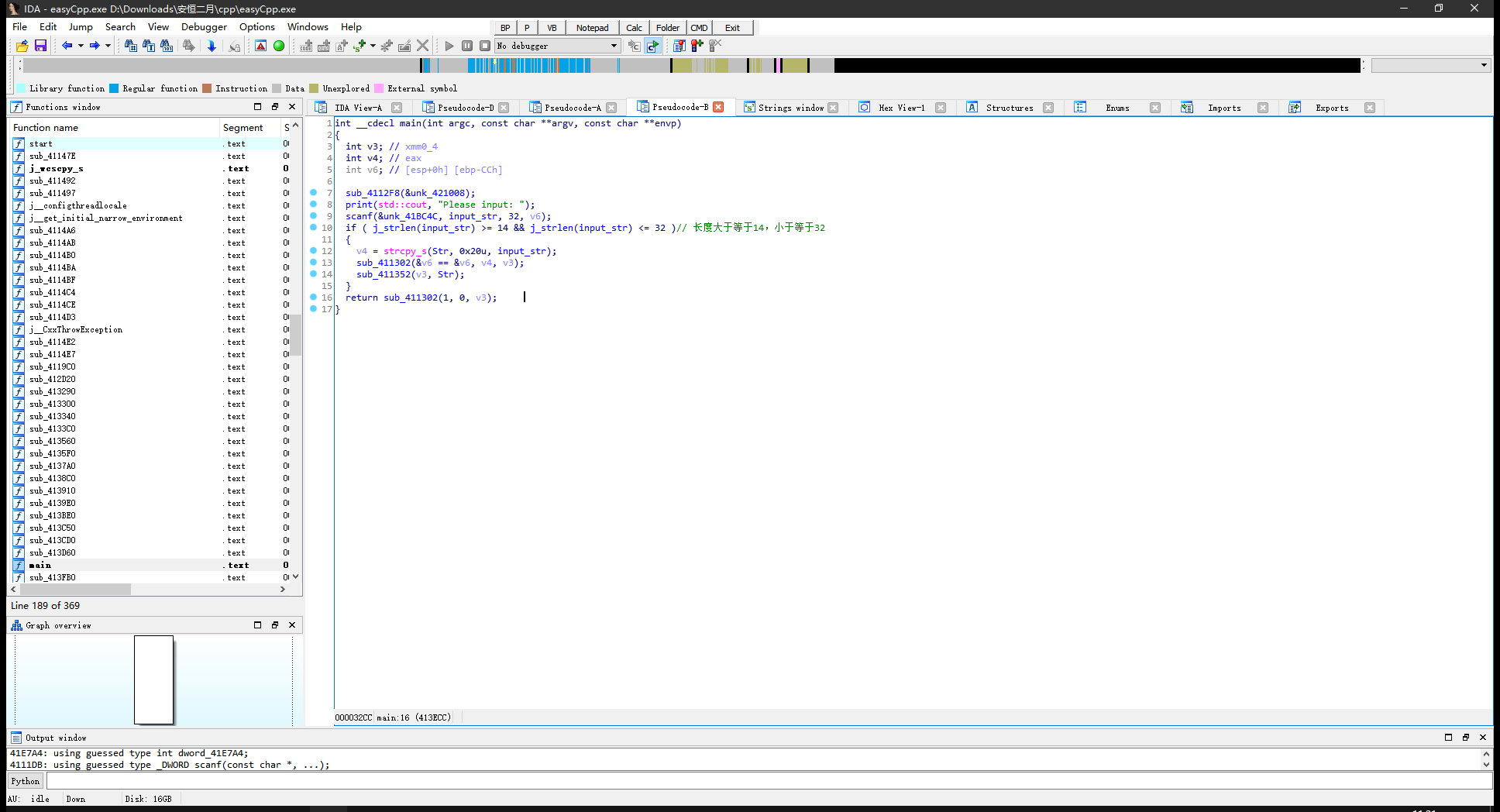
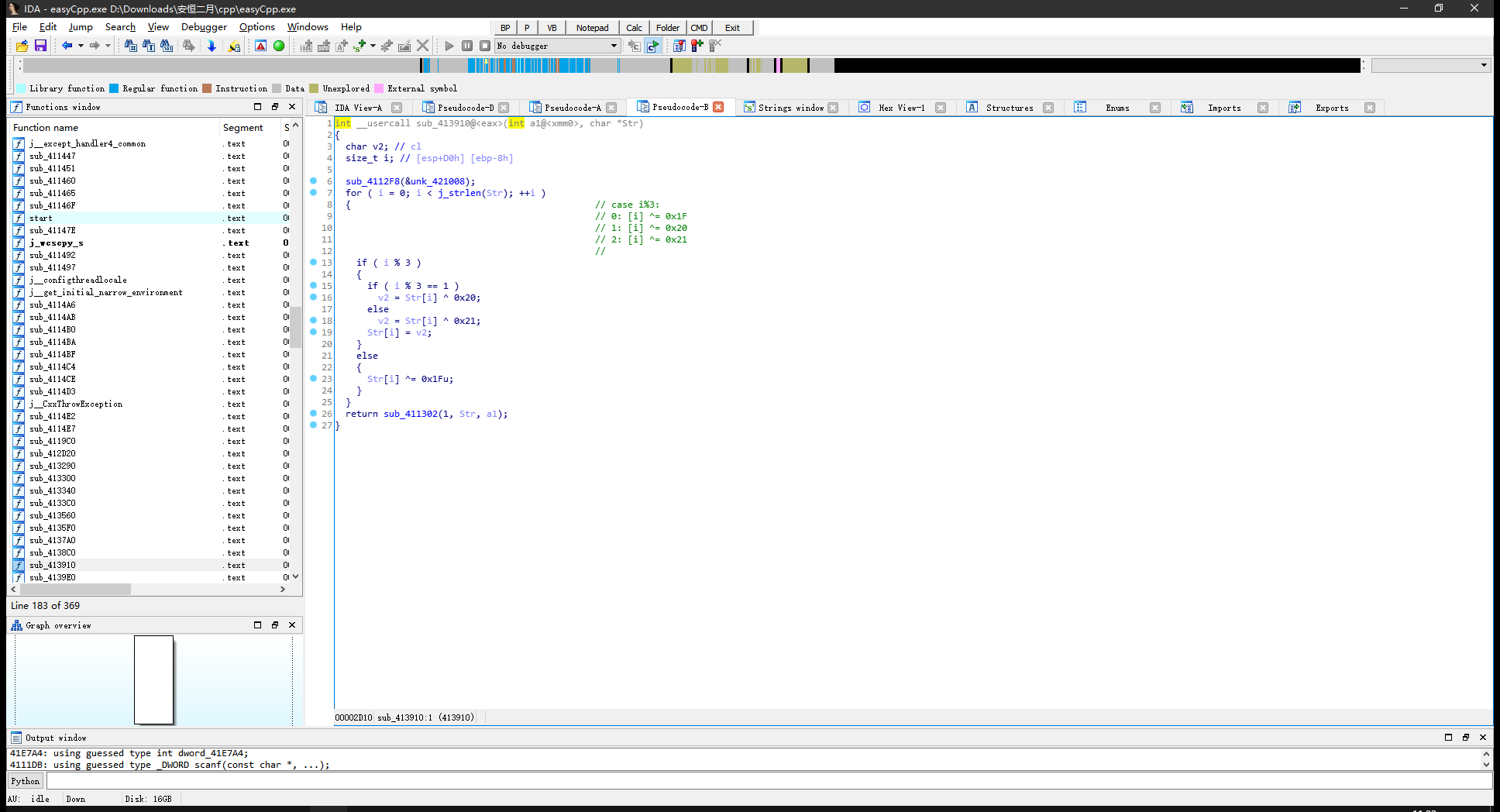
CPP

PEID检查一下，发现是debug版，没发现加密算法。

打开IDA，根据字符串”Please Input:”定位到main函数



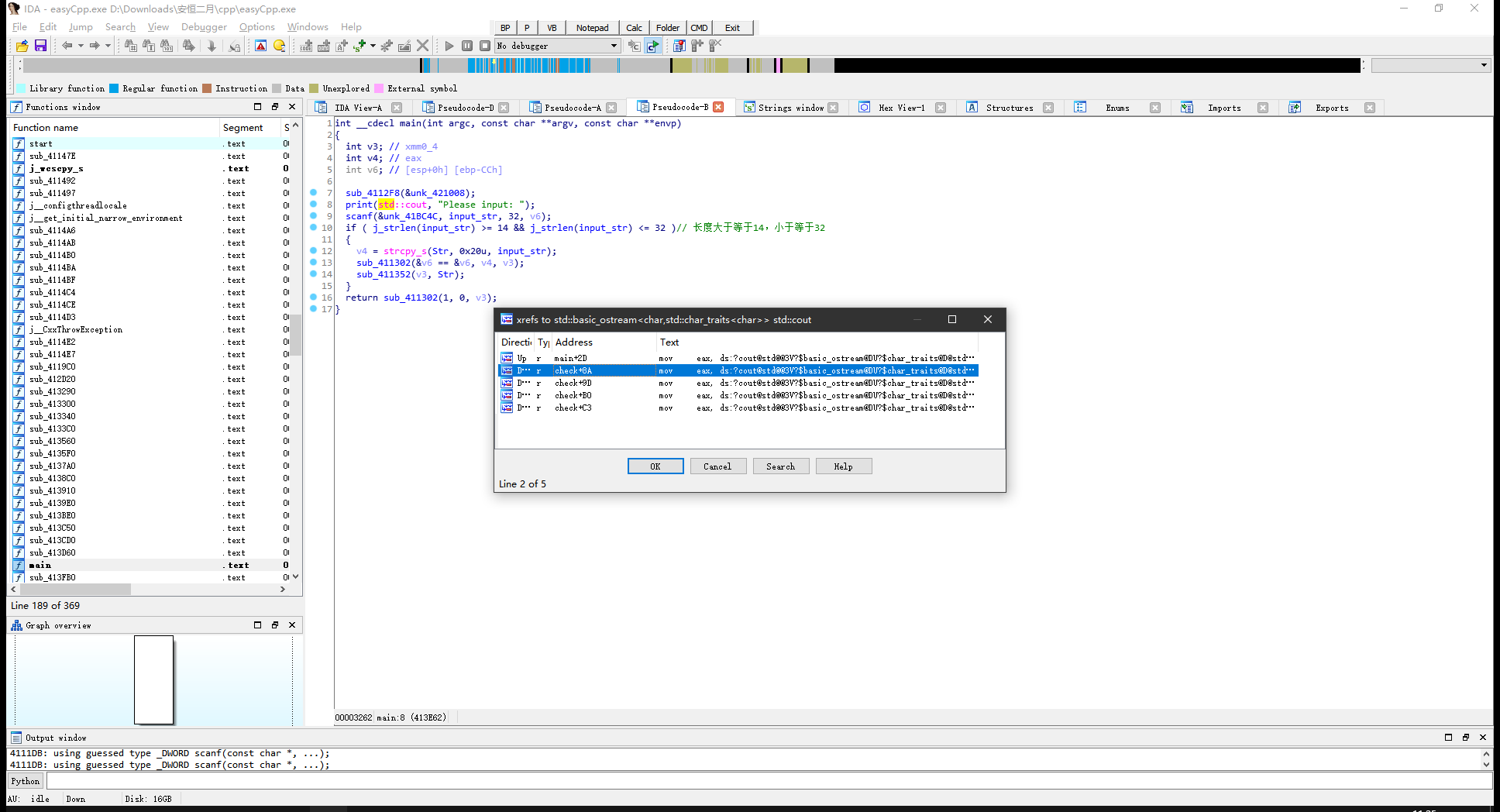
找到一些对输入字符串进行处理的地方



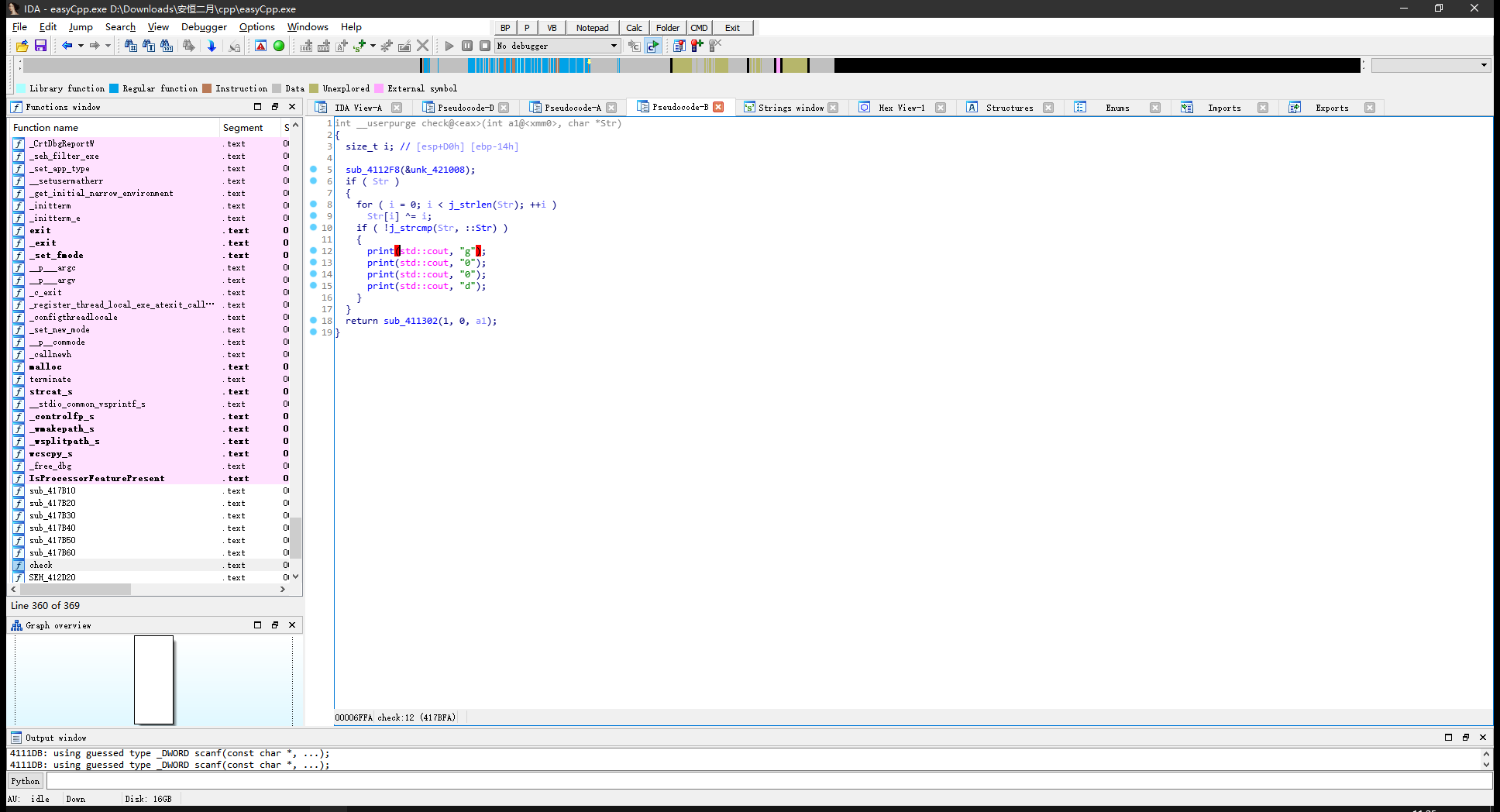
但是并没有发现检查的函数与字符串

想到可能是在main函数结束后，程序退出前进行检查。

于是对stdout标准输出流进行跟踪，

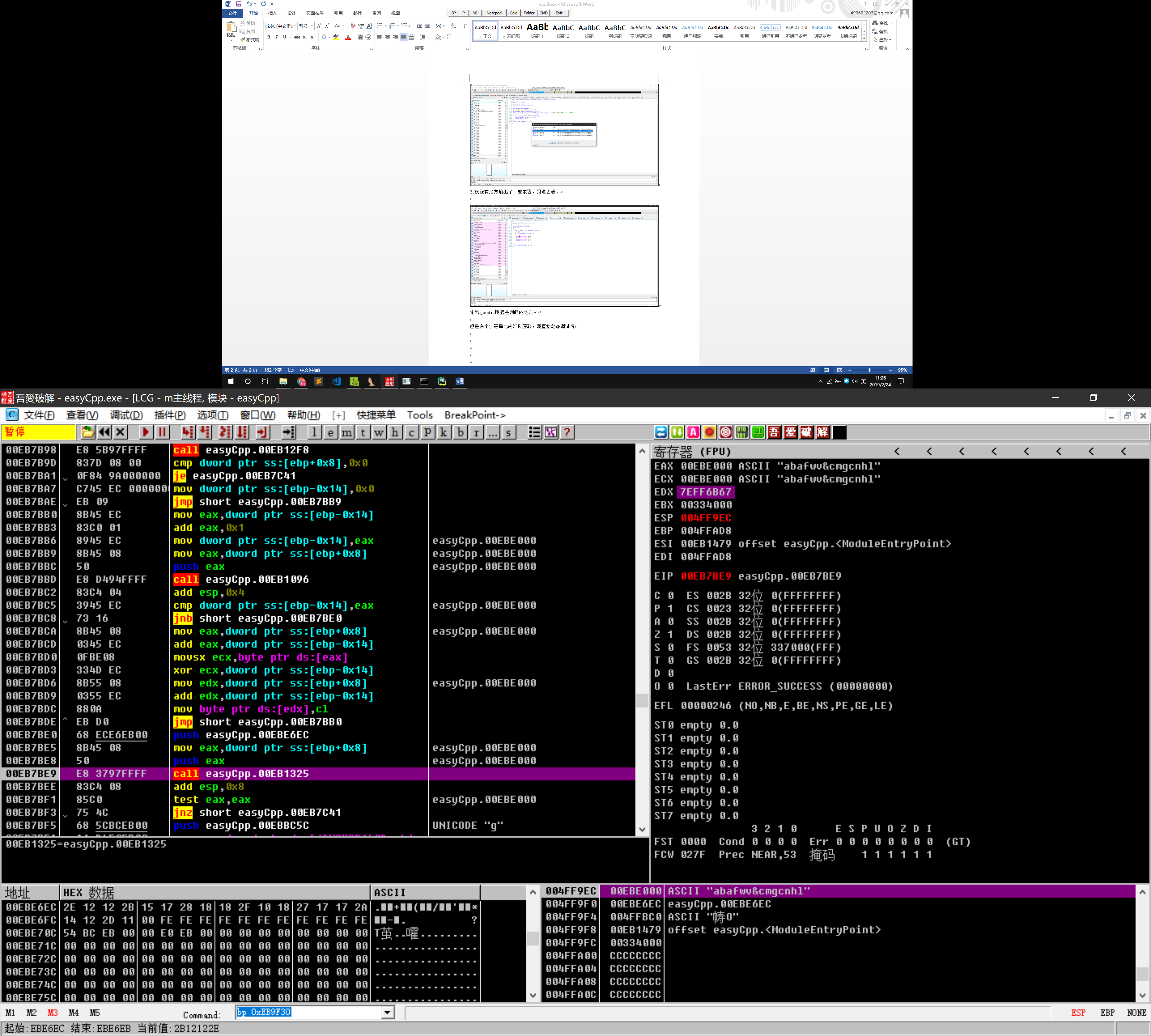


发现还有地方输出了一些东西，跟进去看，



输出good，明显是判断的地方。

但是有个字符串比较难以获取，我直接动态调试得



两个比较的字符串分别是，’accessxxxxxxxx’进行简单异或得的’ abafwv&cmgcnhl’，以及之前进行处理过的输入字符串。

写出解密脚本：

target\_str = "abafwv&cmgcnhl"  
  
print("len: %d" % len(target\_str))  
  
origin\_str = ""  
  
**for** i **in** range(len(target\_str)):  
  
 origin\_str += chr(ord(target\_str[i]) ^ (0x1F + i%3))  
  
print(origin\_str)

得字符串

~B@yWW9CLxCOwL

验证：

