年前到现在南通项目的安全改动如下：

# 南通的安全测试

## 已修改

1. webview启动文件范围问题，hybrid 设置不可使用本地文件域

2. 增加ssl证书默认校验（各个手机上自身信任的CA机构）

3. 隐式意图调用

涉及南通百通业务本身的已修复，若第三方sdk涉及有隐式意图的，对南通百通业务无影响。

5. Intent Scheme URLs 攻击

涉及南通百通业务本身的已修复，若第三方sdk涉及有隐式意图的，对南通百通业务无影响。

6. 和第二条重复

7. DexClassLoader风险，南通百通之前未加固导致可能存在风险，以后打包会加固。

## 未修改部分和解释

4. WebView 忽略SSL 证书

暂未做证书下载功能，如果不忽略，如果访问第三方网站证书有任何问题都可能导致网页打不开

8. 可以用浏览器跳转到南通页面，能跳转的页面是南通百通启动页，是为了让用户从网页打开南通百通，没有敏感数据。

9. 动态注册广播风险，无需修改：扫描结果显示为第三方SDK（百度地图、腾讯X5）及组件库动态注册Receiver，与业务无关，不涉及敏感信息

10. 南通百通自己没有开发so库，第三方的so库不会泄露南通的敏感数据。

# 平安的安全测试

## 已修改

2:Activity劫持

 答：已修改：已修改为使用爱加密防activity劫持方案，在南通百通app退出到后台时，会检测是否是用户主动退出，如果不是，则会友好的提示用户南通百通app

3：调试日志函数调用风险

 答：已修改：南通百通自身代码日志函数已全部删除，剩余第三方SDK（百度地图、壹钱包、腾讯X5）及组件库日志函数，未涉及业务敏感数据，无需要修改

4：残留URL检测

 答：已修改：南通百通代码残留http类型 url 已全部删除，https类型url因已做证书校验，可不用处理，其他检测的南通自身代码只是域名而不是接口URL故无需处理，剩余其他为第三方SDK（壹钱包）及JDK内部代码，不影响南通百通安全

6：日志泄露风险：

 答：已修改，南通百通自身标准打印日志函数代码已全部删除，第三方SDK（腾讯bugly、百度地图）及组件库标准打印日志函数无业务信息打印，不涉及敏感信息

23：服务端证书校验

 答：已修改，现修改为对证书签发机构及南通百通域名进行证书校验

34：webview隐藏接口风险

 答：已修改：扫描结果中的南通百通自身的三个内置的接口已经删除，其他的第三方SDK（百度地图）不影响APP安全

## 未修改部分和解释

1:WebView远程代码执行

 答：无需修改：该问题只有在4.2以下版本才会出现，

南通百通支持的最低版本为19，即4.4版本，故不会出现该问题

5：存储卡的操作行为

 答：无需修改：南通百通头像上传功能中获取头像（拍照）涉及到存储卡操作，无其他敏感信息保存在存储卡中，其他第三方SDK操作存储卡不影响南通百通安全

7：动态注册Receiver风险

 答：无需修改：扫描结果显示为第三方SDK（百度地图、腾讯X5）及组件库动态注册Receiver，与业务无关，不涉及敏感信息

8：设备信息手机号操作行为

 答：无需修改：业务所需，设备信息手机号即IMEI，可作为手机唯一标识，南通百通需要统计用户相关数据，需要该IMEI作为用户唯一标识

9：获取地理位置：

 答：无需修改：业务需要，南通百通天气、公交等功能需要获取用户定位才能为用户提供服务，

10：AES/DES 弱加密

 答：无需修改：扫描结果显示为第三方SDK（腾讯X5、平安人脸）提供AES/DES，南通百通自身代码仅对非敏感的下载文件进行加密，不涉及敏感信息

11：Activity 配置安全

 答：无需修改：南通百通业务场景需要使用到腾讯授权及第三方照片选择，调用时需要用户授权和传递必要的参数才能正常使用，有权限控制和参数校验的逻辑，故无需修改

12：webview无HTTPS校验风险

 答：无需修改，扫描结果显示为第三方SDK（腾讯X5），不涉及南通业务敏感信息，故无需修改

13：残留账号密码检测

 答：无需修改，扫描结果显示为第三方（腾讯X5）及壹钱包所需公钥，为公开可查询信息，无风险

14：PendingIntent错误使用Intent风险

 答：无需修改：扫描结果显示为第三方（百度地图）使用，不涉及南通业务敏感信息，故无需修改

15：BroadcastReceiver配置安全

 答：无需修改：第三方推送服务需要，南通百通通过第三方提供的推送ID才能使用receiver,有参数校验的过程，无风险

16：联系人操作行为

 答：无需修改：南通百通业务所需，缴费需要填写手机号需要获取联系人手机号码自动填写手机号，且获取联系人时需用户手动确认才能通过

17：升级包数据串改风险

 答：无需修改：南通百通自身apk升级均有签名校验机制且升级包有加固，且升级包安装有用户确认过程，故无风险

18：Service配置安全

 答：无需修改：推送业务需要用到此特性，有参数校验的过程，故无风险

19：SharedPreferences任意读写

 答：无需修改：南通百通业务无此方面的相关内容，

第三方SDK（腾讯X5）内部使用亦无关南通百通敏感业务，故无需修改

20：intent隐式调用

 答：无需修改，推送业务需要用到该特性，有参数校验的过程，无风险，第三方SDK（百度地图）内部使用亦无关南通百通敏感业务，故无需修改

21：控制力安全

 答：无需修改：地理位置，相机调用，水电缴费等业务需要相关权限，且权限申请需经过用户同意

22：程序反编译

 答：无需修改：南通百通已使用爱加密的高级付费加固方案，且所有代码均使用了混淆

24：客户端证书校验

 答：无需修改，已经对服务端证书进行了校验，客户端并无证书，所以不需要校验

25：数据库创建模式检测：

 答：无需修改：扫描结果显示为第三方SDK（百度地图）内部问题，与南通百通无关

26：使用反射检测

 答：无需修改：南通百通代码中所使用的反射均为正常编码使用，且不涉及敏感数据，所以无需修改。

27：Intent SchemeURL

 答：无需修改：南通代码已经对该种调用方式的参数传递做了校验，其他第三方SDK（百度地图，腾讯X5）及组件库，与南通敏感业务无关，无敏感数据泄露。

28：广告插入风险

 答：无需修改，南通百通自身业务全使用https协议，其他第三方SDK及网页不影响APP安全

29：敏感函数调用

 答：无需修改：南通百通调用的敏感数据函数皆为业务所需，且均需要用户手动确认是否授权，故无安全问题

30：加密函数检测

 答：无需修改：扫描结果显示皆为第三方SDK（百度地图、腾讯X5）及组件库，与南通业务无关，无敏感数据泄露，故无需修改

31：残留手机号检测

 答：无需修改：扫描结果显示只是测试用的随便填写的11位数字，并非真正的手机号

32：动态加载DEX文件检测

 答：无需修改：扫描结果显示为第三方SDK（百度地图，腾讯X5）的内部问题，南通百通无此问题，

33：ContentProvider访问路径配置

 答：无需修改：扫描结果中的provider皆只能APP内部调用，第三方应用不能调用，故无此风险

35：应用权限安全

 答：无需修改：扫描结果所列权限皆为业务所需，且均需要用户手动授权权限，故安全可控

36：资源文件保护安全

 答：无需修改：资源文件中并无敏感数据，若启动作检查，则会大大加长启动时间，且APP经过加固、混淆处理，综合考虑并无修改的必要

37：root环境防护检测

 答：无需修改：南通百通APP已经过加固且所有代码经过混淆，所有的数据均经过加密处理，故即使在root环境下也能保证安全

38：模拟器环境防护检测

 答：无需修改：南通百通APP已经过加固且所有代码经过混淆，所有的数据均经过加密处理，所有的接口均为HTTPS协议，故即使在模拟器环境下也能保证安全

39：纯Java代码风险

 答：无需修改：南通百通已经过加固处理，且所有代码均经过混淆，故java代码安全可控

40：随机数生成函数使用错误

 答：无需修改：南通百通仅在非敏感的数据使用该函数进行加密，对敏感数据无影响

## WebView文件域

是禁用file：协议引用本地文件，我搜了一下代码南通暂时没有用这种方式

建议测试方法：写一个web测试页，尝试用file：方式引用手机上的某一个文件

### 引入ssl校验

可能造成的影响：接口访问失败，拿不到数据。

建议测试页面：各种接口（南通接口，第三方接口）的页面都抽取几个测试。

建议测试方法：更改手机日期，让ssl证书过期。

## 隐式意图调用

我们的启动页开放出来分享到网页

腾讯需要他们的规定的页面开放出来，分享时拉取腾讯的应用登陆

建议测试方法：安全部门扫描，是否有除了这两个页面外的隐式意图

## Intent scheme URI攻击

Hybrid框架添加对Intentscheme的过滤

建议测试页面：配一个banner跳转

建议测试方法：网上搜索一个intentscheme语法，尝试在app浏览器中跳转

## DexClassLoader风险

理论上加固的包就没有这个风险

建议测试方法：安全部门扫描

**Activity劫持**

建议测试方法：安全部门扫描

## 调试日志函数调用风险

建议测试方法：测试用测试工具看app的日志打印情况，有没敏感信息日志

## 残留URL检测

建议测试方法：安全部门扫描

**webview隐藏接口风险**

建议测试方法：安全部门扫描