

[登录](#)[注册\[Register\]](#)[网站](#)[新帖](#)[搜索](#)[帮助](#)[快捷导航](#)

请输入搜索内容

搜索

[网站](#)[【软件安全】](#)[『移动安全区』](#)[返回列表](#)[1](#)[2](#)[4](#)[1 / 4 页](#)

[Android 分享] Xposed插件绕过应用证书锁定和动态分析共具分享 [复制链接]

森林雪人 2019-1-15 22:24

[楼主](#) [电梯直达](#)

本帖最后由 森林雪人 于 2019-1-15 23:10 编辑

一、背景：

在使用burpsuite做代{过}{滤}理抓取应用数据包时，如果要抓取到HTTPS数据，需要将burpsuite证书导入到浏览器或手机。

浏览器或手机设置好burpsuite的代{过}{滤}理地址，即可抓取到https数据包。

Line	URL	Method	Path	Response
281	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
282	http://183.232.95.150:8080	POST	?tk=17ccf1bdd0d5081c16c3b436...	✓
283	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
284	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
285	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
286	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
287	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	
288	https://www.baidu.com	GET	/his?wd=&from=pc_web&rf=3&his...	✓
289	https://ss1.bdstatic.com	GET	/5eN1bjq8AAUYm2zgoY3K/r/www/...	

Request Response

Raw Headers Hex

HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 95
Content-Type: baiduApp/json; v6.27.2.14; charset=UTF-8
Date: Tue, 15 Jan 2019 13:08:48 GMT
Expires: Tue, 15 Jan 2019 14:08:48 GMT
Server: suggestion.baidu.zbb.df
Connection: close

jQuery110202569671617820859_1547557733437({"q":"","p":false,"bs":"","csor":"","g":

如果APP应用采用证书锁定后，将无法抓取到https数据，因为此时APP应用校证书不通过，通常APP应用会断开网络连接，防止网络传输数据被抓取。

二、证书锁定

证书锁定（CertificatePinning或SSL Pinning），即HTTPS的证书校验。HTTPS库在接收到证书以后，对证书进行校验，确保其跟自己保存的本地证书或硬编码数据相同，

才可放行。否则视为被中间人监听，拒绝通信。

三、绕过证书锁定

绕过证书锁定，可使用xposed框架下的两大神器来突破证书锁定。SSLUnpinning或Inspeckage。

使用这两个APP应用中的任意一个就可以绕过证书锁定。

要使用这两个APP应用生效，前提是手机已ROOT并且安装好xposed框架，在选择xposed安装时，要选择好手机架构系统版本和CPU对应关系。

安装方式参与下面链接

<https://xposed.appkg.com/2390.html>

<https://xposed.appkg.com/1152.html>

android的版本可以在设置-关于手机查找，CPU是否是64位可查询手机配置参数，也可以使用以下命令查看：arm64-v8a

比如我的荣耀9是android7.0，命令查询结果如下：

```
HWSTF:/ # getprop ro.product.cpu.abi
```

```
arm64-v8a
```

所以选择安装包xposed-v88-sdk24-arm64.zip，具体安装方法可百度搜索：[xposed框架安装](#)。

成功安装xposed后可以安装以下任意一个APP应用，可实现绕过证书锁定。

1、SSLUnpinning

SSLUnpinning安装成功后，需要在xposed框架中选中，并重启手机后才会生效。

手机重启后，打开SSLUnpinning，选择要抓数据包的APP应用，当应用后出现unpinned时，就可以愉快地进行抓包了。

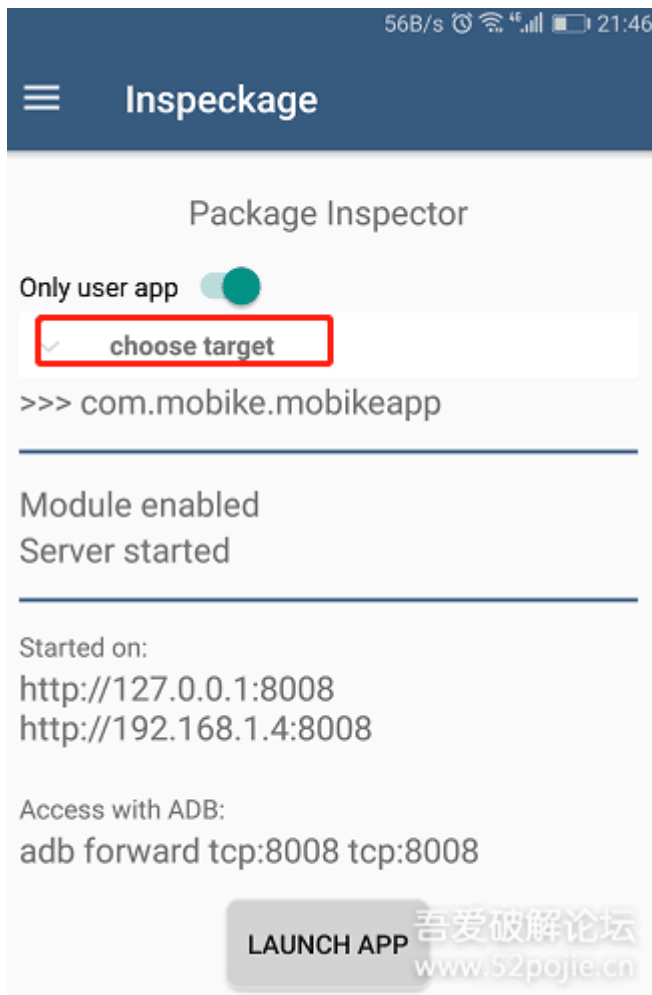


如果需要取消，点击右上角的三个小点，选择clear即可。

2、Inspeckage

Inspeckage是一个用于提供Android应用程序动态分析的工具。通过对Android API的函数使用hook技术,帮助用户了解应用程序在运行时的行为。

2.1 打开Inspeckage点击choose target选择要分析的应用，这次以com.mobike.mobikeapp为例。



2.2 电脑使用adb命令 连接手机，并做端口转发：

```
E:\ProgramFiles\adb>adb devices
```

```
List of devices attached adb server version(31)
doesn't match this client (36); killing...
```

```
* daemon started successfully * emulator-5554 device //连接成功
```

```
E:\ProgramFiles\adb>adb forward tcp:8008 tcp:8008 //本地8008端口转发到手机
8008端口，用于浏览器中直接访问http://127.0.0.1:8008
```

2.3 浏览器中直接访问http://127.0.0.1:8008，效果如下

摩拜单车 7.2.0

UID: 10267 | Debuggable: false
GIDs: 3002-3003-3001
Allow Backup: false

Package: com.mobike.mobikeapp
Data dir: /data/user/0/com.mobike.mobikeapp

Package Information | Shared Preferences | Serialization | Crypto | Hash | SQLite | HTTP | File System | Misc. | WebView | IPC | + Hooks

Exported Activities

- com.mobike.mobikeapp.wxapi.WXEntryActivity
- com.mobike.mobikeapp.WBSHareActivity
- com.umeng.qq.tencent.AuthActivity
- com.mobike.mobikeapp.SplashActivity
- com.mobike.mobikeapp.ui.maintab.MainTabActivity
- com.mobike.mobikeapp.activity.login.LoginActivity
- com.mobike.mobikeapp.activity.login.RegisterFreeTryOutActivity
- com.mobike.mobikeapp.activity.pay.PayWebViewActivity
- com.mobike.mobikeapp.web.WebViewActivity
- com.mobike.mobikeapp.activity.pay.PayActivity
- com.mobike.mobikeapp.wxapi.WXPayEntryActivity
- com.mobike.mobikeapp.activity.riding.MyTripsWebActivity
- com.mobike.mobikeapp.activity.usercenter.MyMessagesActivity
- com.mobike.mobikeapp.activity.usercenter.InviteFriendActivity
- com.mobike.mobikeapp.web.BuyMonthPassWebActivity
- com.mobike.mobikeapp.activity.pay.RechargeHistoryWebViewActivity
- com.mobike.mobikeapp.activity.usercenter.UserDetailActivity
- com.mobike.mobikeapp.activity.customer.ReportRideUnfinishActivity
- com.mobike.mobikeapp.activity.customer.ReportViolationsActivity
- com.mobike.mobikeapp.activity.customer.ReportLockFailActivity

Requested Permissions

- android.permission.NFC
- android.permission.REQUEST_INSTALL_PACKAGES
- android.permission.ACCESS_NETWORK_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.READ_PHONE_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.INTERNET
- android.permission.READ_LOGS
- android.permission.CALL_PHONE
- android.permission.ACCESS_FINE_LOCATION
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.GET_TASKS
- android.permission.CAMERA
- android.permission.VIBRATE
- android.permission.FLASHLIGHT
- android.permission.MODIFY_AUDIO_SETTINGS
- android.permission.BLUETOOTH
- android.permission.BLUETOOTH_ADMIN
- android.permission.CHANGE_WIFI_STATE

点击下图中设置，开启SSL uncheck就可以绕过APP应用的证书锁定。

Settings

OFF Disable

FLAG_SECURE

ON SSL uncheck

Restart App | Finish App

Start App

192.168.1.3

4443

OFF Add Proxy

192.168.1.1

01:23:45:67:89:ab

Set ARP Entry

Disable/Enable

ON Shared Preferences

ON File System

ON Serialization

ON Misc.

ON Crypto

ON WebView

ON Hash

ON IPC

ON SQLite

ON + Hooks

ON HTTP

上图中右侧还有个代理设置。使用方式是手机中不设置代理，在此处设置了burpsuite的代理，即可在burpsuite中抓到数据包。这个方式可绕过APP应用的代理检测。

四、Inspeckage动态分析工具

模块介绍

Logcat	实时查看该app的
logcat输出	
Tree View	可以实时浏览app的数据目录并
直接下载文件到本地	
Package Information	应用基本信息（组件信息、权限信息、共享库信息）
Shared Preferences	LOG: app XML文件读写记录; Files: 具体XML写入内容
Serialization	反序列化记录
Crypto	常见加解密记录
（KEY、IV值）	
Hash	常见的哈希算法记录
SQLite	SQLite数据库操作记录
HTTP	HTTP网络请求记录
File System	文件读写记录
Misc.	调用
Clipboard, URL.Parse() 记录	
WebView	调用webview内容
IPC	进程之间通信
记录	
+Hooks	运行过程中用户自定义
Hook记录	



大部分APP应用使用https加密通道保护传输数据，同时对重要的数据会再次加密防止被截取泄露，使用Inspeckage分析通常可看到相应的明文、密钥以及加密方式。

一个非常好的安卓APP动态分析工具，使用方法见下载地址有详细介绍。下载地址：

<https://repo.xposed.info/module/mobi.acpm.sslunpinning>

<https://repo.xposed.info/module/mobi.acpm.inspeckage>

免费评分

	吾爱币	热心值	理由	收起
 windtrace	+ 1	+ 1	谢谢@Thanks!	
 15616357625		+ 1	好厉害的样子	