漏洞概要

关注数(35) 关注此漏洞

缺陷编号： **WooYun-2013-17306**
漏洞标题： 啪啪任意进入他人账号（OAuth 2.0无绑定token问题）
相关厂商： **啪啪**
漏洞作者： **horseluke**
提交时间： 2013-01-14 18:32
公开时间： 2013-02-28 18:32
漏洞类型： 设计错误/逻辑缺陷
危害等级： 中
自评Rank： 10
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： **OAuth** **认证交换**
分享漏洞： 分享到 2

19人收藏 收藏

漏洞详情

披露状态：

2013-01-14： 细节已通知厂商并且等待厂商处理中
2013-01-15： 厂商已经确认，细节仅向厂商公开
2013-01-18： 细节向第三方安全合作伙伴开放（绿盟科技、唐朝安全巡航、无声信息）
2013-03-11： 细节向核心白帽子及相关领域专家公开
2013-03-21： 细节向普通白帽子公开
2013-03-31： 细节向实习白帽子公开
2013-02-28： 细节向公众公开

简要描述：

啪啪的移动端安全其实是不错的，只是碰巧在OAuth 2.0协议的实现上躺枪了。囧，OAuth 2.0还有多少个坑大家还得中啊？Eran Hammer，你画圈圈诅咒千万别应验.....

此案例在公开后，各开放平台、以及依赖各OAuth平台登录的客户端开发者（典型如手机应用）可以注意一下。理论上，遇到此问题的概率不甚大，至少我半个多月断断续续地大海捞针，才找到一两家存在此问题。

详细说明：

该漏洞原型可见2012年6月份由微软研究组报给IETF的邮件安全案例：http://**.**.**.**/mail-archive/web/oauth/current/msg09270.html

在OAuth协议上，该漏洞分属OAuth 2.0无绑定token问题：由于OAuth 2.0的"无绑定token"特性（http://**.**.**.**/content/674 ），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。

在漏洞本质上，该漏洞分属于认证交换的信任检查问题：当攻击者给出一个认证凭据时，如果服务器没对此认证凭据进行来源等校验，那么攻击者就能成功完成认证交换，从而造成问题。（可以类比"xss盲打后台获得cookies登录"来理解）

啪啪手机客户端极度依赖OAuth平台登录，因此它就容易产生这种问题。啪啪的登录流程可简化如下：

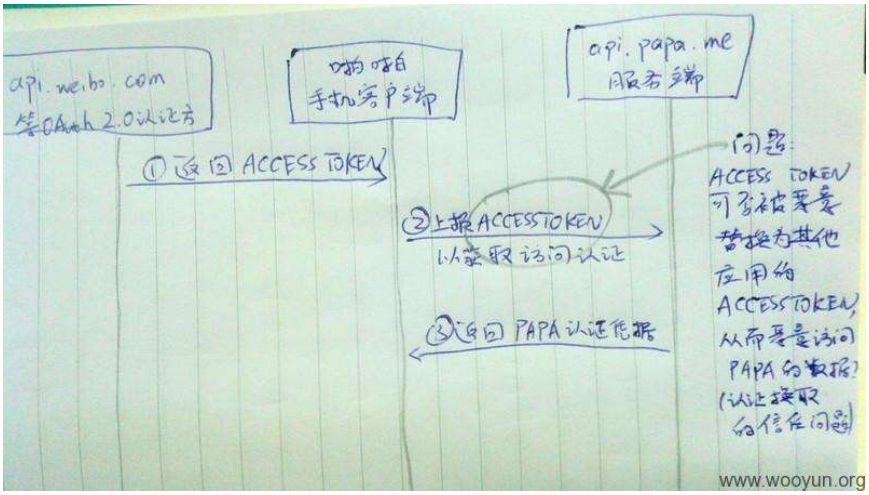
（1）用户点击用新浪微博或者QQ登录，将弹出OAuth平台方的授权页面

（2）用户点击授权后，啪啪客户端获得OAuth平台方给出的access token

（3）啪啪客户端将此access token上报给api.papa.me接口，以获取啪啪的认证字符串

（4）啪啪得到此认证字符串后，即有权限操作绑定的啪啪数据。

那么这个问题就在于，如果有方法可以恶意替换OAuth平台方给出的access token，那是否就以进入他人的啪啪账号？实验证明，是可行的。



漏洞证明：

由于啪啪的代码混淆得比较多，个人时间上不允许进行全脱离模拟，所以在这里也只是在传输过程取了个巧，证明问题就可以了。

（1）配置fiddler2，使得android模拟器等一定可以解密微博api的数据；

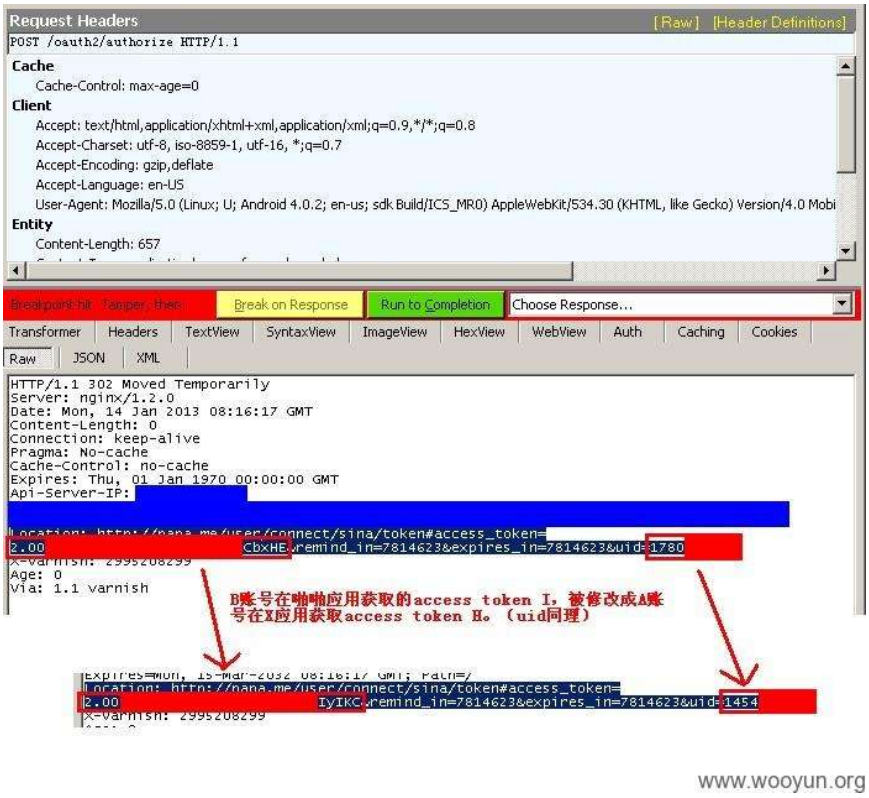
（2）在网页端上，以A账号在X应用获取access token H。

（3）在手机上安装啪啪客户端；fiddler设置为返回拦截。

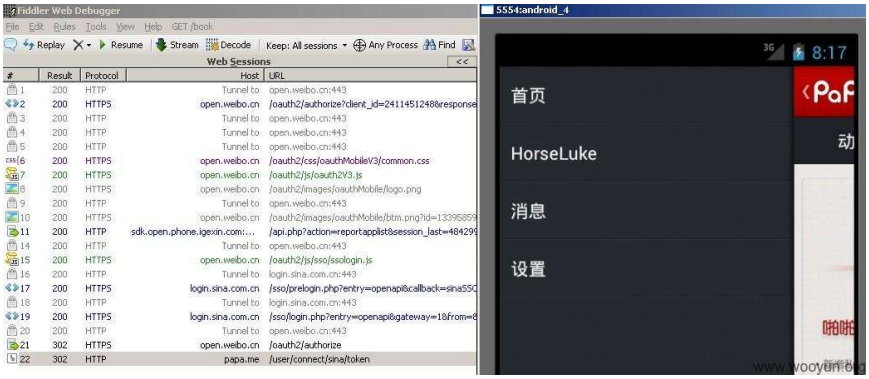
（4）启动啪啪，点击用新浪微博登录，在弹出OAuth平台方的授权页面上输入B账号，并点击授权

（5）在fiddler中，可以找到B账号在啪啪应用获取的access token I。

修改拦截内容，变成A账号在X应用获取到的access token H。



（6）登录到A账号成功。



修复方案：

危害性：

这个漏洞主要危害那些存在认证传递和交换的服务，目前比较常见的场景是用OAuth登录到自家的服务中可能会有这个疏漏。

就啪啪而言，综合认定为“中高”。原因如下：

（1）要获取用户的access token很容易，只需要注册第三方应用并诱导用户授权即可；

（2）定向攻击的最终成功率极高。

（3）啪啪的用户基数大。

（4）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即可解决此问题。

修复建议：

（1）手机客户端有关认证交换的主体部分，一定要有一个服务器把关，这是最基础的。

（2）手机服务器端在接收手机客户端的access token来对换取自家服务的认证凭据时，必须对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。

漏洞回应

厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2013-01-15 09:52

厂商回复：

十分感谢 horseluke 对啪啪安全方面的贡献，已经确认这个漏洞是我们考虑不周全导致.

最新状态：

暂无

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3人评价)：

登陆后才能进行评分

100%

0%

0%

0%

0%

评价

2013-01-14 18:45 | Claud（普通白帽子 | Rank:161 漏洞数:18 | secmobi.com） 0

关注下。最近也发现一个OAuth相关的问题，还没上报。

1#

2013-01-14 18:53 | 疯狗 认证白帽子（实习白帽子 | Rank:44 漏洞数:2 | 阅尽天下漏洞，心中自然无码。） 0

OAuth对于初学者来说很混乱，换来换去的key，token啥的，洞主考虑给drops投稿不？

2#

2013-01-14 18:54 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

@Claud ，我完成这项问题的排查后，OAuth的东西基本就差不多完毕了。未来想研究什么，甚感迷惘...

3#

2013-01-14 18:58 | 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

@horseluke 不搞未来搞现在啊

4#

2013-01-14 18:58 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

@疯狗 协议没读过，现在都是基于实践层面，实在不敢写...

5#

2013-01-14 19:10 | 疯狗 认证白帽子（实习白帽子 | Rank:44 漏洞数:2 | 阅尽天下漏洞，心中自然无码。） 0

@horseluke 实践才是真理啊

6#

2013-01-14 19:38 | Claud（普通白帽子 | Rank:161 漏洞数:18 | secmobi.com） 0

@horseluke 加Q私聊.....刚打了一些字准备回复，发现是下下个月要发的内容，还是先不公开吧。

7#

2013-01-14 20:16 | 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

@Claud 干嘛不发乌云

8#

2013-01-14 20:21 | 小胖胖要减肥 认证白帽子（普通白帽子 | Rank:686 漏洞数:101 ） 0

@疯狗 @xsser 找马甲胖投稿啊，剑心你懂的

9#

2013-01-14 21:04 | Claud（普通白帽子 | Rank:161 漏洞数:18 | secmobi.com） 0

@xsser 说的是被约稿的技术文章，不是洞。另外Android系统的0洞我直接报Google了……

10#

2013-01-15 10:47 | se55i0n（普通白帽子 | Rank:1571 漏洞数:174 ） 0

@xsser @疯狗 最近发什么类型的洞都不能秒了，大婶RP要这么补呀？

11#

2013-01-19 01:47 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

@啪啪 ，验证已修复

12#

2013-01-19 01:48 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

@啪啪 ，验证已修复。PS：在android模拟器的intel镜像下，啪啪老出错闪退

13#

2013-02-04 09:54 | se55i0n（普通白帽子 | Rank:1571 漏洞数:174 ） 0

@horseluke 楼主过程写的很详细，很赞！

14#

2013-02-20 09:47 | 白胡子（路人 | Rank:24 漏洞数:3 ） 0

写得很详细,感谢分享

15#

2013-02-21 08:51 | 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

感谢分享~

16#

2013-02-28 15:28 | horseluke（普通白帽子 | Rank:116 漏洞数:18 | Realize the dream in earnest.） 0

缺陷关联： WooYun: 金山快盘手机客户端任意进入他人快盘账号

17#

2015-03-15 23:57 | mango（核心白帽子 | Rank:2165 漏洞数:312 | 解决问题的第一步，是要承认问题的存在。） 0

博主 撸的一手好字体@@

18#

登录后才能发表评论，请先 登录 。