frida ssl unpinning

1. 电脑端安装frida

   首先你的电脑得有python3，没有你就装一个

   然后呢，解压frida+shell.zip，运行install_frida.bat文件。

   最后，推送frida-server到你的手机咯，我已经写好脚本了，大佬可以直接跑脚本。

   ```
   frida-server-arm.bat
   frida-server-arm64.bat
   frida-server-x86.bat
   ```

   三个脚本，根据处理器的型号不同区别，如果你不知道跑那个，就先跑第一个脚本。

2. 手机端安装burpsuite证书，配置手机代理端口

   请百度

3. frida ssl unpinning js脚本

   ```
   Java.perform(function() {
       var array_list = Java.use("java.util.ArrayList");
       var ApiClient = Java.use('com.android.org.conscrypt.TrustManagerImpl');
       // console.log('Start ssl bypass.');

       ApiClient.checkTrustedRecursive.implementation = function(a1,a2,a3,a4,a5,a6) {
           console.log('Bypassing SSL Pinning');
           var k = array_list.$new();
           return k;
       }
   },0);
   ```

   我已经修改为frida_android_bypass_ssl_pining.js

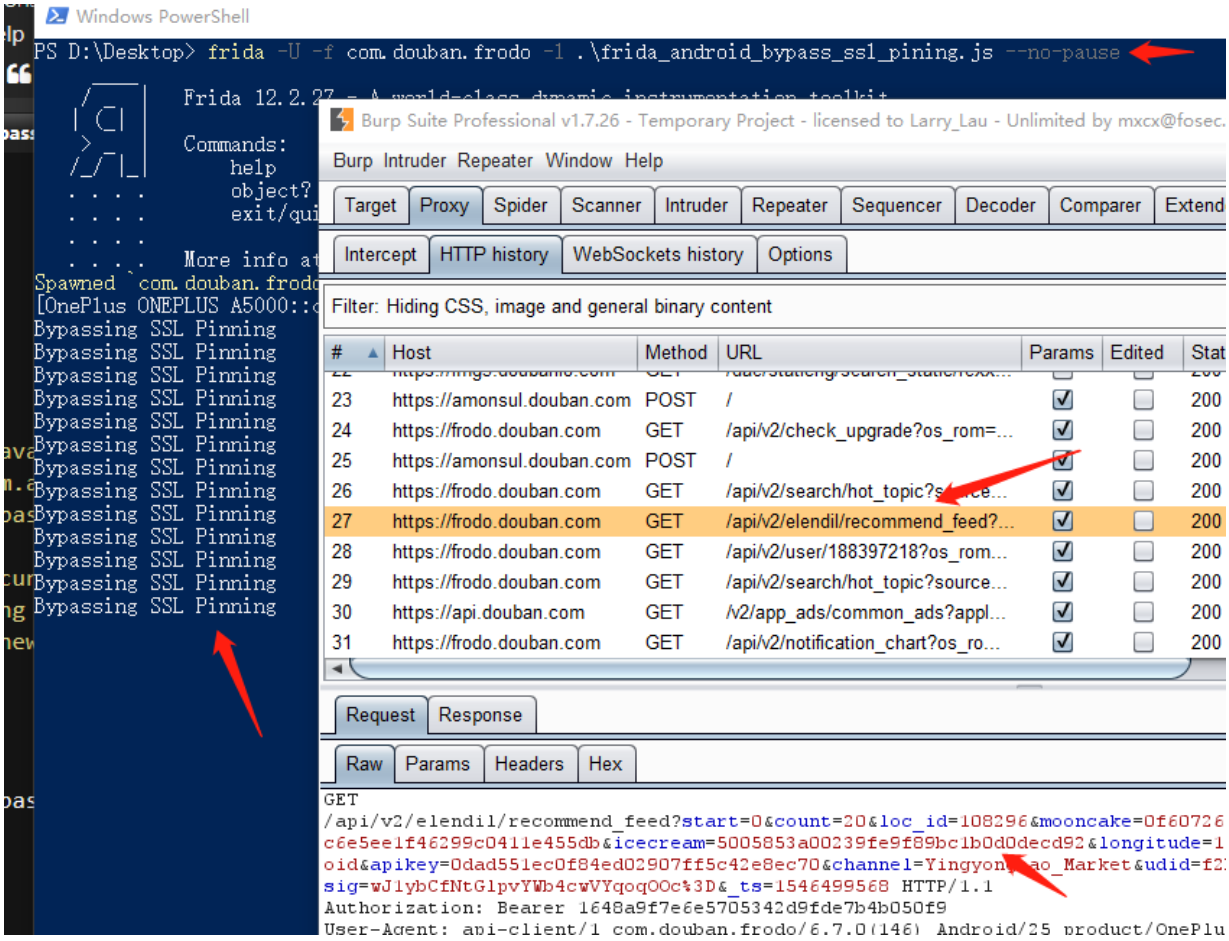
   先找到我们需要hook的进程

   ```
   frida-ps -U
   ```

   以豆瓣apk为例，豆瓣apk的进程名为com.douban.frodo，打开shell运行如下命令

   ```
   frida -U -f com.douban.frodo -l frida_android_bypass_ssl_pining.js --no-pause
   ```

   正常运行没有报错的话，就是如下图这样，你看，https的包就可以正常查看了。


Windows PowerShell
PS D:\Desktop> frida -U -f com.douban.frodo -l .\frida_android_bypass_ssl_pining.js --no-pause
Frida 12.2.27
Commands:
help
object?
exit/quit
More info at
Spawned `com.douban.frodo`
[OnePlus ONEPLUS A5000::com.douban.frodo]
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Bypassing SSL Pinning
Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extend
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Stat
23 https://amonsul.douban.com POST / 200
24 https://frodo.douban.com GET /api/v2/check_upgrade?os_rom=... 200
25 https://amonsul.douban.com POST / 200
26 https://frodo.douban.com GET /api/v2/search/hot_topic?s...ce... 200
27 https://frodo.douban.com GET /api/v2/elendil/recommend_feed?... 200
28 https://frodo.douban.com GET /api/v2/user/188397218?os_rom... 200
29 https://frodo.douban.com GET /api/v2/search/hot_topic?source... 200
30 https://api.douban.com GET /v2/app_ads/common_ads?appl... 200
31 https://frodo.douban.com GET /api/v2/notification_chart?os_ro... 200
Request Response
Raw Params Headers Hex
GET
/api/v2/elendil/recommend_feed?start=0&count=20&loc_id=108296&mooncake=0f60726
c6e5ee1f46299c0411e455db&icecream=5005853a00239fe9f89bc1b0d0decd92&longitude=1
oid&apikey=0dad551ec0f84ed02907ff5c42e8ec70&channel=Yingyon...ao_Market&udid=f2
sig=wJ1ybCfNtGlpvYWb4cwVYqoqOOc%3D&_ts=1546499568 HTTP/1.1
Authorization: Bearer 1648a9f7e6e5705342d9fde7b4b050f9
User-Agent: api-client/1 com.douban.frodo/6.7.0(146) Android/25 product/OnePlu