

Android 7.0+ 抓包https的一种方案(支持微信7.0)

sheenaghWS [关注](#)

3 2019.01.20 18:39:51 字数 972 阅读 10,414

一、背景

Android 7.0 之后增加了对第三方证书的限制，抓包工具（charles、fiddler等）提供的证书都无法通过校验，也就无法抓取HTTPS请求了，对测试工作影响很大。

最近更新的微信 7.0 也增加了第三方证书校验，导致无法正常抓包。

解决该问题一般有三个思路：

1. 让开发打一个测试包，关闭对证书的校验。
2. 将设备root，将证书安装到system分区。
3. 将设备root，利用Xposed框架，利用justTrustme/SSL-killer等模块绕过第三方ssl的校验

以上三个思路虽然可行，但都比较复杂，配置成本比较高。有没有更简单的方法呢？

当然是有的。

这个方法仍然是利用思路3，不过利用virtualXposed工具，能够省去root的过程，安装两个软件即可搞定。

二、virtualXposed简介

经常折腾 Android 刷机的同学应该都知道Xposed这个神级hook框架的存在。借助该框架以及开源插件，能够在不修改apk的情况下影响程序的运行。简而言之，借助Xposed框架和该框架之上的插件，能让app的功能强大十倍！

最常见的插件比如：

微信自动抢红包、消息防撤回、自定义界面、自动回复、消息屏蔽。。

抖音自动关注点赞，下载视频。。

修改系统界面、修改步数、虚拟定位。。

。。。

JustTrustme 就是其中一个插件，用于绕过 ssl 证书检查，借助它可以实现对 https 的抓包。类似的插件还有 SSLkiller、sslunpinning 等。

当然，这么强大的工具也有其缺点。最大的问题还是安装过程和系统兼容性。

1. Xposed 安装需要root。如今root本身就是一件比较麻烦的事。。
2. 国产手机厂商最热衷定制rom，导致Xposed存在很大的兼容性问题，一不小心就容易让手机变砖。。
3. 微信 检测到相关插件后，会有封号风险。。

为了解决以上问题，国内一位大神借助 [VirtualApp](#) 实现了Xposed的一种免root方案 [VirtualXposed](#)。

简单来说就是，VirtualXposed 制作了一个虚拟环境（可以理解为虚拟机），该虚拟环境中内置Xposed环境，用户只需将软件安装到该虚拟环境中，就能使用xposed的功能了。

详细使用参考官方说明：[无root使用 Android 最强大的 Xposed 框架](#)

写下你的评论...

评论5

赞20

...

推荐阅读

这是一份面向Android开发者的复习指南

阅读 9,301

丧心病狂的Android混淆文件生成器

阅读 6,847

Android | 一文带你全面了解 AspectJ 框架

阅读 878

深入浅出Android屏幕刷新原理

阅读 1,725

如何加载100M的图片却不撑爆内存，一张 100M 的大图，如何预防...

阅读 8,813

- virtualXposed.apk
- justTrustme.apk 或 SSLkiller.apk 或 sslunpinning.apk

工具下载：
链接：<https://share.weiyun.com/5T0MOuV>（密码：EbVV）

四、使用方法

先阅读官方说明：<https://mp.weixin.qq.com/s/8bpyljRS21NGseq1DFQmQQ>

以Justtrustme.apk为例，SSLkiller.apk 和 sslunpinning.apk类似。

1. 安装 virtualXposed.apk 和 justTrustme.apk 模块。
2. 启动virtualXposed，安照提示赋予相应的权限。
3. 在主界面点击菜单按钮，选择"添加应用"
4. 在添加应用列表选择 "justTrustme" 和 需要抓包测试的App（比如微信、微博），并安装
5. 在 virtualXposed 中打开 xposed 应用。点击左上角菜单按钮，切换到模块。此时会看到 "justTrustme" 选项。
6. 在 "justTrustme" 选项后打钩，并按照提示，返回菜单界面重启virtualXposed
7. done！

完成以上设置后，virtualXposed 中的 https 应用都能直接抓包，不会再提示证书无效了。

五、参考

- [如何使用Xposed+JustTrustMe来突破SSL Pinning](#)
- [重磅！VirtualXposed，让你无需Root也能使用Xposed框架！](#)

20人点赞 >


测试工作

...

"小礼物走一走，来简书关注我"

赞赏支持

还没有人赞赏，支持一下



sheenaghWS

总资产5 (约0.51元) 共写了1.3W字 获得53个赞 共17个粉丝

关注

写下你的评论...

全部评论 5

只看作者

按时间倒序 按时间正序



且试天下Always

5楼 04.29 16:23

▲

想抓包其他 App 里的 https 数据也可以吗

写下你的评论...

评论5

赞20

...