IDA操作手册笔记1

原创

一条不更新的懒狗 于 2021-10-31 19:13:39 发布 175 收藏

文章标签： IDA

本文链接：https://blog.csdn.net/lw_zhaoritian/article/details/121068349

1.汇编转C语言后如何还原函数?

附件

以 看雪课程的libmyjni的函数 JNIOnLoad 函数为例，使用32位的IDA7.0打开so

1.点击 Exports(名词解析:导出函数列表)

2.双击击对应的JNI_OnLoad函数进入IDA View-A视角

3.直接按下F5快捷键转换为C语言伪代码 这时候发现没有正确对应 需要修复参数类型

4.修复int a1 鼠标放在a1上 点击 快捷键 Y 输入 JNIEnv* 确定

5.修复 g_env + 860 g_env + 24 这两个其实也是函数 只是无法正确识别为JNIEnv* 同理点击 快捷键Y 让函数名显示出来

6.修复函数没有参数显示的问题 第五步的函数FindClass 和 RegisterNatives 缺少必要的参数构造 实际上并没有缺少 只是隐藏了 点击函数前面灰色区域 右键选择 Force call type 即可修复

现在显示正常了。

2.FindClass 和 RegisterNatives 是什么函数?有什么作用?
作用:动态注册JNI函数 JNI_OnLoad方法和RegisterNatives方法的结合可以做到更佳方便的注册你的jni方法。