



无孔不入



关于我

Only\_Guest

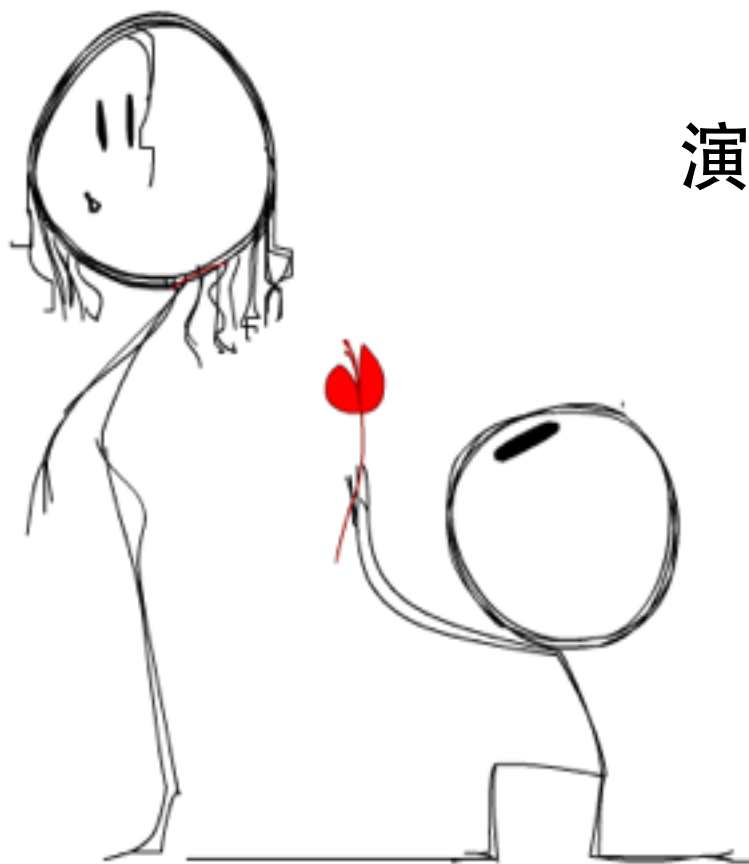
PKAV团队负责人  
双螺旋攻防实验室负责人  
段子协会幕后写手



## 免责声明

以下所有演示视频均为已修复漏洞  
以下所有演示数据均为已公开数据  
以下所有段子.....反正我不会负责。

## 演示一：黑客吃饭不花钱





本视频由“我全身都很硬”的锤子手机友情拍摄

缺陷编号: **WooYun-2011-01050**

漏洞标题: 土豆网肯德基活动免费吃漏洞。☔

相关厂商: 土豆网

漏洞作者: [only\\_guest](#)▼

提交时间: 2011-01-02 13:19

公开时间: 2011-01-07 15:00

漏洞类型: 设计缺陷/逻辑错误

危害等级: 中

自评Rank: 10

漏洞状态: 漏洞已经通知厂商但是厂商忽略漏洞

漏洞来源: <http://www.wooyun.org>

Tags标签: 业务缺陷 中奖/抽奖等敏感商业逻辑

分享漏洞:  分享到     0

缺陷编号: **WooYun-2014-73470**

漏洞标题: 饿了么某福利, 可导致无限免费吃饭, 免费上门送饮料等等

相关厂商: 饿了么

漏洞作者: 凉冬实验室

提交时间: 2014-08-25 14:41

公开时间: 2014-10-09 14:44

漏洞类型: 网络设计缺陷/逻辑错误

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>

Tags标签: 设计缺陷/边界绕过 逻辑错误

分享漏洞:  分享到     0

缺陷编号: **WooYun-2014-79123**

漏洞标题: 辉煌国际饭卡可被无限复制篡改从而可免费吃饭(射频卡设计安全隐患) 💰

相关厂商: 九鼎辉煌

漏洞作者: [Ano\\_Tom](#)

提交时间: 2014-10-13 00:24

公开时间: 2015-01-11 00:26

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: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: RFID

分享漏洞:  分享到     0

妹子：我一个人打车回家不安全，要不你买个车吧？

演示二：没事，我会看着你到家





U B E R

本视频由我虽然不会被监控但我可是约炮小能手的  
“**UBER**”豪车团特别赞助播出！





缺陷编号: **WooYun-2012-07477**

漏洞标题: 中国银行某支行运钞车辆监控系统

相关厂商: 中国银行

漏洞作者: 小风

提交时间: 2012-05-24 13:48

公开时间: 2012-07-08 13:48

漏洞类型: 后台弱口令






危害等级: 低

自评Rank: 3

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 敏感信息泄露 后台被猜解 配置错误 测试程序泄漏 测试

分享漏洞:  分享到     0

缺陷编号: **WooYun-2015-105163**

漏洞标题: 某车辆监控调度系统存在漏洞, 可断开大量车辆油路和控制时速

相关厂商: 国家互联网应急中心

漏洞作者: 路人甲

提交时间: 2015-04-02 15:52

公开时间: 2015-05-22 13:16

漏洞类型: SQL注射漏洞




危害等级: 高

自评Rank: 20

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞:  分享到     0

缺陷编号: **WooYun-2014-85228**

漏洞标题: 贵州高速公路车辆监控系统存万能密码

相关厂商: 贵州高速公路

漏洞作者: 路人甲

提交时间: 2014-12-01 11:58

公开时间: 2015-01-15 12:00

漏洞类型: 网络未授权访问



危害等级: 中

自评Rank: 9

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

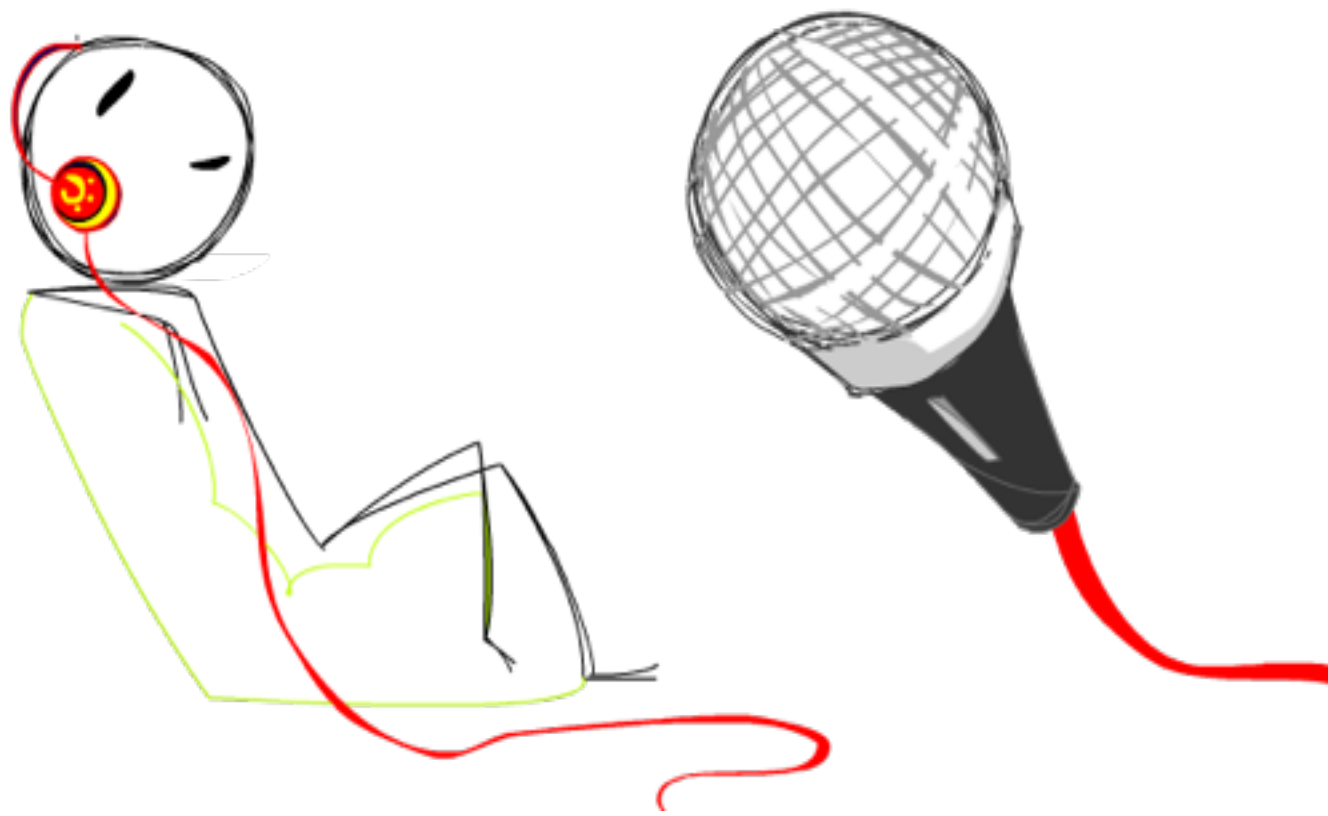
漏洞来源: <http://www.wooyun.org>

Tags标签: 管理后台对外 后台被猜解 运维管理不当

分享漏洞:  分享到    0

演示三：

我以为我把电话打给了你，你却打给了全世界。





本视频由斯诺登联盟下属分支机构“反老王协会”  
特别播出。  
有了斯诺登！再也不用担心隔壁老王了！！！！



缺陷编号: **WooYun-2014-50023**

漏洞标题: 某网络电话注册任意号码/修改任意号码密码(可伪造号码与对方通话) ☁

相关厂商: 某网络电话

漏洞作者: 随随意意

提交时间: 2014-07-08 14:38

公开时间: 2014-08-22 14:40

漏洞类型: 设计缺陷/逻辑错误

危害等级: 高

自评Rank: 5

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞:      0

缺陷编号: **WooYun-2014-68693**

漏洞标题: 某云呼叫中心服务提供商信息泄露可下载任意通话录音

相关厂商: xl59.com

漏洞作者: 凹点

提交时间: 2014-07-17 11:07

公开时间: 2014-08-31 11:08

漏洞类型: 重要敏感信息泄露

危害等级: 高

自评Rank: 20

漏洞状态: 厂商已经确认

漏洞来源: <http://www.wooyun.org>

Tags标签: 敏感信息泄露

分享漏洞:      0

缺陷编号: **WooYun-2015-113574**

漏洞标题: 加拿大Rogers可以控制任意电话号码

相关厂商: rogers

漏洞作者: ziwon

提交时间: 2015-05-12 13:25

公开时间: 2015-06-29 18:14

漏洞类型: 设计缺陷/逻辑错误

危害等级: 高

自评Rank: 20

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 逻辑错误 设计错误

分享漏洞:      0

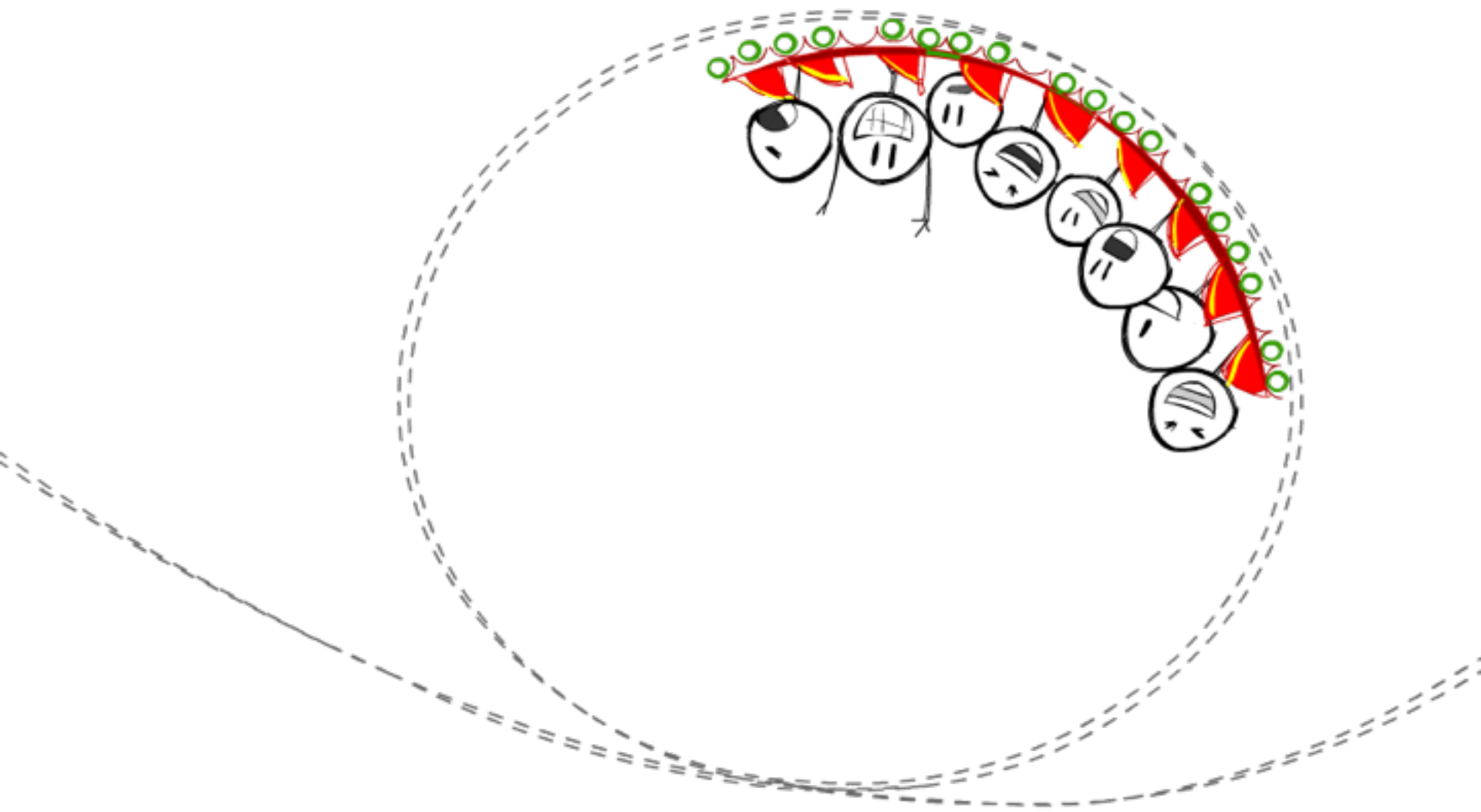
演示四：  
去给我查查车主是谁。



大哥！不好了！嫂子坐车跟人跑了！



本视频由“我是过山车，我没有车牌”协会尖叫放映



缺陷编号: **WooYun-2015-97636**

漏洞标题: 全国大量车主信息互联网疯传包括几百万车主姓名/身份证号/家庭住址/车牌号等等(公然售卖)

相关厂商: **车主信息**

漏洞作者: **路人甲**

提交时间: 2015-02-18 19:19

公开时间: 2015-04-04 19:20

漏洞类型: 用户资料大量泄漏

危害等级: 高

自评Rank: 20

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞:  分享到     0

缺陷编号: **WooYun-2015-97685**

漏洞标题: 某市交通局注入漏洞影响几十万车主信息(包括身份证号, 电话号, 车牌等)

相关厂商: **tljt.gov.cn**

漏洞作者: **路人甲**

提交时间: 2015-02-18 12:09

公开时间: 2015-04-04 12:10

漏洞类型: SQL注射漏洞

危害等级: 高

自评Rank: 15

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞:  分享到     0

缺陷编号: **WooYun-2015-105025**

漏洞标题: 比亚迪汽车存安全漏洞可导致大量车主敏感信息泄漏

相关厂商: **byd.com.cn**

漏洞作者: **路人甲**

提交时间: 2015-03-31 17:30

公开时间: 2015-05-16 17:38

漏洞类型: 敏感信息泄露

危害等级: 高

自评Rank: 20

漏洞状态: 厂商已经确认

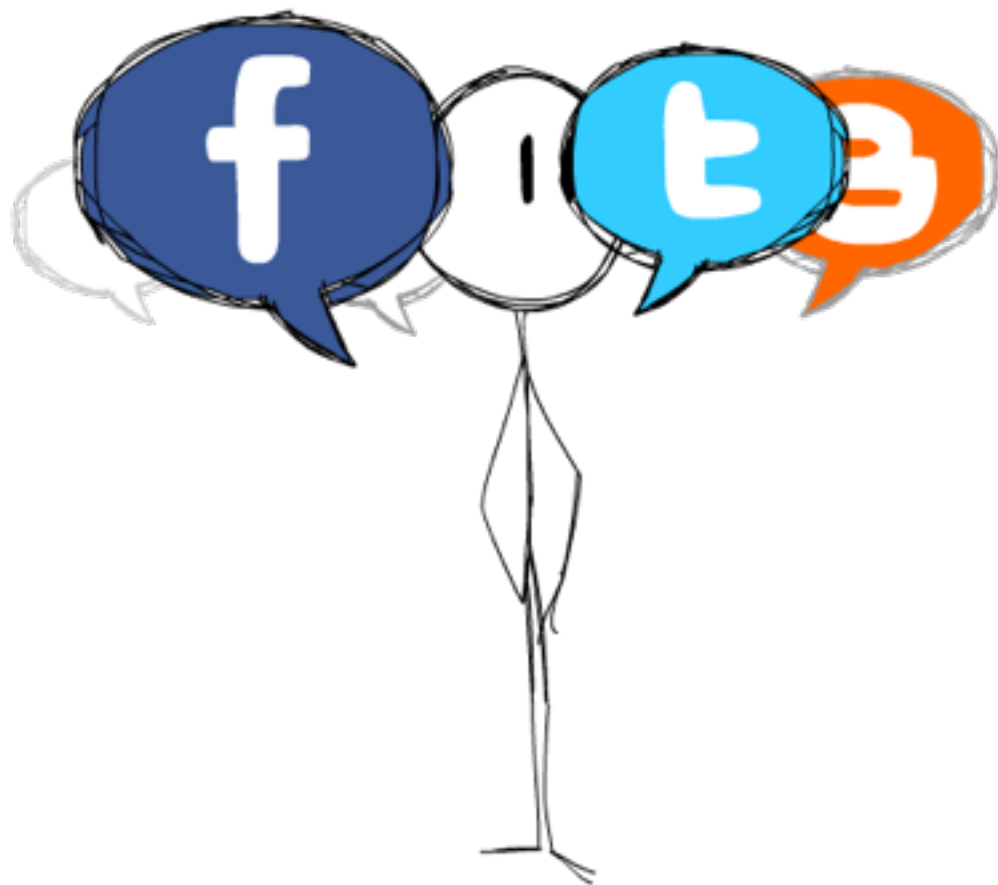
漏洞来源: <http://www.wooyun.org>

Tags标签: **用户敏感信息泄漏**

分享漏洞:  分享到     2



演示五：我只注册帐号，从不发帖，你要人肉我？



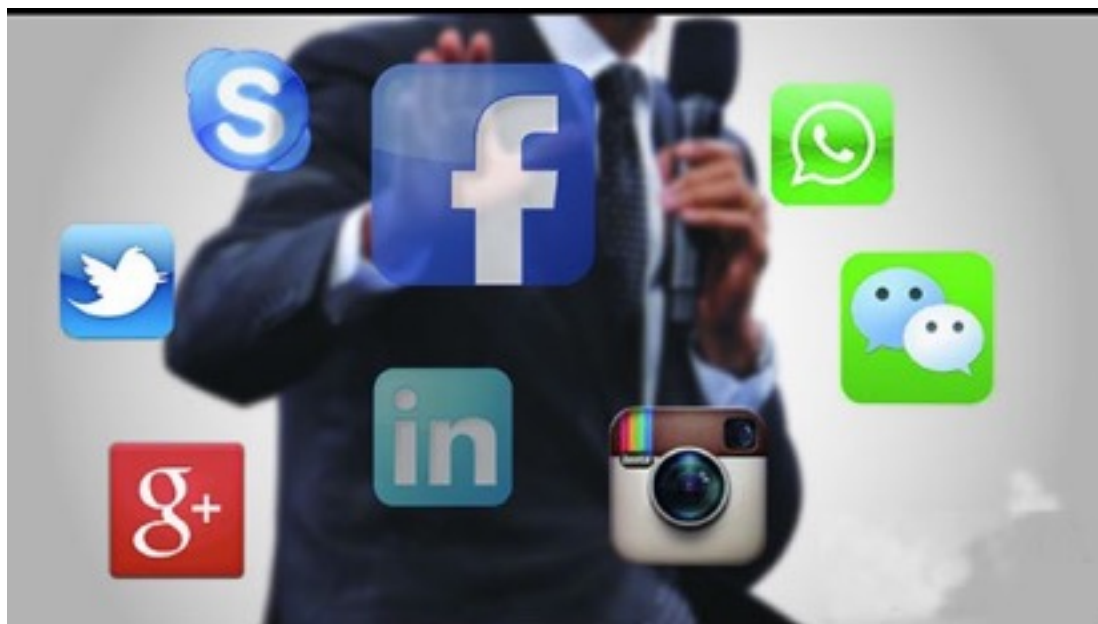


本集由“我没有注册会员，我只是借用试衣间”  
的XXX品牌赞助播出

这个....没有案例。

演示六：放学别走！我现在就打电话叫人！





本集由“我们只是帮你看看你有哪些朋友在用我”  
的社交APP联盟冠名播出。

缺陷编号: **WooYun-2014-88140**

漏洞标题: QQ邮箱某处设计缺陷导致可枚举腾讯企业内部通讯录(间接危害企业安全) ⚡

相关厂商: 腾讯

漏洞作者: **0x\_Jin**

提交时间: 2014-12-22 14:39

公开时间: 2015-02-05 14:40

漏洞类型: 账户体系控制不严






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>

Tags标签: 设计缺陷/边界绕过 逻辑错误 设计不当 QQ 邮箱

分享漏洞:  分享到     3

缺陷编号: **WooYun-2015-112652**

漏洞标题: 魅族科技flyme某接口撞库泄露用户登录凭证(有批量账号证明)

相关厂商: 魅族科技

漏洞作者: 路人甲

提交时间: 2015-05-07 16:43

公开时间: 2015-06-21 18:08

漏洞类型: 设计缺陷/逻辑错误

危害等级: 高

自评Rank: 18

漏洞状态: 厂商已经确认

漏洞来源: <http://www.wooyun.org>

Tags标签: 撞库

分享漏洞:  分享到     0

缺陷编号: **WooYun-2015-116202**

漏洞标题: 某通讯录同步服务权限控制不严导致用户联系人信息泄露

相关厂商: [leeab.com](http://leeab.com)

漏洞作者: **GAVVA**

提交时间: 2015-05-26 08:51

公开时间: 2015-07-10 08:52

漏洞类型: 未授权访问/权限绕过



危害等级: 高

自评Rank: 10

漏洞状态: 未联系到厂商或者厂商积极忽略

漏洞来源: <http://www.wooyun.org>

Tags标签: 安全意识不足 越权操作 用户信息泄露 安全意识不足

分享漏洞:  分享到     0

**PKAV团队招人**

欢迎登陆团队网站  
了解具体情况

**WWW.PKAV.NET**



谢谢观看