serial-150 攻防世界

原创

北风~ 于 2020-04-08 22:00:04 发布 880 收藏

分类专栏： 逆向与保护

本文链接：https://blog.csdn.net/weixin_45055269/article/details/105397707

逆向与保护 专栏收录该内容

65 篇文章 4 订阅

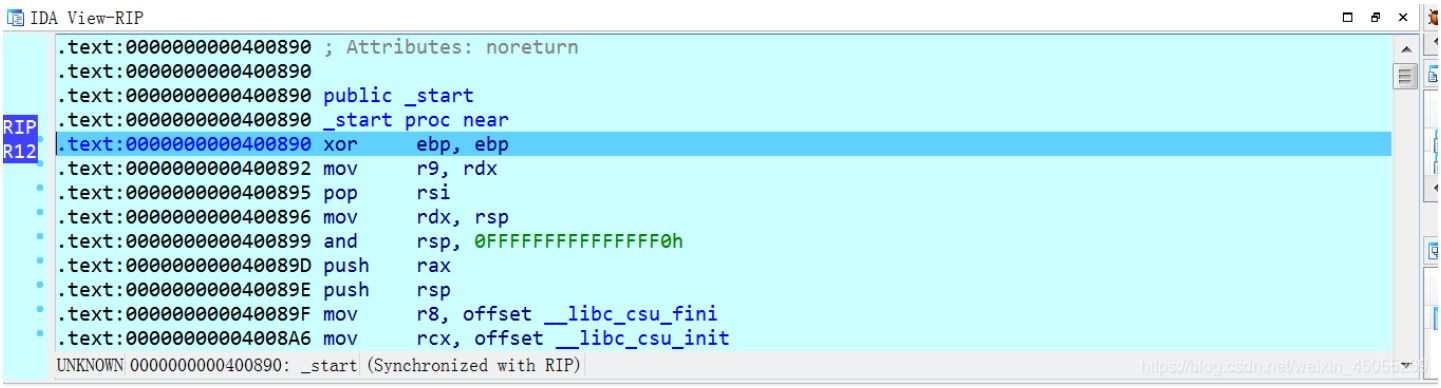
订阅专栏

ida64 直接反编译，你会发现没有函数，而且代码段里是数据，这一点决定让我们使用动态调试，看程序跑起来之后，代码段里的数据会变成什么代码。

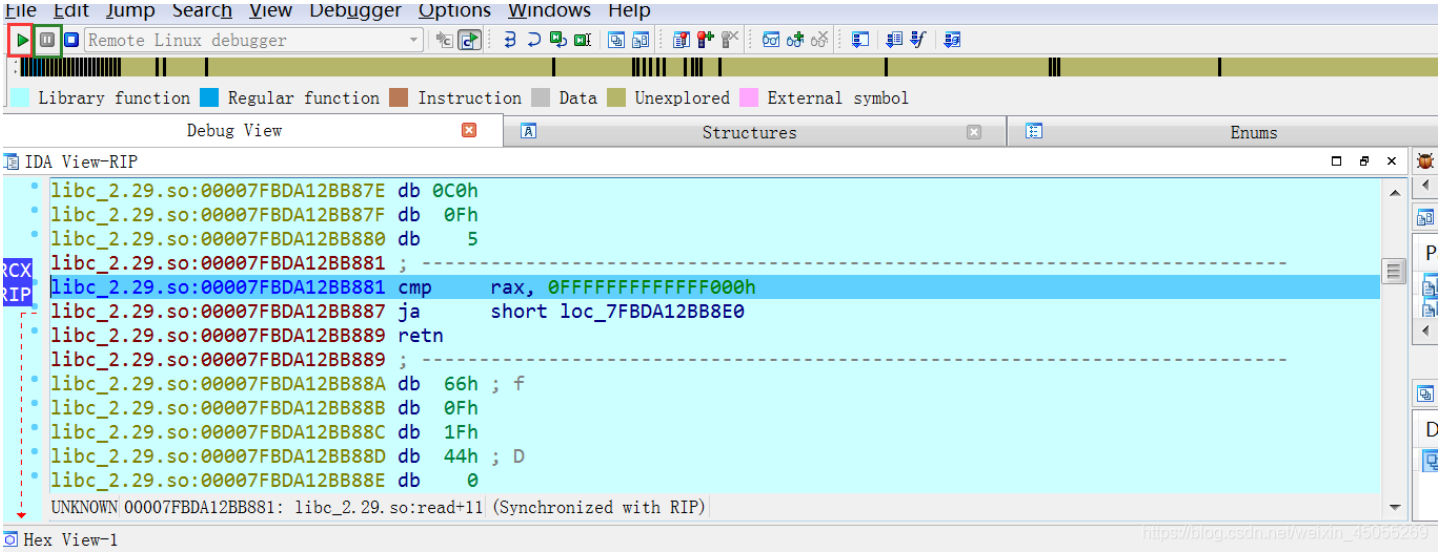
IDA远程动态调试配置：无坑版

这里分析如何找到输入字符后对字符检测的部分

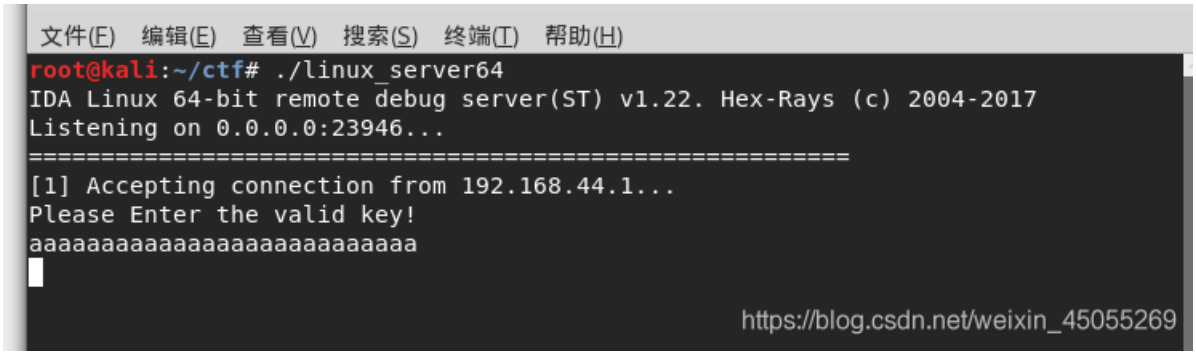
1.刚打开IDA时的样子



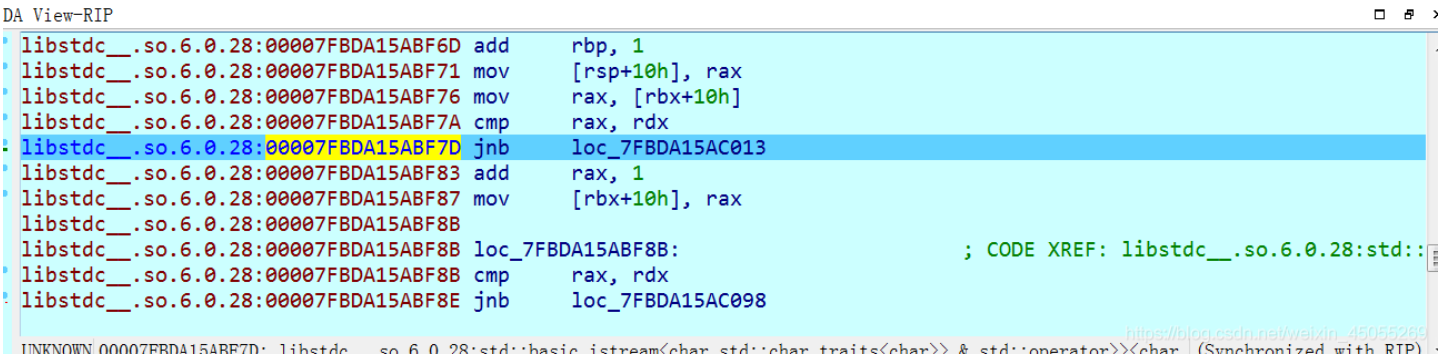
2.先点击红框，看程序停下来，再点击绿框内容



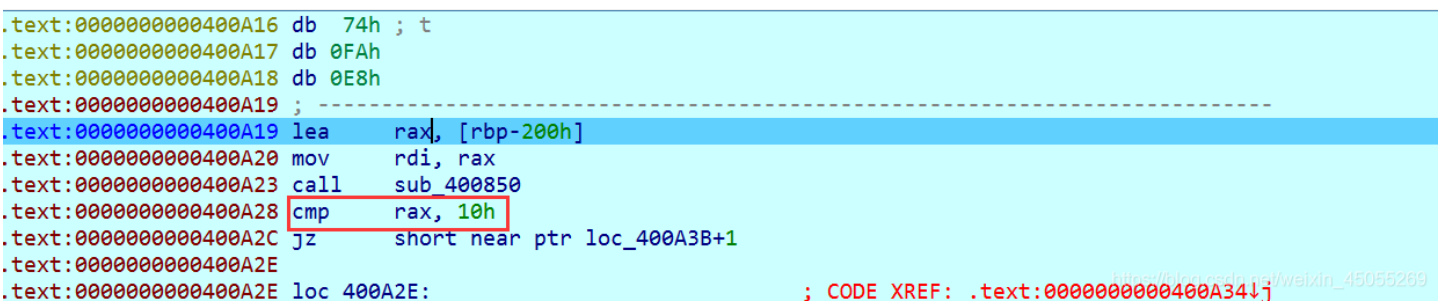
程序停下来，发现是让你输入字符先随便输入一串a



3.然后会发现进入7F开头的地址里，一直按F8，直到出现4开头的地址

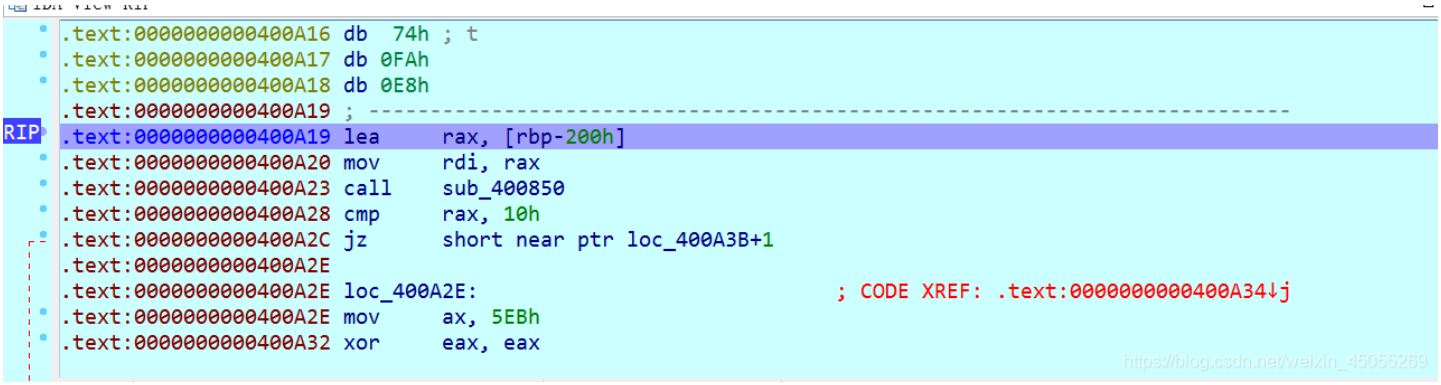


4.发现关键比较，字符长度16



5.设置断点，不断满足条件写出flag

首位字符规定好，再规定末位字符加首位字符的和，这样两两一组逐渐往里缩，不断修改尝试



EZ9dmq4c8g9G7bAV