# APP渗透 | 安卓模拟器7.0以上的抓包方法

原创Cacker HACK学习呀
2020-12-31原文

**抓包前准备：**
模拟器:雷电模拟器4.0 Android7.1内核版本
Proxifier、代理抓包工具(burpsuite、Fiddler)均可

通常情况下需要在模拟器中修改wifi代理其实我觉得这种是比较麻烦的、何必不只要我运行了burpsuite和Proxifier之后就可以抓模拟器包，不需要修改其内部配置呢。并且某些app也会检测代理情况，如果修改了或开启了代理app就无法正常运行，我们通过在模拟器外部进行抓包来绕过app检测。

**开始配置：**
首先运行burpsuite监听默认8080端口
Proxifier第一步
打开Proxifier添加代理服务器


地址127.0.0.1 端口8080 协议https


开始测试通过即可（在进行这一步之前你要确保你的电脑已经安装了burpsuite的证书并且可以正常抓取https的包）

**Proxifier第二步**

添加代理规则


应用程序选择 dnplayer.exe;LdVBoxHeadless.exe;

dnplayer雷电模拟器启动程序和模拟器主程序

LdVBoxHeadless雷电模拟器对外网络协议走的都是这个程序

动作选择刚才添加的代理服务器。


进行到这一步后我们在模拟器中打开浏览器就可以从Proxifier中看到流量情况，但是目前我们只能抓取http的包还不能抓https的包。

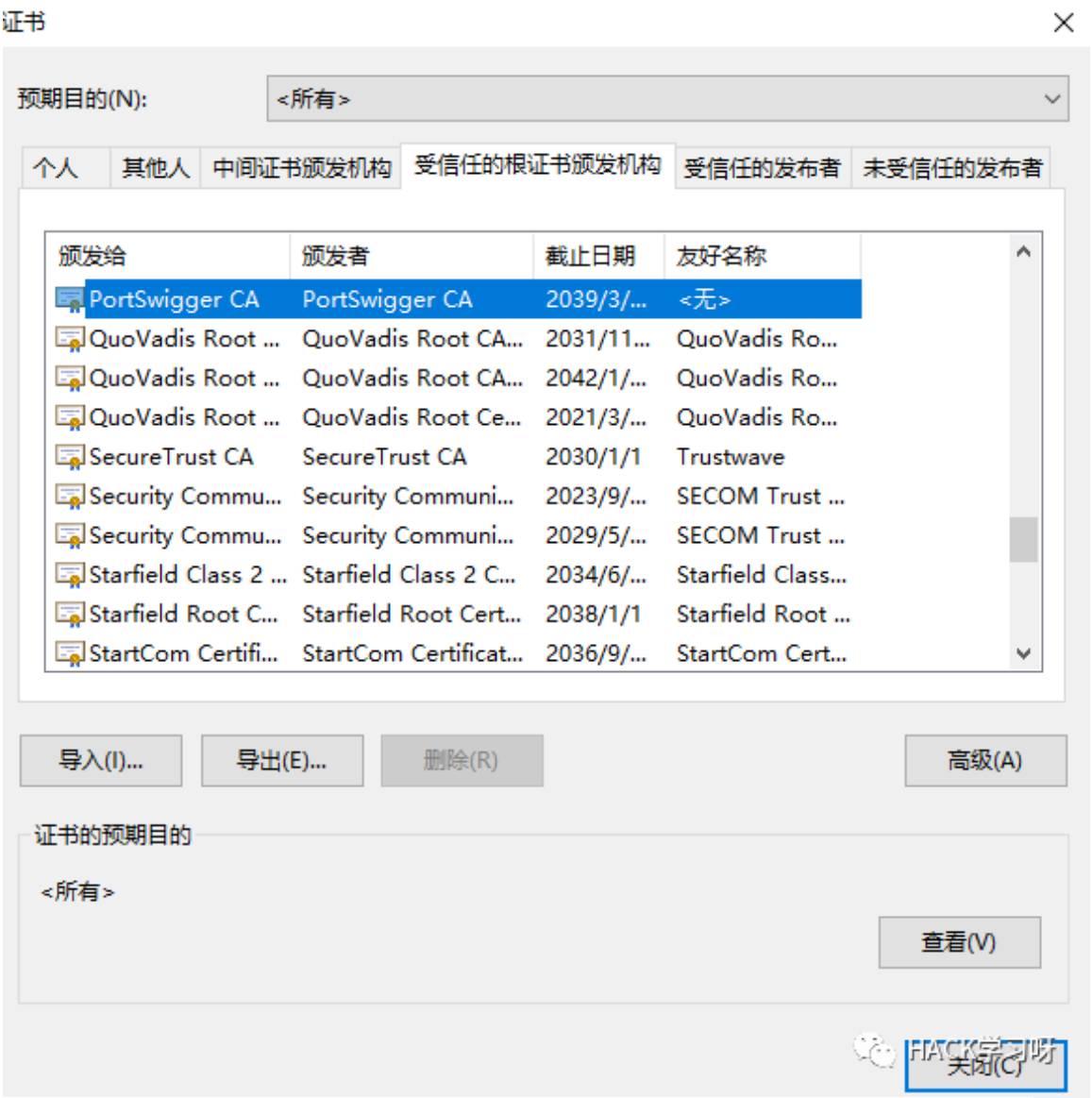

浏览器提示证书问题

**解决抓取https问题：**

不能抓取https的包肯定是没多大意义的。所以我们要来解决这个问题，经过查询资料了解到安卓7.0以上后默认不在信任用户自行安装的证书文件、如果需要抓包我们就要把自己的证书放到系统目录下、或者对app进行修改从而进行抓包。在这里我选择安装系统证书的方式进行更加通用的方式进行处理。

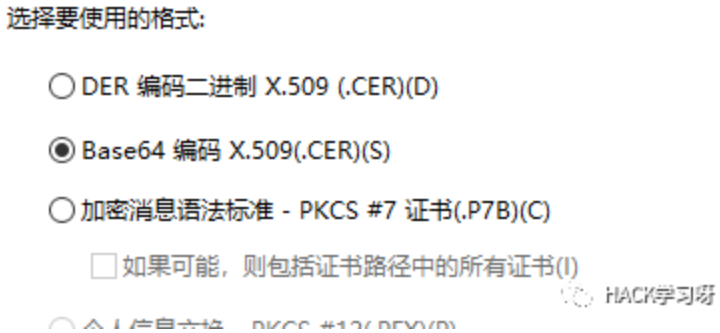
1:从浏览器中导出burpsuite的证书


在谷歌浏览器设置中搜索管理证书-安全下找到管理证书。



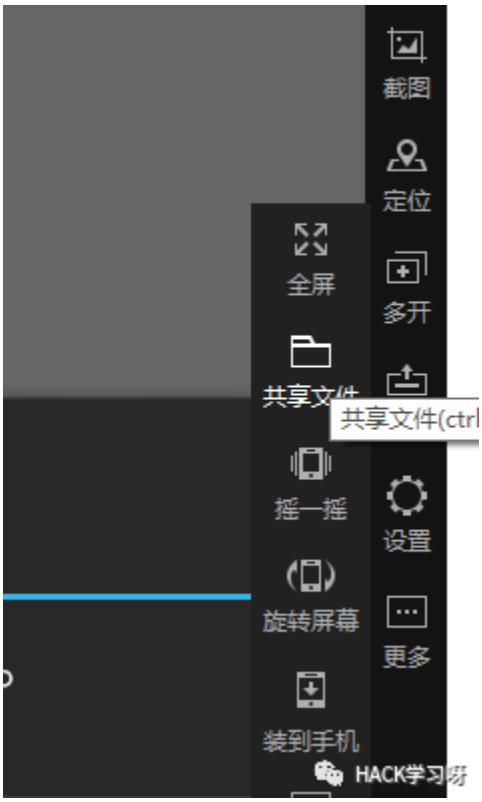

我的证书是安装在受信任的根证书颁发机构然后找到PortSwigger CA

选择导出



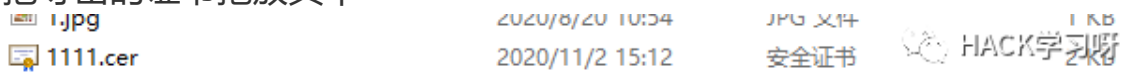

导出格式选择base64编码 cer方式、保存文件名任意xxxx.cer即可

2：导入模拟器




模拟器右边的功能条中选择共享文件、打开电脑文件夹

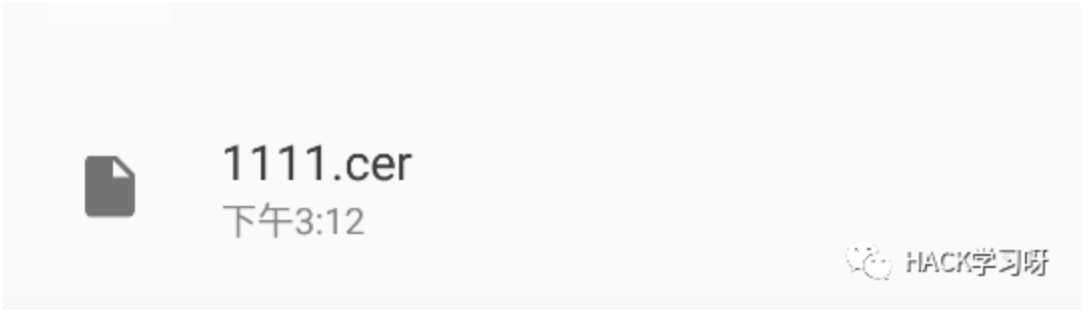
把导出的证书拖放其中



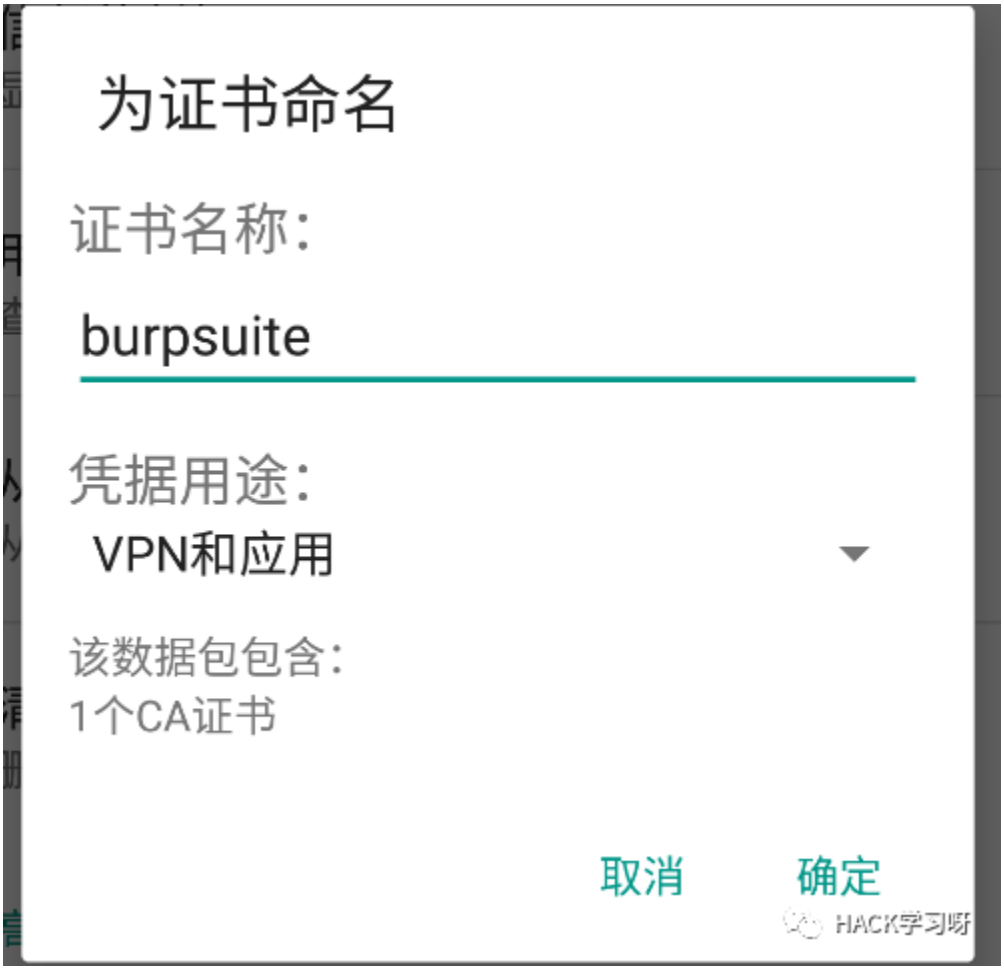

或者直接把文件放到C:\Users\Administrator\Documents\leidian\Pictures目录下即可

3：安装证书

在模拟器中找到设置-安全-从SD卡中安装




找到放入的证书进行安装




安装完毕后在模拟器中下载re文件管理器

进 入 : /data/misc/user/0/cacerts-added

这个文件夹下（该目录存储的是用户自己安装的证书文件）


复制该.0文件（文件名可能是不一样的）

复制到系统证书目录/etc/security/cacerts下（re文件管理器需要挂载读写权限、模拟器中自带root管理授权即可）


/etc/security/cacerts
CACERTS
CACERTS-AD...
542.57MB 已用, 281.19MB 可用, r/o
挂载为可读写
..
上层文件夹
00673b5b.0
02 3月 20 19:09:38 4.66K rw-r--r--
02756ea4.0
02 3月 20 19:09:37 7.03K rw-r--r--
02b73561.0
02 3月 20 19:09:38 4.80K rw-r--r--
03f2b8cf.0
02 3月 20 19:09:38 6.97K rw-r--r--
04f60c28.0
02 3月 20 19:09:38 2.81K rw-r--r--
052e396b.0
02 3月 20 19:09:38 4.72K rw-r--r--
08aef7bb.0
02 3月 20 19:09:36 5.20K rw-r--r--

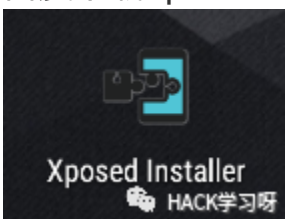

确认后把证书已经放到系统证书目录即可。


重新刷新即可正常抓取https。

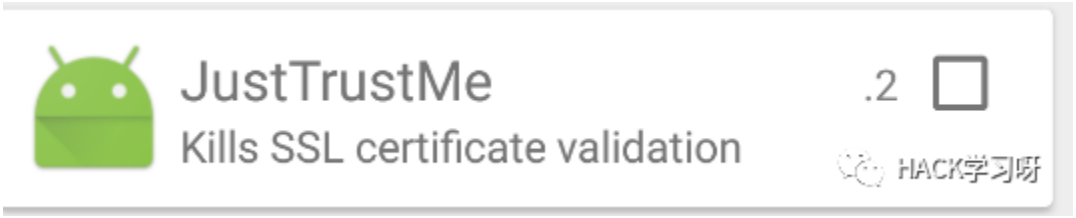
**其他拓展：**

双向认证app，有些app会认证客户端和服务器证书。一般反编译app到其中找到其内置的证书。但是我们可以通过xposed框架对ssl进行hook从而来绕过检测。

百度下载xposed installer




安装

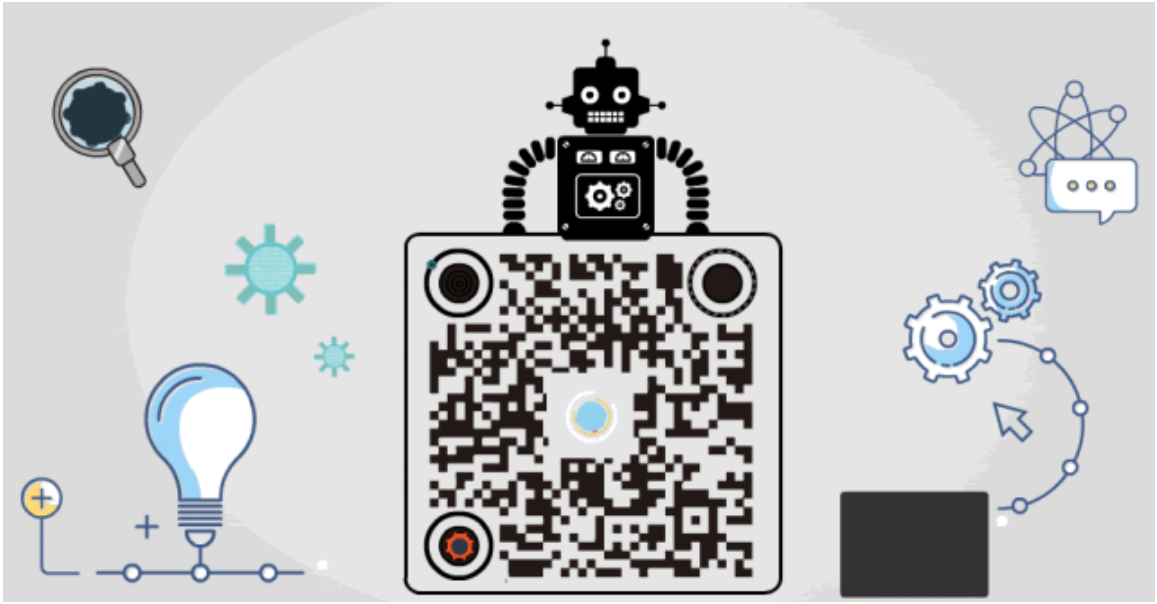



justtrustme模块、有时候启用这个模块就会出问题、我更加推荐SSL Unpinning这个xposed模块，安装完毕后选择有双向认证的app即可愉快的进行抓包调试。

END

**点赞，转发，在看**

投稿作者：cacker



精选留言

用户设置不下载评论