

Android入门指南

0x00 语言

- 1.现在大部分的Android程序都是用Java写的，所以要看懂一个程序在干什么就应该了解Java的语法
- 2.要更改安卓程序的执行流程，就应该了解安卓的“汇编语言”，Smali代码
- 3.涉及到native层的时候，能看懂C或C++

0x01 工具

- 1.熟练使用jeb和jadx
- 2.熟练使用jeb或Android Studio调试java层
- 3.熟练使用ida调试native层
- 4.熟练使用APK改之理或其它工具对Apk进行更改

0x02 其它

- 1.可以了解一些关于hook的东西，对于爆破或更改程序流程有奇效
- 2.了解apk加壳脱壳的方法过程

0x03 资料

- 1.开发入门的经典书籍《第一行代码》，进阶书籍《Android开发艺术探索》
- 2.关注一些大佬们的文章，比如：<https://mp.weixin.qq.com/s/Slbc0Ulc5ZbL4bzQbl32KQ> <-----详细入门知识！！
- 3.学会看官方文档JNI,Android API,Smali
- 4.我整理的smali语法(T▽T)
- 5.Hook的文章，官方文档
- 6.历代壳

0x04 写在最后

- 1.我该怎么学呢？

学习的过程是一个练习的过程，在学习过程中应该多进行练习

2.学了这个有什么用呢？

说的骚一点，你可以更改游戏里面的数据，改货币什么的都没问题。（当然不是所有游戏）