神州租车APP客户端设计缺陷导致的一系列安全问题（算法破解/权限遍历等）

**漏洞概要**

缺陷编号： [**WooYun-2015-105766**](http://10.199.252.80:8080/bugs/wooyun-2015-0105766)

漏洞标题： 神州租车APP客户端设计缺陷导致的一系列安全问题（算法破解/权限遍历等）

C:\F25ADB45\E86A91B9-CDD7-491D-B289-526C3827D459.files\image001.png

相关厂商： [**神州租车**](http://www.wooyun.org/corps/%E7%A5%9E%E5%B7%9E%E7%A7%9F%E8%BD%A6)

漏洞作者： [**feng**](http://www.wooyun.org/whitehats/feng)

提交时间： 2015-04-10 13:45

公开时间： 2015-07-09 15:00

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**](http://www.wooyun.org/)

Tags标签： [**客户端程序设计错误**](http://10.199.252.80:8080/tags/%E5%AE%A2%E6%88%B7%E7%AB%AF%E7%A8%8B%E5%BA%8F%E8%AE%BE%E8%AE%A1%E9%94%99%E8%AF%AF)

**12**人收藏 [收藏](javascript:void(0))

分享漏洞：

C:\F25ADB45\E86A91B9-CDD7-491D-B289-526C3827D459.files\image002.jpg

**漏洞详情**

披露状态：

2015-04-10： 细节已通知厂商并且等待厂商处理中

2015-04-10： 厂商已经确认，细节仅向厂商公开

2015-04-13： 细节向第三方安全合作伙伴开放

2015-06-04： 细节向核心白帽子及相关领域专家公开

2015-06-14： 细节向普通白帽子公开

2015-06-24： 细节向实习白帽子公开

2015-07-09： 细节向公众公开

简要描述：

神州租车APP客户端设计缺陷导致的一系列安全问题

详细说明：

首先先列举一下安卓客户端的一些问题：

1、allowBackup="true"

2、代码未做混淆

3、未做重打包防护

4、使用AES对称加密算法，且秘钥硬编码

5、调试代码过多

对于第一个问题本文将不做证明，危害请看http://www.droidsec.cn/%E8%AF%A6%E8%A7%A3android-app-allowbackup%E9%85%8D%E7%BD%AE%E5%B8%A6%E6%9D%A5%E7%9A%84%E9%A3%8E%E9%99%A9/

本文将重点说明使用AES加密算法且秘钥硬编码带来的危害。

AES是对称加密算法，即加密秘钥和解密秘钥是一样的，当其秘钥硬编码的时候，则无法起到真正隐藏信息的作用。

漏洞证明：

下面将一步一步讲解如何解密神州租车安卓APP客户端请求数据从而进行攻击。

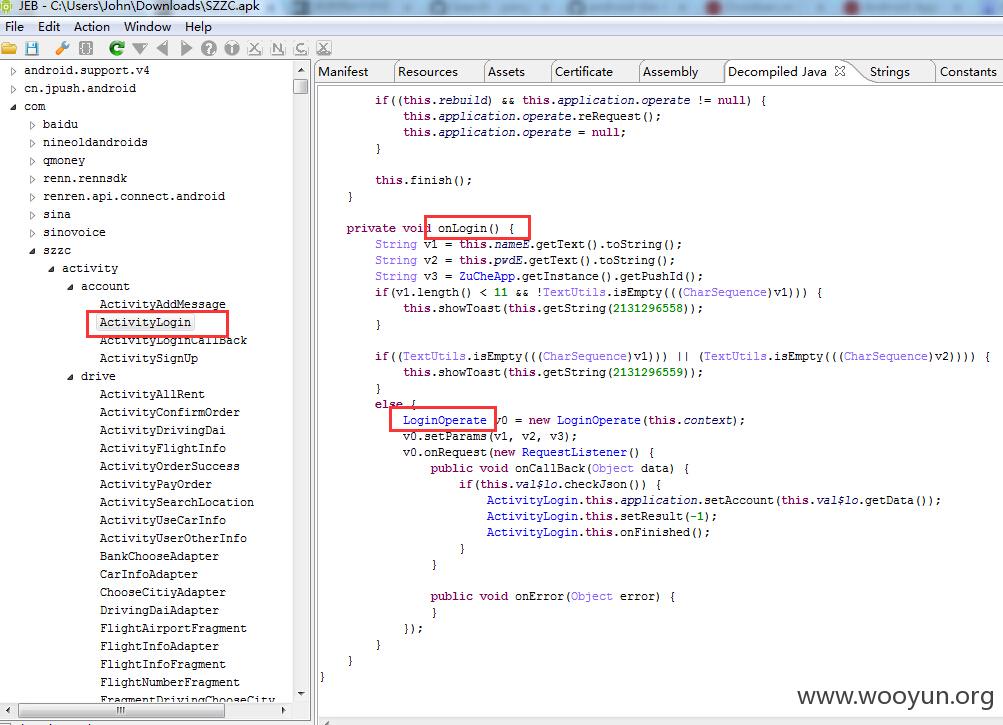
首先，通过burp代理app的数据，抓包如下：

<http://mapi.zuche.com/m/order/queryShortOrderList.action?cid=100305&uid=ca92db58-3046-455f-a333-3194aa8590f5&q=IpoxHm9eMFWsQi%2br867eFaAKiSNt7WuTELTu7oOqqoI%3d>

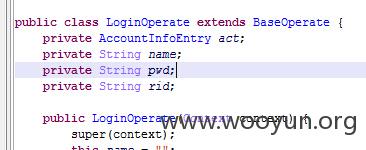
可见请求的关键数据被加密了，我们只有找到加密算法并解密才能进行进一步的安全测试。

一、算法逆向分析：

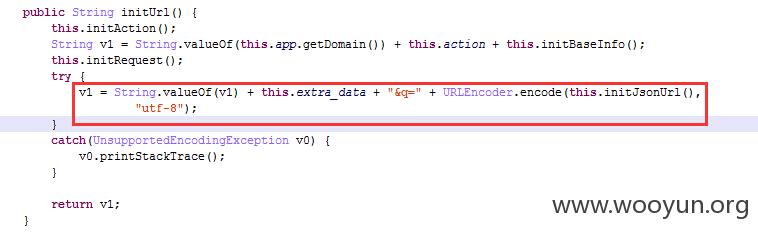
使用JEB或者dex2jar逆向客户端代码，JEB的效果更好一点，本文使用JEB。



从上图可以看出，此APP并未对代码做混淆处理，我们可以很容易地通过名称猜想ActivityLogin为登陆界面的代码实现，通过查看其代码也进一步证实了我们的猜想。分析得出处理逻辑主要在onLogin()方法里面。在此方法里面，声明了一个LoginOperate对象，进一步分析得出，LoginOperate继承自BaseOperate



在BaseOperate 的initUrl()方法里面，我们找到了请求数据的拼接



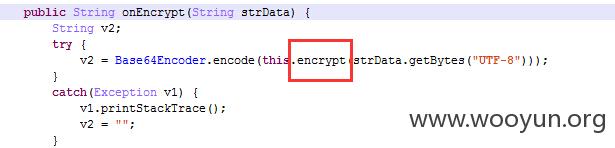
看，里面有“&q=”是不是跟我们第一步抓包的请求参数是一致的。

继续跟进initJsonUrl()方法，



看到其返回了aes.onEncrypt方法加密后的数据。

继续跟进aes.onEncrypt



跟进encrypt（）



很明显看出了其使用了AES加密算法，且秘钥硬编码为key = "shenzhoucar123123";

那么我们现在就理出了请求数据的装载过程

原始数据-》AES加密-》base64编码-》URL编码

数据还原过程相反，这样我们就可以对自己实现请求数据，同时解密返回数据了。实现过程只要把逆向代码中相关的类抠出来放到自己的代码里就好了。

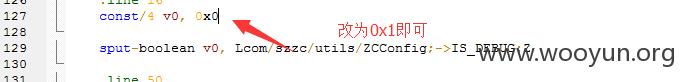
二、 重打包客户端：

通过上面的分析，可以看出BaseOperate类是处理数据请求的基类，可以通过在其中添加打印代码的方式，来直接将加密前的数据打印到日志中，这样方便程序的分析。

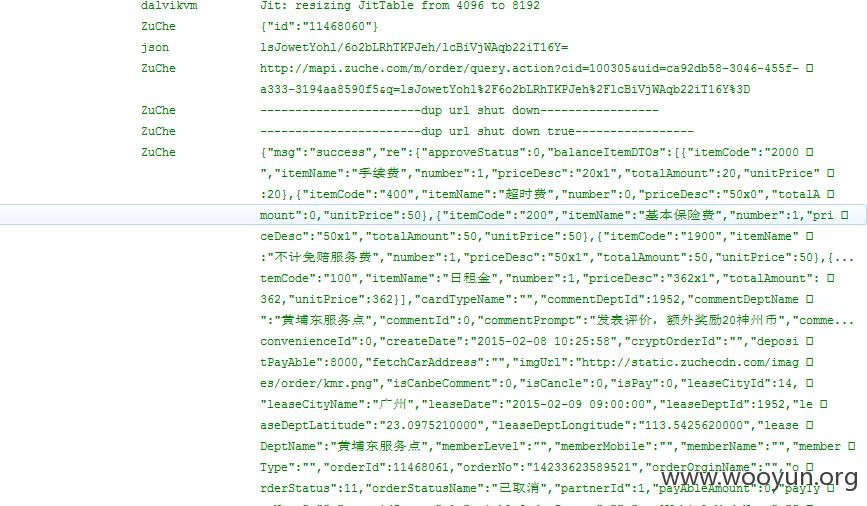
在以下代码中看到，只要ZCConfig.IS\_DEBUG为true，即可打印原始json数据。



使用APP改之理打开apk文件，找到对应的smali文件，将其改为true，重新打包，安装



这样我们使用DDMS就能在日志中看到请求的原始数据了，

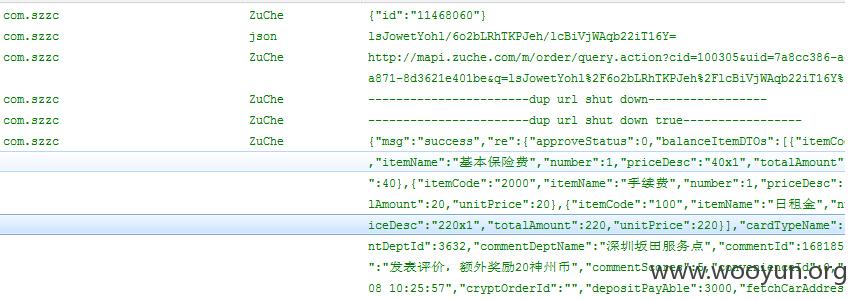


三、安全测试

当我们可以构造请求数据时，就可以开始安全测试了。

1、越权访问，

当访问客户端的自驾订单，订单详情时，发现请求数据为：{"id":"11468060"}



那我们构造{"id":"11468061"}的请求

<http://mapi.zuche.com/m/order/query.action?cid=100305&uid=ca92db58-3046-455f-a333-3194aa8590f5&q=Xop43hFpZ%2FEA4RlB%2Fvj%2btvYr1v0kqFLFdrAQ08e8YYI%3d>

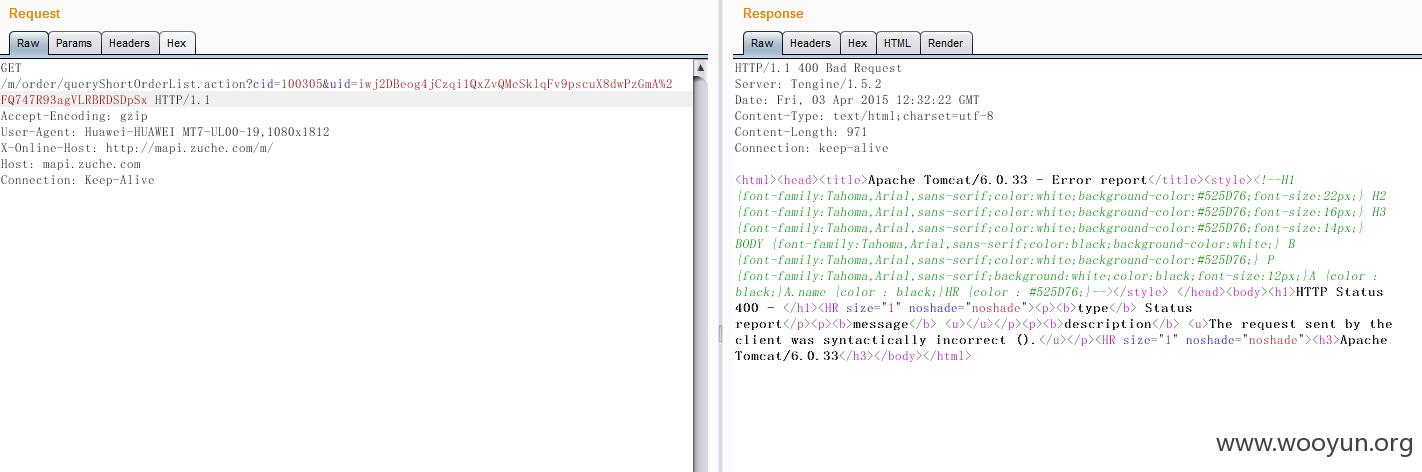
其中uid设置为你自己的uid即可，可以成功看到其他人的订单



好了，在代驾订单、顺风车订单里面应该存在同样的问题。

2、sql注入

如果我们请求{"id":"11468061'"}的数据将会出现什么情况呢，注意单引号



好了，看到服务器报错了，由于测试起来很麻烦，暂时未找到能读取数据的方法，留给一哥吧。

修复方案：

本文主要是说明密码学误用造成的危害，而且客户端加密也不是解决所有安全问题的解决方案，其只是增加了攻击成本而已，服务端验证才是王道。

此类问题在现在的安卓app中大量存在，值得注意。

版权声明：转载请注明来源 [feng](http://www.wooyun.org/whitehats/feng)@[乌云](http://www.wooyun.org/bugs/wooyun-2010-0105766)

**漏洞回应**

厂商回应：

危害等级：高

漏洞Rank：15

确认时间：2015-04-10 14:58

厂商回复：

感谢对神州租车安全的支持，过程非常漂亮，以后需要多多关注客户端的问题了，再次对@feng表示感谢~

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0人评价):**

登陆后才能进行评分

**评论**

1. 2015-04-10 13:46 | [疯狗](http://www.wooyun.org/whitehats/%E7%96%AF%E7%8B%97)

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  
漂亮的过程  
1#

1. 2015-04-10 13:48 | [袋鼠妈妈](http://www.wooyun.org/whitehats/%E8%A2%8B%E9%BC%A0%E5%A6%88%E5%A6%88) ( 普通白帽子 | Rank:449 漏洞数:61 | 故乡的原风景.MP3)  
   0  
   算法破解 等披露  
   2#
2. 2015-04-10 14:08 | [feng](http://www.wooyun.org/whitehats/feng) ( 普通白帽子 | Rank:674 漏洞数:80 | 想刷个6D)  
   0  
   @疯狗 求闪电,写了这么详细；）  
   3#
3. 2015-04-10 16:55 | [feng](http://www.wooyun.org/whitehats/feng) ( 普通白帽子 | Rank:674 漏洞数:80 | 想刷个6D)  
   0  
   这次给的rank还不错，期待下一个洞吧  
   4#
4. 2015-04-10 17:33 | [Adra1n](http://www.wooyun.org/whitehats/Adra1n) ( 普通白帽子 | Rank:441 漏洞数:69 )  
   0  
   @feng 求带。。。  
   5#
5. 2015-07-09 15:09 | [milan](http://www.wooyun.org/whitehats/milan) ( 普通白帽子 | Rank:129 漏洞数:32 | 妈妈说：搬不完砖就别回家。)  
   0  
   漂亮  
   6#
6. 2015-07-14 21:29 | [小鲜肉](http://www.wooyun.org/whitehats/%E5%B0%8F%E9%B2%9C%E8%82%89) ( 实习白帽子 | Rank:34 漏洞数:6 | 努力学习，不想在浪费时间了。)  
   0  
   大神谢谢分享，好漂亮的分析。  
   7#
7. 2015-07-14 22:30 | [qhwlpg](http://www.wooyun.org/whitehats/qhwlpg) ( 普通白帽子 | Rank:226 漏洞数:54 | 潜心代码审计。)  
   0  
   漂亮！  
   8#
8. 2015-07-31 09:46 | [theone](http://www.wooyun.org/whitehats/theone) ( 路人 | Rank:23 漏洞数:3 | hodor，hodor)  
   0  
   很详细的分析，赞一个！  
   9#

[Back](http://10.199.252.80:8080/bugs)