




# Reverse 解法2: bang Writeup (安卓简单的加壳) (2020网鼎杯青龙组)

原创

龙雪  于 2020-05-11 21:09:11 发布  2661  收藏

分类专栏: [CTF](#) 文章标签: [android apk 安全 经验分享](#)

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/lostnerv/article/details/106061517>

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

在强力大佬的教导下, 使用了另一种解法脱壳

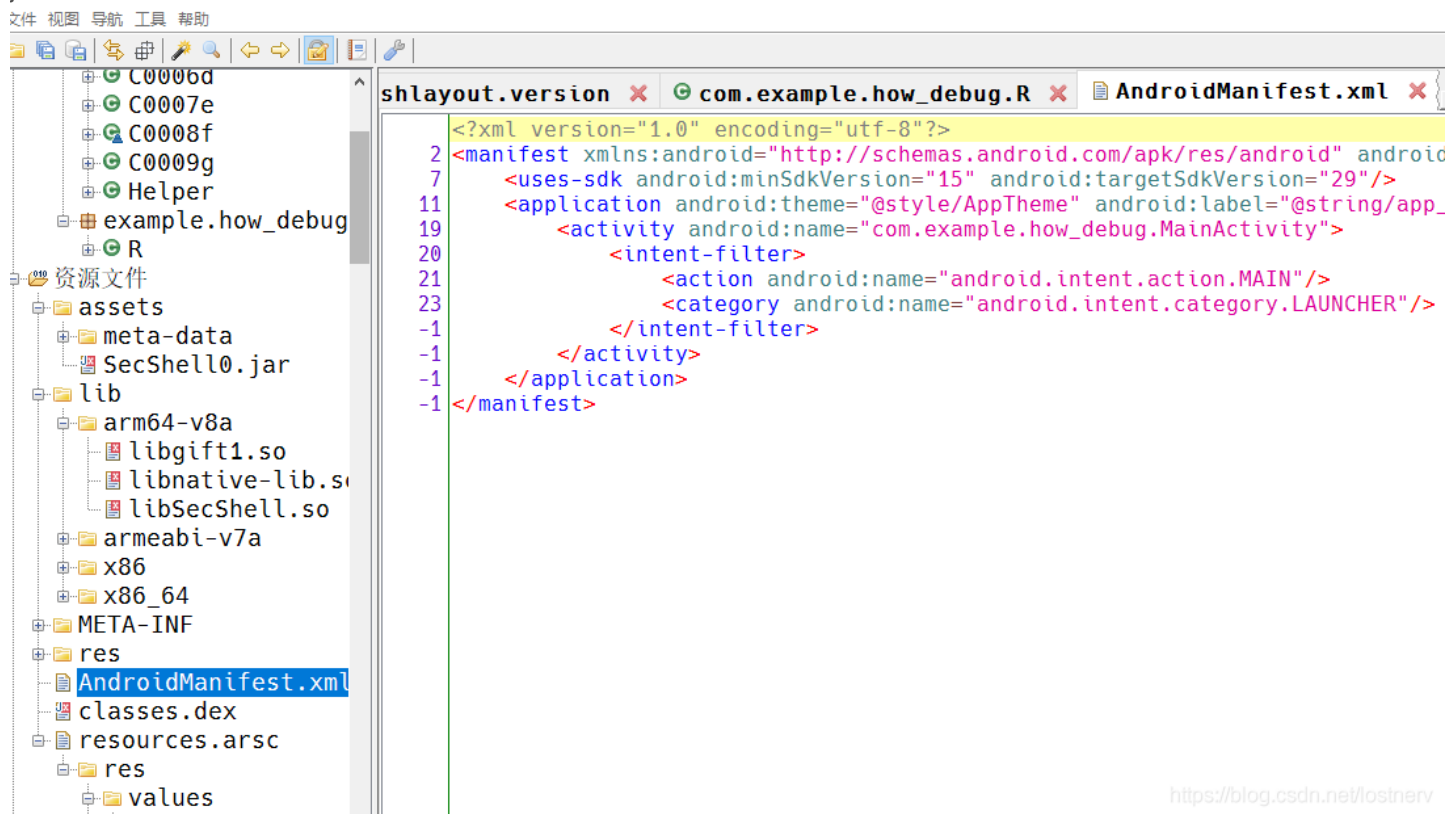
一个脱简单壳的Xposed模块

解法1: [点我](#)

## 我用到的工具:

- [ApkShelling](#)模块
- Xposed
- android 8.0以下的模拟器或某能刷的实机 (不做介绍)
- Android Studio
- jadx

jadx导入截图还是如下:



## 模拟器

先说说这个模拟器，自己用AVD Manager创建或者网上下载的游戏模拟器，甚至用实体机都可以，但据dumpDex和Xposed安装最好是Android 8.0以下，高版本的还需要另换工具这里就不介绍了。

## root

首先要有root权限，比如我的游戏模拟器自带root:



手动root的方法可参考搞机：AS自带模拟器AVD Root 和 Xposed安装

## Xposed

- 当然如果本机已有安装，可以跳下一步解题~

下载一个了xposex.installer.5.11.apk安装，端口号不清楚的话可以百度或者自己查本机监听。

```
adb connect 127.0.0.1:9974
adb install xposex.installer.5.11.apk
```

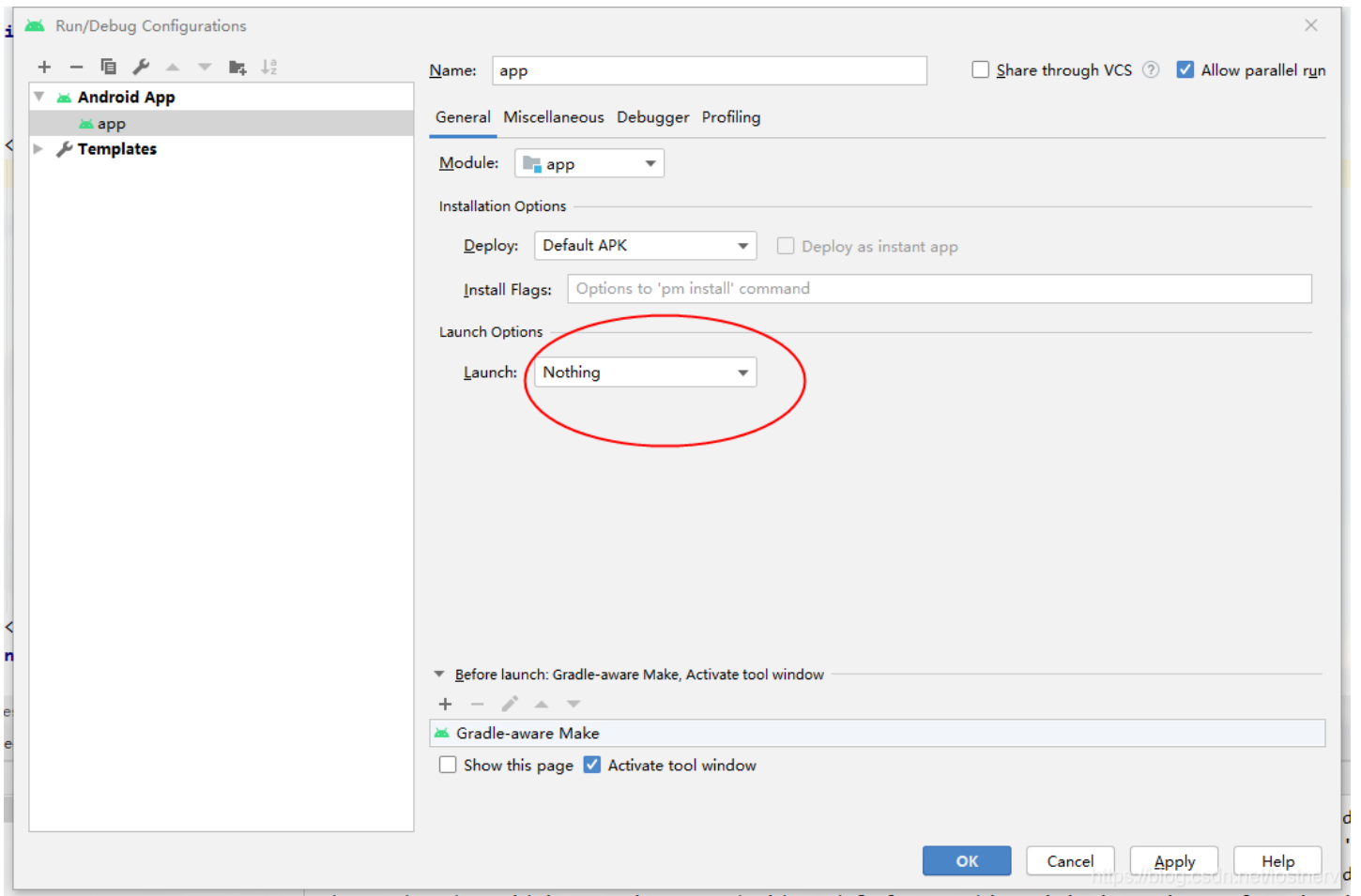
安装上之后运行，完成下载，重启。

## 开始正式解题

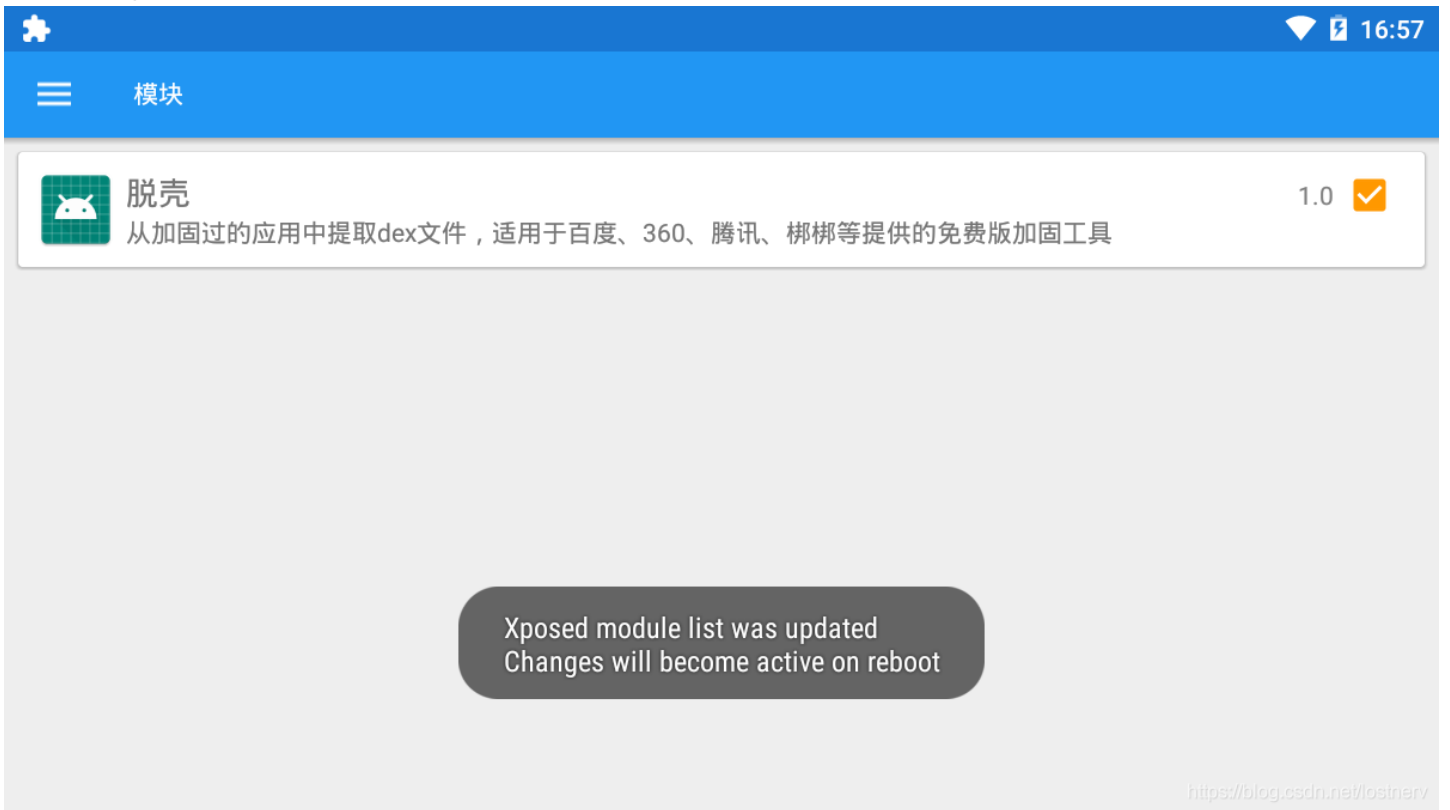
Android Studio 打开 ApkShelling，修改 targetPackages 值加入需要脱壳的包名：

```
private static final String[] targetPackages =  
    new String[]{"com.example.how_debug", "com.sfysoft.shellingtest2"};
```

launch option改为nothing:



run安装，Xposed勾选模块，重启。



重启后安装并且启动题目apk，取 `/data/data/题目包名/` 路径下的dex

```
adb pull /data/data/com.example.how_debug/00067-02.dex d:/test
```

jadx直接打开dex，找flag~

## 其他提示：

通过日志查看Xposed把xxx.dex dump到了哪里：

```
adb -logcat -s Xposed
```

去路径下瞄一眼等：

```
adb shell
cd /data/data/com.example.how_debug/
ls -l
等等...
```

主要参考的文章：

[搞机：AS自带模拟器AVD Root 和 Xposed安装](#)  
[ApkShelling](#)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)