Fiddler代理抓包抖音提示网络错误的解决

转载

黑贝是条狗 于 2020-05-08 15:21:53 发布 10909 收藏 17
分类专栏： 其他 文章标签： http android
原文链接：https://jiezhe.net/post/68.html
版权

其他 专栏收录该内容
26 篇文章 0 订阅
订阅专栏

最近在折腾抖音，想抓一些数据，上Fiddler，设置好代理跟安装证书以后，抖音一直提示网络错误。但是浏览器什么的都是可以上网跟抓到包的，证明肯定不是Fiddler的错，折腾了半天，确认是安卓app抓包出现的https证书不被信任的问题。

解决起来也简单，在安卓里安装Xposed跟JustTrustMe模块就可以了。

Xposed到处都有，就不多说了，

安装完Xposed再安装JustTrustMe

JustTrustMe在https://github.com/Fuzion24/JustTrustMe/releases

JustTrustMe安装完后打开Xposed里的模块选项，打√，再重启安卓，抖音就可以正常被抓到包了。

----------分割线----------

20210916，最近上看雪，发现一个新方法，上面的可能都不能用了

抓包

当你信心满满的吧抓包环境配置的非常完美,准备大干一场的时候. 发现某音apk用了SSLPinning
又当大家信心满满的把frida过SSLPinning 以及xposed的justtrustme安装到手机上的时候再次打开apk,发现某音apk用的竟然是非系统的的ssl库

以上就是我的经历,为了各位同学不必走我的弯路,今天带大家解决一下如何去除这种sslpinng方案

最新版的某音用上了sslpinng技术,而且还是so层,导致很多想要一窥究竟的小伙伴抓不到包,让人十分头大.

这里给大家带来一个不需要frida hook 抓最新版包的方案!

本文中以17.3 32位某音apk为例

因为每次都frida hook libttboringssl.so 觉得十分繁琐,又想快速抓包.所以我用了Patch的方案

开工

打开某音的libsscronet.so 一顿乱找 然后根据关键字"SSL_CTX_set_custom_verify"找到

```
  v0[1] = 0;
  CRYPTO_library_init();
  *v0 = SSL_get_ex_new_index(0, 0, 0, 0);
  v1 = TLS_with_buffers_method();
  v2 = SSL_CTX_new(v1);
  sub_10FDC8(v0 + 1, v2);
  SSL_CTX_set_cert_cb(v0[1], sub_1CD190, 0);
  SSL_CTX_set_reverify_on_resume(v0[1], 1);
  SSL_CTX_set_custom_verify(v0[1], 1, sub_1CCAF0);
  SSL_CTX_set_session_cache_mode(v0[1], 769);
  SSL_CTX_sess_set_new_cb(v0[1], sub_1CD2D8);
  SSL_CTX_set_timeout(v0[1], 3600);
  v3 = SSL_CTX_set_grease_enabled(v0[1], 1);
  v4 = v0[1];
  v5 = sub_1C3ABC(v3);
  SSL_CTX_set0_buffer_pool(v4, v5);
  SSL_CTX_set_msg_callback(v0[1], sub_1CD428);
  SSL_CTX_add_cert_compression_alg(v0[1], 2, 0, sub_1CD4F4);
  if ( sub_17AD60(&off_2AF660) )
    SSL_CTX_set1_curves(v0[1], &unk_A17A4, 4);
  sub_17F920(&dword_2B4930, v0, 0, 0);
}
```

根据老哥所说 第三个参数就是校验的地方 并且是个回调函数,那我们就进去看看那

ps:恕我直言,没有ollvm是真的爽,ida看起来真是太过瘾了

```
text:001CCCAA                 MOV             R0, R4
text:001CCCAC                 BL              sub_1CCD28
text:001CCCB0
text:001CCCB0 loc_1CCCB0                                  ; CODE XREF: sub_1CCAF0+D0↑j
text:001CCCB0                 ADD             SP, SP, #0x94
text:001CCCB2                 POP.W           {R4-R11,PC}
text:001CCCB6 ; ---------------------------------------------------------------------------
text:001CCCB6
```

首先找到ret的地方,动下小手按下X键 查找引用 找到了一个

```
.text:001CCBBA                 BL              sub_1CD69A
.text:001CCBBE                 MOVS            R0, #0  ; Keypatch modified this from:
.text:001CCBBE                                         ;   MOVS R0, #1
.text:001CCBC0                 B               loc_1CCCB0
.text:001CCBC2 ; ---------------------------------------------------------------------------
```

看返回值是1,但是经过查阅发现 返回值为0的时候才是 **ssl_verify_ok**
所以我们动下小手给他改成0 然后这种点位一共有4个 ,全部保存为0 然后save一下

然后拿出我们心爱的安卓手机
adb shell
su
一顿操作 找到自己的17.3apk的安装位置

```
coral:/data/local/tmp #  cp libsscronet.so /data/app/com.ss.android.ugc.aweme-NBV5S-Lj6N_jj_Fjh6PBTw==/lib/arm/
coral:/data/local/tmp #
```

cp一下 然后
chgrp system libsscronet.so
chown system libsscronet.so
chmod 777 libsscronet.so

然后打开某音就会神奇的发现自己可以抓包啦,理论上所有版本通杀,只要找到关键字

如果不想动小手patch的同学,这里也有一份小弟搞好的32位的17.3版本的so 可以手动下载食用

记得流程哦 找到自己/data/data/下的某音安装目录 然后cp进去 设置个权限就可以愉快食用了哦

地址：[原创] 听说最新版的某音大家都抓不到包,给大家一个方案-Android安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com[原创] 听说最新版的某音大家都抓不到包,给大家一个方案 https://bbs.pediy.com/thread-269028.htm