

Burp 抓手机 App 包

说明：

如果要对手机 App 或者 App 的服务器进行渗透，首先需要抓到 App 发出的 HTTP 请求包。

准备工作：

- 1、可以连上无线网络的电脑，并且安装好 Burp
- 2、手机，本文以华为手机为例，其他品牌手机的网络代理设置可以自行搜索步骤

1、开启电脑 Burp 监听

首先电脑需要连接到 WiFi，不能使用有线网络，这样才能让手机和电脑处于同一网络环境（如果台式机的有线和手机 WiFi 是同一个网络环境也可以）。

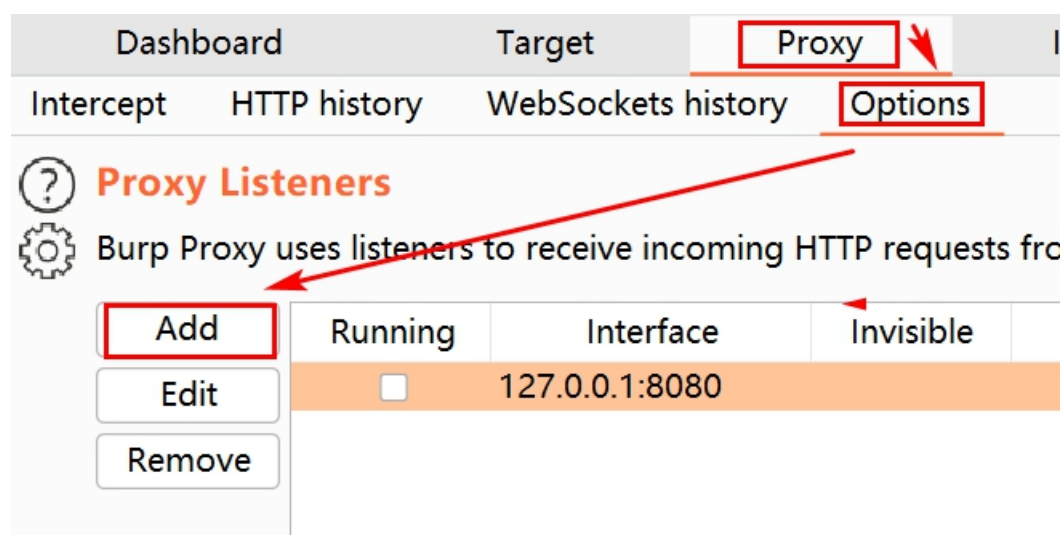
电脑打开 cmd，输入 `ipconfig -all`，查看 WLAN 的 IPv4 地址：

```

无线局域网适配器 WLAN:
    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    物理地址. . . . . : 68-3E-26-B4-D6-F1
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::b856:3c2d:c9b1:9a8c%10(首选)
    IPv4 地址 . . . . . : 192.168.10.142(首选)
    子网掩码 . . . . . : 255.255.254.0
    获得租约的时间 . . . . . : 2022年3月10日 14:08:48
    租约过期的时间 . . . . . : 2022年3月12日 15:23:03
    默认网关. . . . . : 192.168.10.1
    DHCP 服务器 . . . . . : 192.168.10.1
    DHCPv6 IAID . . . . . : 107494950
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-27-8C-C9-FF-8C-8C-AA-6B-18-E4
    DNS 服务器 . . . . . : 114.114.114.114
    TCP/IP 上的 NetBIOS . . . . . : 已启用
  
```

比如当前 IP 是 192.168.10.142，记住它，等下要用到。

启动 Burp，打开 Proxy——Options——Add



在打开的添加窗口中，端口依然填写 8080，绑定地址选择刚才看到的那个 IP 地址，如图：

⚡ Add a new proxy listener

Binding Request handling Certificate TLS Protocols

ⓘ These settings control how Burp binds the proxy listener.

Bind to port:

Bind to address: ☐ Loopback only
☐ All interfaces
☒ Specific address:

点 OK 确定。

这时候监听器要勾选新建的这个而不是默认的：

Dashboard

Target


Proxy


Intercept

HTTP history

WebSockets history

Options

 Proxy Listeners

 Burp Proxy uses listeners to receive incoming HTTP requests from

Add

Edit

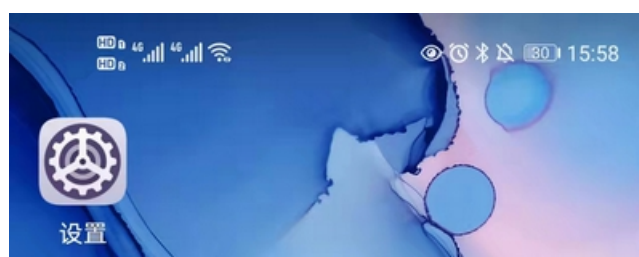
Remove

Running	Interface	Invisible
<input type="checkbox"/>	127.0.0.1:8080	
<input checked="" type="checkbox"/>	192.168.10.142:8080	

2、配置手机 WiFi 代理

首先将手机连接到与电脑相同的 WiFi 中。

从手机的“设置”，进入 WLAN 设置





长按当前连接的 WiFi 名字，点击弹出的“修改网络”。



在打开的窗口中，勾选“显示高级选项”



开启代理：点击代理开关，在弹出的窗口中选择“手动”。



开启代理开关之后，需要配置代理：

4G 4G 4G 16:07

← F [redacted] ee

(未更改) **WiFi密码，不用动**

☒ 显示高级选项

代理 手动 >

该浏览器使用 HTTP 代理，但其他应用可能不会使用

服务器主机名 **填burp监听的IP**
proxy.example.com ←

服务器端口 **填burp监听的端口，默认8080**
8080 ←

对以下对象绕过代理：
这里不用填
example.com, localho:

IP DHCP >

改完了保存一下

取消 保存

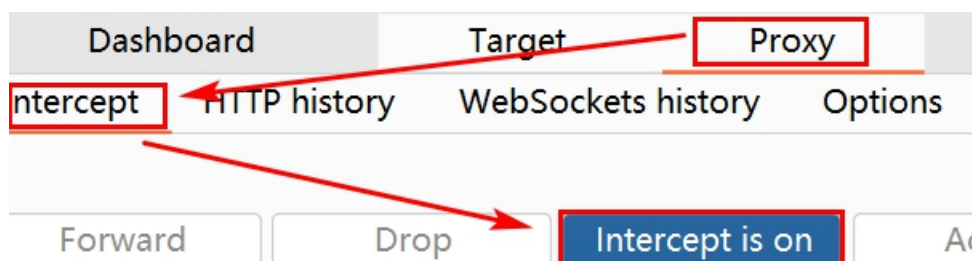
□ ○ ◀

代理已经配置完了。接下来手机上所有的网络请求都会发送到 Burp 上。

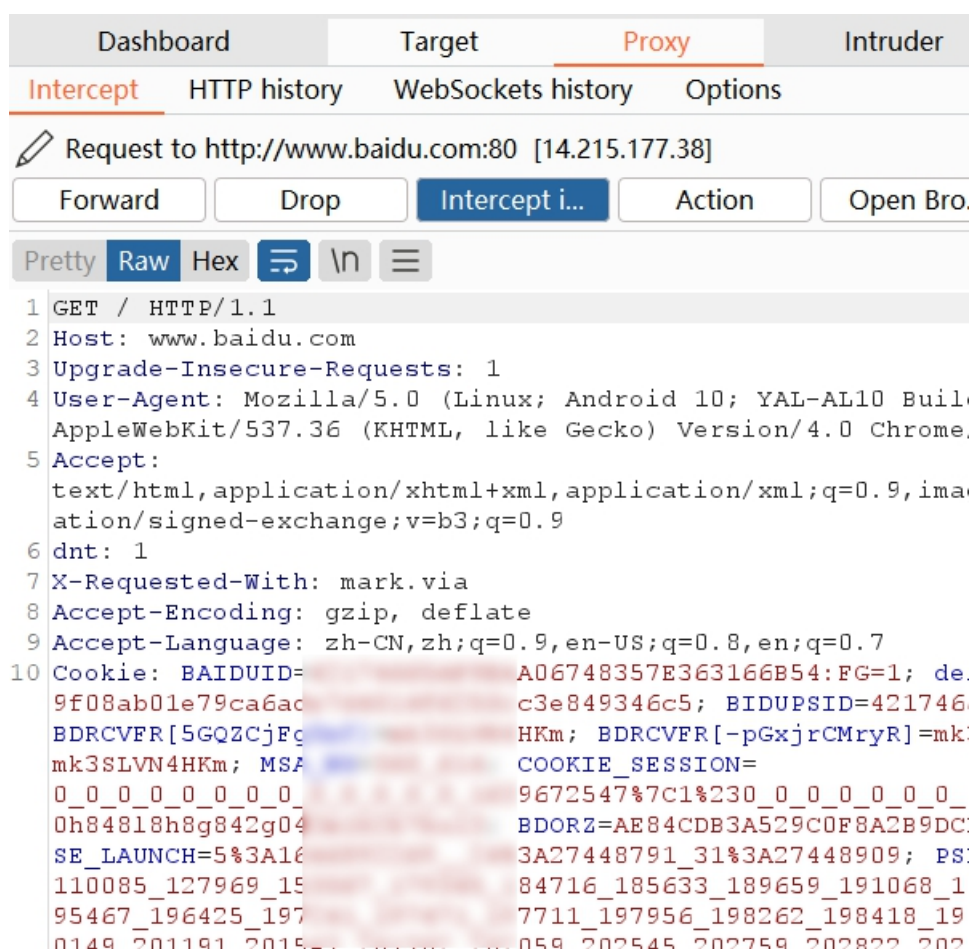
需要注意：并不是你在操作 App 的时候才会有网络请求。手机上的 App 无时无刻都在访问网络，所以会抓到很多无关的包。

建议在手动操作之前才打开 Burp 的拦截开关，这样可以准确地抓到包。

在 Proxy——Intercept 打开拦截开关：



比如：手机浏览器打开百度搜索，通信包被电脑上的 Burp 抓到：



至此，抓包的设置就完毕了。

3、手机安装证书

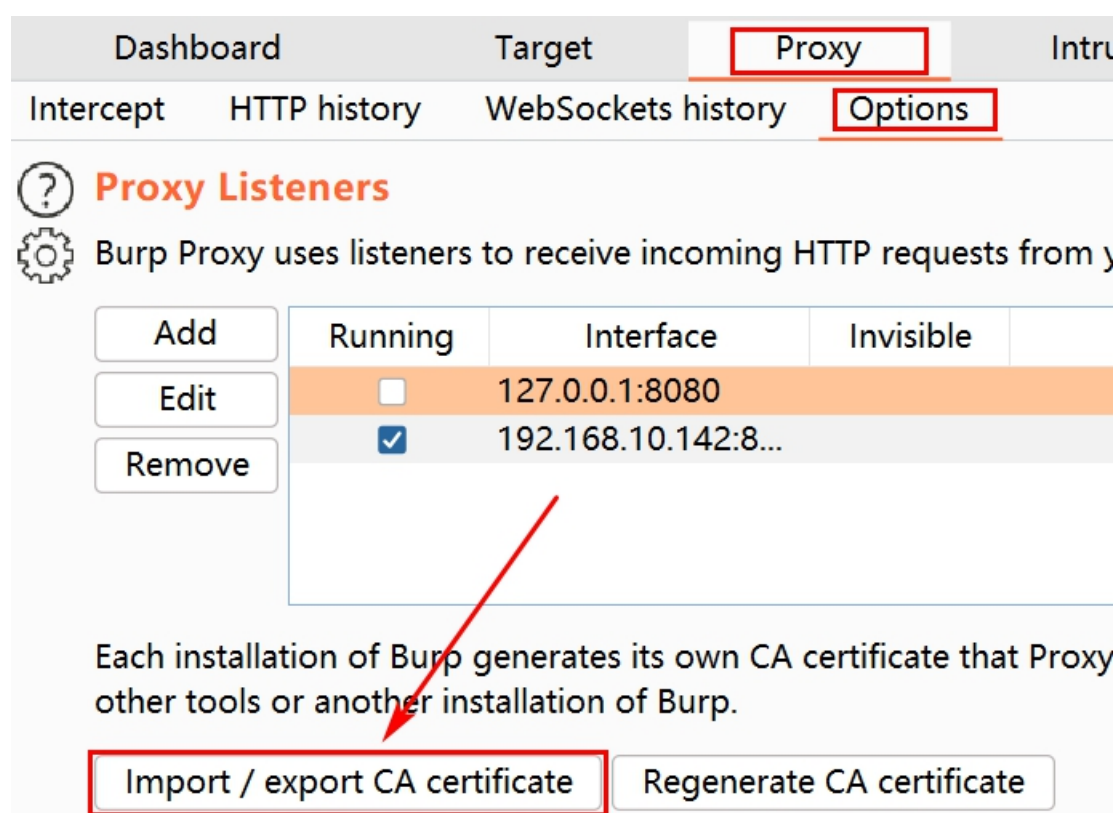
对于 HTTPS 的网站，客户端需要用服务器的密钥加密消息以后发出。

当配置了代理，客户端（浏览器）向 burp 请求证书，但是 burp 没有证书，浏览器就会提示不安全。或者，使用了服务器的证书加密，burp 抓到的是加密以后的消息，是无法查看和修改的。

所以完整的流程是这样的：

客户端先用 burp 的密钥加密消息。burp 解密称明文以后，再用服务器的密钥加密消息。

所以这里要在手机上安装 burp 的证书。



选择第一个，DER 格式证书，点 Next

⚡ CA Certificate

❓ You can export your certificate and key for use in other t of Burp. You can import a certificate and key to use in th you can also export the current certificate by visiting http browser.

Export

☒ Certificate in DER format

☐ Private key in DER format

☐ Certificate and private key in PKCS#12 keystore

Import

☐ Certificate and private key in DER format

☐ Certificate and private key from PKCS#12 keystore

选择保存的 CA 路径（比如 D 盘），文件后缀命名为.cer，非常重要，因为手机只能安装.cer 的证书类型，默认的 der 格式是不能被识别安装的。点击保存，然后 Next

⚡

Save In: 工作 (D:)

00软件	Drivers
01工作资料	LenovoQMDownload
02技术资料	LenovoSoftstore
360data	Program Files
appuse	Program Files (x86)

File Name: ca.cer

Files of Type: 所有文件

导出完毕，关闭窗口：

⚡ CA Certificate

② The certificate was successfully exported.

把文件发送到手机，比如用微信的“文件传输助手”。在手机上“用其他应用打开”。



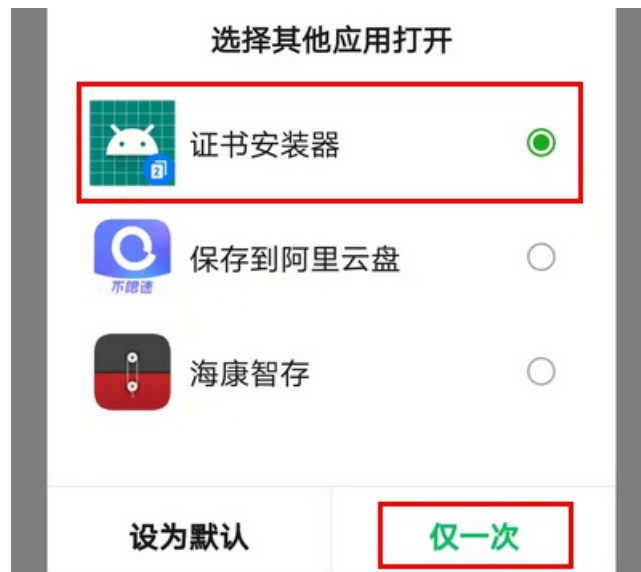
ca.cer

文件大小: 0.9KB

用其他应用打开

🔗 更多打开方式

选择“证书安装器”打开，仅一次



写入证书名称，选择 WLAN，确定，安装成功。



在设置里面搜索“证书”，用户凭据，查看证书：



可以看到已经安装的证书：



4、取消 burp 抓包

如果不需要抓手机的包了，需要正常访问，取消代理即可。

长按 WiFi 名字进入设置——显示高级选项——代理，设置为“无”，保存，即可



此外，也可以在电脑上安装 Android 模拟器，这样可以直接在电脑上抓模拟器的包，大家可以自己尝试。

马士兵教育 运维安全学院 无涯老师

最后修改时间：2022 年 3 月 11 日 21:43:31