

03_抓包工具的使用

=====

背景：

抓包：

主要抓取网络之间传输在应用层的用户数据。

价值：在软件测试中，特别是APP客户端（IOS与Android）和H5页面与后端服务之间进行HTTP通信的时候，

抓包这个操作应该是最常见的，这项技术的掌握可以说是测试人员的一门必修课，为什么这么说呢？

至少下面的三个因素是最重要的：

- 1. 通过抓包我们能清晰的知道前后端交互的数据细节。
- 2. 通过抓包我们对Http接口进行测试。
- 3. 当我们发现系统有bug的时候，可以通过抓包来鉴定问题是出现在客户端还是服务端。

通常业界的抓包工具也较多比如wireshark, charles, Fiddler等，但相对charles用得比较多，我们这个文档以charles来举例就好。

Charles 通过将自己设置成系统的网络访问代理服务器，使得所有的网络访问请求都通过它来完成，从而实现了网络封包的截取和分析。

抓包工具charles的获取

由于互联网的研发工程师基本使用的是mac电脑，本教程以mac笔记本为例子来编写。

下载链接：<https://www.charlesproxy.com/download/>

打开上述的链接找到对应的操作系统版本即可，这里选择macOS,dmg版本，下载到本机直接安装即可。

下载完后在本机的桌面可以看到一个茶壶的图标，表明安装是成功的。



默认安装的版本是一个试用版，只有30天的试用期，当然破解是很简单的，各位网上随便搜搜就好。

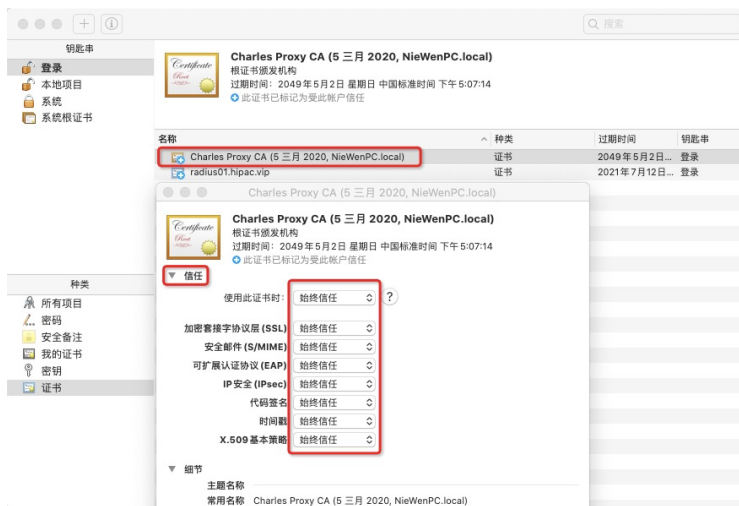
=====

我是分隔区域

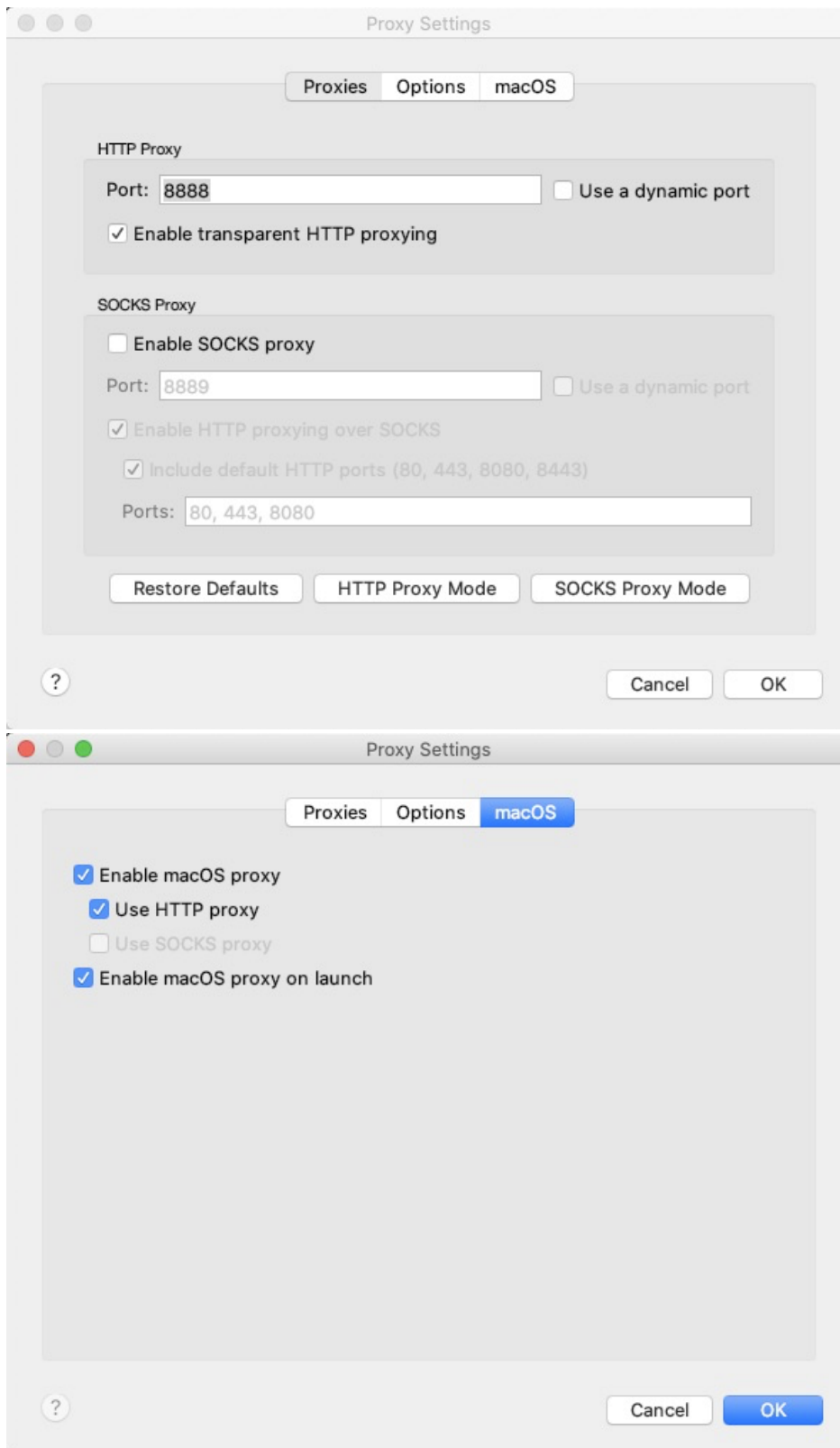
=====

Charles 的配置

- Step1: 在本机安装安装证书文件。 Help→SSL Proxying→ install Charles Root Certificate，按下面的截图全部信任。



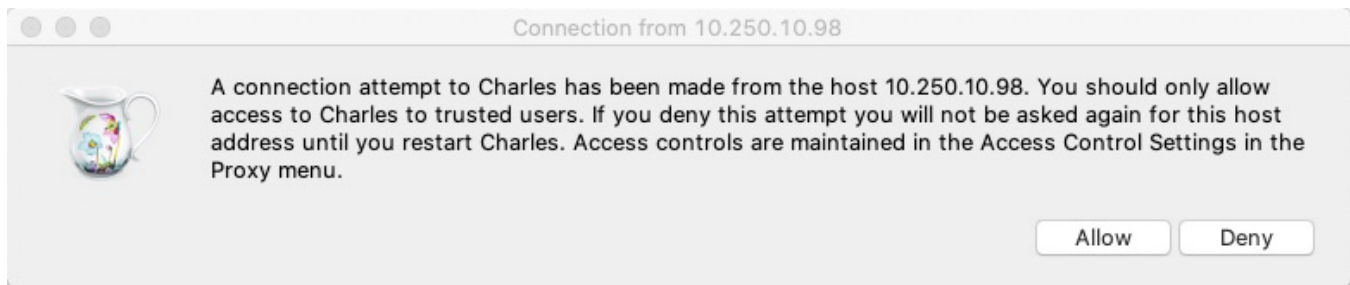
- Step2: 配置代理：proxy→Proxy Settings, 按照下面的截图配置即可。



- Step3: 在手机端设置代理访问（前提：手机和笔记本mac连接的是同一个wifi热点）

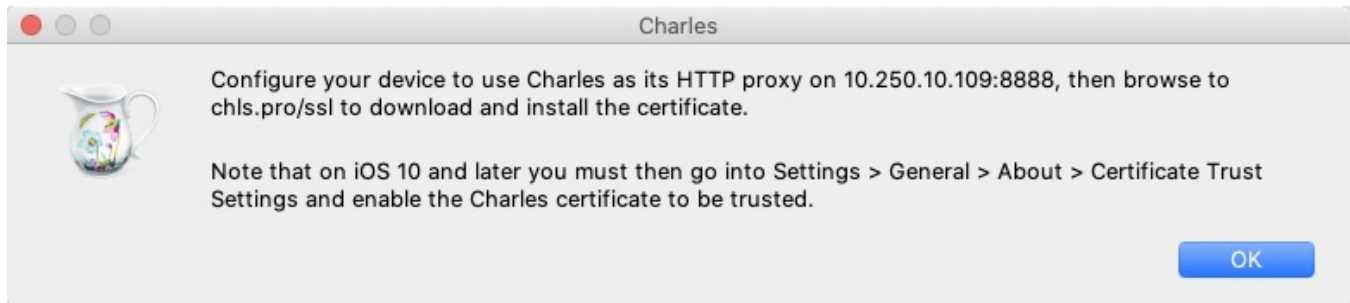
以iPhone为例，安卓机型类推，先获得macbook的IP地址：Charles Help → Local IP Address

设置 → 无限局域网 → 点击wifi热点hipac-port 最右边的 感叹号小图标，进入一个新的页面往下拉，找到HTTP代理（配置代理）点击 → 点击“手动”
在下面的服务器一栏中输入MAC IP 地址，端口一栏中输入8888后点击右上角的存储退出。这时会在Charles这边弹出一个框点击“Allow”。



正常到这里手机上面操作就能在charles上抓到手机端发送的请求信息了，但是只能是http协议的，对于https协议需要在手机端再安装证书才能抓到。

- step4: charles 点击菜单 Help→SSL Proxying→ Install Charles Root Certificate on a Mobile Device or Remote Brower， 点击ok按钮。



- step5: 按照步骤4中的提示，在手机端打开一个浏览器输入 chls.pro/ssl, 这个时候会提示安装手机的证书，点击允许后在点击下载即可。
- step6: 打开iPhone 设置 → 通用 → 描述文件， 点击刚刚下载的证书（charles Proxy CA...），在新的页面点击右上角的安装。安装完成后会显示已验证。
- step7: 打开iPhone 设置 → 通用 → 关于本机 → 证书信任设置 开启证书的信任。

这时所有的设置结束，能正常的抓取http和https的数据包。

Structure	Sequence	Overview	Contents	Summary	Chart	Notes
https://h-adashx.ut.taobao.com		Name	Value			
http://galaxy.yangtuoja.com		api	hipac.mall.orderList.regularItem.get			
http://k.yangtuoja.com		apiKey	1101			
rest		appv	4.45.0			
mywork		data	{*osdType:"100",*orderType:"1",*tabName:"全部订单_待支付"}			
quickreload		deviceId	C77105BD-8AF7-43D6-A131-B6A77A293585_tongdun			
latest		model	iPhone 8 Plus			
52274473?since=1606208746814&_=1606208716530		os	iOS			
52274473?since=1606208776820&_=1606208716532		osv	13.6.1			
52274473?since=1606208806828&_=1606208716534		refPage	hipacapp://mall/ShopOrder			
tinyfce		sign	fa6bfda82b857aa217bb1cca84bdb02			
jiraanywhere		signType	new			
shortcuts		t	1606208793432			
api		token	voqHo5By5dBI-ZYnpFFXqGTROY9gd7bZ2n2k1KOzPG0nL3UsmH-X2gS			
autoconvert		v	1.0.0			
ui						
analytics						
synchrony-proxy						
json						
http://log.kibina.yangtuoja.com						
https://content-autofill.googleapis.com						
https://lgstatic.com						
https://iesdouyin.com						
https://autohome.com.cn						
https://api.hipac.cn						
config						
1.0.0						
polling?api=polling&apiKey=1101&appv=4.45.0&deviceId=C77						
process						
prod						
1.0.0						
buy_order.getCancelReason.app						
hipac.mall.orderList.regularItem.get						
1.0.1						
buy_order.queryTrade.app						
1.0.6						
mall.item.recommendItem.app						
https://ios.bugly.qq.com						
https://gateway.icloud.com						
https://douyin.com						
https://test-www.douyin.com						

Headers	Cookies	Text	Hex	Form	Raw
{ "api": "hipac.mall.orderList.regularItem.get", "v": "1.0.0", "code": 200, "message": "OK", "data": { "linkUrl": "hipacapp://mall/RegularPurchase", "itemList": [{ "brandName": "联想你", "buyCount": null, "itemType": 2, "categoryIdFirst": 6, "buyTime": null, "pic": "http://img.hicdn.cn/202005/item/05141606412648w380_800x800.jpg", "redPill": { "utp": "1", "extendFields": "{ \"item_id\":250022,\"tab_name\": \"全部订单_待支付\", \"trace_p\": \"全部-购物车-点击可购买的商品\", \"redPillType\": null, \"utrp\": \"6.1.9.4.1\", \"areaExpose\": null }, "itemId": 250022, "itemName": "粮珍东北大米五常大米稻花香2号5kg (10斤)", "brandId": null, "linkUrl": "hipacapp://mall/RegularPurchase?itemId=250022&storeId=2879ce3cc870", "itemTypeName": "国内仓发货", "id": null }] }, "itemId": 250022, "itemName": "粮珍东北大米五常大米稻花香2号5kg (10斤)", "brandId": null, "linkUrl": "hipacapp://mall/RegularPurchase?itemId=250022&storeId=2879ce3cc870", "itemTypeName": "国内仓发货", "id": null }					

安卓机型类似的方式设置

=====

=====

我是分隔区域 ~ ~ ~ ~

=====

=====

数据包怎么看？

charles支持两个格式查看包数据

Structure：按照数据包的请求地址的结构分层次的展示，相同的请求会被放入同一个目录下。

Sequence：按照时间线的维度展示请求信息，后发送的请求在先发送的请求后面。

StructureSequence

▶ https://h-adashx.ut.taobao.com

▼ http://galaxy.yangtuojia.com

- ▼ jacocorecordhistory
 - ⌚ getData?params%5BRandom_id_parent%5D=1606203983322¶
 - ⌚ getData?params%5BRandom_id_parent%5D=1606203983322¶
 - ⌚ getData?params%5BRandom_id_parent%5D=1606203983322¶
 - ⌚ getData?params%5BRandom_id_parent%5D=1606203983322¶

▼ http://k.yangtuojia.com

- ▼ rest
 - ▶ mywork
 - ▼ quickreload
 - ▼ latest
 - ⌚ 52274473?since=1606208746814&_=1606208716530
 - ⌚ 52274473?since=1606208776820&_=1606208716532
 - ⌚ 52274473?since=1606208806828&_=1606208716534
 - ▶ tinymce
 - ▶ jiraanywhere
 - ▶ shortcuts
 - ▶ ani

StructureSequence

	Code	Method	Host	Path
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	GET	safebrowsing.googleapis.com	/v4/threatListUpdates:fetch?\$req=Ch
⌚	200	GET	k.yangtuojia.com	/rest/mywork/latest/status/notification,
⌚	200	POST	k.yangtuojia.com	/synchrony-proxy/v1/bayeux-sync1
⌚	200	POST	k.yangtuojia.com	/ison/startheartbeatactivity.action

每一条请求数据怎么看？

我们以structure格式为例：随机点击一个请求，右边会有一个详情框显示出来。

先看Overview标签的内容有哪些，我们把经常关注的信息标示出来了。

Charles 4.2.8 - Session 1

Structure Sequence

- autoconvert
- ui
- analytics
- experimental
- synchrony-proxy
- json
- plugins
- download
- http://log.kibina.yangtuoja.com
- https://content-autofill.googleapis.com
- https://lgstatic.com
- https://iesdouyin.com
- https://autohome.com.cn
- https://api.hipac.cn
 - config
 - 1.0.0
 - polling?api=polling&appKey=1101&appv=4.45.0&deviceId=C77
 - process
 - prod
 - 1.0.0
 - buy.order.getCancelReason.app
 - hipac.mall.orderList.regularItem.get
 - 1.0.1
 - buy.order.queryTrade.app
 - 1.0.6
 - mall.item.recommendItem.app
 - https://ios.bugly.qq.com
 - https://gateway.icloud.com
 - https://douyin.com
 - https://test-www.douyin.com
 - https://www.google.com
 - https://ya.hipac.cn
 - https://dispatcher.is.autonavi.com
 - http://img.hicdn.cn
 - https://analytics.yinxiang.com
 - https://gateway.icloud.com.cn
 - https://k.yangtuoja.com:80
 - https://adashbc.ut.taobao.com
 - https://hmma.baidu.com
 - https://static.dingtalk.com
 - https://safebrowsing.googleapis.com

Filter:

Overview Contents Summary Chart Notes

Name	Value
URL	https://api.hipac.cn/process/prod/1.0.6/mall.item.recommendItem.app 请求的地址
Status	Complete
Response Code	200 OK 返回的状态码 200 表示成功
Protocol	HTTP/1.1 HTTP的协议版本
TLS	TLSv1.2 (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
Protocol	TLSv1.2
Session Resumed	No
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ALPN	http/1.1
Client Certificates	-
Server Certificates	2
Extensions	
Method	POST 请求的方式 get, Post, Put 等
Kept Alive	No
Content-Type	application/json; charset=UTF-8
Client Address	10.250.10.98:54712 请求的源地址
Remote Address	api.hipac.cn/47.110.173.229:443 请求的目的地址
Connection	
WebSockets	-
Timing	
Request Start Time	20-11-24 17:06:33
Request End Time	20-11-24 17:06:34
Response Start Time	20-11-24 17:06:34
Response End Time	20-11-24 17:06:34
Duration	278 ms
DNS	2 ms
Connect	7 ms
TLS Handshake	21 ms
Request	1 ms
Response	6 ms
Latency	241 ms
Speed	117.65 KB/s
Request Speed	2.84 MB/s
Response Speed	4.85 MB/s
Size	
Request	2.91 KB (2,980 bytes)
Response	29.80 KB (30,512 bytes)
Total	32.71 KB (33,492 bytes)

Contents 标签内容，右边框内的上半部分是请求的body内容，下半部分是响应的body部分，具体的数据支持多种格式呈现。

StructureSequence

autoconvert

ui

analytics

experimental

synchrony-proxy

json

plugins

download

http://log.kibina.yangtuoja.com

https://content-autofill.googleapis.com

https://lgstatic.com

https://iesdouyin.com

https://autohome.com.cn

https://api.hipac.cn

config

1.0.0

polling?api=polling&appKey=1101&appv=4.45.0&deviceId=C77

process

prod

1.0.0

buy_order.getCancelReason.app

hipac.mall.orderList.regularItem.get

1.0.1

buy_order.queryTrade.app

1.0.6

mall.item.recommendItem.app

https://os.bugly.qq.com

https://gateway.icloud.com

https://douyin.com

https://test-www.douyin.com

https://www.google.com

https://ya.hipac.cn

https://dispatcher.is.autonavi.com

http://img.hicdn.cn

https://analytics.yinxiang.com

https://gateway.icloud.com.cn

https://k.yangtuoja.com:80

https://adashbc.ut.taobao.com

https://hmma.baidu.com

https://static.dingtalk.com

https://safebrowsing.googleapis.com

OverviewContentsSummaryChartNotes

POST /process/prod/1.0.6/mall.item.recommendItem.app HTTP/1.1

Host api.hipac.cn

Content-Type application/x-www-form-urlencoded

Cookie SERVERID=dec2d3bc0ae061c64f0a76f4533208bc|1606208793|1606208721; LOGIN_ROLE=SHOP_MAN

Connection keep-alive

Accept */*

User-Agent YTMall/4.45.0 (com.ytmallapp.ios; build:4; iOS 13.6.1) Alamofire/5.1.0

Accept-Language zh-Hans-CN;q=1.0

Content-Length 451

Accept-Encoding br;q=1.0, gzip;q=0.9, deflate;q=0.8

HeadersCookiesTextHexFormRaw

HTTP/1.1 200 OK

Date Tue, 24 Nov 2020 09:06:34 GMT

Content-Type application/json; charset=UTF-8

Transfer-Encoding chunked

Content-Disposition inline; filename=f.txt

Access-Control-Allow-Credentials true

Access-Control-Allow-Headers X-Requested-With

Access-Control-Allow-Methods GET,POST,OPTIONS

timing-allow-origin *

Set-Cookie SERVERID=dec2d3bc0ae061c64f0a76f4533208bc|1606208794|1606208721; Path=/

Connection keep-alive

HeadersSet CookieTextHexJavaScriptJSONJSON TextRaw

POST http://k.vanhuia.com/vnchreow-nmev/v1/bawuc-kue1

StructureSequence

autoconvert

ui

analytics

experimental

synchrony-proxy

json

plugins

download

http://log.kibina.yangtuoja.com

https://content-autofill.googleapis.com

https://lgstatic.com

https://iesdouyin.com

https://autohome.com.cn

https://api.hipac.cn

config

1.0.0

polling?api=polling&appKey=1101&appv=4.45.0&deviceId=C77

process

prod

1.0.0

buy_order.getCancelReason.app

hipac.mall.orderList.regularItem.get

1.0.1

buy_order.queryTrade.app

1.0.6

mall.item.recommendItem.app

https://os.bugly.qq.com

https://gateway.icloud.com

https://douyin.com

https://test-www.douyin.com

https://www.google.com

https://ya.hipac.cn

https://dispatcher.is.autonavi.com

http://img.hicdn.cn

https://analytics.yinxiang.com

https://gateway.icloud.com.cn

https://k.yangtuoja.com:80

https://adashbc.ut.taobao.com

https://hmma.baidu.com

https://static.dingtalk.com

https://safebrowsing.googleapis.com

OverviewContentsSummaryChartNotes

Name	Value
api	mall.item.recommendItem.app
appKey	1101
appv	4.45.0
data	{\"recommendType\":\"121\",\"sortType\":\"2\"}
deviceId	C77105BD-8AF7-43D6-A131-B6A7A293585_tongdun
model	iPhone 8 Plus
os	iOS
osv	13.6.1
refPage	hipacapp://mall/ShopOrder
sign	6a05d60b8b042fd944ccf7cc855fcdab
signType	new
t	1606208793903
token	voqHo5By5dBi-ZYnnpFXqGTROY9gd7bZ2n2k1KOzPG0nL3UsmH-X2gSu6kgUASXL
v	1.0.6

HeadersCookiesTextHexFormRaw

```
{  \"api\": \"mall.item.recommendItem.app\",  \"v\": \"1.0.6\",  \"code\": 200,  \"message\": \"\",  \"data\": {    \"sourceType\": 0,    \"pageNo\": 2,    \"pageSize\": 10,    \"index\": 1,    \"itemList\": [{      \"delivery\": null,      \"topImgUrl\": null,      \"itemType\": {        \"name\": \"国内贸易\",        \"value\": \"2\",        \"formatValue\": null      },      \"activeTag\": \"巨划算\",      \"orderStock\": \"月进货 3031 人\",      \"itemTagCode\": 1,      \"itemPicMaskCode\": 0,      \"itemStyle\": null,      \"hotLevel\": \"3031\",      \"pic\": \"http://img.hicdn.cn/202010/item/1020152638958253j9_800x800.png\",      \"redpill\": {        \"utp\": \"1\",        \"extendFields\": \"{\\\"originType\\\":0,\\\"itemType\\\":0,\\\"groupType\\\":2,\\\"item_id\\\":300882,\\\"uttl\": \"待支付推荐\",\"}
```

至此你已经知道如何去查看一个数据包的具体内容了。

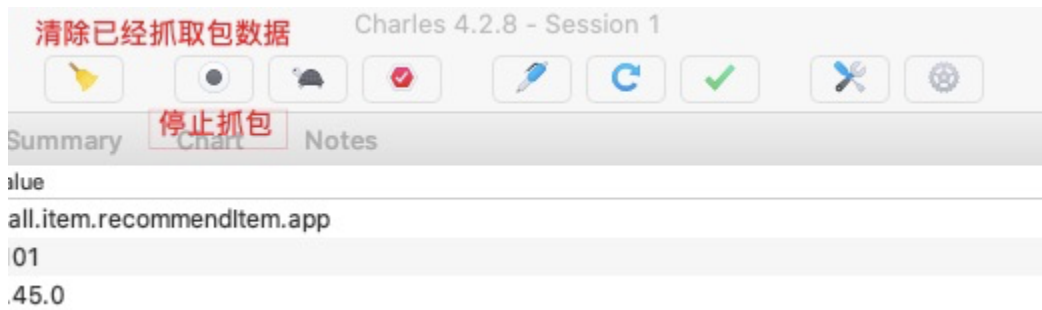
=====

=====

我是分隔区域 ~ ~ ~ ~

charles其他基本功能

- 抓包的基本设置

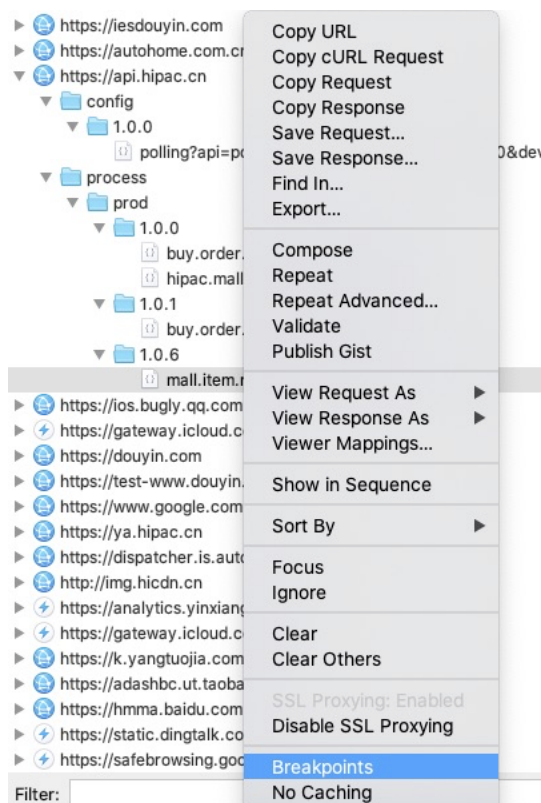


- 模糊查找数据包：

Edit → Find, 在打开的对话框中输入你想要查找的任意内容，charles会搜索出来所有跟关键匹配的请求。

它支持按包路径查找，也支持指定的消息列表中查找，搜索的关键词支持正则表达式，大小写是否敏感等。

- 请求过程中修改请求参数：这个功能非常有价值，类似于代码中调试断点功能，在需要断点的请求上右击选择BreakPoints



设置之后当有这条请求发送的时候会停下来，你可以从容的修改请求head和body，修改后再发送，也可以修改response的head和json数据。

这个功能在后端功能没有完全开发好之前验证前端非常管用。

- repeat功能：重复发送请求，这个可以让你不用从客户端操作，直接在charles中重发就行，该功能最常和Breakpoints配合使用。

其他比如模拟网络延时，数据包过滤，映射等功能可以参照互联网的知识文档查看，更多功能需要你更深入的使用才能理解和掌握

=====

作业:

1.自己负责抓取mall app的测试环境请求的hop地址的url,入参,返回,并进行网络延迟,返回结果的mock

结束