

NJSD

中国（南京）软件开发者大会

China (Nanjing) Software Developers Conference

2016

安全专项测试方案

Android版 钱辉



NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

测试方
案

测试的
点

测试案
例

测试总
结

2

3

1

4

目录页
Contents Page

测试方
案

测试的
点

测试案
例

测试总
结

NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

2

3

1

4

过渡页
Transition Page

3

3

平台	网址
腾讯御安全	http://yaq.qq.com
阿里聚安全	http://jaq.alibaba.com
爱内测	http://www.ineice.com
腾讯云乐固	http://legu.qcloud.com
阿里云测	http://mqc.aliyun.com

NJSD中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016



3

- App有哪些安全漏洞
- 如何检测安全漏洞
- 漏洞有什么危害
- 如何修复这些漏洞

NJSD

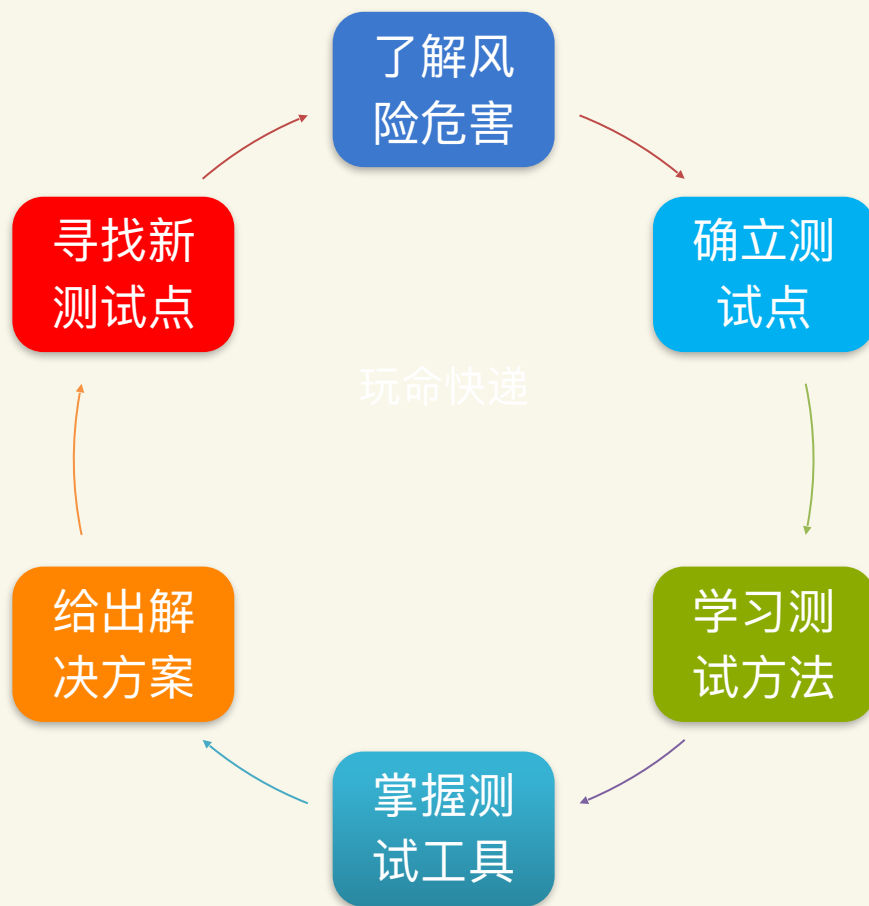
中国（南京）软件开发者大会

China (Nanjing) Software Developers Conference

2016



3

**NJSD**中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

测试方
案

测试的
点

测试案
例

测试总
结

NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

2

3

1

4

过渡页
Transition Page

7

总览

包含8大类，一共23测试点

序号	类别	测试点个数
1	反编译	3
2	权限扫描	1
3	应用组件检测	5
4	本地数据存储安全检测	2
5	Logcat日志检测	2
6	Xposed获取用户输入信息检测	1
7	配置信息风险	2
8	风险代码扫描	7
	总共	23

含有3个测试点

序号	检测点	说明	检测方法
1	反编译检测	可以使用apktool工具来反编译查看源码来窥探APK源码	apktool d <apkname></apkname>
2	二次打包检测	修改反编译后的文件，重新打包，伪装APK	apktool b <apkfolder></apkfolder>
3	重新安装检测	安装后，应该给出提示，提醒用户APK被修改	



含有1个测试点

序号	检测点	说明	检测方法
1	权限扫描	扫描出所有的权限,别给出每个权限使用情况,定位出使用权限的代码	Androguard的show_Permissions(dx)的方法

NJSD

中国（南京）软件开发大会

China (Nanjing) Software Developers Conference

2016



含有5个测试点

序号	检测点	说明	检测方法
1	Activity安全	暴露的activity组件,也就是exported属性设置为true的activity	检测方法是先用 <code>run app.package.attacksurface</code> 包名 找出暴露的个数,再用drozer中的 <code>run app.activity.info -a</code> 包名 找出具体的activity
2	Service安全	暴露的service组件,exported属性设置为true的	检测方法是先用 <code>run app.package.attacksurface</code> 包名 找出暴露的个数,再用drozer中的 <code>run app.service.info -a</code> 包名 找出具体的service
3	Broadcast Receiver安全	暴露的broadcast组件,exported属性设置为true的	检测方法是先用 <code>run app.package.attacksurface</code> 包名 找出暴露的个数,再用drozer中的 <code>run app.broadcast.info -a</code> 包名 找出具体的broadcast
4	ContentProvider安全	Content Provider的不安全使用会产生sql注入、文件遍历等漏洞,导致用户数据泄露	1.使用 drozer 运行 <code>run app.provider.info -a</code> 包名, 检查是否存在 content provider风险.
5	Intent安全	intent scheme URLs(意图协议URL),可以通过解析特定格式的URL直接向系统发送意图,导致自身的未导出的组件可被调用,隐私信息泄露。Intent隐式调用发送的意图可能被第三方劫持,如果含有隐私信息可能导致内部隐私数据泄露	检测有没有添加预防代码,比如 <code>addCategory</code> http://wolfeye.baidu.com/blog/intent-scheme-url/

NJSD

中国(南京)软件开发者大会

China (Nanjing) Software Developers Conference

2016



含有2个测试点

序号	检测点	检测方法
1	本地数据敏感信息检测	检查 /data/data/<packagename>、/sdcard/ 及其他应用使用到的存储的数据是否经过加密，尝试使用主流解密方法进行解密，本地没有经过加密的存储数据均非敏感信息（如密码、金额、cookie、token） </packagename>
2	本地数据防篡改检测	当手动篡改本地存储数据后，应用能检测到此篡改并自动修正并给出警

NJSD

中国（南京）软件开发大会

China (Nanjing) Software Developers Conference

2016



含有2个检测点

序号	检测点	说明
1	调试信息	debug信息在发布版本中不应该出现
2	敏感信息	logcat中不应该出现一些敏感信息



含有1个测试点

序号	检测点	说明	检测方法
1	用户名密码防hook	防止利用xposed获取用户名密码信息	自己编写的小工具来利用xposed获取TextView中的值



包含2个监测点

序号	检测点	说明	检测方法
1	allowBackup	当allowBackup为true时,用户信息可以被备份到pc端,然后用另一个手机的相同客户端打开,就可以打开被备份的信息	用ClassyShark工具打开APK, 查看Manifest文件中的application节点下的allowBackUp有没有配置, 要显式的改为false才可以,但是要记住, 也有的app通过比对设备号来清空缓存信息来规避这种风险
2	debuggable	也存在application节点中, 发布时应该改为false	同上

NJSD

中国(南京)软件开发大会

China (Nanjing) Software Developers Conference

2016



1	文件权限风险	检测数据是否被授权用户或应用进程访问。如果开发者使用openFileOutput(String name,int mode)方法创建内部文件或者使用getSharedPreferences读取配置信息时,如果MODE_WORLD_READABLE或MODE_WORLD_WRITEABLE模式,就会让这个文件变为全局可读或全局可写的	反编译代码搜索上面两个方法
2	WebView默认开启密码保存功能	WebView默认开启密码保存功能,如果该功能未关闭,在用户输入密码时,会弹出提示框,询问用户是否保存密码,如果选择"是",密码会被明文保存到/data/data/com.package.name/databases/webview.db	检索WebSettings.setSavePassword代码
3	https证书校验风险	开发者在代码中不检查服务器证书的有效性,或选择接受所有的证书。这种做法可能导致的问题是中间人攻击。分析方案 检测程序与服务器的通信验证是否有证书,是否有证书合法性和一致性校验,checkServerTrusted方法不能实现为空,应严格校验,可以实现或者调用父类函数	代码检索checkServerTrusted
4	webview使用searchBox.JavaBridge_风险	webview组件的接口函数searchBox.JavaBridge_存在远程代码执行漏洞,远程攻击者利用此漏洞能实现本地java和js的交互,可以对Android移动终端进行网页挂马从而控制受影响设备。	调用removeJavascriptInterface("searchI
5	webview使用三方插件风险	当系统辅助功能中的任意一项服务被开启后,所有由系统提供的WebView都会被加入两个JS objects,分别为是"accessibility"和"accessibilityTraversal",如果应用使用了系统的WebView,并且设置了setJavaScriptEnabled(true),那么恶意攻击者就可以使用"accessibility"和"accessibilityTraversal"这两个Java Bridge来执行远程攻击代码	在onPageStarted()方法中调用WebView.removeJavascriptInterface("ac方法显示的移除accessibility、accessibil

NJSD

中国(南京)软件开发者大会

China (Nanjing) Software Developers Conference

2016



测试方
案

测试的
点

测试案
例

测试总
结

NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

2

3

1

4


















过渡页
Transition Page

```
58deMacBook-Pro-7:apk wuxian$ apktool d zhuanzhuan.apk -r -f
I: Using Apktool 2.0.3 on zhuanzhuan.apk
I: Copying raw resources...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs
```

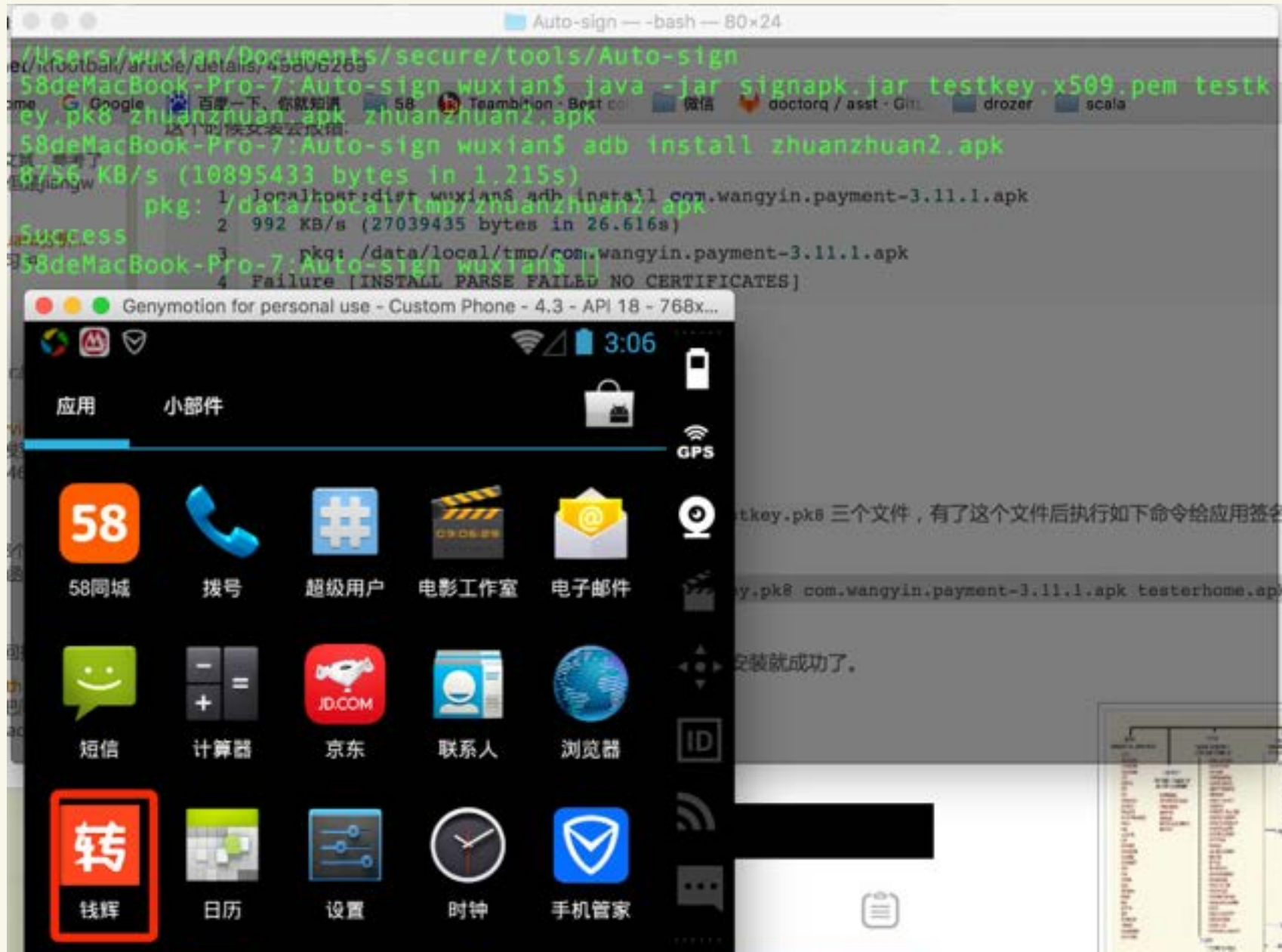
> mipmap-mdpi-v4	25	<string name="about_us_title">关于转转</string>
> mipmap-xhdpi-v4	26	<string name="about_zhuanzhuan_app_name">转转</string>
▼ mipmap-xxhdpi-v4	27	<string name="about_zhuanzhuan_app_version">V1.0.0</string>
ic_launcher.png	28	<string name="action_settings">Settings</string>
> mipmap-xxxhdpi-v4	29	<string name="add_address">新增地址</string>
> raw	30	<string name="address_hint">请输入详细的地址信息</string>
▼ values	31	<string name="agree_refund_success">退款成功</string>
animations.xml	32	<string name="agree_refund_when_arbi_dialog_title">同意退款后, 钱
arrays.xml	33	<string name="all_evaluation">全部评价</string>
attrs.xml	34	<string name="all_picture">所有图片</string>
booleans.xml	35	<string name="app_name">钱辉</string>
colors.xml	36	<string name="apply_arbi_fail_tip">提交失败</string>
dimens.xml	37	<string name="apply_arbi_success_tip">提交成功</string>
drawables.xml	38	<string name="apply_service">申请客服帮助</string>
strings.xml	39	<string name="apply_service_help">申请人工客服</string>



```
[58deMacBook-Pro-7:apk wuxian$ apktool b zhuanzhuan
I: Using Apktool 2.0.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether sources has changed...
I: Smaling smali_classes2 folder into classes2.dex...
```

归档实用工具	其他	The Unarchiver
 app-debug.zip	 assets ▶	 zhuanzhuan.apk
 com.wuba.zh...1003001.zip	 build ▶	
其他	 dist ▶	
 .DS_Store	 lib ▶	
 58 ▶	 original ▶	
 cmb.pb_4.1.0_410 ▶	 res ▶	
 qq ▶	 smali ▶	
 weixin ▶	 smali_classes2 ▶	
	 unknown ▶	





NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

转

钱辉

1.Xposed恶意插件

2.原理：Hook住TextView.setInputType和Activity.onPause方法

3.演示:xposed_mm_alipay.mov

4.防护

5.防护后的效果演示:xposed_protect.mov

NJSD

中国（南京）软件开发者大会

China (Nanjing) Software Developers Conference

2016



测试方
案

测试的
点

测试案
例

测试总
结

NJSD

中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016

2

3

1

4

过渡页
Transition Page

- 一个测试点的确立需要经过反复的论证，实践
- 要不间断的学习了解新兴的漏洞，及时补充你的测试点
- 在给出解决方法前，你的工作都不算结束

The logo for the China (Nanjing) Software Developers Conference (NJSD) 2016. It features a blue ribbon-like shape with the text "NJSD" in large white letters, followed by "中国(南京)软件开发者大会" and "China (Nanjing) Software Developers Conference" in smaller white text. Below this, the year "2016" is displayed in white on a darker blue background.

NJSD

中国(南京)软件开发者大会
China (Nanjing) Software Developers Conference

2016



看雪论坛

[http://bbs.pediy.com/
forumdisplay.php?f=161](http://bbs.pediy.com/forumdisplay.php?f=161)*freebuf*<http://www.freebuf.com/>

安卓安全中文网

<http://www.droidsec.cn/>

阿里聚安全

[http://jaq.alibaba.com/blog.htm?
spm=0.0.0.0.Do7Xjx](http://jaq.alibaba.com/blog.htm?spm=0.0.0.0.Do7Xjx)**NJSD**中国（南京）软件开发者大会
China (Nanjing) Software Developers Conference

2016



感谢您的聆听