爱开发 重创新 更智慧

Innovate2011

IBM Rational 软件创新论坛

Software. Everyware.

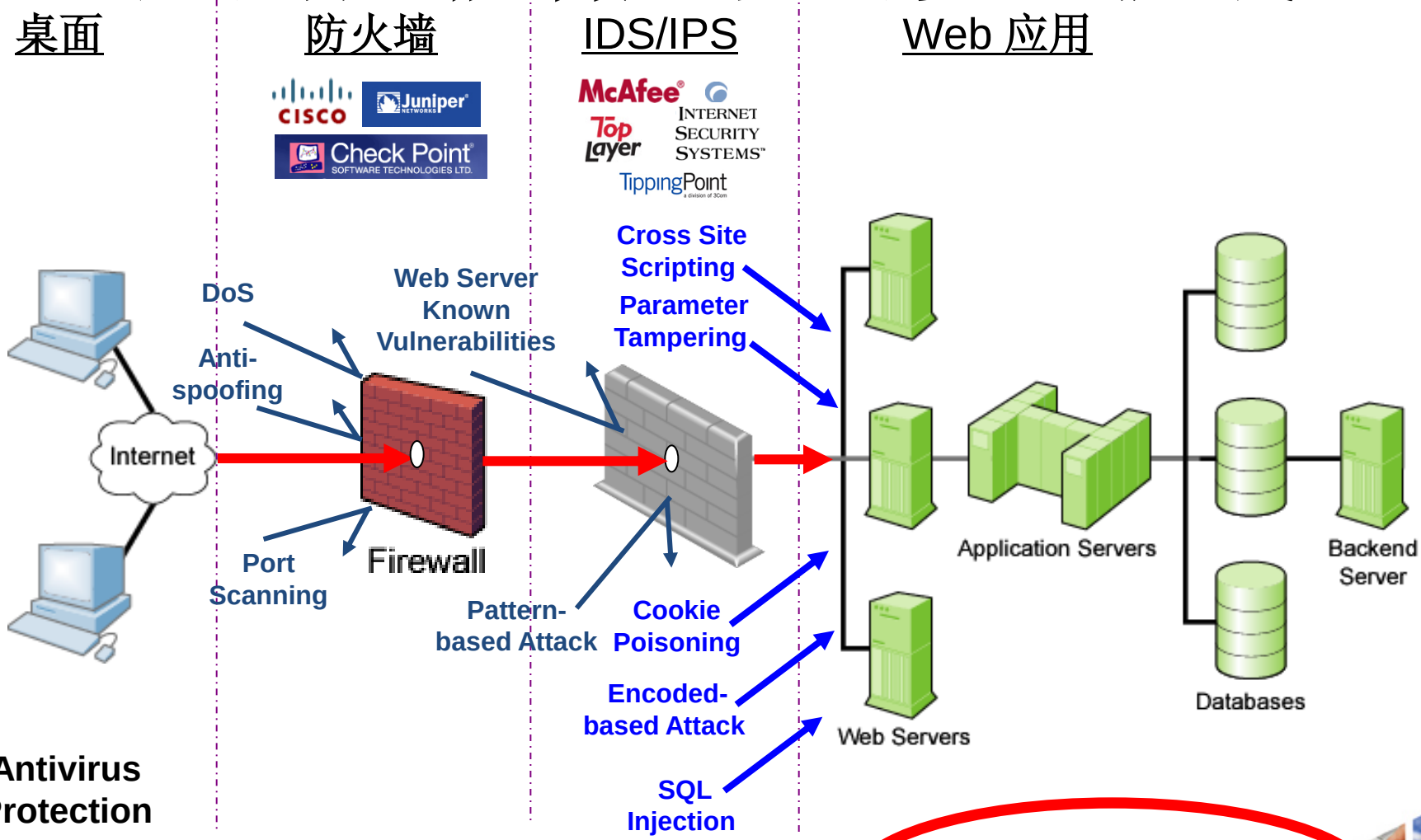
Rational 应用安全和合规测试解决方案

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...



ISS

Rational AppScan

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

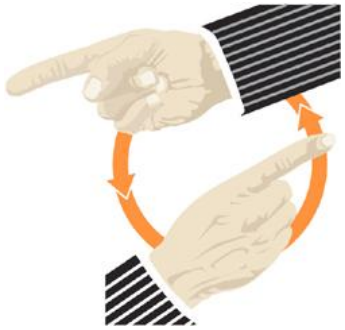
攻击方式

- 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

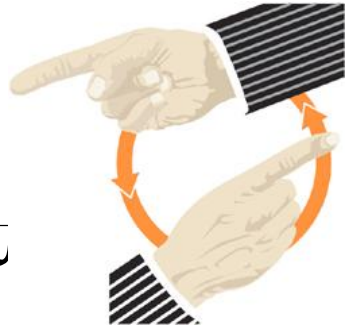
X-force 2010年安全分析报告

- **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

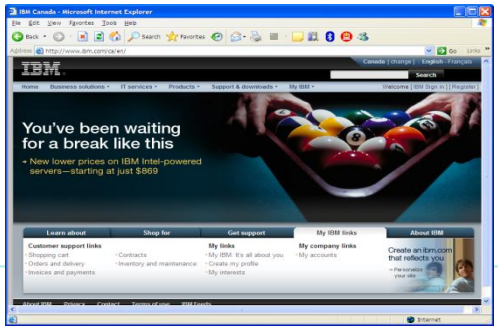
应用安全测试:单一技术向复合技术转变

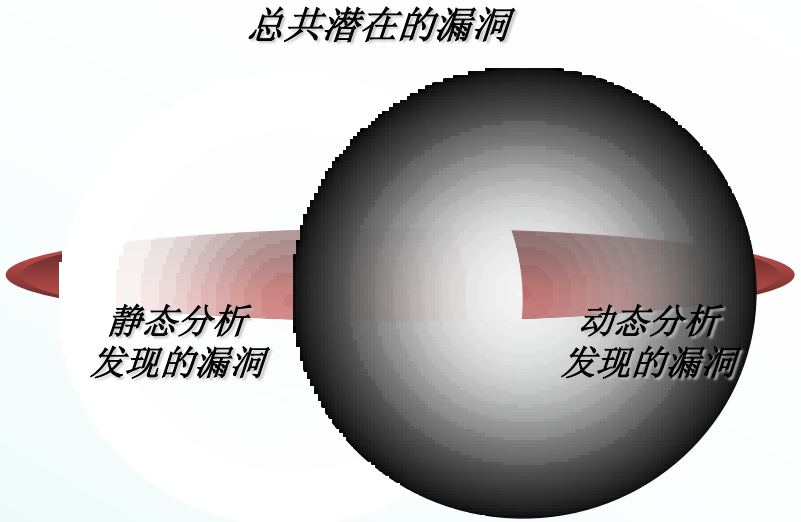
静态分析 = 白盒

- *扫描源代码发现漏洞*

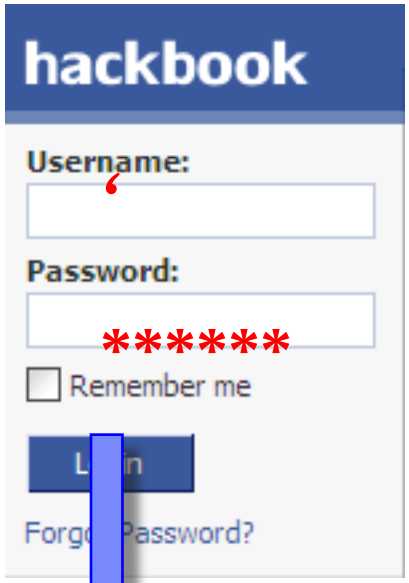
动态分析 = 黑盒

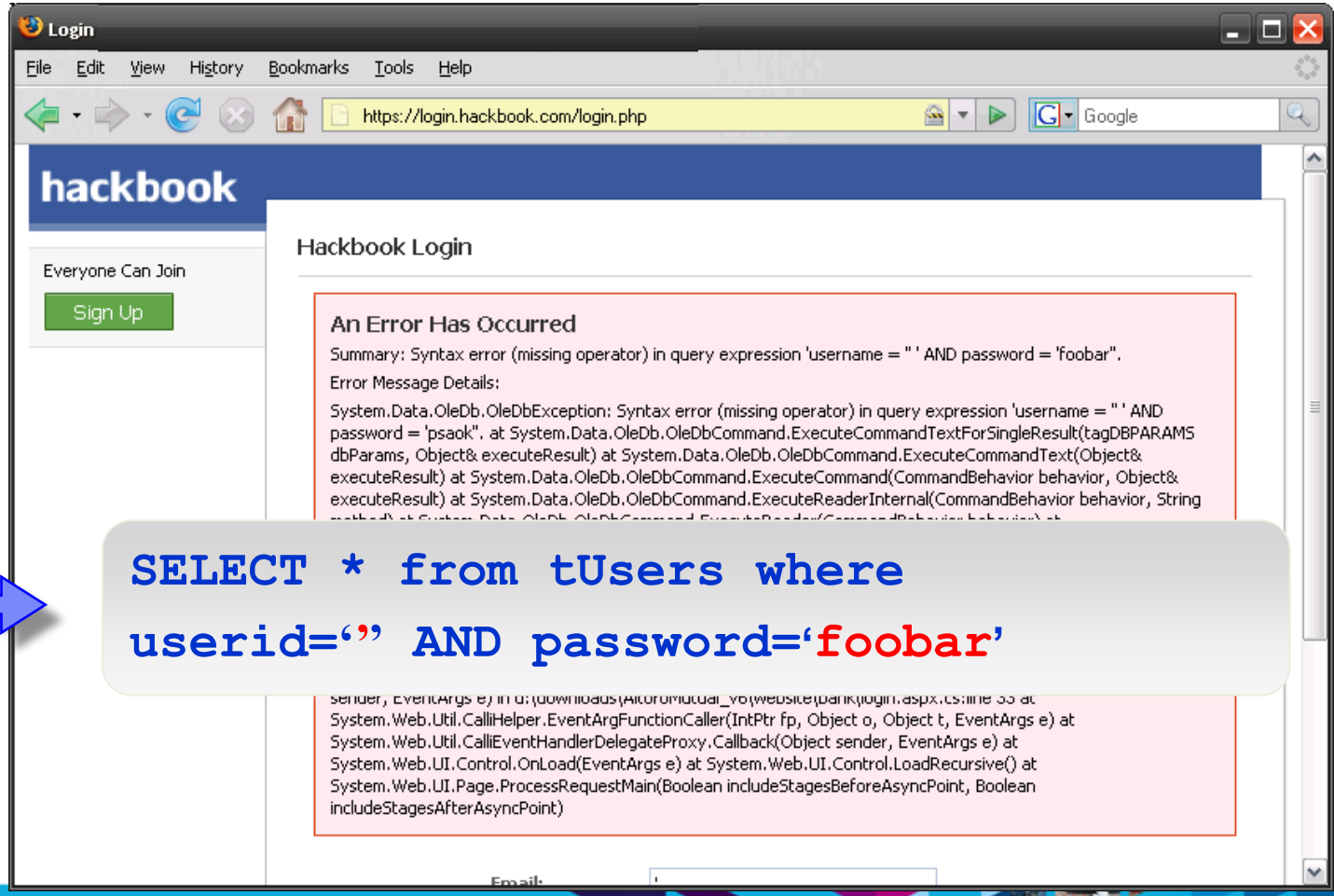
- *模拟真实的动态攻击以发现漏洞*





黑盒分析技术原理--SQL注入

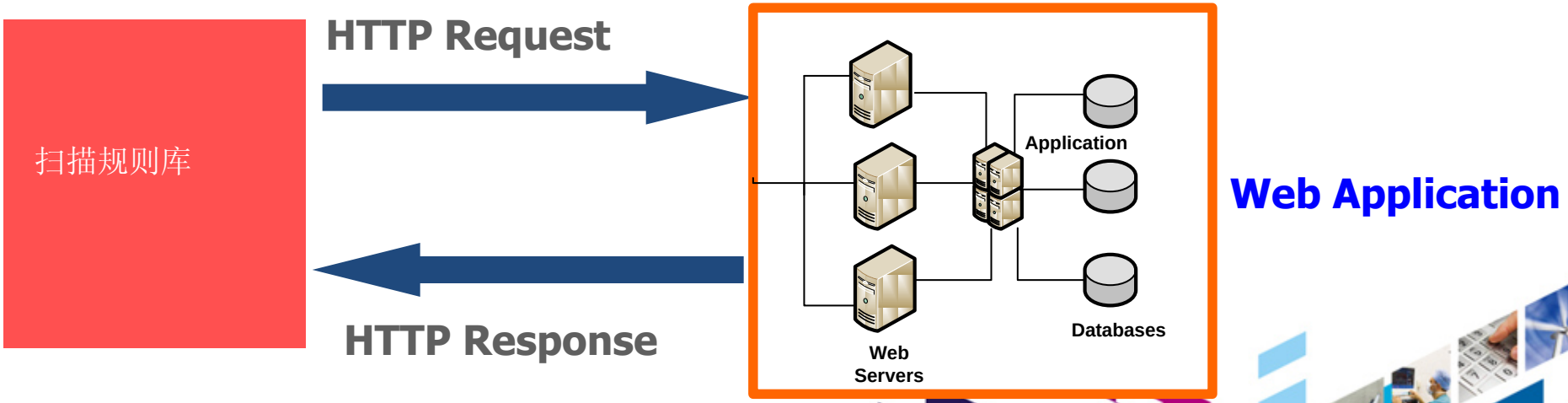





```
SELECT * from tUsers where
userid='' AND password='foobar'
```

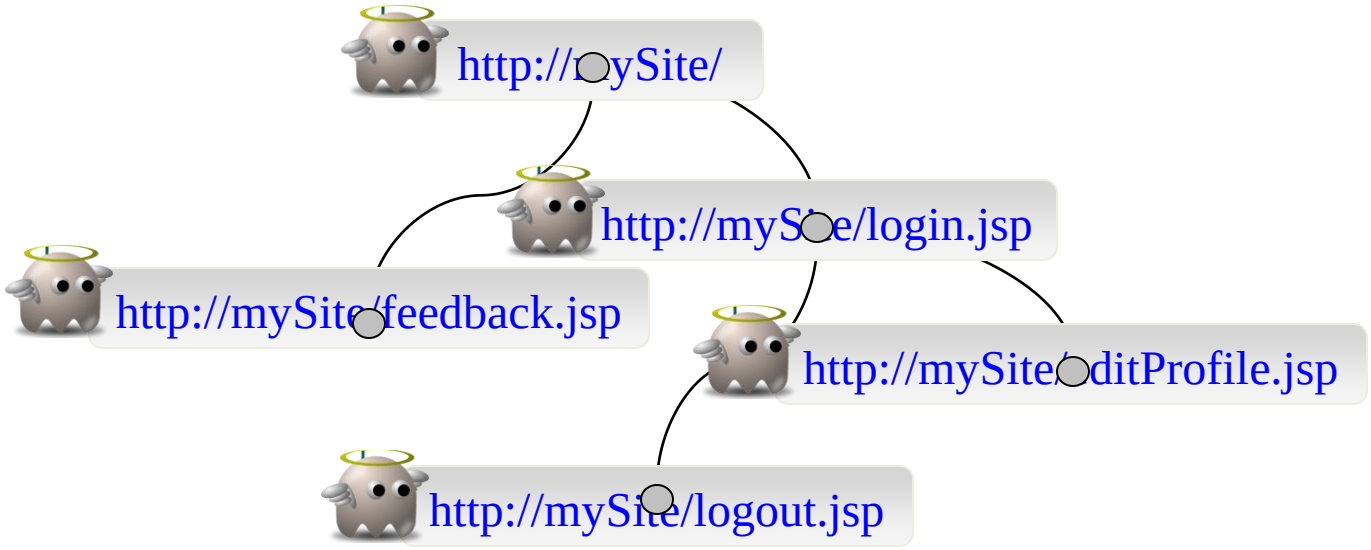
AppScan工作原理(扫描规则库,爬行,测试)

- 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



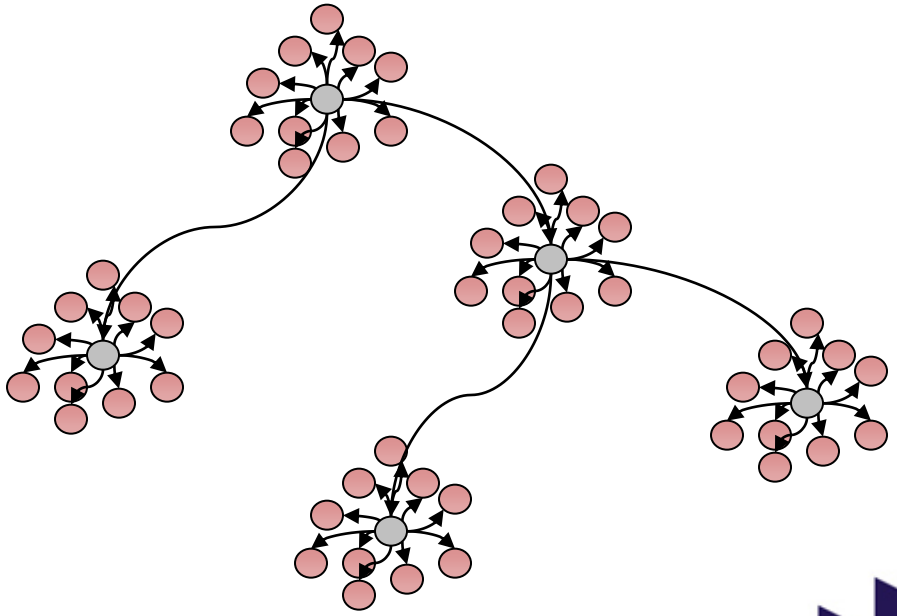
黑盒分析技术工作原理(核心技术1: 爬行/探索)

- 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

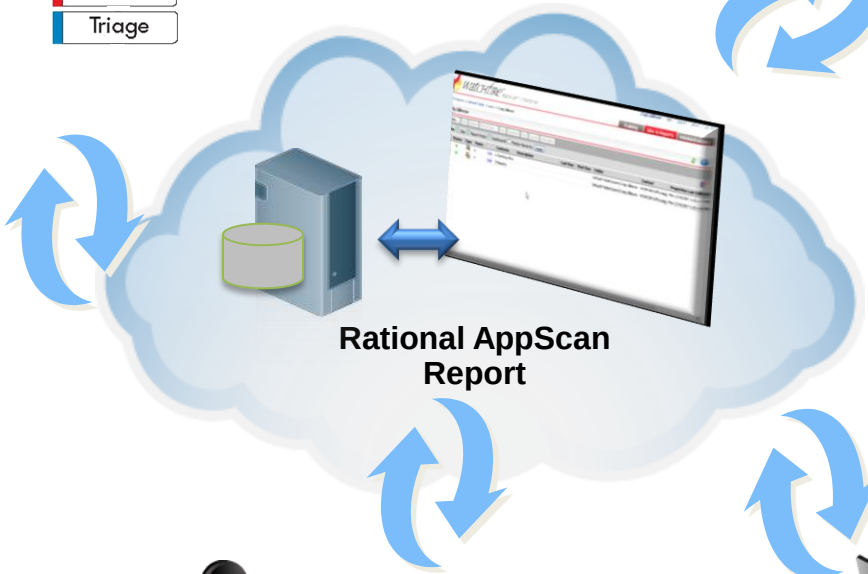
Rational AppScan:
-Source for Automation
-Standard Ed

自动化编译

Configure
Scan
Triage

开发部门

Rational AppScan:
- Source Ed Developer



Rational AppScan Report

Configure
Scan
Triage
Remediate
Verify

SOX或外审

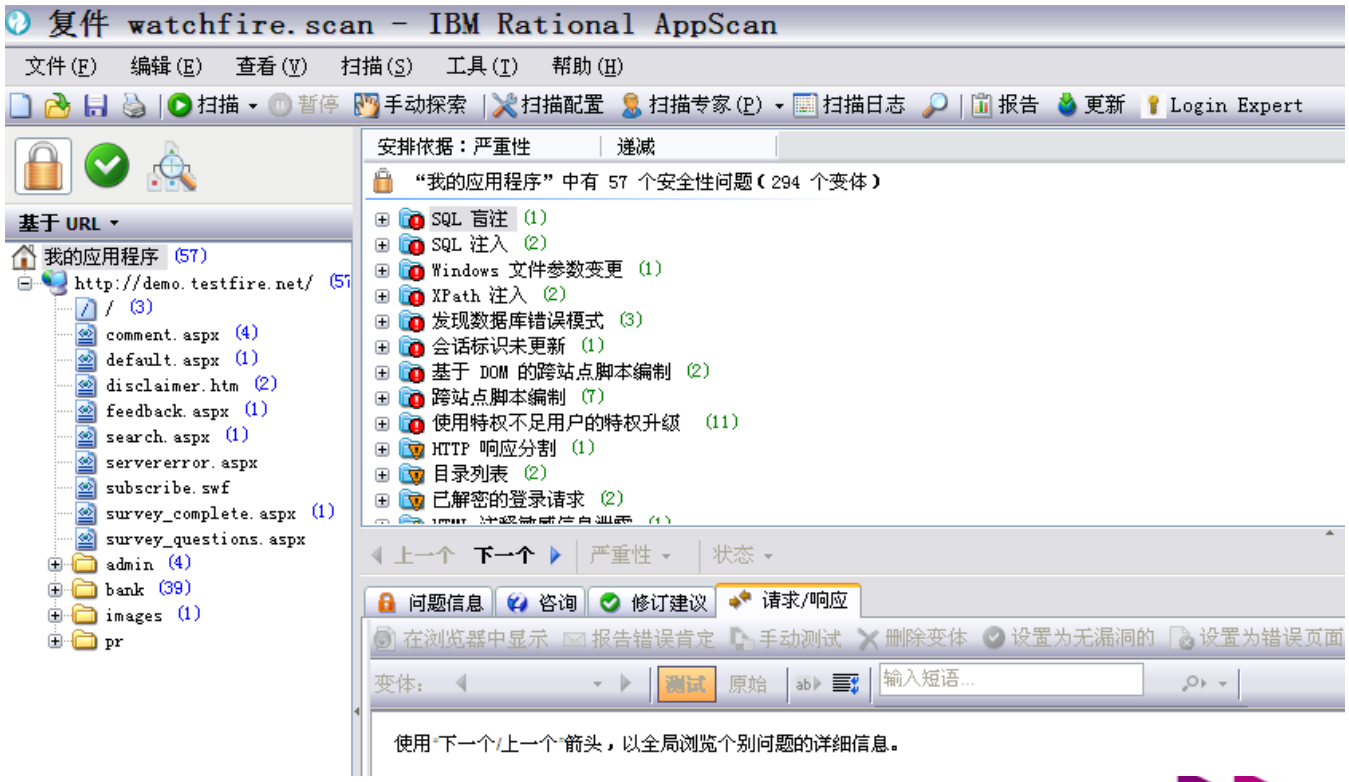
Security Requirements

Configure
Scan
Triage

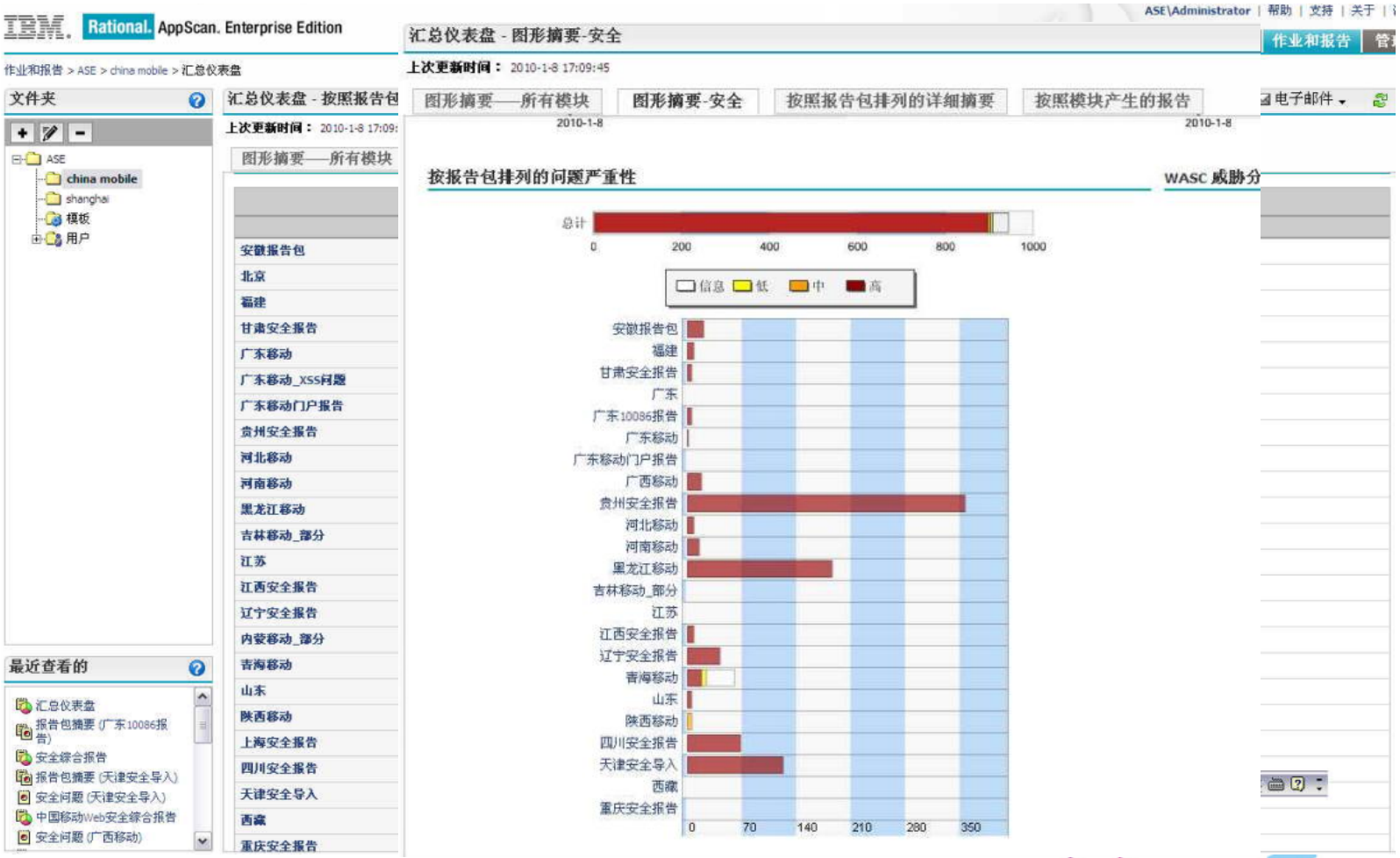
Rational AppScan:
-Standard Ed
-Source Ed for Security

安全审计

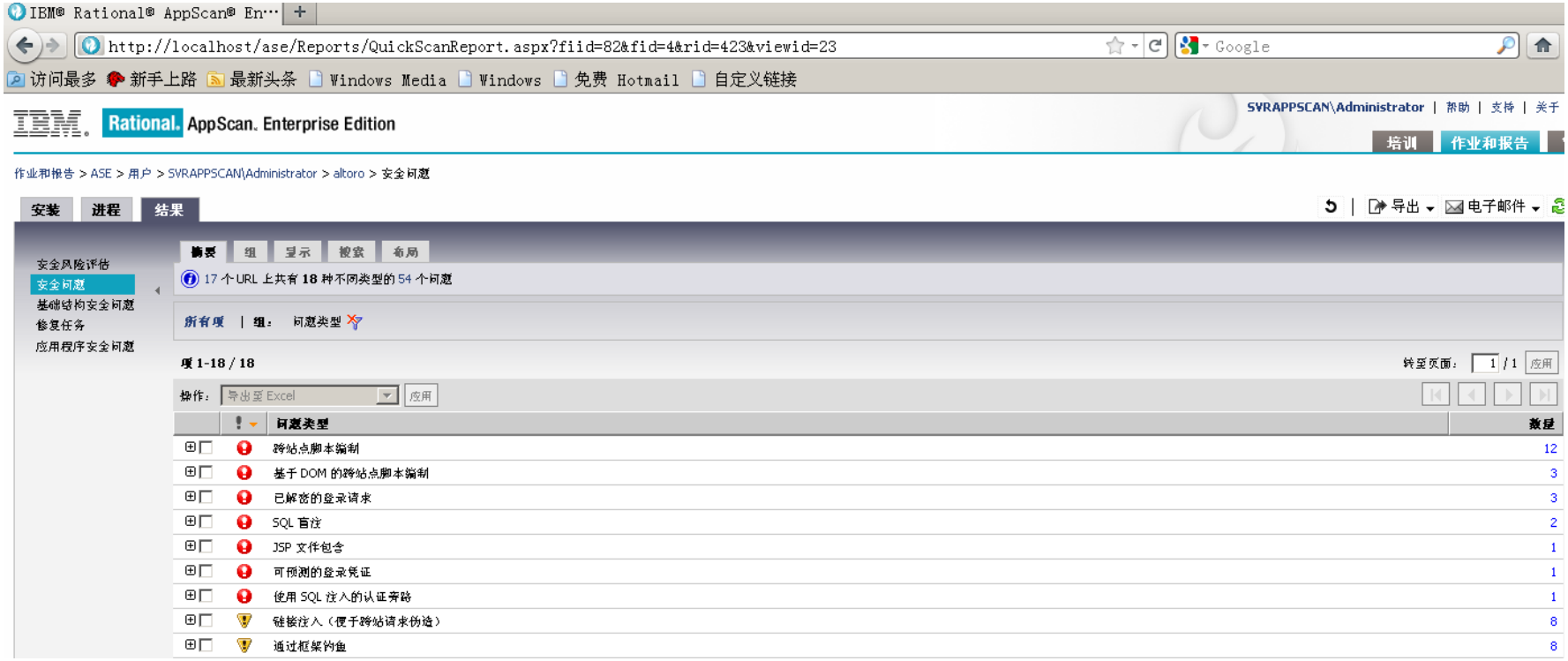
对部署环境: AppScan 标准版对WEB网站的安全扫描：



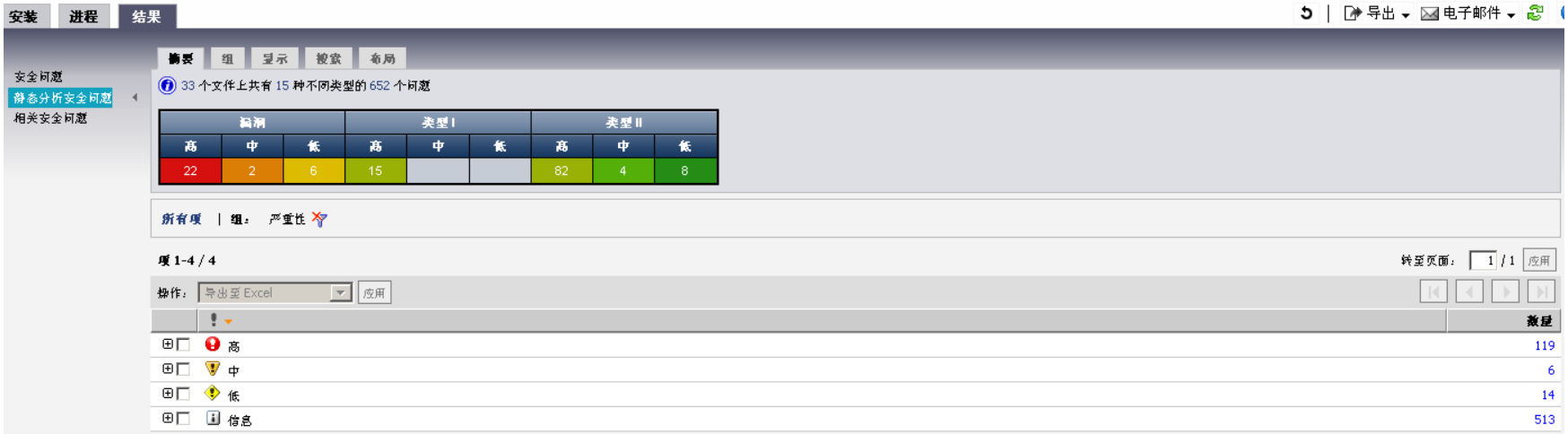
报告的集中展现（WEB上）



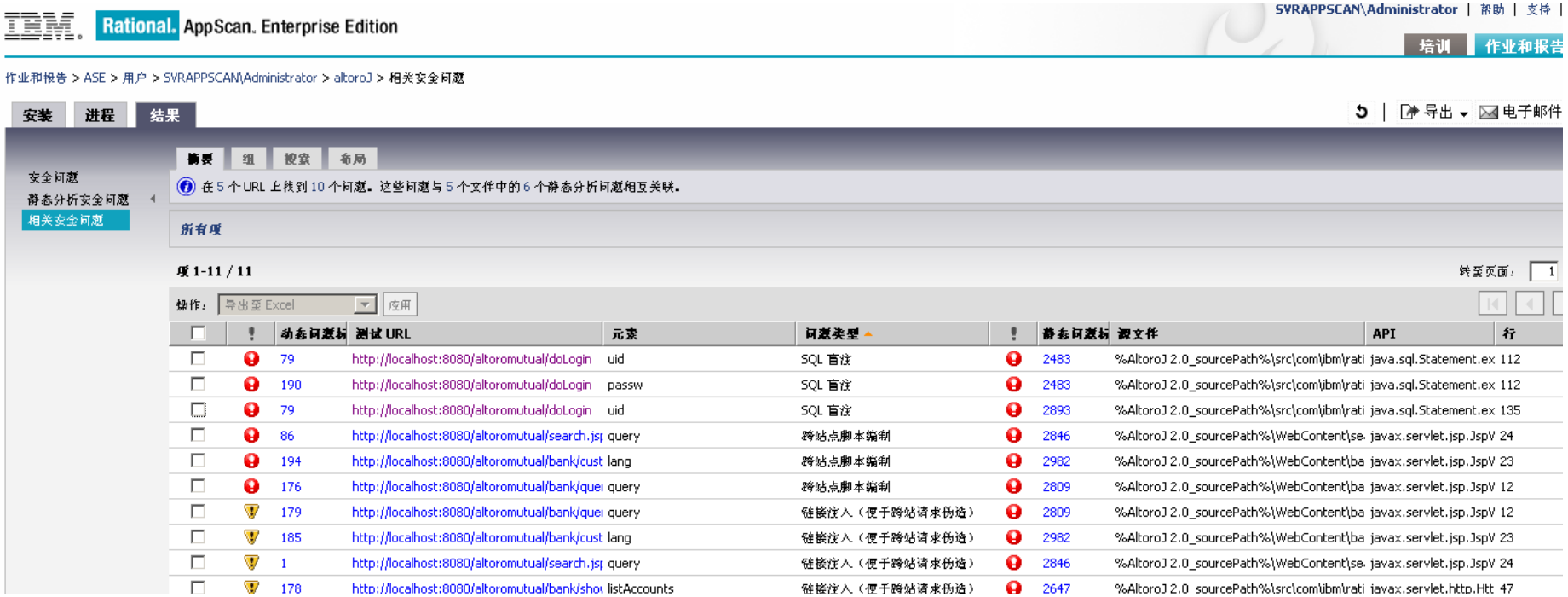
黑盒安全报告：应用级别


IBM® Rational® AppScan® En…
http://localhost/ase/Reports/QuickScanReport.aspx?fiid=82&fid=4&rid=423&viewid=23
Google
访问最多 新手上路 最新头条 Windows Media Windows 免费 Hotmail 自定义链接
IBM Rational. AppScan. Enterprise Edition
SVRAPPSCAN\Administrator | 帮助 | 支持 | 关于
培训 作业和报告
作业和报告 > ASE > 用户 > SVRAPPSCAN\Administrator > altoro > 安全问题
安装 进程 结果
导出 电子邮件
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 被套 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
转至页面： 1 / 1 应用
操作： 导出至 Excel 应用
问题类型 数量
跨站点脚本编制 12
基于 DOM 的跨站点脚本编制 3
已解密的登录请求 3
SQL 盲注 2
JSP 文件包含 1
可预测的登录凭证 1
使用 SQL 注入的认证旁路 1
链接注入（便于跨站请求伪造） 8
通过框架钓鱼 8

白盒安全报告-代码级别

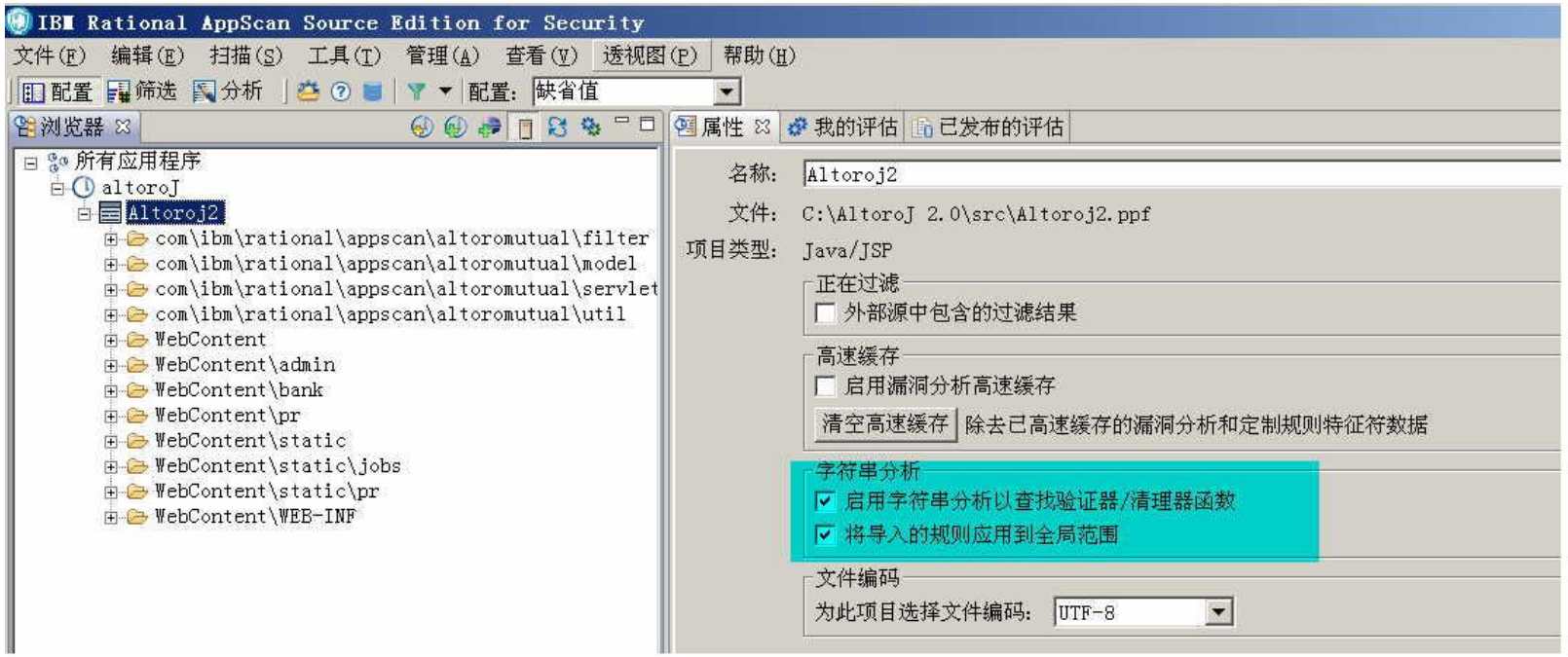

安装
进程
结果
导出
电子邮件
摘要
组
显示
搜索
布局
安全问题
静态分析安全问题
相关安全问题
33 个文件上共有 15 种不同类型的 652 个问题
漏洞
类型 I
类型 II
高
中
低
22
2
6
15
82
4
8
所有项 | 组： 严重性
项 1-4 / 4
转至页面：
1 / 1
应用
操作：
导出至 Excel
数量
高 119
中 6
低 14
信息 513

黑盒白盒关联的报告分析



动态问题标	测试 URL	元素	问题类型	静态问题标	源文件	API	行
79	http://localhost:8080/altoromutual/doLogin	uid	SQL 盲注	2483	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati	java.sql.Statement.ex	112
190	http://localhost:8080/altoromutual/doLogin	passw	SQL 盲注	2483	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati	java.sql.Statement.ex	112
79	http://localhost:8080/altoromutual/doLogin	uid	SQL 盲注	2893	%AltoroJ 2.0_sourcePath%\src\com\ibm\rati	java.sql.Statement.ex	135
86	http://localhost:8080/altoromutual/search.jsp	query	跨站点脚本编制	2846	%AltoroJ 2.0_sourcePath%\WebContent\se	javax.servlet.jsp.JspV	24
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
176	http://localhost:8080/altoromutual/bank/que	query	跨站点脚本编制	2809	%AltoroJ 2.0_sourcePath%\WebContent\ba	javax.servlet.jsp.JspV	12
179	http://localhost:8080/altoromutual/bank/que	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
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
1	http://localhost:8080/altoromutual/search.jsp	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
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:

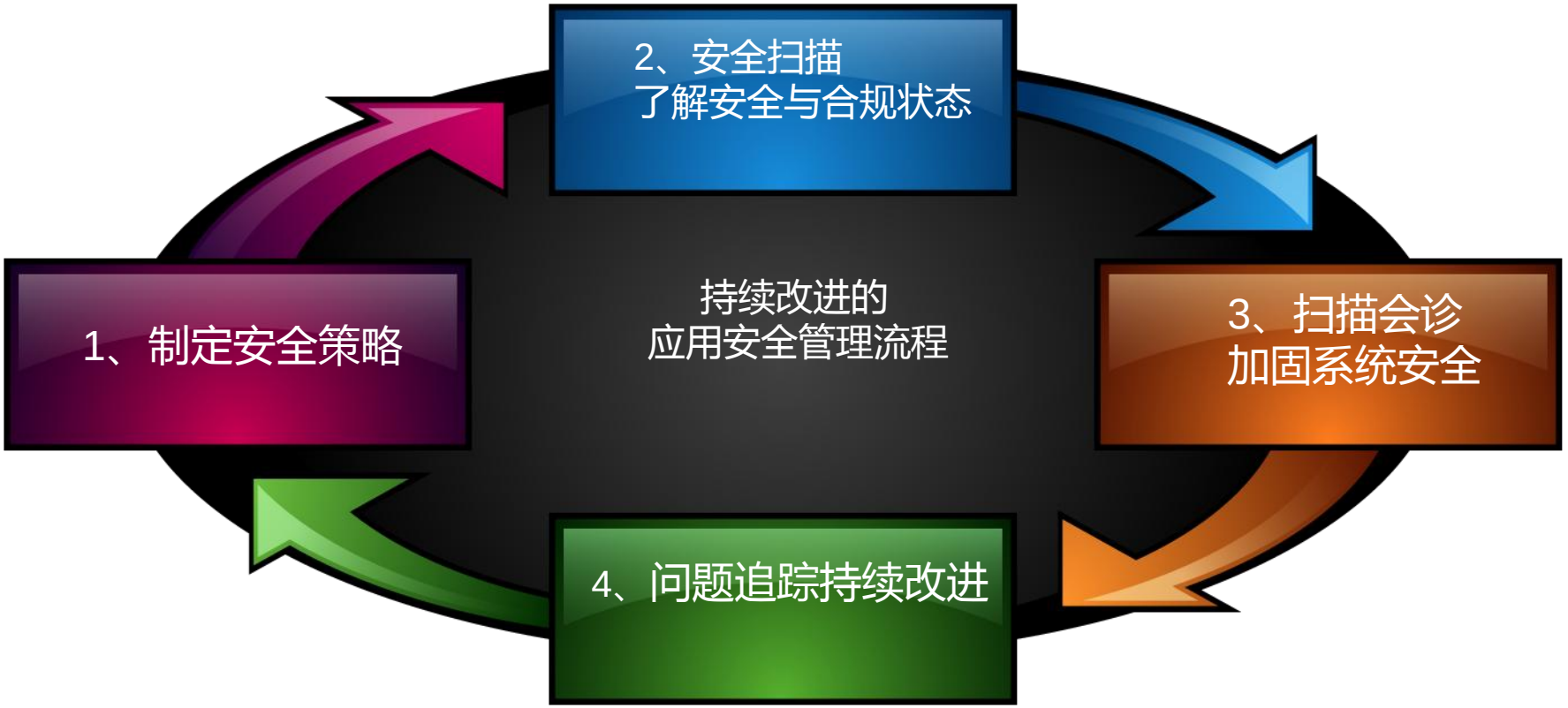
```
21 :   var iPos = document.URL.indexOf("url=")+4;

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方法》
- 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账户
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—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

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

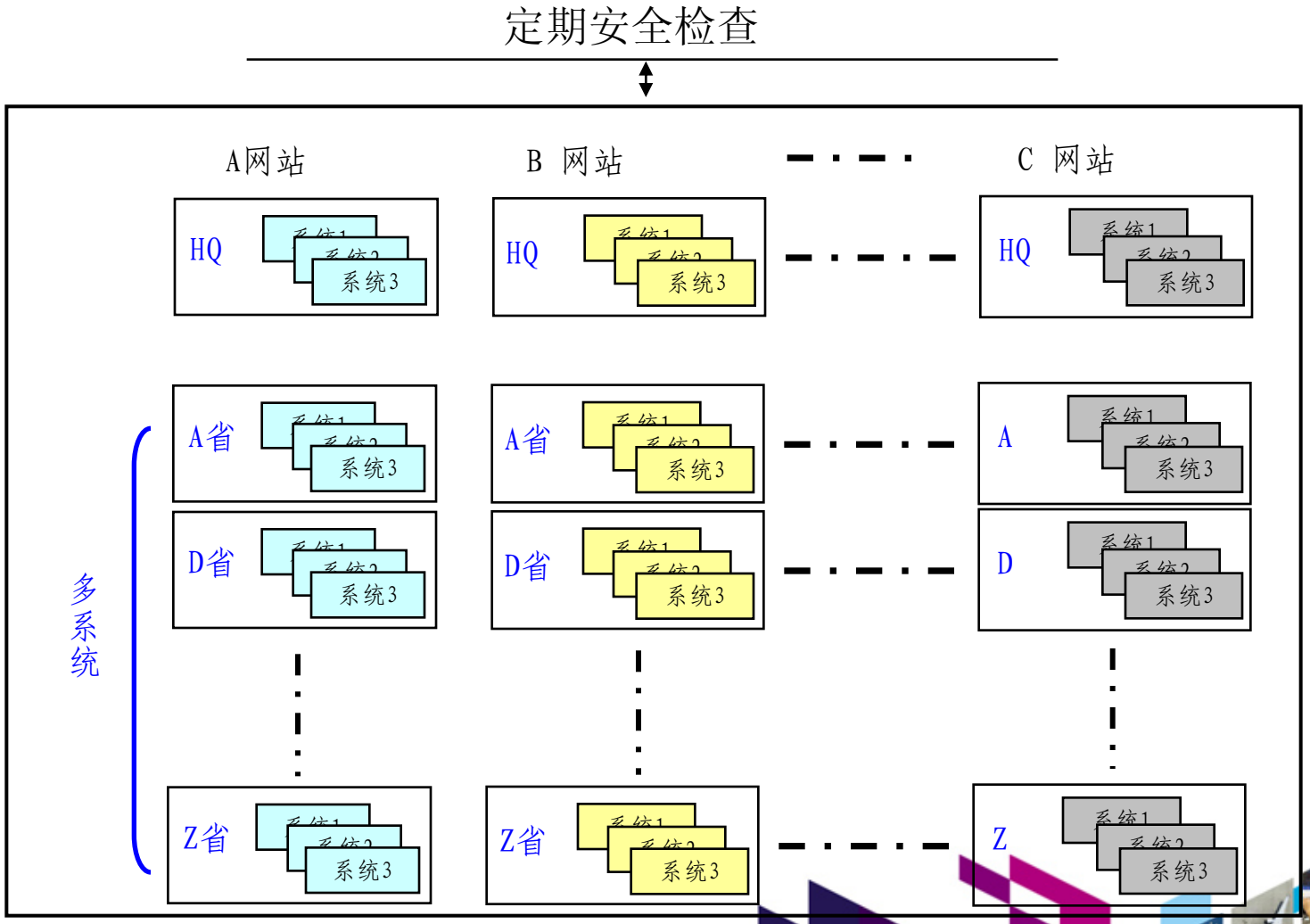
应用安全现状及需求分析

- 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

- 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，关于应用安全评估的比重非常小。

内部安全月报、内审和企业外部的SOX安全合规审计

选择核心系统进行安全评估



了解信息系统的安全与合规现状

- 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

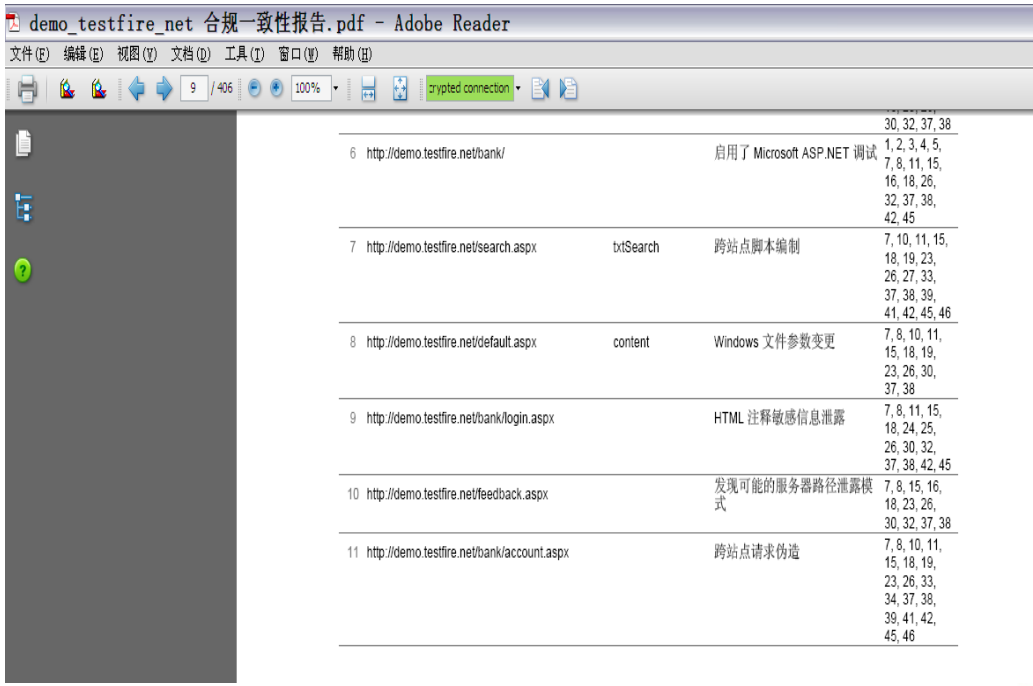
了解信息系统的安全与合规现状

- 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



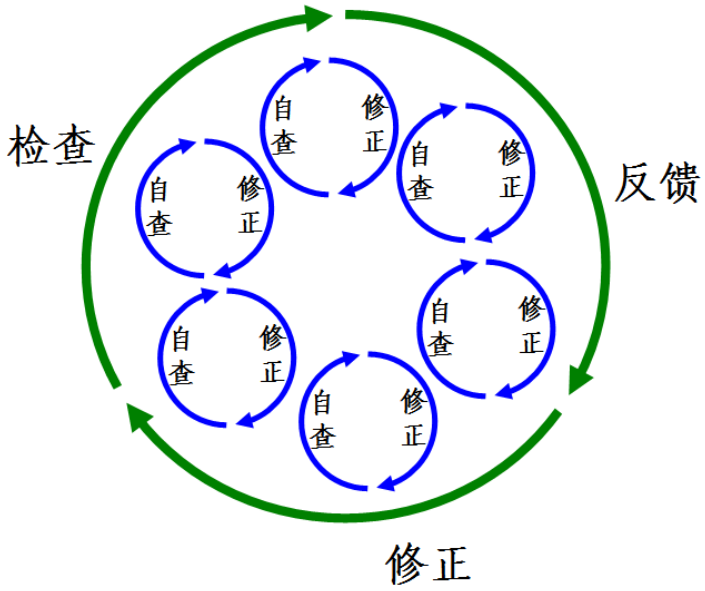
				30, 32, 37, 38
6	http://demo.testfire.net/bank/		启用了 Microsoft ASP.NET 调试	1, 2, 3, 4, 5, 7, 8, 11, 15, 16, 18, 26, 32, 37, 38, 42, 45
7	http://demo.testfire.net/search.aspx	txtSearch	跨站点脚本编制	7, 10, 11, 15, 18, 19, 23, 26, 27, 33, 37, 38, 39, 41, 42, 45, 46
8	http://demo.testfire.net/default.aspx	content	Windows 文件参数变更	7, 8, 10, 11, 15, 18, 19, 23, 26, 30, 37, 38
9	http://demo.testfire.net/bank/login.aspx		HTML 注释敏感信息泄露	7, 8, 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

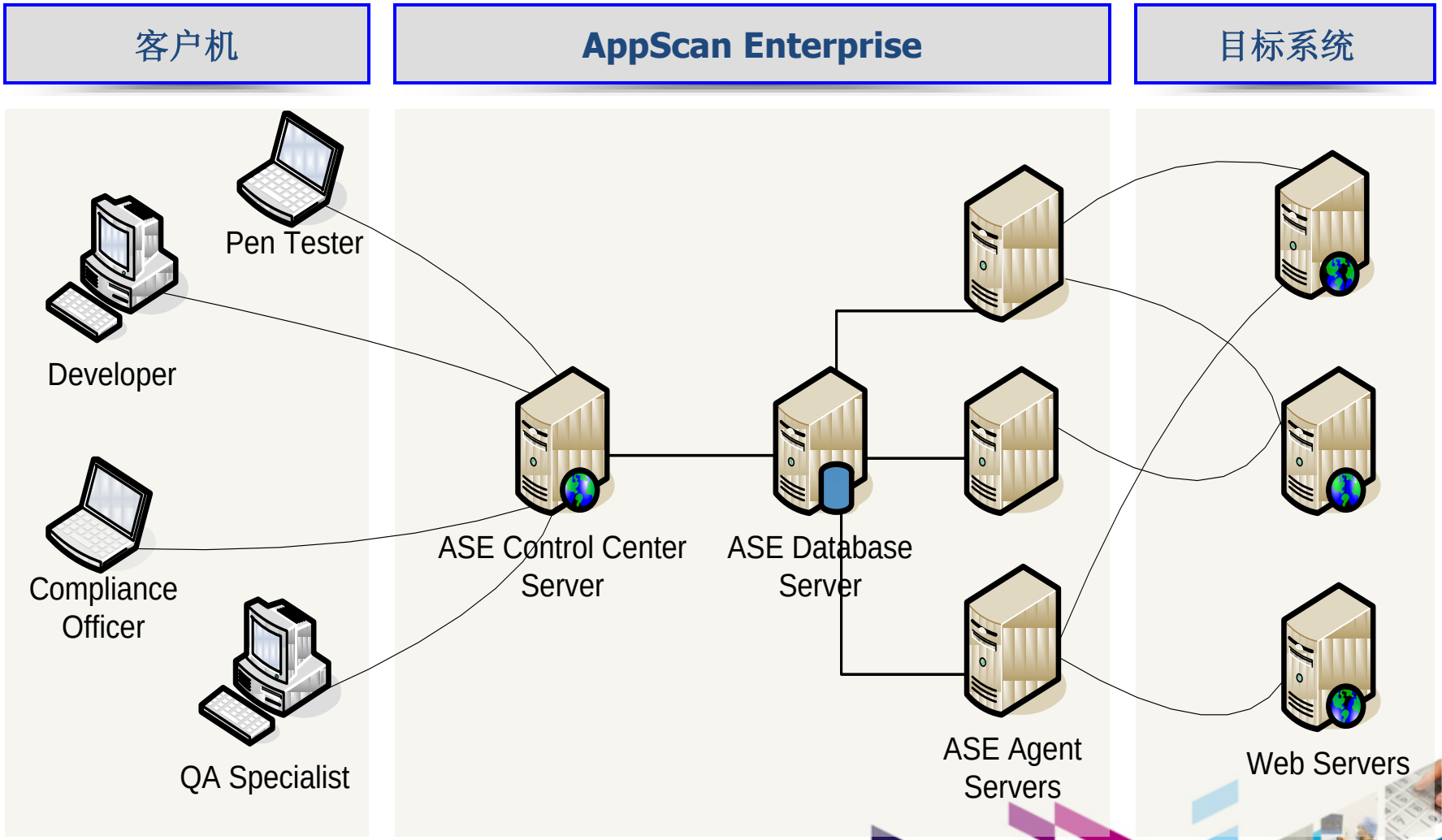
安全问题分析和确认
安全问题整改
相关人员的应用安全意识
报告汇总和分析
历史趋势分析



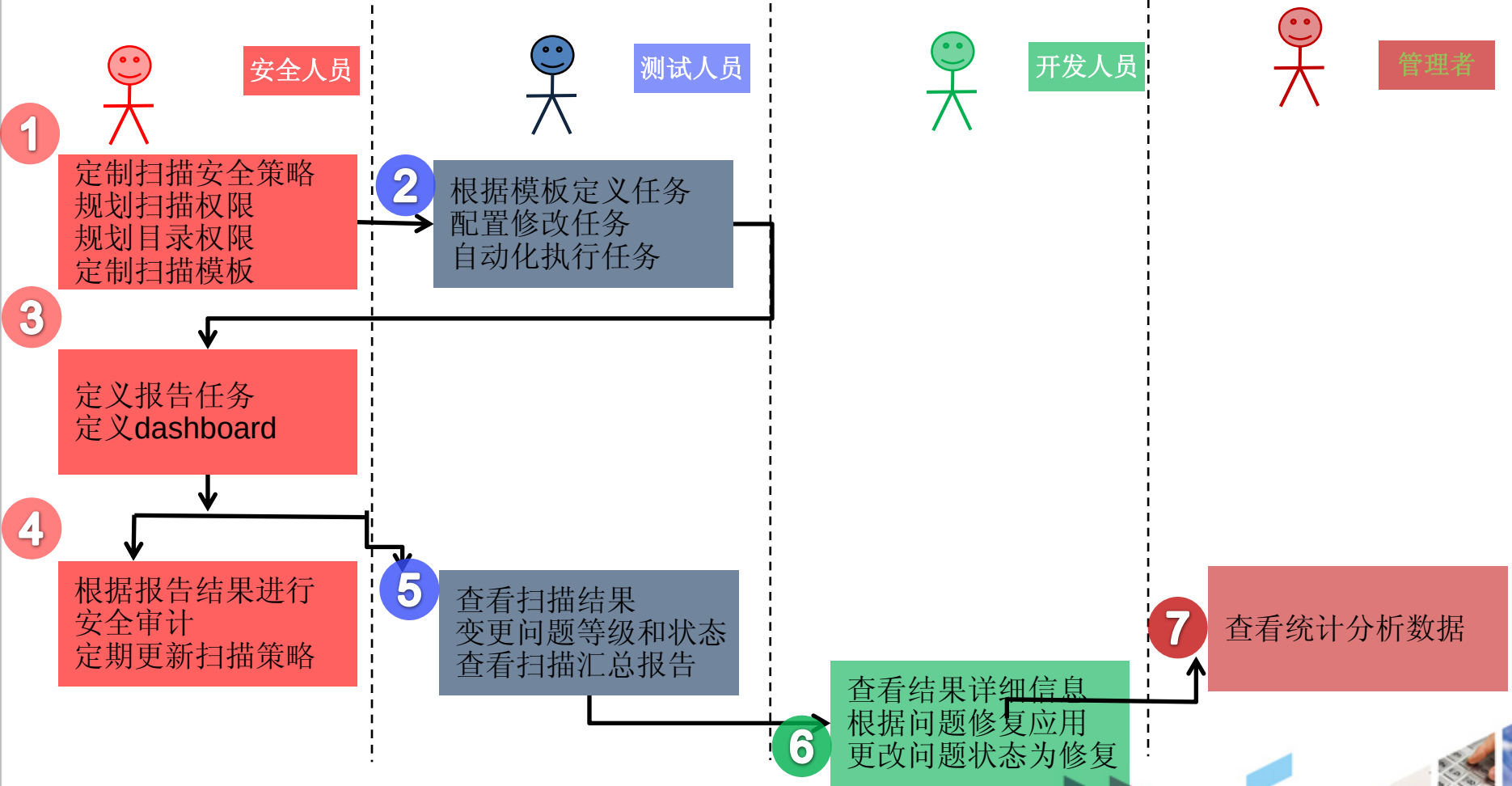
趋势分析 报告对比


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)
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
2010-1-8
按报告包排列的问题严重性
总计
0
200
400
600
800
1000
信息
低
中
高
安徽报告包
福建
甘肃安全报告
广东
广东10086报告
广东移动
广东移动门户报告
广西移动
贵州安全报告
河北移动
河南移动
黑龙江移动
吉林移动_部分
江苏
江西安全报告
辽宁安全报告
青海移动
山东
陕西移动
四川安全报告
天津安全导入
西藏
重庆安全报告
0
70
140
210
280
350
安徽报告包
北京
福建
甘肃安全报告
广东移动
广东移动_XSS问题
广东移动门户报告
贵州安全报告
河北移动
河南移动
黑龙江移动
吉林移动_部分
江苏
江西安全报告
辽宁安全报告
内蒙移动_部分
青海移动
山东
陕西移动
上海安全报告
四川安全报告
天津安全导入
西藏
重庆安全报告
ASE\Administrator | 帮助 | 支持 | 关于
培训
作业和报告
导出
电子邮件
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
关闭(C)

使用企业级AppScan



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

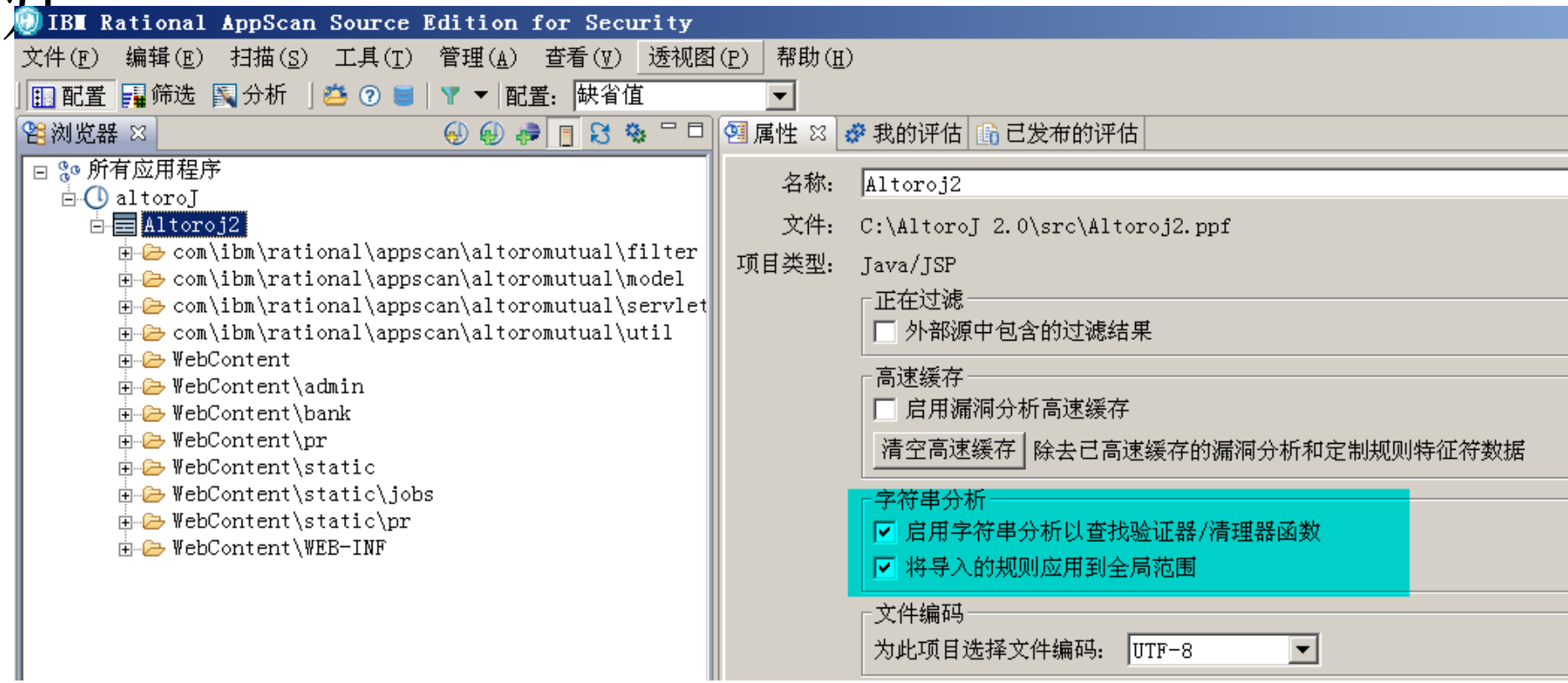
建设目标:

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



黑盒测试中的白盒测试：JavaScript 安全分析