# 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

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

native 方法

load/loadLibrary