**抓取微信小程序数据包的三种方法**

1. **前言**

做安全测试的都会遇到测试某微信小程序，而微信小程序基本都是基于HTTPS的，所以抓取HTTPS数据包就是最关键的一步。最近几天折腾了一下，整理了比较简单、方便的三种方法。

1. **条件**

抓取微信小程序数据包的关键点，就是SSL证书绑定的问题。  
在安卓系统7.0以下的版本，不管微信是什么版本，都会信任系统提供的证书，而现在微信版本已经到了7.0.15 且安装老版本也会强制用户升级，且微信只信任系统及自身内置的证书。  
具体如下

安卓系统7.0以下：微信的任意版本，都会信任用户提供的证书

安卓系统7.0以上：微信7.0以下版本，微信会信任用户提供的证书

安卓系统7.0以上：微信7.0以上版本，微信只信任系统及自身内置的证书

IOS不做探讨。  
实验环境  
Redmi Note 4X 手机（未ROOT）

Android 手机：MIUI 11.0.2

Android 内核版本：7.0

微信：WeChat 7.0.15

MuMu 模拟器 版本：1.9.15

Android 内核版本：6.0.1

微信：WeChat 7.0.10

VirtualXposed ：0.15.1

1. **XPosed 和 JustTrustMe 抓包**

简介：XPosed 是一个框架，用来改变系统的某些关键操作。JustTrustMe 用来禁用、绕过SSL 证书验证，使用这种方法进行抓包的时候要求安卓手机必须需要ROOT。

1. **安装网易MuMu模拟器**

官网：<http://mumu.163.com/>

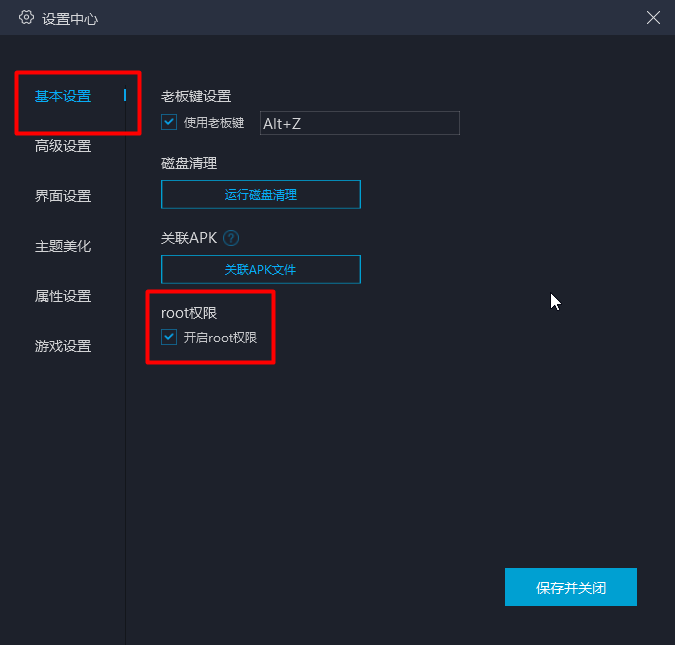
安装模拟器之后，安装Android 内核版本为6.0.1，打开设置，如下图：



1. **安装XPosed框架**
2. **开启root权限**

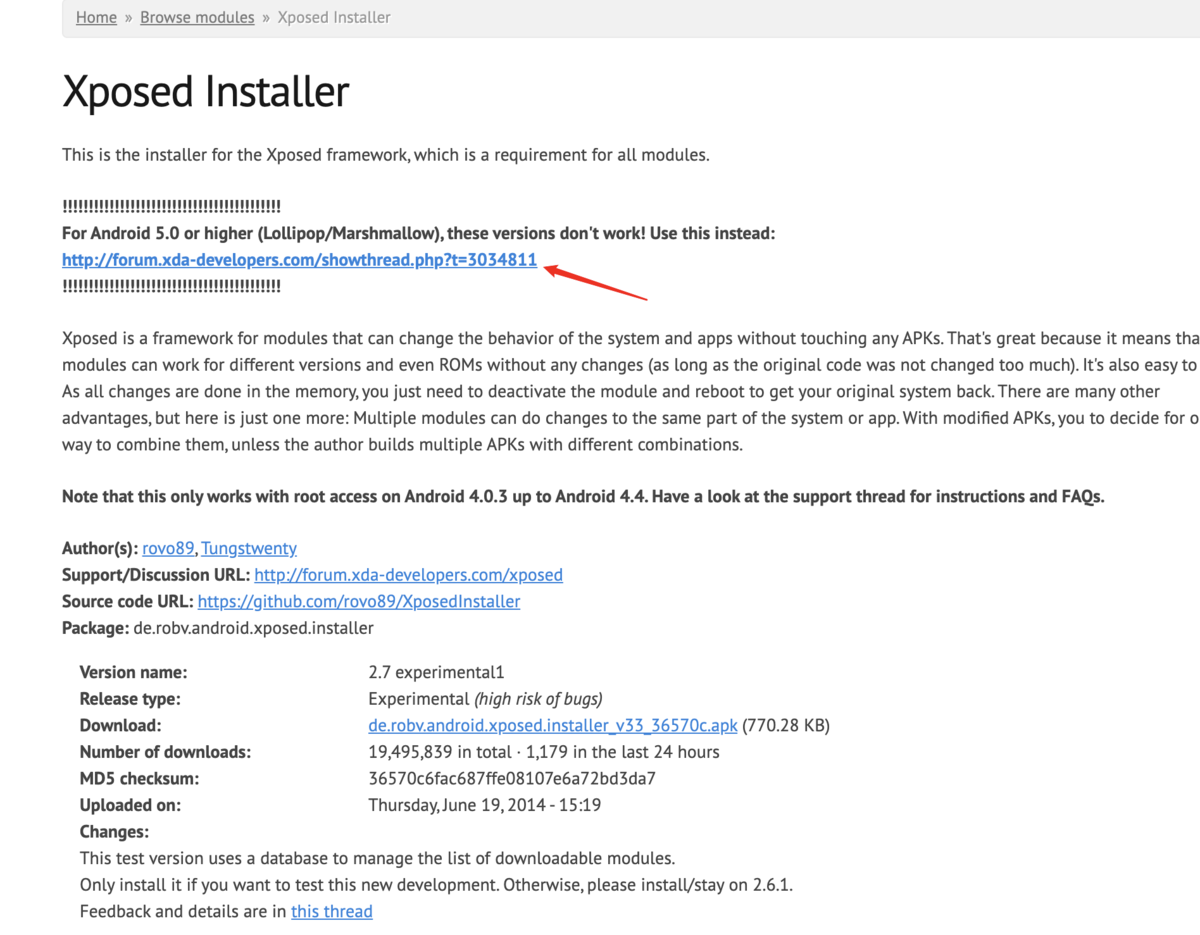
安装XPosed往往需要root权限，所以在模拟器开启root权限，确保成功安装XPosed



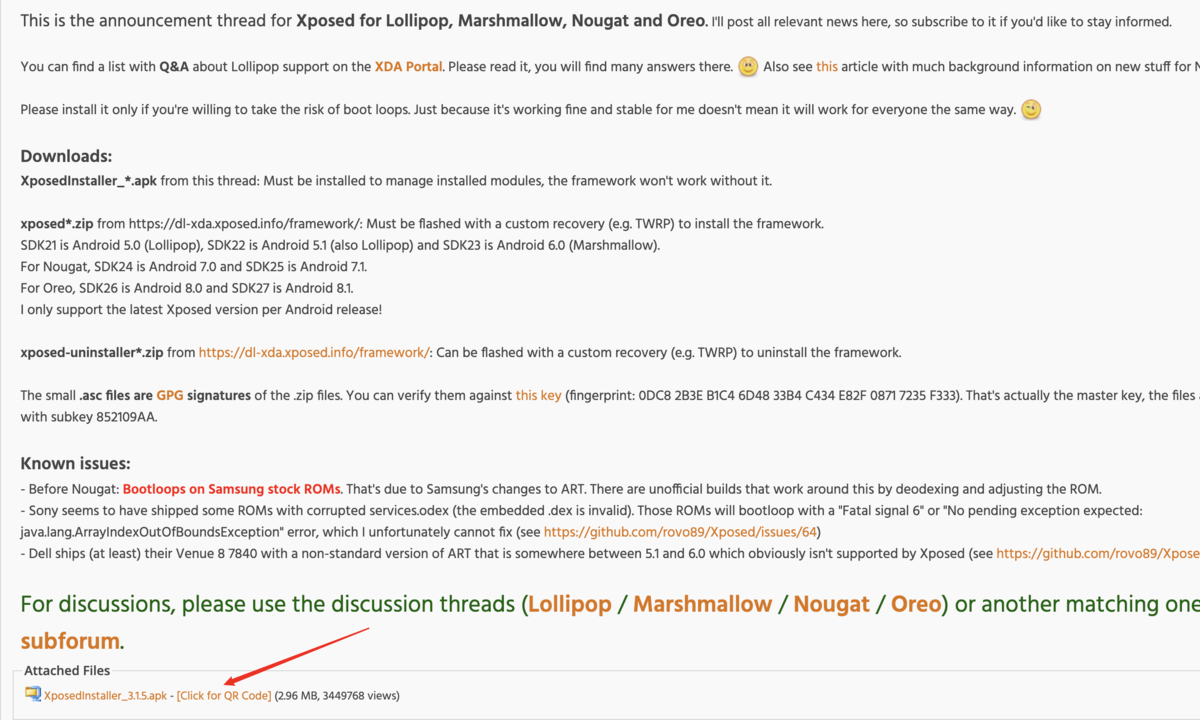


1. **安装XPosed**

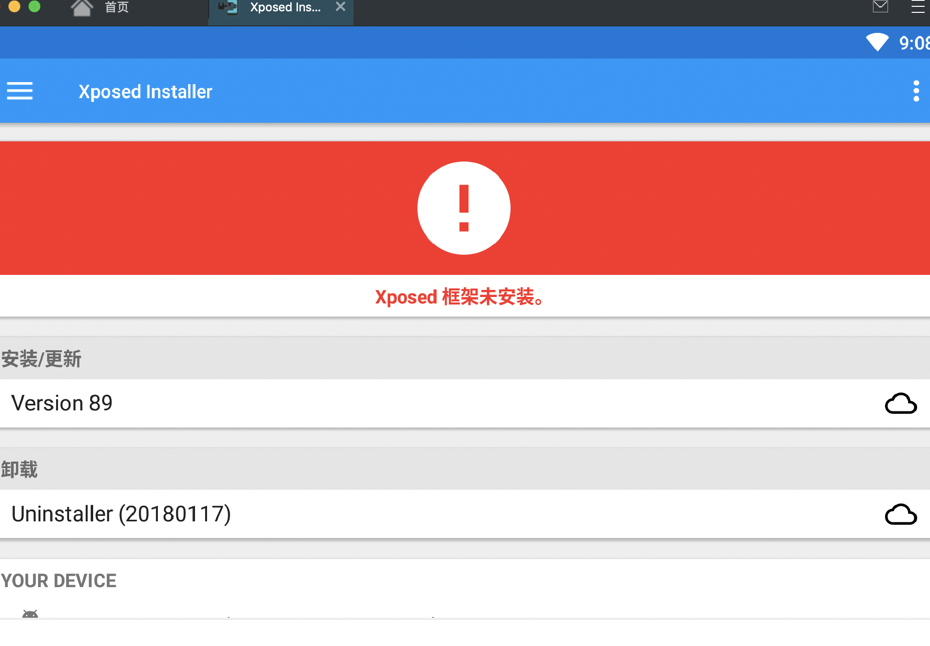
XPosed 官网地址：[https://repo.xposed.info/module/de.robv.android.xposed.installer](https://links.jianshu.com/go?to=https://repo.xposed.info/module/de.robv.android.xposed.installer" \t "_blank)



Android 版本5.0 以上点击该链接。



来到该页面。点击apk下载并安装到网易MuMu模拟器。

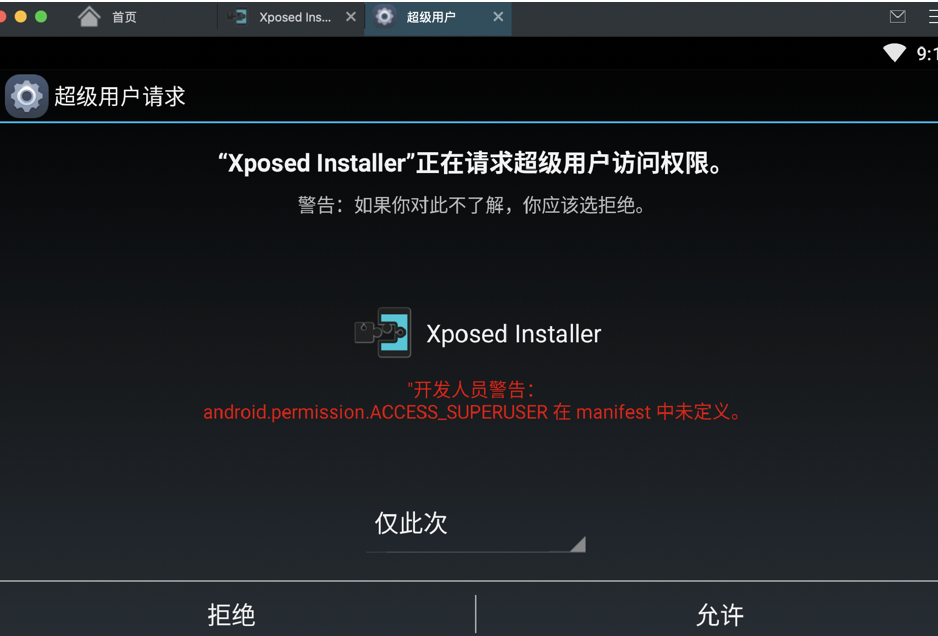
安装Xposed框架。



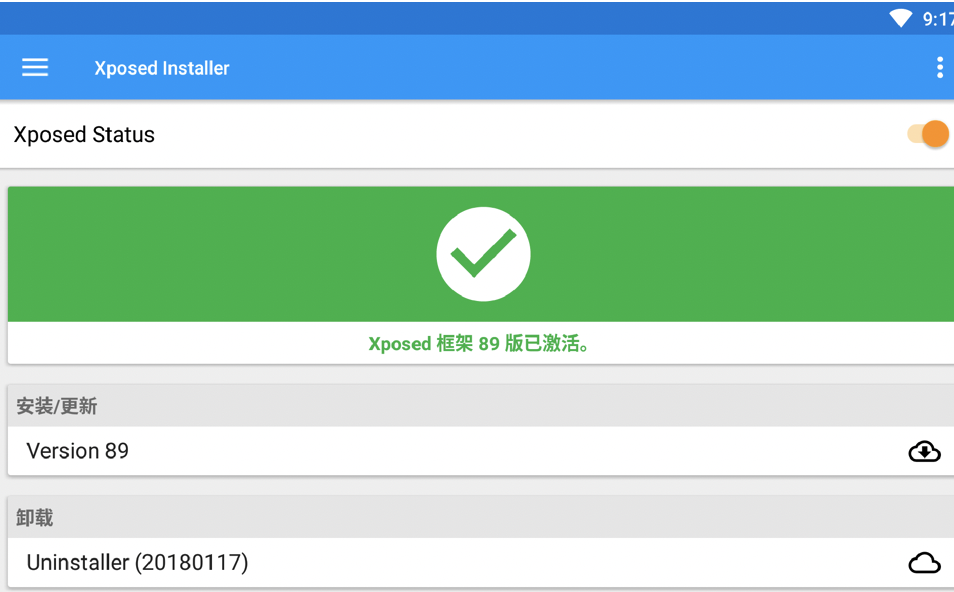
注意这里设置MuMu开启ROOT权限。否则安装不成功。

勾选"开启ROOT权限"。解决"Failed to get root access"错误。

下载安装以后。

点击"允许"，之后重启设备。

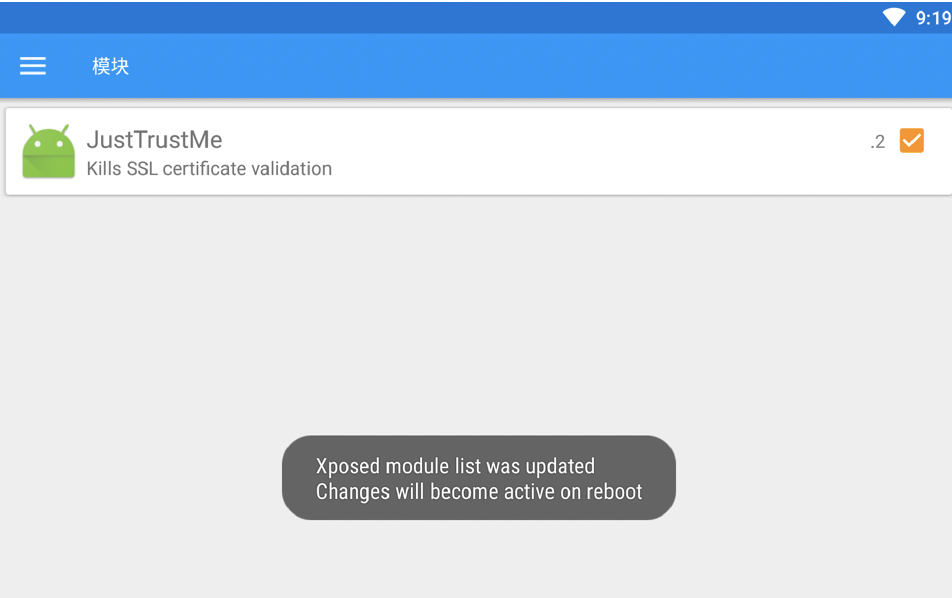


显示Xposed框架成功激活。

1. **安装JustTrustMe**

JustTrustMe官网地址：<https://github.com/Fuzion24/JustTrustMe/releases/tag/v.2>

[直接下载](https://links.jianshu.com/go?to=https://github.com/Fuzion24/JustTrustMe/releases/tag/v.2" \t "_blank)后拖进MuMu模拟器即可，在Xposed install 中选择模块，勾选"JustTrustMe"



安装成功，重启安卓系统设备后

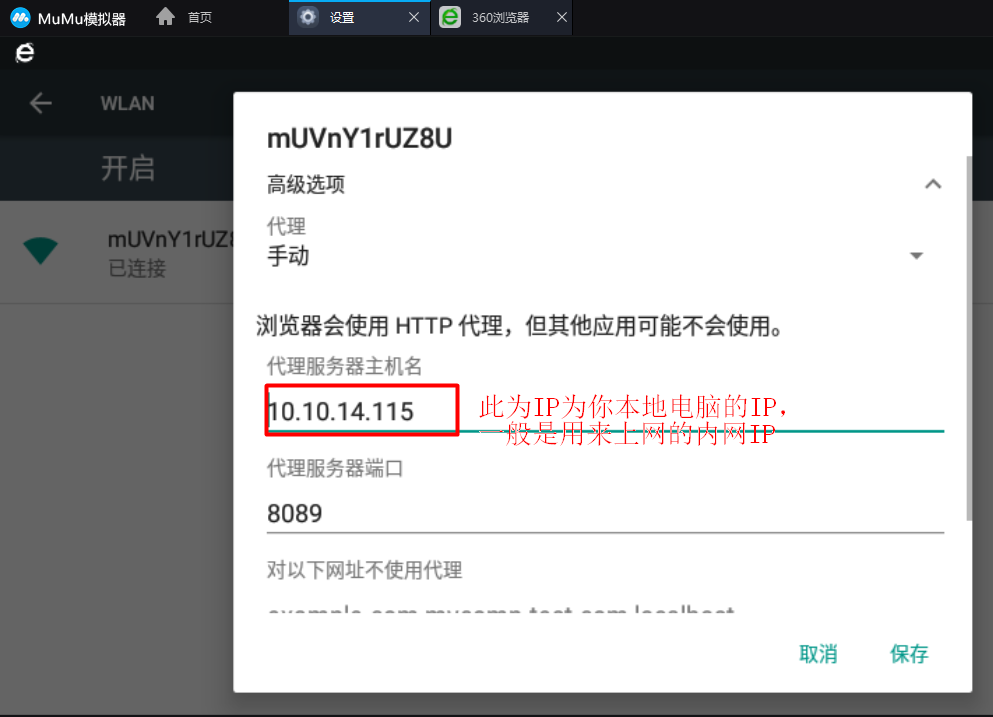
1. **设置网络代理，转发流量**
2. **配置手机网络代理**

此处在手机或者模拟器里面的安装系统上进行配置



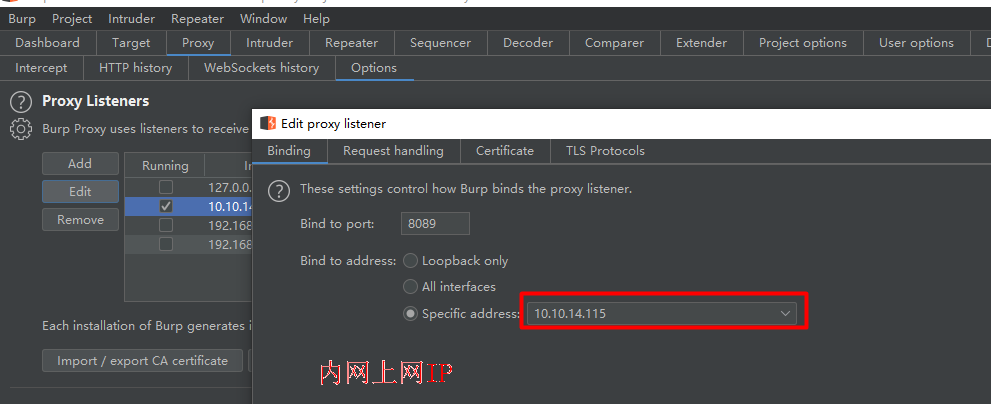


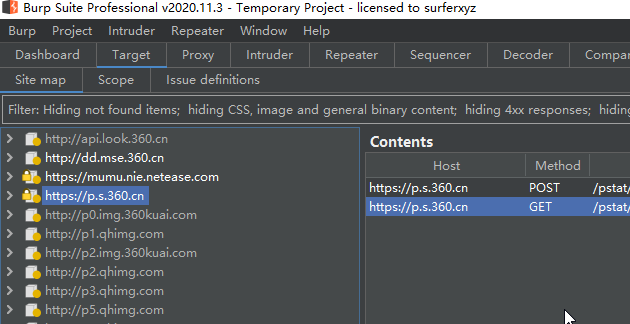




在手机的网络上配置代理为：本地电脑的IP地址。

**B、配置电脑burpsuite代理**





1. **VirtualXposed 和 JustTrustMe 抓包**

简介：和上一种方法原理一样。都是利用的Xposed框架和JustTrustMe模块。只不过可以在非ROOT环境下运行。这是因为VirtualXposed是基于VirtualApp和epic在非ROOT环境下运行Xposed框架的实现。

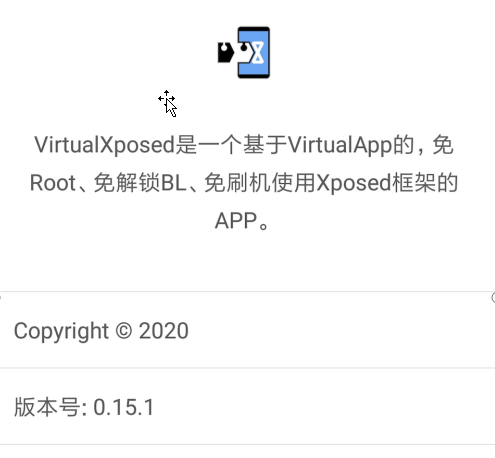
我这里选择安装在红米非ROOT的安卓手机上。

1. **安装VirtualXposed**

VirtualXposed 官网地址：

[https://github.com/android-hacker/VirtualXposed/releases](https://links.jianshu.com/go?to=https://github.com/android-hacker/VirtualXposed/releases" \t "_blank)

我这里下载的是0.15.1版本。

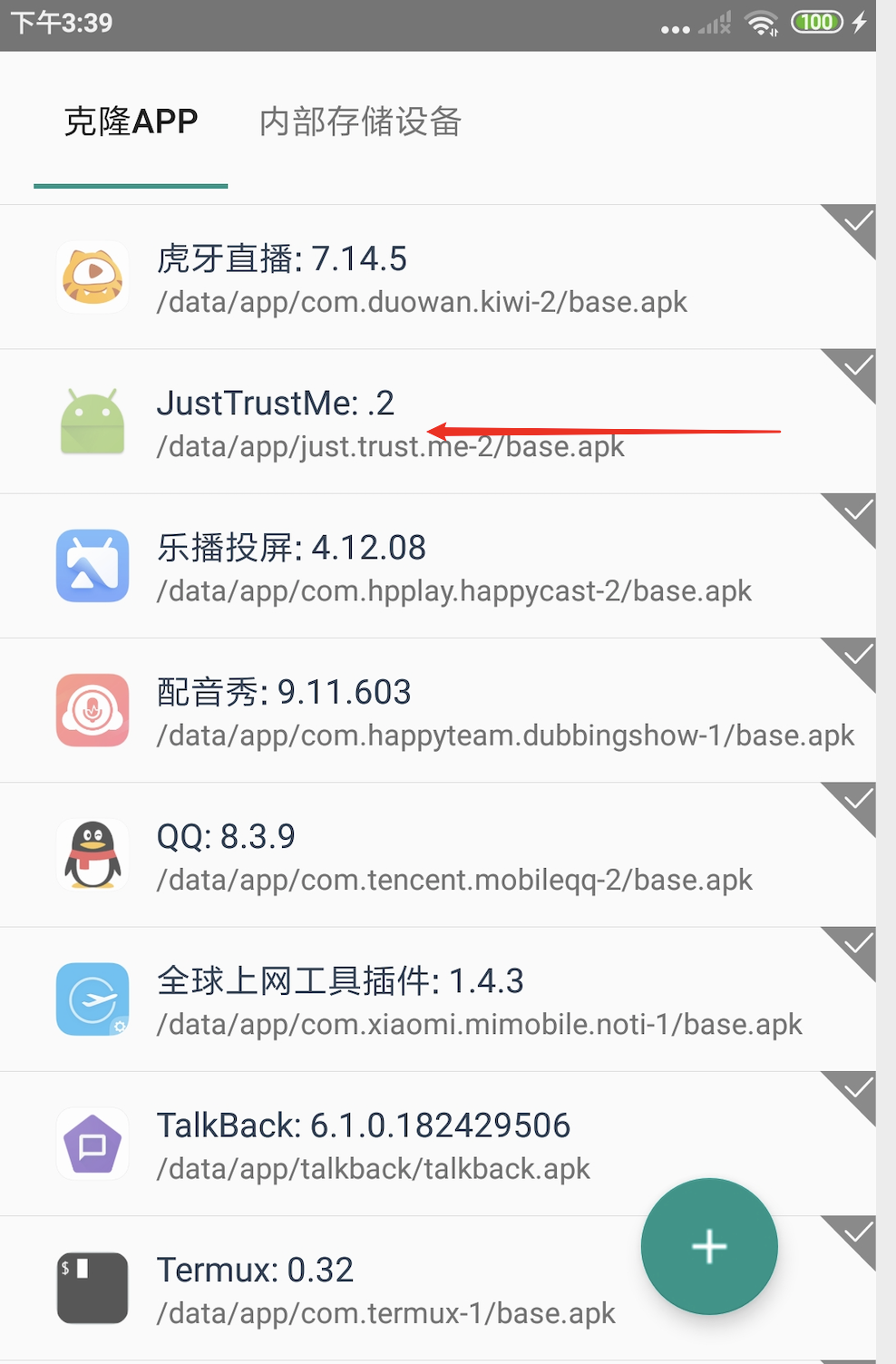


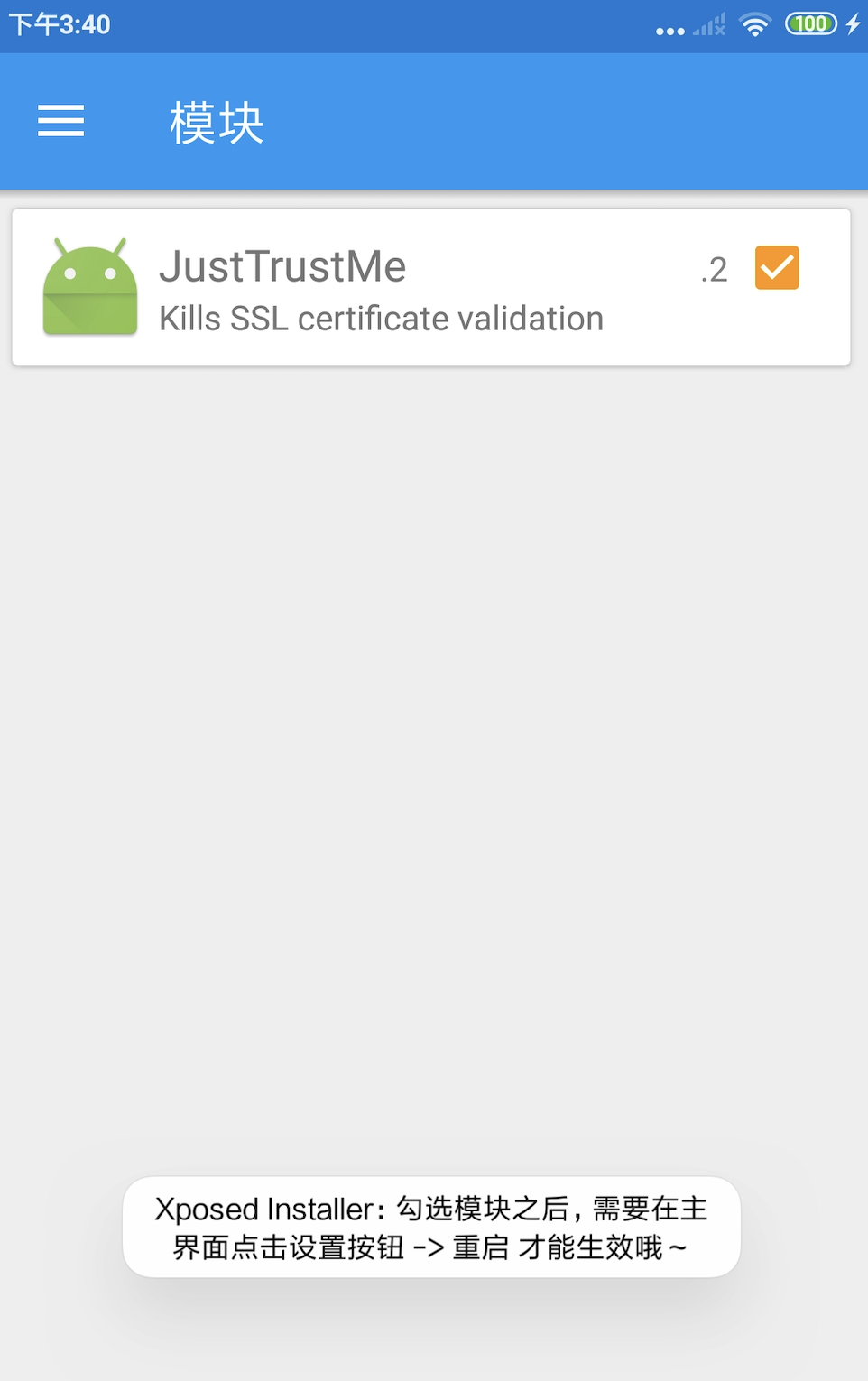
安装完成显示Xposed框架为激活状态。

1. **安装JustTrustMe**

JustTrustMe官网地址：<https://github.com/Fuzion24/JustTrustMe/releases/tag/v.2>

从github下载后，再将JustTrustMe克隆安装在VirtualXposed中，并启用JustTrustMe模块。

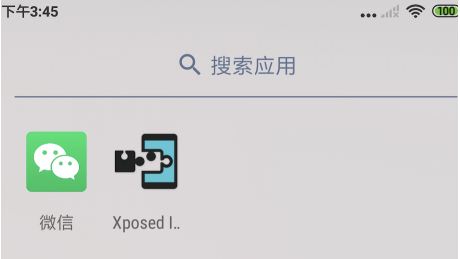




重启设备。

1. **应用克隆到VirtualXposed**

再将需要抓取数据包的app（微信）克隆到VirtualXposed中。



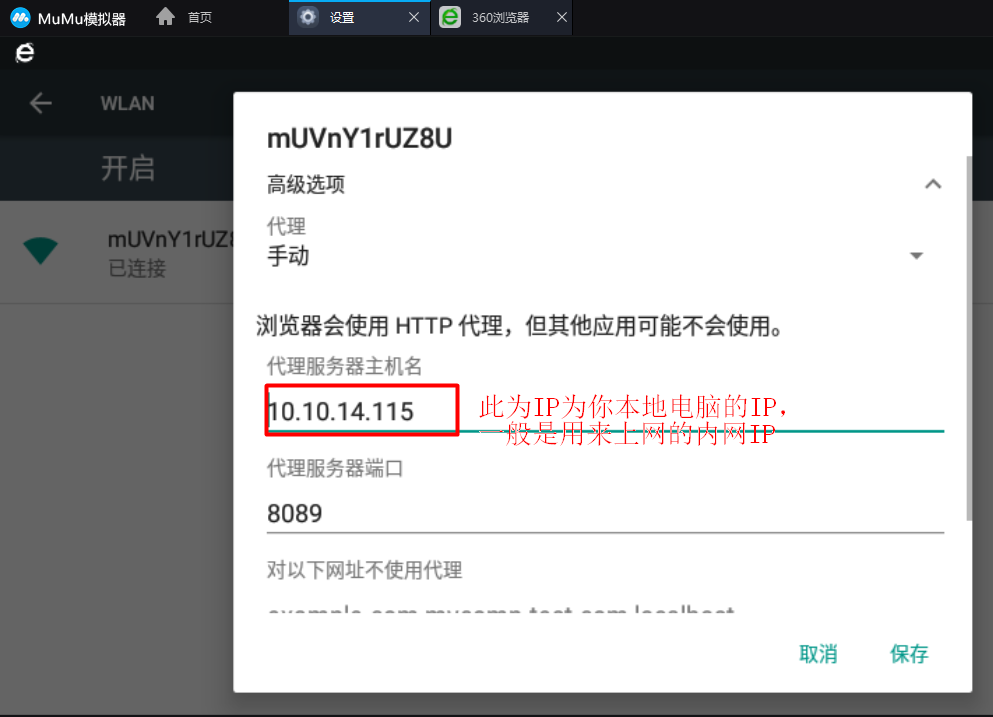
1. **设置网络代理，转发流量**
2. **配置手机网络代理**

此处在手机或者模拟器里面的安装系统上进行配置



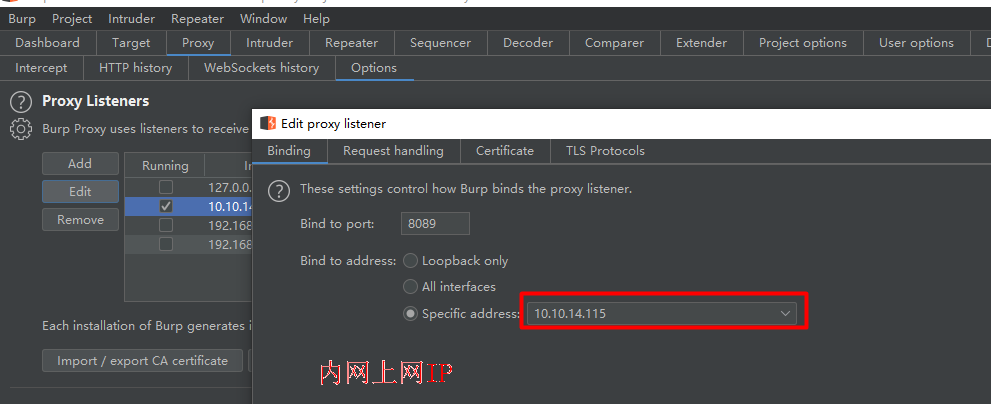


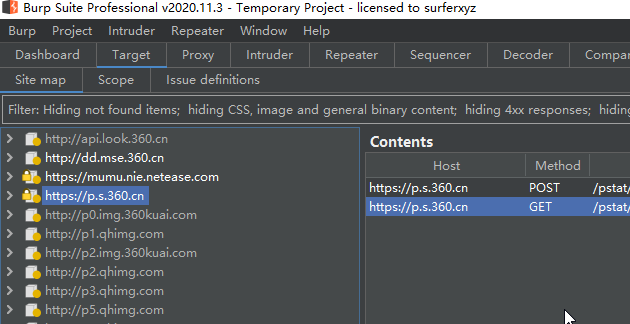




在手机的网络上配置代理为：本地电脑的IP地址。

**B、配置电脑burpsuite代理**





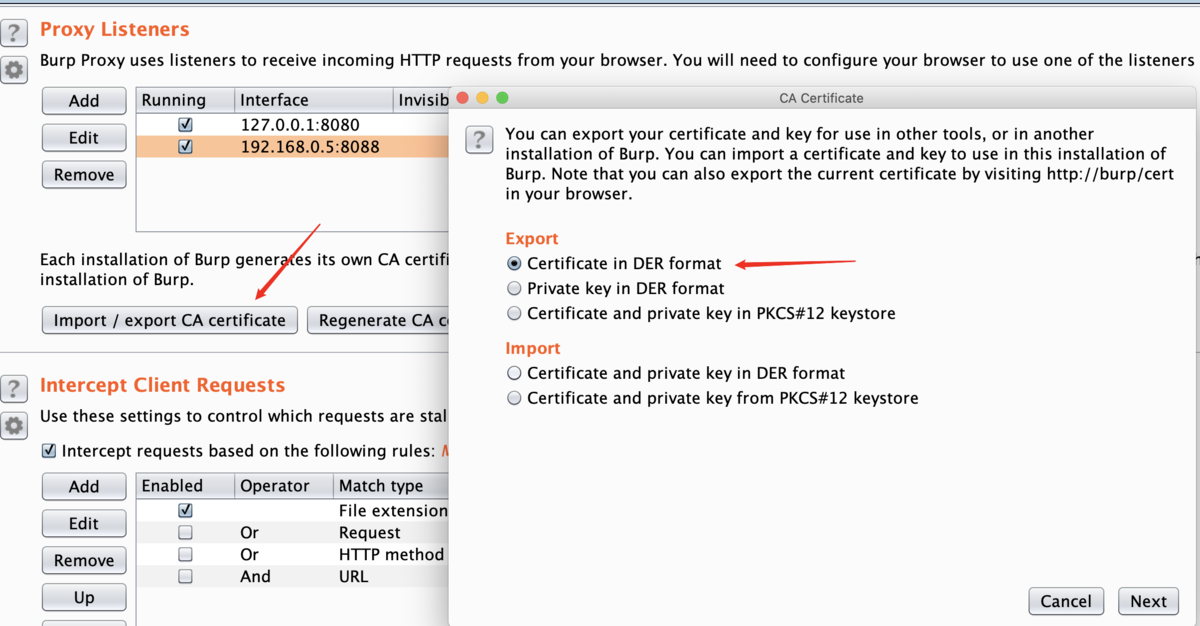
坑点：在VirtualXposed打开微信时，有可能提示"打开应用 com.tencent.mm 失败"。尝试从老版本微信更新有可能解决该问题。

1. **Burp CA抓包**

简介：在一台已经ROOT环境的设备上，如模拟器，把burp CA证书安装在系统可信任证书中，来抓取微信小程序的数据包。条件是微信版本7.0以下。

1. **导出burp CA证书**

先导出burp CA证书，以DER格式导出CA证书，保存为cacert.der。





1. **转为证书格式**

Android用PEM格式的证书，并且文件名为subject\_hash\_old值并以.0结尾，存储在/system/etc/security/cacerts目录下。我们需要使用openssl工具将DER转换成PEM，然后输出subject\_hash\_old并重命名该文件。  
命令为

openssl x509 -inform DER -in cacert.der -out cacert.pem

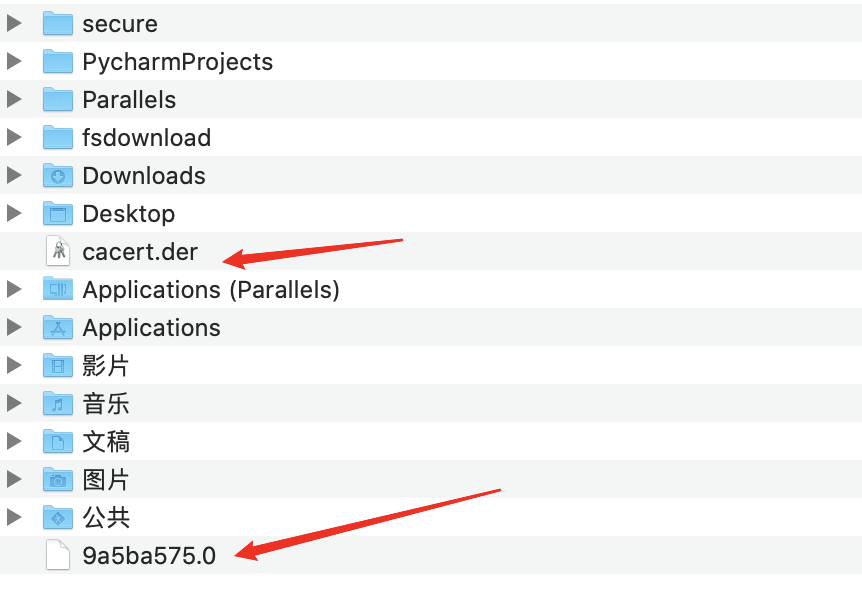
openssl x509 -inform PEM -subject\_hash\_old -in cacert.pem |head -1

mv cacert.pem <hash>.0

在MAC终端上依次运行以上命令。

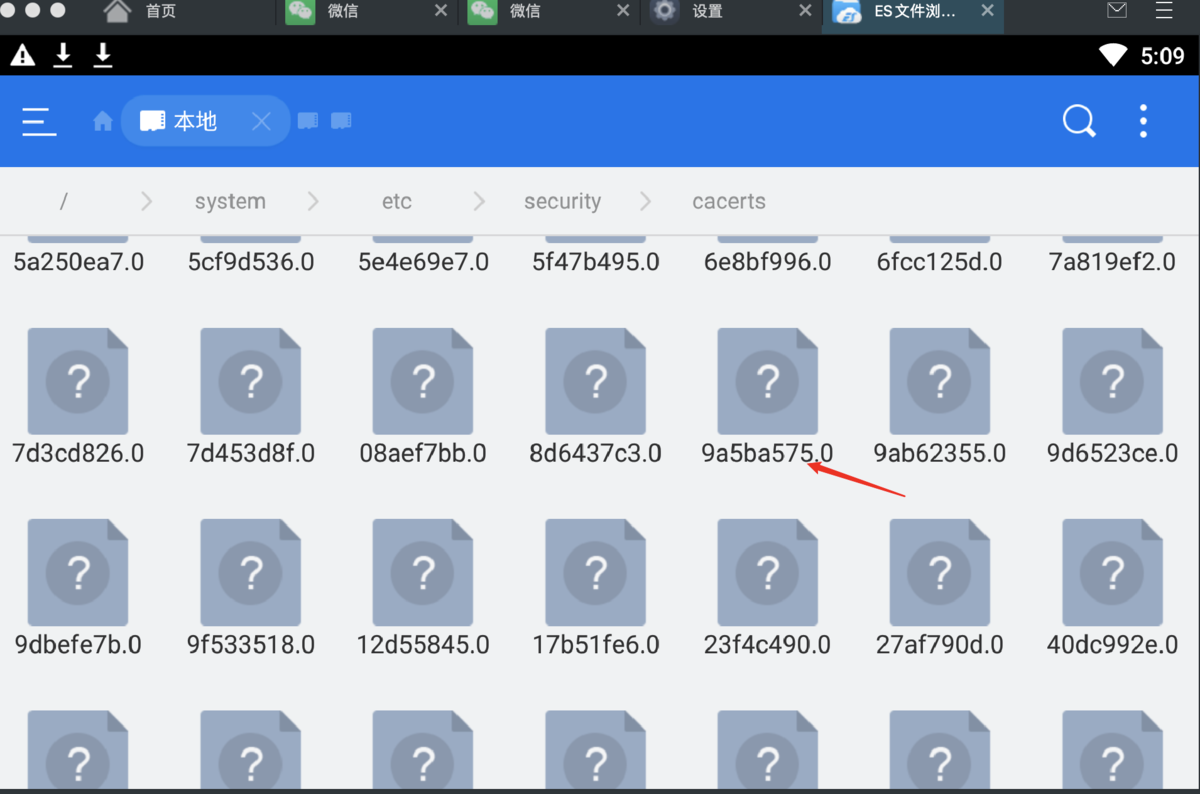


本地就会输出9a5ba575.0文件。



1. **导入证书到模拟器里面**

将该证书文件拷贝到MuMu模拟器的/system/etc/security/cacerts 目录下。



配置网络代理，burp即可抓取微信小程序数据包。



注意：这里测试的是微信 6.6.0版本（从PP助手的历史版本下载来的）。测试微信7.0版本无法抓取HTTPS数据包。

1. **总结**

力所能及，没有太复杂的流程，但这三种方法也并非完全的一劳永逸。

1. **参考资料**

[听说安卓微信 7.0 不能抓 https?](https://links.jianshu.com/go?to=https://testerhome.com/articles/17746" \t "_blank)  
[如何使用Xposed+JustTrustMe来突破SSL Pinning](https://links.jianshu.com/go?to=https://zhuanlan.zhihu.com/p/36538699" \t "_blank)  
[如何在Android Nougat中正确配置Burp Suite？](https://links.jianshu.com/go?to=https://www.freebuf.com/articles/network/160900.html" \t "_blank)