



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

教育网安全监测和主要安全威胁

上海交通大学

汪为农

2015.11.23



主要内容

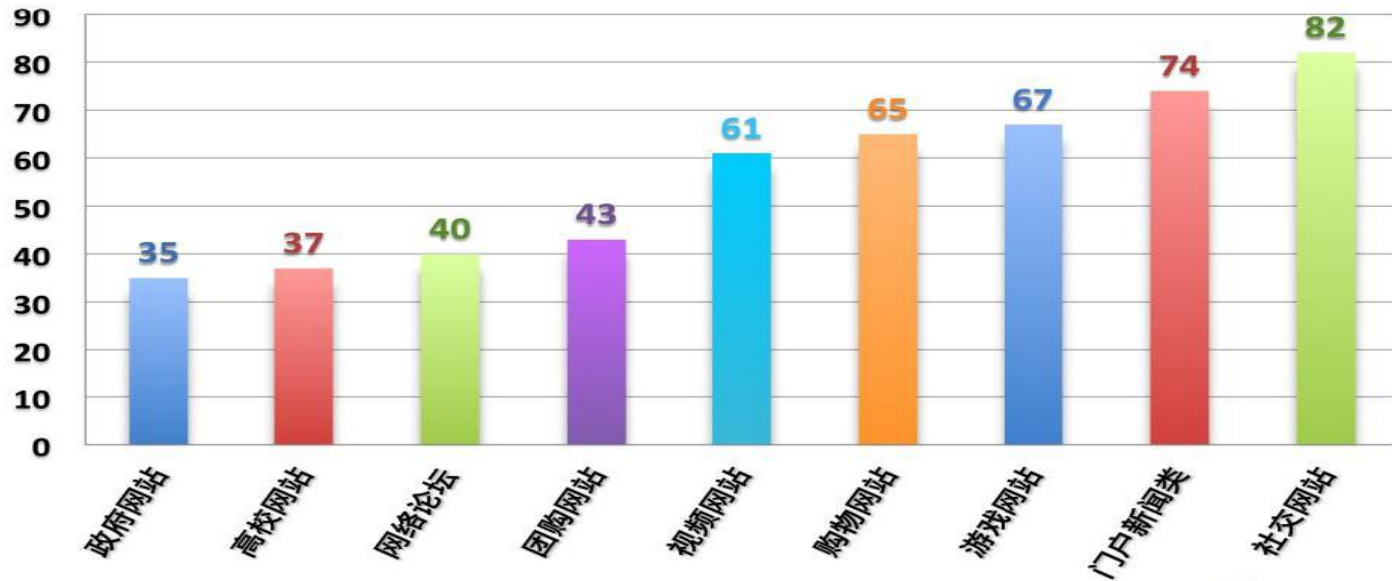
- 1、CERNET网络安全威胁监测
- 2、教育网当前主要安全威胁
- 3、高校应用系统安全问题举例



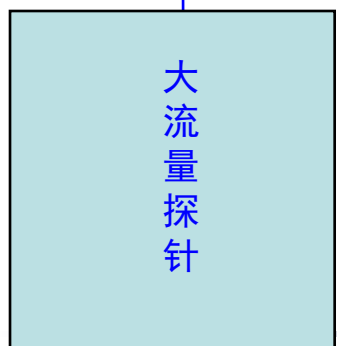
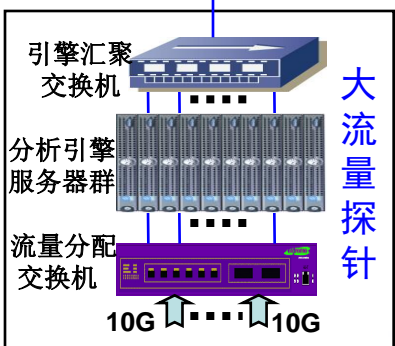
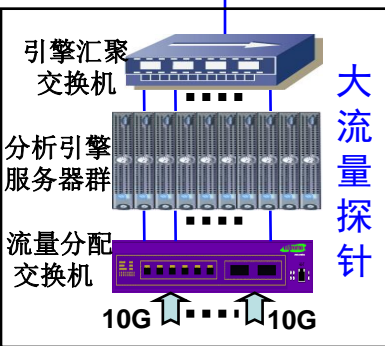
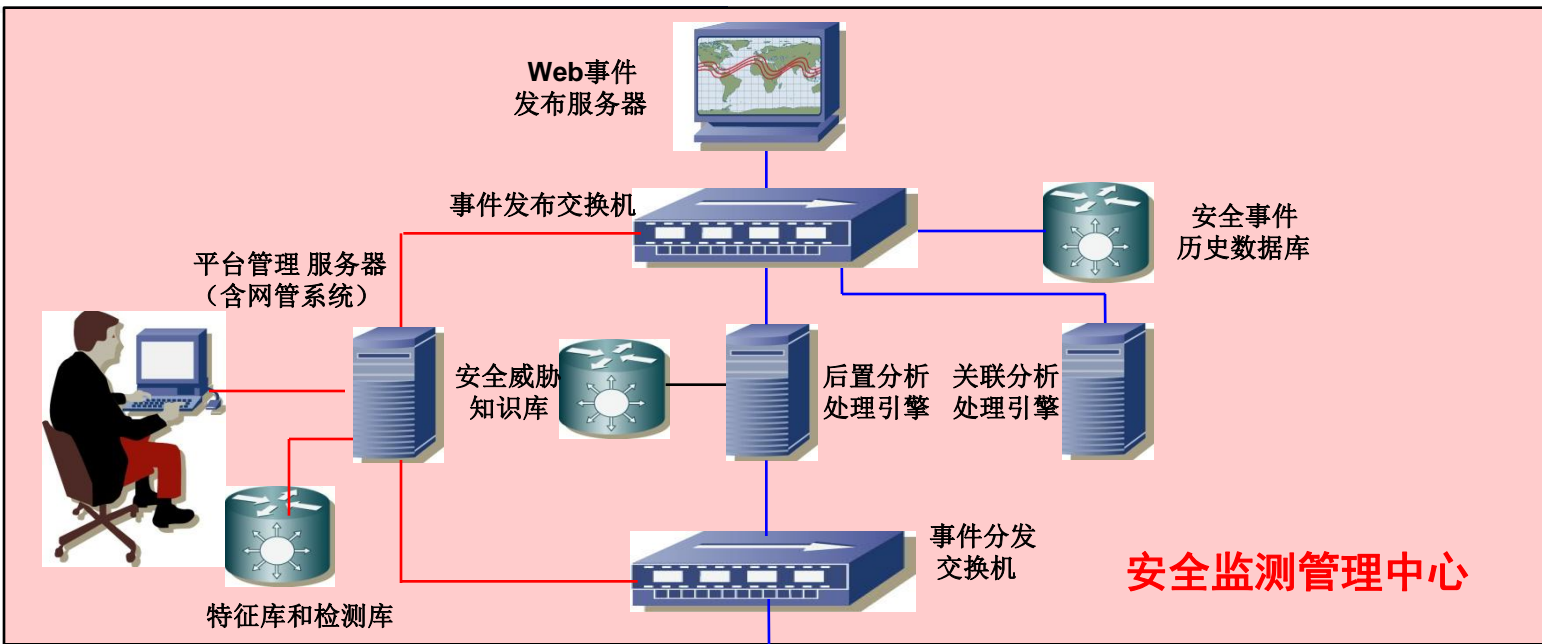
中国高校网站安全性排名全国倒数第二

“中国高校网站安全情况极差，在全国各类网站安全情况排名中，高校网站安全性排名倒数第二，意味着高校网站非常容易被黑客入侵、篡改和窃取资料。”

2012年国内各类网站安全性测评平均成绩



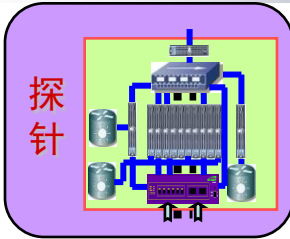
CERNET 网络安全实时监测平台架构 (2013)





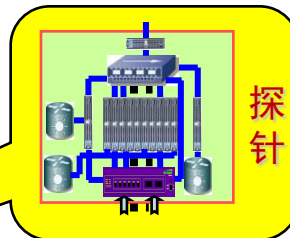
在CERNET上部署的系统 (2013)

CERNET主干网拓扑结构图



探针

北京公网交互点
监测流量: 40G

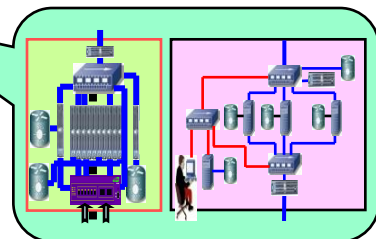


探针

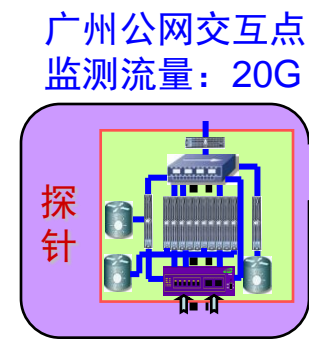
北京国际边界
监测流量: 20G



南京网络恶意
行为发布平台



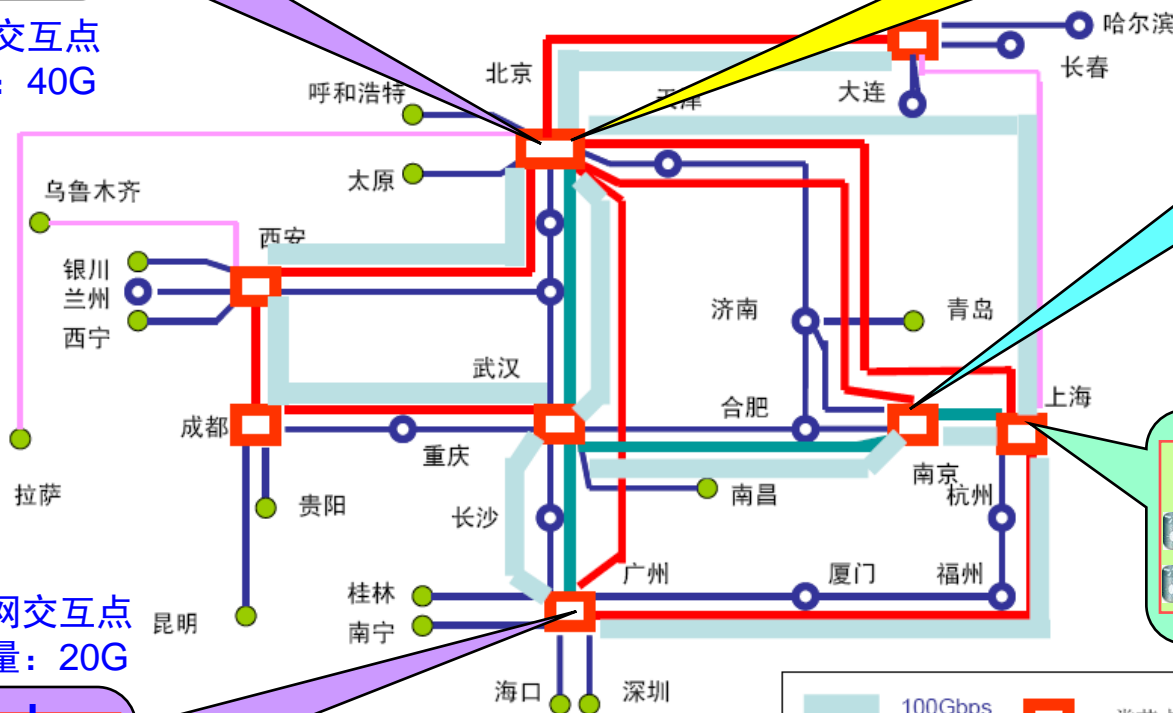
上海监测平台+探针
监测流量: 60G



探针

广州公网交互点
监测流量: 20G

监测总流量: 140G
发布对象: 38个省市节点网络中心



	100Gbps		一类节点
	40Gbps		二类节点
	20Gbps		三类节点
	10Gbps		
	2.5Gbps		



CERNET安全监测平台存在的主要问题

CERNET安全监测平台建成以来曾经发挥过一定作用，但由于各种原因，并没有为CERNET高校用户提供很好的安全服务，究其原因，主要是：

- 1、监测平台未有后续开发和进一步完善，安全威胁检测能力和检测效果尚有很大不足；
- 2、缺乏一个可长期持续发展的运维机构、运行机制和协作机制，依靠个别学校运维并为全国范围内的高校提供服务是不现实的；
- 3、安全监测平台核心价值在于具有能够及时和不断发现最新安全威胁的能力，这就需要一支很强的网络安全研究团队，对监测平台进行及时、有效维护，目前CERNET尚未组建这样一支团队。

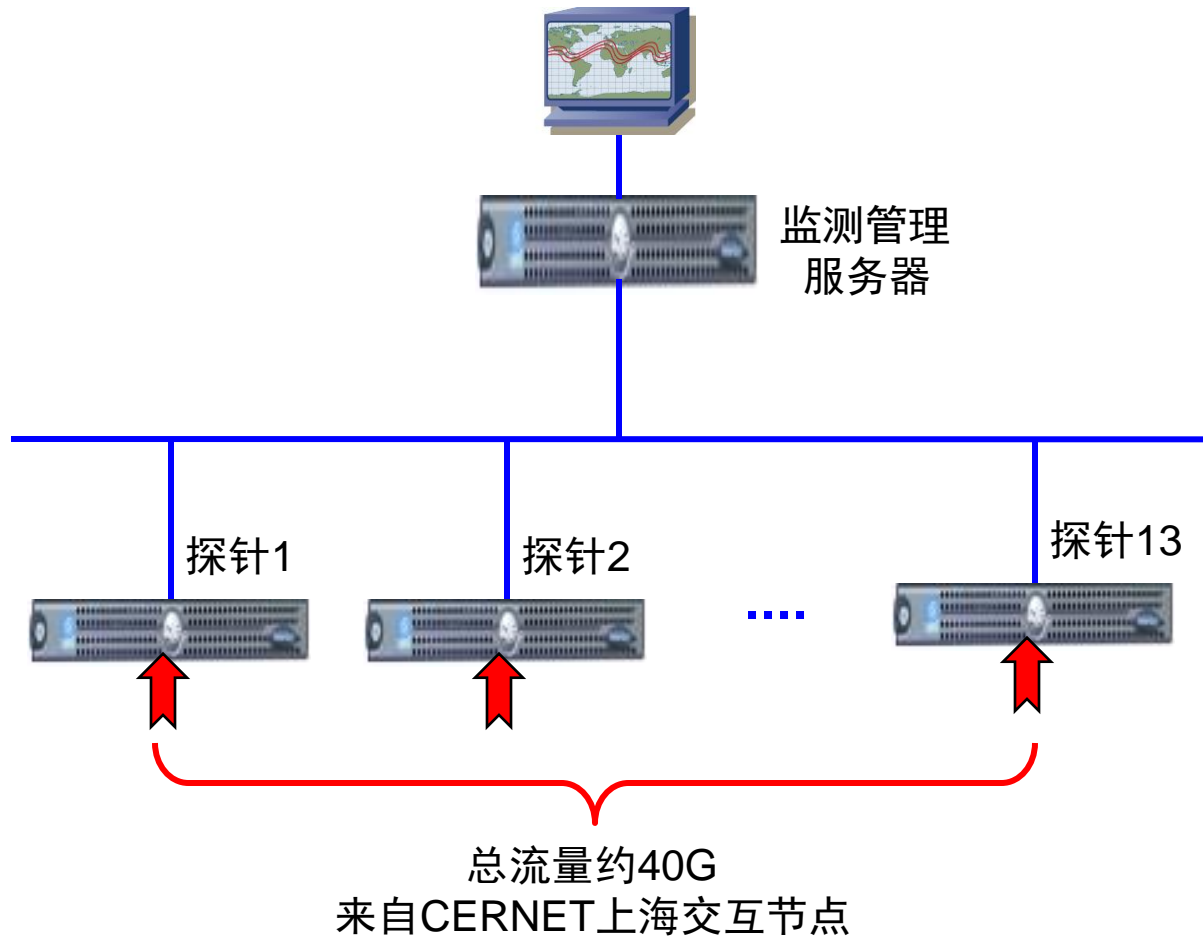
对CERNET全网的安全监测、安全运维和安全服务，赛尔公司是最合适的承担者，因此呼吁赛尔公司尽快地推进此项工作，帮助CERNET高校用户改善网络安全状况



一个新建安全监测试验系统(2015.9)

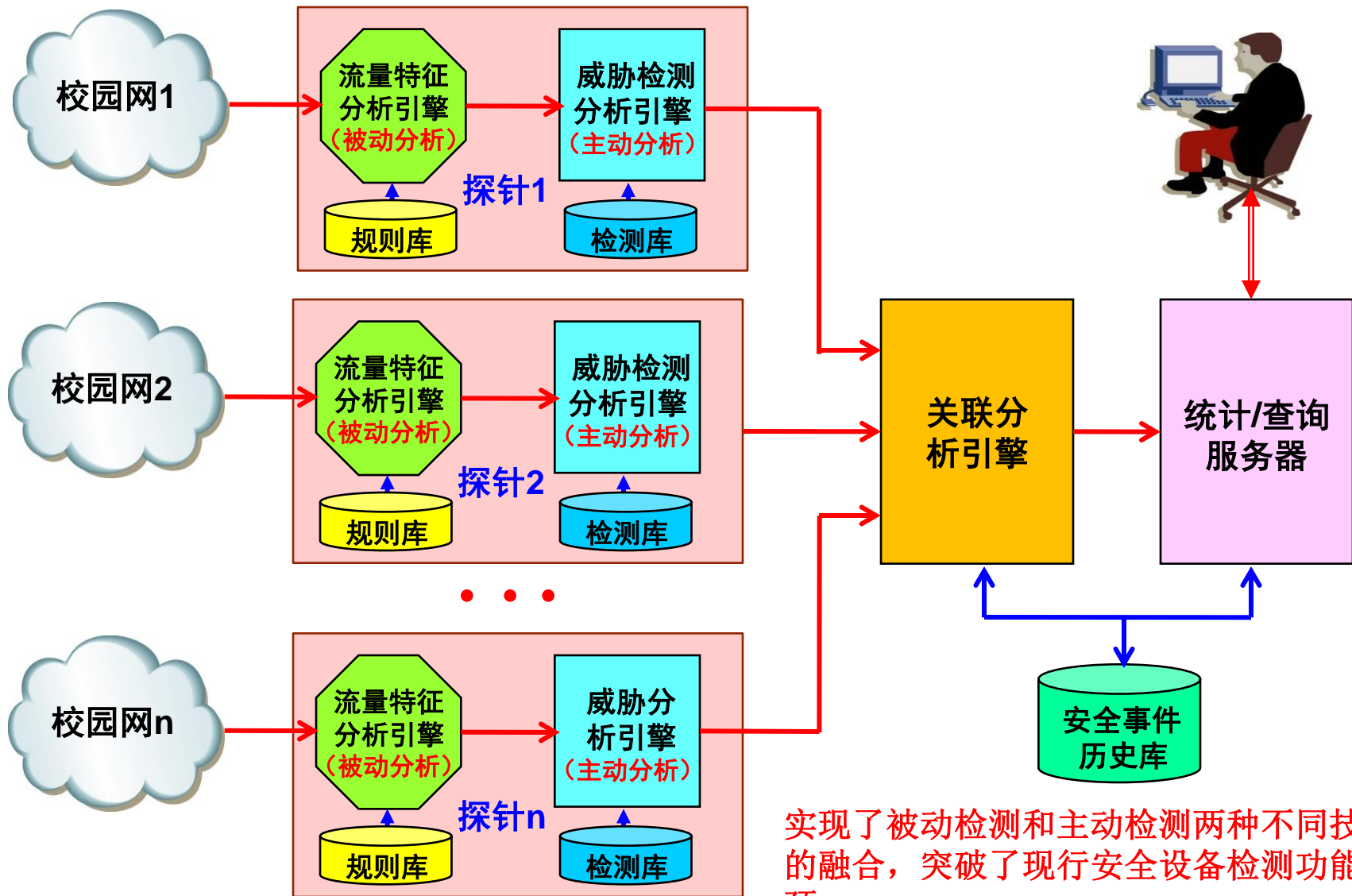
检测能力:

远程控制
僵尸网络
网站后门
网页篡改
漏洞利用
数据泄漏
网络盗号
网络欺诈
DDoS攻击





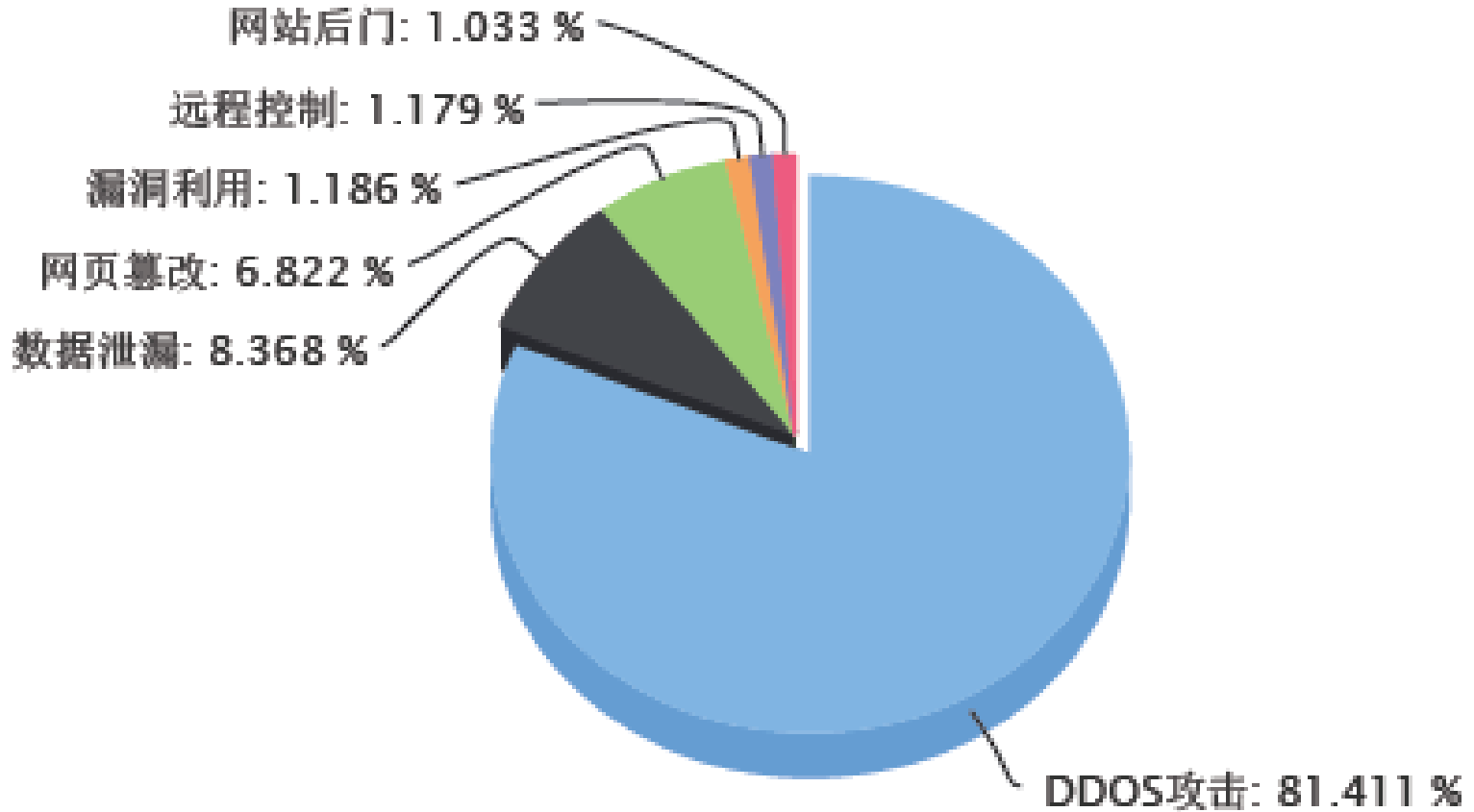
安全威胁分布监测系统三级引擎架构



实现了被动检测和主动检测两种不同技术的融合，突破了现行安全设备检测功能瓶颈。



教育网主要安全威胁种类分布



试验网监测结果，表明当前主要安全威胁是：

- 公共安全：DDOS攻击态势在网上日益严峻；
- 主机安全：远程控制、僵尸网络安全威胁长期存在，经久不衰；
- 网站安全：漏洞利用、网站后门和网页篡改是当前三大主要的网站安全问题。



基于僵尸网络的DDoS攻击

传统的DDoS攻击由僵尸网络组成，大量肉鸡在黑客控制下，向某一特定目标发起流量攻击，攻击流量取决于僵尸网络规模的大小。

基于网站的PHP shell DDoS攻击

通过网站漏洞入侵网站并上传PHP代码级的木马程序，黑客利用大量感染PHP木马网站服务器在同时对目标服务器发起攻击，形成大流量UDP/TCP DDoS 分布式攻击。

基于反射放大技术的DDoS攻击

利用互联网上广泛存在的、开放的服务资源，如DNS域名解析服务器、NTP定时服务器等，通过源地址欺骗实现流量反射，和通过小包长的服务请求获取大包长的服务响应实现流量放大，形成超大流量的DDoS攻击，这也是黑客当前主要的攻击手段。



反射放大DDOS攻击

1、原理

(1) 流量反射

UDP通信中，由于无连接源地址可以任意伪造，黑客发送一个伪造源地址的请求包，其应答包将会被送到伪造的IP地址，是一种反射攻击，具有高度隐蔽性，无法追踪黑客。

(2) 流量放大

一个小字节长度的请求包，返回一个很大字节长度的应答包，形成流量放大效应。DNS攻击流量放大倍数可达50-60倍，NTP攻击流量放大倍数可达200倍

2、常见反射 放大攻击资源

网上采用UDP协议且为公众提供服务的服务器都可能成为潜在DDOS攻击资源，如支持DNS、NTP、SSDP、SNMP等协议的设备。

3、泛在、高效、低成本的DDOS攻击平台

由于网上存在大量的可利用的DNS、NTP等服务器资源，因此DNS/NTP放大攻击已逐渐成为DDOS攻击的主流，DNS/NTP放大攻击流量曾达到300G（spamhaus）。



面对DDoS攻击的无奈

- 1、DDoS分布式拒绝服务攻击目的在于消耗网站等服务器资源或阻塞通信线路的带宽，破坏网络应用和网络服务，目前技术上几乎还没有有效的解决方案。
- 2、随着DDoS攻击工具的泛滥及地下黑色产业市场的发展，DDoS攻击越来越多，攻击流量越来越大。几年前DDoS攻击流量一般为1G左右，现在有些DDoS攻击流量已经上升到300G、500G，甚至1T流量级别，面对这样的攻击，对于一般的高校网络用户毫无招架之力，只能求助于电信运营商，但有时连电信运营商也难于有效应付。
- 3、针对DDoS攻击虽然有流量清洗设备可选择，但在大流量攻击情况下，由于接入带宽的限制，流量清洗设备对校园网用户根本解决不了问题，流量清洗设备只有在远端（主干网或接入网）才能发挥较好的作用（远端清洗策略），但运营商提供流量清洗业务高昂费用使得一般用户望而却步。



DDoS监测案例



NTP-DDoS监测案例



1、主干网上抑制源地址欺骗

- 不少洪泛攻击如SYN Flood、UDP Flood、ICMP Flood也采用伪造源地址的方法为对逃避攻击源的追踪；
- 反射放大攻击依靠将数据包的源地址篡改为攻击目标地址的方法实现流量向目标地址反射。

在主干网和用户网络接入点配置uRPF (Unicast Reverse Path Forwarding) 是单播反向路径转发检查，可有效抑制源地址欺骗。

uRPF通过获取包的源地址和入接口，以源地址为目的地址，在转发表中查找源地址路由对应的出接口是否与入接口匹配，如果不匹配，认为源地址是伪装的，丢弃该包。

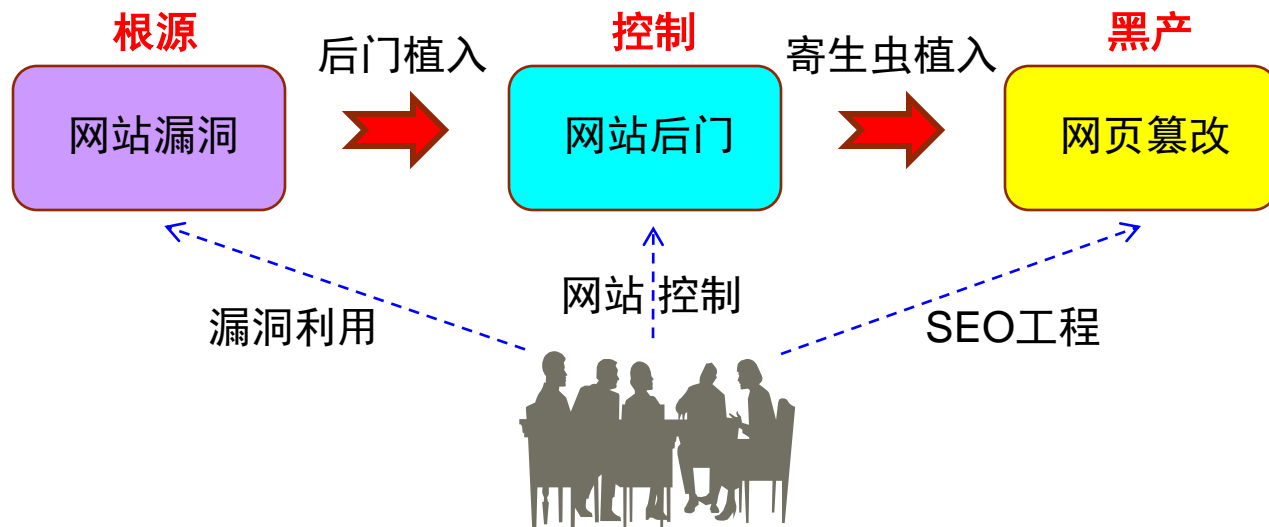
2、校园网中相关主机和服务器的管控（近源抑制策略）

不少校园网既是DDoS攻击的受害者同时也是DDoS的参与者

- **清理园区网中僵尸主机和肉鸡，以免被黑客利用去攻击他人；**
- **限定DNS、NTP等服务器只向信任的网络用户提供服务；**
- **控制SSDP协议通信范围；** SSDP是通用即插即用uPnP设备（如打印机、扫描仪等）简单服务发现协议，没有必要开放到公网上被黑客当枪使。

网站安全

网站已成为当今各种互联网应用的主要承载，而网站的安全问题构成网络安全的主要威胁。当前网站安全威胁主要包括：网站漏洞、网站后门和网页篡改，三者之间存在密切关联。



1、网站漏洞

网上大量网站存在陈旧的安全漏洞，除开源的**中间件漏洞**外，还有相当数量**应用系统漏洞**
中间件漏洞典型案例有5个：

Struts2远程命令执行漏洞

FCKeditor文件上传漏洞

ckfinder文件上传漏洞





Discuz!后台注入漏洞

eWebEditor数据库下载漏洞

2、网站后门

网站后门已成为黑客对网站实施控制和窃取数据的主要手段，网站后门主要有2大类：

(1) WebShell

几年前webshell作为主流网站后门充斥于问题网站，近年数量明显减少；

(2) 一句话木马

由于代码极其简单、易于变形、可嵌入其他文件或图片和隐蔽性好等特点受到黑客广泛青睐。



网站后门监测

3、网页篡改

网页篡改已成为黑色产业的一部分，由初期黑客手工篡改和维护，逐步向自动批量篡改，定时刷新方向发展，一个被黑客掌控的网站中被植入的篡改网页从几百到几万页不等。

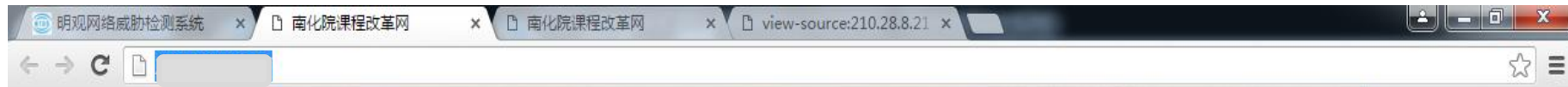


网页篡改监测



网页篡改(暗链)

http://210.: 217/



技术学院
课程改革专题

校内导航 >> 学院主页 院庆网 招生就业 学生工作 教务管 站内搜索：类别 文章标题 关键字 搜索

课改动态 更多>>

- [社教部信息] 社教部德育教研室召开教... 11-13
- [应化系信息] 以生为本, 补学补差一一... 11-13
- [教务处信息] [教务处信息] 新教师教学能力测试顺利进... 10-18
- [社教部信息] [社教部信息] 社教部刘俊芳老师参加省教... 9-29
- [应化系信息] [应化系信息] 《基础化学》课程分层次教... 9-27
- [社教部信息] 社教部召开《思想道德修养... 6-26

课改心得 更多>>

- ◆新教师岗前培训个人小结(图书馆 俞梦乐) 10-19
- ◆学习中成长 探索中前进(信息系 成建宇) 10-19
- ◆2012年度南化院新教师院内岗前培训学习... 10-19
- ◆新教师培训学习心得(党政外办 郭元龙) 10-19
- ◆成就人类灵魂的工程师的梦想(化工系 周... 10-19
- ◆2012年教师岗前培训学习体会(保卫处 ... 10-19

课改公告

150120240@qq.com

点击排行

- ◆拿什么献给你, 我的未来? (...)
- ◆南化院教师教学能力测试完成情...
- ◆[学院信息] 南化院课改培训...
- ◆课改培训小结
- ◆[江苏教育电视台消息] 南化...



学习材料 更多>>

- ◆教育部办公厅关于召开全国职业教育教学改革... 6-6
- ◆关于公布2013年职业教育与产业对话活动... 6-6
- ◆教育部办公厅关于下达职业院校教师素质提高... 6-6
- ◆江苏省教育厅 江苏省财政厅关于印发《“十... 10-29

课改成果 更多>>

- ◆[学院信息] 2013年江苏省普通高校本... 3-3
- ◆[学院信息] 关于表彰2013年全国全省... 2-25
- ◆[学院信息] 我院两门课程入选国家级精品... 12-24
- ◆[学院信息] 2013年新教师教学能力测... 10-15

友情链接

- 全国高校精品课程网
- 中国职业核心能力网
- 江苏省教师国际合作培训网
- 中国教育信息网



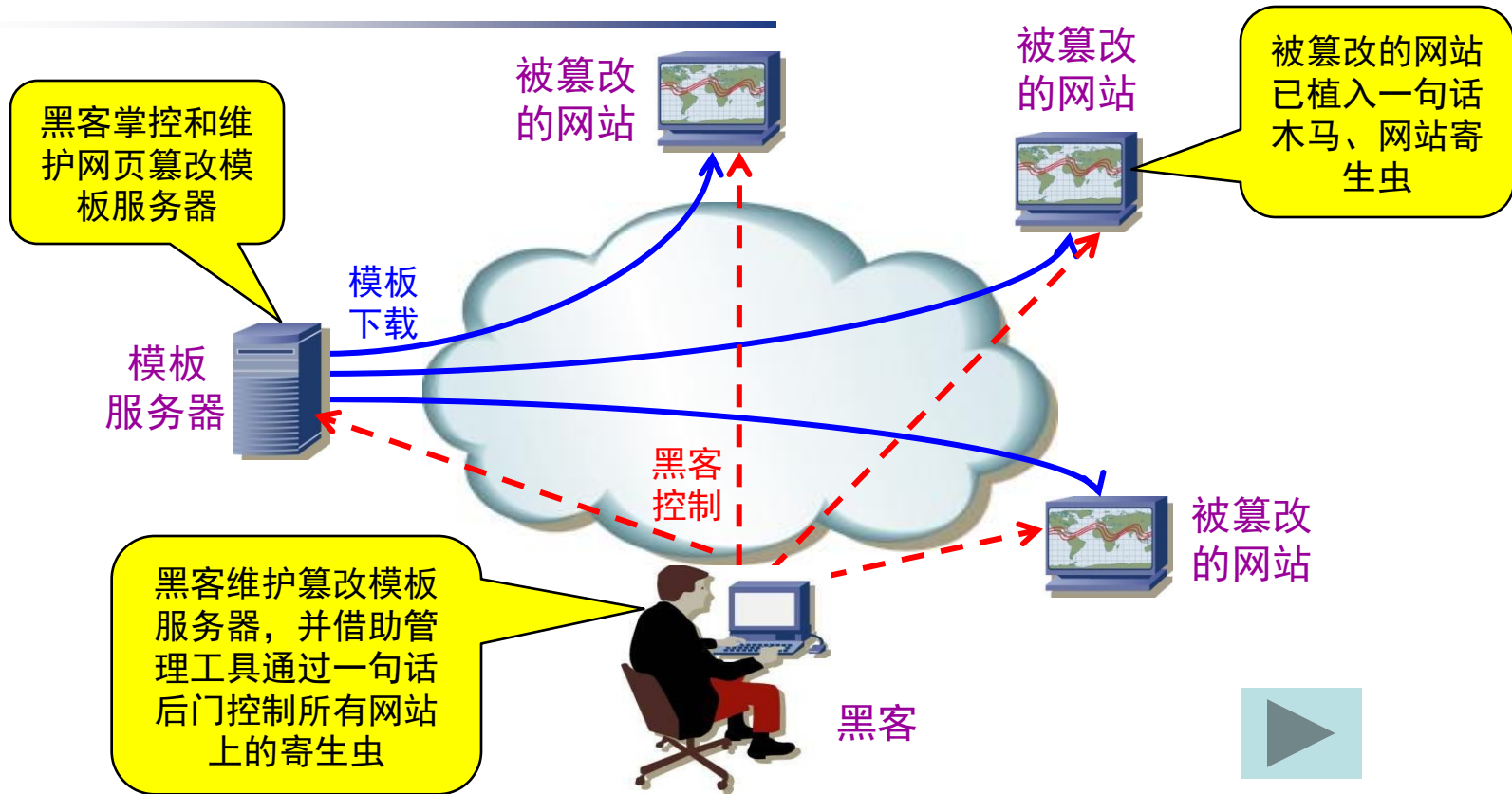


网页篡改(暗链)

```
文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
明观网络威胁检测系统 x 明观网络威胁检测系统 x 明观网络威胁检测系统 x file:///C:/U...网页篡改暗链.html x +
file:///C:/Users/wnwang/Desktop/教育网监测/网页篡改暗链.html 搜索
</TD>
</TR></TBODY></TABLE>
</div><div id="ImportantPage">
<a href="http://www.chuanqizhifu.co.cc">传奇开区一条龙</a>
<a href="http://www.chuanqisi195.co.cc">新传奇外传好玩吗</a>
<a href="http://www.chuanqishifu.co.cc">天翼脱机挂</a>
<a href="http://www.chuanqisf185.co.cc">激情服</a>
<a href="http://www.chuanqisf180.co.cc">传奇外挂论坛</a>
<a href="http://www.chuanqi3ditu.co.cc">私服游戏</a>
<a href="http://www.chuanqi17205.co.cc">加速外挂</a>
<a href="http://www.chiyuehaomen.co.cc">辉煌传奇</a>
<a href="http://www.chibichuanqi.co.cc">访逐鹿传奇</a>
<a href="http://www.bazheyinyue.co.cc">帝王传奇</a>
<a href="http://www.baqitianying.co.cc">cq私服</a>
<a href="http://www.baitanbuding.co.cc">传奇名字符号</a>
<a href="http://www.meiguishu.co.cc">传奇名字</a>
<a href="http://www.huanjing.co.cc">1.96轻变内挂无英雄黄金皓月</a>
<a href="http://www.hejisifa.co.cc">虎啸祥瑞传奇</a>
<a href="http://www.haosf176.co.cc">jjj.cm传奇</a>
<a href="http://www.gangkaif.co.cc">传奇师傅网</a>
<a href="http://www.fuwudian.co.cc">传奇私服版本购买</a>
<a href="http://www.fuguheji.co.cc">万宇论坛</a>
<a href="http://www.fanawuvi.co.cc">1.76彪哥蓝魔传奇</a>
```



基于网站寄生虫的批量网页篡改

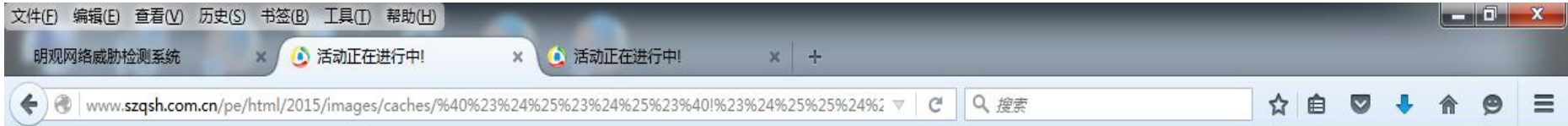


- 1、黑客利用网站漏洞在拿下众多网站后，分别植入一句话后门，并通过一句话后门批量植入网站寄生虫，在黑客触发下寄生虫可在网站上大量自我繁殖。
- 2、网站寄生虫在黑客远程控制下定时从黑客指定的网页篡改模板服务器下载各种不同网页模板或挂链内容，并在网站随机目录下生成大量篡改网页。
- 3、除了安全漏洞外，一个受害的网站往往包含了3种恶意代码：**一句话后门、网站寄生虫和篡改的网页**，且每种恶意代码数量不止一个。



冒充腾讯中奖欺诈

<http://www.szqsh.com.cn/pe/html/2015/images/caches/%40%23%24%25>



正在进行的活动

 腾讯网
qq.com

来自腾讯QQ系统发给您的消息

尊敬的QQ用户：恭喜您的QQ号已被系统抽选中为“二等奖”幸运用户
您将获得奖金【¥12,000元】人民币与苹果笔记本电脑一台！

请记住您的验证码 **【5168】**



登陆领奖



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

被黑客篡改为钓鱼网站

http://: .jx.cn/

浏览器地址栏: zsb.asc.jx.cn

网站导航: 招生首页 | 走进应科 | 报考指南 | 专业介绍 | 录取查询 | 招生咨询 | 联系我们

学院公告

专业设置

经济管理系

院内动态 >> 更多

招生计划 >> 更多

录取查询 ADMITTED THE QUERY

招生咨询 在线问答

江西理工大学应用科学学院

志存高远 责任为先

2015江西招生计划



骗取银行账号等信息

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

明观网络威胁检测系统 × 明观网络威胁检测系统 × 活动正在进行中! × 活动正在进行中! × +

:/default/label_tpl/article/caches/%40%23%24%25%23%24%25%23%40!%23%24%25% ▾ ↻ 🔍 搜索 ☆ 自 下载 家 消息 三

性别: 请选择您的性别,以便公司对您的称呼。

相关证件类型: 请您选择有效证件

证件号码: 请认真填写当您奖品到时,凭着您选择的证件领取

领奖人的信息

联系电话: 非常重要,请认真填写方便本公司与您联系领奖事宜!

收件详细地址: 请认真填写以便公司把您奖品邮寄到您当地

邮政编码: 您填写地址的邮政编码

领奖的银行账户

所属银行类型: 您领取奖金的银行类型

银行帐号: 您的奖金将会通过网银转到这个账户,务必准确无误!



骗交保险抵押金

明观网络威胁检测系统 x 活动正在进行中!

1/tools/catalog/view_msg/arclistsg/caches/%40%23%24%25%23%24%25%23%40!%23%24%25%25%24%23%23%40/ne



恭喜您

您已登记成功!

温馨提示： 亲爱的幸运用户，办理领取个人所得到的奖金以及奖品的手续费由个人自己支付！

腾讯客服热线: 010-57103283

腾讯公司地址: 深圳市高新科技园南区高新南一道飞亚达高科技大厦3-10

下面是收费详细说明。



注明

太平洋保险抵押金收取说明：本次活动送出的奖品属于贵重物品，奖金属于高额奖金！根据中华人民共和国相关法律条文规定！属于正规举办的活动，必须经过权威有效部门公证后方可举办！举办活动奖品金额高于1万元人民币，必须有相关风险部门承担安全担保。因为相关物品属于贵重物品，活动奖金属于高额奖金，所以必须承担奖品运送风险安全以及银行转帐奖金业务高出5万元人民币，必须由获取方购买相关金额担保。

为了保障获奖的权利，本次活动二等奖幸运用户必须办理奖项的风险保证手续。

保险抵押金为**5000元**，必须交纳保险抵押金后本公司才发送奖金及奖品。

为了避免获奖用户与本公司在领取奖项过程中产生任何的纠纷事件，所产生的任何费用，不能在奖金里面扣除，经过司法部门公证处拟订的条款。获奖用户必须事先承担以下的领取手续费用！

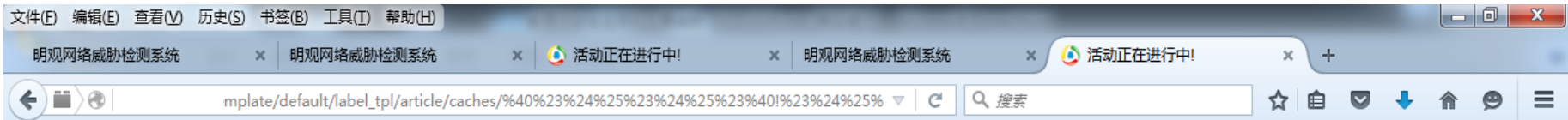
注：在您顺利签收到奖品后，保险抵押金：**5000元**将全额返还到您指定银行帐户上！

活动正在进行中!-4.html

显示所有下载内容...



诱骗银行支付



开户银行	账户	收款人	缴纳费用
 中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA	联系客服索取	王玲	¥ <u>5000</u>
 中国农业银行 AGRICULTURAL BANK OF CHINA	联系客服索取	王玲	¥ <u>5000</u>
 中国建设银行 China Construction Bank	联系客服索取	王玲	¥ <u>5000</u>
 中国邮政 CHINA POST	联系客服索取	王玲	¥ <u>5000</u>



注：以上银行账户由公司名誉开户，请幸运用户放心办理，若选择银行柜台办理请携带本人身份证
最快捷的方式是通过ATM柜员机直接现金转账到以上帐号中的任意一个。

唯一指定客服热线：0755-3637-9830



传至第三方服务器的用户信息

明观网络威胁检测系统 x

View/frame.php

NTDS 网络威胁检测系统 Network Threat Detect System

系统信息

查询统计

威胁事件数据列表

事件类别选择

僵尸网络 DDOS攻击 数据泄漏

日期/时间
2015-11-18 12:37:14
2015-11-18 11:39:23
2015-11-18 10:45:41
2015-11-18 10:45:34
2015-11-18 10:31:16
2015-11-18 10:21:10
2015-11-18 09:33:05
2015-11-18 00:56:00
2015-11-17 23:10:09
2015-11-17 22:34:08
2015-11-17 22:33:19
2015-11-17 22:07:59
2015-11-17 18:06:00

mo
bile=12435623&real_name=%CA%C7%C4%E3%C2%F0&sex=%C5%AE&card_type=%BE%FC%C8%CB%D6%A4&card=423536143&post_tel=15157632568&addr=shanghai&post_code=123112&bank=%D6%D0%B9%FA%C3%F1%C9%FA%D2%F8%D0%D0&bank_card=4512354363412342314&bank_username=%CA%C7%C4%E3%C2%F0&zhiye=%BC%C6%CB%E3%BB%FA%2FIT%D2%B5&cip=111.198.29.250&x=135&y=41

&mobile=12435623

&real_name=是你吗

&sex=女

&card_type=军人证

&card=423536143

&post_tel=15157632568

&addr=shanghai

&post_code=123112

&bank=中国民生银行

&bank_card=4512354363412342314

&bank_username=是你吗

&zhiye=计算机/IT业

关于产品
退出系统

过滤/误报



传至第三方服务器的用户信息

real_name=苏
sex=男
card_type=身份证
card=11010819530
post_tel=1025365
addr=北京市海淀区
西南7楼: 号
post_code=100084
bank=中国建设银行
bank_card=621700
9 5
bank_username=苏
zhiye=教师

qq=1779034
type=邮寄领取
real_name=周
sex=女
card_type=身份证
card=6104031965
&addr=天津市津南区
育园区内雅观路1
post_tel=1337037
bank=中国建设银行
bank_card=4367+420
4+110: 4
bank_username=周

userqq=250396:
type=邮寄领取
real_name=吴
sex=男
card_type=身份证
card=3624281992(7712
post_code=430074
addr=湖北省武汉市洪山区关
山街道华中科技大学 舍
post_tel=1582731 !
bank=中国邮政储蓄
bank_card=6217+9943+500
0+1007+3697· 00+1
007
bank_username=吴





上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

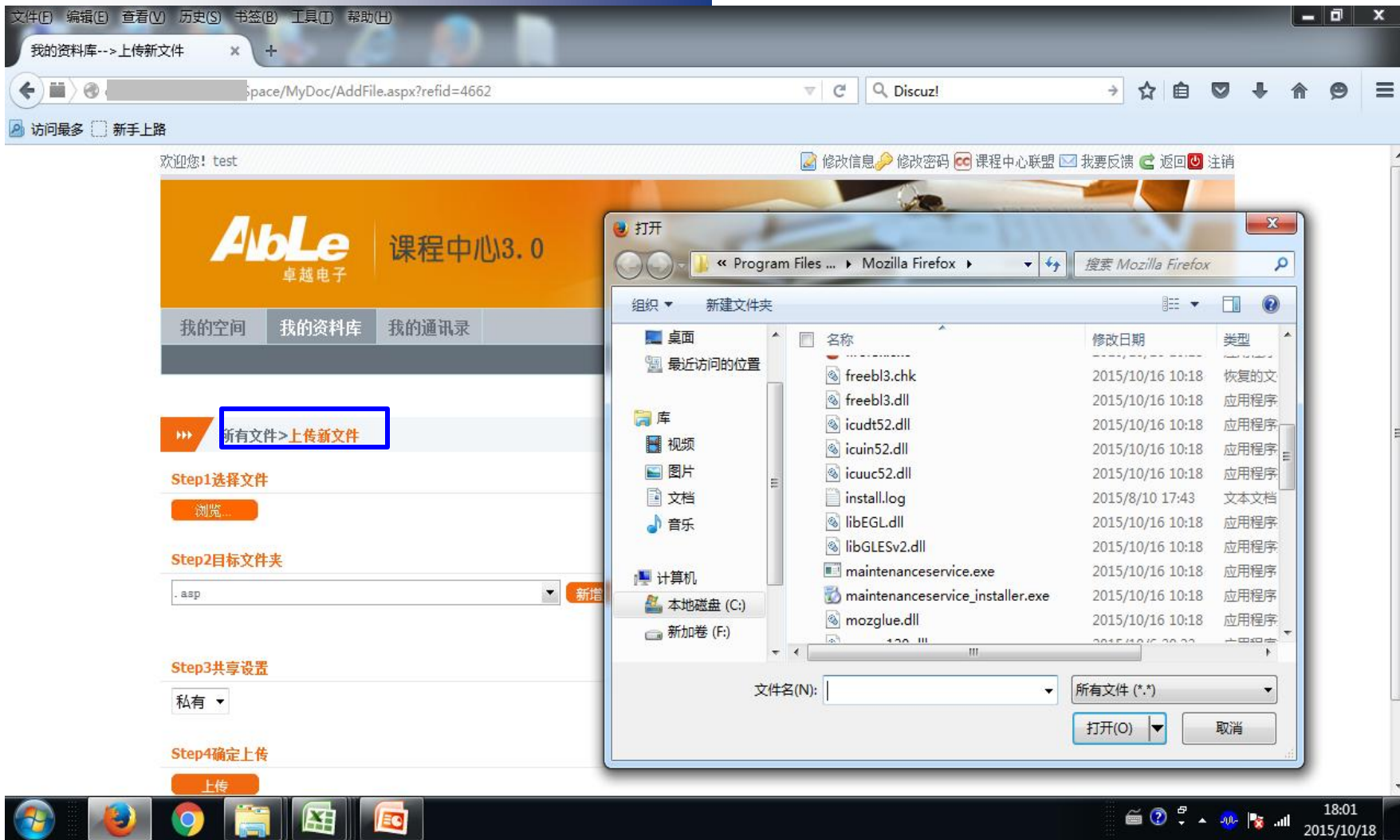
卓越课程中心缺省口令漏洞(管理漏洞)

The screenshot shows a web browser window displaying the Shanghai Business School Course Center website. The URL in the address bar is 55/G2S/ShowSystem/index.aspx. The page features a navigation menu with options like '首页', '教学组织', '专业设置', '课程资源', '师资队伍', '教学成果', and '教学服务'. A login form is visible in the top right corner, with fields for '用户名' (Username) and a password field, along with '统一认证' (Unified Authentication) and '登录' (Login) buttons. Below the navigation menu, there are sections for '热门课程' (Popular Courses), '热门人物' (Popular Figures), and '热门视频' (Popular Videos). The '热门课程' section lists several courses, including '大学英语 姜荷梅' (297549), '职业生涯规划与管理 陈敏' (280807), and '面向对象程序设计与Java 胡巧多' (81025). A large white box is overlaid on the right side of the page, partially obscuring the '新闻公告' (News and Announcements) section. At the bottom of the page, there is a red text overlay that reads: 用缺省账号：test/test就可进入系统 (Use default account: test/test to enter the system).

用缺省账号：test/test就可进入系统



卓越课程中心缺省口令漏洞(管理漏洞)



除了可以修改账号外，在“我的空间”—>“我的资料库”可以上传任意文件



LDAP服务器匿名访问(管理漏洞)

The screenshot shows the JXplorer application window. The main interface includes a menu bar (档案, 编辑, 检视, 书签, 搜寻, LDIF, 选项, 工具, 安全, 说明), a toolbar, and a search bar with the text 'cn'. A dialog box titled '开启 LDAP/DSML 联机' is open in the foreground. The dialog box contains the following fields and options:

- 主机: 202.120.x.x
- 端口: 389
- 协定: LDAP v3
- DSML 服务: (empty)
- 选值的值: (empty)
- 基底 DN: (empty)
- 安全: 层级: 匿名
- 使用者 DN: (empty)
- 密码: (empty)
- 使用模板: 储存 (dropdown), 删除, 预设
- Buttons: 确定, 取消, 说明

The background window shows a file browser view with 'HIML 检视' and 'simple.html' visible. The status bar at the bottom left of the window displays '没有连接'.



LDAP服务器匿名访问(管理漏洞)

JXplorer -

档案 编辑 检视 书签 搜寻 LDAP 选项 工具 安全 说明

快速搜寻

展开 结果 概要

- zang-sj
- zbxiao
- zfcso
- zhang-dm
- zhang-fy
- zhang-gy
- zhang-lq
- zhang-ss
- zhang-tz
- zhang-wd
- zhang-yy
- zhangyz
- zhangyz
- zhang-zh
- zhang-zn
- zhaohai
- zhao-jj
- zhaorun
- zheng-gy
- zhonghao
- zhou-hy
- zhou-jy
- zhou-wei
- zhrong
- zhuang-th
- zhuangying
- zhu-hj
- zou-hm
- zqliu**

attribute type	value
subschemaSubentry	cn=Subschema
structuralObjectClass	person
modifyTimestamp	20101229065507Z
modifiersName	cn=admin, dc=cs, dc=sjtu, dc=e...
hasSubordinates	FALSE
entryUUID	50bed91a-a764-102f-8c15-4d4...
entryDN	uid=zqliu, ou=people, dc=cs, d...
entryCSN	20101229065507.352258Z#0000...
creatorsName	cn=admin, dc=cs, dc=sjtu, dc=e...
createTimestamp	20101229065507Z
cn	Liu Zhiqiang
gidNumber	1200
homeDirectory	/home/zqliu
objectClass	person
objectClass	posixAccount
sn	Liu
uid	zqliu
uidNumber	1133
loginShell	/bin/bash
mail	zqliu@cs. sjtu.edu.cn
ou	people
accountActive	
description	
gecos	
seeAlso	

送出 重设 更改类别 属性

连接到 'ldap://202.120.38.143:389'



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

Discuz!后台注入漏洞(中间件漏洞)

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

http://yzblt...y%20x)a)%23 x 上

注册 登录

财经大学
研究生招生办公室

论坛 搜索 帮助 导航

上海财经大学研究生招生论坛 > 首页

发帖 你可以注册一个帐号,并以此登录,以浏览更多精彩内容,并随时发布观点,与大家交流。

论坛版块 论坛动态 今日: 0, 昨日: 0, 会员: 41274

招生政策 分区版主: admin, yzbhan

硕士招生 6279 / 22155
只解答政策类问题。复习交流类请去“学院天地”相应板块,勿“在线等”,有急事请致电
021-65903795/65...ruitment
/planSearchAll.do?method=home查询

博士招生 792 / 2590

港澳台招生

国内大部分论坛网站都采用开源Discuz!论坛软件系统，但不少版本的Discuz!存在后台注入漏洞。



Discuz!后台注入漏洞(中间件漏洞)

Discuz! info: MySQL Query Error

Time: 2015-10-18 5:12pm
Script: /faq.php

SQL: SELECT * FROM [Table]usergroups u LEFT JOIN [Table]admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('7','\') and (select 1 from (select count(*),concat((select concat(0x5E5E5E,username,0x3a,password,0x3a,salt) from [Table]uc_members limit 0,1),floor(rand(0)*2),0x5E)x from information_schema.tables group by x)a)#')

Error: Duplicate entry '^'^^admin:4cb7c7120^'^^39153b1c:8af7a21^'^^' for key 'group_key'

Errno.: 1062

Similar error report has been dispatched to administrator before.

到 <http://faq.comsenz.com> 搜索此错误的解决方案

admin:4cb7c7120^'^^ee0d9a399153b1c:8af7a21^'^^

天翼财务系统远程代码执行漏洞(中间件漏洞)

红杏台歌--C x 明观网络威 x 欢迎访问南 x 明观网络威 x 明观网络威 x 网络安全监 x 网络安全监 x 明观网络威 x 明观网络威 x

WFManager/login.jsp

大學 财务处 综合信息门户

信息公告 Information

广大师生：
学财务处综合信息门户已全新改版，
欢迎使用!

全新改版
欢迎使用

用户登录 Login in

用户名:

密 码:

验证码: 6208

登录

财务新闻 News

- 2014年工资说明
- 关于部属高校开展科研经费管理专项检查的情况介绍
- 到账查询 (2013.1.1-2013.5.15)
- 关于个人所得税的说明

wingsoft

您是本系统的第 4691816 位访问者

天翼财务系统远程代码执行漏洞(中间件漏洞)

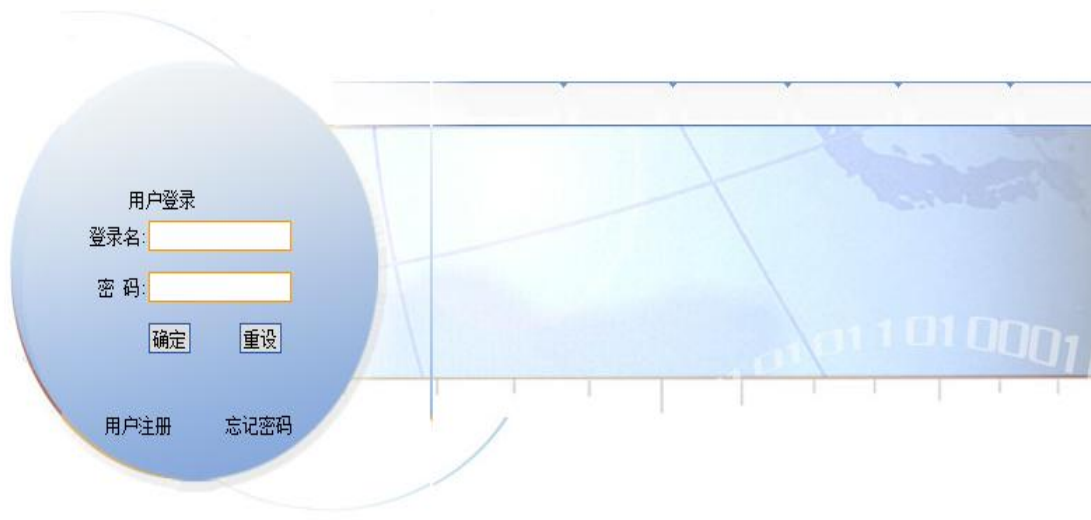


该财务系统采用了开源应用程序框架Struts2，Struts2漏洞导致黑客可远程执行任意命令包括文件上传和下载等。

科发高校财务管理系统权限绕过漏洞(应用漏洞)



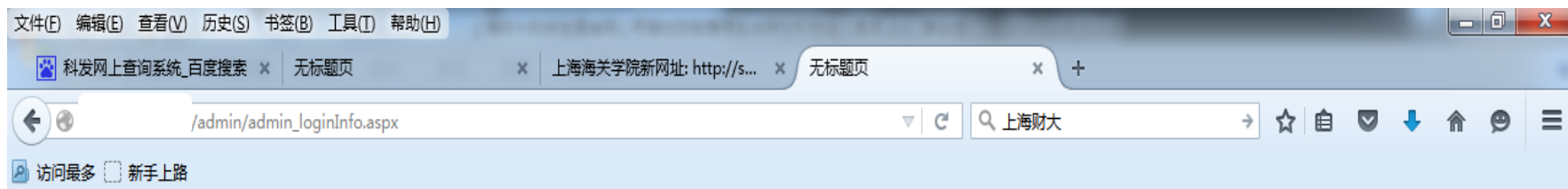
财务信息综合查询系统



上海一高校科技发展有限公司开发
产品名称：科发网上查询系统

共有4处漏洞

科发高校财务管理系统权限绕过漏洞(应用漏洞)



	登录用户名	登录用户姓名	用户权限	财务管理	工资管理	收费管理	数据管理
删除 修改	Admin	管理员	√	√	√	√	√
删除 修改	系统管理员	system	√	√	√	√	
删除 修改	wls	管理员一	√	√	√	√	
删除 修改	test	管理员二	√	√	√	√	
删除 修改	jlsu	jlsu		√	√	√	

管理员添加和修改

科发高校财务管理系统权限绕过漏洞(应用漏洞)

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

科发网上查询系统_百度搜索 x 无标题页 x 无标题页 x 无标题页 x +

v/admin/GenerateRegUser.aspx 科发网上查询系统

访问最多 新手上路

人员信息 部门信息

增加	导入	更新	工号:	姓名:	查询	个人账务	个人往来	往来汇总	项目查询	项目汇总	工资查询	工资汇总	收费汇总	特
修改 删除	0001	赵	2201041	712443x	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0002	张	3701021	1213337	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0009	宋	2201021	1240216	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0025	王	2201051	315224X	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0038	李	2205811	290371	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0047	徐	2204021	1296410	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0069	臧	2201021	1123319	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0090	高	2201021	1233345	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0112	钟	2203221	1240613	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
修改 删除	0134	杜	2290041	125080520	学院办公室	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

总人数: 650 页码: 1/65 首页 上一页 [1] 2 3 4 5 ... 下一页 尾页 转到 1 页

人员添加修改和个人信息泄露

科发高校财务管理系统权限绕过漏洞(应用漏洞)

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

科发网上查询系统_百度搜索 x 无标题页 x 无标题页 x 无标题页 x 无标题页 x +

cn/admin/UserManager.aspx 科发网上查询系统

访问最多 新手上路

工号或姓名: 过滤 清除的用户名: 清除

	用户名	工号	姓名	所在部门	注册时间	最近登录时间	权限查询
封存 正常 密码初始 清除	0001	0001	赵冠一	学院办公室	2014/12/19 10:00:12	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0002	0002	张琼	学院办公室	2014/12/19 10:00:12	2015/10/11 14:22:37	查询权限
封存 正常 密码初始 清除	0009	0009	宋维	学院办公室	2014/12/19 10:00:12	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0025	0025	王月	学院办公室	2014/12/19 10:00:13	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0038	0038	李祚	学院办公室	2014/12/19 10:00:12	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0047	0047	徐睿	学院办公室	2014/12/19 10:00:13	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0069	0069	臧德	学院办公室	2014/12/19 10:00:14	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0090	0090	高源	学院办公室	2014/12/19 10:00:13	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0112	0112	钟涛	学院办公室	2014/12/19 10:00:13	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0134	0134	杜涛	学院办公室	2014/12/19 10:00:13	2015/10/20 10:18:27	查询权限
封存 正常 密码初始 清除	0381	0381	刘峰	学院办公室	2014/12/19 10:00:13	2015/10/17 20:21:33	查询权限
封存 正常 密码初始 清除	0023	0023	姜洪	组织部	2014/12/19 10:00:13	2015/10/20 14:49:01	查询权限
封存 正常 密码初始 清除	0095	0095	勾峰	组织部	2014/12/19 10:00:13	2015/10/9 15:21:44	查询权限
封存 正常 密码初始 清除	0245	0245	牛娟	组织部	2014/12/19 10:00:13	2015/10/9 15:21:45	查询权限

注册用户添加、删除和口令修改

新中大大学一卡通系统管理员密码重置漏洞(应用漏洞)



用 `http://域名/managerEditNManager.action?id=1`
就可直接进入后台

新中大一卡通系统管理员密码重置漏洞(应用漏洞)

浏览器地址栏显示: `/managerEditNManager.action?id=1`

用户信息

用户名	<input type="text" value="WEBMANAGER"/>
密码	<input type="password" value="....."/>
密码确认	<input type="password" value="....."/>
校区名称	<input type="text" value="....."/>
所在单位	<input type="text" value="系统管理员"/>

确定 重填 返回

存在三大安全威胁:

- 1、管理员WEBMANAGER口令可重置;
- 2、查看网页源码可获得管理员口令密文;
- 3、递增`http://域名/managerEditNManager.action?id=1`中`id=1`参数可遍历所有持卡用户的账号

新中大一卡通系统管理员密码重置漏洞(应用漏洞)

```
源: http://managerEditNManager.action?id=2 - Mozilla Firefox
文件(F) 编辑(E) 查看(V) 帮助(H)
83 form1.action="managerDoEditNManager.action";
84 form1.submit();
85 return(1);
86
87 }
88 function doReset(){
89     form1.reset();
90 }
91 //-->
92 </script>
93 <body topmargin="5">
94 <form name="form1" method="post">
95 <input type="hidden" name="hiddenPasswd" size="20" value='26BF601 40925' >
96 <input type="hidden" name="name" size="20" value='YKT' >
97 <table width="100%" border="0" cellpadding="0" cellspacing="0" >
98 <tr>
99 <td width="23%" height="33" align="center" background="/images/style1/biaotoul.jpg" class="baizi">用户信息 </td>
100 <td width="77%" align="left" background="/images/style1/biaotou2.jpg" class="baizi">&nbsp;  </td>
101 </tr>
102 </table>
103 <table align="center" width="95%" border="0">
104 <tr>
105 <td colspan="3" scope="col">
106 <table width="95%" class="dangrichaxun">
107 <tr class="listbg">
108 <th width="238" height="21" class="neiwen" scope="col" align="right">用&nbsp;  户&nbsp;  名</th>
109 <td width="87%">
110 <input type="hidden" name="id" value='2'>
111 <input class="and" type="text" name="username" size="19" value='YKT' >
112 </td>
113 </tr>
```

size="20" value='26BF601 40925' >
size="20" value='YKT' >

size="20" value='26BF601 40925' >
size="20" value='YKT' >



西安知先三才期刊采编系统文件包含漏洞

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

URP 综合教务系统 - 登录 x 正在连接... x 新标签页 x 版) x +

访问最多 新手上路

学报

Journal of Shaanxi University of Science and Technology (Natural Science)

自然科学版

本刊荣获：
1996年国家科委、中宣部、新闻出版署颁发的全国优秀科技期刊奖
1992年、1996年、1999年、2006年国家教育部系统优秀科技期刊奖

2015-10-18 星期天 首页 学报简介 文章查询 期刊动态 作者园地 投稿须知 网上订阅 在线留言 联系我们

用户中心

在线投稿查询

专家在线审稿

编辑在线办公

在线注册

文章检索

上期目录 下期目录 刊期索引

文章检索 下载排名 浏览排名

作者园地

作者园地测试

期刊简介

本学报是自然科学综合性学术刊物，主要刊登数学、化学、生命科学、技术科学、信息科学、管理科学、医学科学等基础研究和应用研究方面的学术论文、研究快报、研究简报等。它的任务是：为各理工科院校（系）、所的最新科研和教学成果，促进国内外学术交流，为繁荣和发展我国科技事业服务，为我国社会主义现代化建设服务。读者对象是国内外科技工作者、高等院校理工、医科教师和研究生。

中国期刊方阵，百种重点科技期刊
中国科技论文统计源核心期刊
中国科学引文数据库来源期刊
中国学术期刊综合评价数据库来源期刊

期刊动态

2013海峡两岸(上海)电子电镀...

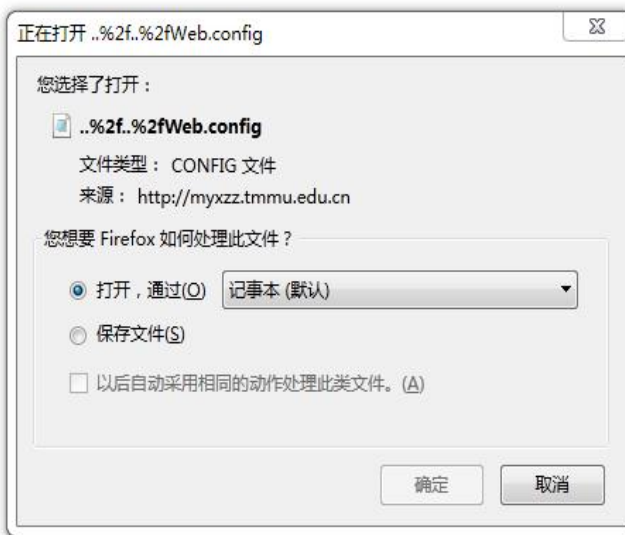
中国环境规划40年发展学术研...

我刊3编委当选院士

(自然科学版) 2015年05



西安知先三才期刊采编系统文件包含漏洞



黑客利用可直接获取网站的配置文件





西安知先三才期刊采编系统文件包含漏洞

```
..%2f..%2fWeb.config - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?xml version="1.0"?>
<!--
Note: As an alternative to hand editing this file you can use the
web admin tool to configure settings for your application. Use
the Website->Asp.Net Configuration option in Visual Studio.
A full list of settings and comments can be found in
machine.config.comments usually located in
\Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration>
  <configSections>
    <!--
The <configSections> element must contain a <section> tag for the <RewriterConfig> section element.
The type of the section handler is RewriterConfigSerializerSectionHandler, which is responsible for
deserializing the <RewriterConfig> section element into a RewriterConfig instance...
-->
    <section name="RewriterConfig" type="Samson.UrlRewriter.Config.RewriterConfigSerializerSectionHandler, Samson.UrlRewriter"/>
    <sectionGroup name="QQSectionGroup">
      <section name="QzoneSection" type="System.Configuration.NameValueSectionHandler, System, Version=4.0.0.0, Culture=neutral, PublicKeyTok
    </sectionGroup>
  </configSections>
  <QQSectionGroup>
    <QzoneSection>
      <add key="AppKey" value="100333814"
      <add key="AppSecret" value="c6def3c11e3a81c022" />
      <add key="CallBackURL" value="http://myxxx.tmmu.edu.cn/login.aspx" />
      <add key="AuthorizeURL" value="https://graph.qq.com/oauth2.0/authorize" />
    </QzoneSection>
  </QQSectionGroup>
  <RewriterConfig>
    <Rules>
      <RewriterRule>
        <LookFor>~/news/([\w]+)/([\d+)\.aspx</LookFor>
        <SendTo>~/News/Details.aspx?ShortName=$1&NewsId=$2</SendTo>
      </RewriterRule>
      <RewriterRule>
        <LookFor>~/news/([\w]+)/default\.aspx</LookFor>
        <SendTo>~/News/Column.aspx?ShortName=$1</SendTo>
      </RewriterRule>
    </Rules>
  </RewriterConfig>
</configuration>
```

网站配置文件中包含许多敏感信息



上海
SHANGHAI JIAO TONG UNIVERSITY

期刊稿件远程处理系统认证绕过漏洞

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

明观网络威胁检测系统 x 明观网络威胁检测系统 x http://202....01&magId=1 x 北京玛格泰克公司稿件远... x +

journalx_jkb/Login.action 搜索

访问最多 新手上路

Journ@lx® 2015-10-9- 星期五

 **大学学报(教育科学版)**
Journal of East China Normal
University(Educational Sciences)
1000-5560
31-1007/G4
-62232305
journalx@ecnu.edu.cn

杂志主页

北京玛格泰克公司稿件远程处理系统

-  作者中心
-  专家中心
-  编委中心
-  主编中心
-  编辑中心



期刊稿件远程处理系统认证绕过漏洞

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

明观网络威胁检测系统 x 明观网络威胁检测系统 x http://202.10...ledit.action x 北京玛格泰克公司稿件远... x +

journal_xjkb/author/Authorledit.action

访问最多 新手上路

作者 修改个人信息 安全退出

大学学报
(教育科学版)

- 修改个人信息
- 修改登录信息
- 人员身份信息

返回作者主界面

尊敬的 zhangjian 作者,非常感谢您登录我们的作者中心!

基本信息

称呼: 教授 副教授 先生 女士

姓名: (必须)

英文姓名: First Name
(名, 例如晓明 对应的英式姓名为Xiao-Ming)

Middle Name

Last Name
(姓, 全大写, 例如张, 对应ZHANG)

首选E-mail: @126.com (必须)
(在此输入您最常用的E-mail地址. 注意不要输入多个. 如果有多个E-mail, 请在抄送框中输入)

抄送E-mail: 启用 不启用

研究领域

学科和专业:

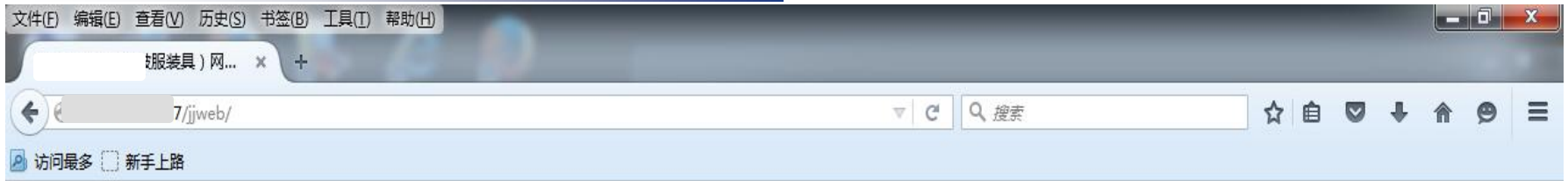
添加或修改 (必须)

绕过身份认证, 可以修改或获取所有作者的个人信息



上海普诺迪
SHANGHAI PNUODI INFORMATION SYSTEM TECHNOLOGY RESEARCH CO., LTD.

普诺迪管理系统后台万能密码登录漏洞



用户名称：**管理员**
万能密码：**' or 1=1 or '='**



北京普诺迪信息系统技术研发有限责任公司

北京普诺迪信息系统技术研发有限责任公司同类产品：**家具管理系统**、**被服装具管理系统**、**低值耐用品管理系统**、**图书馆管理系统**等都有相同问题。



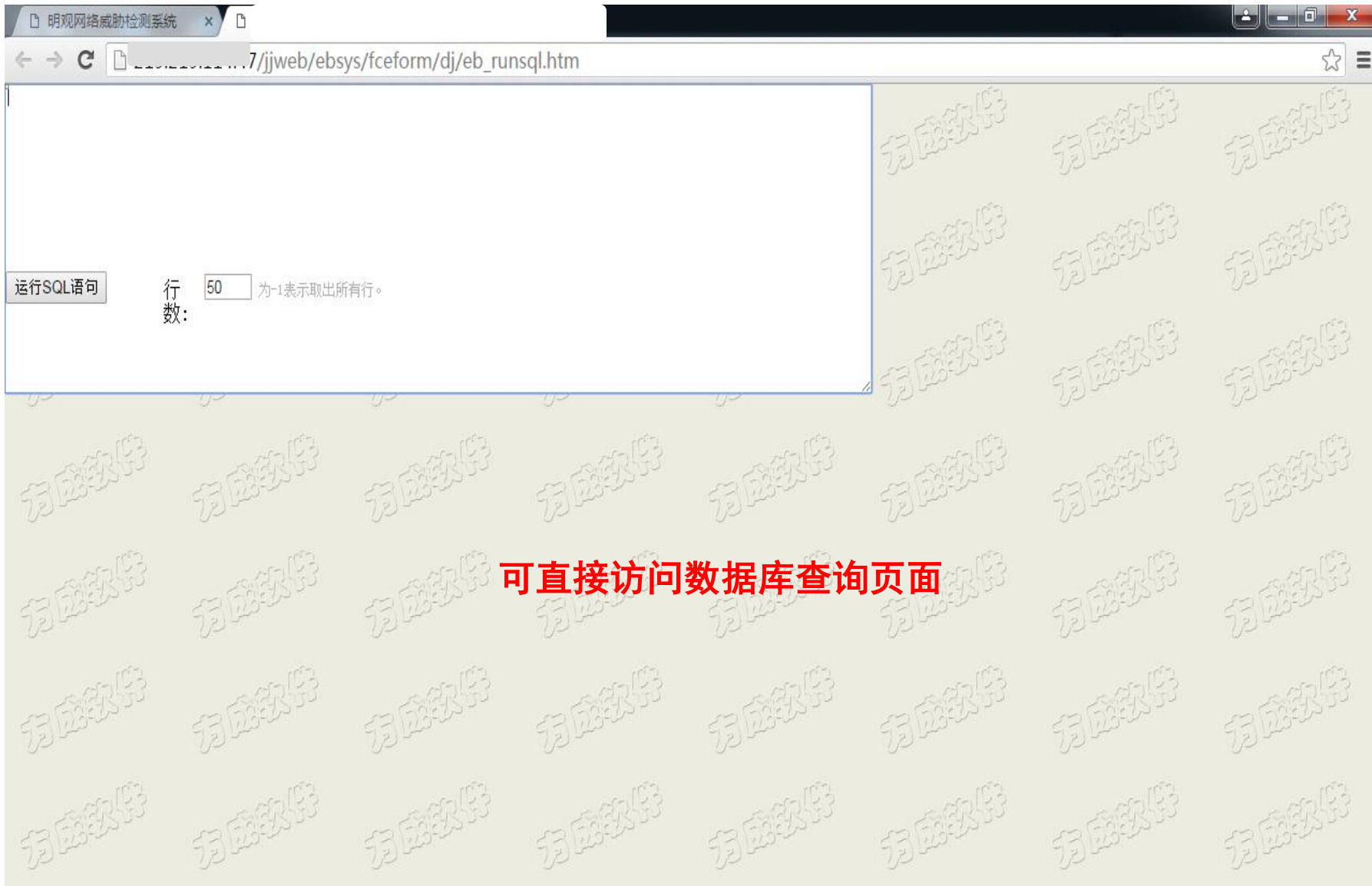
普诺迪管理系统后台万能密码登录漏洞

The screenshot shows a web browser window with the address bar displaying `219.219.114.47/jjweb/default.asp`. The page title is "家具（被服装具）网络管理系统" (Furniture (Clothing) Network Management System). The navigation menu includes: 家具登记, 家具审核, 财务审核, 账目修改, 变动申请, 变动审核, 家具查询, 报表打印, 系统维护, 附属功能, 退出系统. The "附属功能" (Auxiliary Functions) menu is expanded, showing options like 密码修改 (Password Change), 信息管理 (Information Management), 联系我们 (Contact Us), and 系统帮助 (System Help). The main content area is titled "修改密码" (Change Password) and contains a form with the following fields: 用户名 (Username) with the value "管理员" (Administrator), 原密码 (Original Password), 新密码 (New Password), and 确认密码 (Confirm Password). At the bottom of the form are buttons for "确认" (Confirm) and "返回" (Return).

登录后可以修改密码、查看和修改账目、发布消息等



普诺迪管理系统数据库任意查询漏洞



可直接访问数据库查询页面



- 1、乾豪综合教务管理系统DB配置文件泄露漏洞
- 2、南京先极科技教育类CMS文件包含漏洞
- 3、天翼财务系统远程代码执行漏洞
- 4、北京希尔OA系统文件包含漏洞
- 5、上海万欣高校教学管理系统文件上传漏洞
- 6、西安知先三才期刊采编系统文件包含漏洞
- 7、北京清元优软URP综合教务系统文件包含漏洞
- 8、新中新一卡通系统管理员密码重置漏洞
- 9、神州浩天网上银行缴费系统文件包含漏洞
- 10、期刊稿件远程处理系统认证绕过漏洞
- 11、THEOL网络教学综合平台测试账号漏洞
- 12、正方招生管理系统后台缺省口令漏洞
- 13、卓越课程中心缺省口令漏洞
- 14、普诺迪管理系统后台万能密码登录漏洞
- 15、科发高校财务管理系统权限绕过漏洞
- 16、浙大万朋ZDSOFT.NET信息发布平台文件包含漏洞



高校网络安全问题

- 以上是从网上看到的高校网络安全问题的一小部分，每个案例都不是个案，相当一部分学校都有类似的问题；
- 在网上监测到的高校网络安全问题都不是新出现的安全问题，而是几年前在乌云和国家互联网应急中心都曾通报过的老问题，只是一些高校有关部门没有关心和没有引起足够重视；
- 各高校在校园信息化建设中采购了各种成熟的信息管理应用系统，这些应用系统一旦出现安全问题将影响一大批学校，且不少开发商不会主动、及时地帮助各高校升级更新系统，致使安全威胁长期存在或一再被黑客利用，各校应有清醒认识。



上海交通大學
SHANGHAI JIAO TONG UNIVERSITY



谢谢!

