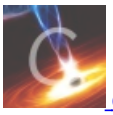
攻防世界re1

原创

hello@kitty 于 2020-09-26 15:16:14 发布 118 收藏

分类专栏： ctf逆向

本文链接：https://blog.csdn.net/keep_reading/article/details/108482073



文章目录

攻防世界re1

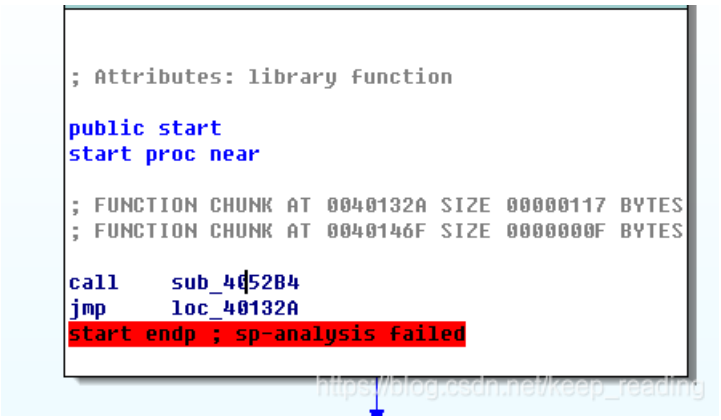
(dword：由 4 字节长(32 位整数)的数字表示的数据)

查壳脱壳

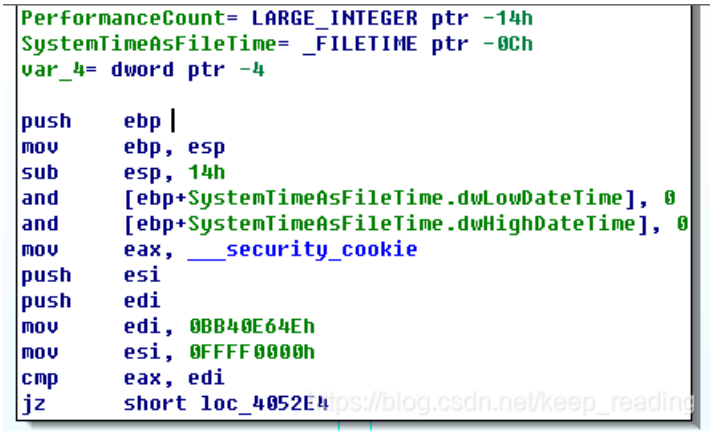
先找main函数翻译成伪代码

打开IDA，一般自动定位到start函数

在start，双击定位，找到了一个

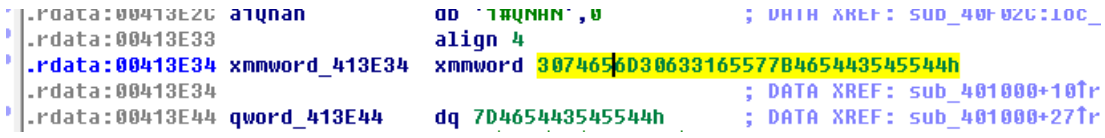


……推测这里有main函数线索的可能性比较大，再双击以下试试



调到了汇编语言的部分，（不太会，把这几行都点开看了看F5，发现mov后边那个比较像……找到main函数）双击ctrlx 再F5

分析伪代码找到这个字符串（还有下边那个dq）



16进制大端小端存储