# 签名绕过

## java绕过

搜索Landroid/content/pm/PackageInfo;->signatures:[Landroid/content/pm/Signature;定位。

定位到的方法为：

Lcom/kingroot/kinguser/ace;->dx(Ljava/lang/String;)Landroid/content/pm/Signature; = is call

Lcom/kingroot/kinguser/ace;->dv(Ljava/lang/String;)Landroid/content/pm/Signature; = is called

进一步查找：

Lcom/kingroot/kinguser/ace;->dx(Ljava/lang/String;)Landroid/content/pm/Signature; = is call----------------------------为获取手机已安装程序的

Lcom/kingroot/kinguser/ace;->du(Ljava/lang/String;)Ljava/lang/String; = is called

param = /data/app/com.kingroot.kinguser-1/base.apk-----------为本apk的签名信息获取

Lcom/kingroot/kinguser/ace;->dv(Ljava/lang/String;)Landroid/content/pm/Signature; = is called

Lcom/kingroot/kinguser/ace;->du(Ljava/lang/String;)Ljava/lang/String; : res = E89B158E4BCF988EBD09EB83F5378E87

因此，只需要将程序的返回值永远是真是的apk签名的md5信息就好了。

## so绕过

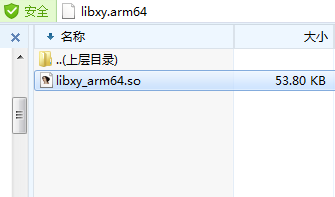
native 方法

load/loadLibrary

Lcom/kingroot/kinguser/zu;->F(Ljava/lang/String;Ljava/lang/String;)Z:load = /data/data/com.kingroot.kinguser/applib/libpu.so------------------------------------初步确定为反调试的so

Lcom/kingroot/kinguser/zu;->F(Ljava/lang/String;Ljava/lang/String;)Z:load = /data/data/com.kingroot.kinguser/applib/libhxy64.so -------------------------------初步确定为签名验证的so

进一步分析上面libhxy64.so,发现是libxy.arm64解压(为gzip格式)后得到的。



通过ida逆向，



因此将so修改后，重新打包为gz格式的压缩包，放到assets目录下。