

writeup"女装大佬想你了"

原创

瑟瑟发抖的萌新  于 2017-11-06 19:45:08 发布  468  收藏

分类专栏: [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_38275468/article/details/78461019

版权



[writeup](#) 专栏收录该内容

1 篇文章 1 订阅

订阅专栏

关于RE4的那个“女装大佬想你了”的逆向题

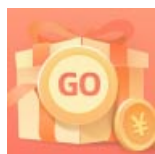
昨天刚做的时候, 想的就是用ida反编译一下, 但是最后发现完全用。

再然后就想着要是能把源码解析出来就好了, 于是就用AndroidKiller反编译了一下得到了一堆smali代码在从网上看过相关语法以后不得不承认自己还是看不懂的事实, 于是才想办法找到smali2Java将它转换成Java代码, 然后经过分析发现, Java代码中调用了一个非Java语言方法 (我是第一次知道Java中还有这种操作), 该方法的返回值就是flag, 但是反编译出来的全是Java文件, 根本没法找到一个非Java的文件, 这条路暂时走不下去了。

```
public native String PwdFromC();
```

然后是今天, 看了大佬们在群里发的消息才知道, 原来apk这种文件是可以直接解压的, 解压后用ida打开libPwd.so文件通过search data找了flag。但是这么做总觉得是瞎猫碰上死耗子, 所以打算明天好好问下别人。虽然这道题到现在到现在也搞得不是太明白, 但在这个过程中确实也学到了不少东西。

我对于直接反编译成Java代码的原理还有点疑惑, 不知道转换过程中对于原来非Java的代码程序是怎么处理的, 是转换成Java代码, 还是有什么其他的处理方式, 打算再查一查。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)