WooYun 月“爆”

本期看点：

诈骗大揭秘之航班取消的秘密

“猪一样的”手机 APP

眼见未必为真

传统短信伪造攻击的可能性证明

WooYun WIFI 成长史

[2014 年 11 月总第 8 期]

序

实际上这一期的月报小编是从 8 月开始准备的，可是从八月开始小编就一直忙呀忙呀忙所以耽搁到了现在，不过值得高兴的是咱们乌云的线下活动也算是有个开篇了，不管是规模较大的乌云安全峰会还是比较小型的乌云技术交流沙龙都已经开始步入正轨。接下来小编会尽量保持乌云月报的稳定性，谢谢你们陪着小编和乌云月报一起成长。

这一期月报的灵感来自于看到了许多关于诈骗的报道。其实从古至今从来不缺骗子，也没有缺过被骗的人。以往骗子的手法很拙劣，并且会先使用一些明显不合逻辑的信息挑选出最容易上当的一批人再行骗，但是从一部分案例来看现在的骗子貌似不会再挑人行骗，甚至把目光放在了高学历人群。是什么给了骗子这样的自信！实际上如果掌握了足够多的信息要骗到智商够高逻辑够清晰的人也并非难事的。那这样的信息怎么会落到骗子手中呢？其实途径有非常多，在这一期月报中小编用一些实际的漏洞案例来证明要获取你的信息可能比你想象中容易得多。

经过长期思考，小编对咱们月报进行了一些调整，同时增加了白帽子专访版块。这个版块是给咱乌云白帽子的舞台，除了能看到各种大牛的风采，并且每个人都是有机会站上来的。

诈骗大揭秘

几乎每天，各种诈骗信息充斥着各大新闻媒体，好像被骗已经不是新鲜事但又都是新鲜事。层出不穷的诈骗技巧让人防不胜防，乌云月报第八期，小编带你了解那些诈骗中唬住人的神秘因素。

航班取消的秘密

WooYun 缺陷编号：WooYun-2014-65767
乌云白帽子 **铁蛋火车侠** 提交于 2014-06-21

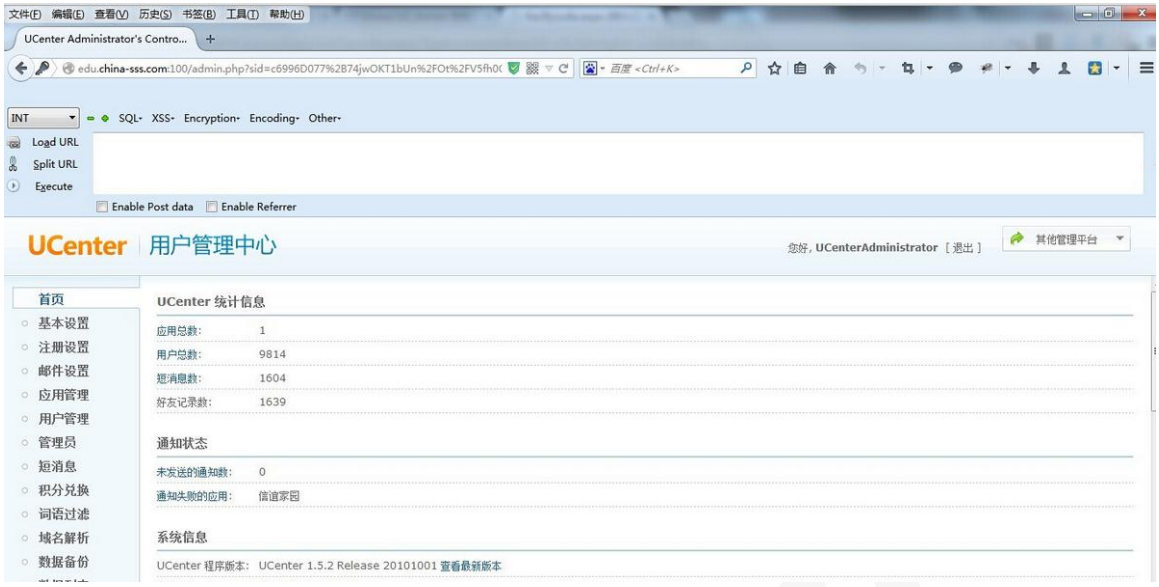
据网友反映不知道从什么时候开始在航班起飞的前一天左右总会收到“尊敬的××旅客，您所预订的××航班因机械故障已被取消，导致不能正常起飞。收到短信后请及时与本公司联系，如退票票款全退，并补偿 200-300 元，改签收 20 元工本费，请致电 xx 航空公司客服 400xxxxxxx 办理”这样姓名，航班号都是正确的短信。但是小编要告诉你，这其实是呢诈骗短信，可是这么准确的信息怎么就到骗子手上了呢，小编猜可能和一些航空公司的安全漏洞有关，咱们乌云上就有不少航空公司的案例，比如 6 月的这个乌云白帽铁蛋火车侠提交的这个漏洞。

漏洞过程重放：

吉祥航空某分站后台登录地址是 http://edu.china-sss.com:100/

帐号：admin

密码：admin



从后台可看到用户总量：9814

由图中可见后台的功能很多的，会导致很严重的后果，因为仅仅是为了发现问题就不再深入研究了

漏洞点评：

“过程简洁明了，结果简单粗暴”，这十二个字来形容这一个漏洞再合适不过。显然春秋航空还是有安全意识的，后台登录的端口并不是 8080 ，可是很明显有些低估了网络安全爱好者的能力呀，就算是 100 端口，找登录地址有难

度但是不等于找不到的，小编好想问问那个网站管理员为什么要用弱口令呀，还是这样弱到家的口令？？？所以，有管理网站的看官们，赶紧回去看看吧，该改的改该加强的加强，不要太贪图方便了，黑客可是最喜欢这类人的哦。

.....

“猪一样的”手机 APP

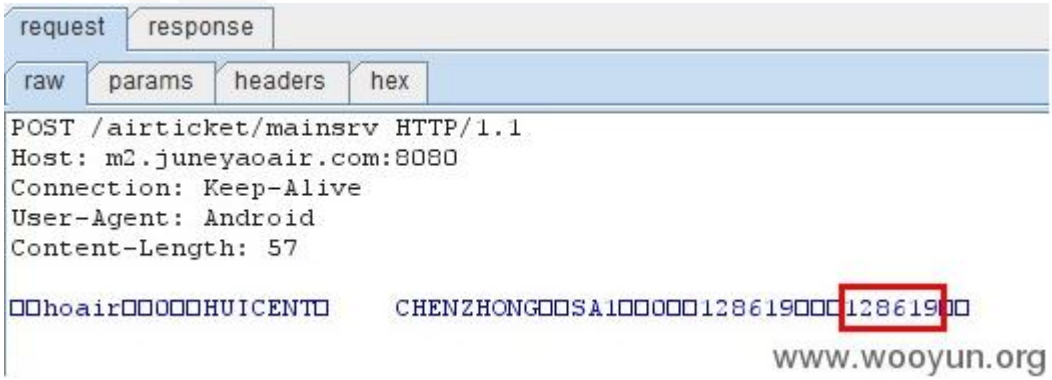
WooYun 缺陷编号：wooyun-2013-65767
乌云白帽子 **铁蛋火车侠** 提交于 2014/06/21

什么是“猪一样的”手机 app 呢？所谓不怕神一般的对手就怕猪一样的队友。现在厂商的安全意识都有明显的提高，网站的安全也做得越来越好，原以为这样就不会出现因为安全问题而导致用户信息泄露了。可是手机 APP 呢？你们把 APP 的位置放哪儿了！吉祥航空有一个导致乘客信息泄露的漏洞就是因为 APP 出了问题，这难道不就是传说中的“猪队友”么

漏洞过程重放：

吉祥航空 APP 可遍历他人信息，具体步骤为：

点击亲友名录管理，截断 POST，可看到用户 ID



直接修改此 ID 可获取，测试了三个作为案例


吉祥航空
林
其他
证件号码 51112
手机号码 18


吉祥航空
哲
居民身份证
证件号码
39
手机号码

漏洞点评：

这是一个手机 app 的遍历问题，归根结底还是权限控制不到位。为什么强调了那么久的权限控制问题还是存在呢？估计是没有注意到这里的问题。正所谓安全是一个整体，而这个整体不仅仅是网站，各种客户端也是整体的一份子，所以企业在对自身进行安全检测的时候一定不要忘记了这些客户端，别让客户端沦为猪队友。

.....

平安校园中的危机

WooYun 缺陷编号：WooYun- 2014-65365
乌云白帽子 **魇** 提交于 2014/06/18

现如今，孩子可是父母的心头肉，所以从孩子信息下手的诈骗事件的成功率是比较高的。可是那些骗子怎么大量地获取孩子的信息并且将孩子的信息和父母的信息联系起来的呢?其实小编要告诉你的是有时候这种信息的获取比你想象中要简单得多。比如联通的平安校园管理系统本意是为了应对各种不安全因素最后却因为系统的安全问题反而导致不安全因素增加了呢。

漏洞过程重放：

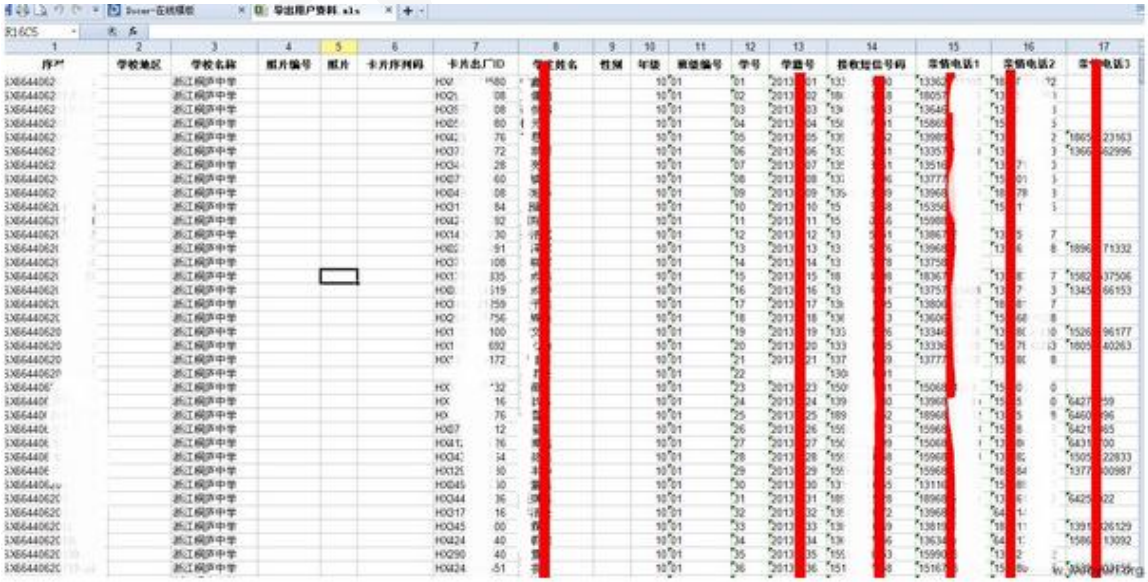
http://paxy.10010zj.com.cn/ 平安校园管理系统 浙江联通

存在后台未授权访问的问题：

打开 http://paxy.10010zj.com.cn/admin/admin_index.aspx 直接进入后台

后台的功能非常多，包括学校管理，教师管理，中小学用户管理，幼儿园用户管理等。

更可怕的是多个地区学校的教师跟学生信息，以及该系统自带导出功能，可批量导出学校，中小学用户师生，幼儿园用户师生等信息



能够看到共有 238 考勤机，联网 164,断网 74,亲情电话 129,远程考勤设备 107,摄像头 2。

漏洞点评：

这又是一个权限控制的问题，就好比制造了一把好锁却不用，只需要找到了门任何人都可以不费吹灰之力地打开，更恐怖的是在因为锁的缘故这个屋里放了很多宝贝。不知道小编的比喻能不能让各位看官明白权限问题的严重性，希望厂商能重视安全，“一不小心被进了后台”还是挺糟糕的。

.....

错误志愿误一生

WooYun 缺陷编号：WooYun-2014-70199
乌云白帽子 **Summer** 提交于 2014/07/30

经历过高考的小伙伴一定知道高考志愿对于一个高中生来说有多重要，多少人因为被调配到其他专业抱怨了一生，多少人因为没有读到喜欢的专业遗憾了一辈子，多少人因为选错专业只有在后来的日子里遥想想当年。所以，只要有人能说出关于志愿的准确信息别说是假冒高校老师了就是假冒教育局的也都信了呀，所以为什么会有那多的人因此受骗也是可以理解的。可是，如果不是高校老师或者教育局的人怎么会知道准确的志愿信息呢？这可能并不难，比如今天的这个漏洞就可能导致 16 万+考生信息泄漏甚至任意修改考生志愿。

漏洞过程重放：

首先是逻辑漏洞：

我先用我的帐号登录 http://www1.**.zsks.cn/kscx

可以看到如果你得到了考生号和密码，就可以为所欲为了！修改考生志愿？在报考最后阶段修改考生密码？我是不是太邪恶了？这样别人就没有大学上了 !所以说威胁程度比较高。

看到那个有我头像的地方，这个可以遍历到所有某省高考生的头像。

例如：http://www1.**.zsks.cn/kscx/zy/picture.gif?ksh=考生号

其中那个考生号可以用来遍历，这样就可以把全省高考生头像下载下来，这样就可以认真挑选妹纸了，比如，看到那个妹纸漂亮，我们就把考生号记录下来，但是这样只有头像，没有其他信息啊，其实是可以获取其他信息的。

那么下面就是如何获取高考生信息了，其实是有 2 处没有设置验证码，从而导致暴力破解，在考生服务平台暨网上填报志愿这里设置了，为什么在其他处没有设置呢？

下面我们来看：

2014 年某省普通高校招生考生状态信息查询

http://www1.**.zsks.cn/query/pz14_ksgj.jsp

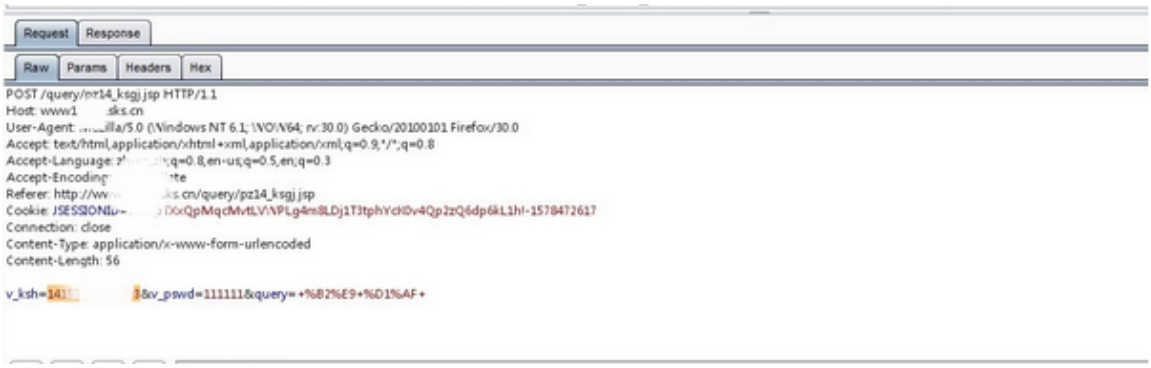
2014 年某省普通高校招生考生状态信息查询

http://www1.**.zsks.cn/query/pz14_kscx.jsp

这两处都没有设置验证码，导致我们可以暴力破解。

考生号命名规律是这样的：14 15***2 11 XXXX

其中 14 代表是 2014 年，15***2 是身份证前 6 位(代表某省的某个城市)，11 代表是 2011 年入学(11 届) ,XXXX 目前还没想出来 ,估计就是一个简单的编号，那么这样就可以构造考生号暴力破解了，那么密码呢？密码是 6 位的，为什么是 6 位呢？因为默认密码是我们身份证后 6 位，这样就可以制作密码字典 0-9 数字，生成 6 位的。



自由可投，看来她就是我明天的对手了！！！

考了 367 分，没我高，看来我还是能把她挤掉的，嘿嘿嘿。

进她的报志愿网站，去瞧瞧，各种信息一目了然，我会说，我明天要放暗招？最

后一分钟直接修改她志愿，修改密码，好像这样就邪恶到爆了。。。善哉善哉！！

在附上一个帐号，说明问题。

好高的分数！！！羡慕嫉妒恨！！！

漏洞点评：

幸好咱们的 Summer 是个好白帽没有因为羡慕嫉妒恨就修改了别人的志愿

而是提交了漏洞等待厂商修复，不然得让多少人伤心呀。这个漏洞的影响呢其实作为高考生的 Summer 已经在在漏洞详情中进行了描述。可能有些人认为遍历头像不是个大问题，但是像这种高辨识度的头像结合后面的爆破到能查看成绩和志愿，如果落到骗子手中，真的可以一骗一个准啊。所以小编建议，厂商对待没有必要公开的个人信息还是限制只有登录状态下才可查看，登录的验证码还是应该有的。

.....

眼见未必为真

WooYun 缺陷编号：WooYun-22014-50101
乌云白帽子 **happylyang** 提交于 2014/01/31

10010 打电话来说你的手机将在两个小时内停机你会不相信这是真的吗（小编说的联通的手机哦，电信和移动的手机也敢信的那小编还是画圈圈去），按照电话中所说的去做最后发现被骗啦，难道是联通设置的骗局么？其实不然，只是，你看到的是 10010 的来电未必真是 10010 打来的，不要以为电话号码就不会骗人，小编用漏洞来告诉你，来电显示就算眼见未必为真。

漏洞过程重放：

发现了一款客户端，据说能把事先录制好的声音，发给指定的人，显示自己的手机号拨打的，试了下确实可以，不自觉得想能否让接听者点电话显示随便一个号码而不只是自己的呢？于是。。。

我用的是 ios 版本的，用 burpsuite 抓下包，配置好无线网络段，然后，直接发现

```
POST /***Act/*** HTTP/1.1

Host: [马赛克]:8080

Proxy-Connection: close

Accept-Encoding: gzip

Content-Length: 227

Connection: close

Cookie: Hm_lvt_3845abcf8101e9b5e3cfe50f635dd78d=1360405417; pgv_pvi=8183689216

User-Agent: ææ¿ä½ è¯´ 1.4.1 (iPod touch; iPhone OS 6.1; zh_CN)


{"Event":"ReservationAct","Command":"Reservation","UserId":"aad9a6ad-f8bb-11e2-8fcc-90b11c58b16b","Phone":"1234567","Com
mentId":289,"Type":0,"Time":0,"PhoneList":[{"Name":"Leek","Phone":"15512345678"}],"QID":"HH:mm:ss.fff"}
```

```
HTTP/1.1 200 OK

Content-Type: text/html;charset=utf-8

Date: Fri, 31 Jan 2014 02:05:38 GMT

Connection: close

Transfer-Encoding: chunked


94

{"Event":"ReservationAct","Command":"Reservation","CommentId":289,"ReservationId

":91783,"Success":true,"Info":"","QID":"HH:mm:ss.fff","FailInfo":""}
```

注意下面的，UserID 是用户的 id，随便伪造个，不要紧，CommentId 是录音的标号，可以使自己的录音也可以是拜年的。。第一个 Phone 参数，是接听人的电话显示的那个拨打者的号码，第二个 phone 是要打给谁的号码，发送这个包，等待 1 分钟左右，15512345678 的手机就会受到 1234567（上面的例子）的电话了，如果用于诈骗会比较严重，因为可以显示任意号码的，内容也可以事先录好音。

就是上面那个数据包，看看效果


138-8888-8888
提醒我
信息
滑动来接听


所有通话
未接来电
编辑
138-8888-8888 (2)
19:10
未知

漏洞点评：

现在的网络电话越来越多，因为价格低所以还是有一定的优势的，但是呢，本身网络电话的通话安全问题就是待解决的问题，现在各种不靠谱的客户端无疑是给网络电话的安全雪上加霜啊。所以嘛，伪造任意号码打电话的可行度越来越高了，接到奇怪的电话不要相信来电显示，一定要记得验证通话内容啊。

.....

中国电信某省未授权绑定他人账户可查话费办业务

WooYun 缺陷编号：WooYun-2014-65290
乌云白帽子 **路人甲** 提交于 2014/06/17

为了方便客户办理业务电信不仅推出了各种手机客户端也借助微信做了微信平台，不得不说还是挺用心的。但是呢，由于对安全的考虑不完善导致存在一些问题，至于问题导致的后果大家看标题应该都知道啦，现在一起去看看这些问题如何被挖掘出来的吧。

漏洞过程重放：

问题出现在微信上，这是我自己的号，

使用另一个山东电信能够接收短信的手机接收验证码

收到验证码后输入验证码并提交 ,收验证码的手机为 1339xxxxxx ,修改 number 为同省其他用户手机号码 1332xxxx

就这样绑定成功了！


中国电信山东网厅
6月17日 晚上19:12
我的账单
6月17日
我的 账单
手机号为1332 的客户,您的手机2014年05月总费用 元。
点击查看近6个月账单详情>>>>
查看全文
精彩活动
流量包办理
自助查询
www.wooyun.org

可查询话费账单哦

看样子还可以办理业务的，办业务没试，不浪费山东用户的钱了

漏洞点评：

据小编了解大部分的业务办理只是会发短信通知一下并不会确认，虽然漏洞提交者没有测试但是应该是可行的，不过就算不能够办理业务，能够登录别人的账号危害也挺大啦。这里更多还是逻辑的问题啦。

安全风向标

无论是互联网还是现实社会，信任是人与人交往的基础，良好的交流必然是建立在互相信任的情况之下。但是，信任又往往容易被人利用，这期风向标给大家来讲讲关于诈骗相关的事 ,来看看聪明的乌云白帽子们都发现了哪些有趣的案例能够拿来诈骗的吧。

来自官方的钓鱼推送

WooYun 缺陷编号：WooYun-2014-070509
乌云白帽子 **s0mun5** 提交于 2014/07/31

一直以来，大家都认为，识别一个伪造网站，只需要看看输入的域名就可以了。但是，谁也没想到，这次出现问题的竟然就是官方自身，白帽子研究发现，中国电信官网竟然因为某个漏洞从而可以导致定向集体推送更新（木马），这要是放在诈骗相关的公司，可是前途无量的漏洞，我们来看看这个案例当中到底是出现了什么问题。

漏洞过程重放：

误打误撞进了一个电信的安卓营业厅发布以及推送后台

http://118.***.**.*:8080/

弱口令 test/test

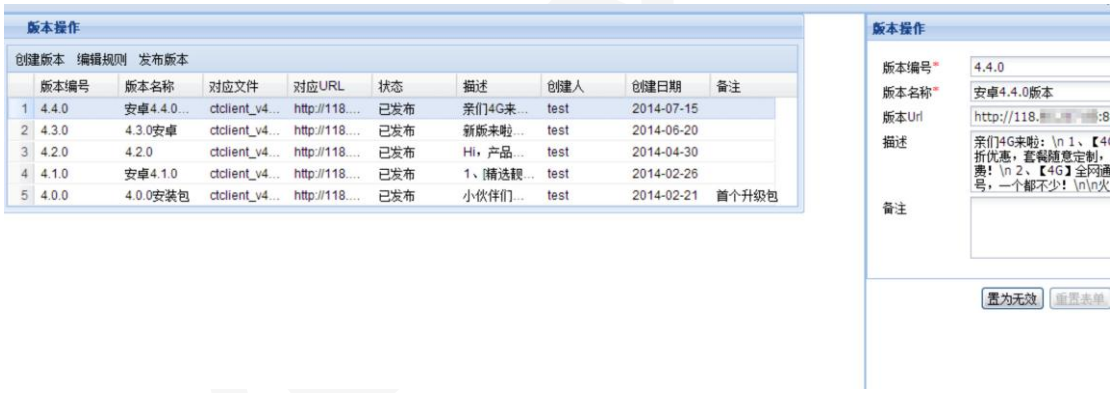
静态配置页面 发布 部署后 直接可以 getshell 两个台内网服务器

（jsp 打包 zip 上传 zip 自动解压缩）

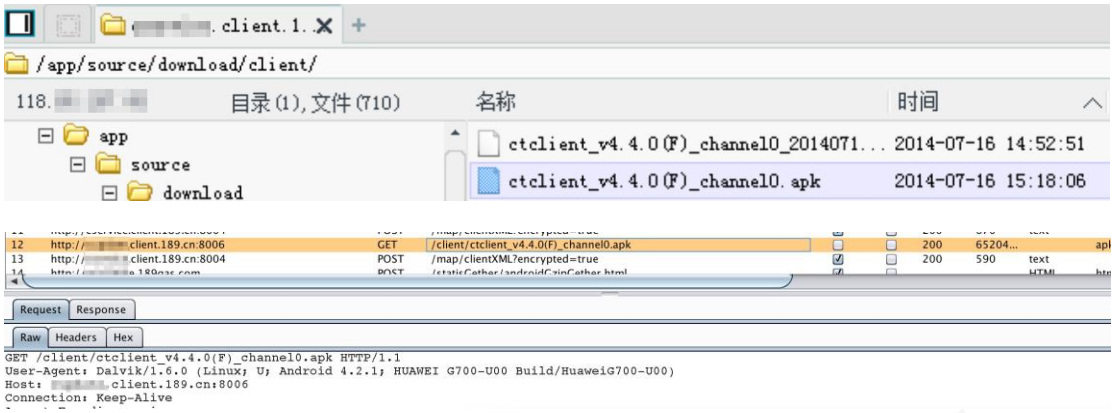
http://118.***.**.*:8080/ 以及 http://***.client.189.cn:8006

发布的时候可以选择是否强制推送或者选择定向推送更新

下面证明该更新确定就是客户端收到的链接



后台中的文字跟推送的文字相同



burp 抓到的更新地址与 shell 地址相同(**ervice 与**update 在内网是同一台服务器 并且做了负载均衡）

配置文件中的数据库连接串

由于库太大读取对业务有影响 没去确定 但是根据客户端登录的数据包可以推断

http://www.189.cn/client/test.html

这里可以做的多了 谁会觉得官网的二级目录是钓鱼呢 传 exe apk 当然也可以

如果结合上面那个后台的推送 把钓鱼页面推送到手机上 是不是可信度更高了:)

漏洞点评：

现阶段而言，黑客攻击大网站的主站似乎难度非常高的情况下，往往会选择比较偏门的地方去入手，这个案例给了企业很好的一个提示，在重视首页安全性的同时，是否也应该考虑周边范围的安全呢？木桶原理是企业在做安全防护时候需要考虑进去的，而弱口令这样的密码，更是需要注意的。稍有不慎，受害的可不仅仅是企业，更是成千上万无辜的网民。

.....

传统短信伪造攻击的可能性证明

WooYun 缺陷编号：wooyun-2010-044927
乌云白帽子 **Mujj** 提交于 2013/12/04

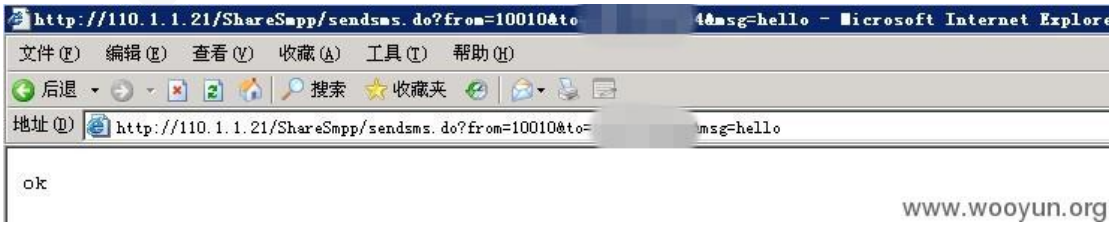
如果上面那个例子告诉你，哪怕是大型运营商的官网多么不可靠，那这个例子估计你要有心理准备了。在人们还在防范如何去避免伪基站给我们生活带来影响的时候，乌云的白帽子就给出了一个传统短信伪造攻击的可能性证明。不需要借助伪基站，就能千里之外，获取你的信任，进行诈骗。下面来看看，白帽子是如何通过这个漏洞，远程锁定指定的 QQ 账户以及其他危害的。

漏洞过程重放：

那是 2012 年一个月黑风高之夜，某人收到了某通近日来的第 N 条推广短信，恰逢上网又弹出劫持广告，于是某人乘着 struts2 的东风恶摸进了短信中的 upay.cc 的短连接服务器，后来就没有然后了，struts2 的东风再度来袭的时候，又摸进去了看了下，嗯，进度比以前提高了，发现了一个文本里面的 URL；

http://110.1.1.21/ShareSmpp/sendsms.do?from=18638384388&to=10010&msg=101

很有意思的一个链接不是吗?然后用某通的号码按照以上的 URL 发送了个 101 过去，就收到余额提示信息了。



然后把 form 和 to 对换了下也能接收成功，到这里只能算是比较有意思和影响使用主动验证方式的一些厂商而已，比如某疼短信改密系列功能(目前已修复)。

继续测试短信功能，发现不只能影响某通，还能影响某信的用户，至于某移，完全没影响。

那么这个接口是做什么用的，是谁架设的，为啥只影响这 2 个呢，这个问题只有北京东×国×科技股份有限公司能回答了，不妨来百度下他们的中标公示记录和年度报告（上市公司都有）；

PS：以上提到的所有漏洞以及某疼的主动验证方式均已修复。

漏洞点评：

在案例中，白帽子给出的过程非常让人震惊，试着想想，一个人只要知道你的手机号码，就能做出伪造号码发送短信等功能，上图只是给出 QQ 锁定的影响，如果把目标换成是支付宝，或者网银相关的，危害又会有多大呢？目前该漏洞已经修复，作为网民，在收到来自 10086 短信的时候，一定要谨慎的去辨别，千万不要一时大意就被上当受骗了。而相对于企业而言，这样的接口哪怕是内网使用，也一定需要加上相关的会话等二次认证，合理的去避免相关的风险做到未雨绸缪。

.....

网银中的安全隐患

WooYun 缺陷编号：WooYun-2014-70306
乌云白帽子 **肉肉** 提交于 2014/07/30

要对于一般人而言，可能很多人都会认为银行的相关系统是安全的，起码，用起来是感觉比较安全的。最近，乌云白帽子肉肉就发现了招商银行网银定向 xss 漏洞，利用这个漏洞，黑客可以获取用户当前余额，甚至可以进行钓鱼。

漏洞过程重放：

以下是用客户端做的测试

招商银行网银自助转账的留言处存在存储型 xss，

查询交易记录的时候触发

可加载执行外部 js，

利用 xss 平台获取 cookie

获取账户余额：

因为转账需要支付密码所以没办法直接转账，不过可利用此 xss 做一个钓鱼页面先获取支付密码再进行转账操作也是可行的。在这样的页面下让输入银行卡支付密码了别说是没有安全意识的人了，就算是有安全意识的人估计会中招的也不会少，所以危害还是挺大的。

经测试招行网银网页版和手机客户端均存在这样的问题。

漏洞点评：

通过上面这个案例，我们可以看到，尽管是银行等相关金融行业，也免不了受到安全问题的冲击，类似这样跨平台的 XSS 代码注入，所见不多，但是不可忽略它给我们带来的危害，类似这样的漏洞是非常容易拿来钓鱼攻击与欺诈的，做为相关的供应服务商，除了要把服务做好以外，安全更加需要重视，一旦有一些小的缺陷，用户则会受到很大的影响。

.....

每天进步一点点

SSLStrip 的未来 —— HTTPS 前端劫持

作者：EtherDream

SSLStrip，中间人攻击利器，可用于 HTTPS 向下降级攻击，将页面中的 HTTPS 超链接全都替换成 HTTP 版本，让用户始终以明文的形式进行通信。

在网页还没有那么多动态元素的过去通过后端来实现流量劫持可行性是非常高的，但是随着动态元素的出现以及数据传输的分片处理使得一些“古老”的方法渐渐失去了用武之地。文中作者讲述了另一种思路的劫持，从前端下手后端配合几乎天衣无缝，具体怎么做呢，关于这种方式怎么解决动态元素的问题以及如何防范，到文中一探究竟吧。阅读请点 http://drops.wooyun.org/tips/3199

密码找回功能可能存在的问题（补充）

作者：BMa

13 年 7 月的时候乌云白帽瞌睡龙结合乌云的案例整理了密码找回可能存在的问题 http://drops.wooyun.org/papers/287 ，这篇文章不管是给企业还是白帽子都带来了很大的帮助，白帽 BMa 在学习过程中发现之前的总结不是很完整，一些密码找回的问题甚至是之前的问题被修补又被绕过的，所以小编觉得这篇文章是非常值得推荐的，阅读地址 http://drops.wooyun.org/web/3295 当然，如果还有小伙伴觉得有没有总结到的地方可以给 ecdragon@wooyun.org 发邮件，期待《密码找回功能可能樽仔的问题（续集）》哦。

WooYun WIFI 成长史

作者：lxj616

不管是不计其数的 wifi 安全报道还是跟随着乌云安全峰会兴起的国内安全会议“场里捞”无疑都让人对 wifi 安全越来越好奇 ,不少人对神器 wifi pineapple 垂涎欲滴但真正能得到的人少之又少。万能的乌云白帽在前辈们的基础上自己研究出了一款有乌云特色的审计路由，Wooyun WIFI,作者也在上一期乌云沙龙中给大家做了分享 ,没有听得过瘾的或者错过了上一次沙龙的小伙伴们可以仔细阅读这篇文章，lxj616 写得可仔细了，小编都能看懂呢。

阅读链接：http://drops.wooyun.org/tips/3248

.....

白帽专访月记

园长 MM 是不是妹妹

园长，这个 id 对很多人来讲都不陌生吧。小编对园长的认识最开始是哎呀好厉害的《攻击 JavaWe 应用》连载，后来才知道，那只是人家的读书笔记，当时就感慨呀同样是读书，差别咋就那么大呢。如果想要重温那 9 篇连载点击 http://drops.wooyun.org/author/%E5%9B%AD%E9%95%BF 访问比较快。当然，园长也有自己的网站，地址是：http://www.p2j.cn 。下面来和小编一起来揭开园长 MM 的神秘面纱吧

小编提问 1：园长啊你什么时候开始学网络安全的呢？为什么会选择学习安全？学习的动力是什么呀？

园长：我呀 2006 年的时候开始接触互联网，在网吧学会了免费上网（网吧还会教人免费上网？我读书少你可不要骗我！）。0 年的时候买了一本《黑防》开始了自学之旅。2010 毕业了本想学安全相关专业的那时候对安全的热情很高，但是没能找到相关的学校无奈学了软件开发。关于动力，不管是学习开发还是安全主要是兴趣。

小编提问 2：那你每天用多长时间来学习，如何合理休息呀？

园长：学不可以已，学习不可以停止（语文学得不错哦）。每天早上上班开始刷 iteye、bluereader 和 wooyun 了解一些新技术和新姿势。平时喜欢写一些简单的小东西练习下，经常为解决各种神奇的 bug 不得不熬夜。以前周末的时候总会约上几个小伙伴儿出来玩，当然不仅限于交流技术。（至于如何合理休息，园

长说“我最近的休息时间调整到 3 点睡觉 9 点起床已经比之前的 5 点睡 9 点起合理多了”）

小编提问 3：对于各种漏洞的灵活性如何学习会更加迅速？

园长：学开发，了解开发整个过程中最容易出问题的点才能更好的理解和利用安全漏洞（从园长 MM 的学习笔记中看确实是这样哦）。尤其是如今程序员安全意识有所提高，更多的漏洞可能来自于一些看似简单而有核心的业务。如：找回密码功能。学一些最基础的东西，比如：B/S 交互细节？Server 和 web 框架为我们做了什么？漏洞出现后快速了解并分析并记录，如果有必要可以写出利用文章和工具加强理解和记忆。

小编提问 4：那这样的话怎样确定学习方向？怎样有针对性的去学习呢？

园长：这主导于个人自身兴趣。如果只是想今后从事渗透测试之类的工作多一些可以学一些脚本语言 php 和 python 相对更加适合，不得不说 java 显得太重了。当然学什么语言不太重要，能满足自己需求足矣。工作或者学习之余可以多看看乌云积累一些经验、收集一些漏洞、收获一些姿势（小编绝对没有给园长广告费哦）。

小编提问 5：就算是非常厉害的大牛在学习中也会遇到问题吧，园长对如何更好地解决遇到的问题有什么建议呢？

园长：首先自然是 google baidu。如果还搞不定多是因为对某个姿势不了解导致的，学习一下相关的东西后再尝试解决。如果是程序开发相关问题 stackoverflow 基本都能找到答案。如果依旧无法解决可以请教下朋友或者去社区看下又没人遇到过，再发帖求助。有的时候不要自己挖个坑把自己埋了，有的

问题别人可能一眼就能给出解决方案。多花时间学基础，懂得太少问题自然会很多（这句话很中肯啊）。问题解决后最后写一篇博客记录下，以便帮助他人（园长 MM 真好）。

小编提问 6：园长啊你认为什么技能比较重要呢？

园长：学习方法是最重要的，只有学会了怎么去学遇到一个新的东西才能更容易上手。巩固基础，多实践，多独立去解决一些问题，请教他人之前自己应努力去解决。多与人交流相互之间学习下其他人的猥琐姿势。其次是要坚持自己的原则，远离黑产的诱惑。

.....

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东西都是有意义的，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。

欢迎联系我们：

网站 http://www.wooyun.org/

社区 http://zone.wooyun.org/

新浪微博 @乌云-漏洞报告平台

反馈意见、建议 help#wooyun.org