

IOS之Burpsuite抓Https问题

 jianshu.com/p/4650ce217038



流弊的小白 关注

2017.12.15 12:29* 字数 645 阅读 1316 喜欢 0

IOS之Burpsuite抓Https问题

最近在测试IOS遇到小坑，之前一般配置代理导入证书就可以信任证书就OK但是最近碰到坑了搞定了分享给大家，顺便写个小笔记给朋友。

所以写出来分享下。文章比较详细，大佬就绕过。总结为IOS版本

下载对应证书-安装描述文件

设置--通用--查看描述文件(自己查看验证而已)

设置---通用---关于本机---信任证书设置(拉倒最底下)---开启信任。

1 要求

- 有很多方法，自己电脑开热点或者在同一WIFI情况下。此文章采用公司WIFI。
- 1.手机和WIFI必须可以同一WIFI。
- 2.你要有台电脑
- 3.你要有台IPhone(肾机)

2 开始搞事情

2.1 配置端口

配置代理IP和端口，采用WIFI，电脑和手机在同一WIFI。所以用电脑IP做代理，此处不能使用127.0.0.1（为什么别人我没时间去给你科普基础）

C:\Windows\system32\cmd.exe

```
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接* 1:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::2cf3:2afe:137c:a158%3
IPv4 地址 . . . . . : 192.168.64.170
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.64.254
```

image.png

BURP会自己列出电脑的IP让你选择。

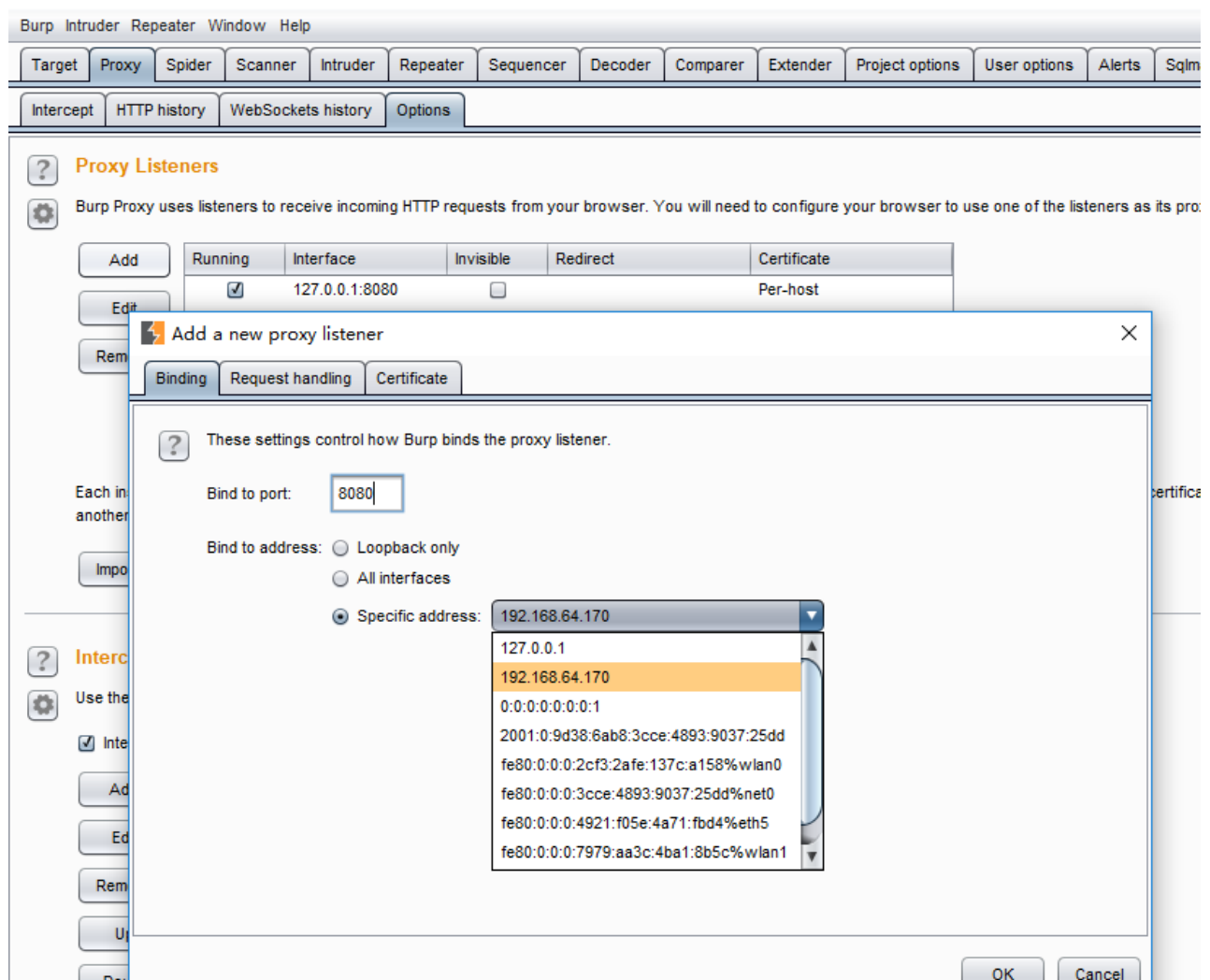


image.png

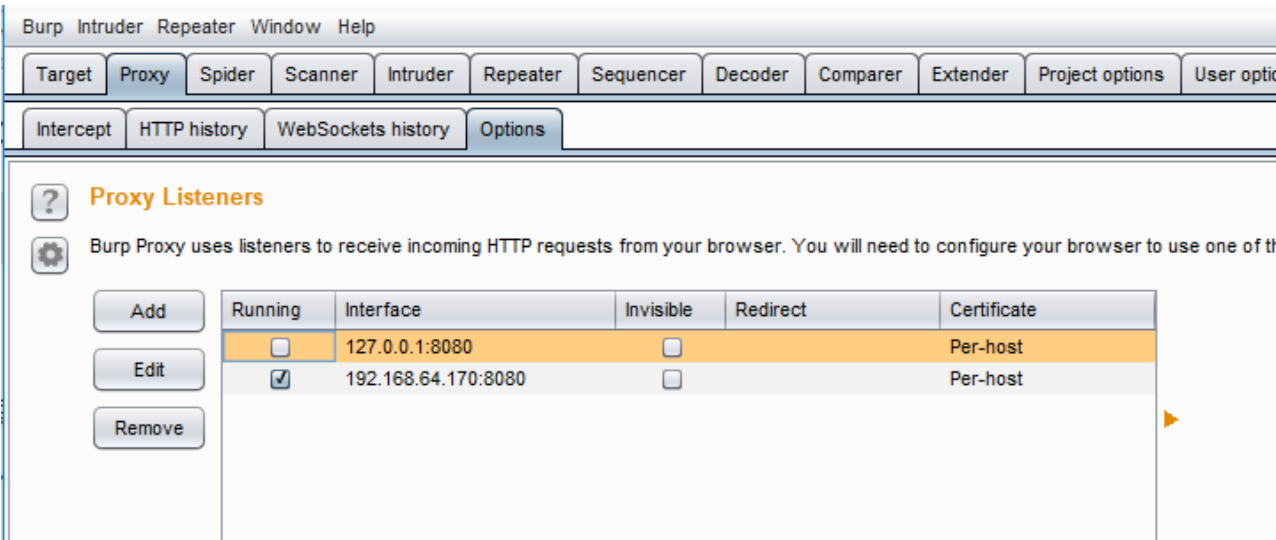


image.png

此处配置成功

代理IP 192.168.64.170端口为8080

2.2验证

- 验证是否成功

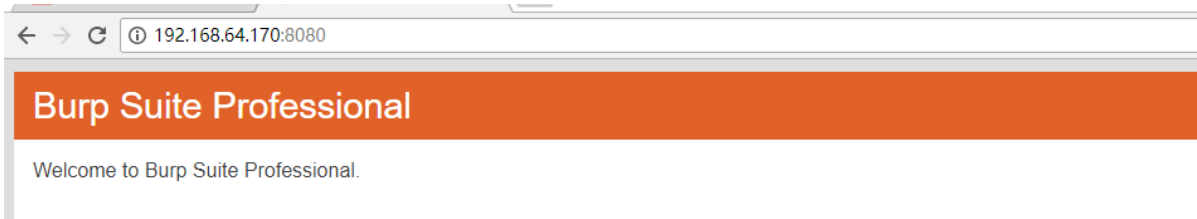
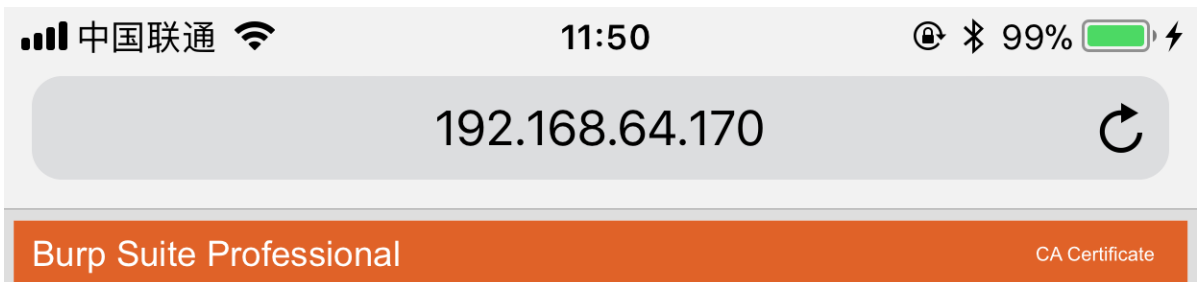


image.png

- 手机链接此WIFI，访问代理没问题。

注意：一定要使用IOS自带浏览器safari浏览器打开！



Welcome to Burp Suite Professional.



fangwen

2.3安装证书

下载对应证书



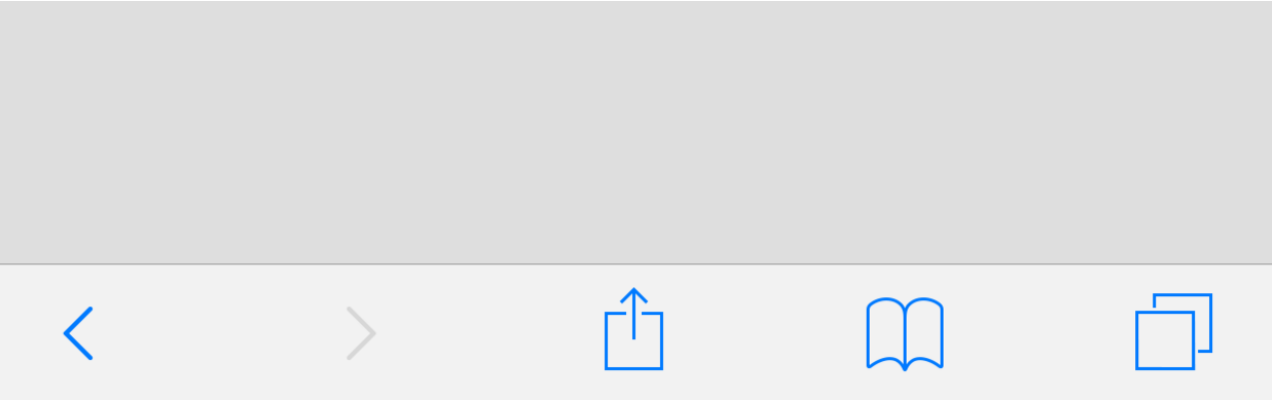


image.png

安装描述文件，



PortSwigger CA

签名者 PortSwigger CA

已验证 ✓

包含 证书

更多详细信息



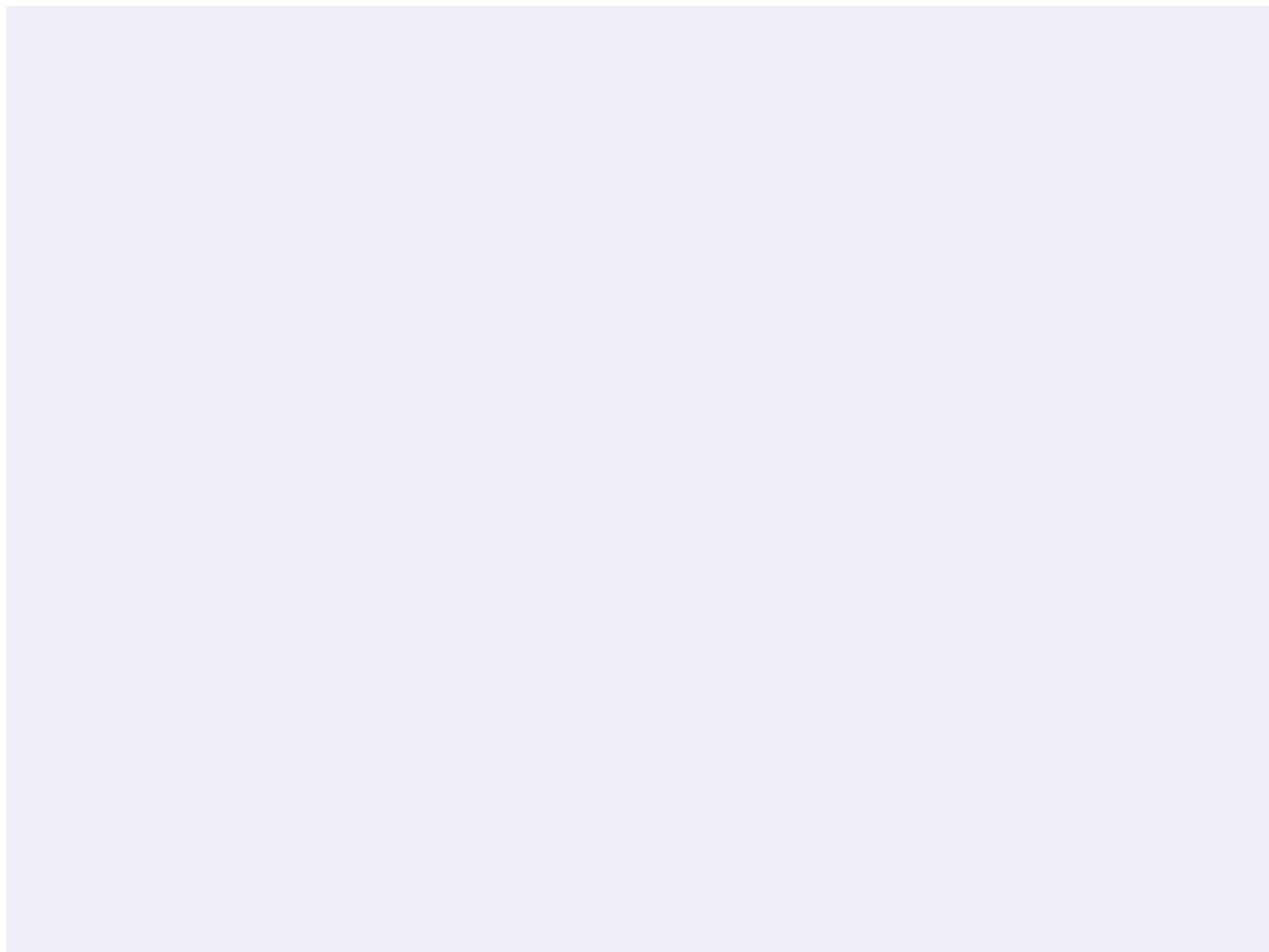


image.png

安装完成变成已安装。



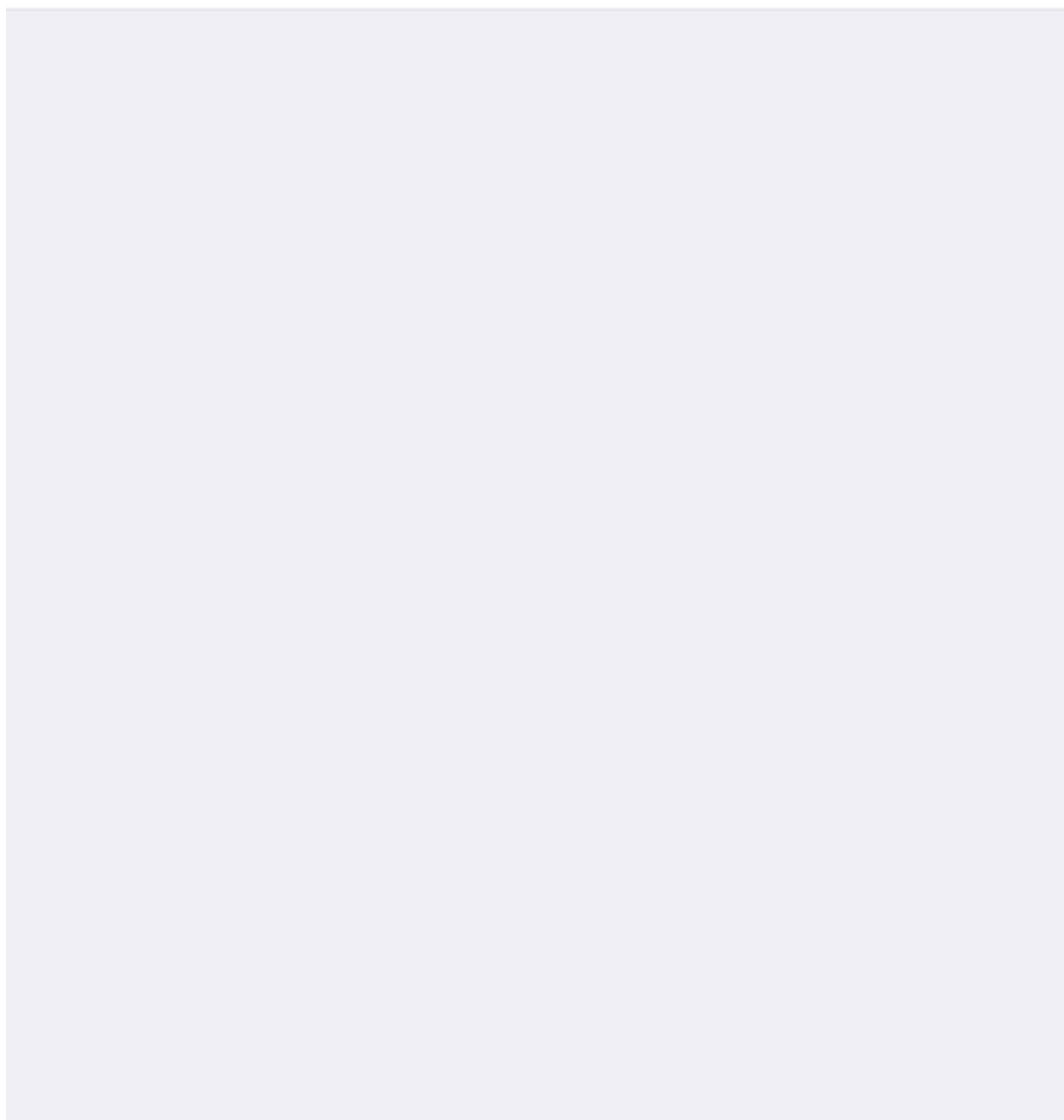
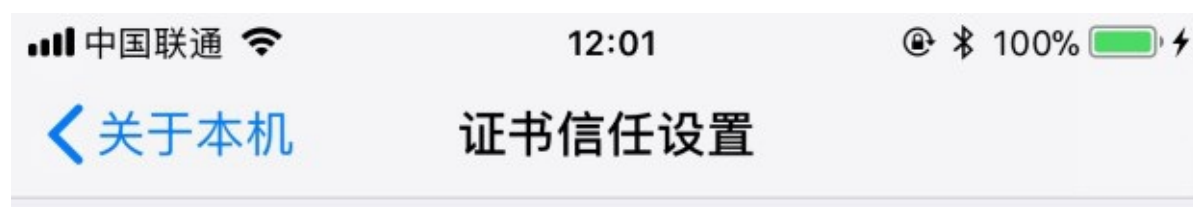


image.png

2.4 信任证书

然后打开手机找到，设置-----通用----关于本机-----信任证书设置(拉倒最底下)---开启信任。



受信任证书存储区版本

2017081600

针对根证书启用完全信任

PortSwigger CA



[进一步了解被信任的证书](#)

如果想删除在
设置-----通用-----描述文件删除即可



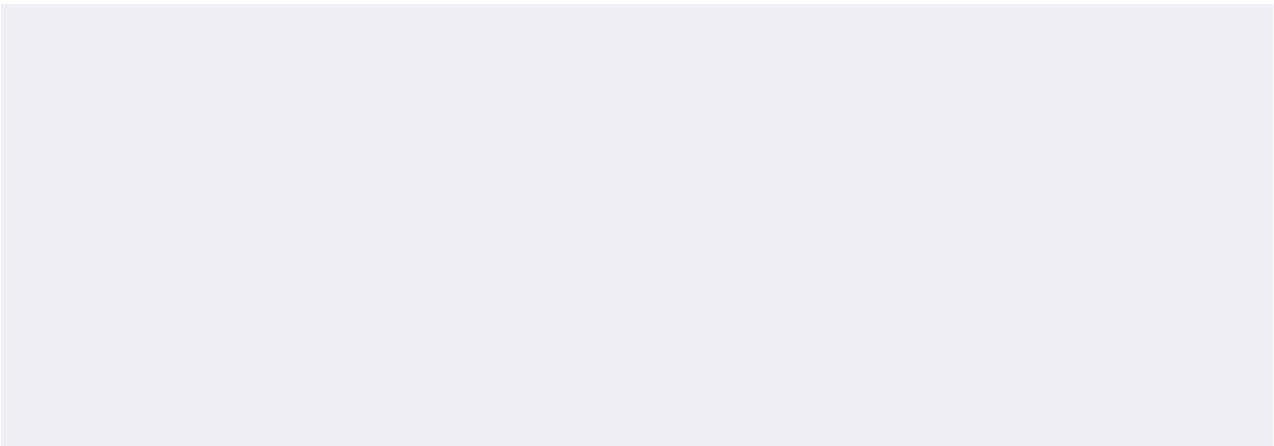


image.png

2.5 配置代理

手机配置代理

中国联通

12:00

100%

< spruce

配置代理

存储

关闭

手动

自动

服务器

192.168.64.170

端口

8080

鉴定

☐

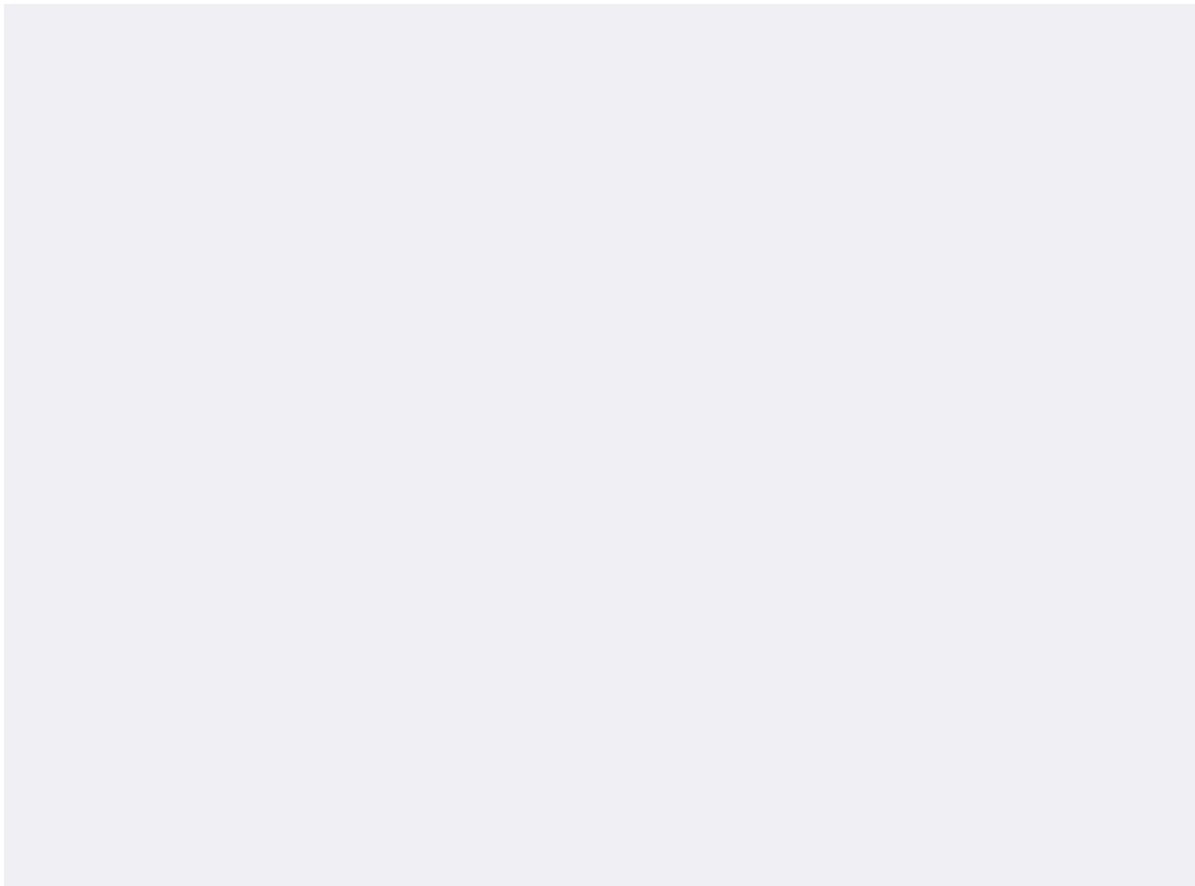


image.png

2.6 配置成功

Burp Intruder Repeater Window Help										
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Sqlmap										
Intercept HTTP history WebSockets history Options										
Filter: Hiding CSS, image and general binary content										
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
100	https://m.baidu.com	GET	/?action=getadsdata&sourceChannel=&...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	2500	script		
98	https://m.baidu.com	GET	/se/static/js/depl/ralltir_min_1a3d103.js	<input type="checkbox"/>	<input type="checkbox"/>	200	40455	script	js	
84	https://m.baidu.com	GET	/?action=getadsdata&sourceChannel=&...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	2491	script		
83	https://m.baidu.com	GET	/se/static/js/depl/ralltir_min_1a3d103.js	<input type="checkbox"/>	<input type="checkbox"/>	200	40452	script	js	
82	https://s.bdstatic.com	GET	/common/openjs/bdbanner.js?bd-refor...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	18976	script	js	
81	https://p62-streams.icloud.com	POST	/10619773664/streams/putmetadata	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1343	XML		
79	https://m.baidu.com	GET	/se/static/js/service/index_polymer_4dc...	<input type="checkbox"/>	<input type="checkbox"/>	200	82766	script	js	
78	https://hm.baidu.com	GET	/hm.js?12423ecbc0e2ca965d84259063...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	227	script	js	
77	https://feed.baidu.com	GET	/feed/api/tab/gettabinfo?pd=wise&sid=...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	4455	script		
76	https://m.baidu.com	GET	/his?callback=jsonp1&type=3&pic=1&lid...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	456	script		
70	https://s.bdstatic.com	GET	/common/openjs/bdbanner.js?bd-refor...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	18977	script	js	

image.png

- 7，部分应用功能操作可能会慢，代理导致的网速问题。
- 8.最近在想办法搞谷歌浏览器HTTPS代理信任问题，火狐导入证书就可以。还有部门安卓手机需要转换是证书格式才可以导入。

3证书转换问题

1.没有转换之前打开

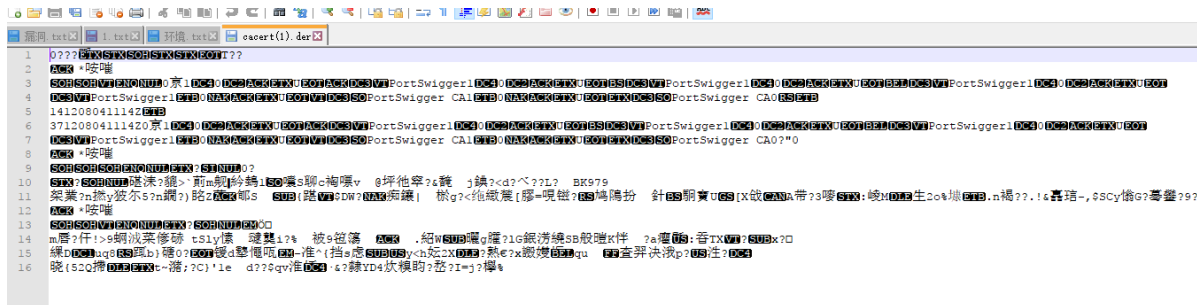


image.png

Firefox的设置里面，选择高级，然后选择证书机构，导入刚才下载的证书
新版本在
Firefox 隐私与安全--证书---查看
然后选择证书机构，导入刚才下载的证书
导入成功后发现证书机构中多出PortSwigger导出就可以。

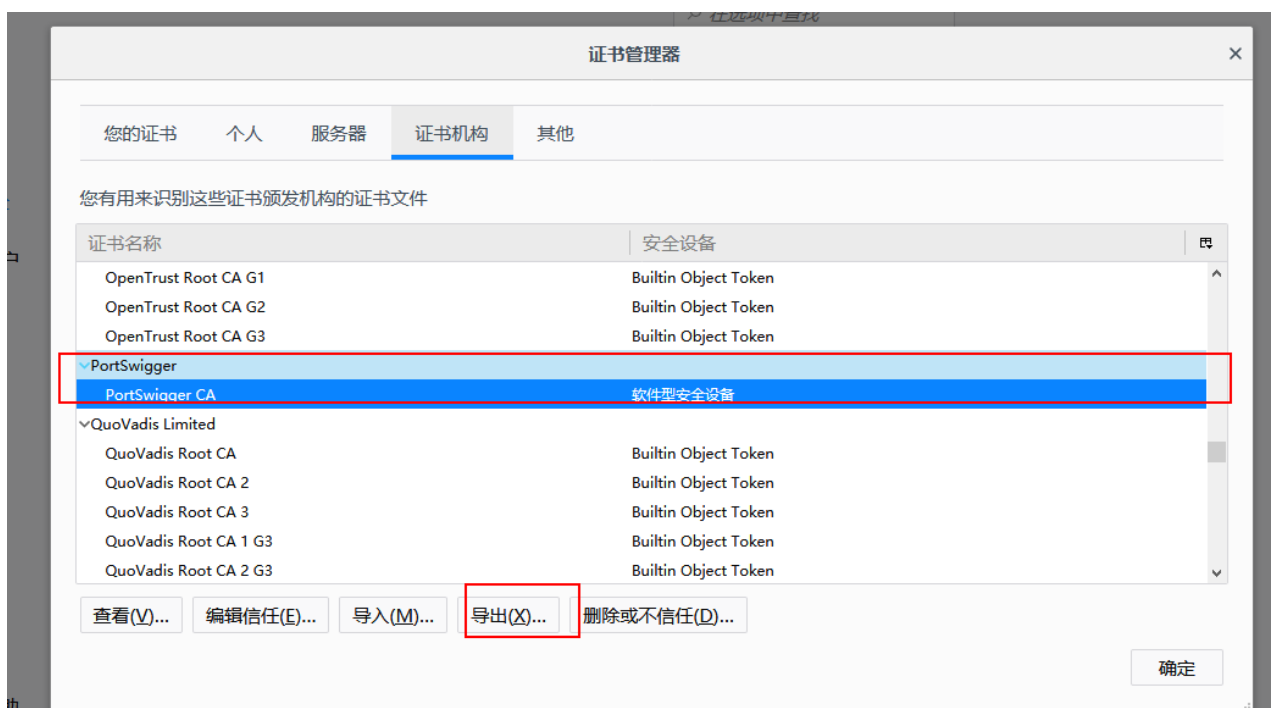


image.png

(为了看对比效果)，转换格式之后抓安卓 安卓安装自行google方法很多了。

```
漏洞.txt x 1.txt x 环境.txt x cacert(1).der x PortSwiggerCA.crt x
1 -----BEGIN CERTIFICATE-----
2 MIIDyTCCArGgAwIBAgIEVIUk4jANBgkqhkiG9w0BAQsFADCBijEUMBIGAlUEBhML
3 UG9ydFN3aWdnZXIxFDASBgNVBAGTC1BvcnRTd2lnZ2VyMRQwEgYDVQQHEwtQb3J0
4 U3dpZ2d1cjEUMBIGAlUEChMLUG9ydFN3aWdnZXIxFzAVBgNVBAsTD1BvcnRTd2ln
5 Z2VyIENBMRCwFQYDVQQDEw5Qb3J0U3dpZ2d1ciBDQTAeFw0xNDEyMDgwNDEzMTRa
6 Fw0zNzEyMDgwNDEzMTRaMIGKMRQwEgYDVQQGEwtQb3J0U3dpZ2d1cjEUMBIGAlUE
7 CBMLUG9ydFN3aWdnZXIxFDASBgNVBAGTC1BvcnRTd2lnZ2VyMRQwEgYDVQQKEwtQ
8 b3J0U3dpZ2d1cjEXMBUGAlUECXMouG9ydFN3aWdnZXIgaQ0ExFzAVBgNVBAMTD1Bv
9 cnRTd2lnZ2VyIENBMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtFWb
10 pM8w9fk+YMhtbdNgqIa8jvluMX804OxTwcRj0Wng0Xanw0DGuo+xEcMDibxS6Fg
11 auVgmT88ZKoFpNmHG682TMAB+uFCSzk3OQ2W9JhJ0gRuk9N5oPiMqjWMGW7nic4n
12 KbGFWsuaSQbbqFP6qBp723sLJERXlTEVs9Xognym/peaZ5E0PK+vv0Dec1vEej2G
13 WulD0RjmEh7wr+tJsOemZOGYCPFvjJpVHVtY6qgYQbT4oxAzh083AjqNkk0Qyfoy
14 byWt9xcubrrWtinEHC4hJtdurEotLCRTQ3mQ+0fBG93rz5s/OfILP6V+TnWBSQVN
15 hYJihqxLBoChdnOpCwIDAQABozUwMzASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1Ud
16 DgQWBBT5SDvxp/h2VQs7RmTCWpZGs/YeHTANBgkqhkiG9w0BAQsFAAOCAQEAGdYN
17 bbS9yhKBnCE+Oc2HrLuyy4K8s5IJdFNseeO6/4Wm/YxpsX81oXOxuzm4h7qCp8Nu
18 Bv8uvUJXGpXxZ8VH1P9sR+KMnEXAQFNCsOOVsEuQRf+K/2Hxs5rOHZqVUVRYC7E6
19 GnJTCr5bRBF1cTge2ldifbRnMNQPBO/MZKDgkZmF9xkt17xee7Wyc8LHGh95PGiK
20 dTJYEPUVyuyAvzt4l2WL/paVB3FlpnkMlsv04L72m+Fwwy4fm4jiPBQKz/57NTJR
21 k58QA3R+5PM70DJDfScxZfnwZiWssTAKcXa7tMluFKGkJtcJ62BZRDS0tvTcsV2e
22 MY22yTtJPWraA5nbJQ==
23 -----END CERTIFICATE-----
24
```

image.png