



爱开发 重创新 更智慧

# Innovate2011

IBM Rational 软件创新论坛

 Software. Everywhere.



# Rational 应用安全和合规测试 解决方案

庄俊乾

IBM 软件部客户技术专家



# 议程

- 应用安全面临的挑战
- Rational应用安全和合规测试
  - 2010年的新发展：黑白集成
- 实施案例分享
  - 在国内某开发中心实施规划



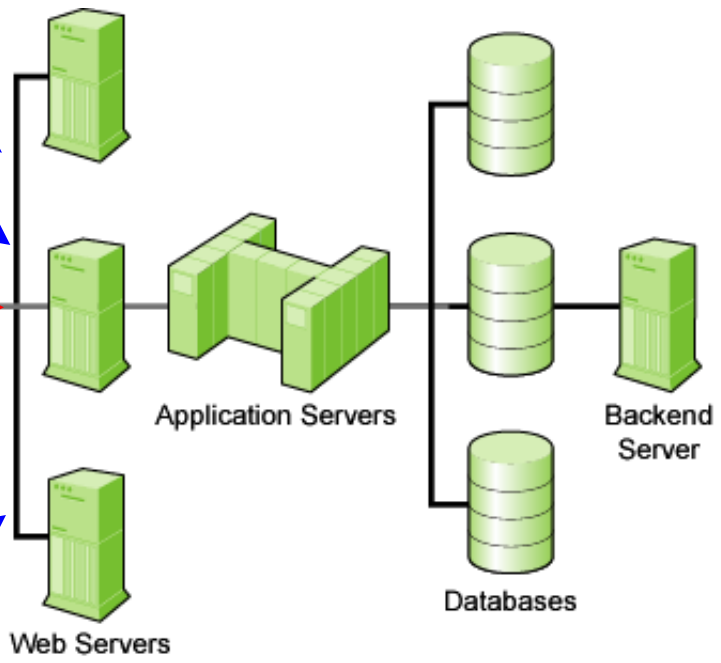
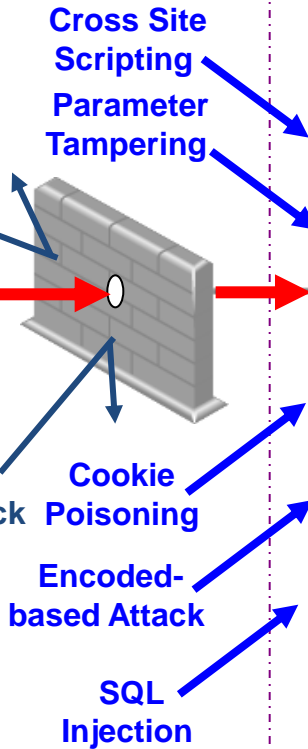
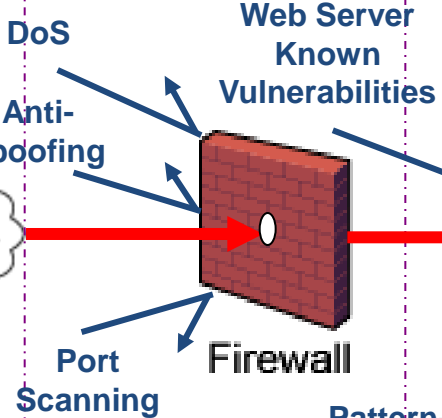
# WEB应用面临着严峻的安全挑战...

桌面

防火墙

IDS/IPS

Web 应用



Antivirus Protection



# 我国政府网站... 10%存在恶意链接

## 统计称我国百万政府网站遭色情等恶意网页暗链

<http://www.sina.com.cn> 2010年09月24日14:56 四川在线-华西都市报

“最好香港马会资料”、“怎样才能买六合彩特码”……前日，在武汉大学信息管理学院博士生导师沈阳的办公室里，在他演示下，记者看到，一些网络“牛皮癣”居然“傍”上了政府某网站，其域名显示为“gov.cn”。

“这就是‘暗链攻击’。”沈阳说，“这些直接浏览时看不见的文本，实际上链接的是一些色情、赌博、欺诈类非法商品、政治性内容的网页。”某市的政府网站页面共计3350张，被植入欺诈类信息“暗链”的网页多达1240张。一些教育类网站也成为攻击对象，“香港赛马会一推算六合彩”“傍”上的是我国公认最好的一所大学。“手机窃听器”粘上了成都某高校通信信息工程学院网站。

沈阳对我国的一些政府网站“暗链攻击”状况作了一个统计：我国3000多万个政府网站，被恶意网站“暗链”上的高达10.22%；其中，有诈骗信息、色情信息、赌博信息的网页最多，达308万个，占10.13%。



# 索尼泄密 ...

- 事件开始于美国当地时间2011年4月17日，索尼旗下Playstation网站遭遇黑客入侵，黑客侵入索尼公司位于美国圣迭戈市的数据服务器，窃取了索尼PS3和音乐、动画云服务网络Qriocity用户登录的个人信息，包括姓名、住址、生日、登录名和密码等，受影响用户多达7700万人，涉及57个国家和地区。同时，索尼旗下另一组负责计算机在线游戏服务的索尼网络娱乐 (Sony Online Entertainment) 也传遭到入侵，可能将有高达2460万笔用户数据也遭外泄。
- 4月19日，索尼宣布关闭网站服务。
- 4月26日，索尼对外公布网站遭遇黑客入侵，用户信用卡等个人信息或遭泄漏。





# 移动时代，攻击更方便

## 攻击方式

谢谢 新浪微博所有的插入链接都显示为t.cn的模式,根本看不到具体的地址,那的确很容易被 XSS利用攻击,然后蠕虫...即使不蠕虫你sina,也可能是其他的XSS恶意连接



6月28日 22:26 来自新浪微博

删除 | 转发(1) | 收藏 | 评论

- 利用weibo平台进行应用层面的攻击 (XSS, SQLi, etc.)
- Web services 攻击 (SOAP array overflow, XML parser DoS, etc.)
- 针对应用逻辑攻击 (WSDL, AJAX libraries)
  - RSS 毒药
  - 非安全 Mashups
  - JavaScript 劫持



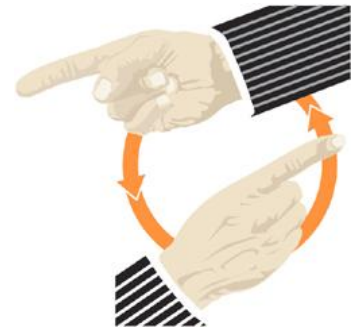
# X-force 2010年安全分析报告

## • WEB应用安全攻击

- 2010年的攻击案例中，WEB应用的漏洞引起的占据49%
- CSRF类型的安全问题日益突出
- ASP.Net应用更容易被攻击(相对于PHP和Java应用)
- 随着WEB2.0技术的广泛应用，客户端的Javascript攻击也日益成为主要威胁

## • 新的安全攻击领域

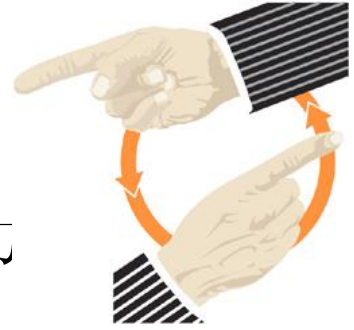
- 移动终端的攻击开始快速增长
- 云计算-人们对云计算的一个重要担心是安全问题





# 同时，其他的研究报告显示

- 开发人员缺乏安全培训和要求
  - 64%的开发人员不具备编写安全代码的能力
  - 开发人员不关心安全
- 缺乏明确的安全策略、流程以及工具
- 安全攻击都基本转向利益驱动



# 议程

- 应用安全面临的挑战
- Rational应用安全和合规测试
  - 2010年的新发展：黑白集成
- 实施案例分享
  - 实施方案的路线图



# 应用安全测试:单一技术向复合技术转变

静态分析 = 白盒

- 扫描源代码发现漏洞

```

184 |
185 | ..... TxnCSSFontStyle .....
186 | }
187 |
188 | constructor TxnCSSFontStyle.Create(aFontStyle: TxnCSSFontStyleEnum):
189 | begin
190 |   inherited Create(aFontStyle);
191 |   FFontStyle := aFontStyle;
192 | end;
193 |
194 | function TxnCSSFontStyle.GetStyleValue: string;
195 | begin
196 |   Result := mxCSSFontStyleStrings[FontStyle];
197 | end;
198 |
199 | procedure TxnCSSFontStyle.SetFontStyle(Value: TxnCSSFontStyleEnum);
200 | begin
201 |   if FFontStyle <> Value then
202 |     begin
    
```

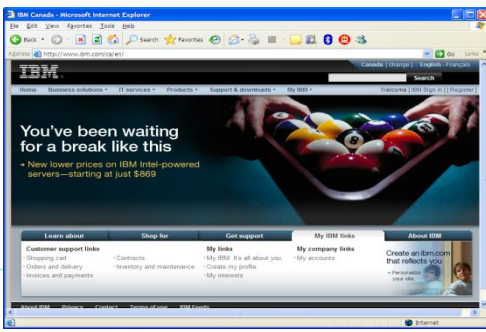
总共潜在的漏洞

静态分析发现的漏洞

动态分析发现的漏洞

动态分析 = 黑盒

- 模拟真实的动态攻击以发现漏洞



# 黑盒分析技术原理--SQL注入

**hackbook**

Username:

Password:

Remember me

[Forgot Password?](#)

Login

File Edit View History Bookmarks Tools Help

https://login.hackbook.com/login.php

hackbook

Hackbook Login

Everyone Can Join

**An Error Has Occurred**

Summary: Syntax error (missing operator) in query expression 'username = '' AND password = 'foobar'.

Error Message Details:

System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'psaok'. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at

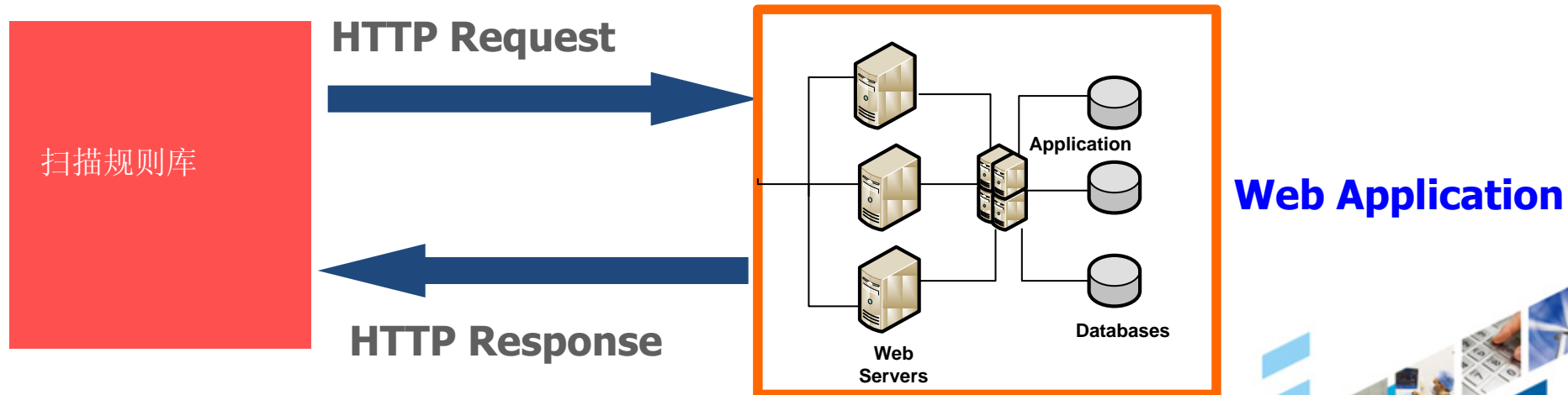
**SELECT \* from tUsers where  
userid="" AND password='foobar'**

sender, EventArgs e) in d:\downloads\hitorom\hual\_yo\website\pank\login.aspx.cs:line 33 at System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)

Email:

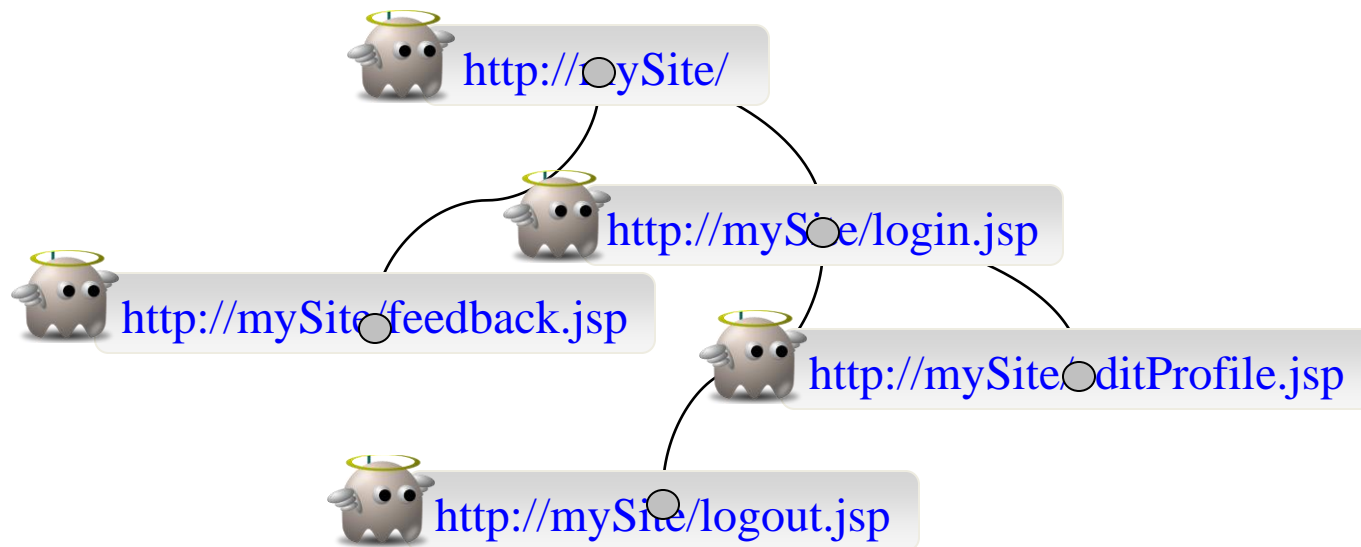
# AppScan工作原理(扫描规则库,爬行,测试)

- 通过探索(爬行)整个Web应用结构
- 以黑盒方式分析被测网站
- 根据分析, 发送修改的HTTP Request进行攻击尝试
- 通过对于Response的分析验证是否存在缺陷



# 黑盒分析技术工作原理(核心技术 1: 爬行/探索)

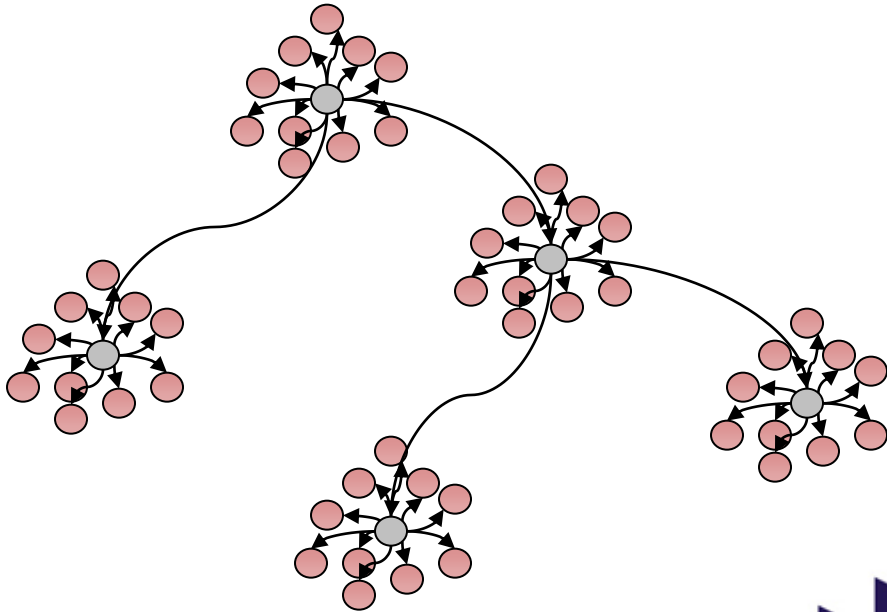
- 第一步: 爬网





# 黑盒分析技术工作原理(测试:模拟攻击)

- 第一步： 爬网
- 第二步： 针对找到的页面， 生成进行模拟攻击



# 白盒分析技术原理--SQL注入

Source – 参数从这里接收

```
// ...
String username = request.getParameter("username");
String password = request.getParameter("password");

// ...
String query = "SELECT * from tUsers where " +
    "userid='" + username + "' " +
    "AND password='" + password +

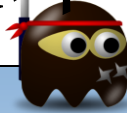
// ...
ResultSet rs = stmt.executeQuery(query);
```

参数在这里被包装和改变

Sink – 在这里输出



# 白盒分析技术工作原理



```
String username = request.getParameter("username");
```

```
// ...
```

```
String username = request.getParameter("username");
```

```
String password = request.getParameter("password");
```

```
// ...
```

```
String query = "SELECT * from tUsers where " +  
"userid='" + username + "'";
```

```
String query = "SELECT ..." + username
```

```
// ...
```

```
ResultSet rs = stmt.executeQuery(query);
```

```
ResultSet rs = stmt.executeQuery(query);
```

# 组合测试和分析

## 黑盒分析技术

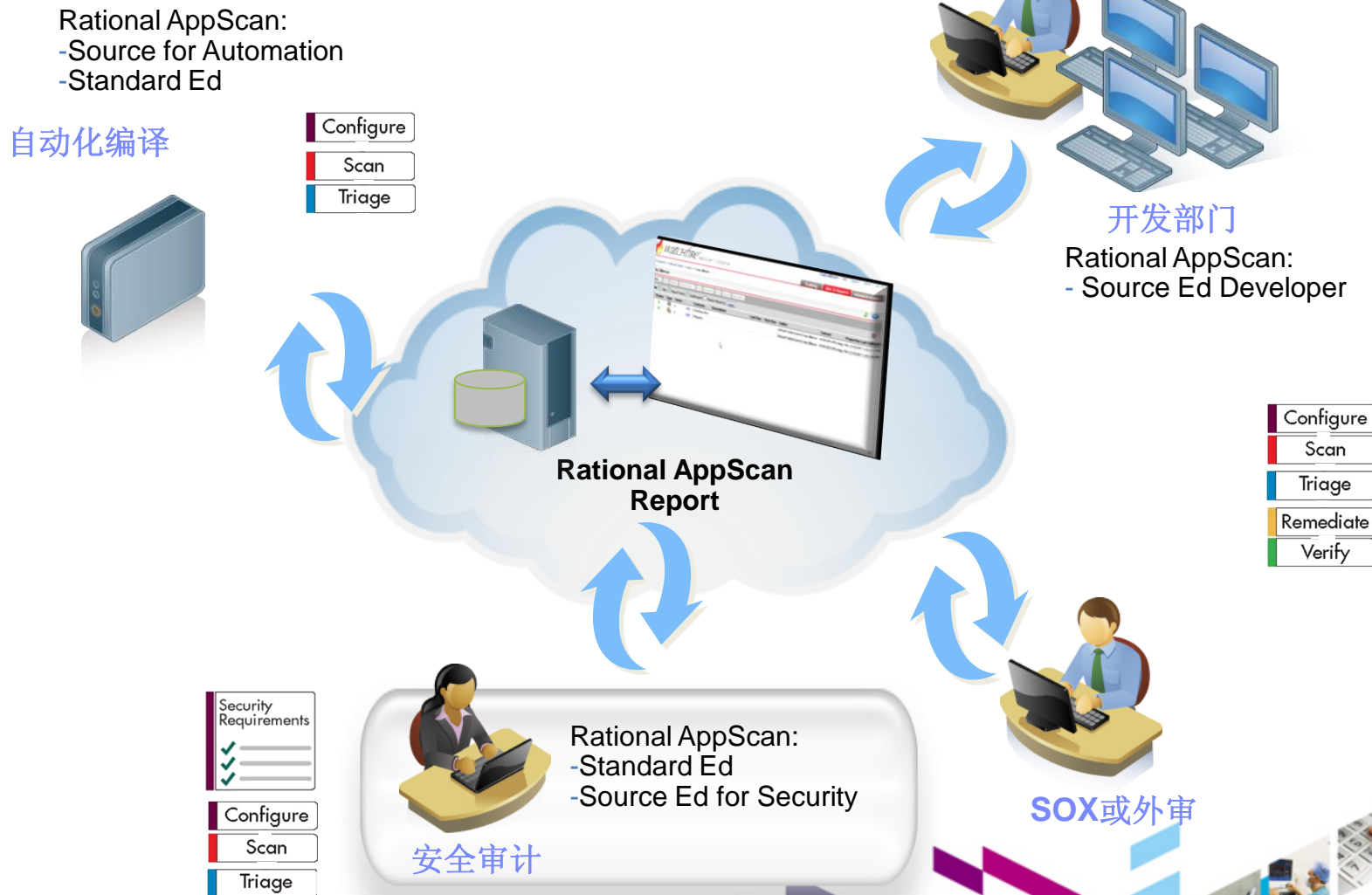
- 准确性
- 无需源代码
- 代码覆盖率低
- 要求满足HTTP协议
- 支持多组件
- 需要可以部署的应用
- 较少前提条件
- 类似黑客的真实攻击

## 白盒分析技术

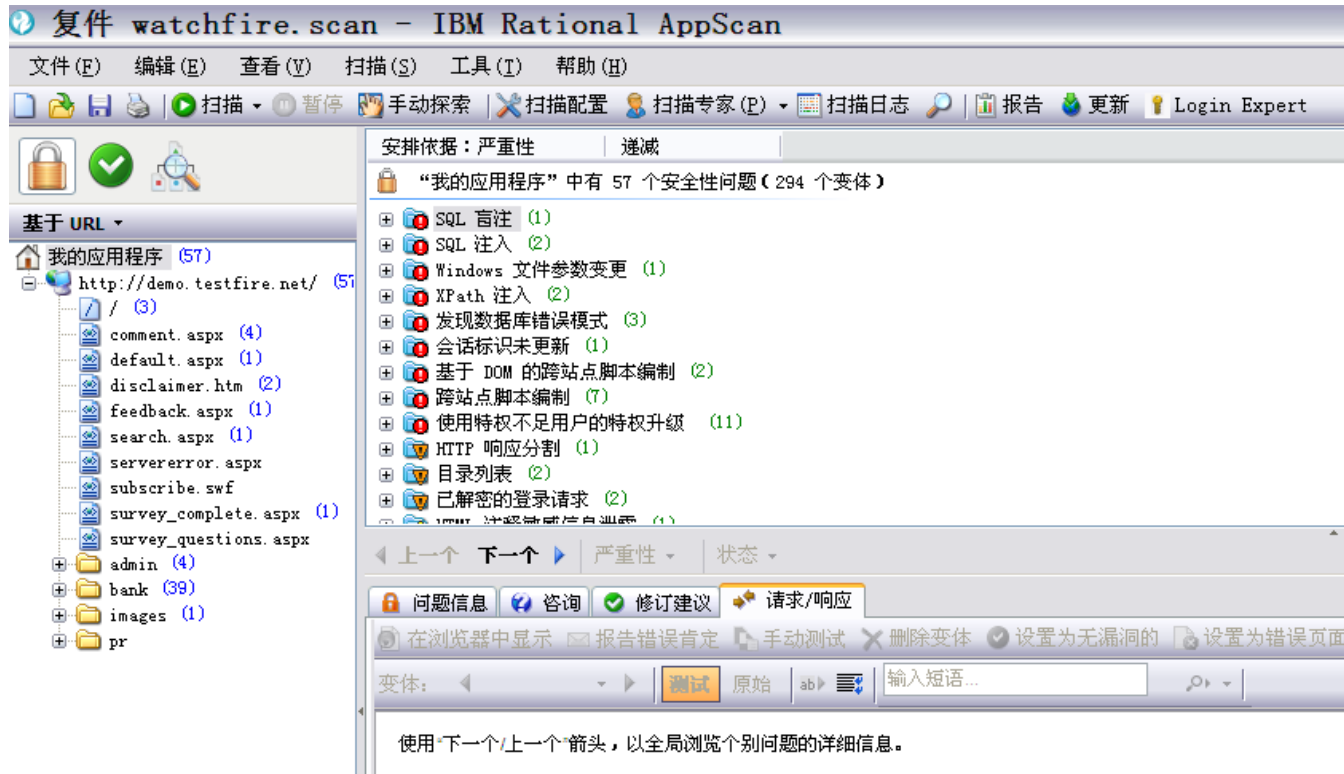
- 代码/路径覆盖率高
- 受限于给定代码
- 不仅仅支持HTTP
- 支持部分应用的分析
- 按照不同程序语言/框架提供支持
- 无需部署应用
- 误报率增加
- 集成/部署的漏洞无法发现



# 基于的企业级应用安全测试平台



# 对部署环境: AppScan 标准版对WEB网站的安全扫描:





# 报告的集中展现 (WEB上)

IBM Rational AppScan, Enterprise Edition

ASE\Administrator | 帮助 | 支持 | 关于

作业和报告 管理

作业和报告 > ASE > china mobile > 汇总仪表盘

上次更新时间: 2010-1-8 17:09:45

文件夹: ASE > china mobile > shanghai > 模板 > 用户

汇总仪表盘 - 按照报告包

上次更新时间: 2010-1-8 17:09:45

图形摘要—所有模块

图形摘要—安全

按照报告包排列的详细摘要

按照模块产生的报告

电子邮件

2010-1-8

2010-1-8

按报告包排列的问题严重性

WASC 威胁分

报告包	信息	低	中	高
总计	~900	~100	~100	~100
安徽报告包	~10	~10	~10	~10
北京	~10	~10	~10	~10
福建	~10	~10	~10	~10
甘肃安全报告	~10	~10	~10	~10
广东移动	~10	~10	~10	~10
广东移动_XSS问题	~10	~10	~10	~10
广东移动门户报告	~10	~10	~10	~10
贵州安全报告	~10	~10	~10	~10
河北移动	~10	~10	~10	~10
河南移动	~10	~10	~10	~10
黑龙江移动	~10	~10	~10	~10
吉林移动_部分	~10	~10	~10	~10
江苏	~10	~10	~10	~10
江西安全报告	~10	~10	~10	~10
辽宁安全报告	~10	~10	~10	~10
内蒙移动_部分	~10	~10	~10	~10
青海移动	~10	~10	~10	~10
山东	~10	~10	~10	~10
陕西移动	~10	~10	~10	~10
上海安全报告	~10	~10	~10	~10
四川安全报告	~10	~10	~10	~10
四川安全报告	~10	~10	~10	~10
天津安全导入	~10	~10	~10	~10
西藏	~10	~10	~10	~10
重庆安全报告	~10	~10	~10	~10

# 黑盒安全报告：应用级别

IBM® Rational® AppScan® Enterprise Edition

SVRAPPSCAM\Administrator | 帮助 | 支持 | 关于

培训 作业和报告

作业和报告 > ASE > 用户 > SVRAPPSCAM\Administrator > altoro > 安全问题

安装 进程 结果

安全风险评估  
**安全问题**  
 基础结构安全问题  
 修复任务  
 应用程序安全问题

摘要 组 显示 搜索 布局

17 个 URL 上共有 18 种不同类型的 54 个问题

所有项 | 组: 问题类型

项 1-18 / 18

操作: 导出至 Excel 应用

转至页面: 1 / 1 应用

<input type="checkbox"/>	问题类型	数量
<input type="checkbox"/>	跨站点脚本编制	12
<input type="checkbox"/>	基于 DOM 的跨站点脚本编制	3
<input type="checkbox"/>	已解密的登录请求	3
<input type="checkbox"/>	SQL 盲注	2
<input type="checkbox"/>	JSP 文件包含	1
<input type="checkbox"/>	可预测的登录凭证	1
<input type="checkbox"/>	使用 SQL 注入的认证旁路	1
<input type="checkbox"/>	链接注入 (便于跨站请求伪造)	8
<input type="checkbox"/>	通过框架钓鱼	8

# 白盒安全报告-代码级别

安装 进程 结果

导出 电子邮件

摘要 组 显示 搜索 布局

安全问题  
静态分析安全问题  
相关安全问题

33 个文件上共有 15 种不同类型的 652 个问题

漏洞			类型 I			类型 II		
高	中	低	高	中	低	高	中	低
22	2	6	15			82	4	8

所有项 | 组: 严重性

项 1-4 / 4 转至页面: 1 / 1 应用

操作: 导出至 Excel 应用

	数量
<input type="checkbox"/> 高	119
<input type="checkbox"/> 中	6
<input type="checkbox"/> 低	14
<input type="checkbox"/> 信息	513

# 黑盒白盒关联的报告分析

IBM Rational AppScan Enterprise Edition

SVRAPPSCAN\Administrator | 帮助 | 支持 |

培训 作业和报告

作业和报告 > ASE > 用户 > SVRAPPSCAN\Administrator > altoroJ > 相关安全问题

安装 进程 结果

5 | 导出 | 电子邮件

安全问题  
静态分析安全问题  
相关安全问题

在 5 个 URL 上找到 10 个问题。这些问题与 5 个文件中的 6 个静态分析问题相互关联。

所有项

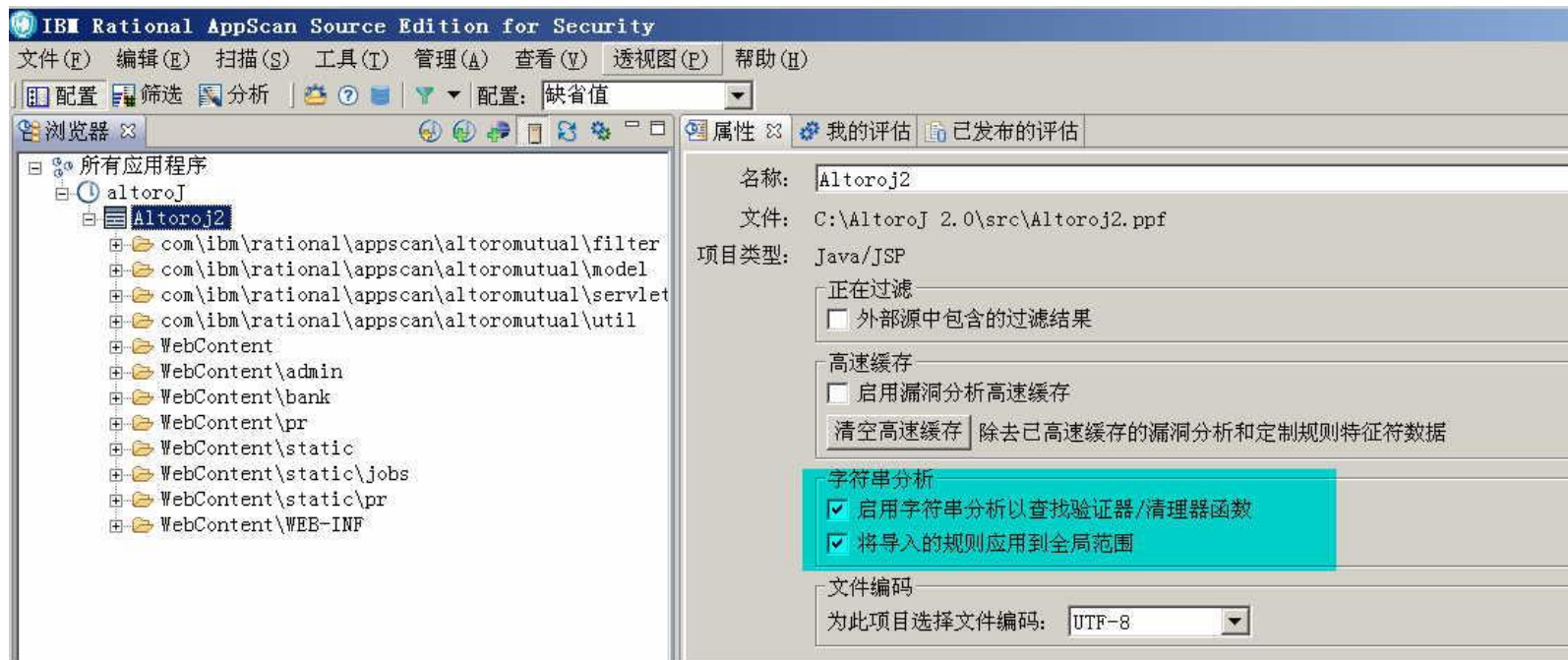
项 1-11 / 11

转至页面: 1

操作: 导出至 Excel 应用

<input type="checkbox"/>	!	动态问题标	测试 URL	元素	问题类型	!	静态问题标	源文件	API	行
<input type="checkbox"/>	!	79	http://localhost:8080/altoromutual/doLogin	uid	SQL 盲注	!	2483	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati java.sql.Statement.ex		112
<input type="checkbox"/>	!	190	http://localhost:8080/altoromutual/doLogin	passw	SQL 盲注	!	2483	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati java.sql.Statement.ex		112
<input type="checkbox"/>	!	79	http://localhost:8080/altoromutual/doLogin	uid	SQL 盲注	!	2893	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati java.sql.Statement.ex		135
<input type="checkbox"/>	!	86	http://localhost:8080/altoromutual/search.js? query		跨站点脚本编制	!	2846	%AltoroJ 2.0_sourcePath%\WebContent%\se javax.servlet.jsp.JspV		24
<input type="checkbox"/>	!	194	http://localhost:8080/altoromutual/bank/cust lang		跨站点脚本编制	!	2982	%AltoroJ 2.0_sourcePath%\WebContent%\ba javax.servlet.jsp.JspV		23
<input type="checkbox"/>	!	176	http://localhost:8080/altoromutual/bank/quei query		跨站点脚本编制	!	2809	%AltoroJ 2.0_sourcePath%\WebContent%\ba javax.servlet.jsp.JspV		12
<input type="checkbox"/>	!	179	http://localhost:8080/altoromutual/bank/quei query		链接注入 (便于跨站请求伪造)	!	2809	%AltoroJ 2.0_sourcePath%\WebContent%\ba javax.servlet.jsp.JspV		12
<input type="checkbox"/>	!	185	http://localhost:8080/altoromutual/bank/cust lang		链接注入 (便于跨站请求伪造)	!	2982	%AltoroJ 2.0_sourcePath%\WebContent%\ba javax.servlet.jsp.JspV		23
<input type="checkbox"/>	!	1	http://localhost:8080/altoromutual/search.js? query		链接注入 (便于跨站请求伪造)	!	2846	%AltoroJ 2.0_sourcePath%\WebContent%\se javax.servlet.jsp.JspV		24
<input type="checkbox"/>	!	178	http://localhost:8080/altoromutual/bank/sho listAccounts		链接注入 (便于跨站请求伪造)	!	2647	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati javax.servlet.http.Htt		47

# 黑白结合：AppScan source edition 中的String Analysis (字符串分析)



# 黑白结合：动态测试中的静态分析

<http://localhost/altoro/disclaimer.htm?url=http://www.netscape.com:>

```
21 : var iPos = document.URL.indexOf("url")+4;
```

```
22 :   var sDst = document.URL.substring(iPos,document.URL.length);
```

```
34 :     <b><script>document.write(sDst);</script></b>
```

- JavaScript Security Analyzer (JSA) 是一项 Rational® AppScan® 扩展，用于执行静态 JavaScript 分析，以检测一系列客户机端问题（主要是基于 DOM 的跨站点脚本编制）
- JSA 完全在本地机器上运行，因此不需要因特网连接。



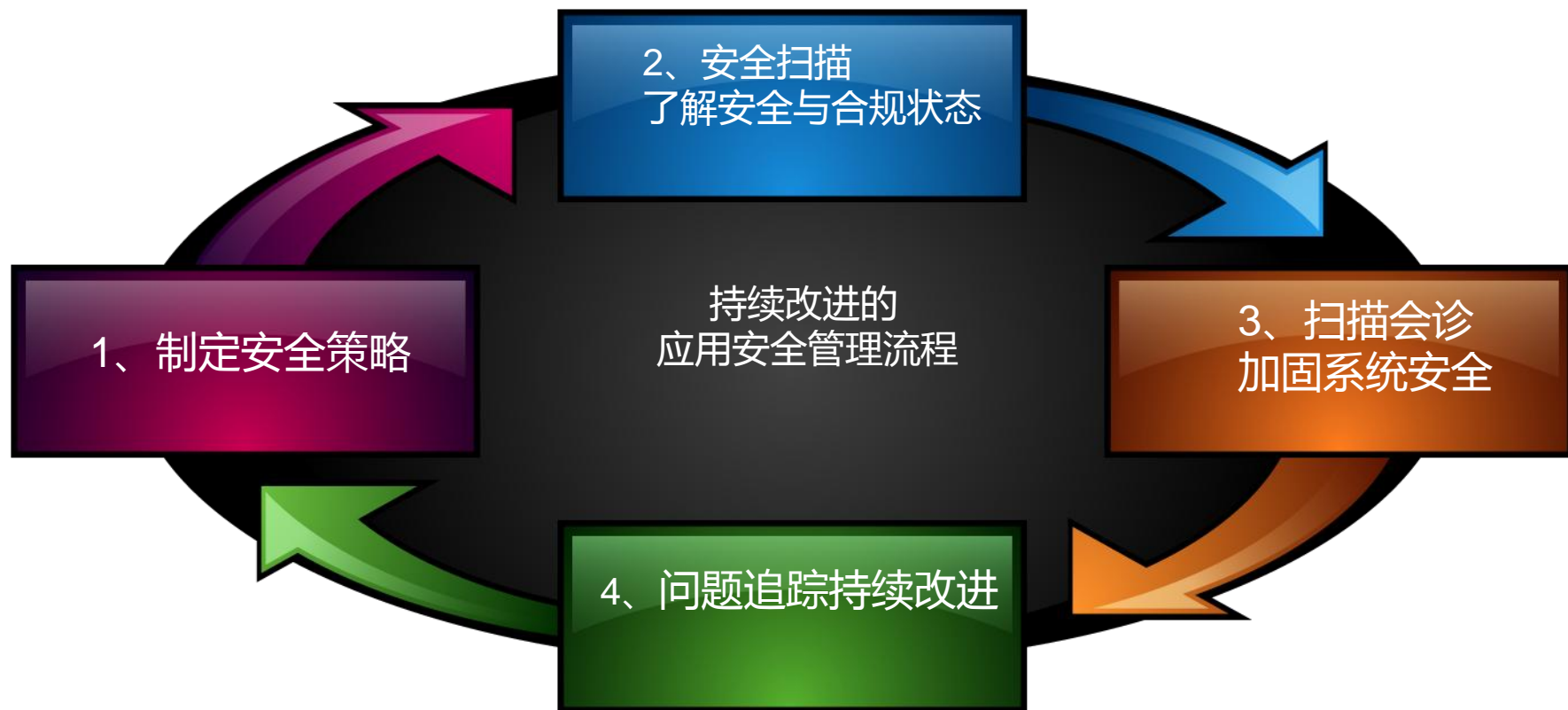


# 议程

- 应用安全面临的挑战
- Rational应用安全和合规测试
  - 2010年的新发展：黑白集成
- 实施案例分享
  - 实施方案的路线图



# 信息系统安全：循序渐进的实施



# 企业信息系统安全与合规管理

## 1、制定安全策略

### 明确IT系统的安全要求

国家政策法规：

- 《信息安全等级保护管理办法》
- Sarbanes-Oxley (US Federal Law)

行业规范：

- 《电子银行业务管理办法》
- ISO 27001

最佳实践：

- ITIL
- OWASP 2010 top10
- WASC
- 2010年CWE/SANS最危险的程序设计错误

业务需要以及自身经验



# OWASP Top10 常见的WEB安全漏洞

应用威胁	产生影响	典型结果
Cross Site scripting	盗取认证, 信息泄漏, ...	伪装正常用户, 或者控制用户操作
Injection Flaws	非法操作数据库/应用服务器...	直接窃取数据
Malicious File Execution	在服务器端执行命令控制服务器	窃取服务器内容
Insecure Direct Object Reference	超越权限控制, 访问敏感的信息和资源	窃取敏感信息内容
Cross-Site Request Forgery	通过调用恶意操作, 借助正常用户进行攻击	通过后台逻辑, 将正常帐户划入黑客帐户
Information Leakage and Improper Error Handling	获取详细的信息, 方便进行攻击	盗取操作系统信息, 进一步攻击操作
Broken Authentication & Session Management	Session控制不适当, 可以方便进行伪造攻击	用户在退出系统后, 通过session信息泄漏数据
Insecure Cryptographic Storage	加密内容过于简单, 易于攻击	对于加密内容进行破解
Insecure Communications	窃取非加密的敏感信息	通过sniffer等方式窃听到用户信息
Failure to Restrict URL Access	对于非授权内容可以直接访问	不通过登陆, 直接访问应用内容



# 行业或者法律法规要求—合规性

- 对部分中央企业网站进行安全状况测试。将通过互联网远程黑盒方式对企业网站进行安全状况测试，不会对企业网站构成威胁。
  - 1、 SQL注入漏洞检查
  - 2、 跨站脚本漏洞检查
  - 3、 CGI漏洞扫描
  - 4、 用户名和密码脆弱性检查
  - 5、 网站结构分析
  - 6、 隐藏文件检查
  - 7、 备份文件安全性检查
  - 8、 数据库挖掘分析
  - 9、 本地权限提升漏洞检查
  - 10、 远程溢出漏洞检查



# 行业或者法律法规关心的安全问题

## 一 行业规定

- 银监会《电子银行业务管理办法》要求金融机构“定期对电子银行系统进行漏洞扫描，并建立对非法入侵的甄别、处理和报告机制”
  - **第四十三条** 金融机构应建立电子银行入侵侦测与入侵保护系统，实时监控电子银行的运行情况，定期对电子银行系统进行漏洞扫描，并建立对非法入侵的甄别、处理和报告机制。
  - **第四十四条** 金融机构开展电子银行业务，需要对客户信息和交易信息等使用电子签名或电子认证时，应遵照国家有关法律法规的规定。
  - 金融机构使用第三方认证系统，应对第三方认证机构进行定期评估，保证有关认证安全可靠和具有公信力。





# IBM Rational AppScan – 业界第一的应用安全扫描工具

## AppScan典型安全问题

- WASC/OWASC（国际应用安全组织）应用安全问题
- Web 2.0应用安全问题
- Web Service安全问题
- 基础架构安全问题（WAS、WebLogic、Apache等配置不当，Dos攻击）
- 网站挂马、钓鱼网站等
- 应用逻辑漏洞（非授权访问等）
- ...

## AppScan的价值

- 不断升级的应用安全规则引擎，直接引入最新的、最全面的应用安全规范
- 全面和准确的安全问题发现和定位，业界第一
- 将安全扫描和管理相结合，保证安全工作开展
- 面向整个应用生命周期提供安全保障

# 配置符合企业的测试策略

- AppScan有一个测试策略库—Test Policy Manager
- 可以为企业选择合适的测试策略
  - 包括预定义策略和用户自定义策略
- 可以定制该方法库，符合企业自身，如：
  - 根据需要修改隐患的优先级别
  - 定制缺陷修复意见

# 配置符合企业的测试策略

**测试策略** 定制

没有分组 输入以查找 导出(E) 导入(I)

测试名称	严重性	使
<input checked="" type="checkbox"/> .NET CS 文件下载	低	是
<input checked="" type="checkbox"/> .NET VB 文件下载	低	是
<input checked="" type="checkbox"/> .NET 解决方案文件下载	低	是
<input checked="" type="checkbox"/> @Mail WebMail 多重跨站点脚本编制	高	是
<input type="checkbox"/> "Behold"Counter.exe 拒绝服务	高	是
<input checked="" type="checkbox"/> "IBM WebSphere"..跨站点脚本编制	高	是
<input checked="" type="checkbox"/> 2532 Gigs activateuser.php 路径遍历	高	是
<input checked="" type="checkbox"/> 8.3 命名系统源代码泄露	低	是
<input checked="" type="checkbox"/> ... .. 路径遍历	高	是

编辑 复位为缺省值

咨询 修订建议

**.NET CS 文件下载**

- 严重性: 低
- 类型: 基础结构测试
- WASC 威胁分类: [信息泄露类型](#); [信息泄露](#)
- CVE 引用: 不适用
- 安全风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

This policy includes all tests except invasive and port listener tests.

更新设置(U)...

当前测试策略是最新版的。

**策略文件**

最近的策略

- my
- 1
- new
- j2ee
- normal
- 浏览...

预定义的策略

- Default
- Application-Only

# 企业信息系统安全与合规管理

## 2、了解安全与合规状态

### 了解现有系统的安全状况、合规状况

基于安全策略，把安全策略转化为IT环境中的具体配置  
产品供应商会提供安全配置的建议、方法、工具等  
安全配置的具体步骤需要文档化，脚本化，自动化  
安全配置需要定期地、自动地根据安全策略进行核查  
自动或者手动部署安全配置  
利用第三方工具，对安全配置进行管理及核查等工作



# 应用安全现状及需求分析

## • IT开发模式

- 业务系统开发外包
- 系统升级更新频繁
- 借助安全咨询公司进行风险评估



内部安全月报、内审和企业外部的  
SOX安全合规审计

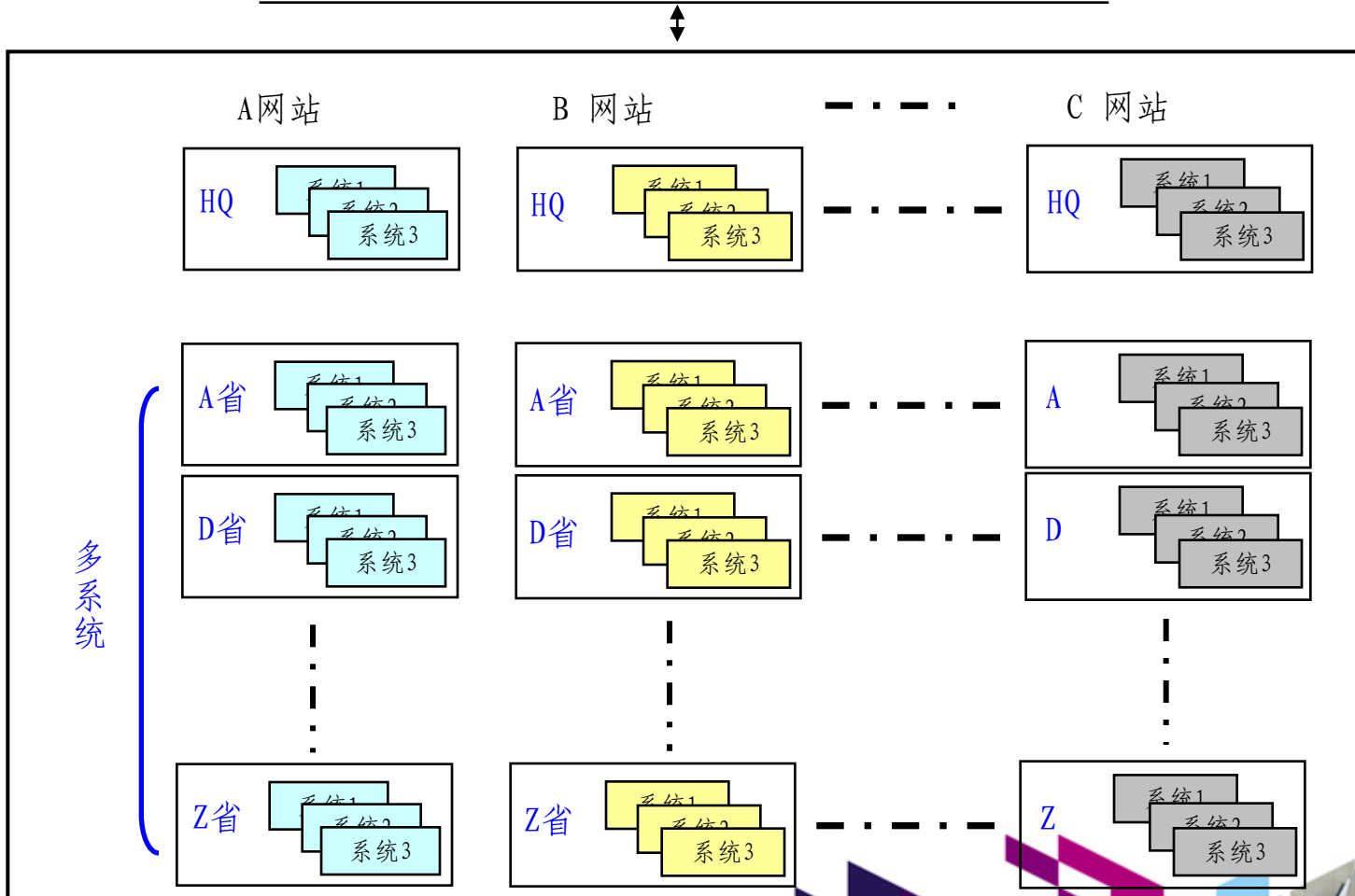
## • 运维部门

- 运维部门往往注重网络等硬件及操作系统安全，对于应用安全关注的精力不到10%，但据Gartner调研来看应用隐患特别是Web应用安全占总体安全的75%；
- 安全咨询公司所做的风险评估的比重非常小。



# 选择核心系统进行安全评估

定期安全检查





# 了解信息系统的的安全与合规现状

- 了解现有环境中的各种人员、流程、技术（产品、设备等）；
- 对现有环境的各个环节进行安全评估和风险评估；



- 根据企业的安全策略以及评估出来的结果，找到风险或者问题



# 企业信息系统安全与合规管理

## 3、加固系统安全

### 确保IT系统更加安全、更好地满足合规要求

#### 应用系统加固：

- 集中用户和账号管理系统（IM）
- 强认证系统（数字证书、动态口令、指纹等）
- 针对SOA/WebService的安全加固



# 了解信息系统的的安全与合规现状

- 把发现的风险（或者问题）按照以下一些因素进行排序：
  - 是否违背必须遵守的法律、法规、行业规范等；
  - 风险（或者问题）造成影响的范围、程度以及发生的概率；
  - 资金的限制；
  - 信息系统发展的整体规划；
  - ...

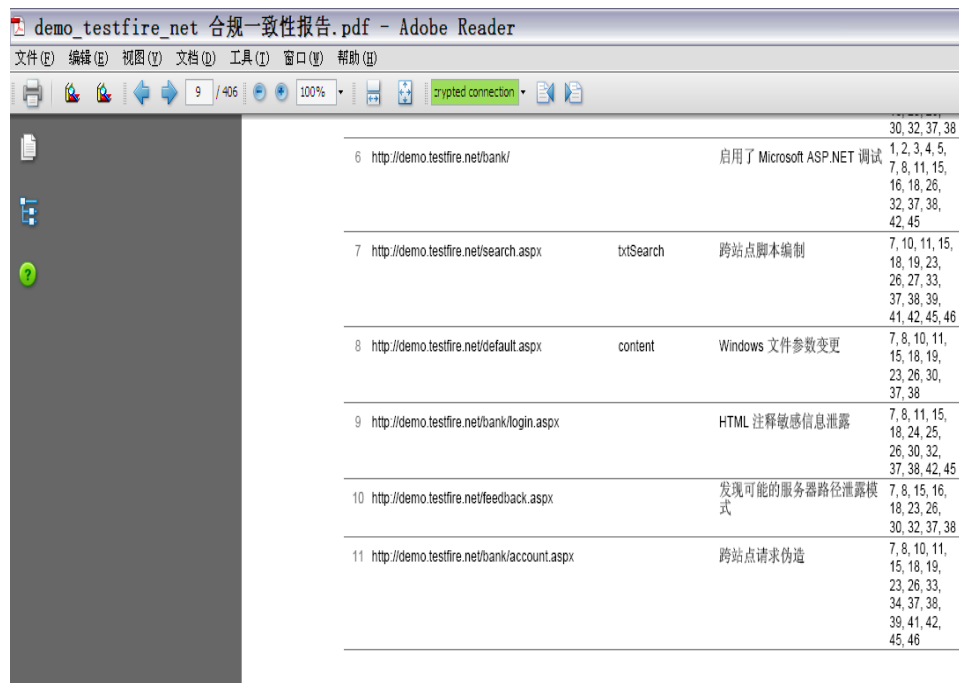


- 针对不同的风险（或者问题）选择不同的处理方式：
  - 减小（Reduce, Mitigate）；
  - 转嫁（Transfer）；
  - 接受（Accept）；



# AppScan提供合规性安全测试报告

- 满足企业自审
- 周期性的审计和持续改进
- 满足法律法规的要求
- 避免安全损失



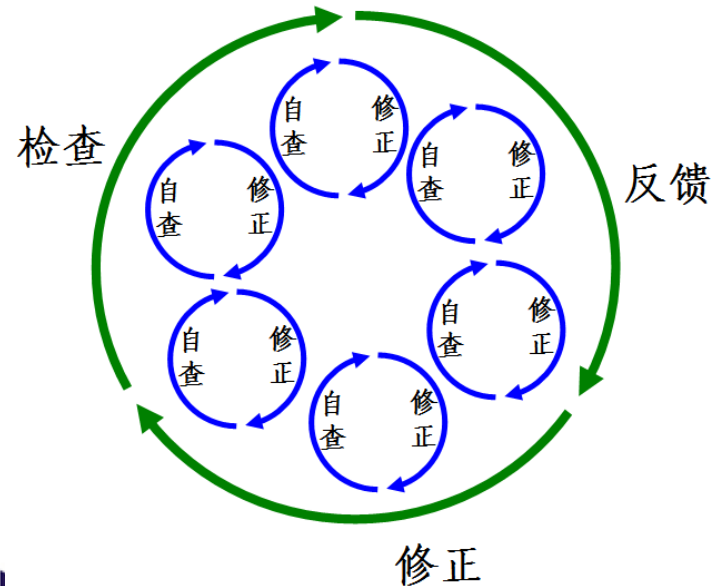
Id	URL	Parameter	Issue	Page Numbers
6	http://demo.testfire.net/bank/		启用了 Microsoft ASP.NET 调试	30, 32, 37, 38
7	http://demo.testfire.net/search.aspx	txtSearch	跨站点脚本编制	1, 2, 3, 4, 5, 7, 8, 11, 15, 16, 18, 26, 32, 37, 38, 42, 45
8	http://demo.testfire.net/default.aspx	content	Windows 文件参数变更	7, 10, 11, 15, 18, 19, 23, 26, 27, 33, 37, 38, 39, 41, 42, 45, 46
9	http://demo.testfire.net/bank/login.aspx		HTML 注释敏感信息泄露	7, 8, 10, 11, 15, 18, 24, 25, 26, 30, 32, 37, 38, 42, 45
10	http://demo.testfire.net/feedback.aspx		发现可能的服务器路径泄露模式	7, 8, 15, 16, 18, 23, 26, 30, 32, 37, 38
11	http://demo.testfire.net/bank/account.aspx		跨站点请求伪造	7, 8, 10, 11, 15, 18, 19, 23, 26, 33, 34, 37, 38, 39, 41, 42, 45, 46

# 企业信息系统安全与合规管理

## 4、监控安全与合规状态

### 实时监控企业信息系统的安全与合规状况

- 安全问题分析 and 确认
- 安全问题整改
- 相关人员的应用安全意识
- 报告汇总和分析
- 历史趋势分析



# 趋势分析 报告对比

创建报告

IBM Rational AppScan Enterprise Edition

作业和报告 > ASE > china mobile > 汇总仪表盘

文件夹

- ASE
  - china mobile
    - shanghai
    - 模板
    - 用户

最近查看的

- 汇总仪表盘
- 报告包摘要 (广东10086报告)
- 安全综合报告
- 报告包摘要 (天津安全导入)
- 安全问题 (天津安全导入)
- 中国移动Web安全综合报告
- 安全问题 (广西移动)

创建报告

ASE | Administrator | 帮助 | 支持 | 关于

培训 | 作业和报告 | 管

导出 | 电子邮件

WASC 威胁分 合规性报告

WASC 威胁分类

7
0
3
2
0
119
3
5
62
0
0
3
14
1
19
2
0
0
23
41
0
0

汇总仪表盘 - 图形摘要 - 安全

上次更新时间: 2010-1-8 17:09:45

图形摘要—所有模块 | 图形摘要-安全 | 按照报告包排列的详细摘要 | 按照模块产生的报告

2010-1-8

按报告包排列的问题严重性

报告包	信息	低	中	高
总计	0	0	0	1000
安徽报告包	0	0	0	10
福建	0	0	0	10
甘肃安全报告	0	0	0	10
广东	0	0	0	10
广东10086报告	0	0	0	10
广东移动	0	0	0	10
广东移动门户报告	0	0	0	10
贵州安全报告	0	0	0	10
河北移动	0	0	0	10
河南移动	0	0	0	10
黑龙江移动	0	0	0	10
贵州安全报告	0	0	0	900
河北移动	0	0	0	10
河南移动	0	0	0	10
黑龙江移动	0	0	0	150
吉林移动_部分	0	0	0	10
江苏	0	0	0	10
江西安全报告	0	0	0	10
辽宁安全报告	0	0	0	10
内蒙移动_部分	0	0	0	10
青海移动	0	0	0	10
山东	0	0	0	10
陕西移动	0	0	0	10
上海安全报告	0	0	0	10
四川安全报告	0	0	0	10
天津安全导入	0	0	0	100
西藏	0	0	0	10
重庆安全报告	0	0	0	10

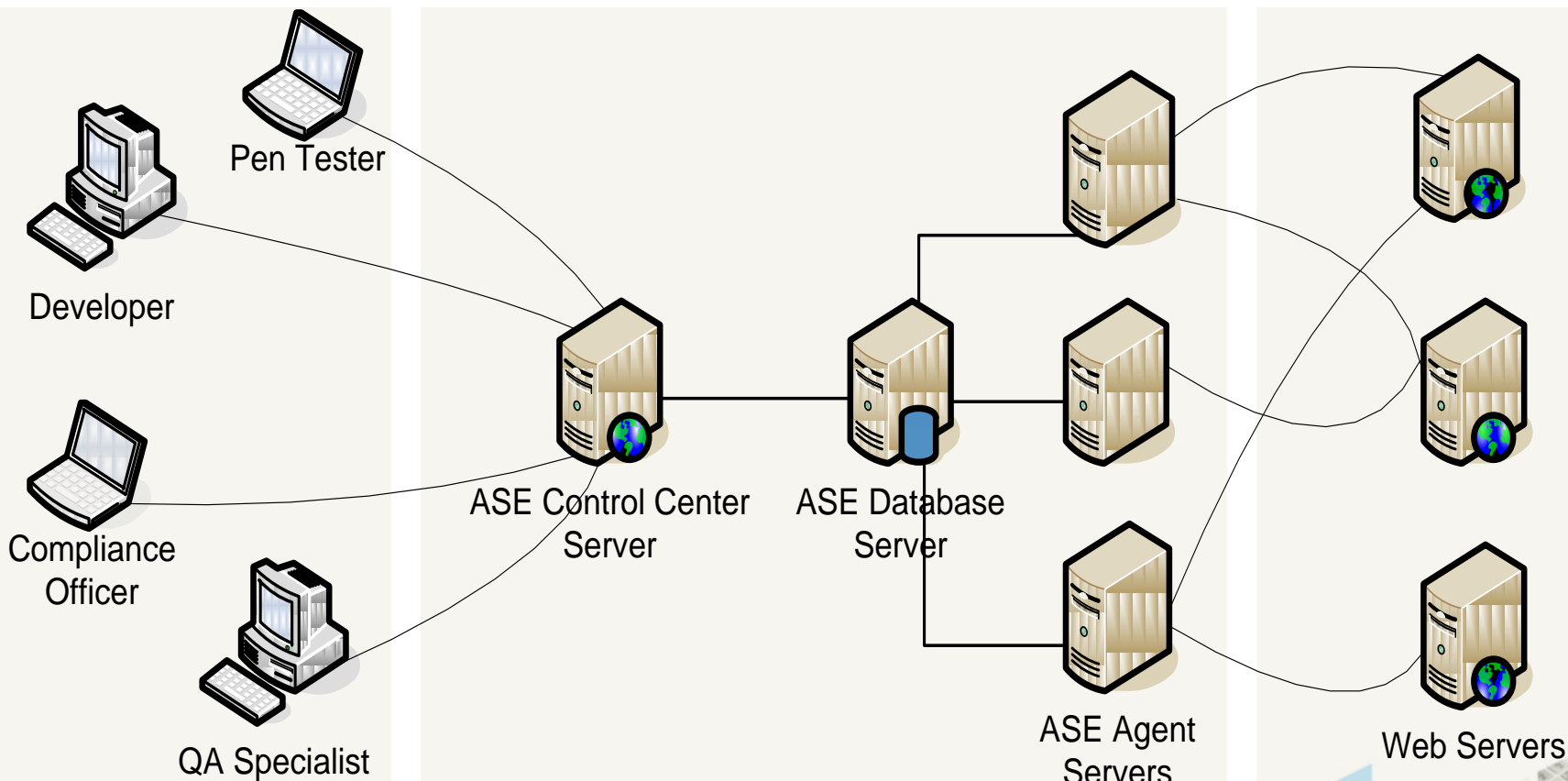


# 使用企业级AppScan

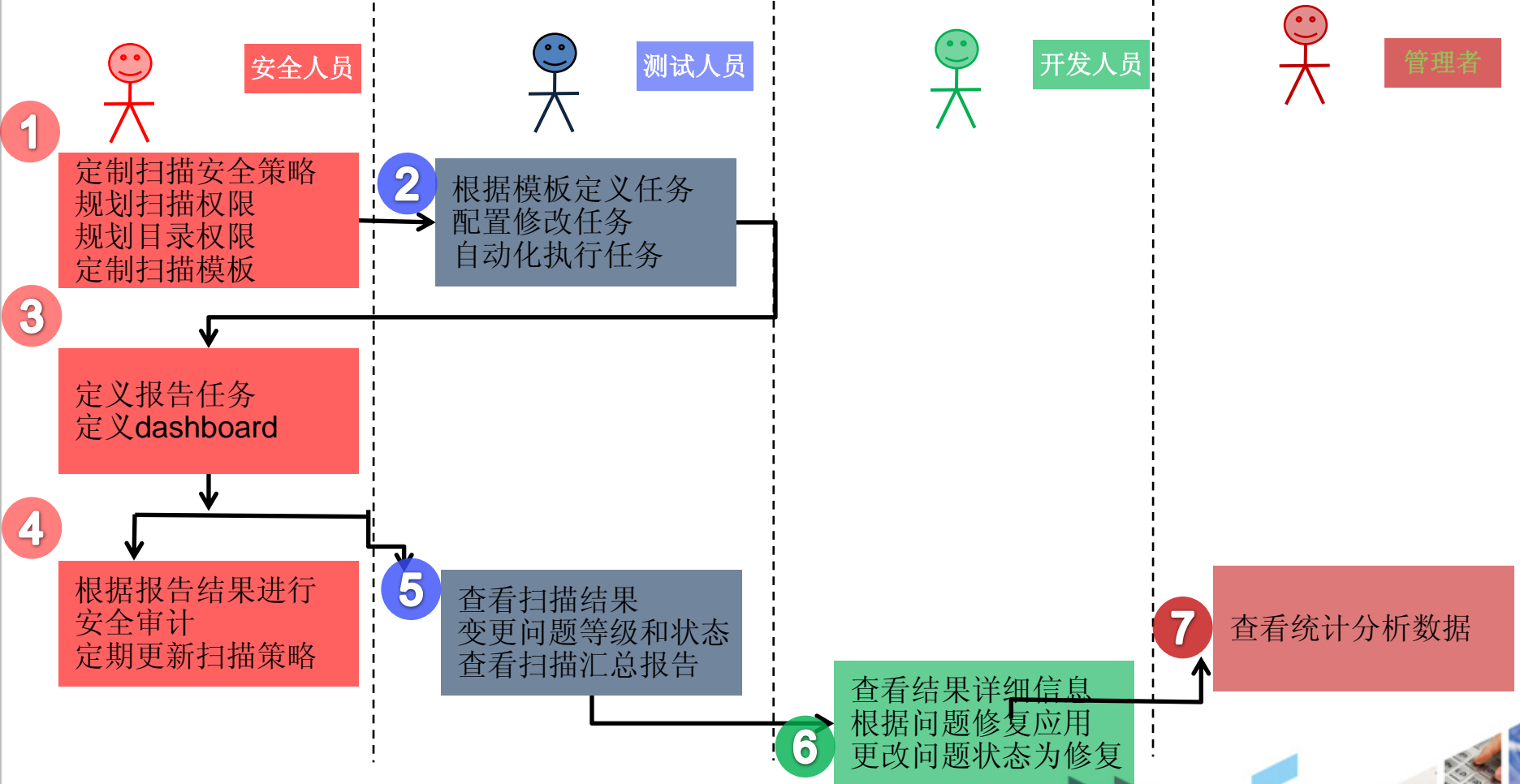
客户机

AppScan Enterprise

目标系统



# 建立适合企业的应用安全使用流程



# 安全规划及演进路线

## 第一阶段

**建设目标:**

黑盒定期检查扫描  
部署黑盒分布扫描系统对众多集中扫描  
扫描结果汇总分析

黑盒扫描系统

## 第二阶段

**建设目标:**

部署白盒代码安全审核版本

白盒分布扫描系统

## 第三阶段

**建设目标:**

黑白盒汇总分析  
完整的应用安全管理建设

应用安全管理



THANK  
YOU



# 白盒测试中的黑盒测试：字符串分析

The screenshot displays the IBM Rational AppScan Source Edition for Security interface. The main window shows a project tree on the left and configuration options on the right.

**Project Tree (Left):**

- 所有应用程序
  - aloroj
    - Altoroj2**
      - com\ibm\rational\appscan\aloromutual\filter
      - com\ibm\rational\appscan\aloromutual\model
      - com\ibm\rational\appscan\aloromutual\servlet
      - com\ibm\rational\appscan\aloromutual\util
      - WebContent
        - WebContent\admin
        - WebContent\bank
        - WebContent\pr
        - WebContent\static
          - WebContent\static\jobs
          - WebContent\static\pr
        - WebContent\WEB-INF

名称: Altoroj2

文件: C:\Altoroj 2.0\src\Altoroj2.ppf

项目类型: Java/JSP

正在过滤

外部源中包含的过滤结果

高速缓存

启用漏洞分析高速缓存

除去已高速缓存的漏洞分析和定制规则特征符数据

字符串分析

启用字符串分析以查找验证器/清理器函数

将导入的规则应用到全局范围

文件编码

为此项目选择文件编码: UTF-8



# 黑盒测试中的白盒测试：JavaScript 安全分析

The screenshot displays the IBM Rational AppScan application interface. The main window shows a tree view of scanned URLs under '我的应用程序 (1)'. A dialog box titled 'JavaScript Security Analyzer' is open, featuring the IBM logo and the text 'With String Analysis Technology'. The dialog contains a checkbox labeled '扫描过程中分析 JavaScript' (Analyze JavaScript during scanning), which is currently unchecked. Below the checkbox, there is a descriptive text: 'JavaScript Security Analyzer 应用静态分析来检测客户机端安全性问题 (如基于 DOM 的跨站点脚本编制)'. At the bottom right of the dialog is a button labeled '立即分析 (A)'. The background interface includes a menu bar with options like '文件(F)', '编辑(E)', '查看(V)', '扫描(S)', '工具(T)', and '帮助(H)'. A toolbar contains icons for '扫描', '暂停', '手动探索', '恶意软件测试', '扫描配置', '扫描专家', '扫描日志', '报告', '更新', 'Login Expert', and '分析 JavaScript'. A status bar at the bottom of the dialog shows navigation buttons: '上一个', '下一步', '严重性', and '州', along with action buttons: '问题信息', '咨询', '修订建议', and '请求/响应'.