

学习目标：

- [] Charles基本功能的使用
 - [] Charles如何安装根证书，手机如何连接Charles进行抓包
 - [] Charles 抓取Https的数据包，抓取手机数据包
 - [] 分析数据包
-

内容复习

- Charles 基础
- Charles安装
- Charles工具栏
- Charles抓取数据包

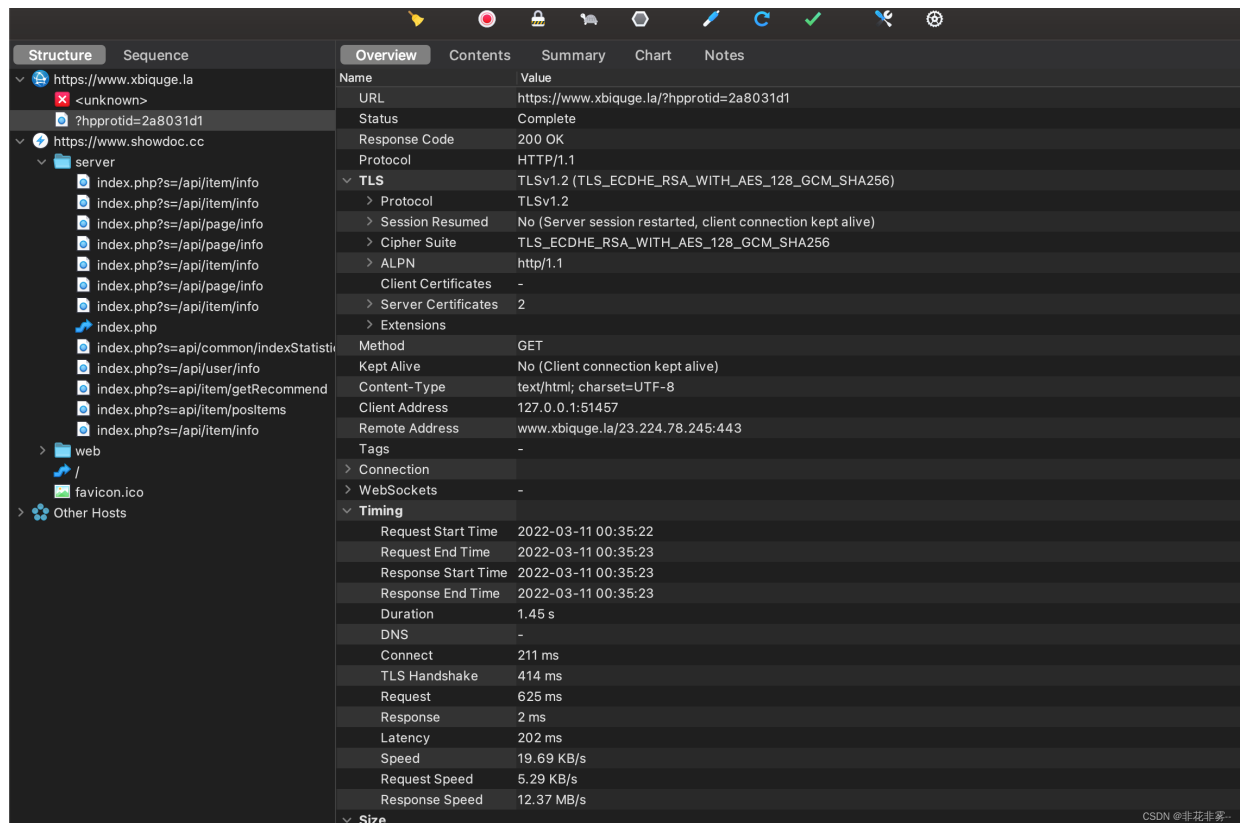
学习内容：

1、学习Charles抓包的基本使用

通过浏览器配合charles抓取网页信息、接口信息并进行简单的分析

<https://www.xbiquge.la/?hprotid=2a8031d1>

<https://www.showdoc.com.cn/item/password/1816133361892181>

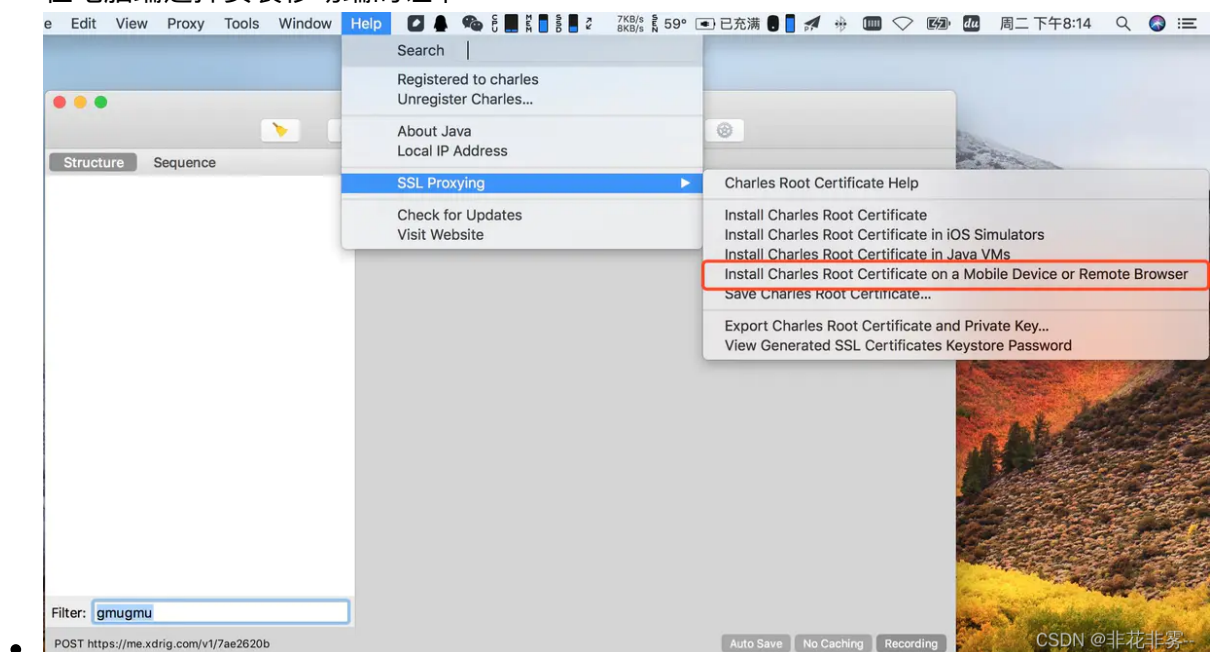


2、配置电脑，手机抓取Https数据包

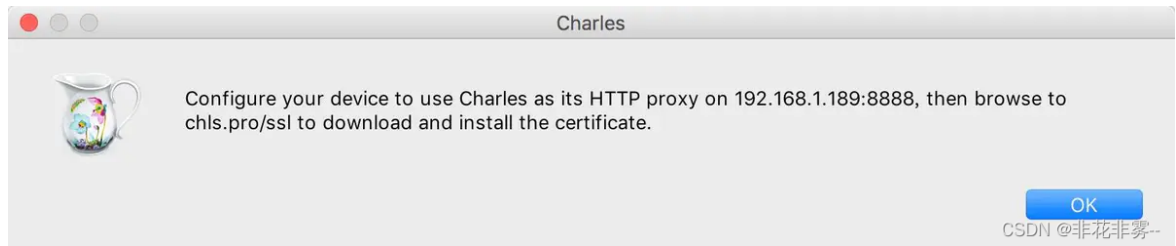
在电脑上配置Https 证书、在手机上安装cert证书，来配置Charles进行手机、电脑的数据包抓取

在手机端配置根证书

- 在电脑端选择安装移动端的证书：



- 选择后会显示IP与端口号，用于手机设置http代理：



- 手机的网络上设置成电脑的http代理：(需要注意的一点就是电脑的网络要与手机的网络处于同一个局域网中，比如连接同一个路由器对应的网络)

☒ 显示高级选项

代理服务器

手动

▼

HTTP代理器浏览器可用，但可能对其他应用程序不可用。

代理主机名

192.168.1.189

代理服务器端口

8888

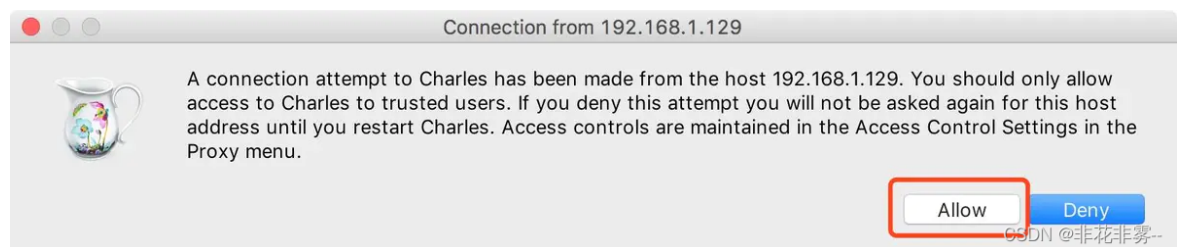
旁路代理

example.com,mycomp.test.com

☐ 验证服务器



- 设置完成后访问网络时，服务端会弹出提示，点击Allow(同意连接):



- 手机浏览器访问chls.pro/ssl，下载证书并安装(证书名任意):

证书名

证书名
Charles

使用于
VPN 与应用程序

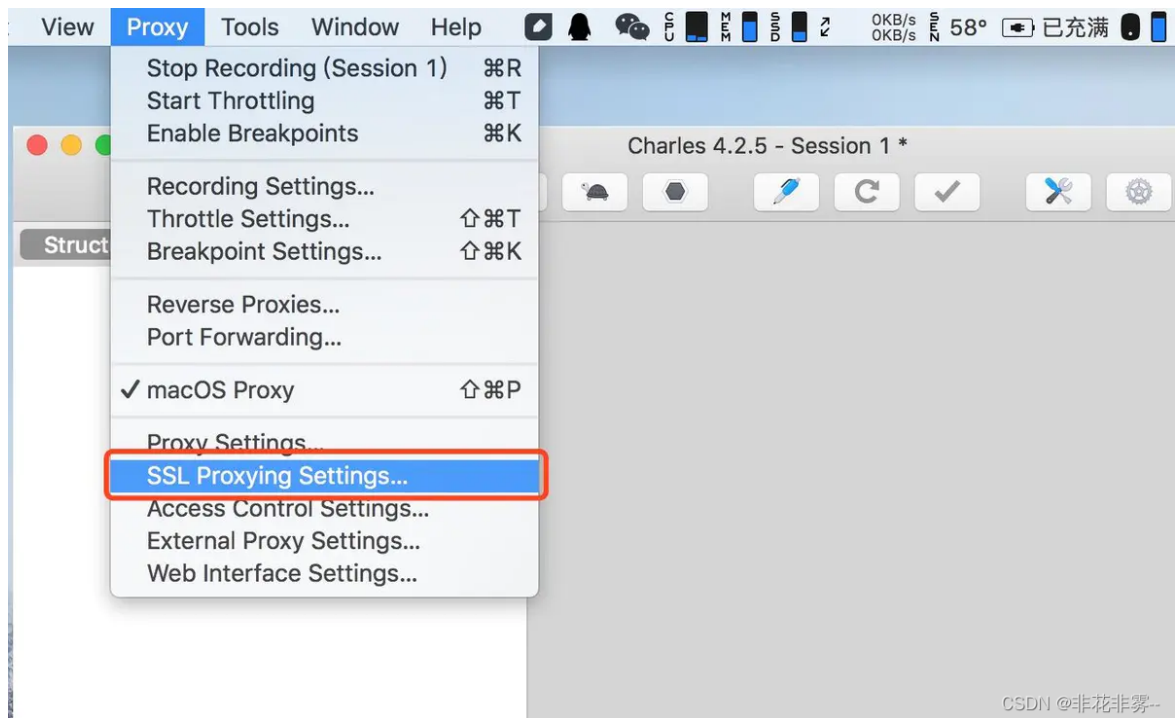
封包含有：
一个CA证书

取消 确认

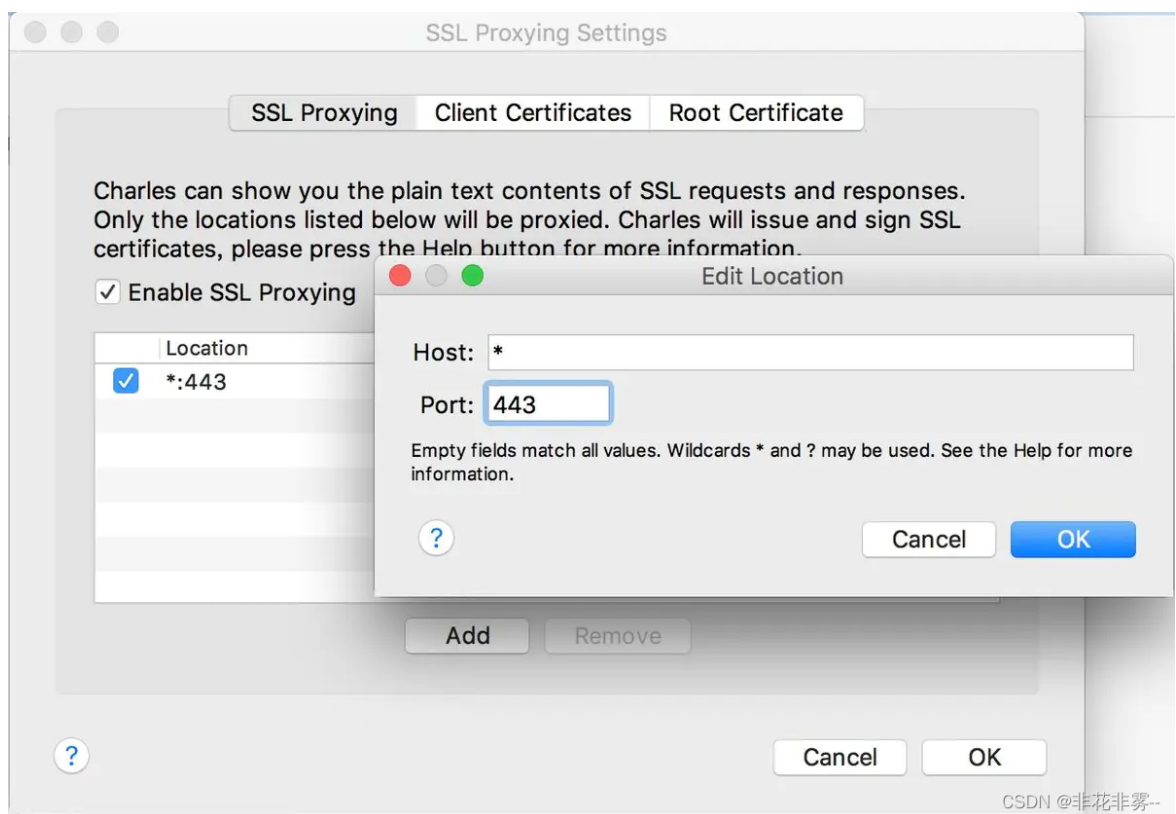
CSDN @非花非雾--

配置电脑端的抓取规则

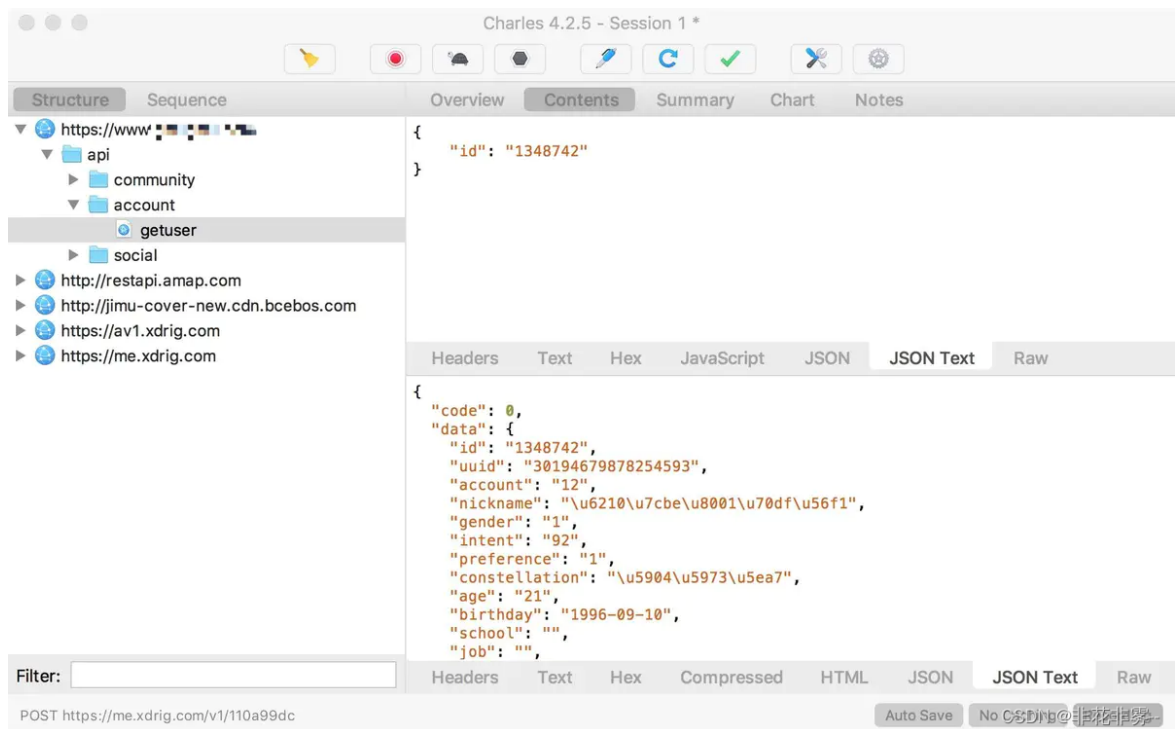
- 进入Charles的SSL代理设置：



- 勾选启动SSL代理，并添加一个抓取规则，比如这里加上一个抓取所有https(443端口)的请求：



- 此时手机上打开https请求的应用，应该就可以正常看到https请求的数据了：如图：



3、抓取手机、电脑数据包

通过以上配置以后我们就可以抓取手机上的数据包了 尝试打开手机浏览器，然后访问网页，查看抓取到的手机数据

4、分析具体的数据包

Overview Contents Summary Chart Notes

Name	Value
URL	https://www.xbiquge.la/?hprotid=2a8031d1
Status	Complete
Response Code	200 OK
Protocol	HTTP/1.1
▼ TLS	TLSv1.2 (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
> Protocol	TLSv1.2
> Session Resumed	No (Server session restarted, client connection kept alive)
> Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
> ALPN	http/1.1
Client Certificates	-
> Server Certificates	2
> Extensions	-
Method	GET
Kept Alive	No (Client connection kept alive)
Content-Type	text/html; charset=UTF-8
Client Address	127.0.0.1:51457
Remote Address	www.xbiquge.la/23.224.78.245:443
Tags	-
> Connection	-
> WebSockets	-
▼ Timing	-
Request Start Time	2022-03-11 00:35:22
Request End Time	2022-03-11 00:35:23
Response Start Time	2022-03-11 00:35:23
Response End Time	2022-03-11 00:35:23
Duration	1.45 s
DNS	-
Connect	211 ms
TLS Handshake	414 ms
Request	625 ms
Response	2 ms
Latency	202 ms
Speed	19.69 KB/s
Request Speed	5.29 KB/s
Response Speed	12.37 MB/s
▼ Size	-
> Request	3.31 KB (3,385 bytes)
> Response	25.33 KB (25,934 bytes)
Total	28.63 KB (29,319 bytes)

请求的地址、请求返回状态码

请求方法

请求的开始结束时间

一个完整的请求的时间

数据包大小

CSDN @非花非雾-

Http状态码

状态码	英文名称	中文描述
100	Continue	继续。客户端应继续其请求
101	Switching Protocols	切换协议。服务器根据客户端的请求切换协议。只能切换到更高级的协议，例如，切换到HTTP的新版本协议
200	OK	请求成功。一般用于GET与POST请求
201	Created	已创建。成功请求并创建了新的资源
202	Accepted	已接受。已经接受请求，但未处理完成
203	Non-Authoritative	非授权信息。请求成功。但返回的meta信息不在原始的服务器，而是一个副本

	Information	
204	No Content	无内容。服务器成功处理，但未返回内容。在未更新网页的情况下，可确保浏览器继续显示当前文档
205	Reset Content	重置内容。服务器处理成功，用户终端（例如：浏览器）应重置文档视图。可通过此返回码清除浏览器的表单域
206	Partial Content	部分内容。服务器成功处理了部分GET请求
300	Multiple Choices	多种选择。请求的资源可包括多个位置，相应可返回一个资源特征与地址的列表用于用户终端（例如：浏览器）选择
301	Moved Permanently	永久移动。请求的资源已被永久的移动到新URI，返回信息会包括新的URI，浏览器会自动定向到新URI。今后任何新的请求都应使用新的URI代替
302	Found	临时移动。与301类似。但资源只是临时被移动。客户端应继续使用原有URI
303	See Other	查看其它地址。与301类似。使用GET和POST请求查看
304	Not Modified	未修改。所请求的资源未修改，服务器返回此状态码时，不会返回任何资源。客户端通常会缓存访问过的资源，通过提供一个头信息指出客户端希望只返回在指定日期之后修改的资源
305	Use Proxy	使用代理。所请求的资源必须通过代理访问
306	Unused	已经被废弃的HTTP状态码
307	Temporary Redirect	临时重定向。与302类似。使用GET请求重定向
400	Bad Request	客户端请求的语法错误，服务器无法理解
401	Unauthorized	请求要求用户的身份认证
402	Payment Required	保留，将来使用
403	Forbidden	服务器理解请求客户端的请求，但是拒绝执行此请求
404	Not Found	服务器无法根据客户端的请求找到资源（网页）。通过此代码，网站设计人员可设置"您所请求的资源无法找到"的个性页面
405	Method Not Allowed	客户端请求中的方法被禁止

406	Not Acceptable	服务器无法根据客户端请求的内容特性完成请求
407	Proxy Authentication Required	请求要求代理的身份认证，与401类似，但请求者应当使用代理进行授权
408	Request Time-out	服务器等待客户端发送的请求时间过长，超时
409	Conflict	服务器完成客户端的 PUT 请求时可能返回此代码，服务器处理请求时发生了冲突
410	Gone	客户端请求的资源已经不存在。410不同于404，如果资源以前有现在被永久删除了可使用410代码，网站设计人员可通过301代码指定资源的新位置
411	Length Required	服务器无法处理客户端发送的不带Content-Length的请求信息
412	Precondition Failed	客户端请求信息的先决条件错误
413	Request Entity Too Large	由于请求的实体过大，服务器无法处理，因此拒绝请求。为防止客户端的连续请求，服务器可能会关闭连接。如果只是服务器暂时无法处理，则会包含一个Retry-After的响应信息
414	Request-URI Too Large	请求的URI过长（URI通常为网址），服务器无法处理
415	Unsupported Media Type	服务器无法处理请求附带的媒体格式
416	Requested range not satisfiable	客户端请求的范围无效
417	Expectation Failed	服务器无法满足Expect的请求头信息
500	Internal Server Error	服务器内部错误，无法完成请求
501	Not Implemented	服务器不支持请求的功能，无法完成请求

502	Bad Gateway	作为网关或者代理工作的服务器尝试执行请求时，从远程服务器接收到了一个无效的响应
503	Service Unavailable	由于超载或系统维护，服务器暂时的无法处理客户端的请求。延时的长度可包含在服务器的Retry-After头信息中
504	Gateway Time-out	充当网关或代理的服务器，未及时从远端服务器获取请求
505	HTTP Version not supported	服务器不支持请求的HTTP协议的版本，无法完成处理

学习产出：

- [x] 掌握Charles如何在手机端电脑端配置抓包
- [x] 掌握数据包中数据参数含义
- [x] 掌握对不同应用、网页的数据抓包