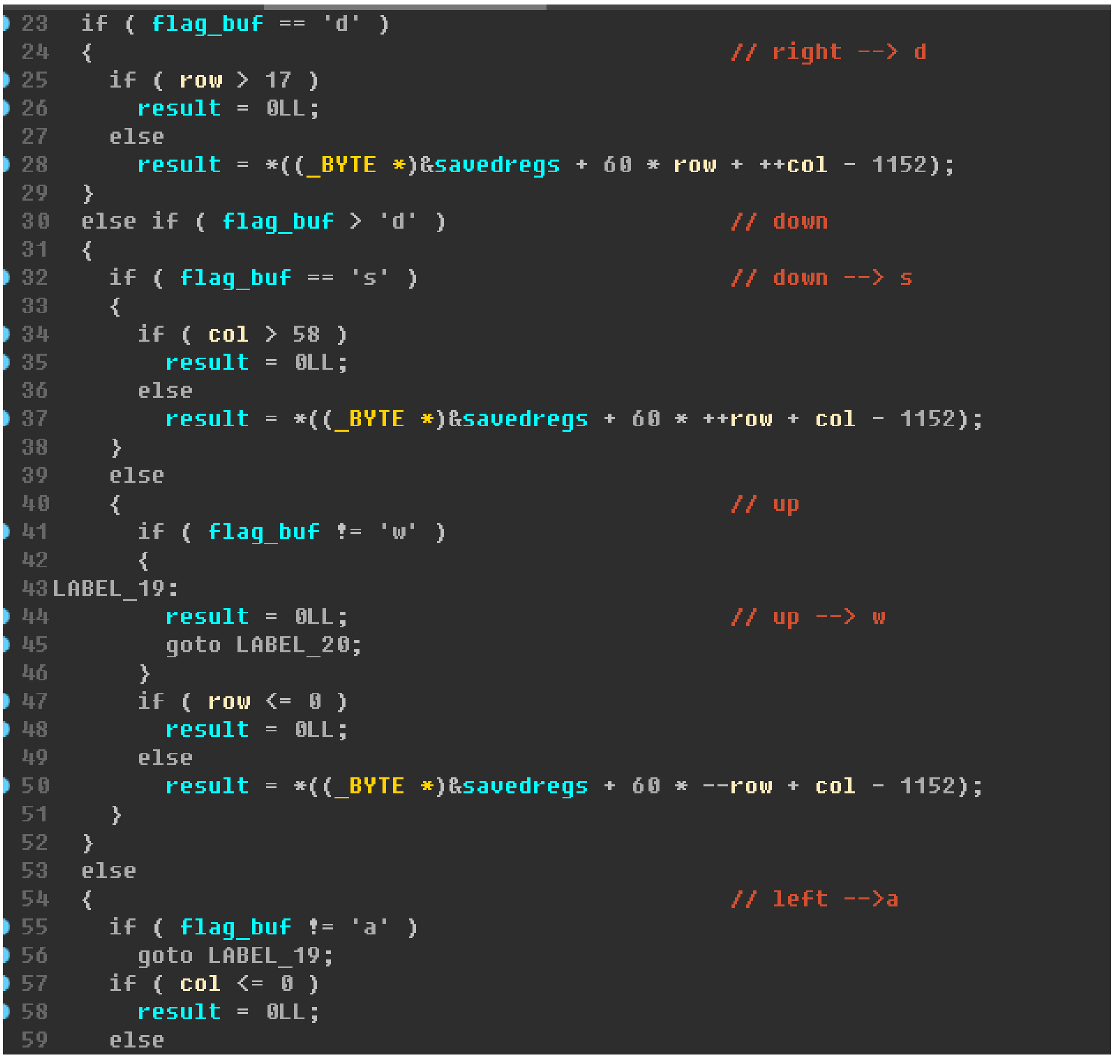
这串东西应该就是地图



```
qmemcpy(
  &v3,
  "111111111111111111111111111111111111111111111111111111111111111111111111111111...............111111111111111...............111"
  "111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111"
  ".111111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111s111111111111111.11111111"
  "1111s111111111111111.1111111111111111111111111111111.1111111111111111111111111111111.1111111111111111111111111111111.11111"
  "11111111111111111111111111.11111111111111111111111111111.1111.11111111111111111111111111.1t..............111111111111111.1"
  "t............111111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.111111111111111"
  "11.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.111111111"
  "111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.111111111111111.1111111111111.11111"
  "111111111.1111111111111.111111111111111...............111111111111111...............1111111111111111111111111111111"
  "111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111",
```

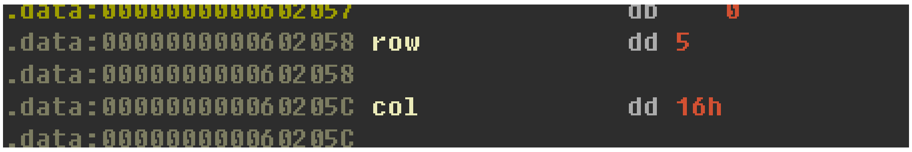
下面分别是 d, s, w, a 分别对应右，下，上，左，

其中还注意到：60*row， 那么相应的每一行的字符数就是 60



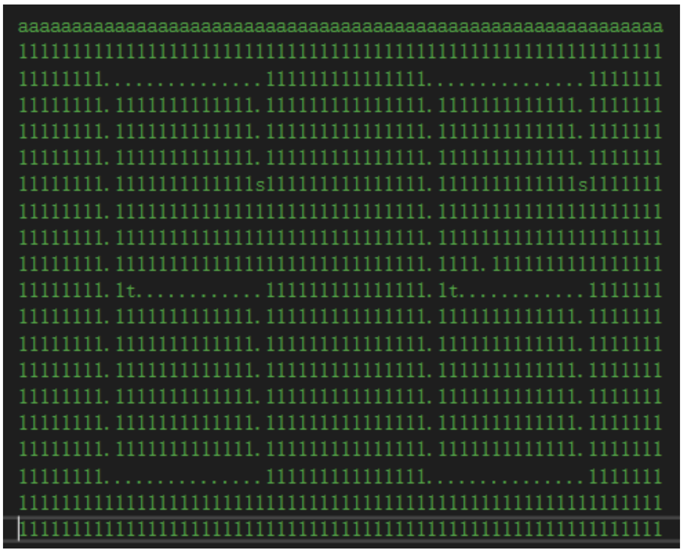
```
if ( flag_buf == 'd' )
{                                                 // right --> d
  if ( row > 17 )
    result = 0LL;
  else
    result = *((_BYTE *)&savedregs + 60 * row + ++col - 1152);
}
else if ( flag_buf > 'd' )                        // down
{
  if ( flag_buf == 's' )                          // down --> s
  {
    if ( col > 58 )
      result = 0LL;
    else
      result = *((_BYTE *)&savedregs + 60 * ++row + col - 1152);
  }
  else
  {                                               // up
    if ( flag_buf != 'w' )
    {
LABEL_19:
      result = 0LL;                               // up --> w
      goto LABEL_20;
    }
    if ( row <= 0 )
      result = 0LL;
    else
      result = *((_BYTE *)&savedregs + 60 * --row + col - 1152);
  }
}
else
{                                                 // left -->a
  if ( flag_buf != 'a' )
    goto LABEL_19;
  if ( col <= 0 )
    result = 0LL;
  else
```

找迷宫的初始位置（5， 22）

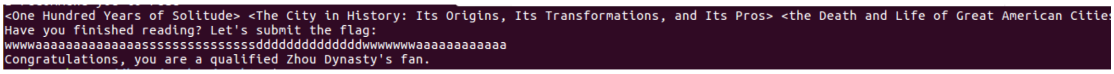


```
.data:0000000000602057                  db    0
.data:0000000000602058 row              dd 5
.data:0000000000602058
.data:000000000060205C col              dd 16h
.data:000000000060205C
```

接下来把地图扒下来，再根据之前得到的信息走迷宫



```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
111111111111111111111111111111111111111111111111111111111111
11111111...............111111111111111...............1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111s111111111111111.1111111111111s1111111
11111111.11111111111111111111111111111.111111111111111111111
11111111.11111111111111111111111111111.111111111111111111111
11111111.11111111111111111111111111111.1111.1111111111111111
11111111.1t............111111111111111.1t............1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111.1111111111111.111111111111111.1111111111111.1111111
11111111...............111111111111111...............1111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
```



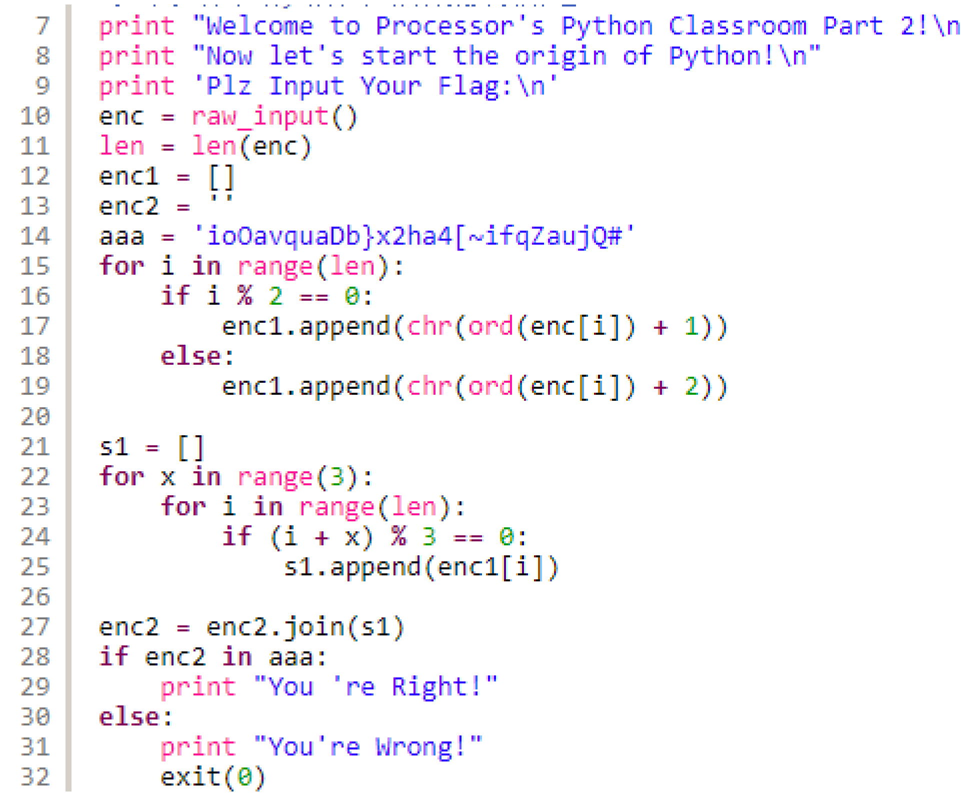
```
<One Hundred Years of Solitude> <The City in History: Its Origins, Its Transformations, and Its Pros> <the Death and Life of Great American Citie
Have you finished reading? Let's submit the flag:
wwwwaaaaaaaaaaaaaasssssssssssssssddddddddddddddwwwwwwwaaaaaaaaaaaa
Congratulations, you are a qualified Zhou Dynasty's fan.
```

套上 hgame{}就是 flag 了

hgame{wwwwaaaaaaaaaaaaaasssssssssssssssddddddddddddddwwwwwwwaaaaaaaaaaaa}

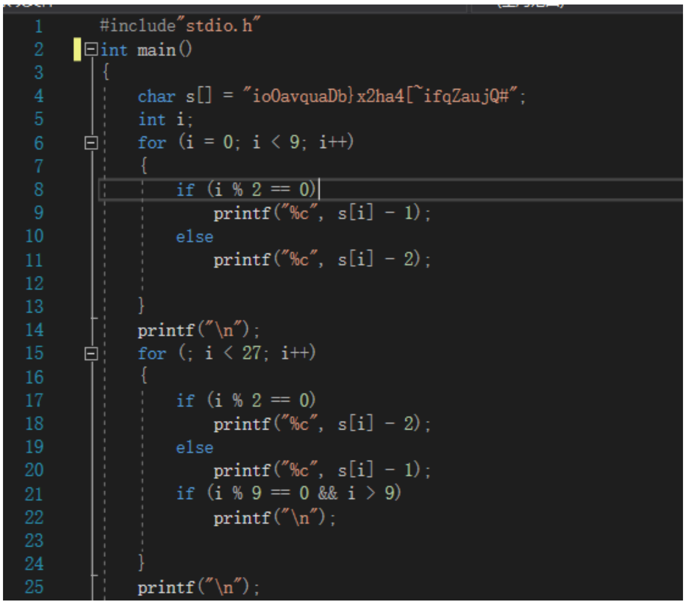
Pro 的 Python 教室(二)

找了一个在线将 .pyc 文件转换成.py 文件的工具



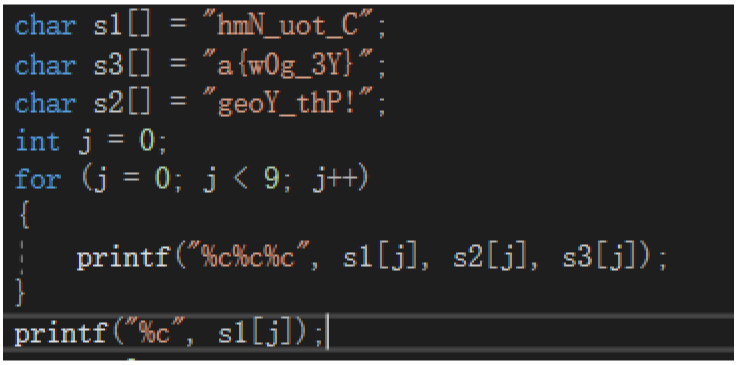
```
print "Welcome to Processor's Python Classroom Part 2!\n"
print "Now let's start the origin of Python!\n"
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
    else:
        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])

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

稍微用纸笔画一下应该就能看懂它的逻辑，附上拆解脚本

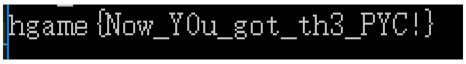


```
#include"stdio.h"
int main()
{
    char s[] = "ioOavquaDb}x2ha4[~ifqZaujQ#";
    int i;
    for (i = 0; i < 9; i++)
    {
        if (i % 2 == 0)
            printf("%c", s[i] - 1);
        else
            printf("%c", s[i] - 2);

    }
    printf("\n");
    for (; i < 27; i++)
    {
        if (i % 2 == 0)
            printf("%c", s[i] - 2);
        else
            printf("%c", s[i] - 1);
        if (i % 9 == 0 && i > 9)
            printf("\n");

    }
    printf("\n");
```

将得到的字符处重新排列下得到 flag



```
char s1[] = "hmN_uot_C";
char s3[] = "a{w0g_3Y}";
char s2[] = "geoY_thP!";
int j = 0;
for (j = 0; j < 9; j++)
{
    printf("%c%c%c", s1[j], s2[j], s3[j]);
}
printf("%c", s1[j]);
```



```
hgame{Now_Y0u_got_th3_PYC!}
```

hgame{Now_Y0u_got_th3_PYC!}