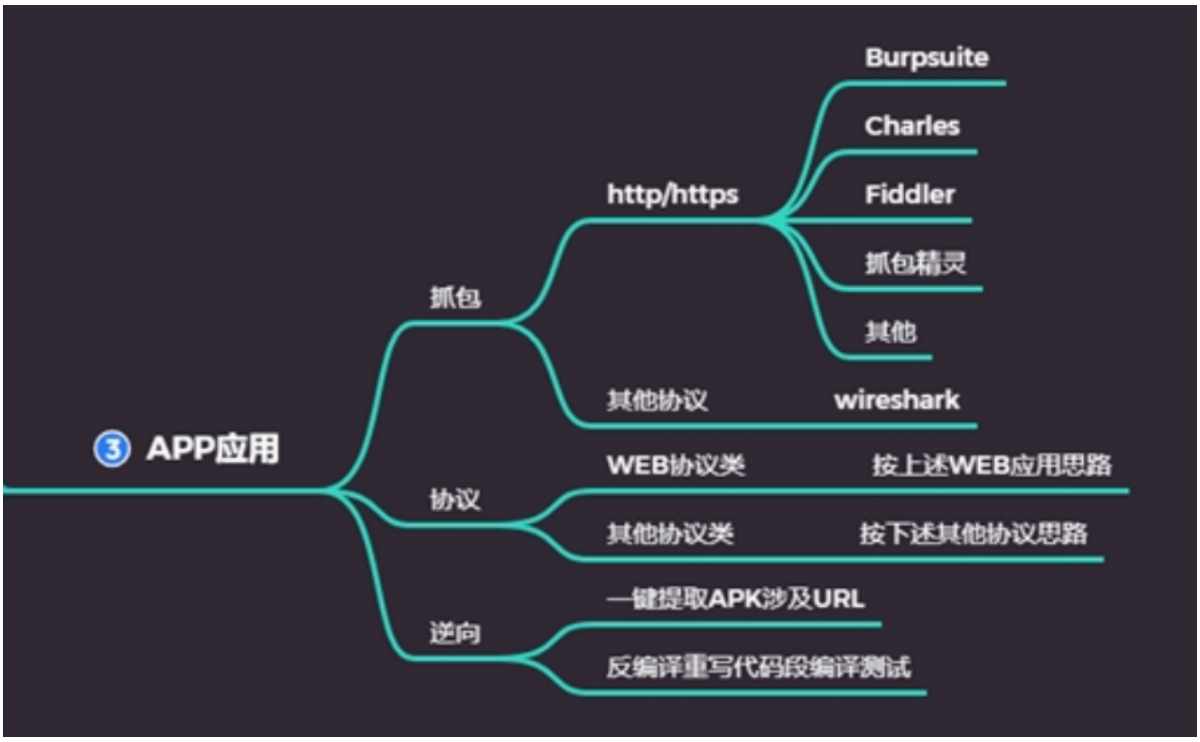
Day44　漏洞发现–APP应用之漏洞探针类型利用修复



44.1 思路说明

```
1  反编译提取 URL 或抓包获取 URL，进行 WEB 应用测试，如不存在或走其他协议的情况下，需采用网络接口抓包进行数据获取，转至其他协议安全测试！
```

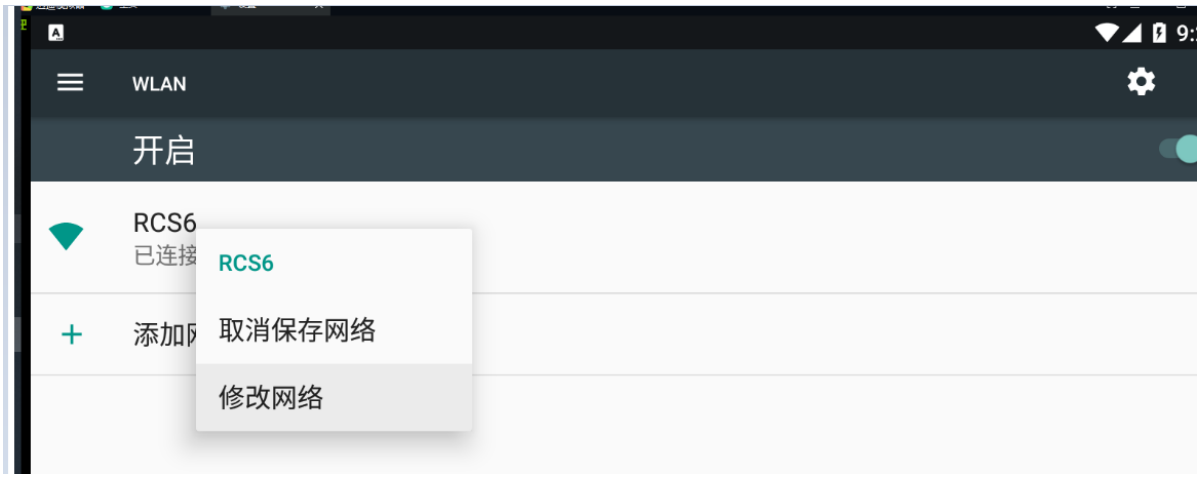
```
1  APP->WEB
2  APP->其他
3  APP->逆向
4  WEB 抓包，其他协议抓包演示及说明
5  未逆向层面进行抓包区分各协议测试
6  逆向层面进行提取 APK 代码层面数据
7  https://www.cnblogs.com/LOading/p/12388928.html
```

44.2 案例演示

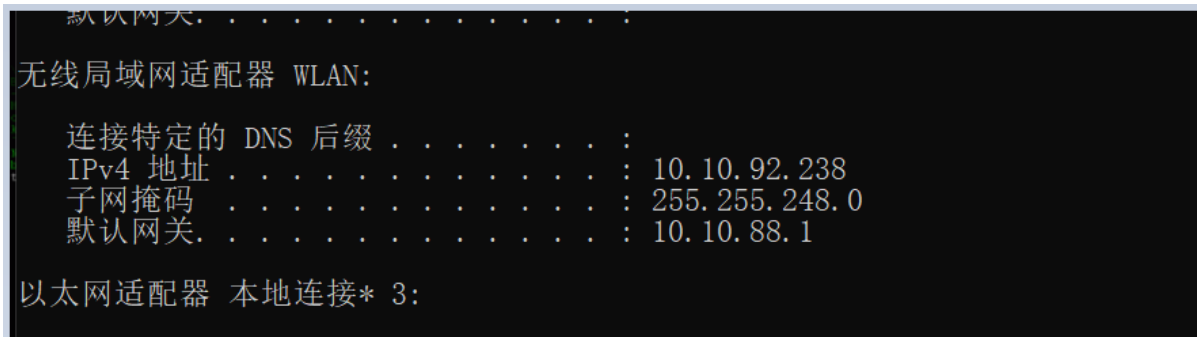
44.2.1 Burpsuite

```
burpsuite优点：在“HTTP history”记录历史数据包，且可以排序，点击空白处还可以筛选数据包；可以抓包还可以在线提交测试，可以做漏洞扫描
```

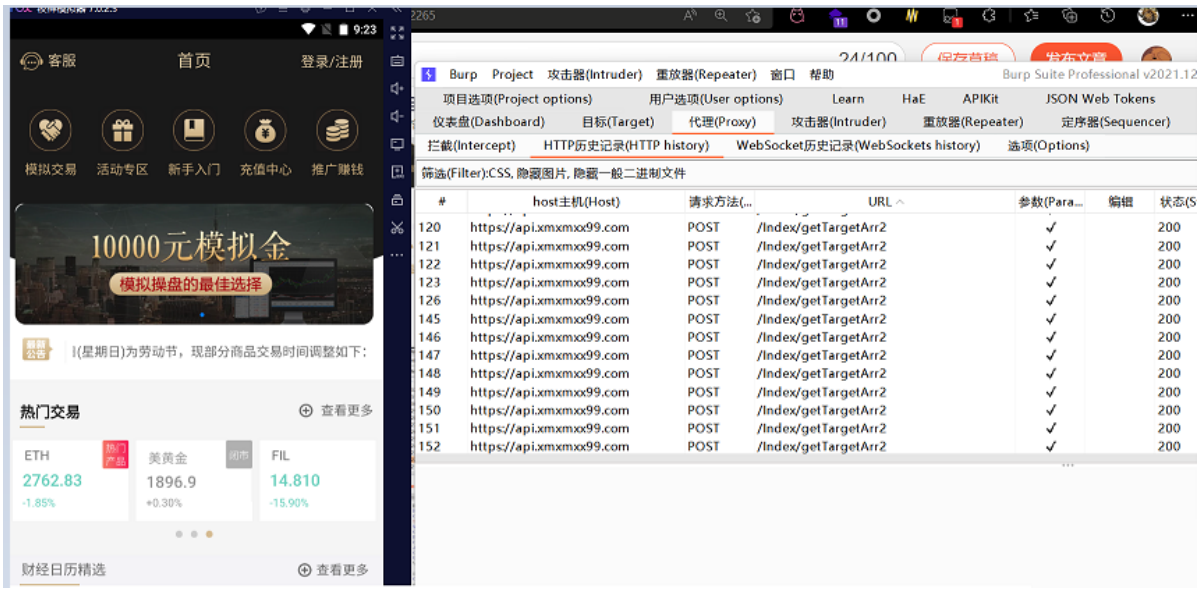
抓包前设置代理：在模拟器上将本机设为代理，注意不是127.0.0.1；在burpsuite上也添加对应的代理并勾选，使用需要抓包的app，产生大量数据包，数据包的“Host”数据以“http://”开头，可知其为HTTP数据包；“Params”处有对勾“√”说明该数据有参数，可以测试漏洞；“Extension”为文件类型，“Status”为状态码，将“Host”中的网址输入到浏览器，发现是网站，按照网站思路测试，安卓模拟器设置代理，鼠标左键长按，修改网络：

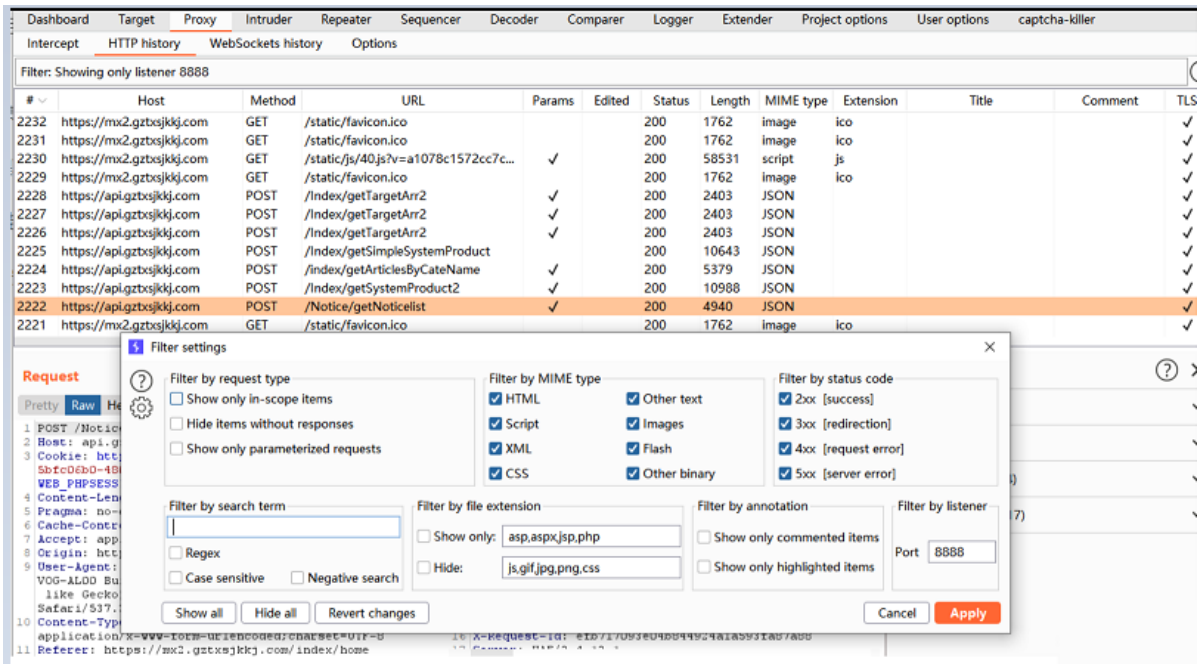


设置主机IP和端口号：

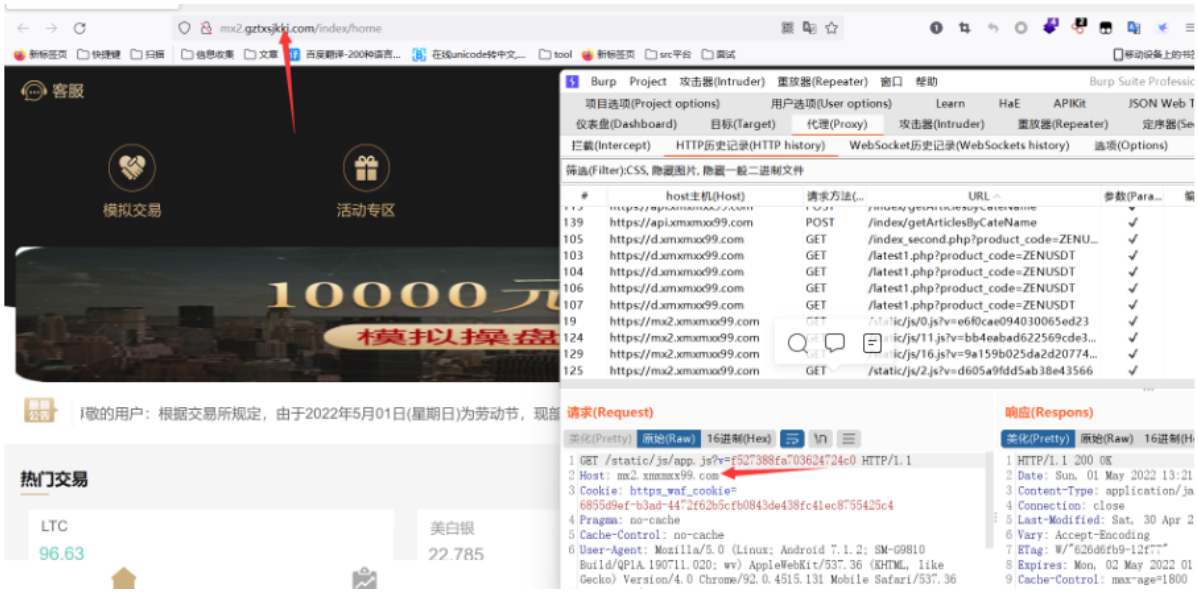


模拟器操作app，产生大量数据包history，进行筛选：



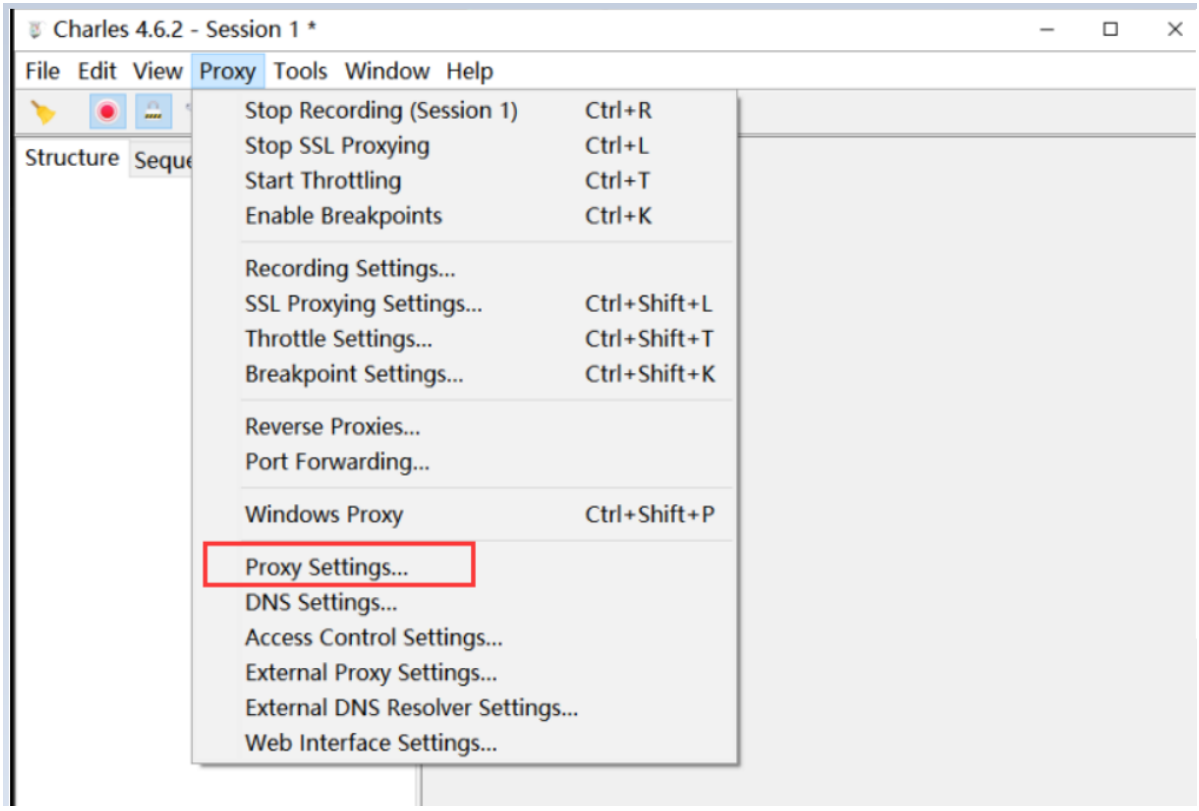


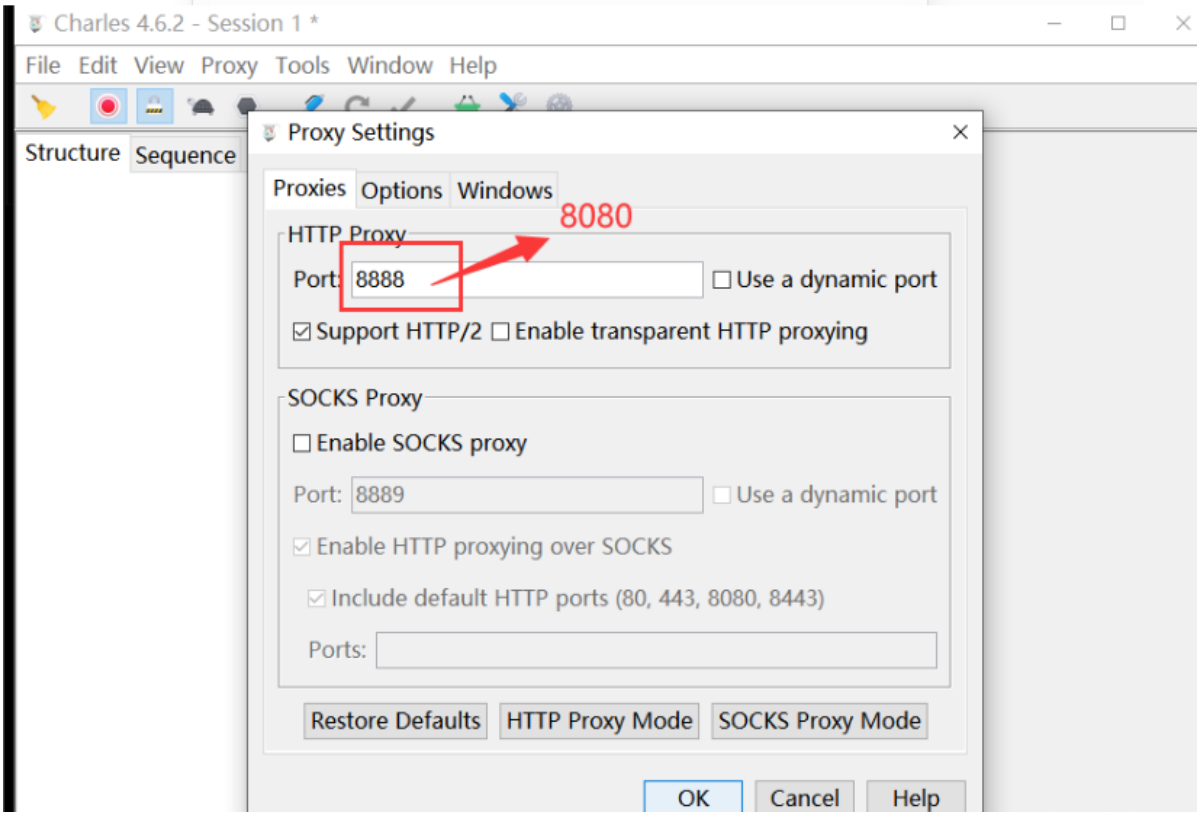
查看记录，访问网址，这个app的网址电脑也能访问，这就是个web站点：

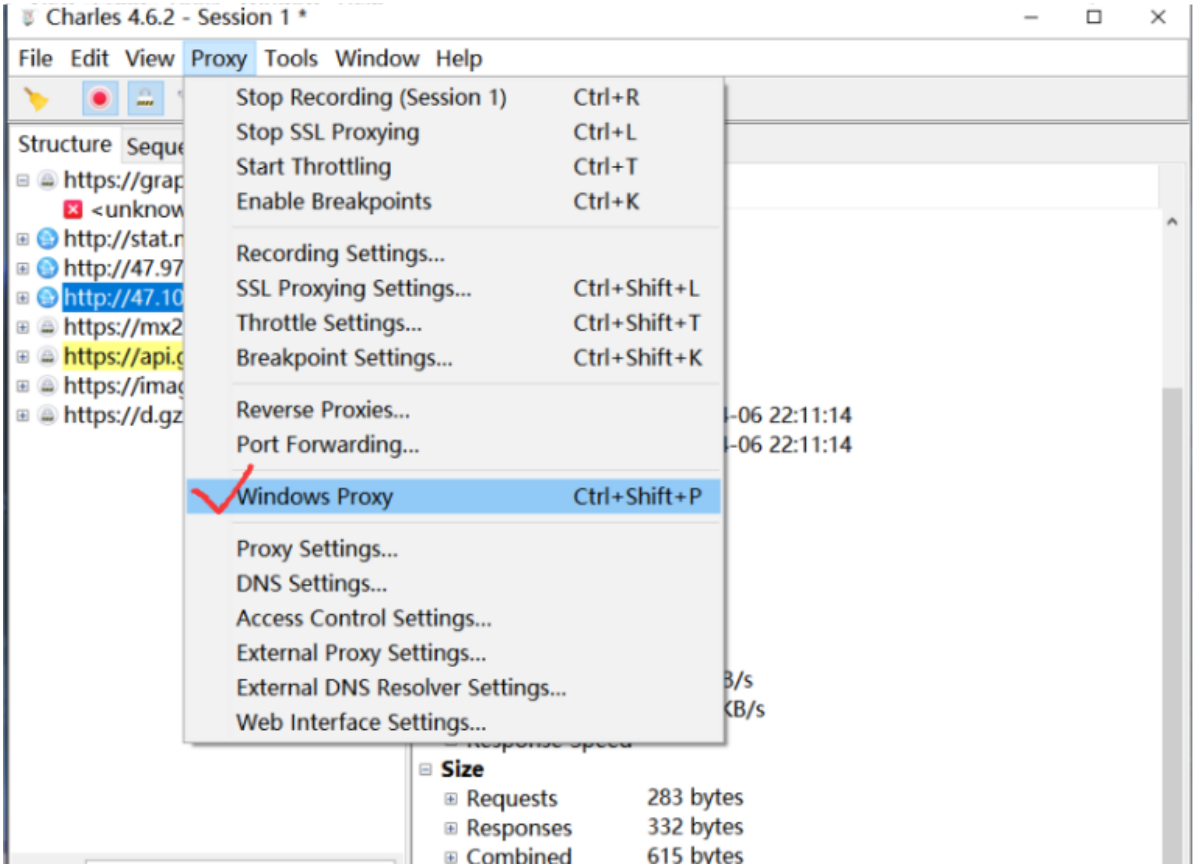


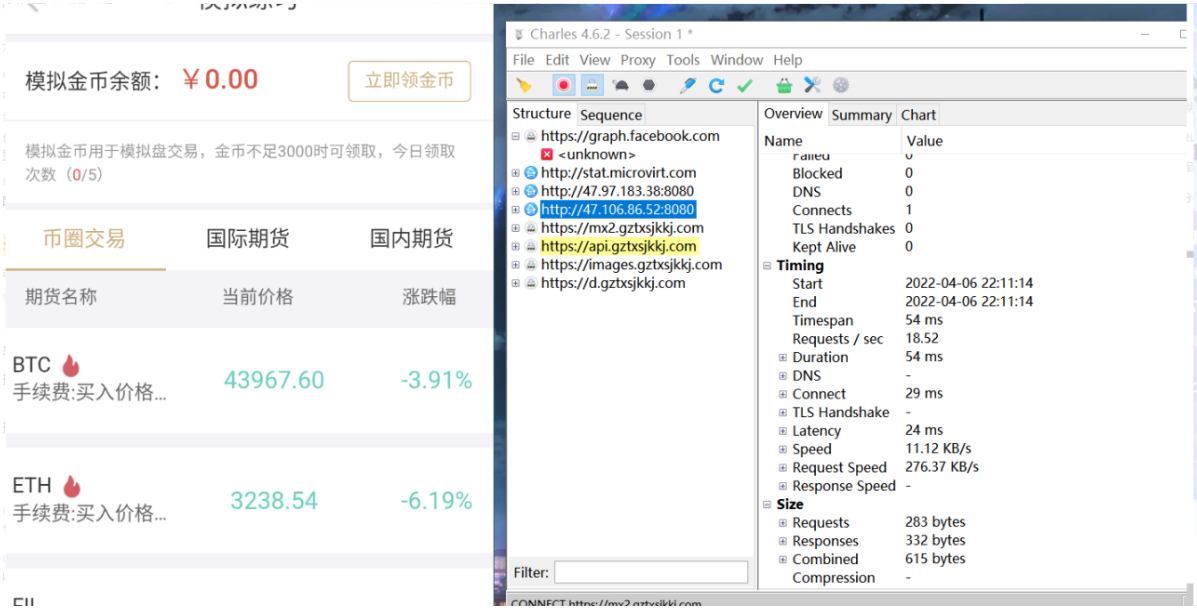
44.2.2 Charles软件使用

1. 抓包前设置代理：“Proxy”“Proxy Settings…”填写HTTP代理的端口，然后选择“Proxy”“Windows Proxy”
2. 使用需要抓包的app，产生大量数据包
3. Charles会将抓包产生的数据按网址分类，每次产生新数据时，对应的网址会有黄色高亮，注意排除调用接口
4. 选择网址会显示有关的数据，有的能够显示网站的结构，有的只能显示抓取的数据包
5. 将与app相关的网址输入到浏览器，无法访问，只有用手机的数据包才能访问
6. 只能修改数据包来访问，如何做漏洞扫描：在扫描工具的设置里面修改扫描的http头部/被动扫描




Charles 4.6.2 - Session 1 *
File Edit View Proxy Tools Window Help
Structure Sequence
Proxy Settings
Proxies Options Windows
8080
HTTP Proxy
Port: 8888
Use a dynamic port
Support HTTP/2
Enable transparent HTTP proxying
SOCKS Proxy
Enable SOCKS proxy
Port: 8889
Use a dynamic port
Enable HTTP proxying over SOCKS
Include default HTTP ports (80, 443, 8080, 8443)
Ports:
Restore Defaults
HTTP Proxy Mode
SOCKS Proxy Mode
OK
Cancel
Help


Charles 4.6.2 - Session 1 *
File Edit View Proxy Tools Window Help
Stop Recording (Session 1) Ctrl+R
Stop SSL Proxying Ctrl+L
Start Throttling Ctrl+T
Enable Breakpoints Ctrl+K
Recording Settings...
SSL Proxying Settings... Ctrl+Shift+L
Throttle Settings... Ctrl+Shift+T
Breakpoint Settings... Ctrl+Shift+K
Reverse Proxies...
Port Forwarding...
Windows Proxy Ctrl+Shift+P
Proxy Settings...
DNS Settings...
Access Control Settings...
External Proxy Settings...
External DNS Resolver Settings...
Web Interface Settings...
Size
Requests 283 bytes
Responses 332 bytes
Combined 615 bytes



电脑浏览器数据包：

```
GET //native/getMsgCount.do HTTP/1.1
Host: 373172.com:59789
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

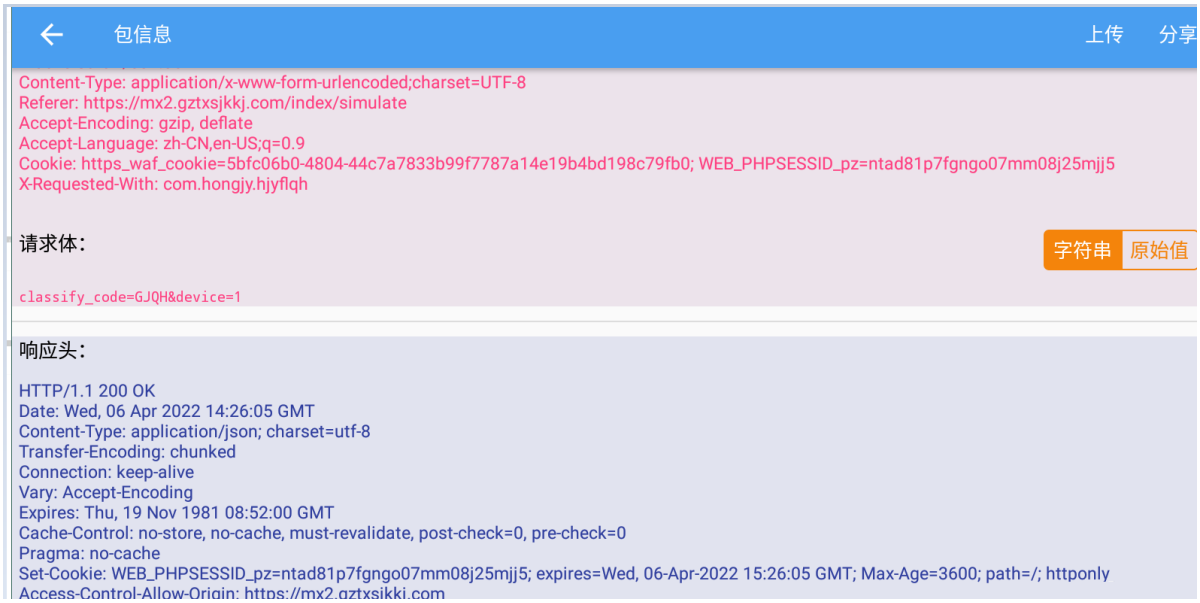
手机数据包：

```
GET /native/getMsgCount.do HTTP/1.1
Accept-Charset: UTF-8
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Connection: close
Accept-Language: UTF-8
X-Requested-With: XMLHttpRequest
Cookie: SESSION=b97bc076-ea55-4646-a9c9-d1f3a5feb8f0
User-Agent: android/v98.9.99923
Accept: application/xml
Connection: close
Accept-Language: zh-CN,en,*
Accept-Charset: utf-8
Host: 373172.com:59789
Accept-Encoding: gzip, deflate
```

44.2.3 抓包精灵app使用

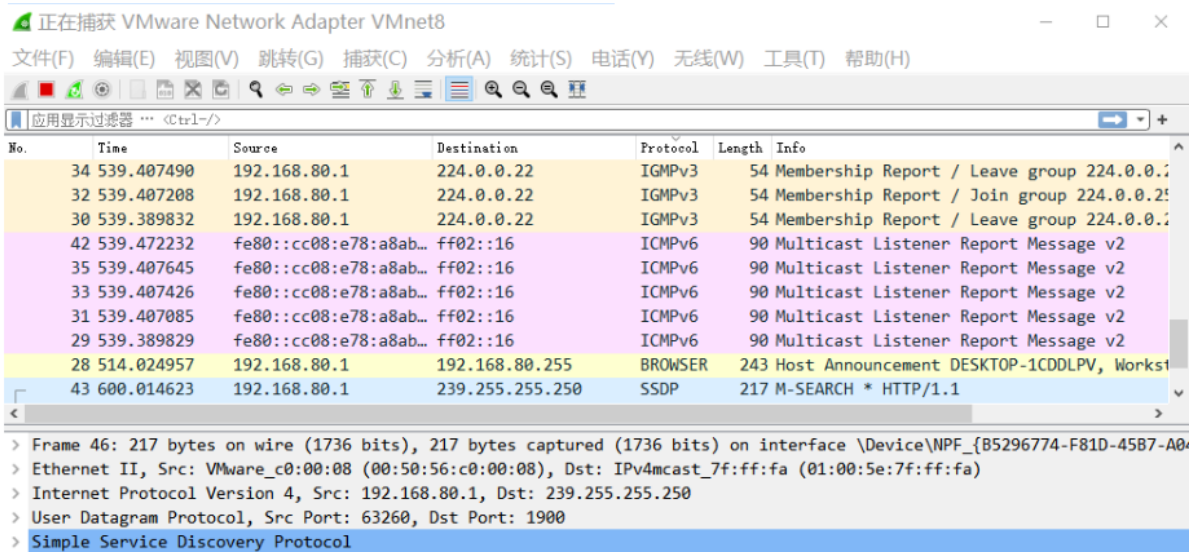
```
1  Android抓包软件，可以安装到手机上，不需要过多设置，即可抓住手机上app产生的http/https包并自动解析，确定是只能看不能操作。
2  地址：https://github.com/huolizhuminh/NetWorkPacketCapture/releases/tag/1.0.4
```

使用需要抓包的app，产生大量数据包,回到抓包精灵，数据包分条显示，内容包括app的图标和进程，点开有详细信息,抓包精灵只抓WEB协议:



44.2.4 wireshark–抓包工具非 WEB 协议面使用说明

选择要抓取的网络接口，由于手机模拟器使用的本机网络出口，所以这里抓取本机的网络出口，也就是“以太网”，显示的IP地址和本机的一致,软件左上方，红色方块表示暂停，蓝色鲨鱼鳍代表开始抓包，可以筛选,选择一条数据，下方会显示数据包的内容:



44.2.5 安卓逆向便捷 APK 一键提取 URL 演示

```
简介：一键提取安卓应用中可能存在的敏感信息。

用法：将所有app放到程序自动创建的apps目录，再运行主程序就好了，不用加参数。

功能：目前提取了APK内所有字符串、所有URLs、所有ip、可能是hash值的字符串、存在的敏感词（如oss.aliyun）、可能是accessKey的值。
```

44.2.6 利用 Burp 筛选及联动功能打出军体拳

```
xray 配置证书

burpsuite到“User options”“Connections”的“Upstream Proxy Servers”部分，添加一条代理规则：“Destination host”为“*”，意为转发一切内容，“Proxy host”为“127.0.0.1”，“Proxy port”填写一个未被占用的端口。别忘记勾选

在模拟器上将burpsuite设置为代理

```

```
管理员运行PowerShell，来到xray的文件夹，“.\xray_windows_amd64.exe”

执行命令“.\xray_windows_amd64.exe webscan --listen 127.0.0.1:端口号”来监听端口，端口号与前面一致

使用需要抓包的app，产生的数据因为代理会先发送到burpsuite，burpsuite再转发给xray

可以在xray再加参数，将扫描结果保存到本地

xray 下载地址 Releases · chaitin/xray (github.com)

webscan --listen 127.0.0.1 :6666
```

xray与burp联动被动扫描:

```
https://www.cnblogs.com/LOading/p/12388928.html
```

资源:

```
https://www.wireshark.org/download.html
https://www.charlesproxy.com/latest-release/download.do
https://github.com/huolizhuminh/NetWorkPacketCapture/releases
https://pan.baidu.com/s/1UGro7nQoBpT9vYRONsQi4w提取码: xiao
```