漏洞概要

缺陷编号： **WooYun-2013-17543**
漏洞标题： 金山快盘手机客户端任意进入他人快盘账号
相关厂商： **金山网络**
漏洞作者： **horseluke**
提交时间： 2013-01-19 17:26
公开时间： 2013-02-28 14:39
漏洞类型： 设计错误/逻辑缺陷
危害等级： 高
自评Rank： 15
漏洞状态： 厂商已经确认
漏洞来源： **http://www.wooyun.org**，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签： 无
分享漏洞：

漏洞详情

披露状态：

2013-01-19： 细节已通知厂商并且等待厂商处理中
2013-01-20： 厂商已经确认，细节仅向厂商公开
2013-02-28： 厂商提前公开漏洞，细节向公众公开

简要描述：

本节目由@imlonghao 独家赞助复测。

（片头）
云端存储，快捷方便。（同期声顾客："通过网盘我就可以在安卓看小说了"）
抓包修改，任意进入。（同期声安全研究者："改几个字节，你的隐私文件就一览无余"）
是什么，让快盘手机版出现漏洞？（同期声快盘竞争对手（某网盘）研发者："一身冷汗，我们侥幸没让用第三方账号登录而已"）
云时代的认证传递，应该由谁保障？（同期声记者："当我们还在打口水仗推脱谁该负责的时候，用户已在云中遭受不测"）

《wooyun调查》即将播出《云安全的认证困惑》。

（以上文体仿CCTV新闻频道《新闻调查》，在此致谢。）

详细说明：

金山快盘手机客户端，在使用微博OAuth 2.0授权信息换取自己认证信息的过程中，一次性犯下两类常见的逻辑设计缺陷，导致可以任意进入他人快盘账号；但前提是，快盘帐号需要绑定微博。

具体犯下的错误有：

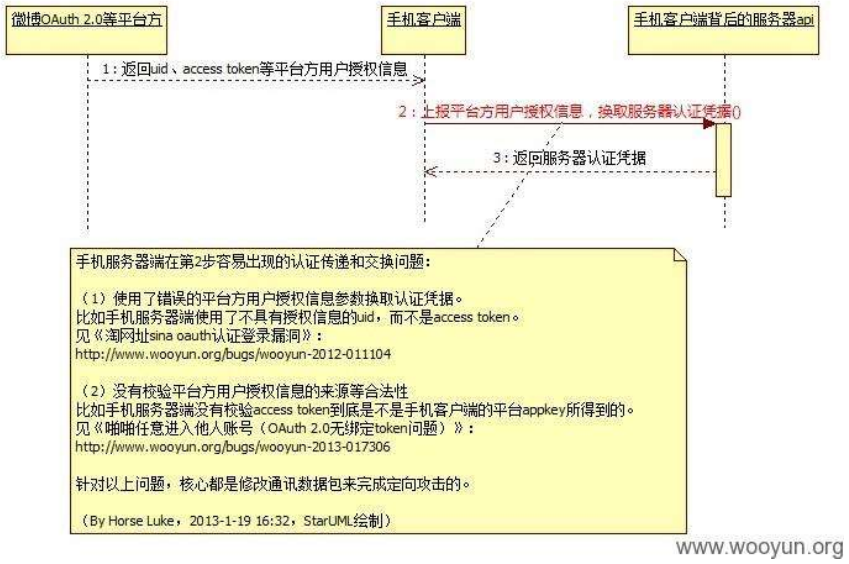
（问题一）OAuth 2.0无绑定token问题：由于OAuth 2.0的"无绑定token"特性（http://**.**.**.**/view/50978/307535 ），导致第三方应用在使用平台方的OAuth 2.0授权（authorize）作为自身应用的认证（authenticate）手段时，缺乏一种有效的认证传递校验和来源检查，从而导致只需要拥有B应用的access token，即可登录到A应用所绑定的服务中。

此案例可见：http://**.**.**.**/bugs/wooyun-2013-017306

（问题二）使用错误的OAuth授权信息来用于认证交换：使用了uid来认证用户信息，而不是access token

此案例可见：http://**.**.**.**/bugs/wooyun-2012-011104

本来想复测其它公司的网盘，但发现他们碰巧都没有提供微博登录，所以侥幸逃脱此问题。但相信一旦开启，估计也很容易中招。故而此种手机客户端威胁云端安全的案例，需要手机开发者（比如说使用了新浪微博sso sdk的开发者）和相关后端留意（见图）。



而这个漏洞还反映出一个问题：Oauth 2.0作为一个框架协议，其中有许多安全细节实际上需要开发者自行去实现，如果平台方将安全细节全部包揽在身上显然是不合适的；但如果将安全细节下放到应用开发者自行保证，那么就很容易出现实现不周而反噬双方，特别在认证传递和交换上会是一个重灾区。如何划分，成为了一个值得研究的后续方向。但无论我们如何争论，用户和黑客已经等不及了……

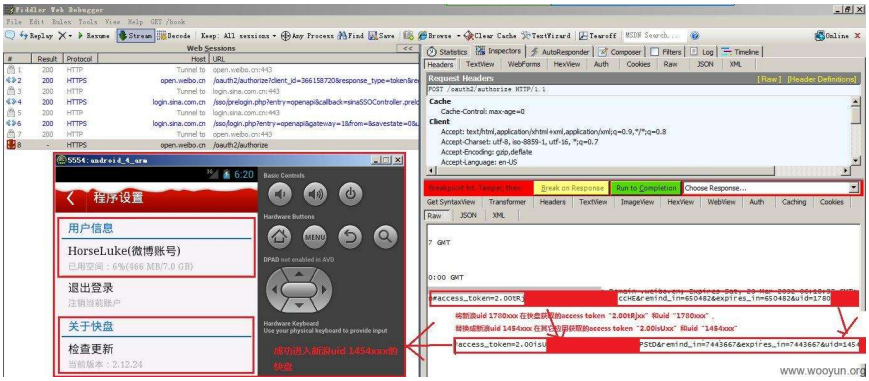
漏洞证明：

问题一证明：

OAuth 2.0无绑定token问题，通过拦截新浪微博返回的access token信息，修改成他人的access token和新浪uid，即可进入他人快盘。请注意，这个access token可以使用其它应用获取到的access token。

修改难度中低，因为需要知道受害者在其它应用的access token。此时，一般需要诱骗受害者授权攻击者指定的应用，才可以完成攻击。

（微博授权过程中，我使用了新浪uid 1780xxx登录；然后在下一步登录成功后截获，并将新浪uid 1780xxx在快盘获取的access token“2.00tRjxx”和uid“1780xxx”，替换成新浪uid 1454xxx在其它应用获取的access token“2.00isUxx”和uid“1454xxx”，成功）

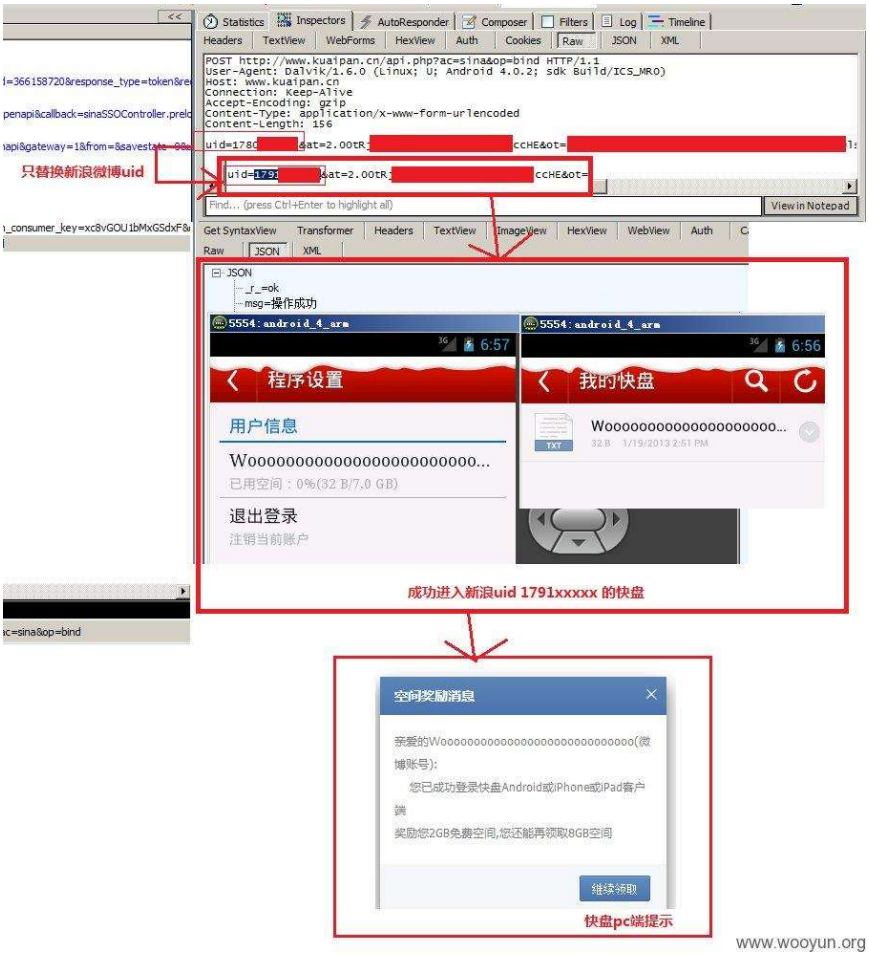


问题二证明：

使用错误的OAuth授权信息获取，通过拦截要往快盘后端服务器api的数据，将新浪uid替换，即可进入他人网盘。

修改难度低，只需要知道新浪uid即可，同时也需要知道该新浪uid曾登录过快盘。

（微博授权过程中，我使用了新浪uid 1780xxx登录；然后在快盘往后端服务器api发送数据前截获，并替换成新浪uid 1791xxxx，成功）



修复方案：

危害评定：

就快盘而言，综合认定为“高”。原因如下：

（1）问题一中，要获取用户的access token比较容易，只需要注册第三方应用并诱导用户授权即可。

（2）问题二中，要获取用户的新浪uid极容易，只需要微博搜索即可获知。

（3）定向攻击容易，只需要修改数据包；最终成功率极高，并且只要用户不修改密码，即有永久进入权限。

（4）快盘的用户基数大。

（5）是否有用于access token的来源查询、证明或签名校验，要视乎开放平台的提供情况。如果有，只需要在服务器端修复一般可解决新绑定和登录的漏洞。

修复建议：

（1）手机服务器端，在接收手机客户端的平台认证信息、以换取自家服务的认证凭据时，不能使用没有授权信息的uid来认证换取，而是必须使用具有授权信息的access token来进行；并且必须要对access token进行来源查询、证明或签名校验。

具体而言，已查证的国内各开放平台已知的接口文档如下：

（A）新浪微博开放平台“授权查询”：

http://**.**.**.**/wiki/Oauth2/get_token_info

（B）QQ登录：通用参数中似乎已经进行了此问题的防御（时间问题未验证）：

http://**.**.**.**/wiki/%E3%80%90QQ%E7%99%BB%E5%BD%95%E3%80%91OpenAPI2.0%E8%B0%83%E7%94%A8%E8%AF%B4%E6%98%8E#2._.E8.B0.83.E7.94.A8OpenAPI.E6.8E.A5.E5.8F.A3

（C）百度开放平台“判定当前用户是否已经为应用授权”（此接口本人未验证是否可防御此问题，请咨询百度开放平台）：

http://**.**.**.**/wiki/index.php?title=docs/oauth/rest/file_data_apis_list#.E5.88.A4.E5.AE.9A.E5.BD.93.E5.89.8D.E7.94.A8.E6.88.B7.E6.98.AF.E5.90.A6.E5.B7.B2.E7.BB.8F.E4.B8.BA.E5.BA.94.E7.94.A8.E6.8E.88.E6.9D.83

（D）人人网“判断用户是否已对App授权”（此接口本人未验证可否可防御此问题，请咨询人人开放平台）：

http://**.**.**.**/wiki/Users.isAppUser

其它开放平台，建议进行相关问题的咨询。

（2）对所有存入的绑定access token进行核查，发现access token中的新浪uid和绑定新浪uid不一致、非快盘appkey授权的access token、过期access token等异常情况均需要全部撤消，要求这些快盘用户重新授权登录。

（3）各开放平台加强教育，提醒开发者注意上述问题。

漏洞回应

厂商回应：

危害等级：高

漏洞Rank：19

确认时间：2013-01-20 15:37

厂商回复：

非常感谢，我们将尽快进行确认和修复。

给高分的原因：

1）安全风险综合考虑为高危；

2）漏洞反馈者在漏洞演示、安全建议都非常详细，非用心；

最新状态：

2013-02-28：已经修复。 这么优秀的案例，我们将提前公开，希望让更多的朋友可以学习与借鉴。

漏洞评价：

对本漏洞信息进行评价，以更好的反馈信息的价值，包括信息客观性，内容是否完整以及是否具备学习价值

漏洞评价(共8人评价)：

登陆后才能进行评分

100%

0%

0%
0%
0%

评价

2013-01-19 17:32 | imlonghao (普通白帽子 | Rank:740 漏洞数:75) 0

................你还真这么写

1#

2013-01-19 17:34 | horseluke (普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.) 0

@imlonghao 感谢你是必须的

2#

2013-01-19 18:13 | 小胖子 认证白帽子 (核心白帽子 | Rank:1888 漏洞数:156 | 不要患得患失，我羡慕你，但是我还是选择做...) 0

片头给力！

3#

2013-01-19 18:55 | gainover 认证白帽子 (普通白帽子 | Rank:1805 漏洞数:97 | PKAV技术宅社区! -- gainover| 工具猫网络-...) 0

前排支持， 目前手机上的应用，在安全方面的考虑是个问题。

4#

2013-01-19 18:57 | xsser 认证白帽子 (普通白帽子 | Rank:297 漏洞数:22 | 当我又回首一切,这个世界会好吗?) 0

@gainover 这些人才应该写小说

5#

2013-01-19 18:59 | horseluke (普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.) 0

@xsser 我只能写纪实小说...

6#

2013-01-19 21:27 | 风萧萧 认证白帽子 (核心白帽子 | Rank:1070 漏洞数:81 | 人这一辈子总要动真格的爱上什么人) 0

碉堡，肿么没人气.

7#

2013-01-19 22:17 | 蓝风 (普通白帽子 | Rank:125 漏洞数:25 | 東汸慾哓 嗼樋糿圷皁 沓鍽圊屾亾沬荖 彨慏...) 0

《wooyun调查》首播：每周六 21:30

8#

2013-01-19 22:28 | zeracker 认证白帽子 (普通白帽子 | Rank:1077 漏洞数:139 | 爱吃小龙虾。) 0

湖南人民发来贺电！

9#

2013-01-19 23:21 | txcbg (普通白帽子 | Rank:392 漏洞数:54 | 说点什么呢？) 0

关系具体细节

10#

2013-01-19 23:40 | 冷静 (路人 | Rank:3 漏洞数:2) 0

测试过程有点繁琐吧~大约感觉到怎么个情况了

11#

2013-01-20 02:49 | circus (实习白帽子 | Rank:54 漏洞数:4 | 你会为一件事去说一句话,也会为一句话去干...) 0

上次研究快盘客户端过，觉得这里隐约会出现问题。。坐等公开。

12#

2013-01-20 02:50 | 鬼魅羊羔 (普通白帽子 | Rank:299 漏洞数:42 | (#'′)凸(#'′)凸(#'′)凸(#'′)凸(#`...) 0

@circus 等吧，看看冲哥怎么说。。

13#

2013-01-20 09:57 | f1eecy (路人 | Rank:21 漏洞数:4 | 图书管理员~) 0

V5 安卓和ios通杀吗？

14#

2013-01-20 15:51 | imlonghao (普通白帽子 | Rank:740 漏洞数:75) 0

19~

15#

2013-01-20 17:28 | xsser 认证白帽子（普通白帽子 | Rank:297 漏洞数:22 | 当我又回首一切,这个世界会好吗?） 0

厂商靠谱

16#

2013-01-20 18:04 | se55i0n（普通白帽子 | Rank:1571 漏洞数:174） 0

哇塞~碉堡了~文艺范儿呀

17#

2013-01-20 18:06 | Coody 认证白帽子（核心白帽子 | Rank:1809 漏洞数:214 | 不接单、不黑产；如遇冒名顶替接单收徒、绝...） 0

厂商回复的最后一句话→→→→→→→→非用心

18#

2013-01-21 08:52 | 围剿（路人 | Rank:17 漏洞数:5 | Evil decimal） 0

作者赤裸裸的文艺范！

19#

2013-01-26 18:53 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

复核：已修复

20#

2013-01-30 15:46 | imlonghao（普通白帽子 | Rank:740 漏洞数:75） 0

@horseluke 那我就转载了！

21#

2013-01-30 21:32 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

@imlonghao 你先别这么急吧...免得又一轮各厂商借机炒作，我都怕了！

22#

2013-01-30 21:56 | imlonghao（普通白帽子 | Rank:740 漏洞数:75） 1

@horseluke 那好吧...

23#

2013-02-20 09:31 | han（路人 | Rank:16 漏洞数:5 | http://www.zzidc.com/SSL） 0

写的真好

24#

2013-02-21 10:36 | qiaoy（普通白帽子 | Rank:122 漏洞数:17） 0

评5星！

25#

2013-03-01 12:37 | 梦琳（实习白帽子 | Rank:69 漏洞数:9 | 追寻梦的足迹！） 0

学习！

26#

2013-04-03 20:17 | wefgod（核心白帽子 | Rank:1829 漏洞数:183 | 力不从心） 0

这个写的太好了

27#

2013-12-07 22:46 | iv4n（实习白帽子 | Rank:49 漏洞数:10） 1

@horseluke, 个人觉得uid那个问题，更多应该是 授权平台方 的问题，授权方 按照标准走，api的认证是access token, 而不引导用户通过uid去使用api， 只会存在无绑定token的问题（利用没这么容易，所以漏洞的危害远远没这么大），但是如果使用uid，暴力猜解和获取的手段比token轻松太多了，

28#

登录后才能发表评论，请先 登录 。