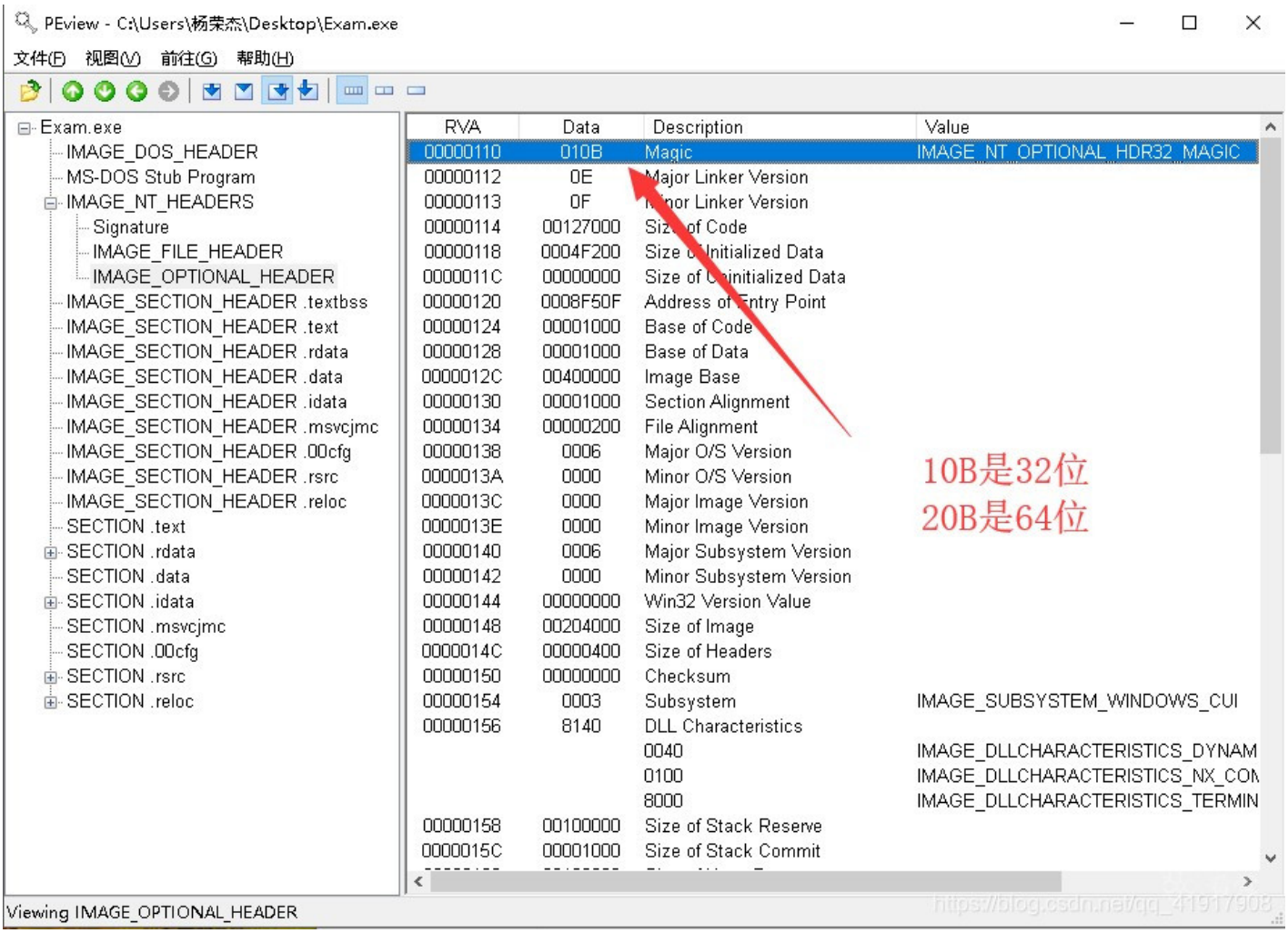
看雪CTF.TSRC 2018 团队赛 第二题 半加器 writeup

原创

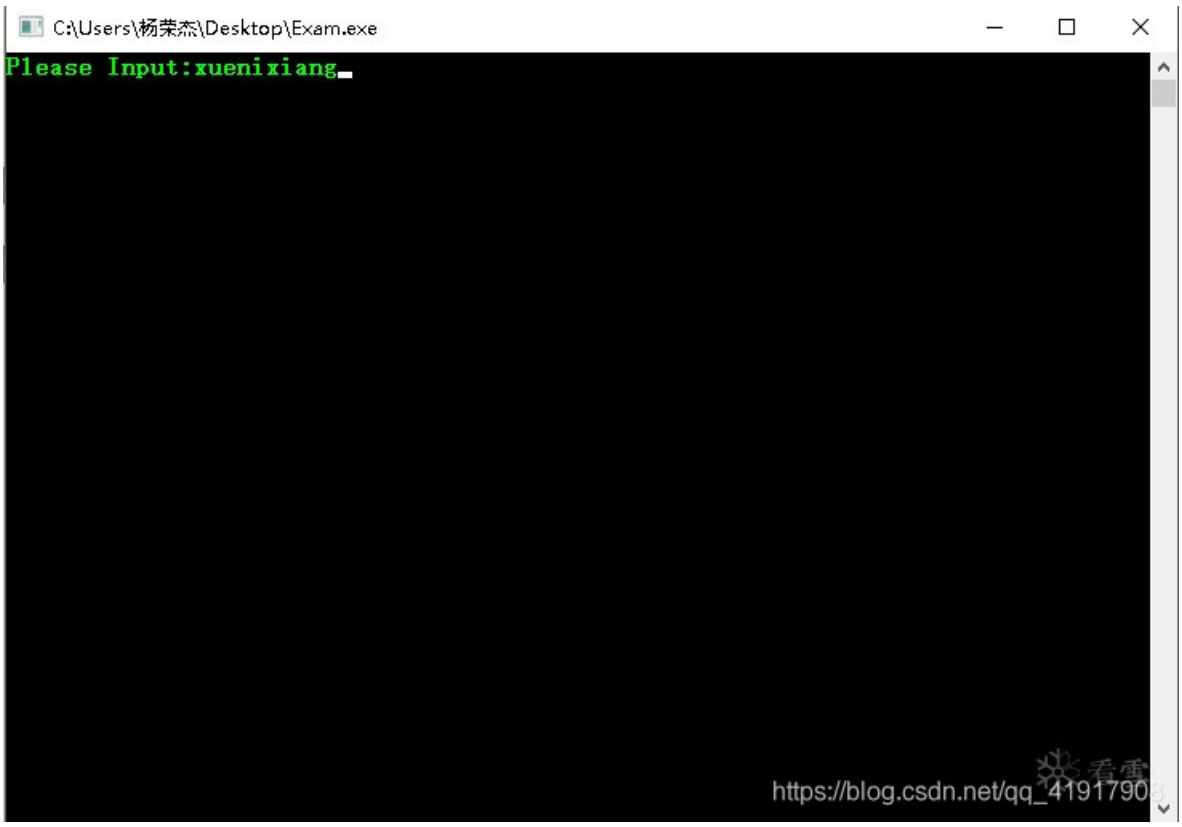
xuenixiang 于 2018-12-05 22:04:05 发布 319 收藏
分类专栏： CTF 文章标签： 半加器 writeup 看雪CTF

首先查壳，发现没有壳

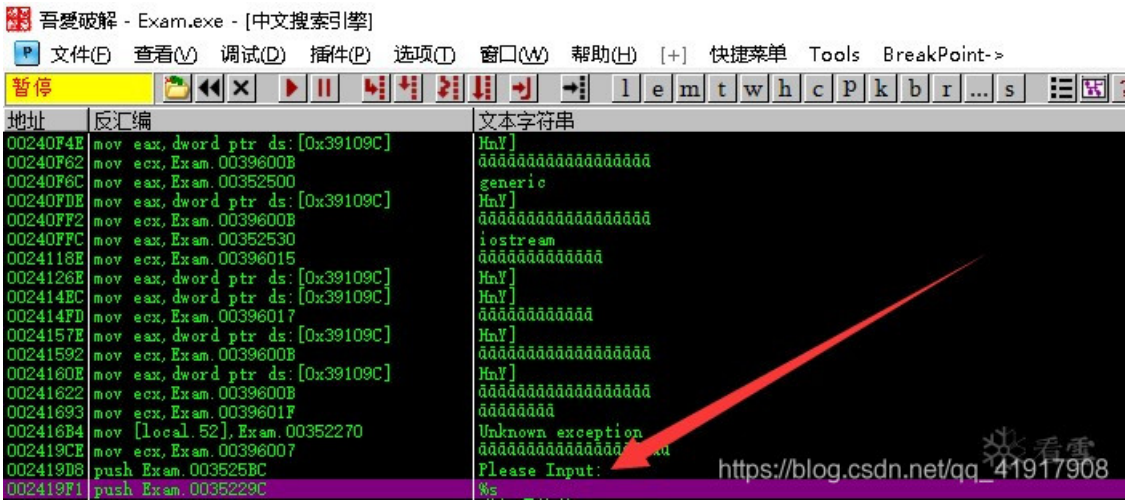
然后根据PE看一下是不是32位程序，这个是32位程序，所以可以用OD来分析（希望OD能早日开发出支持64位的版本）



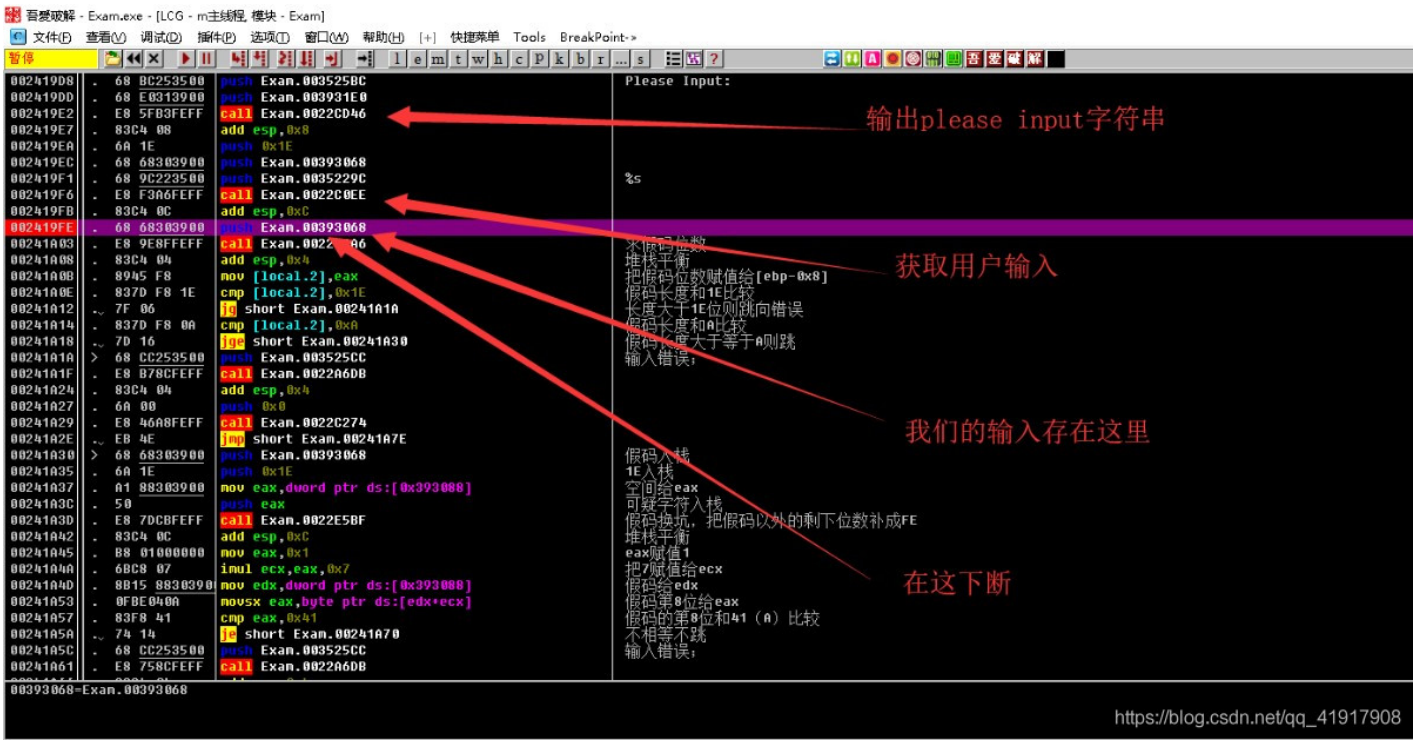
根据程序特征我们可以根据 Peease Input 这个字符串定位到关键点



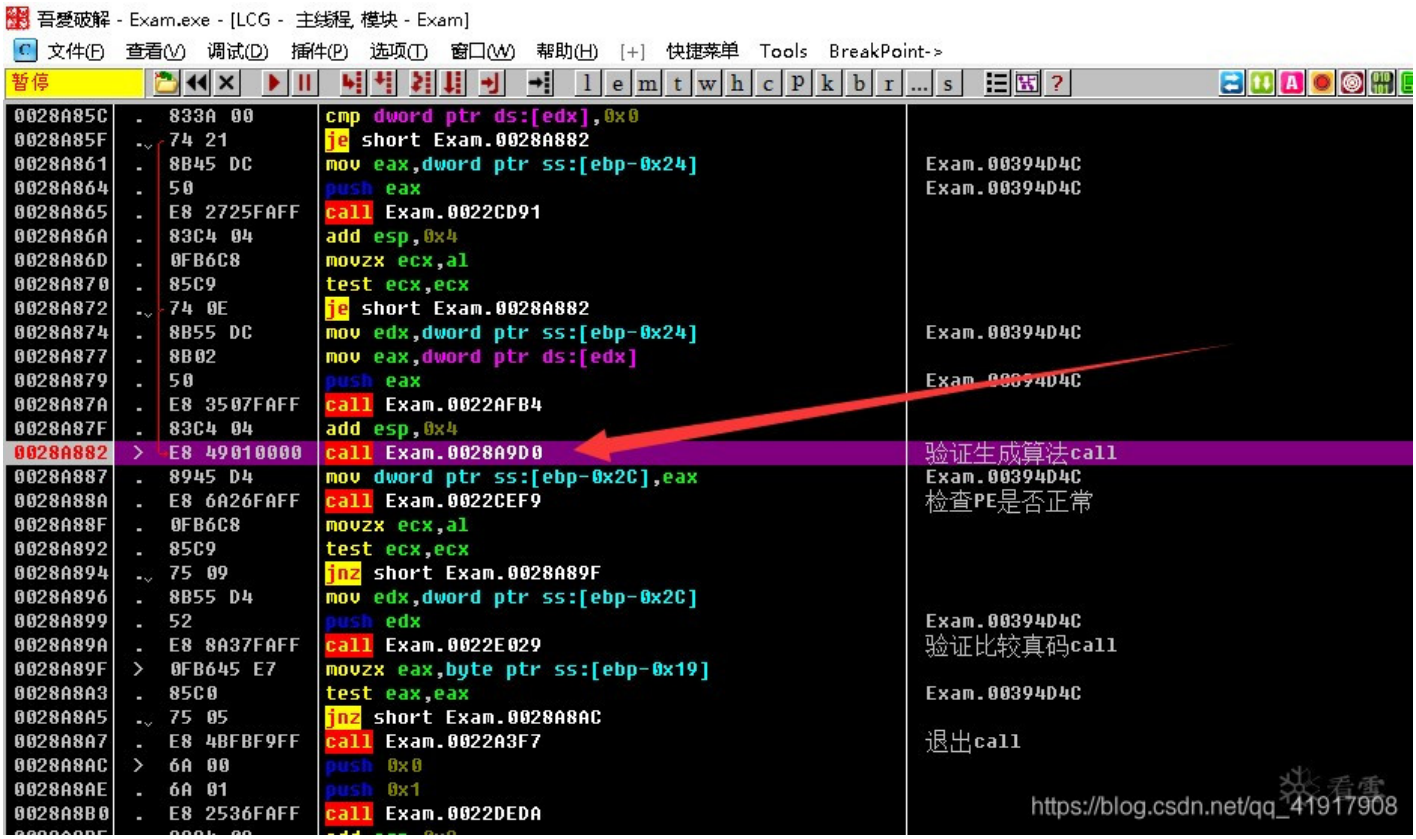
直接载入OD，查找对应字符串



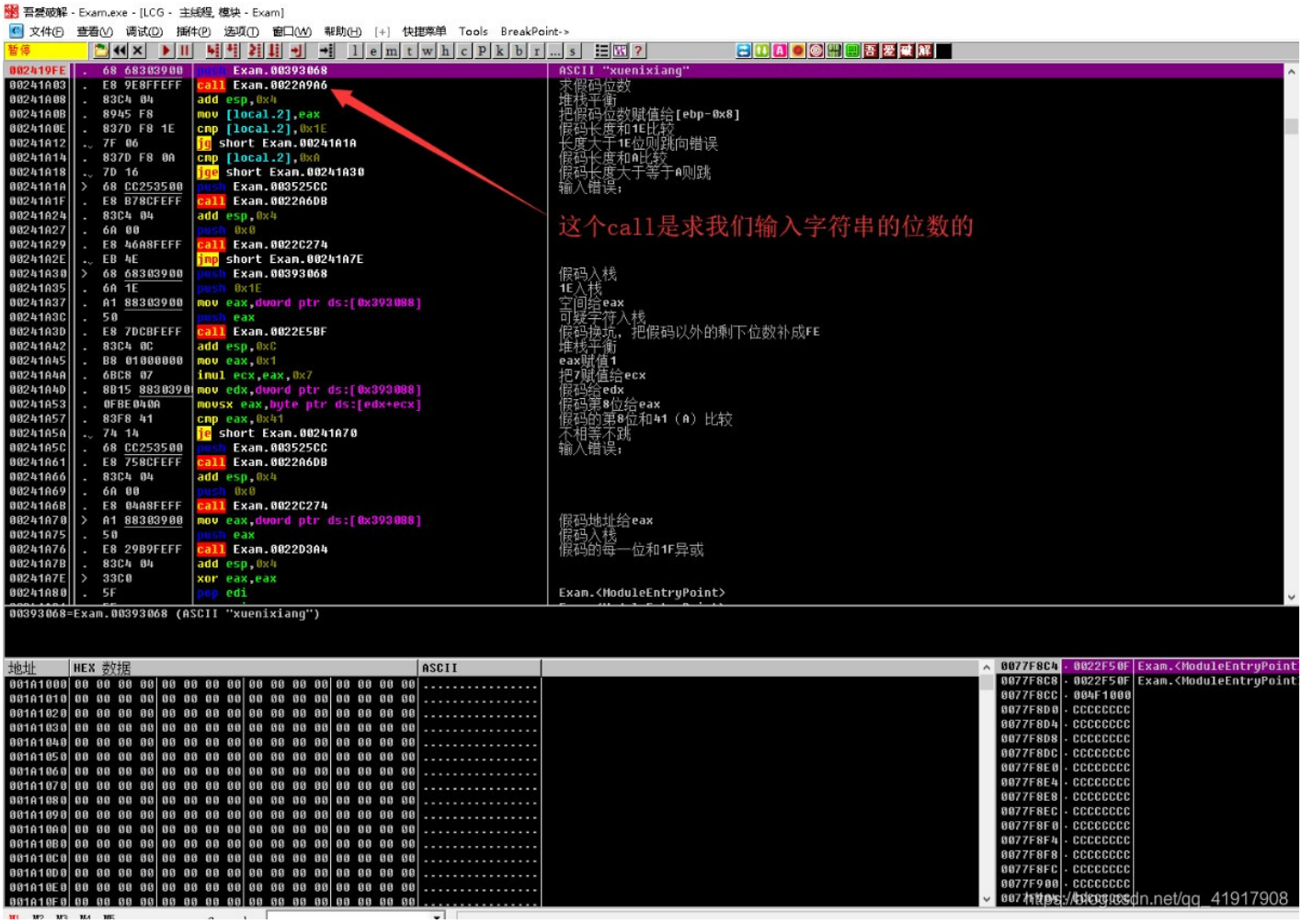
002419FE |. 68 68303900 push Exam.00393068 在此下断



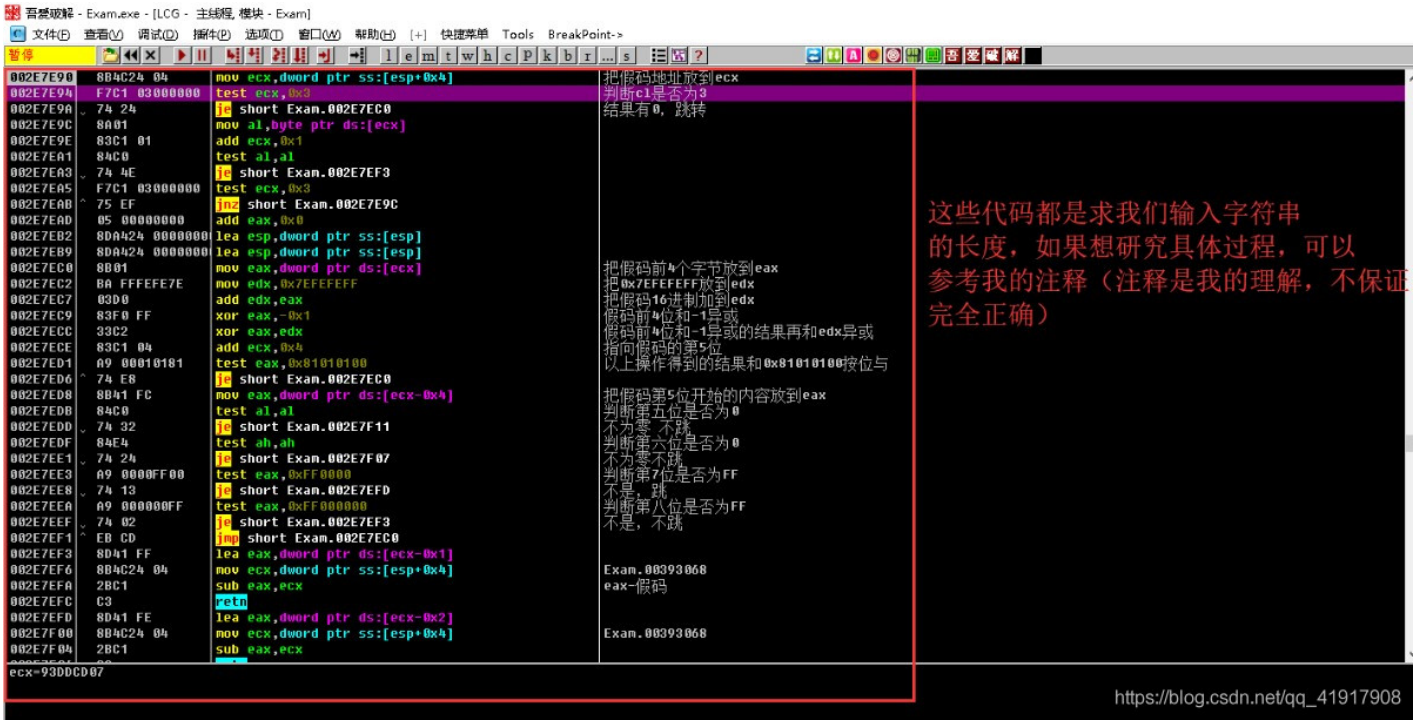
通过回溯可以看到我们目前所在的call（弄清楚自己现在所处位置）



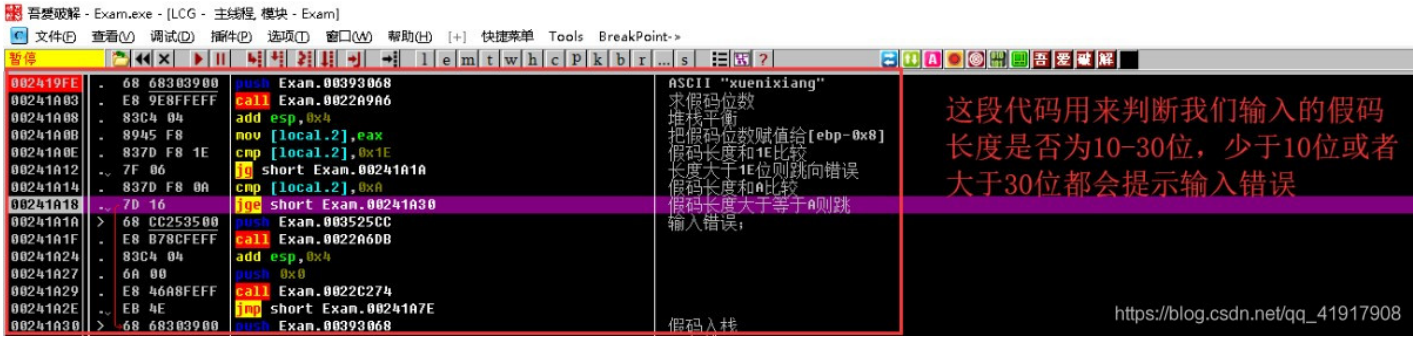
运行程序，输入假码xuenixiang ， 会断在下图位置



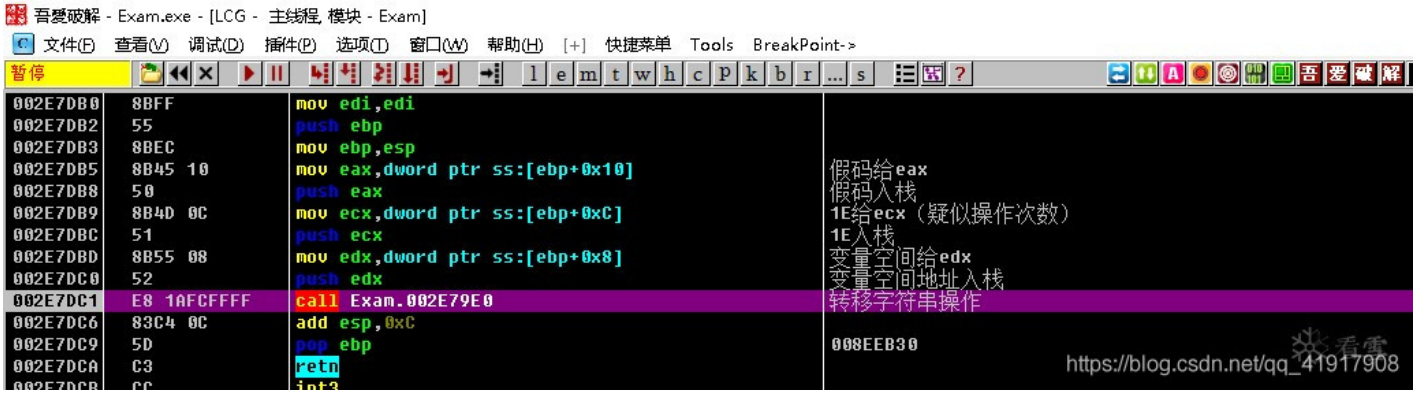
我们进00241A03这个call来看看



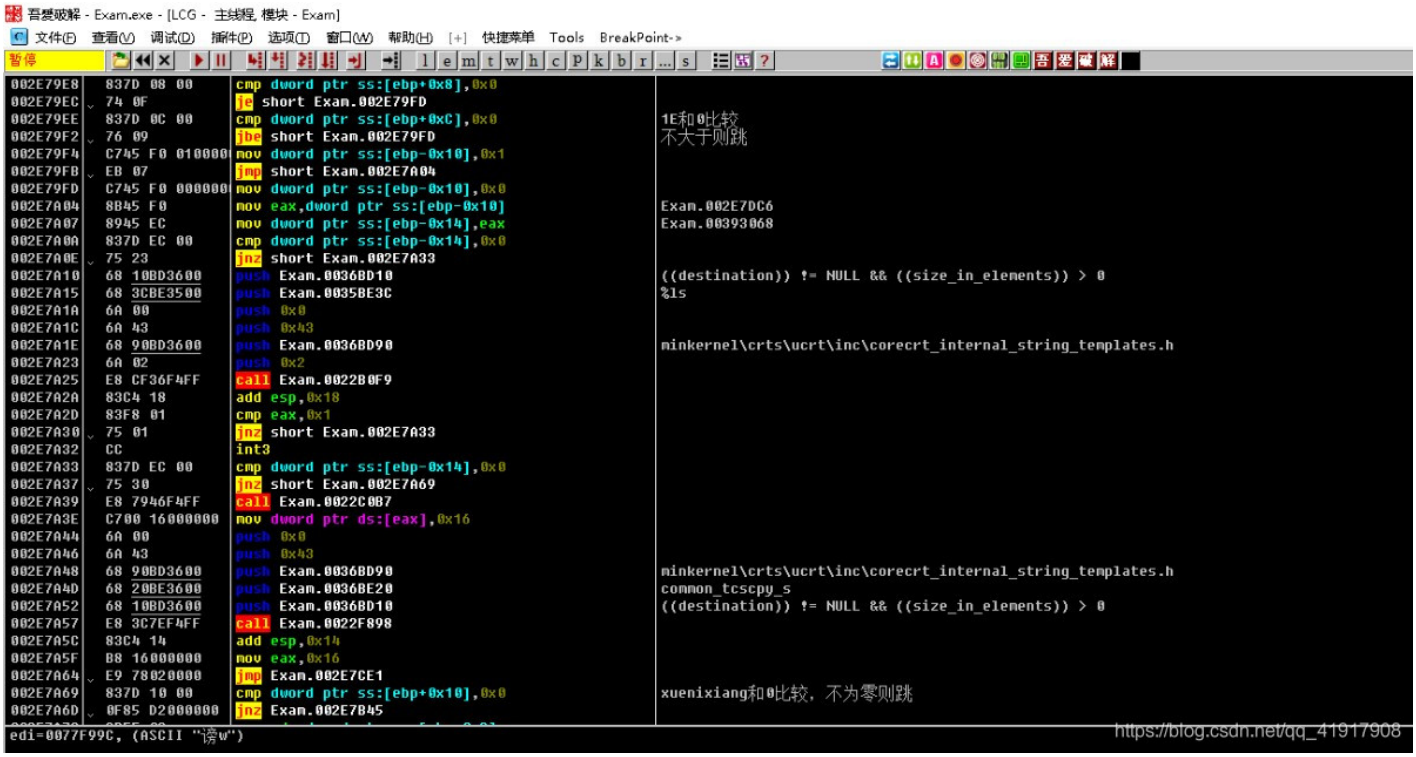
判断我们输入的字符串长度是否在10-30位之间



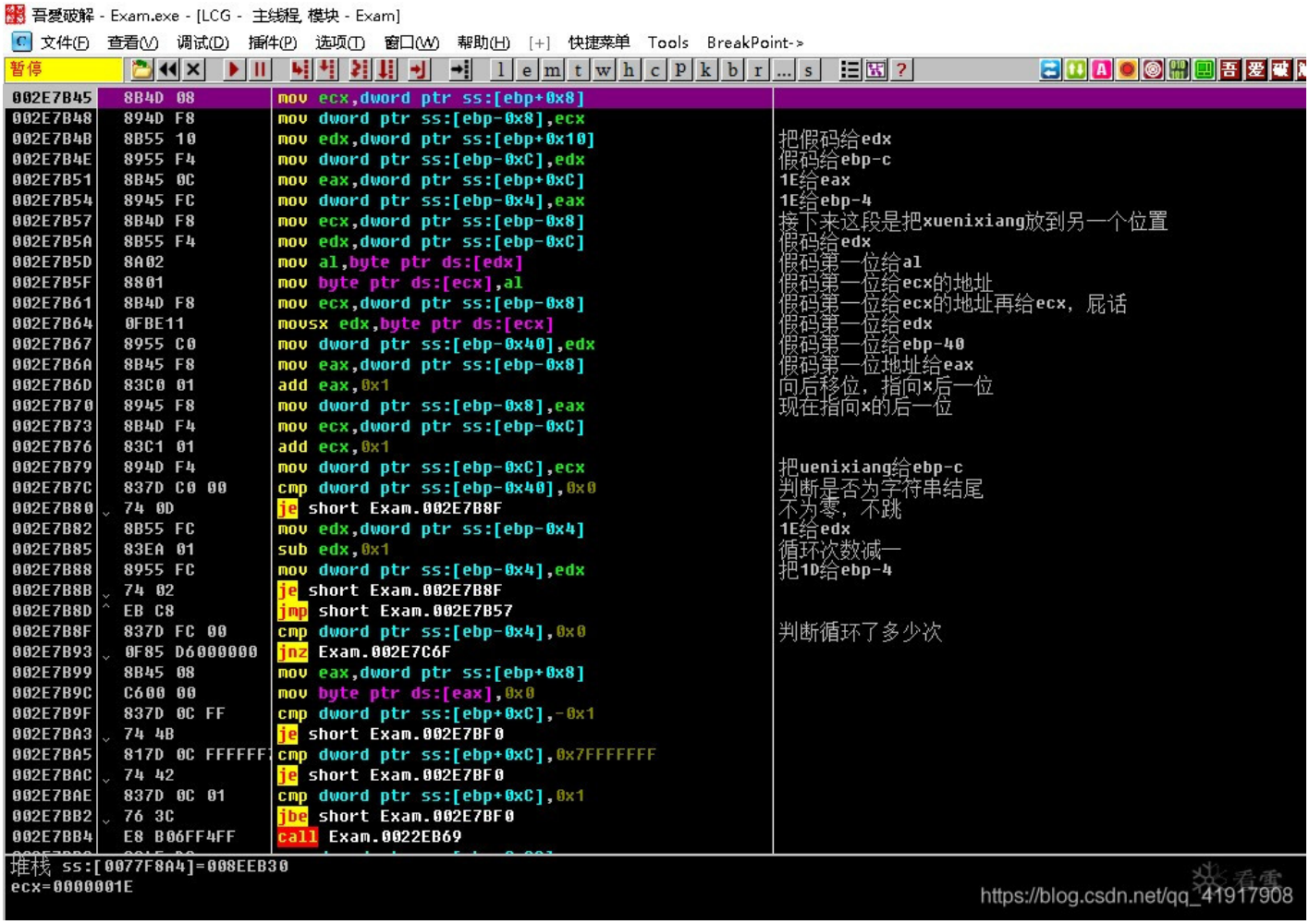
我们进入这个call 0022E5BF 看看



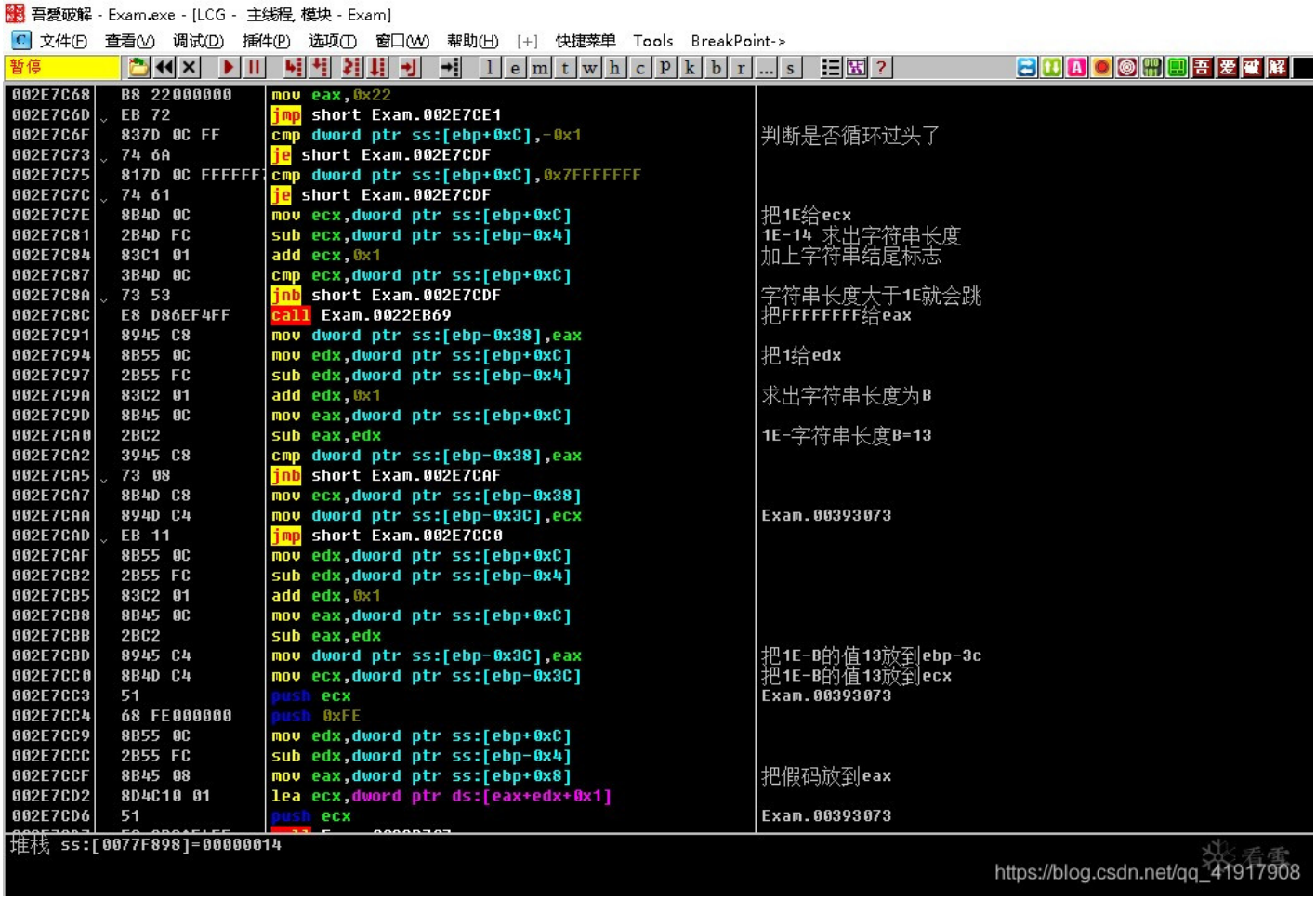
继续进2E7DC1这个call



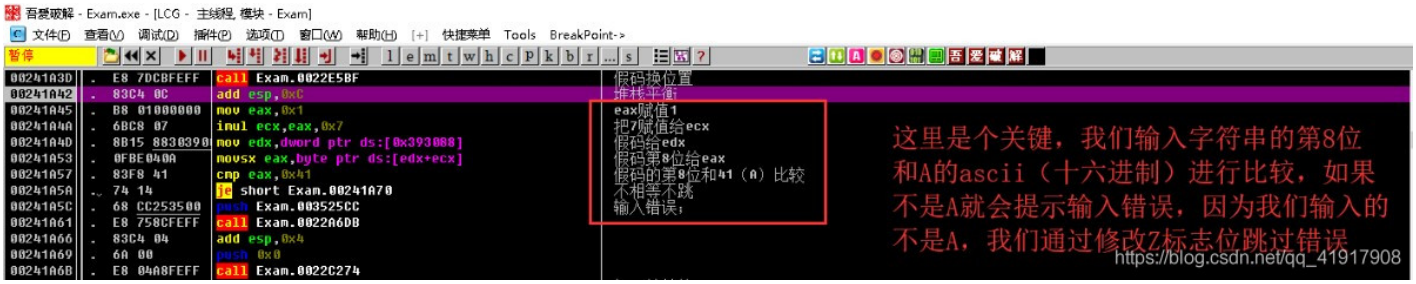
往下单步跟，到达这里可以看到转移假码的过程



这段是在验证假码的长度和假码最高限制1E（十进制的30）的关系

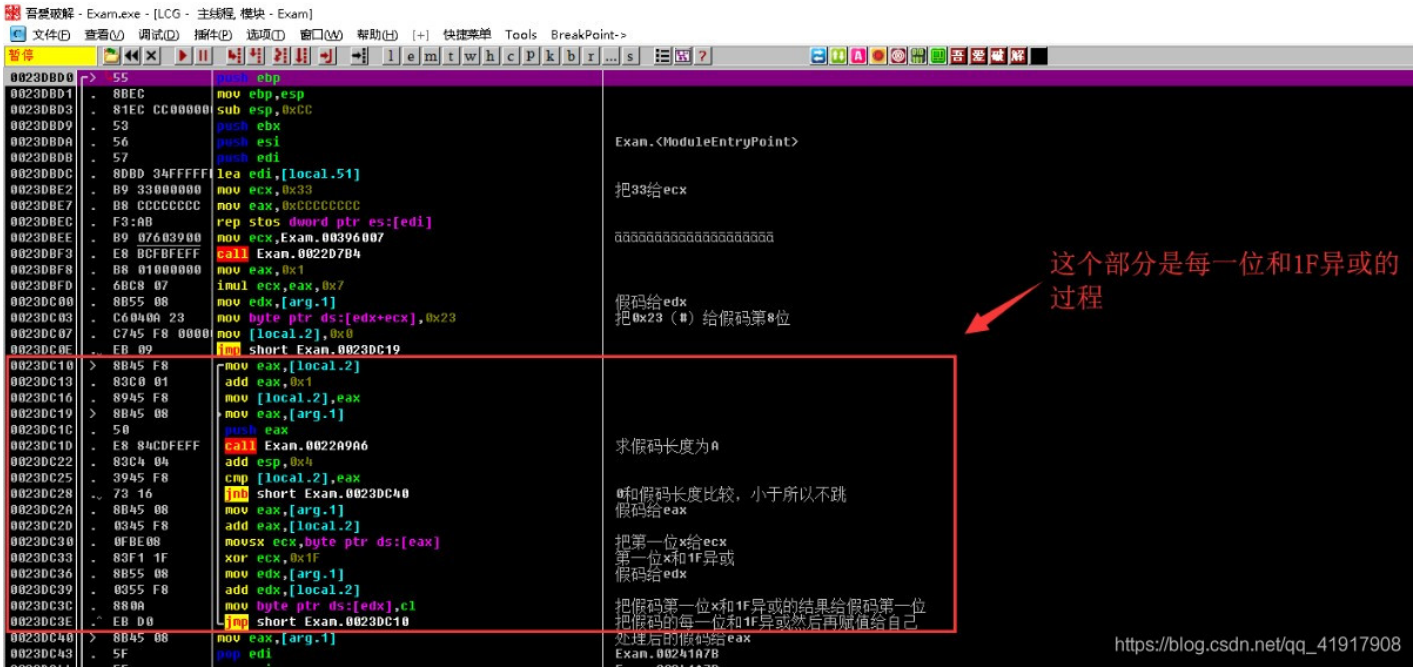


我们出这2个call，看到这个地方，是可以确定flag第8位是A

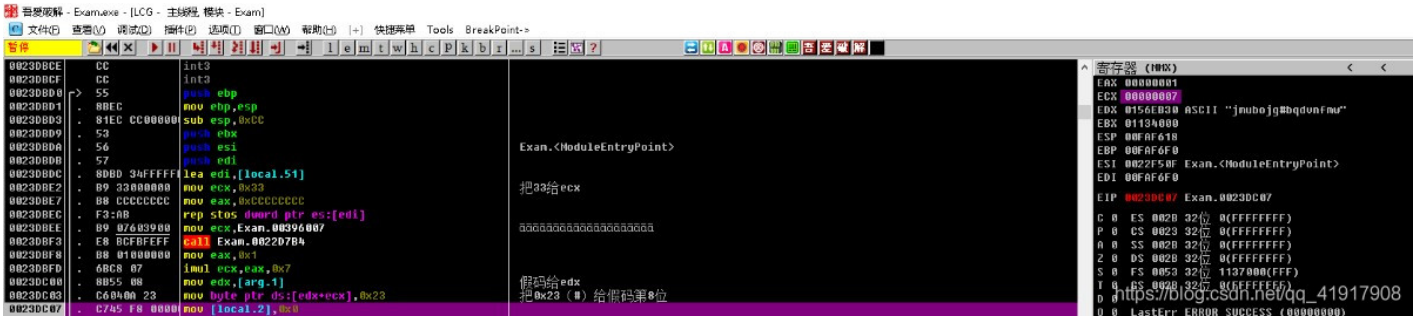


00241A76处的这个call是整个程序的算法部分，它把我们输入假码的每一位都和1F异或，然后把我们输入的原有字符串替换

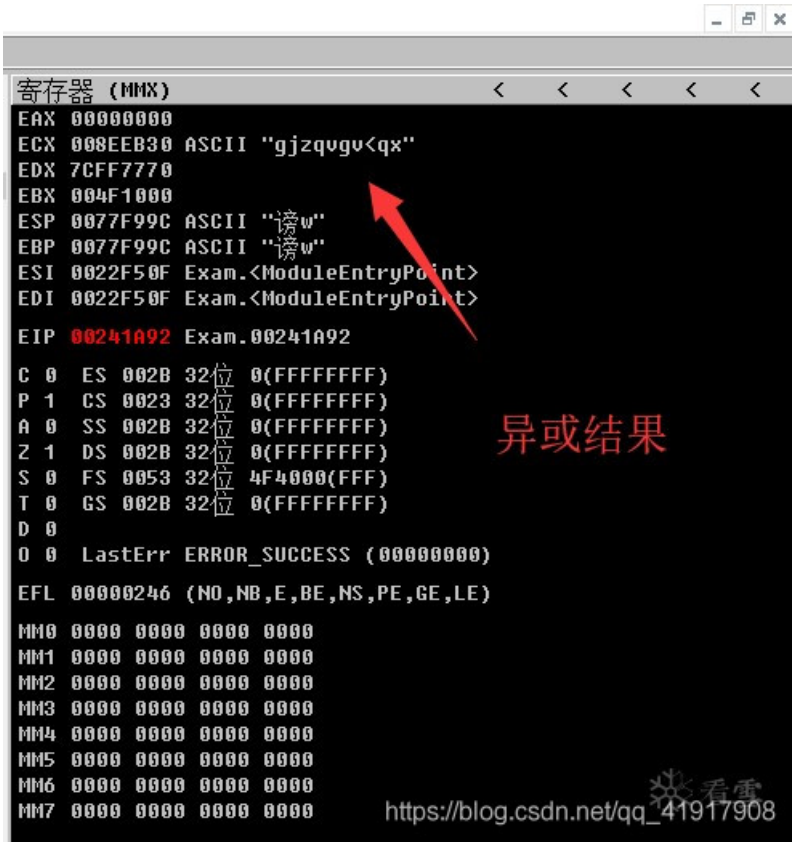
进CALL看看，可以看到异或的具体算法



注意这个地方，程序会将第八位无条件的换成#号，也就是说我们第八位不管是不是41（A），都会先被替换为#再参与下面的异或运算

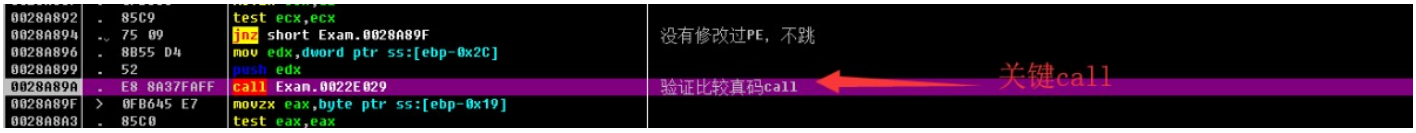


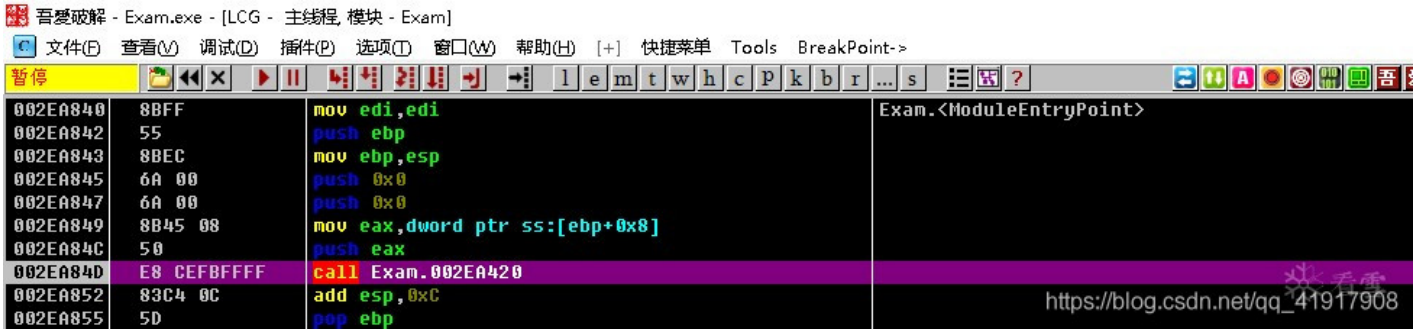
异或的结果保存在ecx



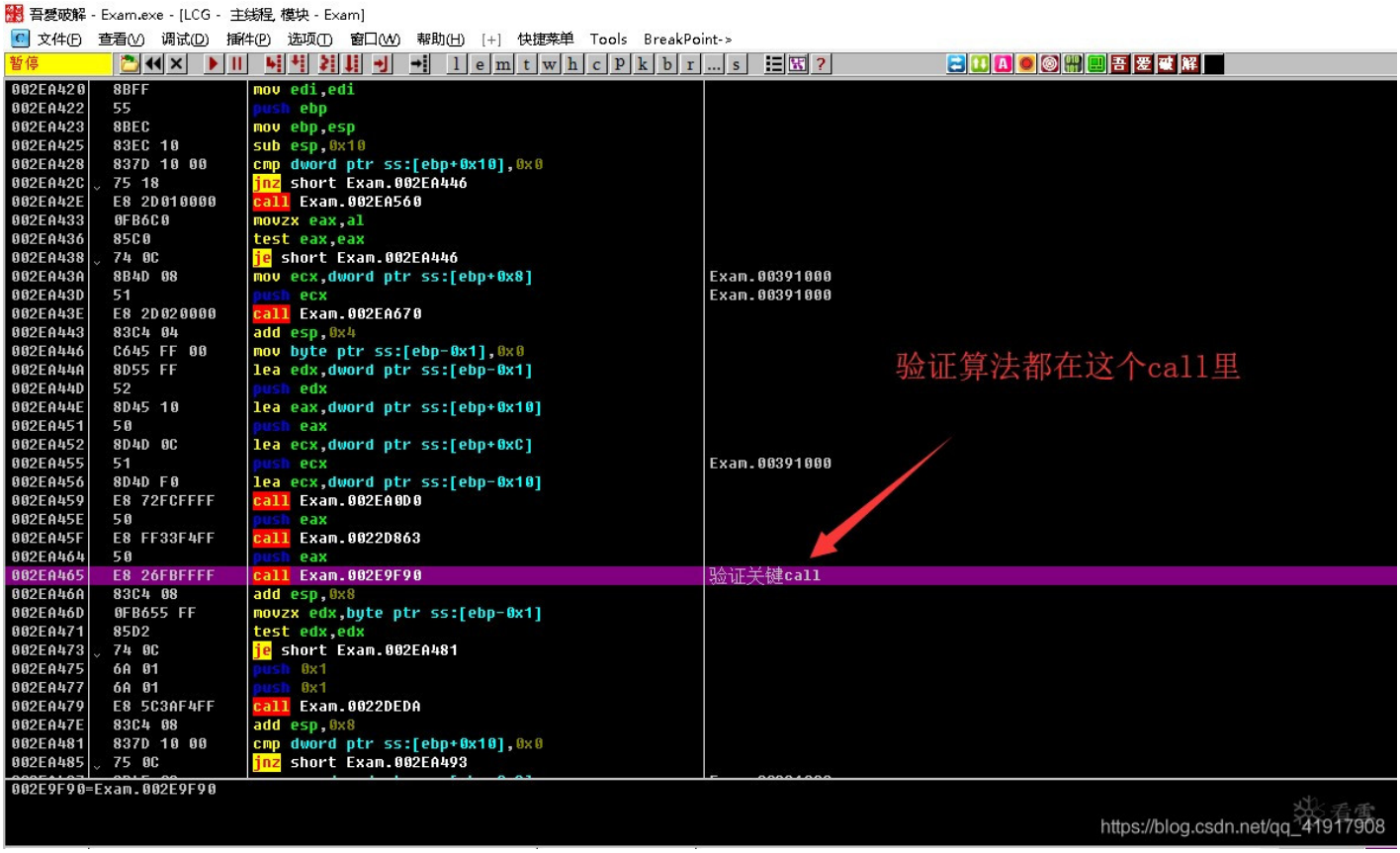
0028A88A 这个call是检查PE是否正常，是否被修改过（会检测PE签名，NT头，等重要的地方）

下面进28A89A这个关键call

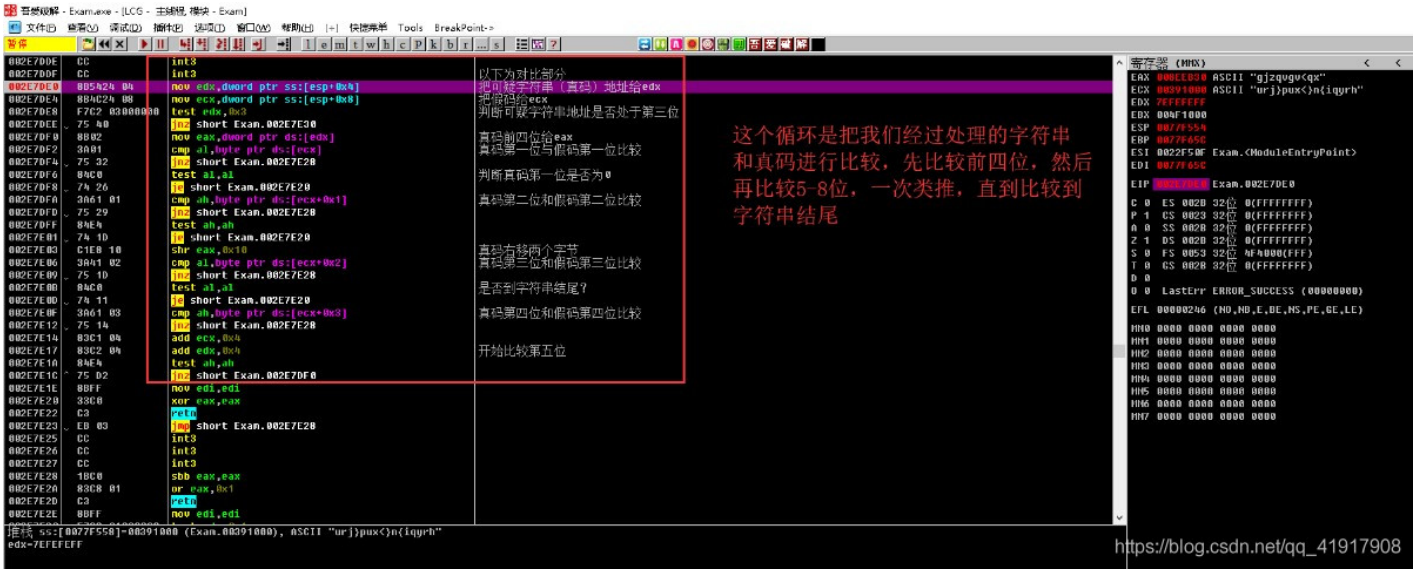




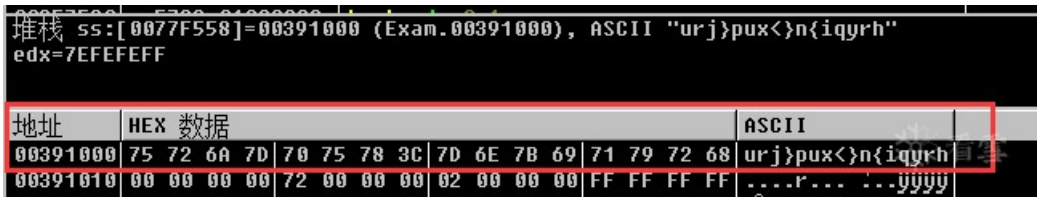
继续进call，往下跟会找到2EA465位置的这个call



进去后就是我们程序最关键的比较部分了



这里我们看到了用来比较的真码



00391000 75 72 6A 7D 70 75 78 3C 7D 6E 7B 69 71 79 72 68 urj}pux<}n{iqyrh

xor 1E

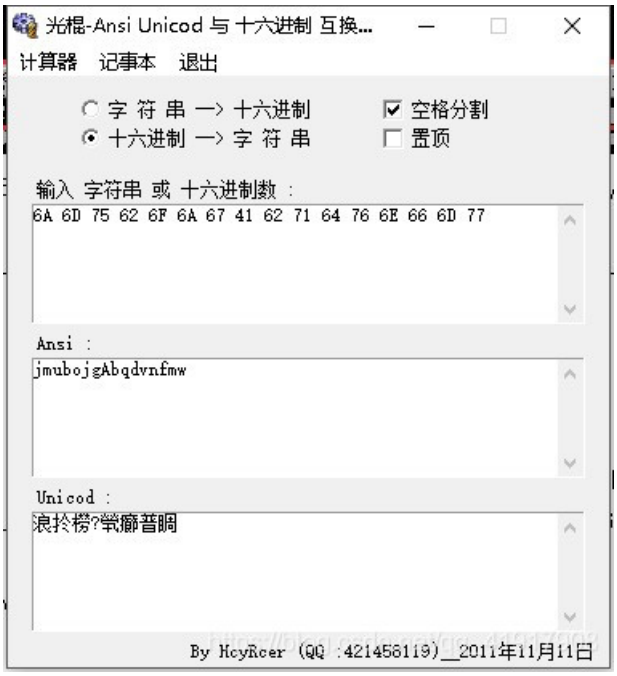
6A 6D 75 62 6F 6A 67 23 62 71 64 76 6E 66 6D 77

41

我们用计算器把 75 72 6A 7D 70 75 78 3C 7D 6E 7B 69 71 79 72 68 每一位和1E进行异或运算， 得到6A 6D 75 62 6F 6A 67 23 62 71 64 76 6E 66 6D 77

又因为我前面提到flag的第8位是41(A)，所以 flag应该是6A 6D 75 62 6F 6A 67 41 62 71 64 76 6E 66 6D 77

我们将 6A 6D 75 62 6F 6A 67 41 62 71 64 76 6E 66 6D 77 转换为ascii 得到jmubojgAbqdvnfmw



输入jmubojgAbqdvnfmw 软件提示了OK

此 writeup若有不正确的地方，欢迎大佬指正~~

2018.12.3

www.xuenixiang.com