上海交通大學
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

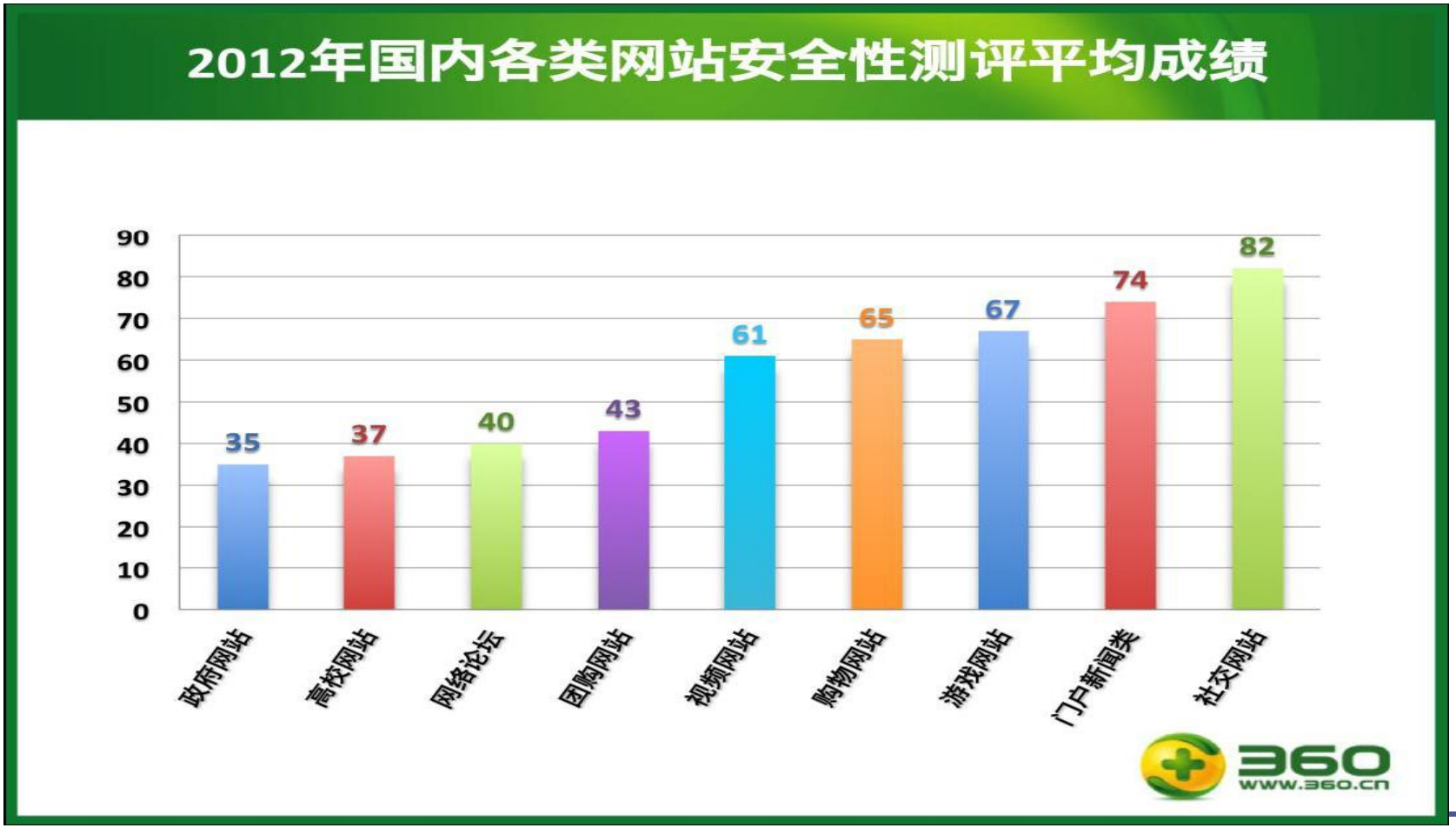
1、CERNET网络安全威胁监测

2、教育网当前主要安全威胁

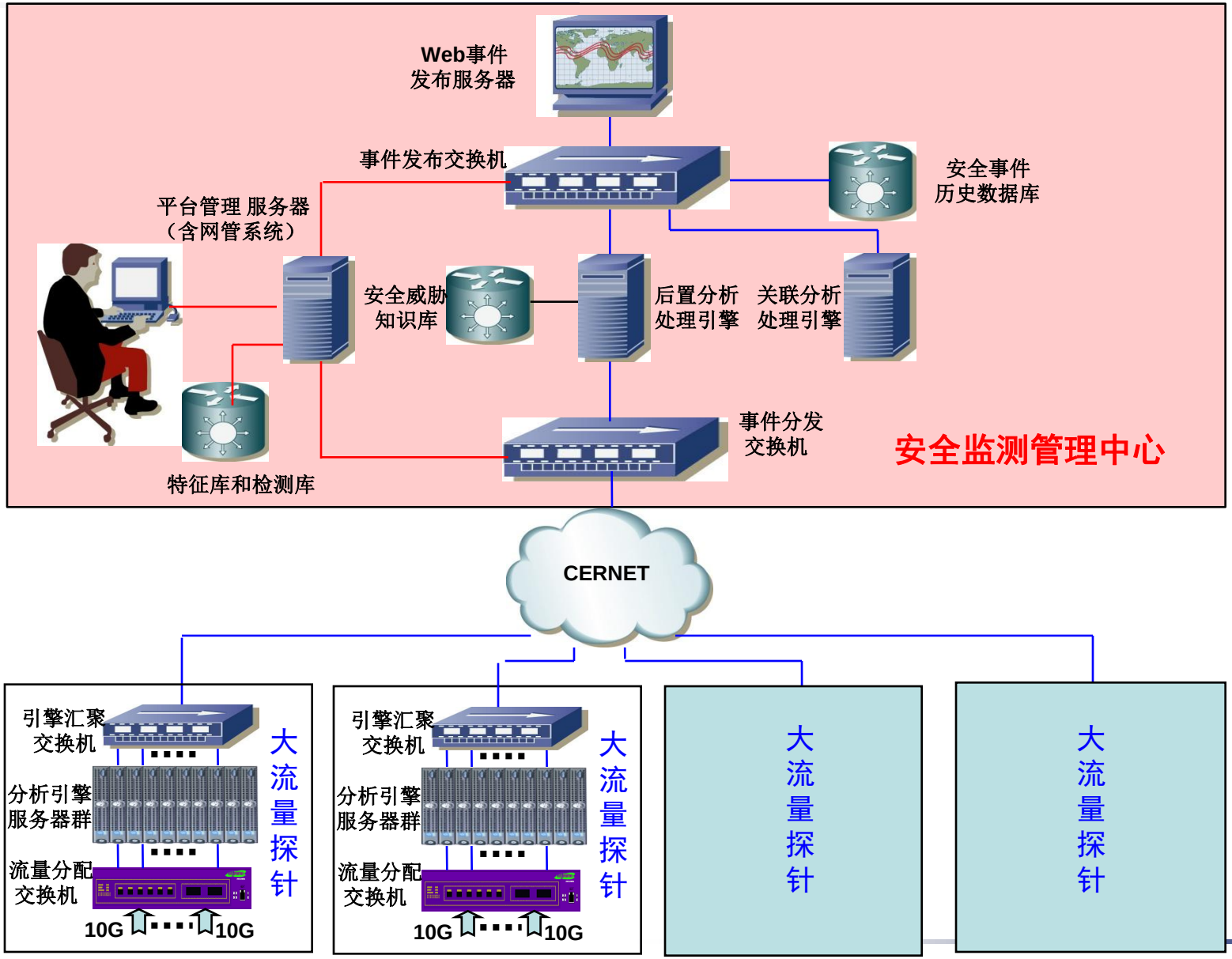
3、高校应用系统安全问题举例

中国高校网站安全性排名全国倒数第二

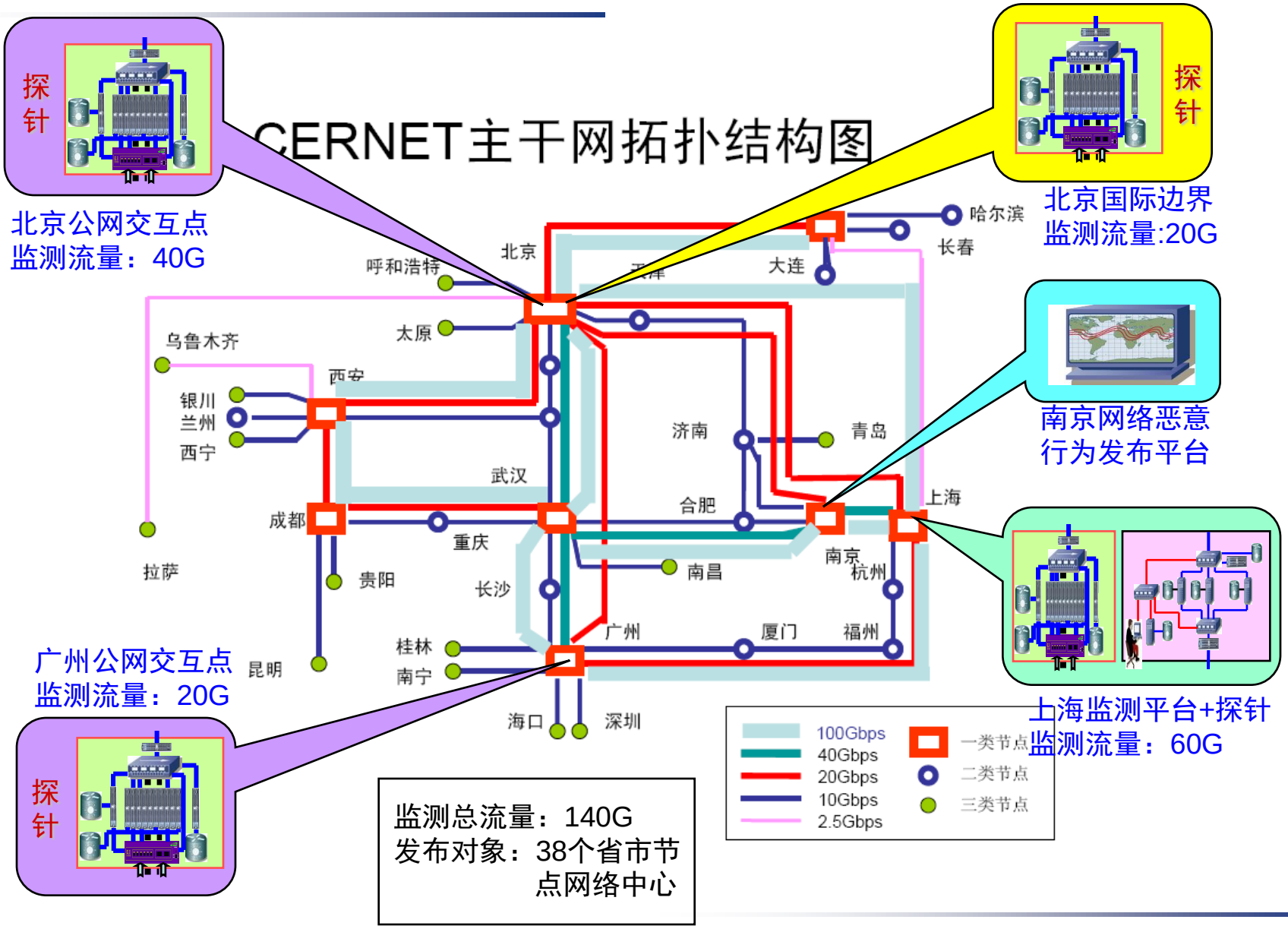
“中国高校网站安全情况极差，在全国各类网站安全情况排名中，高校网站安全性排名倒数第二，意味着高校网站非常容易被黑客入侵、篡改和窃取资料。”



CERNET网络安全实时监测平台架构（2013）



在CERNET上部署的系统（2013）



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；

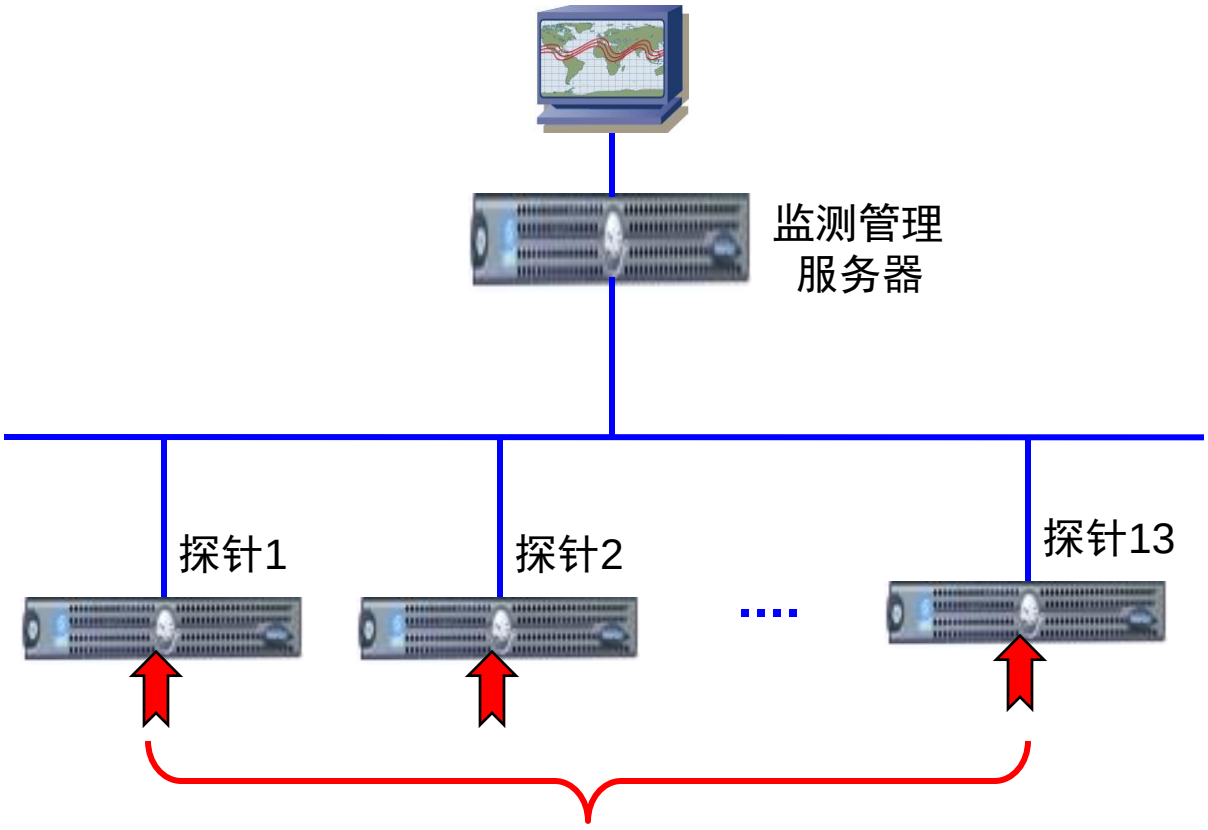
3、安全监测平台核心价值在于具有能够及时和不断发现最新安全威胁的能力，这就需要一支很强的网络安全研究团队，对监测平台进行及时、有效维护，目前CERNET尚未组建这样一支团队。

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。

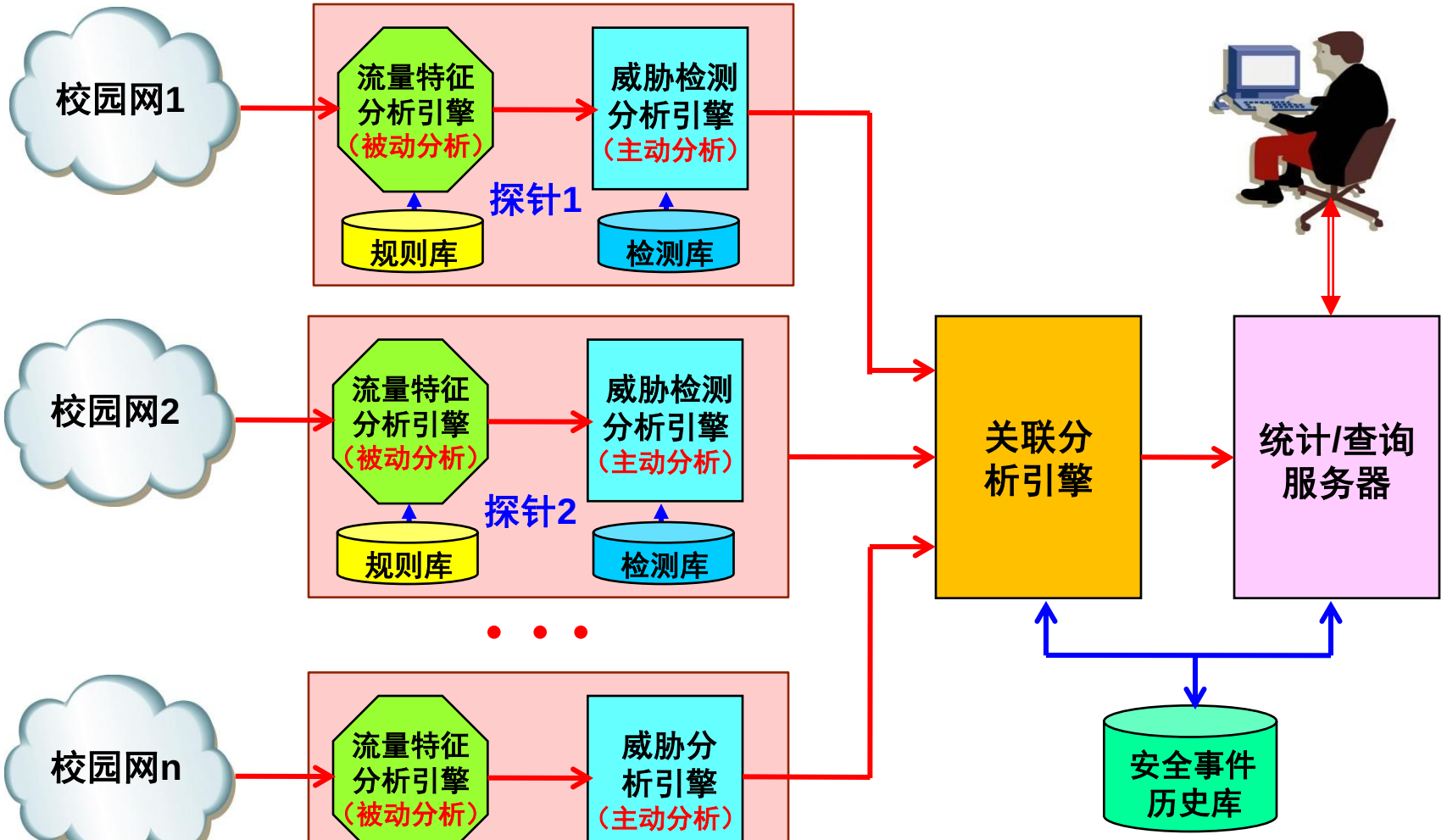
个新建安全监测试验系统(2015.9)

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

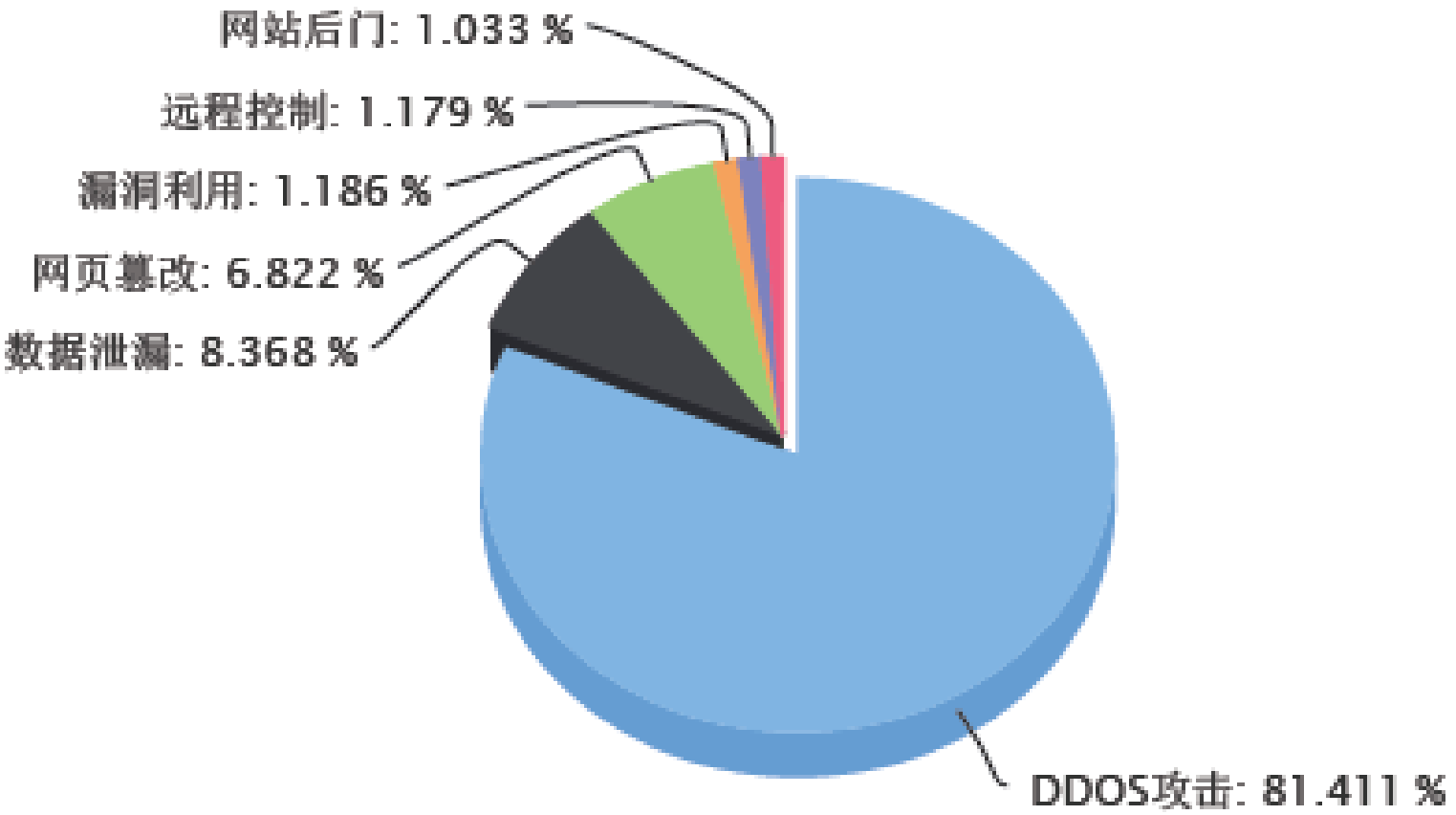


安全威胁分布监测系统三级引擎架构



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。

主要的DDoS攻击技术

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（spamhous）。

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

面对DDOS攻击我们能做什么

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

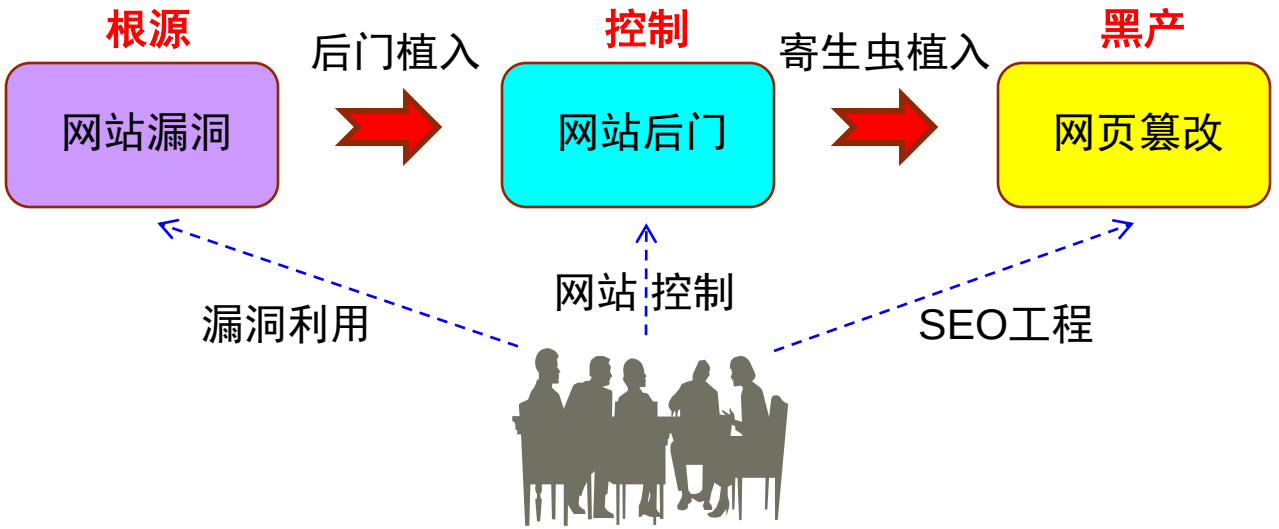
— **清理园区网中僵尸主机和肉鸡，以免被黑客利用去攻击他人**；

— **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

网站安全

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

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

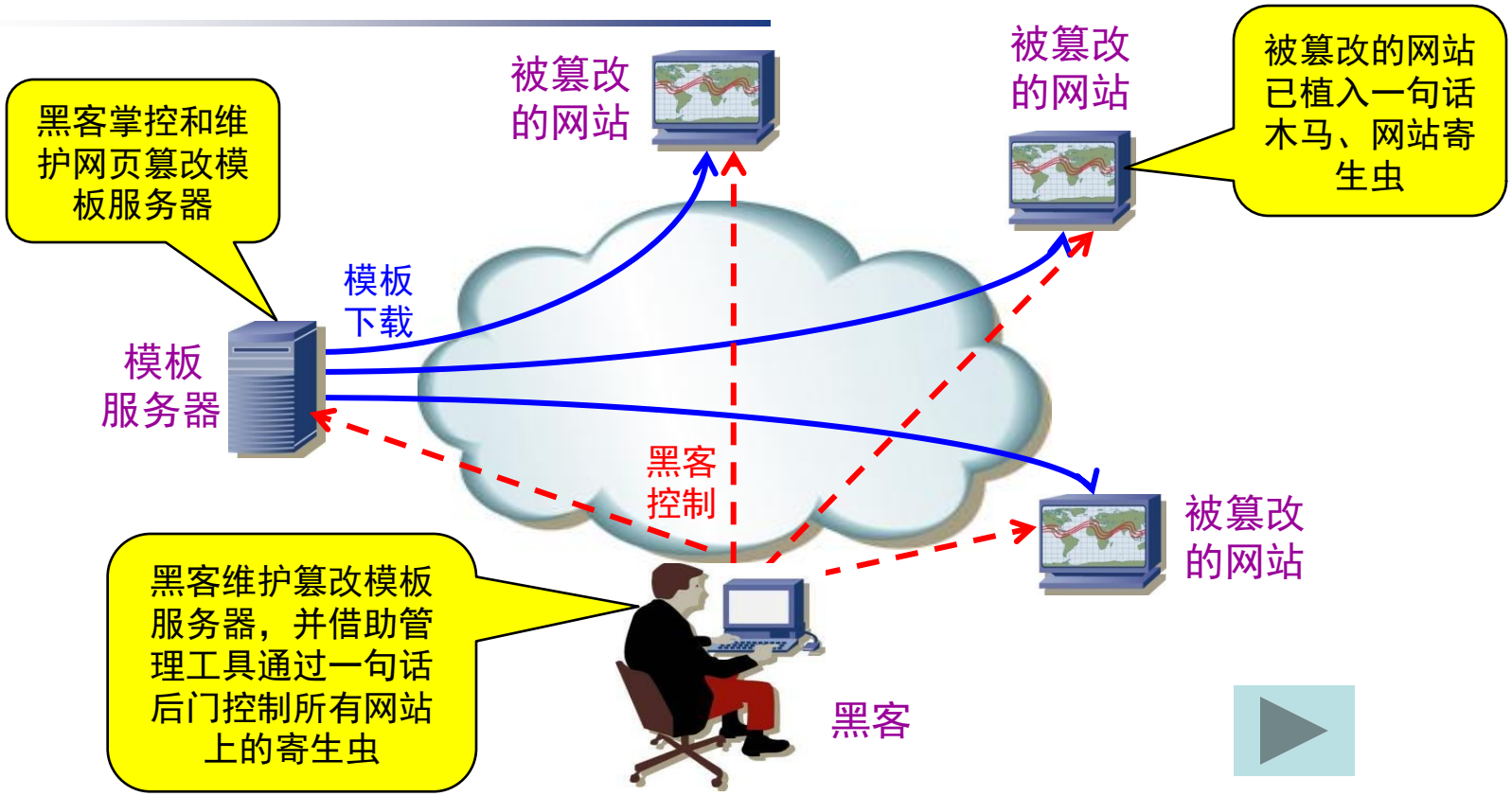
网页篡改(暗链)

http://210. 217/

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

网页篡改(暗链)

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

被黑客篡改为钓鱼网站

http://z.jx.cn/

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

骗取银行账号等信息

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

骗交保险抵押金

诱骗银行支付


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!
明观网络威胁检测系统
活动正在进行中!
mplate/default/label_tpl/article/caches/%40%23%24%25%23%24%25%23%40!%23%24%25%
搜索
银联 活动指定银行账户
开户银行
账 户
收款人
缴纳费用
中国工商银行
联系客服索取
王玲
¥5000
中国农业银行
联系客服索取
王玲
¥5000
中国建设银行
China Construction Bank
联系客服索取
王玲
¥5000
中国邮政
CHINA POST
联系客服索取
王玲
¥5000
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

mo
bile=12435623&re
al_name=%CA%C7%C
4%E3%C2%F0&sex=%
C5%AE&card_type=
%BE%FC%C8%CB%D6%
A4&card=42353614
3&post_tel=15157
632568&addr=shan
ghai&post_code=1
23112&bank=%D6%D
0%B9%FA%C3%F1%C9
%FA%D2%F8%D0%D0&
bank_card=451235
43634123423 14&ba
nk_username=%CA%
C7%C4%E3%C2%F0&z
hiye=%BC%C6%CB%E
3%BB%FA%2FIT%D2%
B5&cip=111.198.2
9.250&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

传至第三方服务器的用户信息

real_name=劳
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=劳
zhiye=教师

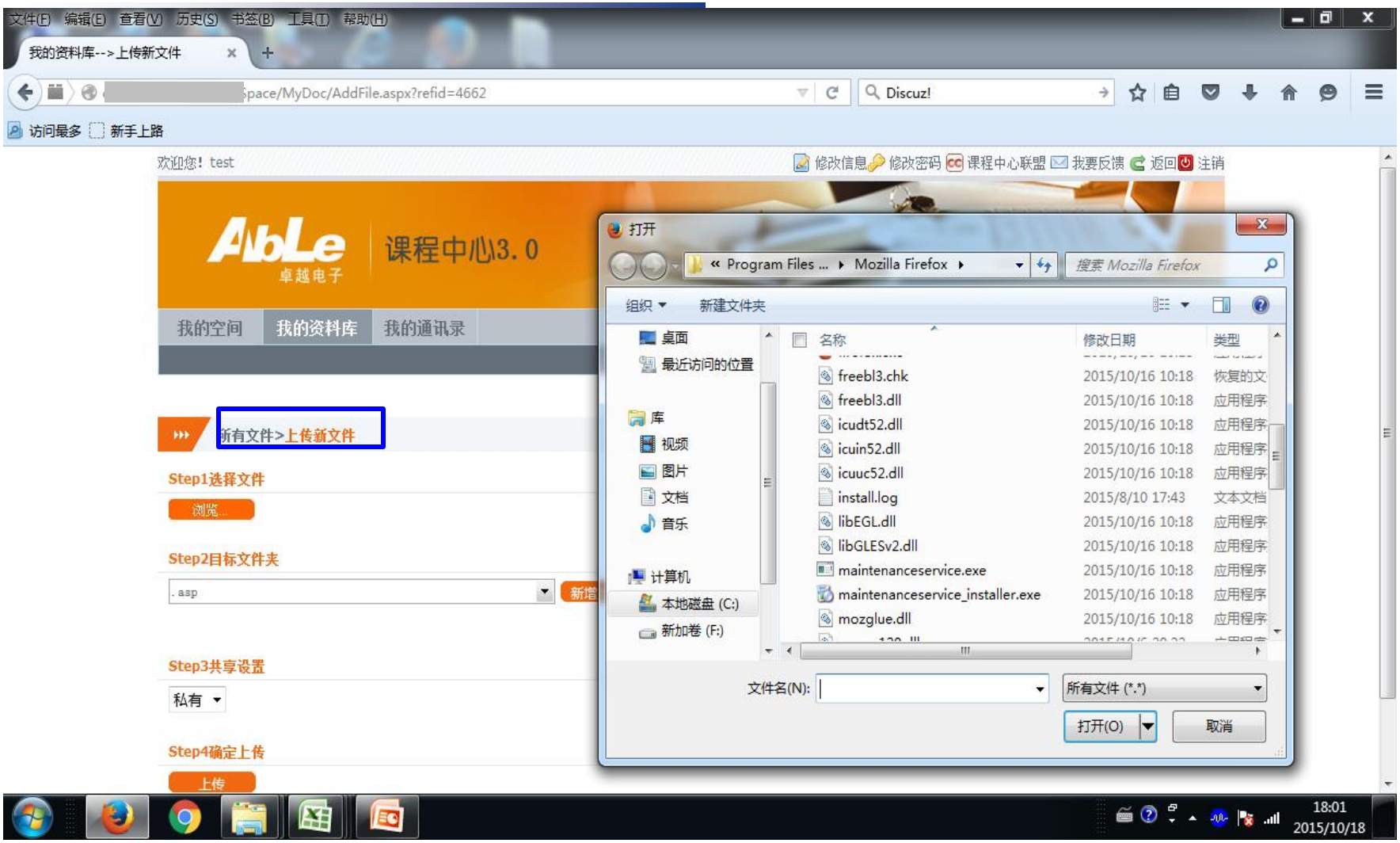
qq=1779034
type=邮寄领取
real_name=周
sex=女
card_type=身份证
card=6104031965
&addr=天津市津南区
育园区内雅观路1
post_tel=1337037
bank=中国建设银行
bank_card=4367+420
4+110 4
bank_username=周

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

。 。 。

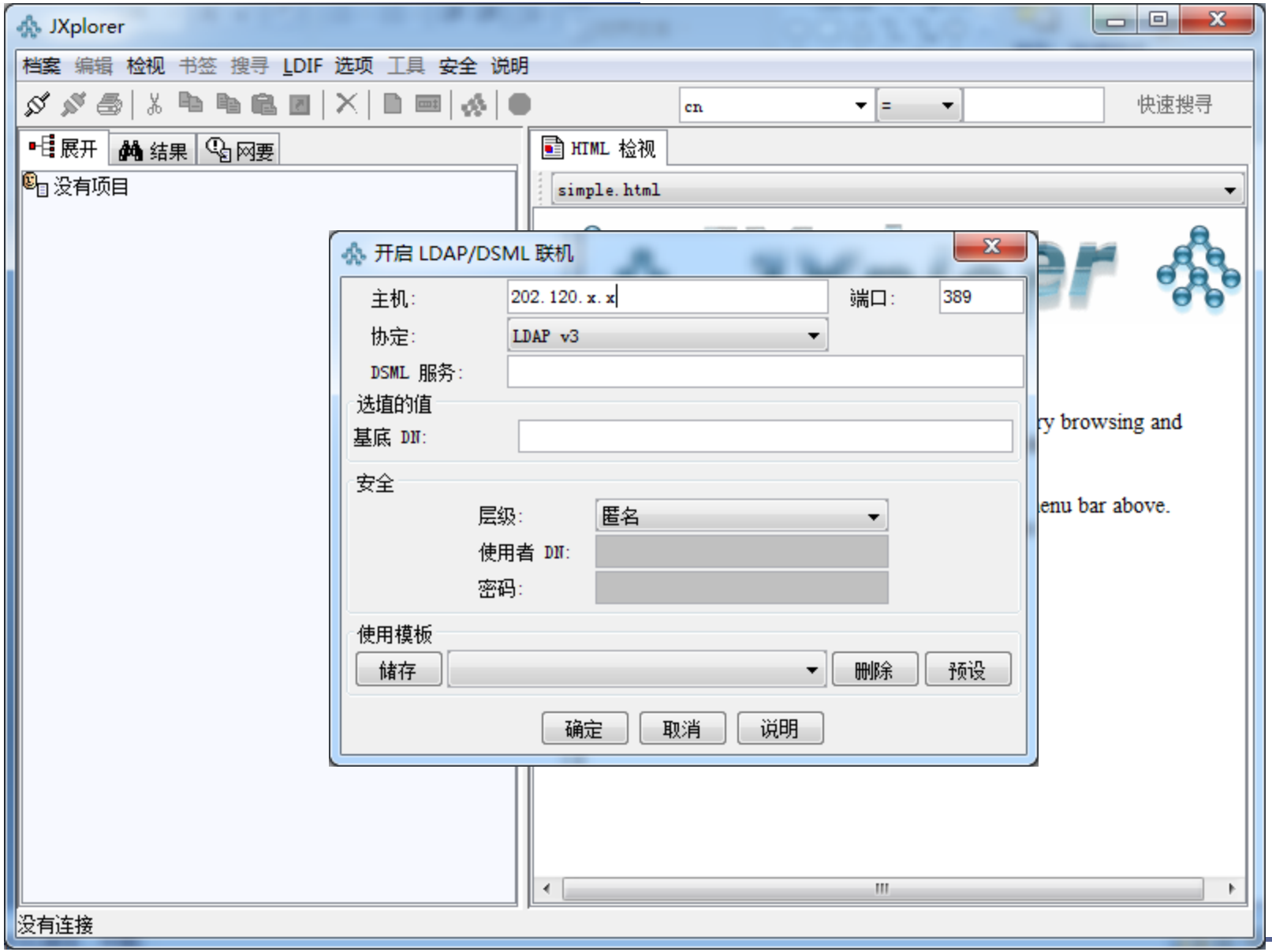
卓越课程中心缺省口令漏洞(管理漏洞)

卓越课程中心缺省口令漏洞(管理漏洞)

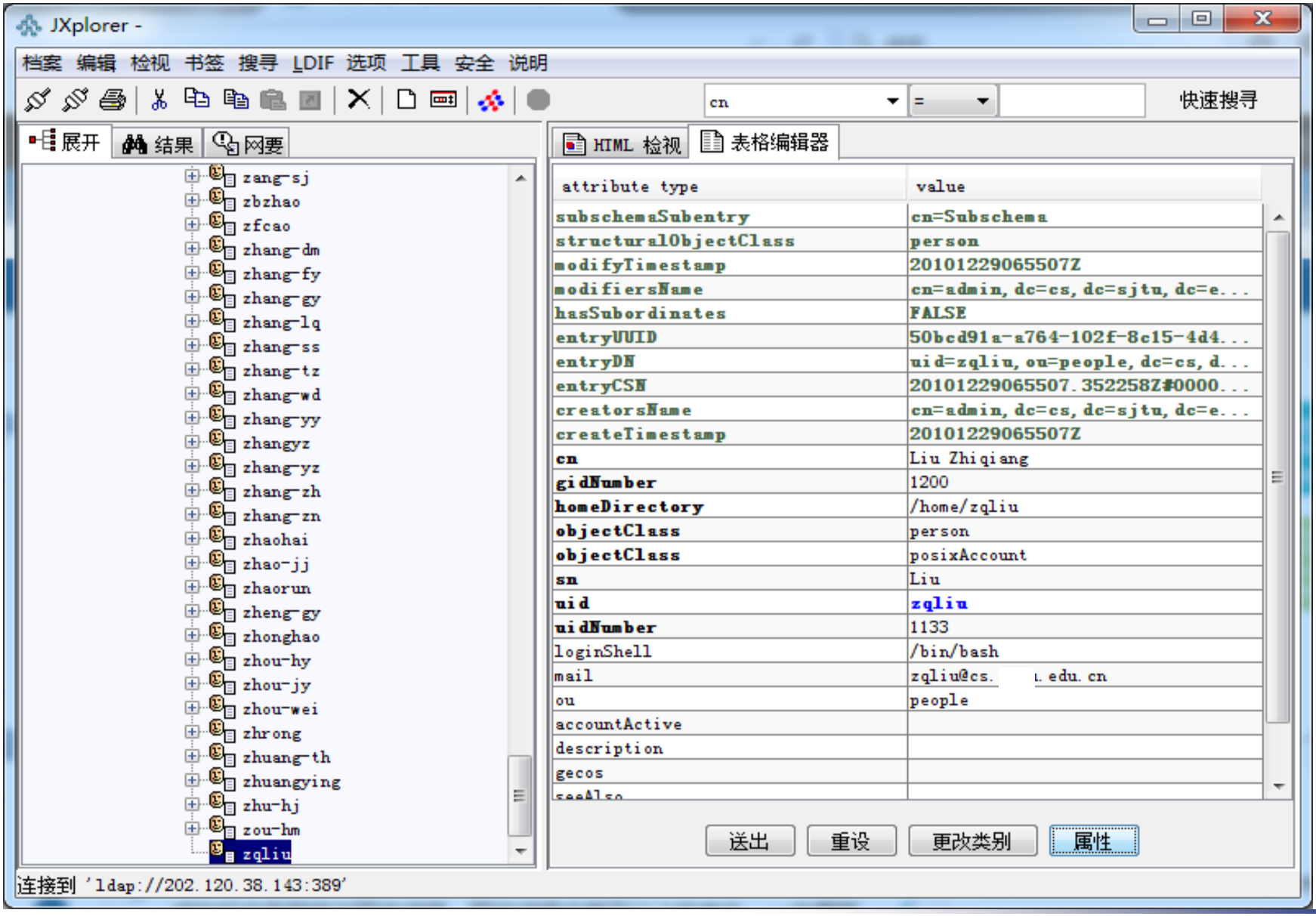


除了可以修改账号外，在“我的空间”—>”我的资料库”可以上传任意文件

LDAP服务器匿名访问(管理漏洞)



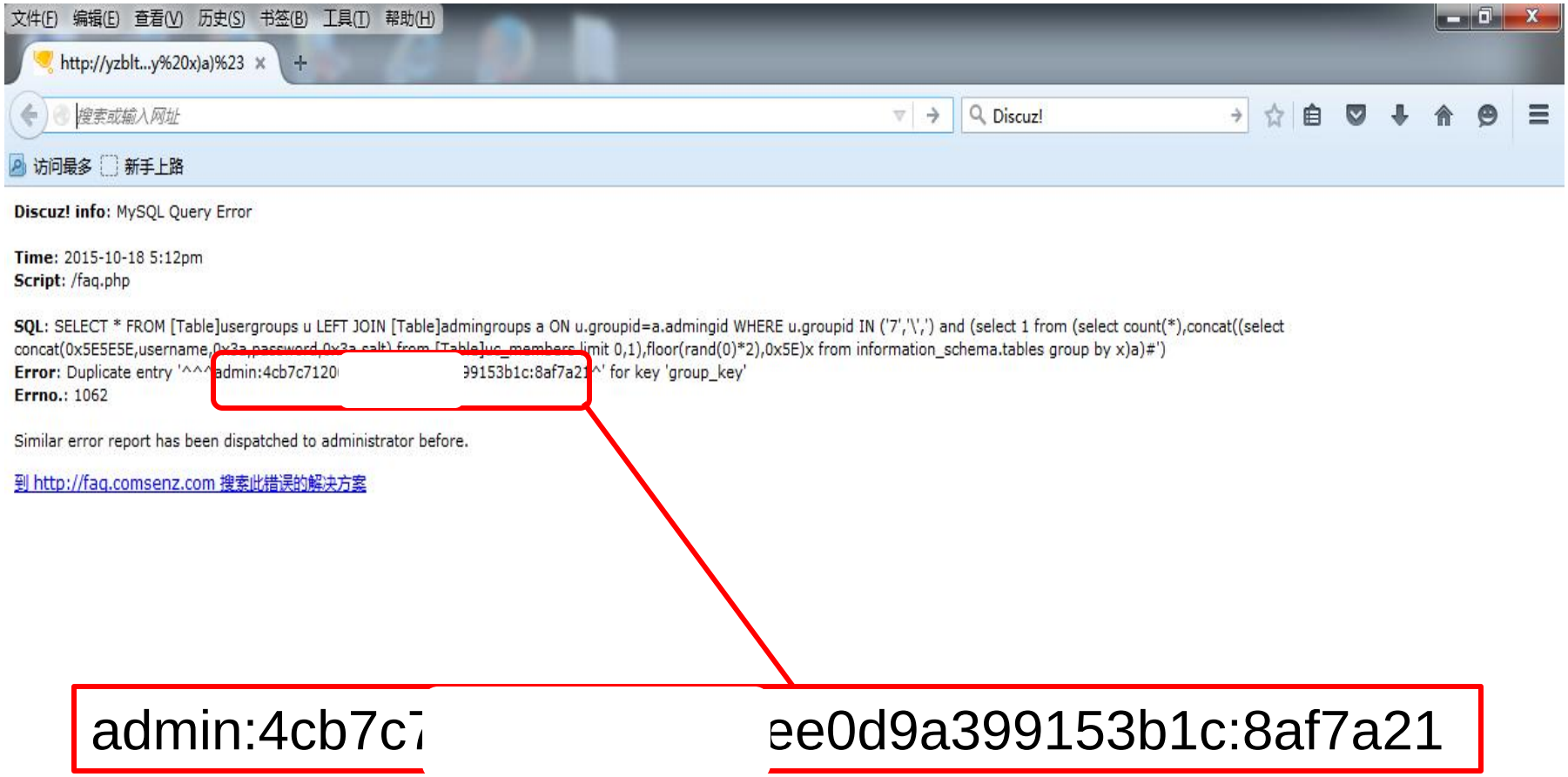
LDAP服务器匿名访问(管理漏洞)



Discuz!后台注入漏洞(中间件漏洞)

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)



admin:4cb7c7 ee0d9a399153b1c:8af7a21

天翼财务系统远程代码执行漏洞(中间件漏洞)

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Strus2，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。

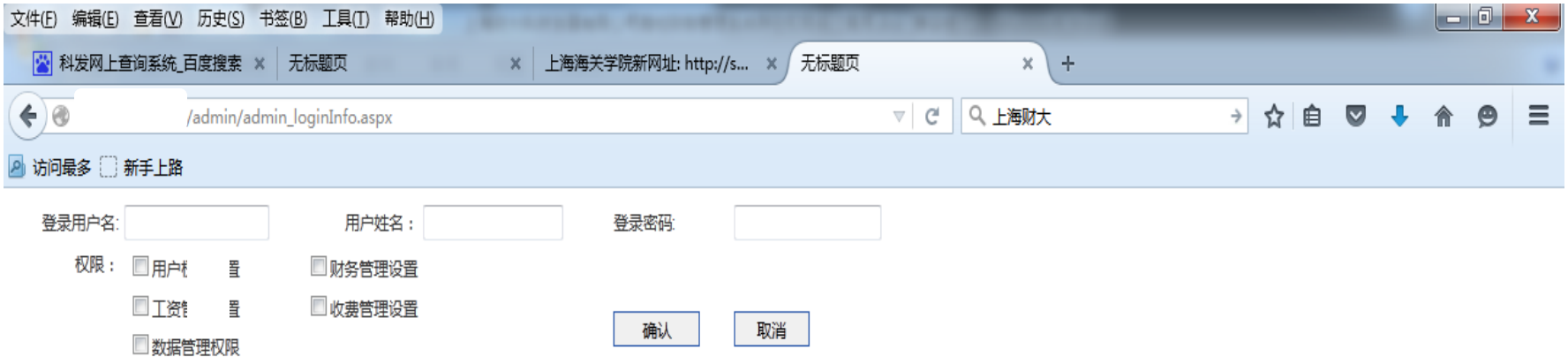
科发高校财务管理系统权限绕过漏洞(应用漏洞)

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)

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)

	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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	[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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[illegible]	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

新中新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

新中新一卡通系统管理员密码重置漏洞(应用漏洞)

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

新中新一卡通系统管理员密码重置漏洞(应用漏洞)

源：http:/ nanagerEditNManager.action?id=1 - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 帮助(H)

```
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='78D000I        3B2' >
96 <input type="hidden"  name="name"  size="20"   value='WEBMANAGER' >
97     <table width="100%" border="0" cellpadding="0" cellspacing="0" >
98       <tr>
99         <td width="23%" height="33" align="center" background="/images/style1/biaotou1.jpg" class="baizi">用户信息 </td>
100        <td width="77%" align="left" background="/images/style1/biaotou2.jpg" class="baizi"> </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 户 名</th>
109              <td width="87%">
110              <input  type="hidden"  name="id"  value='1'>
111                <input class="and" type="text"  name="username"  size="19" value='WEBMANAGER' >
112              </td>
113            </tr>
114             <tr class="listbg">
115              <th width="238" height="21" class="neiwen" scope="col"  align="right">密    码 </th>
116              <td width="87%"><input class="and" type="password"  name="passwd" size="20" value='78D0(        3F8B2' ></td>
```

size="20" value='78D0(B8F8B2' >
value='WEBMANAGER' >

新中新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

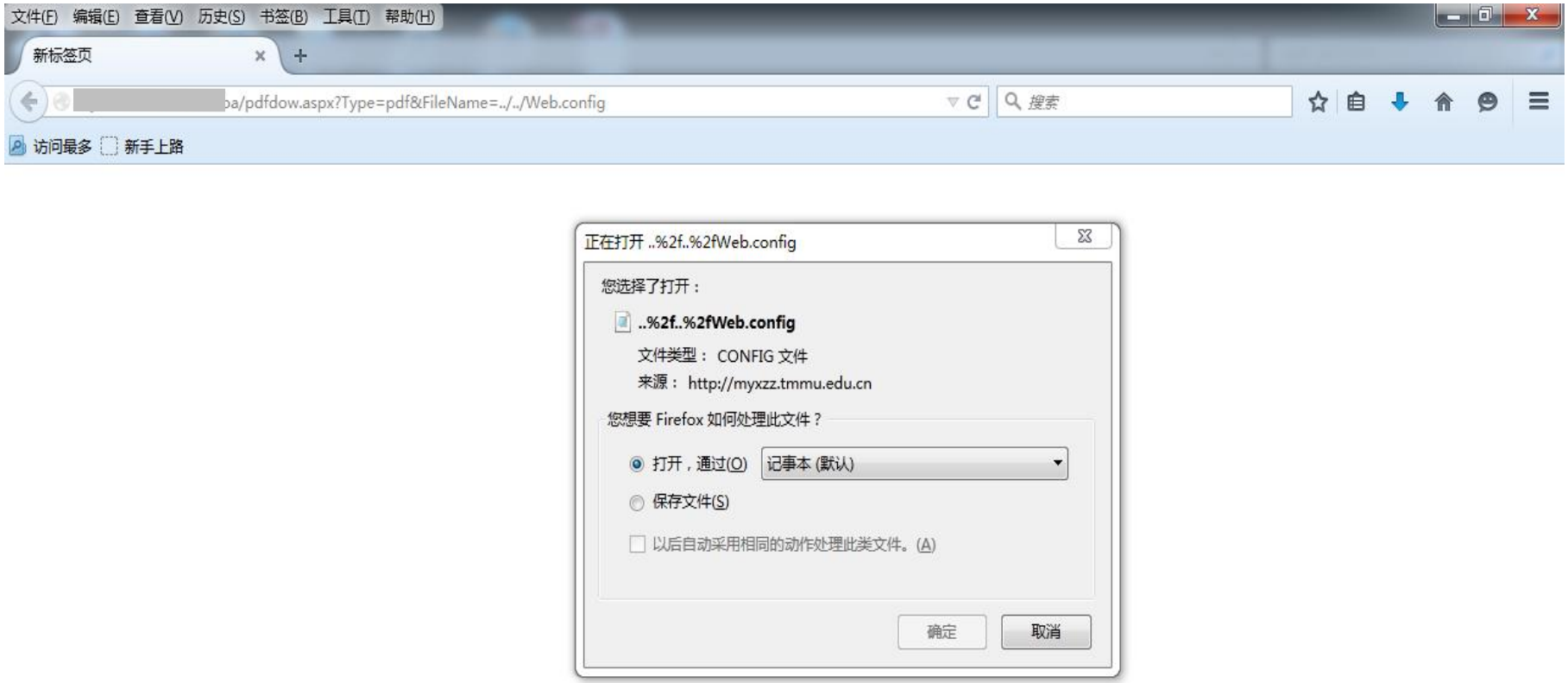
文件(F) 编辑(E) 查看(V) 帮助(H)

```
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/biaotou1.jpg" class="baizi">用户信息 </td>
100        <td width="77%" align="left" background="/images/style1/biaotou2.jpg" class="baizi"> </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 户 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='26BF60_ .. .. .40925' >
size="20" value='YKT' >

西安知先三才期刊采编系统文件包含漏洞

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="c6def3c8                    1e3a81c022" />
                        <add key="CallBackURI" value="http://myxzz.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&amp;NewsId=$2</SendTo>
      </RewriterRule>
      <RewriterRule>
        <LookFor>~/news/([\w]+)/default\.aspx</LookFor>
        <SendTo>~/News/Column.aspx?ShortName=$1</SendTo>
      </RewriterRule>
```

网站配置文件中包含许多敏感信息

20:42
2015/10/5

期刊稿件远程处理系统认证绕过漏洞

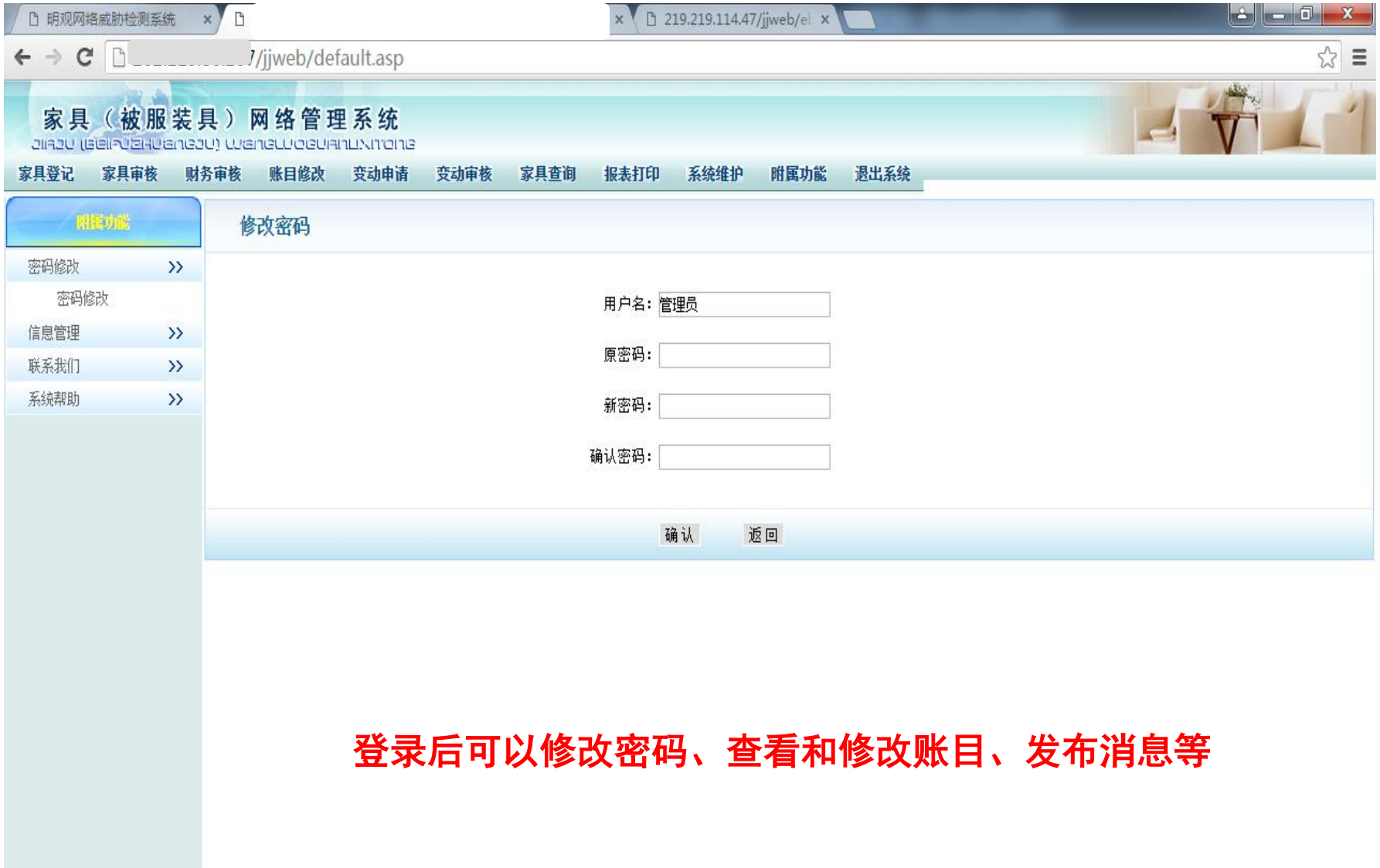
期刊稿件远程处理系统认证绕过漏洞

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 ''='

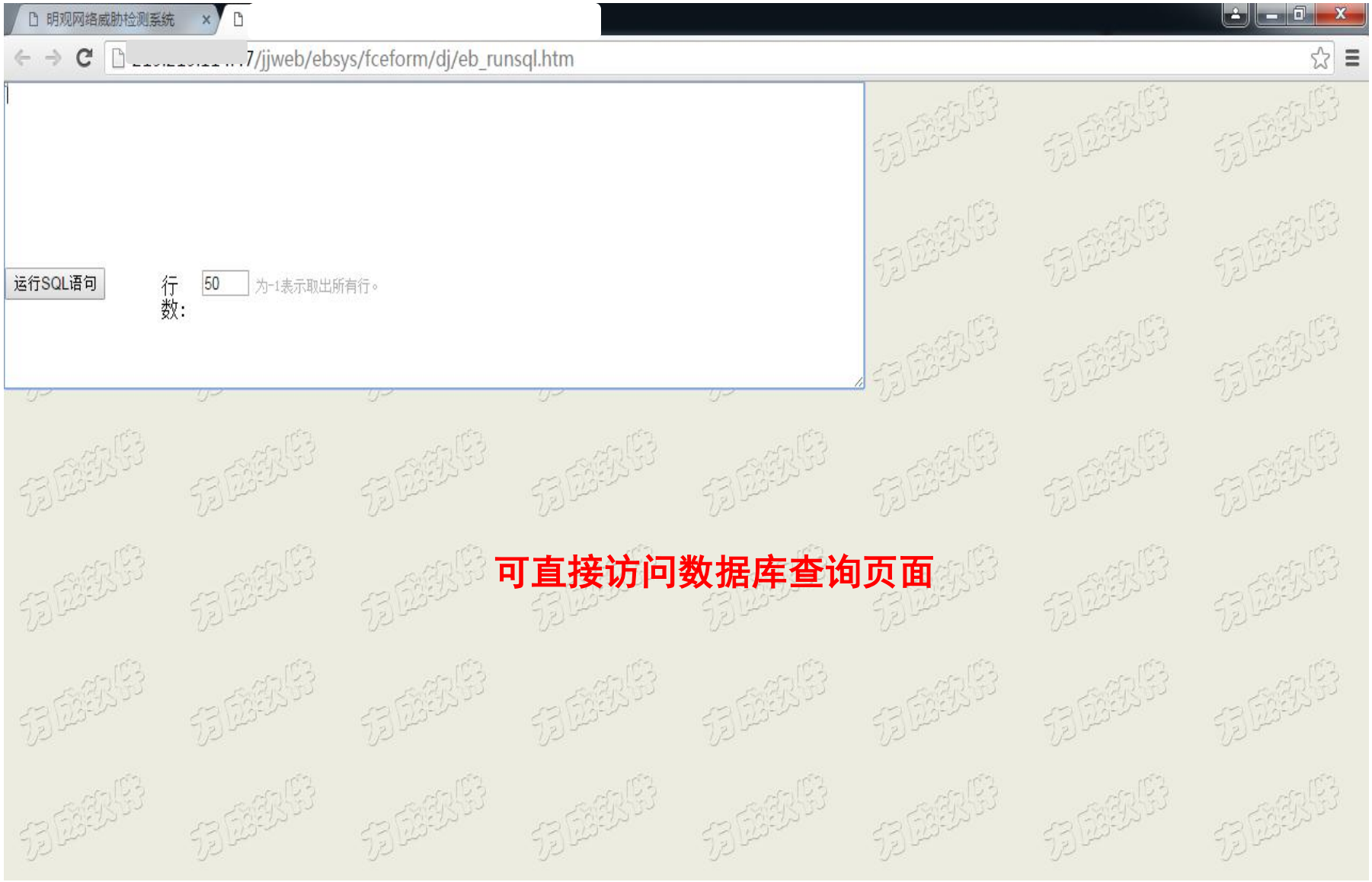
北京普诺迪信息系统技术研发有限责任公司同类产品：家具管理系统、被服装具管理系统
低值耐用品管理系统、图书馆管理系统等都有相同问题。

普诺迪管理系统后台万能密码登录漏洞



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

部分存在安全问题的高校应用系统

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!