# 签名绕过

发现这个签名绕过，是在kingroot原版root后卸载可用，而重启后不可用。

## 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

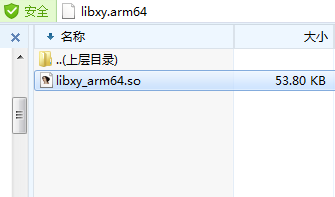
native 方法

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。

## other

在上面两个都搞定了以后，发现在kingroot(原始)root完毕，再安装我的包，还是出现下面的：



界面为：dialog\_repackage\_warning.xml

activity为：Lcom/kingroot/kinguser/activitys/RePackageWarningActivity;

Lcom/kingroot/kinguser/oq;->a(Lcom/kingroot/kinguser/xp;)V

->Lcom/kingroot/kinguser/atg;->w(Z)V======== Lcom/kingroot/kinguser/or;->w(Z)V

->Lcom/kingroot/kinguser/activitys/RePackageWarningActivity;

Lcom/kingroot/kinguser/oq;->a(Lcom/kingroot/kinguser/xp;)V

->Lcom/kingroot/kinguser/op;->c(Lcom/kingroot/kinguser/or;)Z

->Lcom/kingroot/kinguser/op;->b(Lcom/kingroot/kinguser/or;)Z

-> Lcom/kingroot/kinguser/op;->fX()Ljava/lang/String;

-> Lcom/kingroot/kinguser/ace;--------3种方式验证签名

其中一种能够方式ace.bk

Lcom/kingroot/kinguser/acu;->a(Lcom/kingroot/kinguser/acx;J)Lcom/kingroot/kinguser/acw;

-->Lcom/kingroot/kinguser/acw;-><init>(Ljava/lang/String;Ljava/lang/Integer;Ljava/lang/String;Ljava/lang/String;)V

-->iput-object p3, p0, Lcom/kingroot/kinguser/acw;->Hi:Ljava/lang/String;

在acu.a中

调用[Hh:export CLASSPATH=/data/data/com.kingroot.kinguser/applib/tm.dex && /system/bin/app\_process /system/bin com.kingroot.kinguser.TellMe 10124,Hl:export CLASSPATH=/data/data/com.kingroot.kinguser/applib/tm.dex && /system/bin/app\_process /system/bin com.kingroot.kinguser.TellMe 10124,mTimeout:120000,]

获取程序的签名md5

# a

root\_check\_page.xml=0x7f03004a

Lcom/kingroot/kinguser/yj;->kz()V--------Lcom/kingroot/kinguser/yu;->addContentView

->Lcom/kingroot/kinguser/bcq;->kB()Landroid/view/View;

->0x7f03004a and Lcom/kingroot/kinguser/bcq;->acj:Landroid/view/ViewGroup;