

首页

下载APP

搜索



Aα



登录



Android 7以上版本,绕过CA限制,抓取https



WangLane(关注)

♥ 0.697 2019.05.13 13:50:16 字数 558 阅读 3,028

环境

手机: 小米5A 系统: MIUI 10 电脑: win10

抓包: mitmdump (可替换成其他抓包软件)

电脑需要安装:

- mitmdump (可替换成任意抓包软件)
- adb
- openssl

背景

我需要抓取https请求,苹果手机可以毫无问题的抓取,而安卓就不可以。原因是安卓7之后对证书的策略进行变更,应用不再使用用户证书。

有两种方式绕过:

- 在手机上安装系统证书
- 修改app的manifest文件重新打包

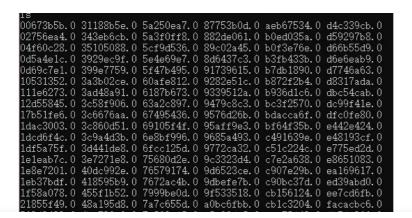
这里我们只讲第一种方法,所以我们需要把证书添加到系统证书中。

为此,我们需要一台已经root的小米手机。root教程在miui论坛中已经非常详细了。官方给出了详细的步骤和工具。

开始

假设到这里你已经有一台root成功的小米手机。

安卓受信任的CA证书以特定的格式存储在 /system/etc/security/cacerts 目录下。我们可以在adb shell中查看到:



写下你的评论...

评论5





WangLane 总资产5 (约0.49元) 关注

Python笔记 | python 合并字典 阅读 6

scrapy | scrapy 和 requests分别对 response进行解码 阅读 26

推荐阅读

这是一份面向Android开发者的复习 指南

阅读 9,299

Python模块-Requests学习与CTF和 AWD实战

阅读 455

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 8,812

公考言语框架

阅读 102

【渗透实例】Fuzz大法好啊

阅读 308

Aa 💝 beta

登录

注

```
1 | adb root
2 | adb remount
3 | adb push 7672ac4b.0 /sdcard/
```

复制到系统目录并修改权限

```
adb shell
su
mount -o rw,remount /system
mw /sdcard/<cert>.0 /system/etc/security/cacerts/
chmod 644 /system/etc/security/cacerts/7672ac4b.0
reboot
```

验证

然后我们在手机中依次进入:设置→安全→信任证书→系统证书



评论5

赞6

写下你的评论...