IBM Software Group

把握软件产品的质量

IBM Rational软件验收管理解决方案

IBM 软件部　　雷勇
leiyong@cn.ibm.com

ON DEMAND BUSINESS

软件验收与测试

- 软件的交付过程实际上是软件验收的过程
- 软件是否合格必须经过验证和确认
- 软件验收以软件测试为基础
- 软件验收不但要验收软件本身，还包括相关文档

议程

- 软件项目验收
- 验收过程与验收要点
- 软件测试
- IBM Rational测试解决方案

软件项目验收的重要目的

- 目的：
  - 验证项目所交付的结果符合需求规格
  - 确认项目所交付的结果在目标的工作环境中能够满足使用的要求
  - 建立起对与所获取的结果进行后续的支持和维护的基础
  - 项目结束

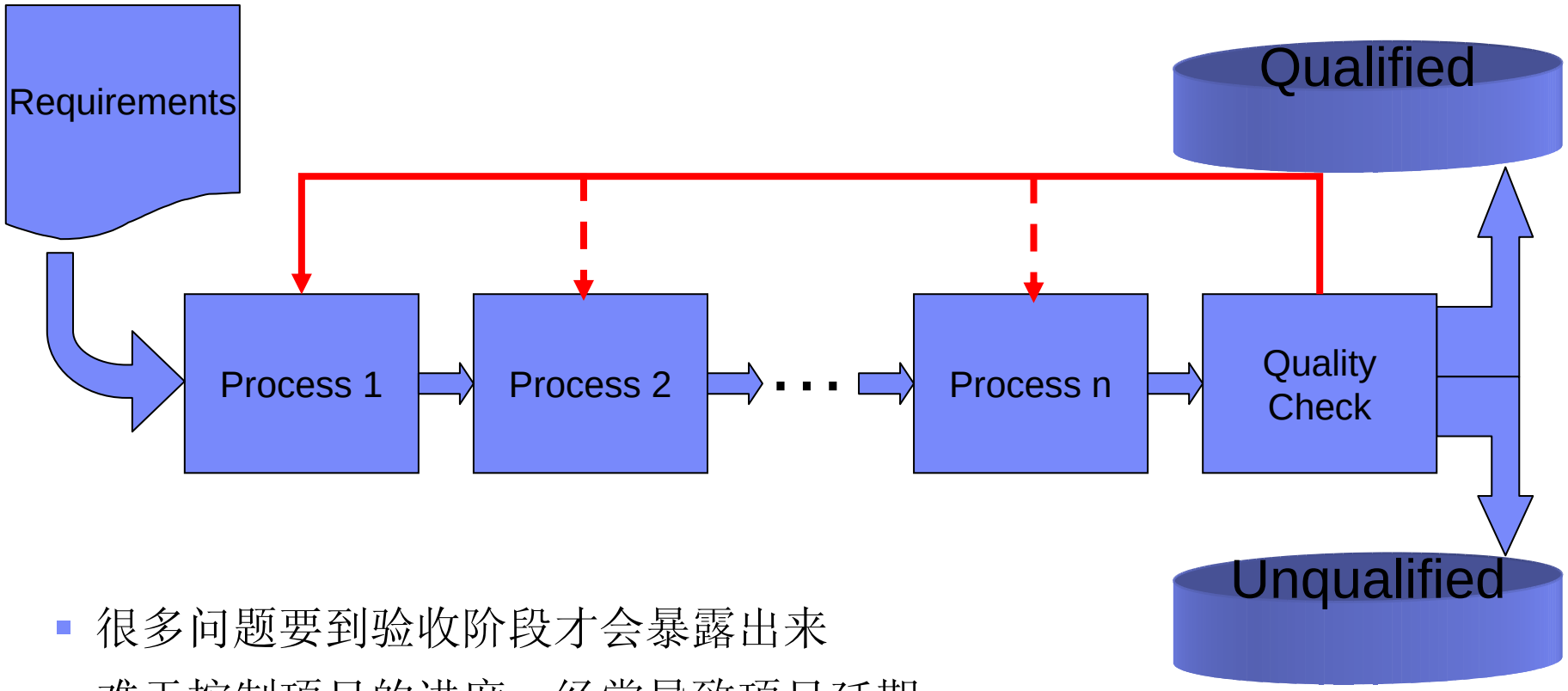
常见问题及其原因

	常见问题	原因
1	系统无法彻底验收，只能将交付物归档	“交钥匙工程”
2	验收的系统还存在质量问题	缺乏需求的掌控，验收进行得不彻底
3	验收的系统后续维护困难	交付物不够完整或存在质量问题，文挡质量问题
4	验收占掉大量时间	缺乏自动化的工具支持，无法进行高效的回归测试

两种质量验收模型

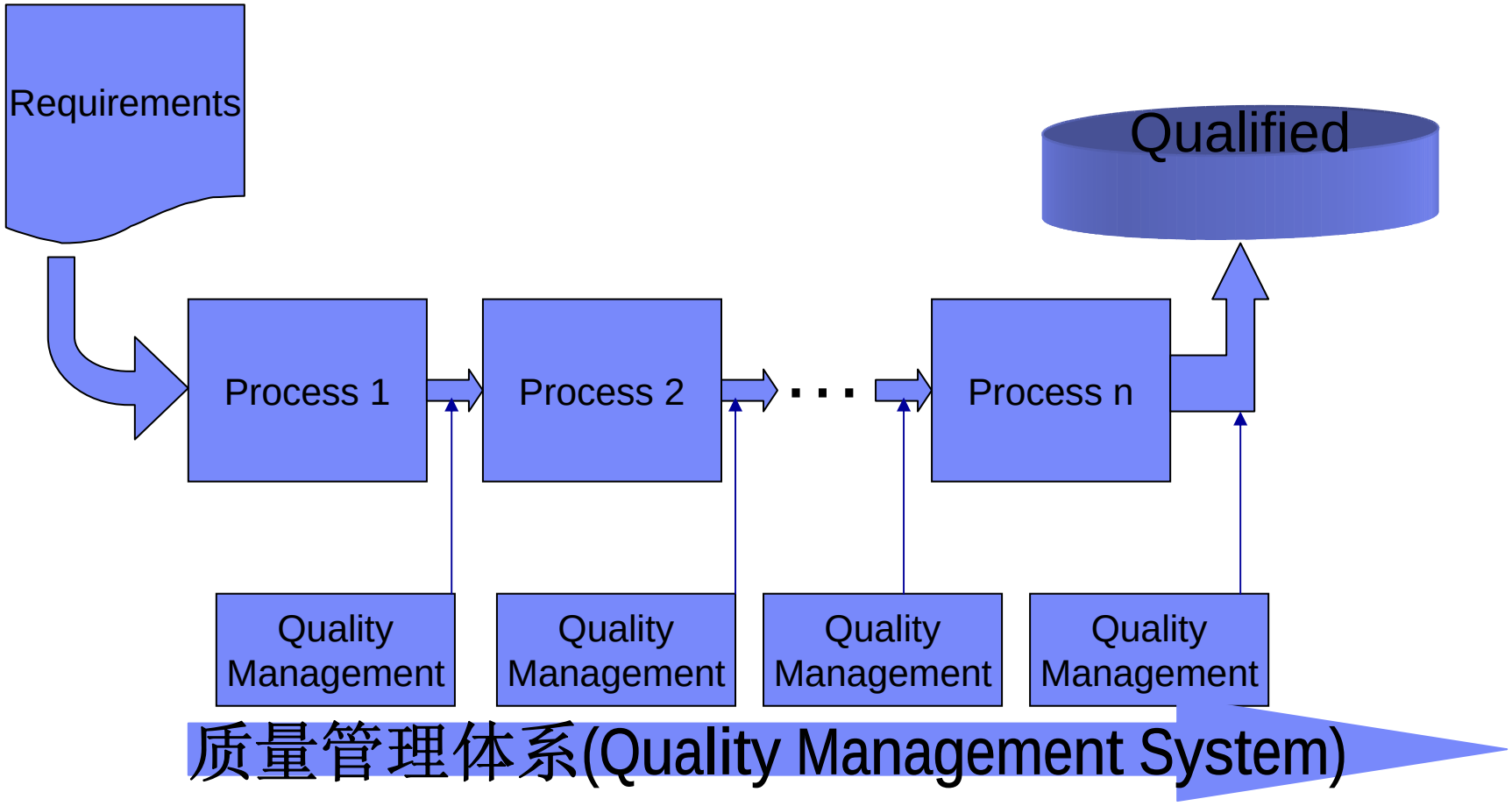
- 事后检验
- 分阶段验收

事后检验



- 很多问题要到验收阶段才会暴露出来
- 难于控制项目的进度，经常导致项目延期
- 开发过程不透明，很难监控开发的进展情况
- 事后验证发现的问题往往难于改正，会花费大量的精力，极端情况导致项目失败

全面质量管理(*Total Quality Management*)



- 变一次验收为多次检验
- 在每个里程碑处设立检验点

质量管理方式

- 事后检验
  - 在软件项目中错误的质量管理方式
- TQM（全面质量管理）——SEI CMM
  - 软件过程改进，通过改进软件过程能力成熟度来提高过程有效性的控制能力
- 质量认证——ISO9001
  - 高级的质量管理方式，已经在工业方面得到有效应用，在软件产业应用不好，什么原因？

议程

- 软件项目验收
- 验收过程与验收要点
- 软件测试
- IBM Rational测试解决方案

验收的两个方面

- 验证(Verification)
  - 评估系统在功能上是否和需求定义相一致
  - 检验系统在技术上是否达到一定质量标准(可靠性、性能等)
- 确认(Validation)
  - 评估系统是否真正满足了生产环境和业务运作的需要
  - 需要业务部门的参与
  - 需要将系统部署到实际生产环境中去进行检验

IBM Rational的软件质量维度定义

软件质量的5个维度

验收的原则

- 质量标准应该是可验证的
- 尽量采用一些量化指标
- 验收的不仅是系统本身，还应该包括项目的所有工件

软件验收

- 功能：
  - 开发商应提交其测试计划和测试报告
  - 提交需求-测试用例覆盖率报告
  - 组织业务部门进行业务功能确认测试
- 性能：
  - 利用测试工具对系统进行压力测试
- 可靠性：
  - 开发商应提交代码覆盖率报告并达到相应的覆盖率指标
  - 利用测试工具来找出内存泄漏、系统运行不稳定方面的原因
- 易用性
  - 业务建模，疏理和优化业务流程把正确的流程变为正确并且优化灵活的流程组织相关的使用人员进行必要的评估并给出改进意见，通过变更控制委员会提交统一的变更请求
- 可支持性
  - Rational不直接提供对兼容性、是否易于安装的验收方法，建议客户就某个软件产品进行多平台的安装测试、并给出各个平台的安装指南和对应平台的版本、补丁等安装必备条件（统一交付件，建立验收标准）。

验收过程

- 审核交付件（交付的内容）
- 对交付件和所交付的产品进行验证
- 对交付结果进行确认
- 对于问题进行处理
- 项目总结和结束

验收时应该注意的事项： (1)统一交付件

- 统一所有的交付件
  - 统一交付件类型和模板及其质量标准
  - 使用统一的开发指南，统一交付件风格
- 有助于交付件的审核，提高产品质量
- 提高交付件的可理解性，增强团队沟通
- 增强系统的可维护性

验收时应该注意的事项： (2)建立验收标准

- 建立软件验收标准体系
  - 统一规定交付件集合及其质量标准
  - 建立量化质量指标，保证验收的客观性和可操作性
- 把软件质量作为项目需求的一部分
- 有效执行验收标准
  - 该质量标准是可验证的(在有限的时间和代价下)
  - 在项目开发的各检验点(里程碑)确保验收标准的执行

验收过程改进

- 需要改进整个软件获取过程
  - 定义完整的交付件体系
  - 重视过程中监控
  - 建立验收标准并且有效执行
  - 注重在过程中建立质量
- 诊断、定义、实践、评估、制度化
- CMMIAM可以作为改进软件获取过程的有效参照
- 选择IBM SDP建立软件管理平台，做到事半功倍

系统交付件(1)：验收过程中，双方关注的内容

RUP工作流	交付件	说明
业务流程	业务模型	描述系统所处的业务背景
需求	前景文档	项目开发的目标、范围及系统的主要特性
	用例模型	定义系统的功能性需求
	补充规约	定义系统的非功能性需求(如性能、可靠性等)
	词汇表	定义项目开发中所用到的专业词汇
分析	设计模型	采用UML语言记录的系统设计结果
	数据模型	采用UML语言记录的数据表结构
编码	源代码	所有的源代码文件
	单元测试报告	所有模块的单元测试报告，包括测试用例报告、代码覆盖率报告等

系统交付件(2)

RUP工作流	交付件	说明
测试	测试计划	该系统是如何被测试的
	测试报告	系统测试的结果，包括通过的测试用例数、未通过的测试用例数及相关分析
部署	安装手册	软件产品安装步骤
	发布说明	该发布版本主要增加了哪些功能、改正了哪些错误等
	用户手册	用户使用手册
	部署计划	如何将将系统部署到生产环境中去
	材料清单	所有交付件的列表
	培训教材	针对最终用户的培训教材
项目管理	项目开发计划	该系统是如何被开发的
	风险管理计划	在开发过程中是如何管理风险的
	迭代计划	每一个迭代的详细开发活动计划

议程

- 软件项目验收
- 验收过程与验收要点
- 软件测试
- IBM Rational测试解决方案

系统质量的常见问题

- 系统运行不稳定，发生异常宕机
- 系统需要定期重启才能正常工作
- 无法支持大容量的用户访问
- 在繁忙时段系统响应时间太慢
- 不能完全满足业务需求
- 客户在系统部署前对系统质量缺乏信心
- 系统无法快速响应业务需求的变化
- 对软件产品的安全性缺乏信心

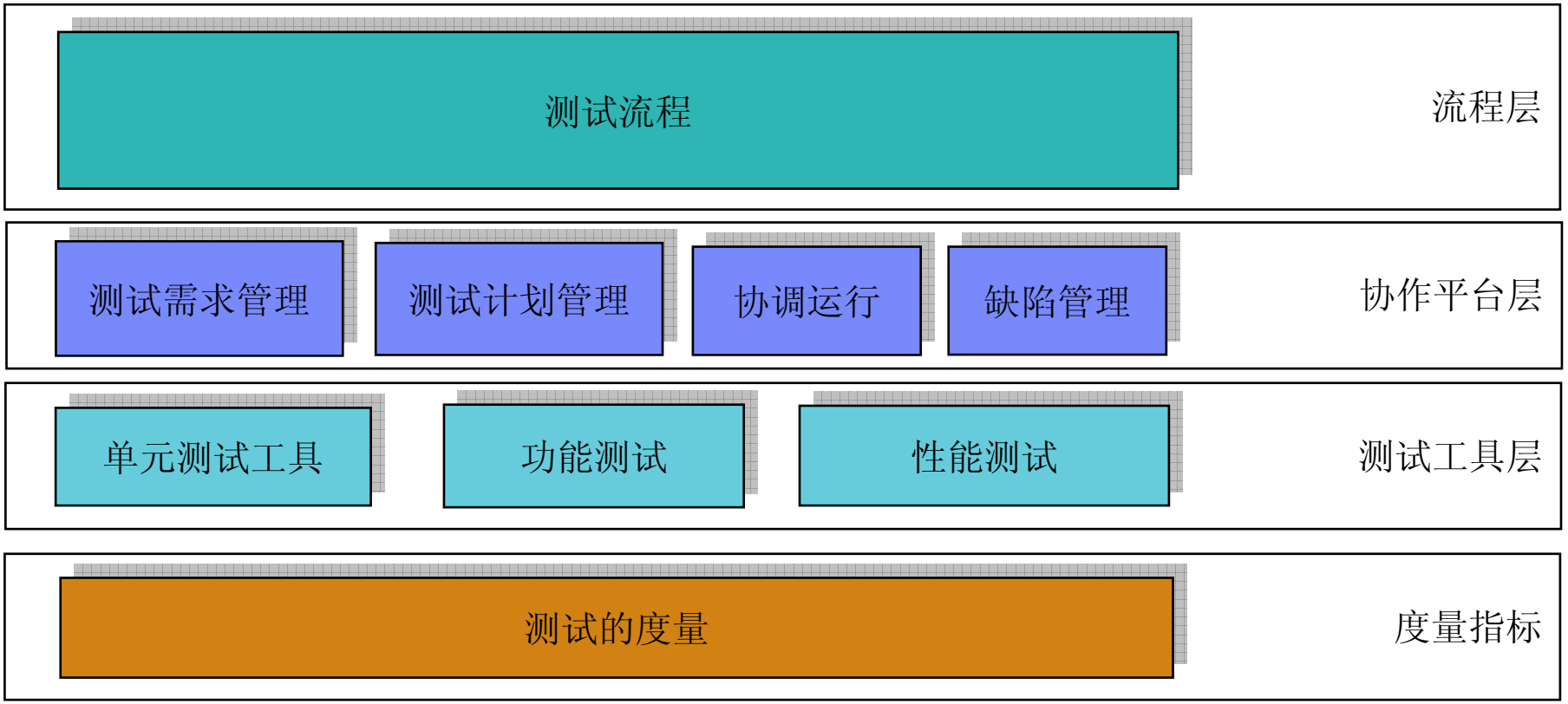
质量问题、原因及解决方法

问题	原因	IBM SDP解决方案
系统不稳定	系统的可靠性不高	PurifyPlus
需要定期重启	系统存在内存泄漏	PurifyPlus
无法支持大容量用户	系统的性能没有达到设计指标	压力测试解决方案
响应速度慢		
无法满足业务需求	对客户的业务需求理解不充分	需求管理解决方案
对质量缺乏信心	缺乏一些客观的指标来帮助判断系统质量	测试管理解决方案
无法响应业务需要	系统难于扩充、维护	可视化建模技术
对Web应用的安全性缺乏信心	Web应用在设计上缺乏安全性考虑，容易收到SQL注入等攻击	Web安全解决方案Watchfire

质量问题、原因及解决方法

问题	原因	IBM SDP解决方案
系统不稳定	系统的可靠性不高	PurifyPlus
需要定期重启	系统存在内存泄漏	PurifyPlus
无法支持大容量用户	系统的性能没有达到设计指标	压力测试解决方案
响应速度慢		
无法满足业务需求	对客户的业务需求理解不充分	需求管理解决方案
对质量缺乏信心	缺乏一些客观的指标来帮助判断系统质量	测试管理解决方案
无法响应业务需要	系统难于扩充、维护	可视化建模技术
对Web应用的安全性缺乏信心	Web应用在设计上缺乏安全性考虑，容易收到SQL注入等攻击	Web安全解决方案Watchfire

软件测试的体系结构


测试流程
流程层
测试需求管理
测试计划管理
协调运行
缺陷管理
协作平台层
单元测试工具
功能测试
性能测试
测试工具层
测试的度量
度量指标

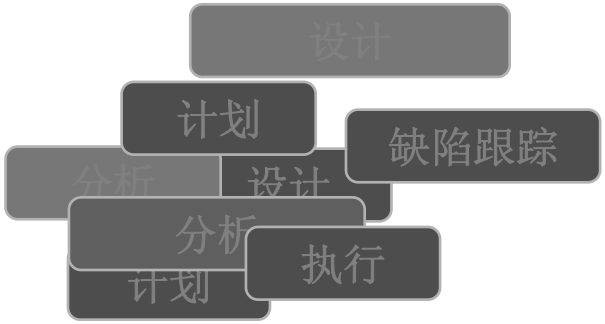
IBM Rational软件测试的理念

- 软件测试的目的
  - 确认软件的质量
  - 提供有效的信息
  - 保证高质量的软件开发流程
- 软件测试的原则
  - 尽可能的发现软件的缺陷
  - 尽可能的降低软件开发的风险
- 软件测试策略
  - 尽早和持续的测试：测试越早越好,覆盖越广越好
  - 自动化测试：测试要经常回归迭代进行
  - 完善测试流程：包含测试案例,测试调度和缺陷修复

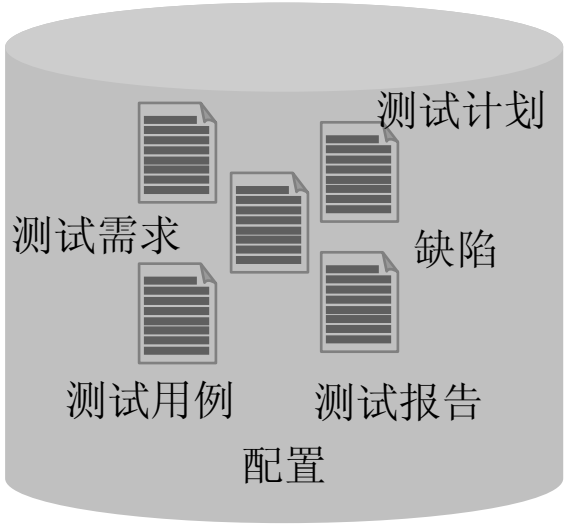
软件测试的三大要素

测试人员

测试活动



测试资产



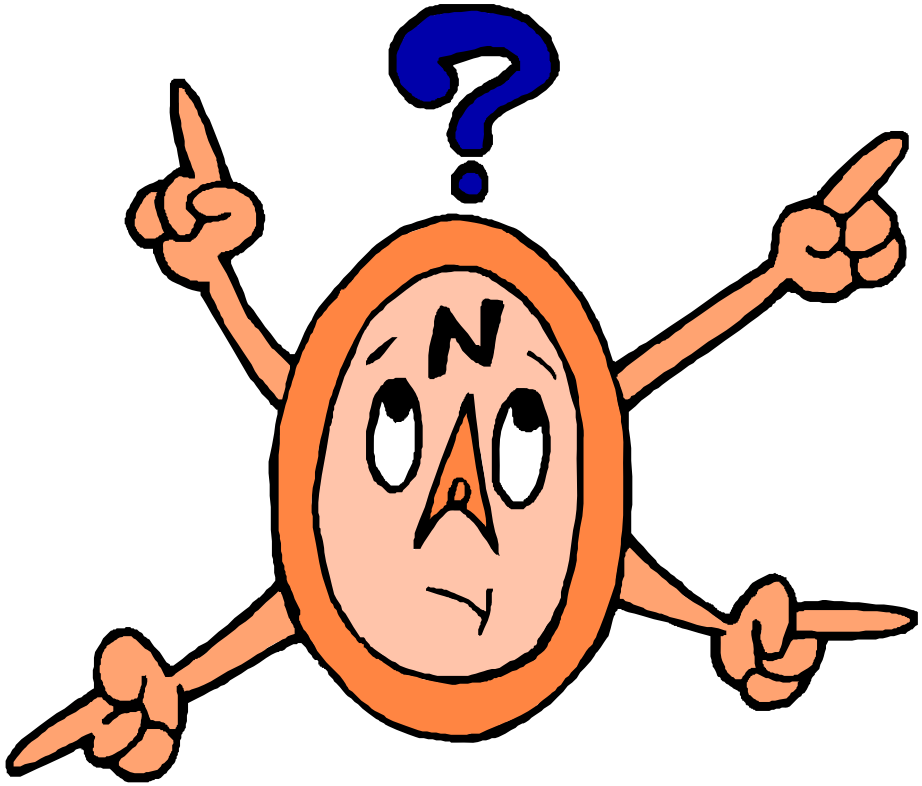
成功的软件测试项目必须要有效的管理相关人员，活动和资产。

测试的分类

- 按测试的不同角度划分
  - 功能测试
  - 易用性测试
  - 可靠性测试
  - 性能测试
  - 可支持性测试
- 按照测试对象划分
  - 软件程序测试
  - 文档测试
- 按照测试方法分类
  - 手工测试
  - 自动化测试
- 测试的阶段划分
  - 单元测试
  - 集成测试
  - 系统测试
  - 用户验收测试
- 测试的技术分类
  - 白盒测试
  - 黑盒测试

软件测试的现状

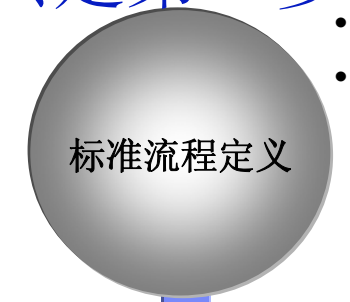
- 流程级别
  - 建立了基本的测试流程(流程已定义)
  - 新人进来培训成本大
  - 在实际过程中无法贯彻落实
- 协作平台层
  - 采用不同的工具管理协作,引入了一套测试管理平台的工具
  - 只涉及到测试中的过程,对于其他的流程无法集成
- 测试工具层
  - 引入了多种测试工具
  - 单元测试无法自动化
  - 自动化功能测试难以实现
- 度量层
  - 缺乏有效的度量指标



路在何方?

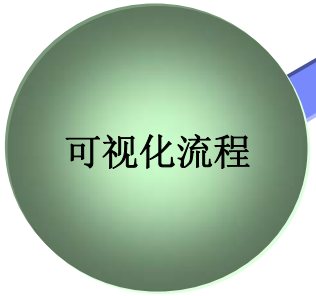
流程层:流程的定义只是第一步

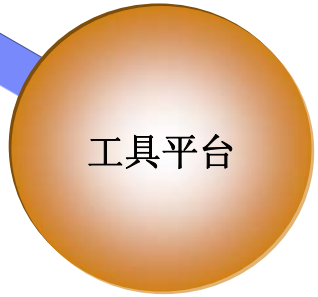
- 依据《企业标准流程定义》
- 符合《国际标准》

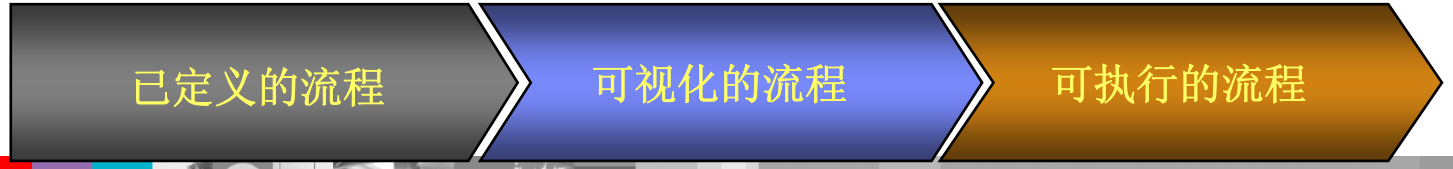


- 准确无误地、形象地表达管理标准；
- 提供操作作业指南；
- 使用者可以方便、灵活的访问；

- 完整的支持流程的要求
- 辅助流程推行过程

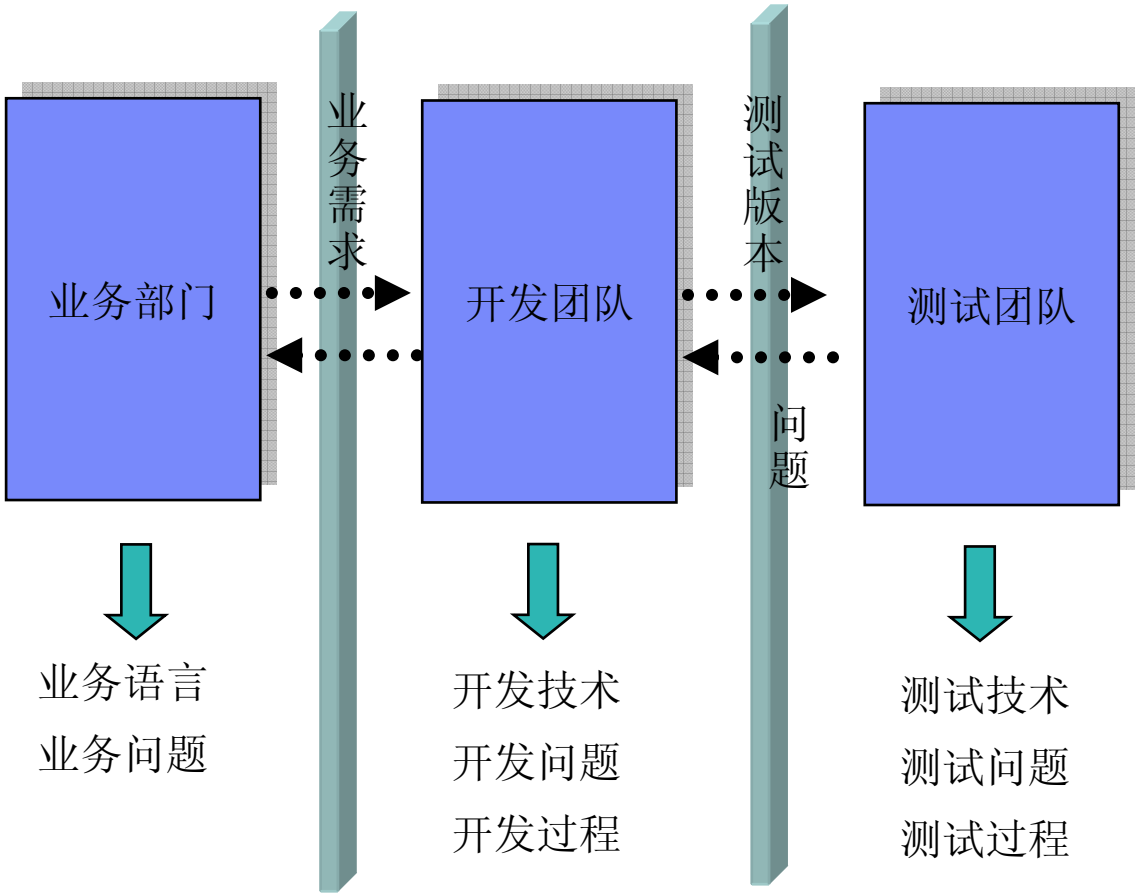






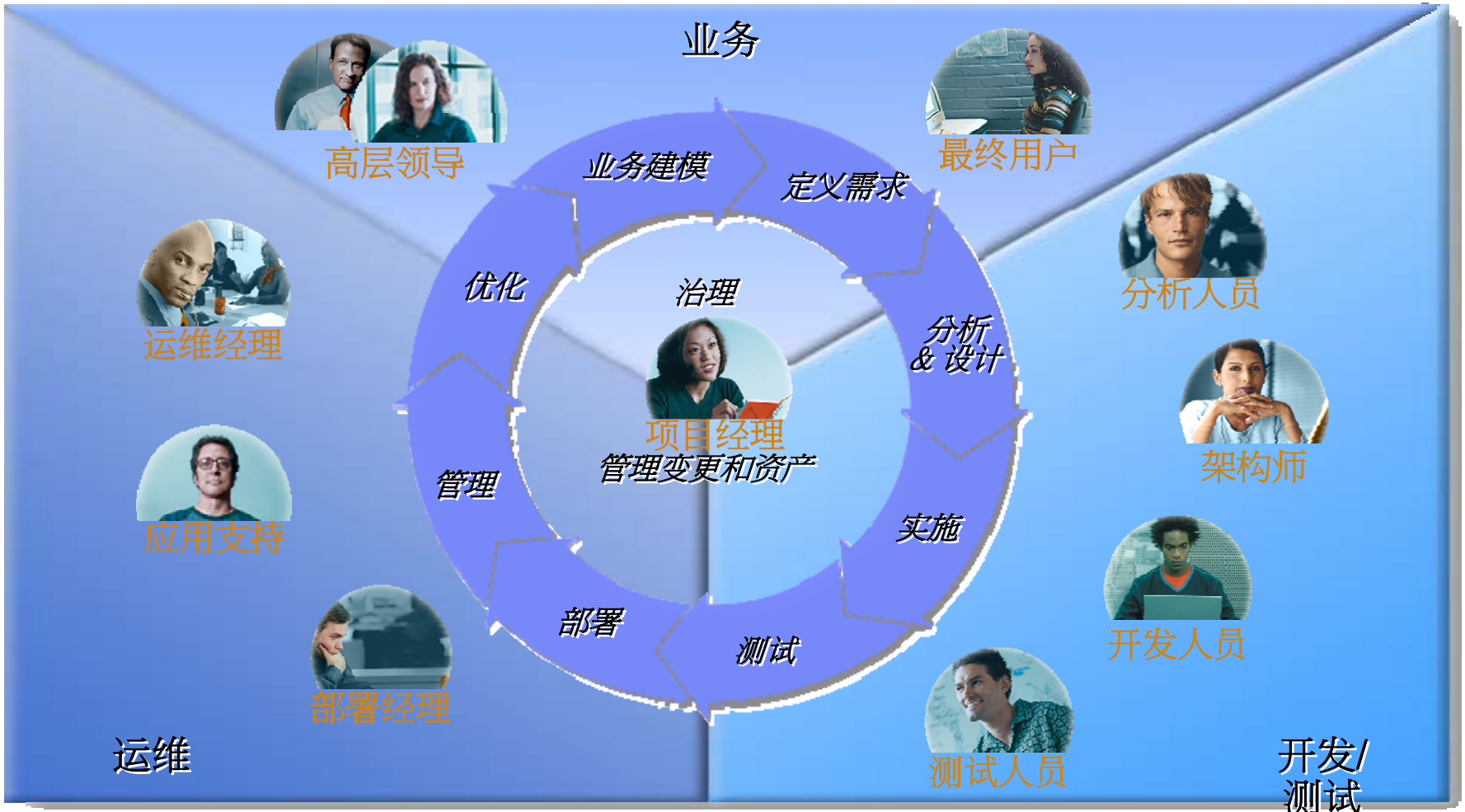
协作平台层:只管理测试过程是不够的

- 开发现状:竖井结构(每个部门都有自己的管理过程和方法)



协作平台层:打破竖井,贯穿不同部门

确定业务优先级　　规划　　管理　　度量



优化　　迭代

测试工具层

- 利用自动化测试工具来支持测试流程

  性能测试解决方案: Rational Performance Tester, Robot

  功能测试解决方案：Rational Functional Tester，Robot

  白盒测试解决方案：Rational PurifyPlus

  实时系统、嵌入式测试解决方案：Rational Test Realtime

  手工测试解决方案：Rational Manual Tester

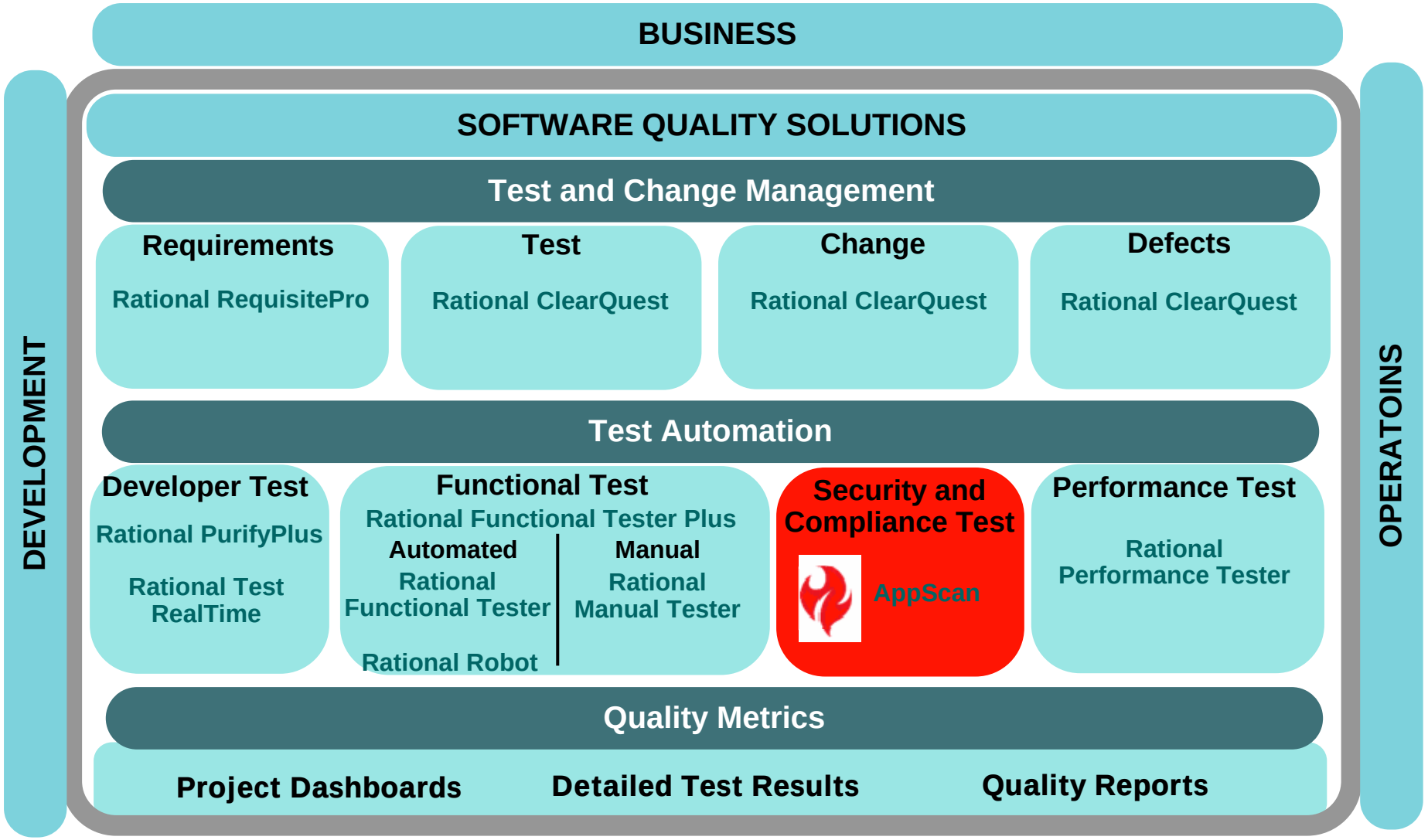
  Web应用安全性测试解决方案：Watchfire

  测试管理平台：Rational TestManager，Rational CQTM

议程

- 软件项目验收
- 验收过程与验收要点
- 软件测试
- IBM Rational测试解决方案

Rational 软件质量解决方案



IBM Rational软件测试工具

功能	收益
▪ 运行时分析（内存、性能、代码覆盖） ▪ 代码自动评审、组件测试、系统功能测试和性能测试 ▪ 覆盖系统测试周期的测试管理和分析	▪ 确保软件的功能、性能和可靠性 ▪ 加快测试周期 ▪ 适合不同技术水平的测试人员 ▪ 全员质量观

Rational家族的新伙伴
—Web应用安全及遵从性解决方案 Watchfire

产			
IBM Rational Manual Tester		✓	✓
IBM Rational Functional Tester		✓	✓
IBM Rational Performance Tester		✓	✓
IBM Rational Robot		✓	
IBM Rational PurifyPlus		✓	✓
IBM Rational Test RealTime			✓
IBM Rational Application Developer		✓	✓

Web应用系统安全问题

- Web应用开发安全

  问题

  - 开发人员更注重软件功能的实现
  - 相对安全意识薄弱

  解决之道

  - 通过部署AppScan插件实现开发期间的安全
  - “Watchfire AppScan企业版和IBM Rational ClearQuest集成，使开发、QA和安全团队能够协同工作。把ClearCase作为一个通用的缺陷跟踪系统和Watchfire的最佳工业级的安全解决方案无缝集成”

- 测试过程安全

  问题

  - 安全评估缺乏有效的手段

  解决之道

  - 通过AppScan和软件测试平台集成实现测试期间的安全

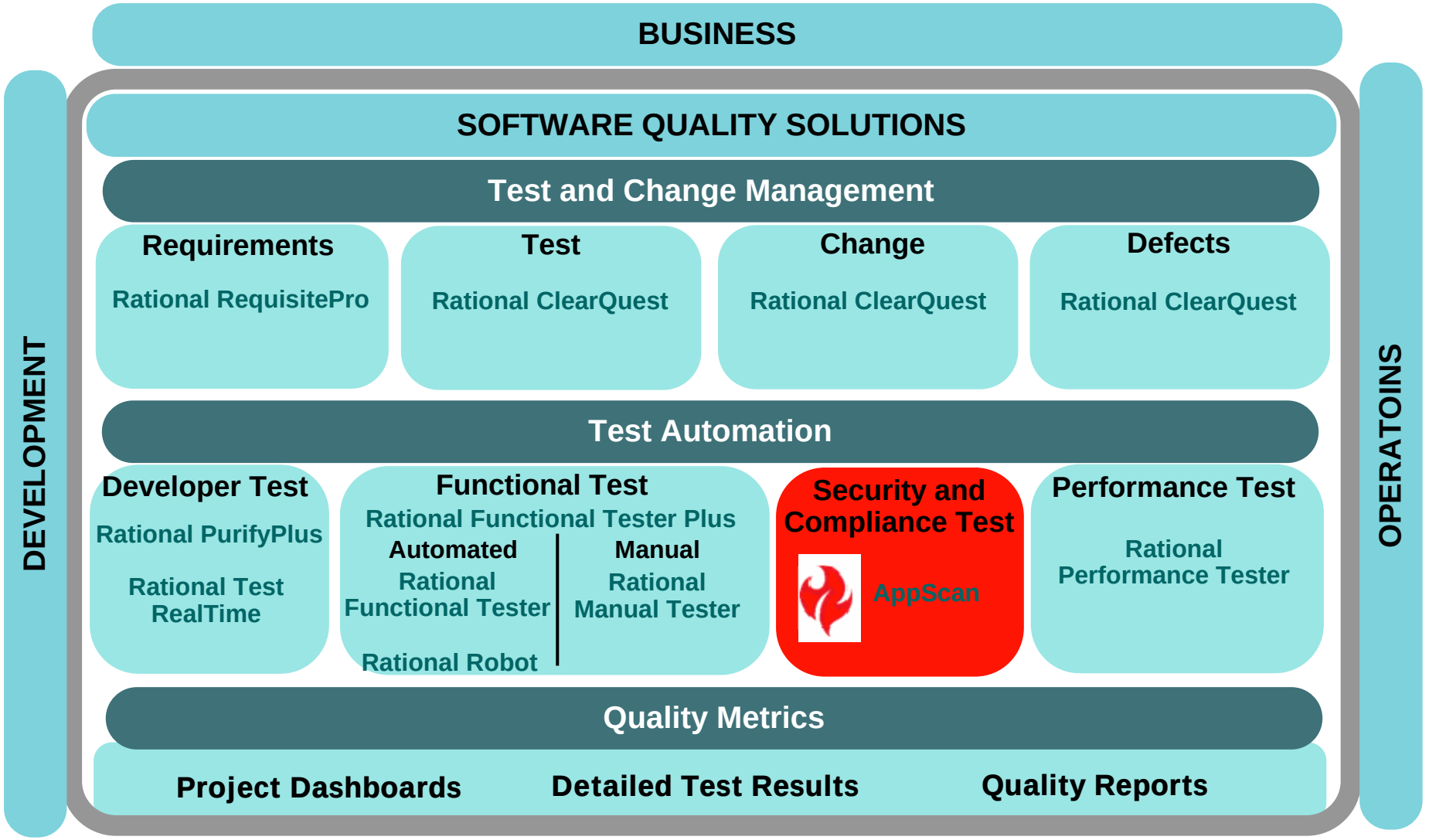
- 生产系统安全
  - 系统一旦上线运行，在对漏洞了解不清晰的时候不会轻易修改系统
  - 以前缺乏有效的手段对Web应用进行安全评估

Web应用安全技术交流

议程安排

- **WatchFire 总体概览**
- **WEB应用安全介绍及演示**
- **AppScan产品介绍及演示**

Rational 软件质量解决方案



- **Who is Watchfire?**
  - **Watchfire**是Web应用软件安全领域的领导者，是业界唯一能够提供端到端解决方案的公司，帮助用户评估、理解和解决问题
  - 产品：**AppScan**

超过800家公司信赖 Watchfire

10大银行中的9家	10大科技公司中的8家	10大医疗 / 药品公司中的7家	各大政府机关和部门
HSBC	Microsoft	Wyeth	Social Security USA Administration
JPMorganChase	Cisco Systems	Novartis	Department of Veterans Affairs
citi	intel	AstraZeneca	Department of the Navy
AIG	DELL	Abbott Laboratories	United States Postal Service
Fidelity	IBM	Aventis	
SunTrust	SONY	Roche	
Liberty Mutual	Adobe	Genentech	
Sovereign Bank	Analog Devices		

网络安全领导者也使用Watchfire来确保他们的Web应用的安全性

科技公司

顾问和调查公司

Info Security Products Guide：Hot Security Company 2006

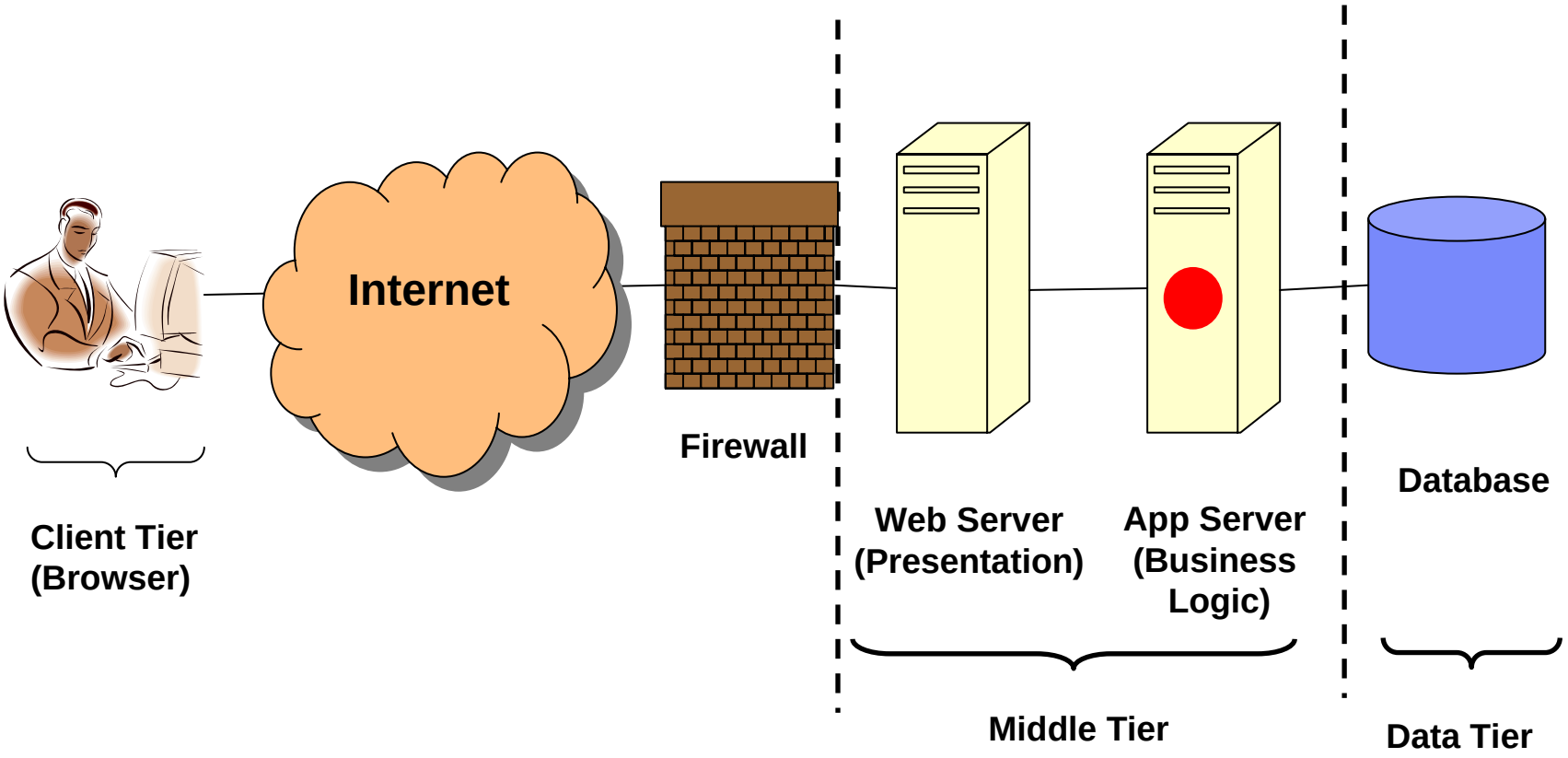
Watchfire荣获Info Security Product Guide 授予的“2006年最热门安全技术公司”称号。这一奖项的评估基于4个方面的标准，即：Products（产品），People（技术专家），Performance（市场表现） & Potential（发展潜力）。

watchfire®

议程安排

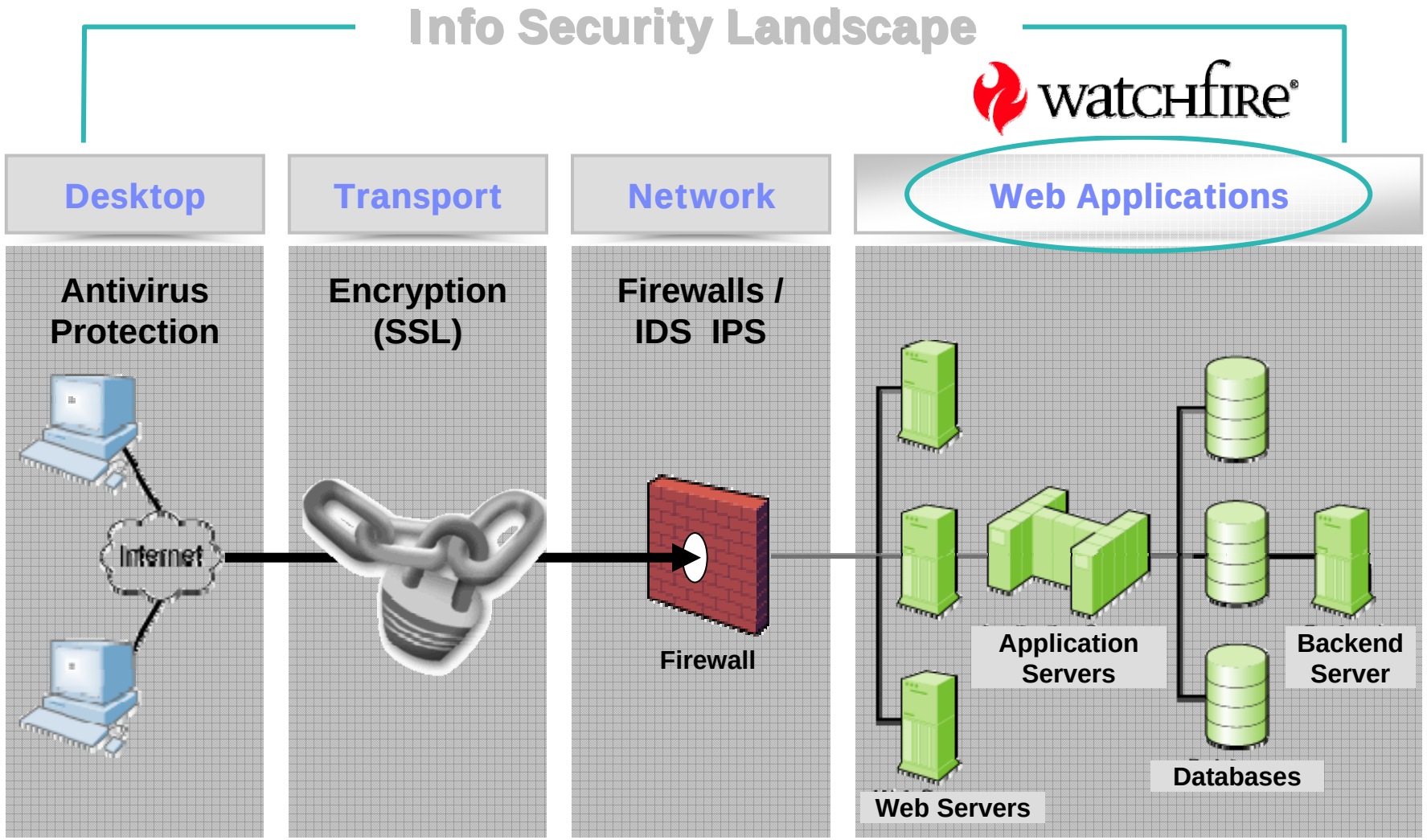
- **WatchFire 总体概览**
- **WEB应用安全介绍及演示**
- **AppScan产品介绍及演示**

Web 应用基础概念


Internet
Firewall
Database
Web Server
(Presentation)
App Server
(Business
Logic)
Client Tier
(Browser)
Middle Tier
Data Tier

神话: “我们的网站是安全的”

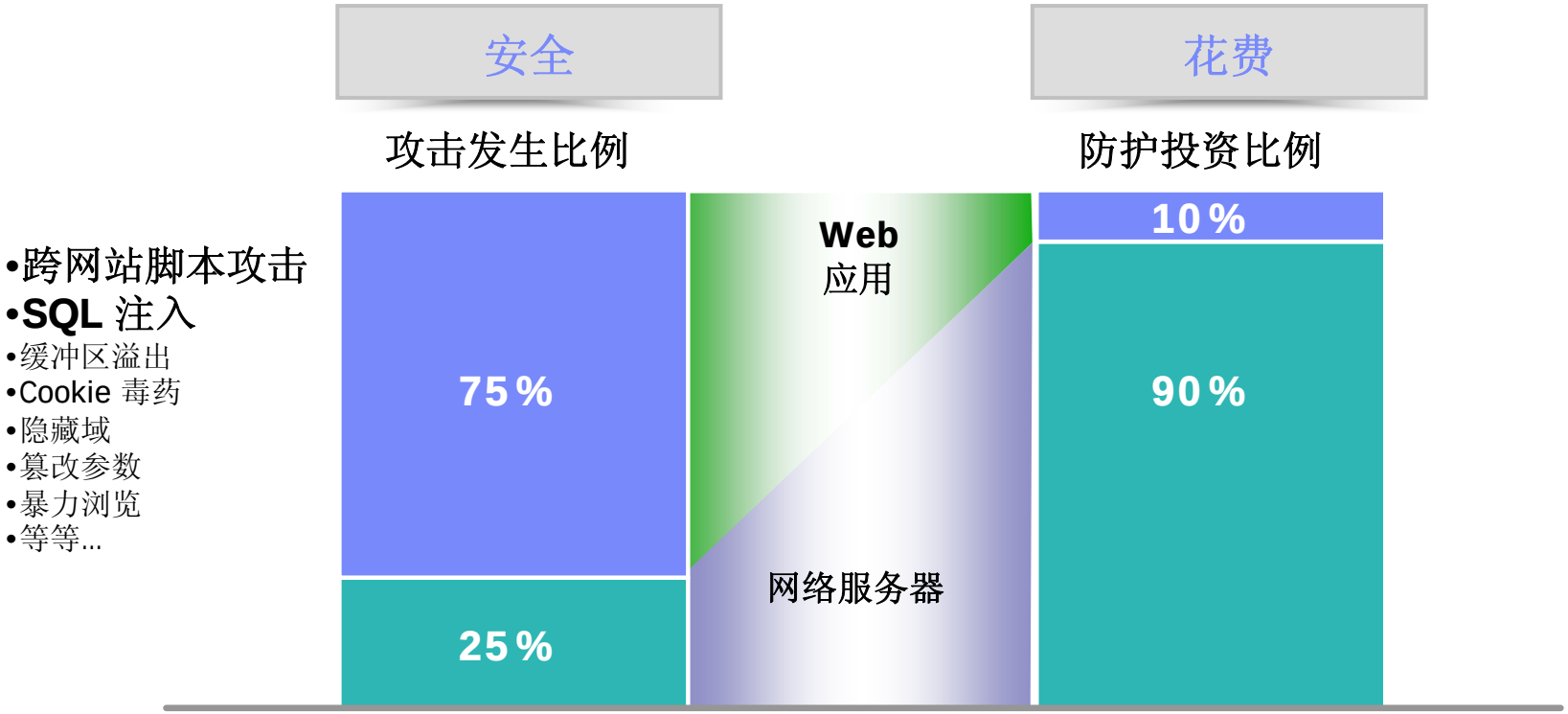
应用安全


Info Security Landscape
watchfire
Desktop
Transport
Network
Web Applications
Antivirus Protection
Encryption (SSL)
Firewalls / IDS IPS
Internet
Firewall
Application Servers
Backend Server
Databases
Web Servers

神话: “我们的网站是安全的”

- “我们运用了网络弱点评估”
  - 忽视了运行在network/web server上的应用软件本身的安全性
- “我们在适当的位置使用了防火墙”
  - 对80 & 443端口的正常应用是开发的
- “我们使用SSL来加密数据”
  - 仅仅保护站点和用户之间交换的数据，但是本身不能保护Web应用本身
- “我们每个季度都要审计我们的web应用”
  - 应用总是在不断地变更
  - 大型的应用环境需要很多 ”moving parts”(可动部件)

真相: 安全和花费是不平衡的



75% 信息安全攻击都来自web应用的层次上

2/3 Web应用是脆弱的

Gartner

Sources: Gartner, Watchfire

WASC

- Web Application Security Consortium (WASC)
- 目的:
  - 发现、接纳和倡导Web应用安全的标准
- 官方网站: www.webappsec.org
- Web安全威胁等级
  - http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf
  - 目的:
  - 澄清和归纳组织对网站安全的威胁种类
  - 对这些问题开发和提升工业标准

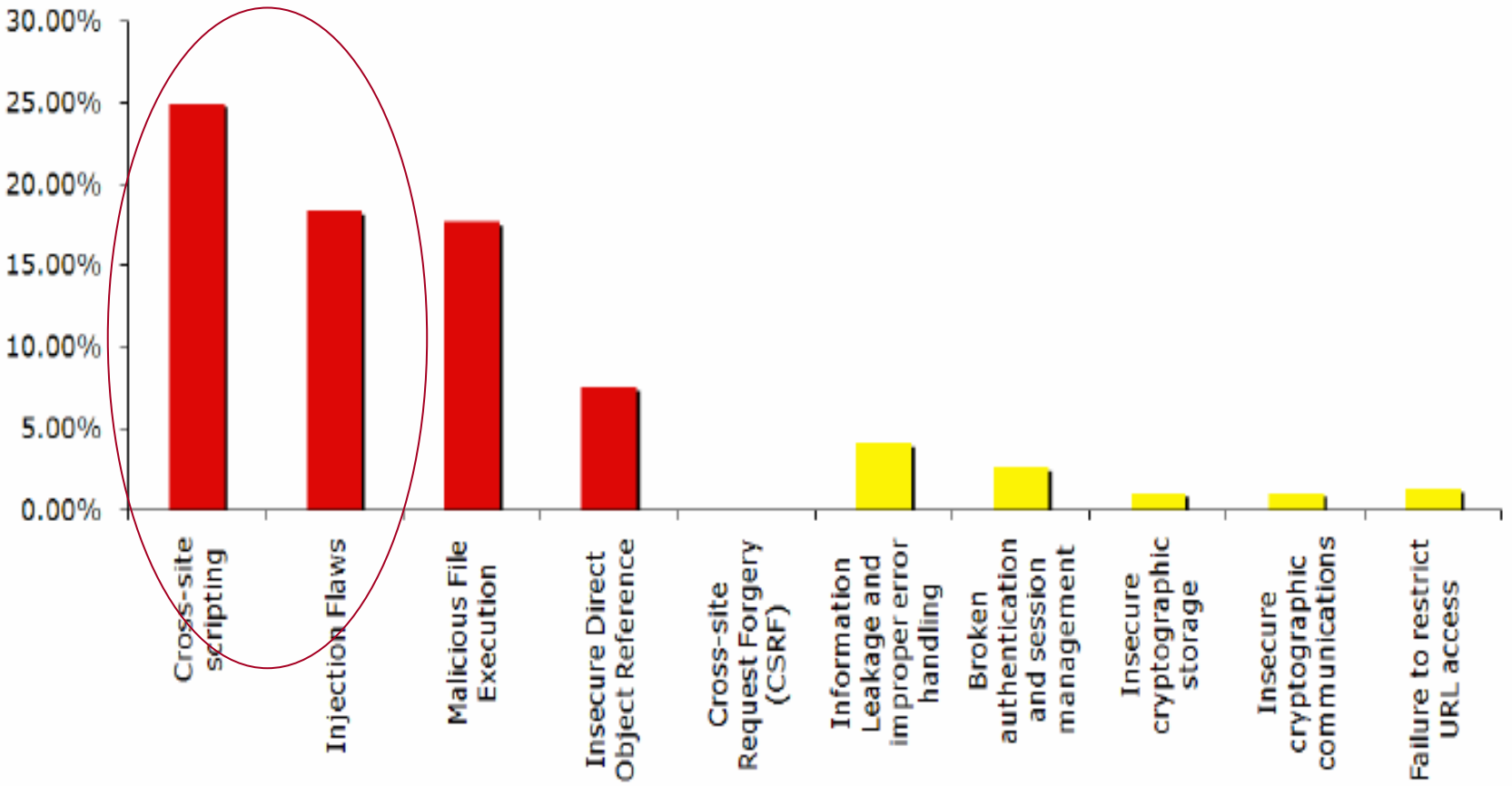
对Web应用的主要威胁(WASC)

- Authentication（验证）
  - 以web站点对确认用户身份的方法、服务或者应用为目标进行攻击
- Authorization（授权）
  - 以web站点确定是否某个用户拥有必要的许可来执行一个请求动作的方法、服务和应用来进行攻击
- Client-Side Attacks（客户侧攻击）
  - 攻击那些乱用或充分利用web站点的用户
- Command Execution（命令执行）
  - 攻击被设计为可执行远程命令的web站点
- Information Disclosure（信息暴露）
  - 攻击被设计为可获取关于网站系统配置信息的站点
- Logical Attacks（逻辑性攻击）
  - 滥用或者充分利用web应用的逻辑流程

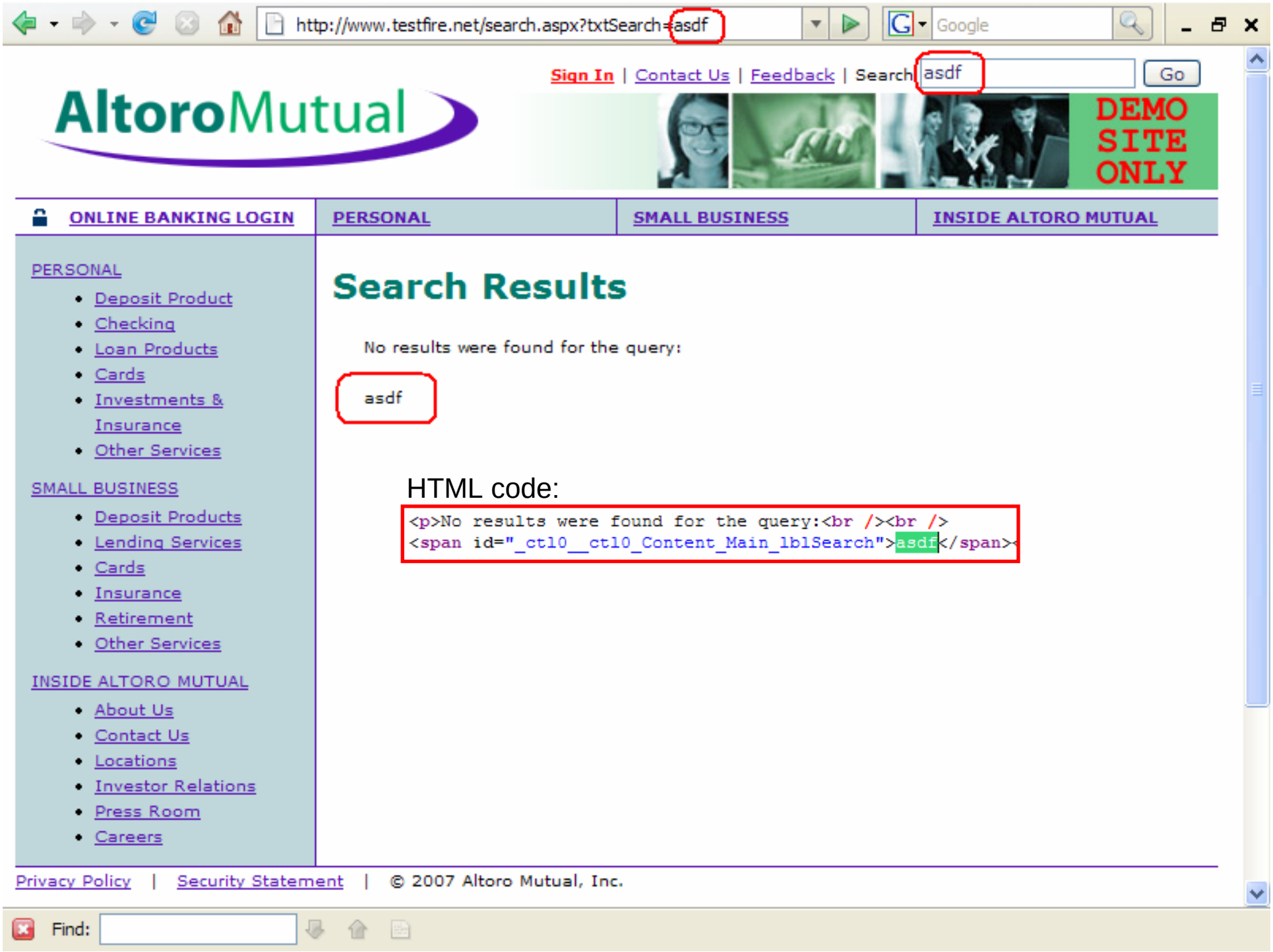
OWASP

- Open Web Application Security Project
- 目标:发现并且解决引起软件不可靠的因素.
- 官方网站: www.owasp.org
- The OWASP Top Ten project
  http://www.owasp.org/index.php/OWASP_Top_Ten_Project
- Purpose:
  - 集思广益有关主要引起web应用安全的问题
  - 提升对待web应用安全问题的意识

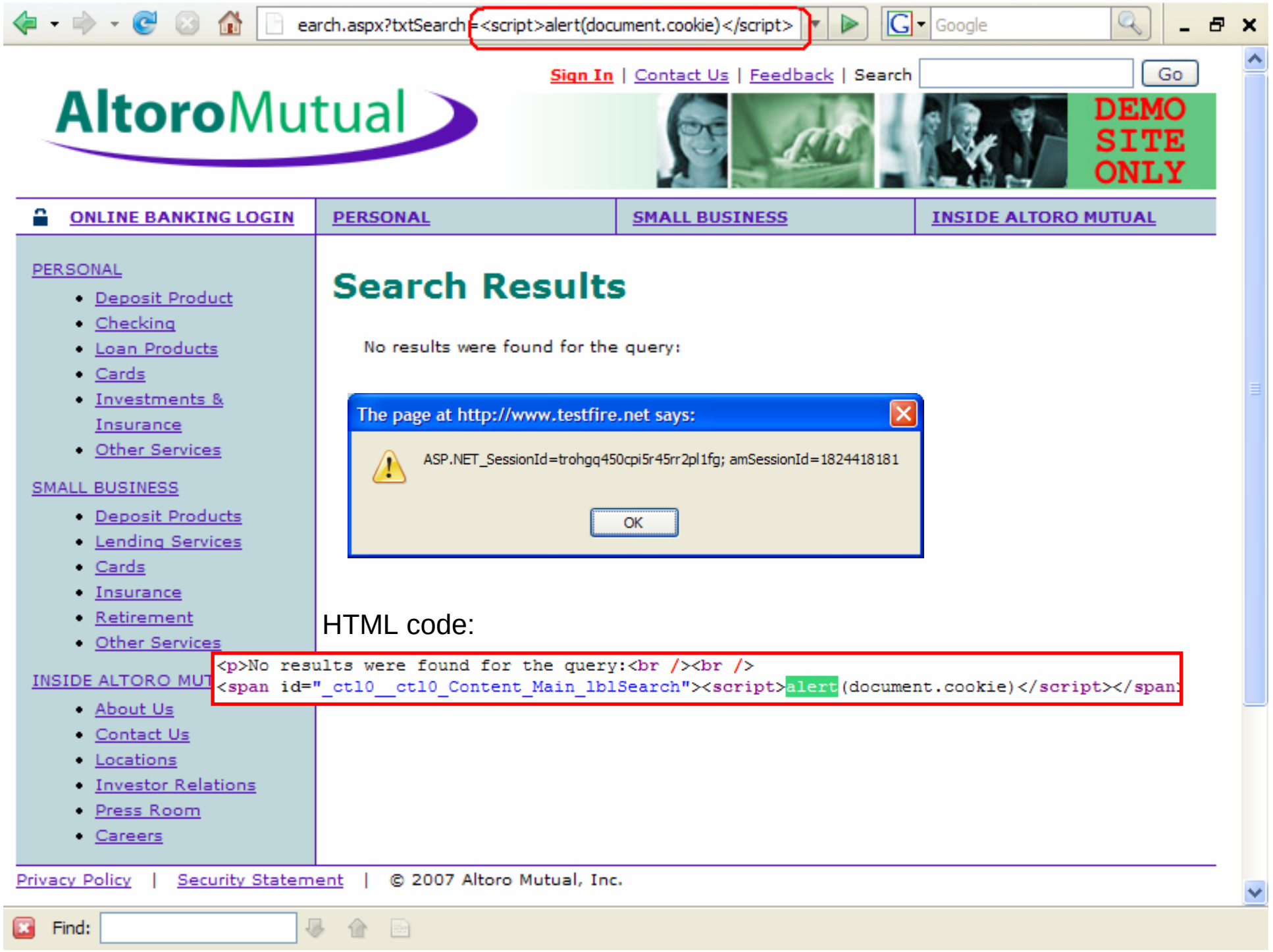
十大应用安全隐患



* 2007 OWASP Top 10


http://www.testfire.net/search.aspx?txtSearch=asdf
Google
Sign In | Contact Us | Feedback | Search asdf Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Search Results
No results were found for the query:
asdf
HTML code:
<p>No results were found for the query:

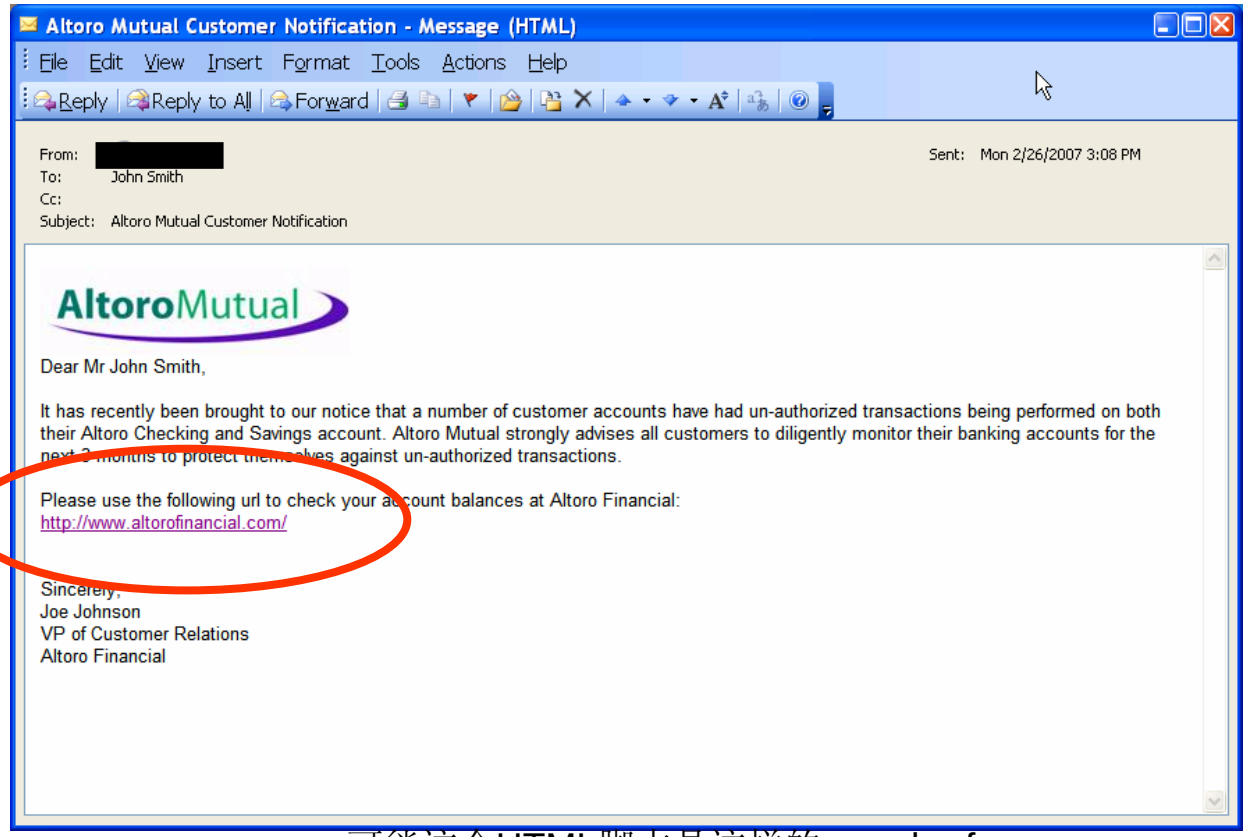
asdf
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.
Find:


earch.aspx?txtSearch=<script>alert(document.cookie)</script>
Google
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUT
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Search Results
No results were found for the query:
The page at http://www.testfire.net says:
ASP.NET_SessionId=trohgq450cpi5r45rr2pl1fg; amSessionId=1824418181
OK
HTML code:
<p>No results were found for the query:

<script>alert(document.cookie)</script>
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.
Find:

Cross Site Scripting（跨站点脚本执行）

- 恶意用户会利用HTML文本创建一个标题图像或者发送一个email
- 通过动态脚本隐藏，这个HTML向目标站点上的搜索框发送JavaScript代码

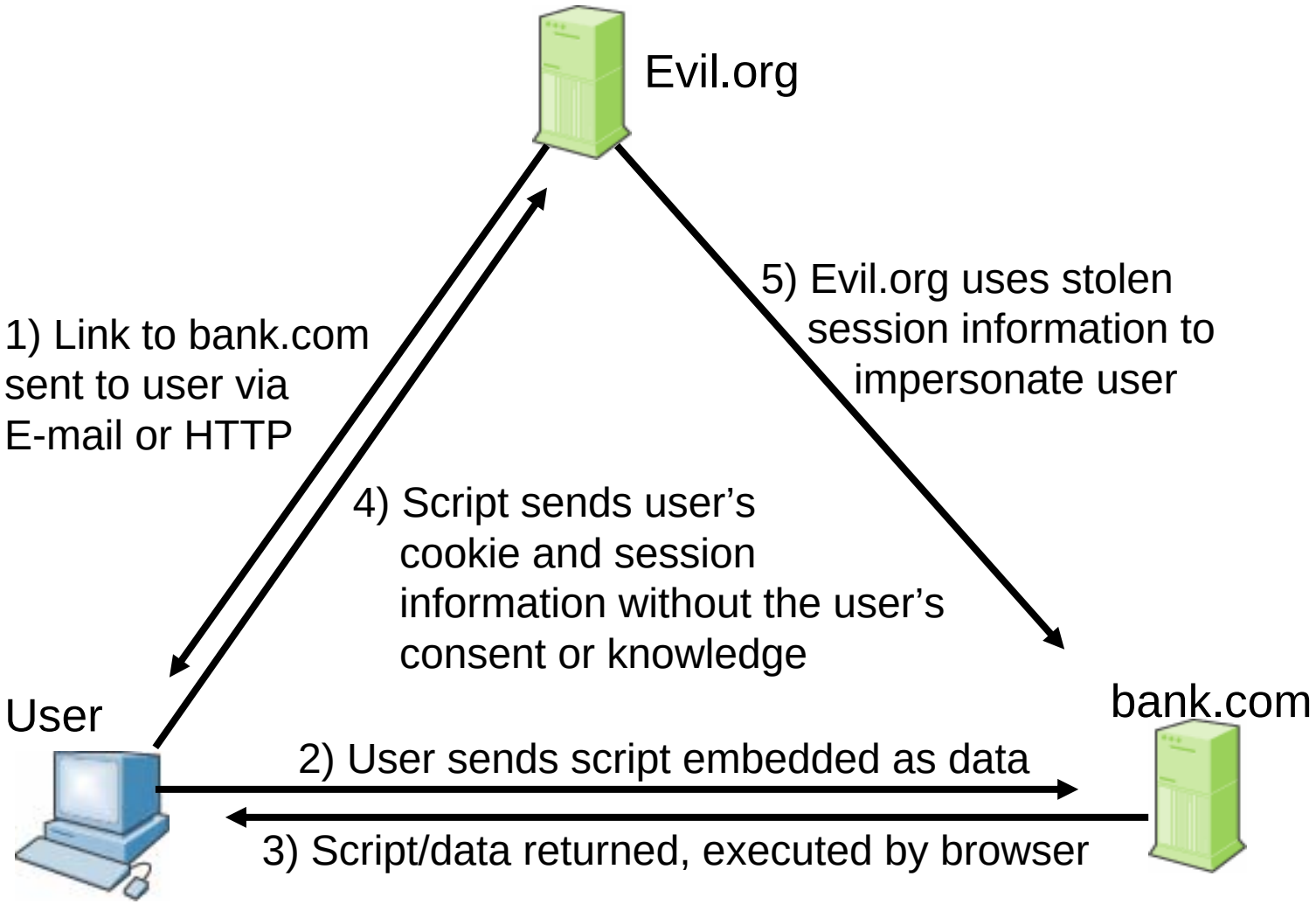


可能这个HTML脚本是这样的：http://altorofinancial.com

Exploiting XSS (cont.) （跨站点脚本执行）

Demo

跨站点脚本执行– 利用过程



利用跨站点脚本执行。。。

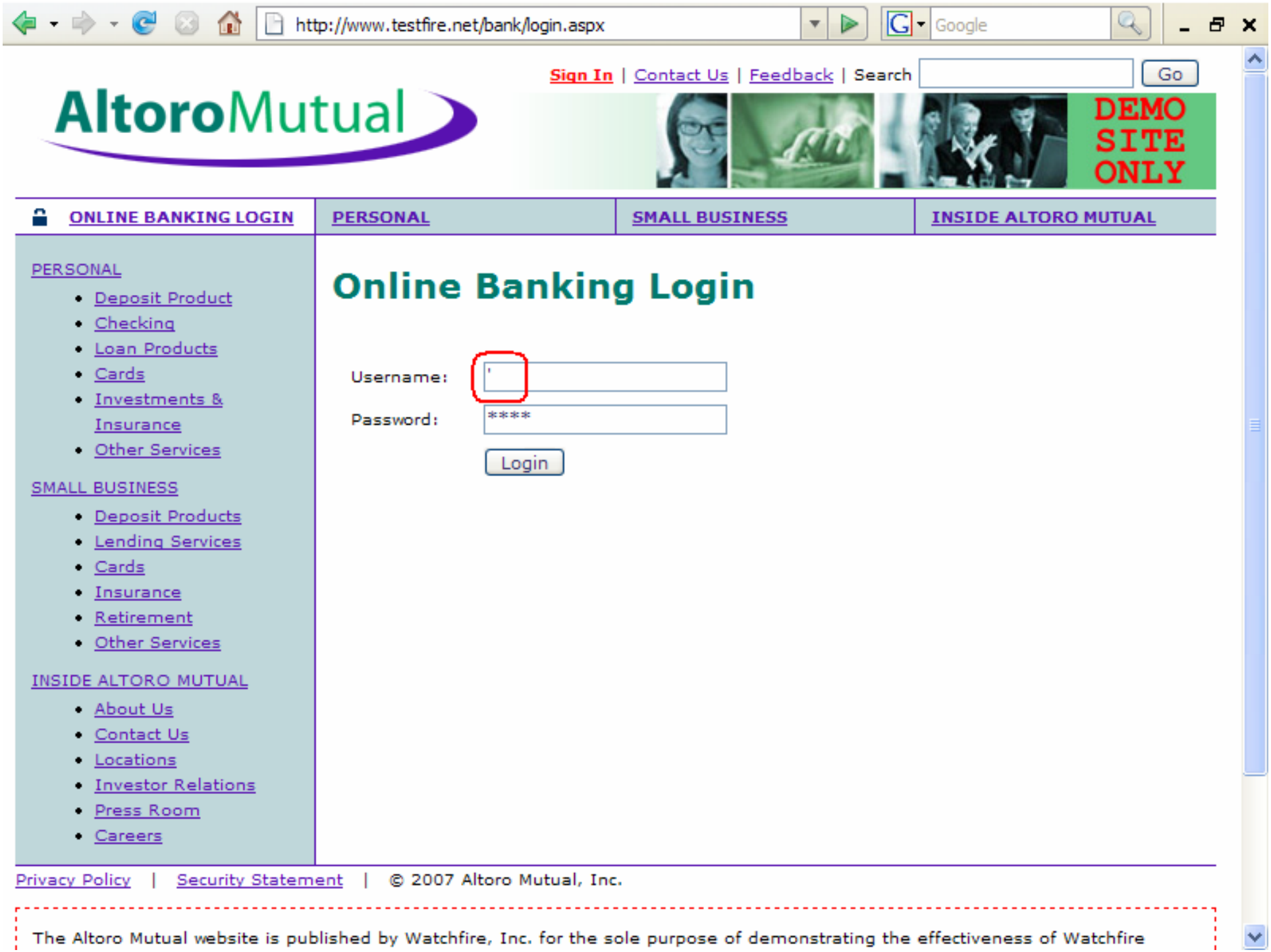
- 如果我能够使你运行我的JavaScript，那么我就能…
  - 窃取你正在浏览区域的cookie
  - 完全修改在这个区域上你能看见的任何页面的内容
  - 跟踪从现在开始你在浏览器上所做的任何操作
  - 把你的访问重定向到Phishing site
  - 利用浏览器的脆弱点来接管你的机器
  - …
- XSS是今天最危险的安全风险

注入缺陷

- 什么是注入缺陷?
  - 用户数据作为命令的一部分发送给解释程序、SQL查询等
- 有那些表现形式?
  - SQL 注入 – 修改或者访问数据库中的数据
  - SSI 注入 – 在Server上执行命令或者访问敏感数据
  - LDAP 注入 – 绕开验证
  - …

SQL 注入

- 用户把SQL命令插入到正常的输入数据中:
  - 通过ID获得产品信息:
  - Select * from products where id='＋myid＋';
  - 黑客: send param id with value ' or ''='
  - 这时后台执行的SQL语句可能会变成:
    Select * from products where id='' or ''=''
  - 黑客就得到所有的产品列表了
  - 使用DAO设计模式或者中间件技术，可以合理地解决SQL注入问题


http://www.testfire.net/bank/login.aspx
Google
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Online Banking Login
Username:
'
Password:
****
Login
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

http://www.testfire.net/bank/login.aspx

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = '' AND password = 'asdf''.

Error Message:

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

黑客猜想验证用户登陆的SQL语句可能是：
select * from customer where username='xx' and password='xx'

System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at Altoro.Authentication.ValidateUser(String uName, String pWord) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object sender, EventArgs e) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 32 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)


http://www.testfire.net/bank/login.aspx
Google
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Online Banking Login
Username: ' or 1=1--
Password:
Login
于是黑客猜利用SQL注入技术得到的SQL语句为：
select * from customer where username='' or 1=1- - and password=''
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

AltoroMutual

Hello, John Smith

Welcome to Altoro Mutual Online.

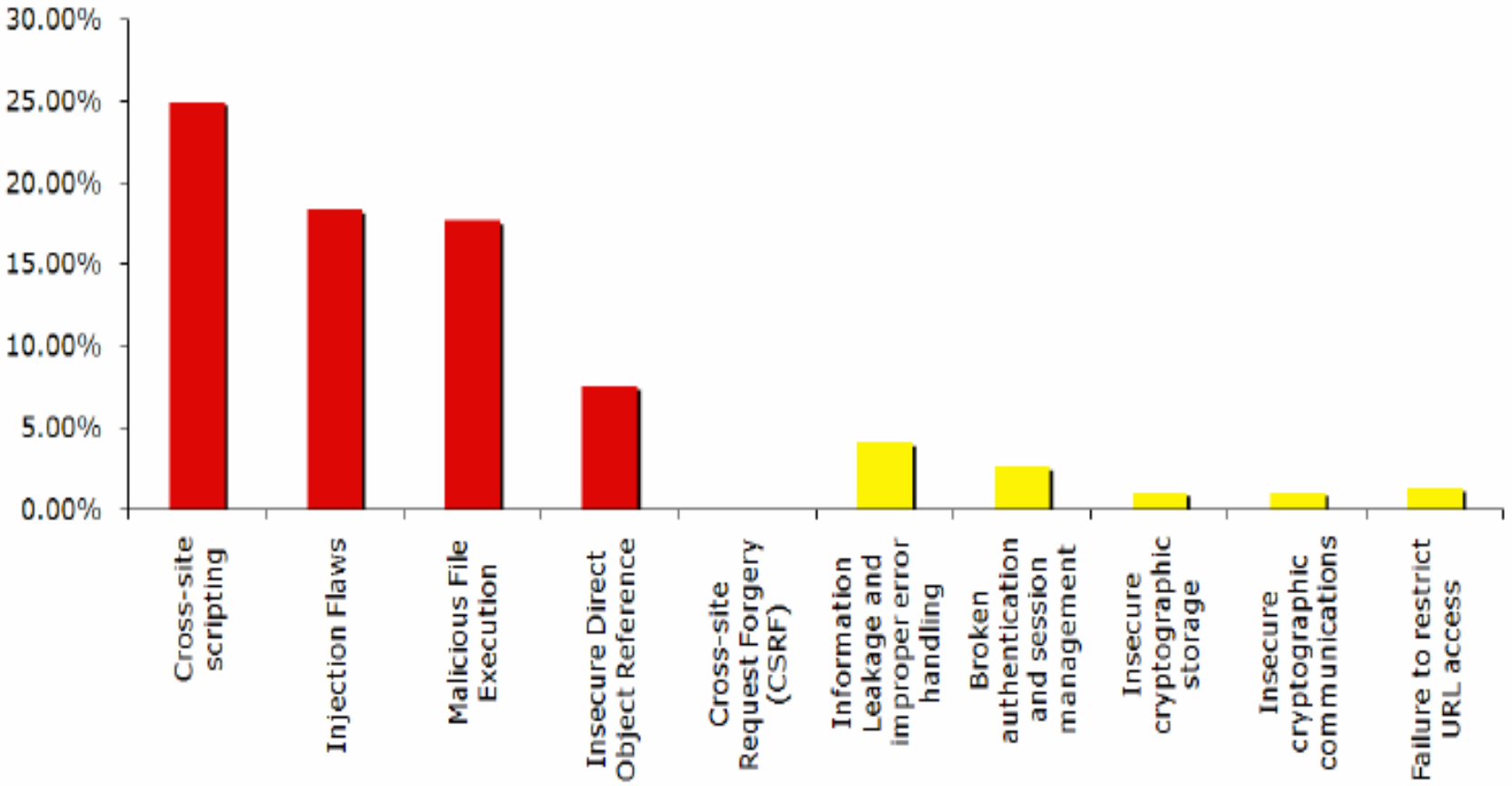
View Account Details: 1001160140 Checking GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Application Security Defects #1 & #2 Vulnerabilities



* 2007 OWASP Top 10

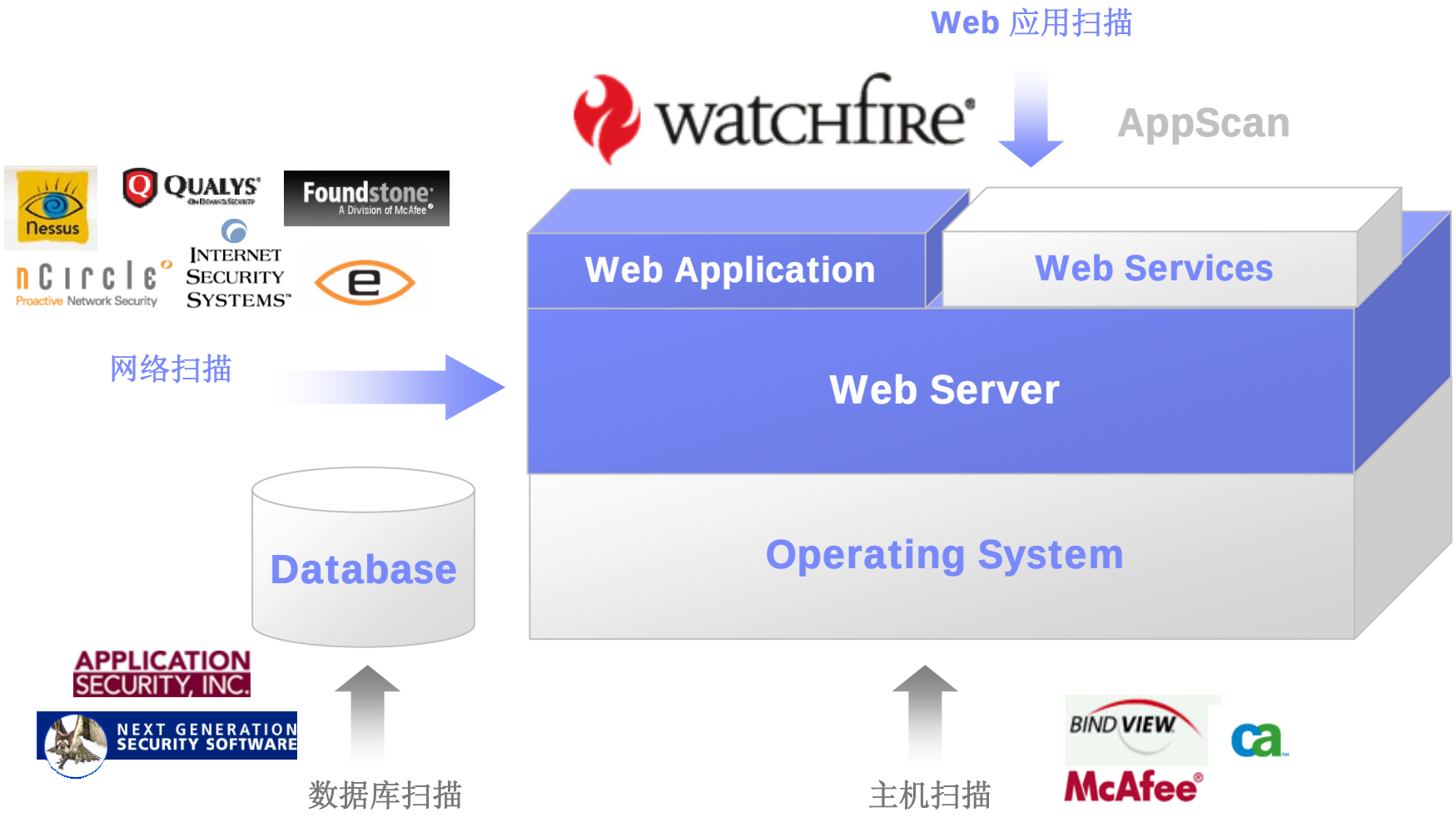
议程安排

- **WatchFire** 总体概览
- **WEB**应用安全介绍及演示
- **AppScan**产品介绍

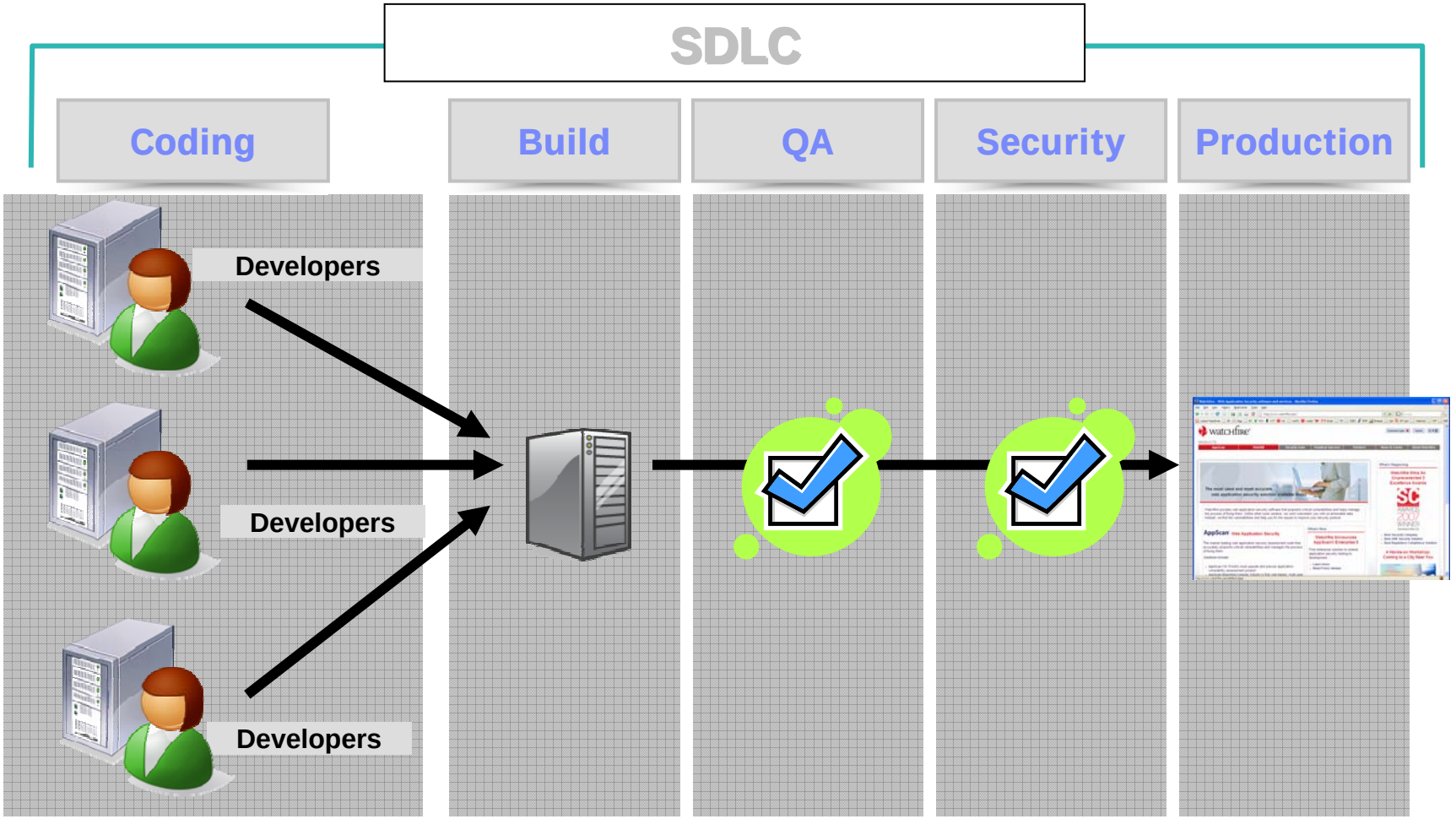
AppScan

- 他是什么?
  - Web应用安全扫描器
- 我们为什么需要它?
  - 我们能够方便地查找和修复Web应用的安全问题
- AppScan怎么做?
  - 扫描web应用、查找安全问题并且将他们及时地记录
- 谁使用它?
  - 安全审计员 – 主要用户
  - QA 工程师
  - Developers – 尽可能早地找到问题（更加有效）

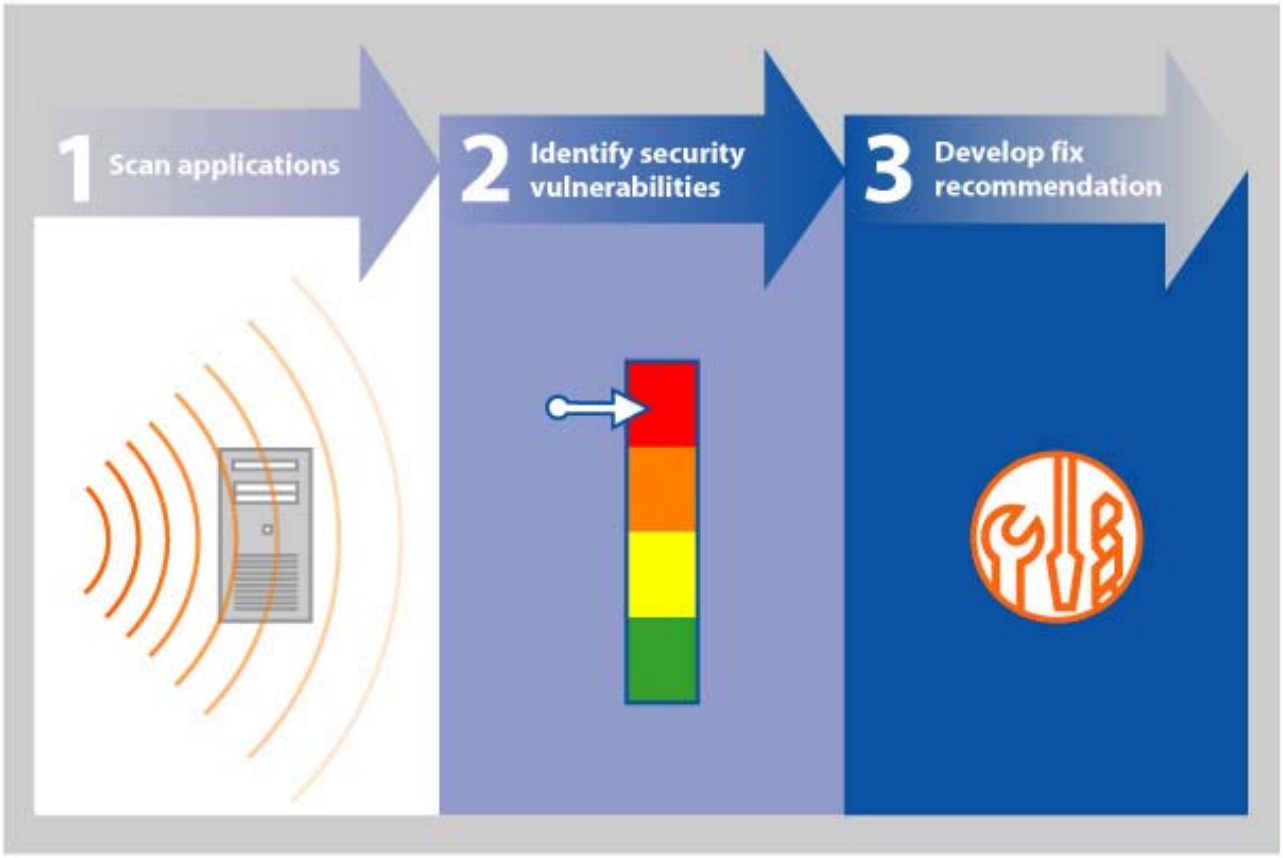
AppScan可以测什么？



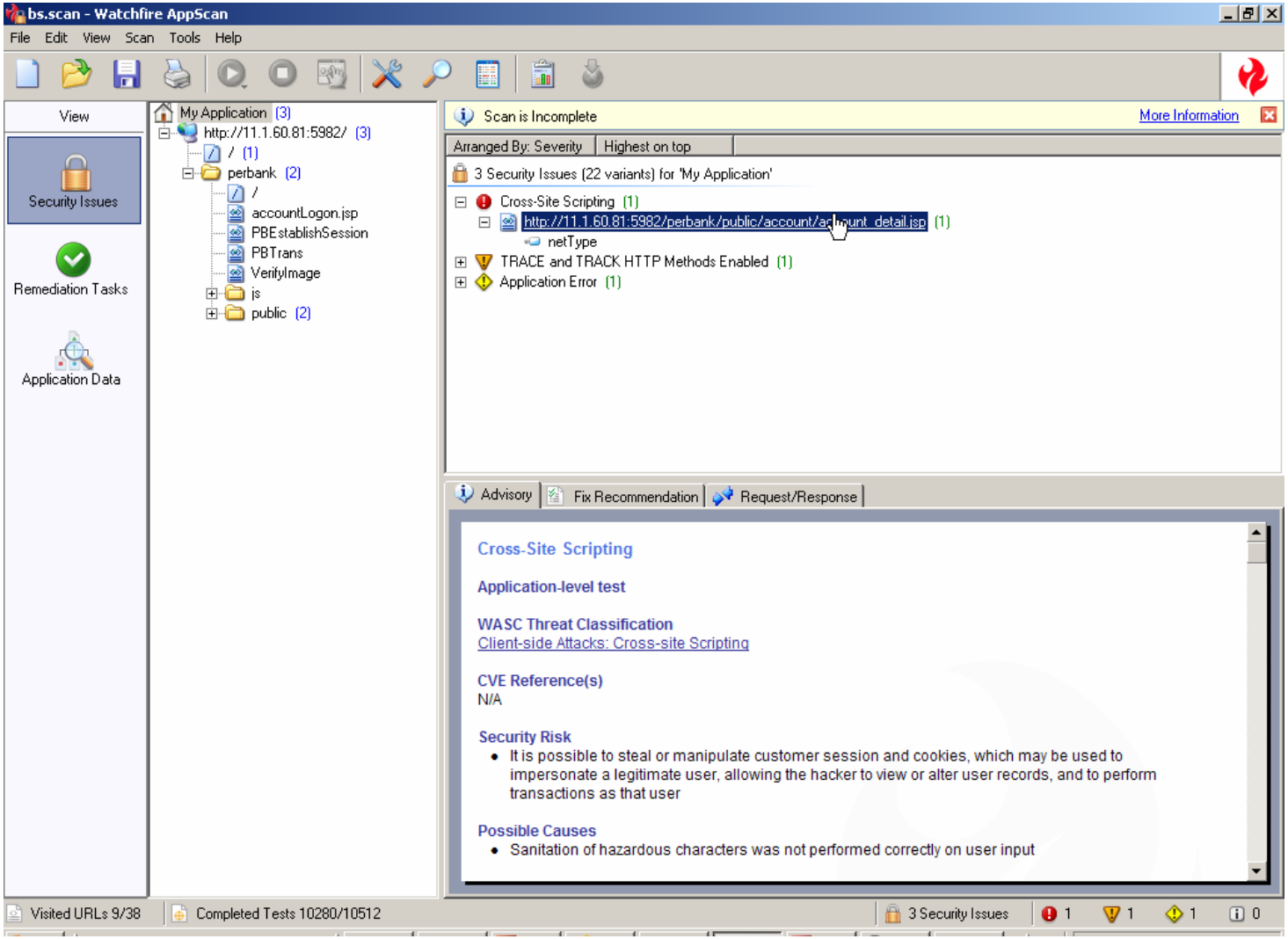
AppScan可以在什么时候测？



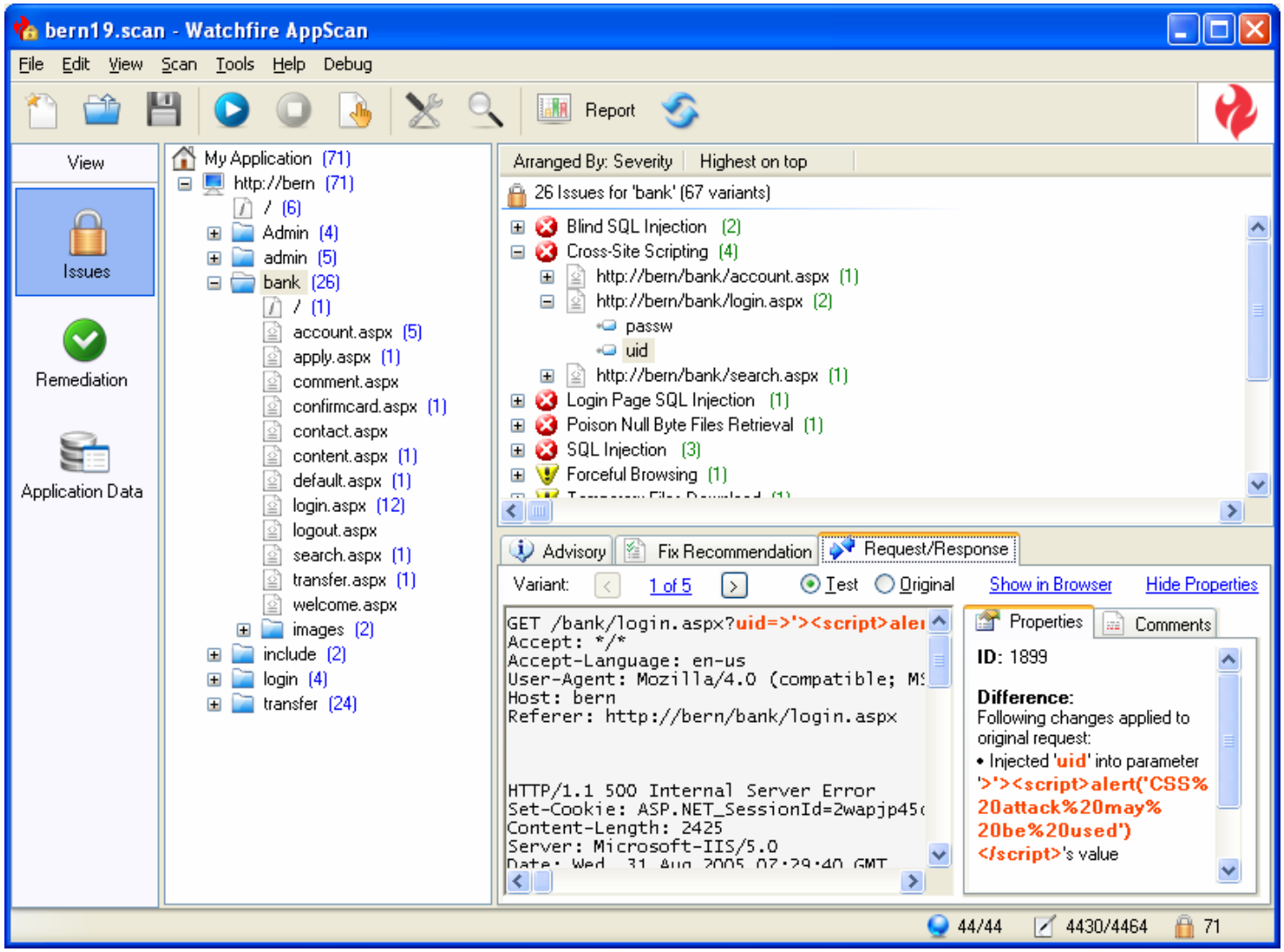
可行性修复建议


1 Scan applications
2 Identify security vulnerabilities
3 Develop fix recommendation

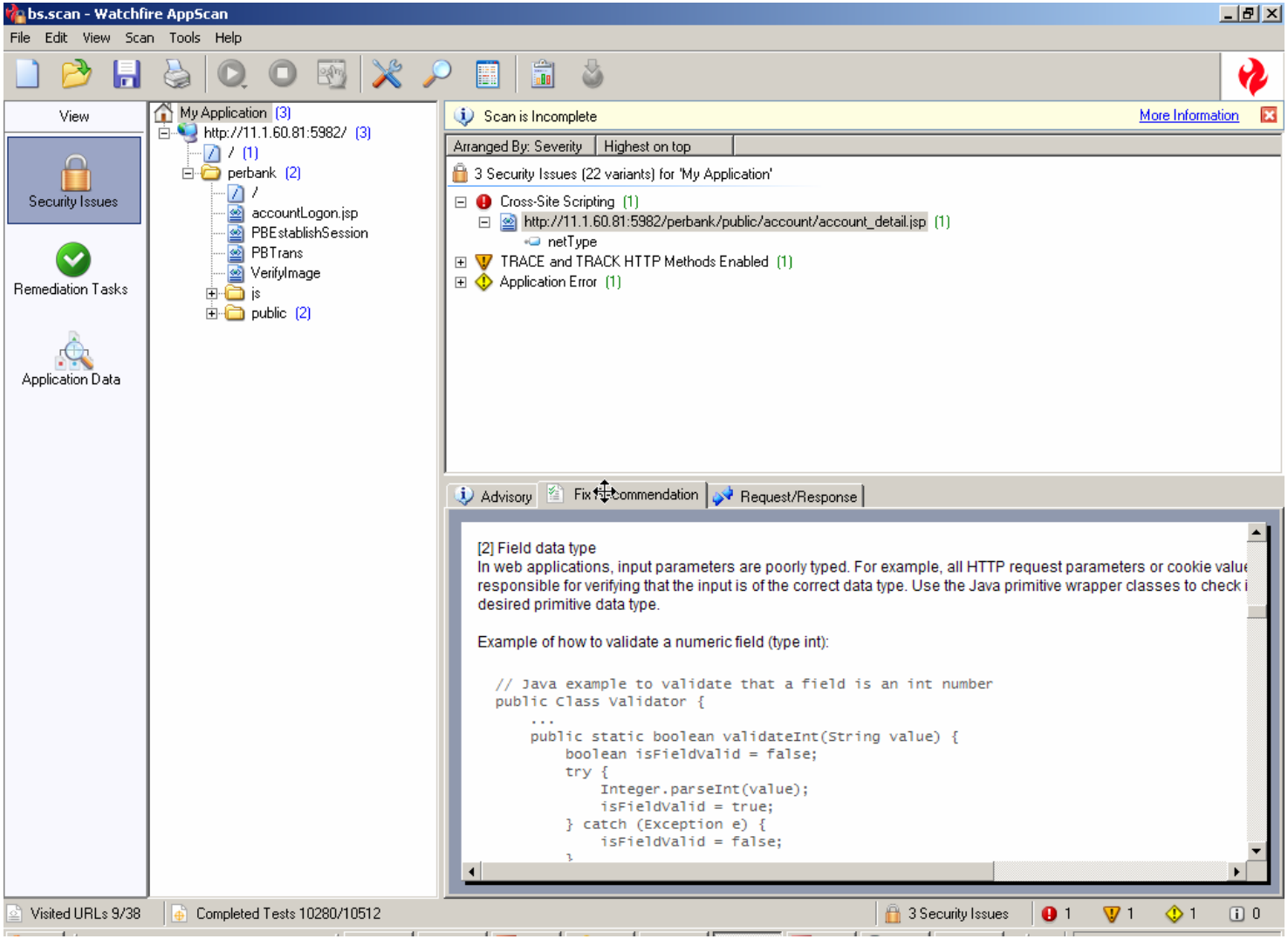
可行性修复建议


bs.scan - Watchfire AppScan
File Edit View Scan Tools Help
View
Security Issues
Remediation Tasks
Application Data
My Application (3)
http://11.1.60.81:5982/ (3)
/ (1)
perbank (2)
/
accountLogon.jsp
PBEstablishSession
PBTrans
VerifyImage
js
public (2)
Scan is Incomplete
More Information
Arranged By: Severity
Highest on top
3 Security Issues (22 variants) for 'My Application'
Cross-Site Scripting (1)
http://11.1.60.81:5982/perbank/public/account/account_detail.jsp (1)
netType
TRACE and TRACK HTTP Methods Enabled (1)
Application Error (1)
Advisory
Fix Recommendation
Request/Response
Cross-Site Scripting
Application-level test
WASC Threat Classification
Client-side Attacks: Cross-site Scripting
CVE Reference(s)
N/A
Security Risk
It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Possible Causes
Sanitation of hazardous characters was not performed correctly on user input
Visited URLs 9/38
Completed Tests 10280/10512
3 Security Issues
1
1
1
0

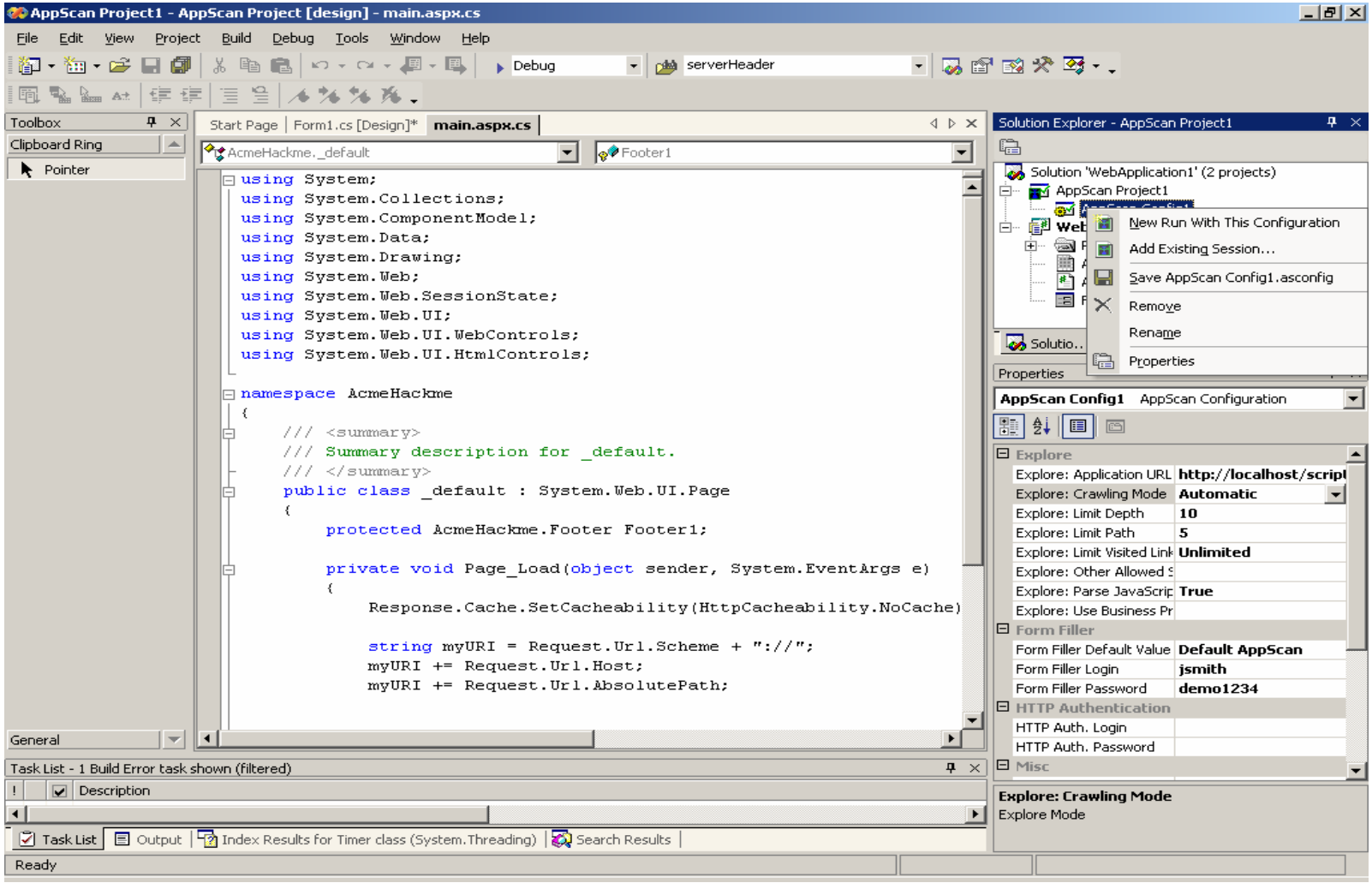
可行性修复建议


bern19.scan - Watchfire AppScan
File Edit View Scan Tools Help Debug
Report
View
Issues
Remediation
Application Data
My Application (71)
http://bern (71)
/ (6)
Admin (4)
admin (5)
bank (26)
/ (1)
account.aspx (5)
apply.aspx (1)
comment.aspx
confirmcard.aspx (1)
contact.aspx
content.aspx (1)
default.aspx (1)
login.aspx (12)
logout.aspx
search.aspx (1)
transfer.aspx (1)
welcome.aspx
images (2)
include (2)
login (4)
transfer (24)
Arranged By: Severity
Highest on top
26 Issues for 'bank' (67 variants)
Blind SQL Injection (2)
Cross-Site Scripting (4)
http://bern/bank/account.aspx (1)
http://bern/bank/login.aspx (2)
passw
uid
http://bern/bank/search.aspx (1)
Login Page SQL Injection (1)
Poison Null Byte Files Retrieval (1)
SQL Injection (3)
Forceful Browsing (1)
Advisory
Fix Recommendation
Request/Response
Variant:
1 of 5
Test
Original
Show in Browser
Hide Properties
GET /bank/login.aspx?uid=>'><script>alei
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MS
Host: bern
Referer: http://bern/bank/login.aspx
HTTP/1.1 500 Internal Server Error
Set-Cookie: ASP.NET_SessionId=2wapjp45
Content-Length: 2425
Server: Microsoft-IIS/5.0
Properties
Comments
ID: 1899
Difference:
Following changes applied to original request:
• Injected 'uid' into parameter '>'><script>alert('CSS%20attack%20may%20be%20used')</script>'s value
44/44
4430/4464
71

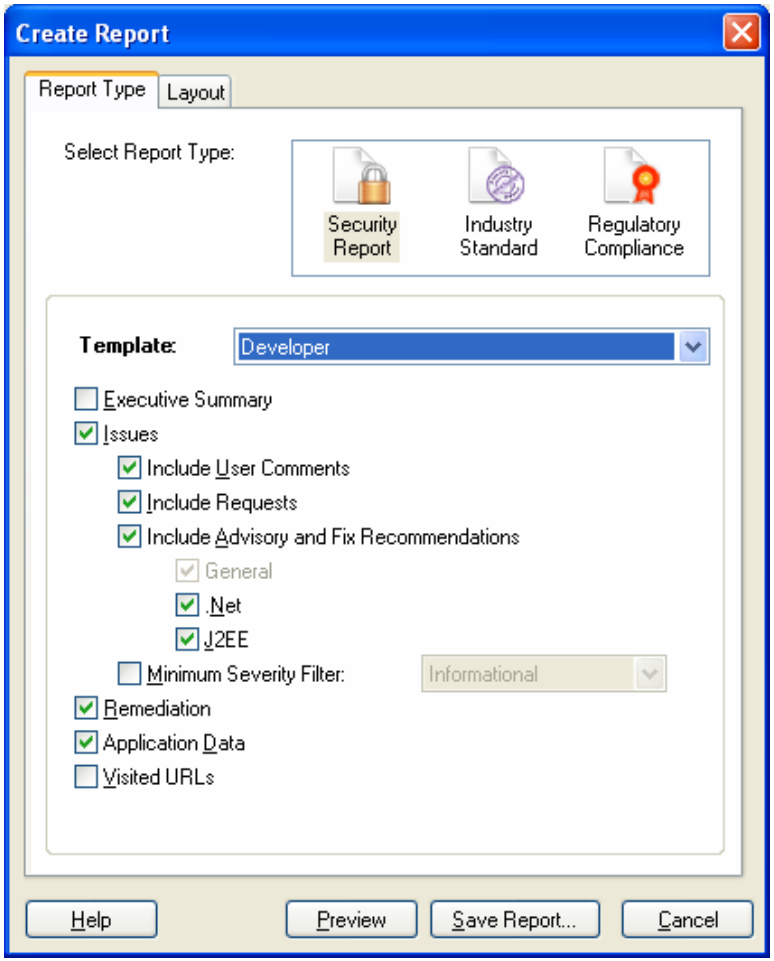
可行性修复建议

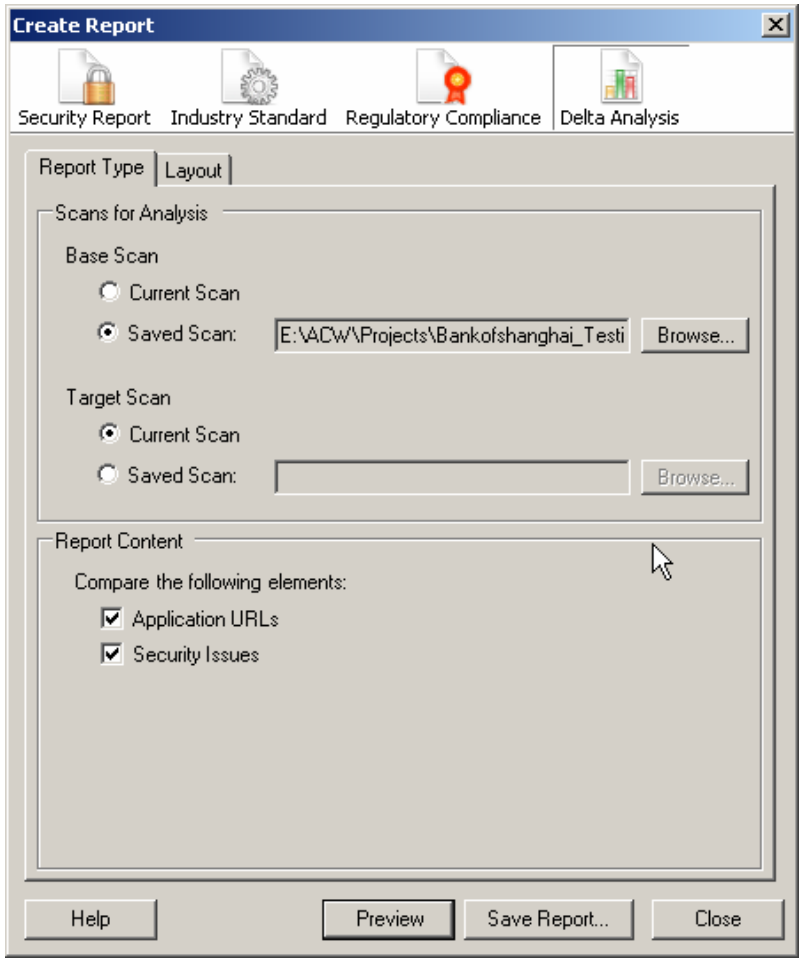

bs.scan - Watchfire AppScan
File Edit View Scan Tools Help
View
Security Issues
Remediation Tasks
Application Data
My Application [3]
http://11.1.60.81:5982/ [3]
/ [1]
perbank [2]
/
accountLogon.jsp
PBEstablishSession
PBTrans
VerifyImage
js
public [2]
Scan is Incomplete
More Information
Arranged By: Severity
Highest on top
3 Security Issues (22 variants) for 'My Application'
Cross-Site Scripting [1]
http://11.1.60.81:5982/perbank/public/account/account_detail.jsp [1]
netType
TRACE and TRACK HTTP Methods Enabled [1]
Application Error [1]
Advisory
Fix Recommendation
Request/Response
[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie value
responsible for verifying that the input is of the correct data type. Use the Java primitive wrapper classes to check i
desired primitive data type.
Example of how to validate a numeric field (type int):
// Java example to validate that a field is an int number
public Class Validator {
...
public static boolean validateInt(String value) {
boolean isFieldValid = false;
try {
Integer.parseInt(value);
isFieldValid = true;
} catch (Exception e) {
isFieldValid = false;
Visited URLs 9/38
Completed Tests 10280/10512
3 Security Issues
1
1
1
0

AppScan DE--Web应用开发插件

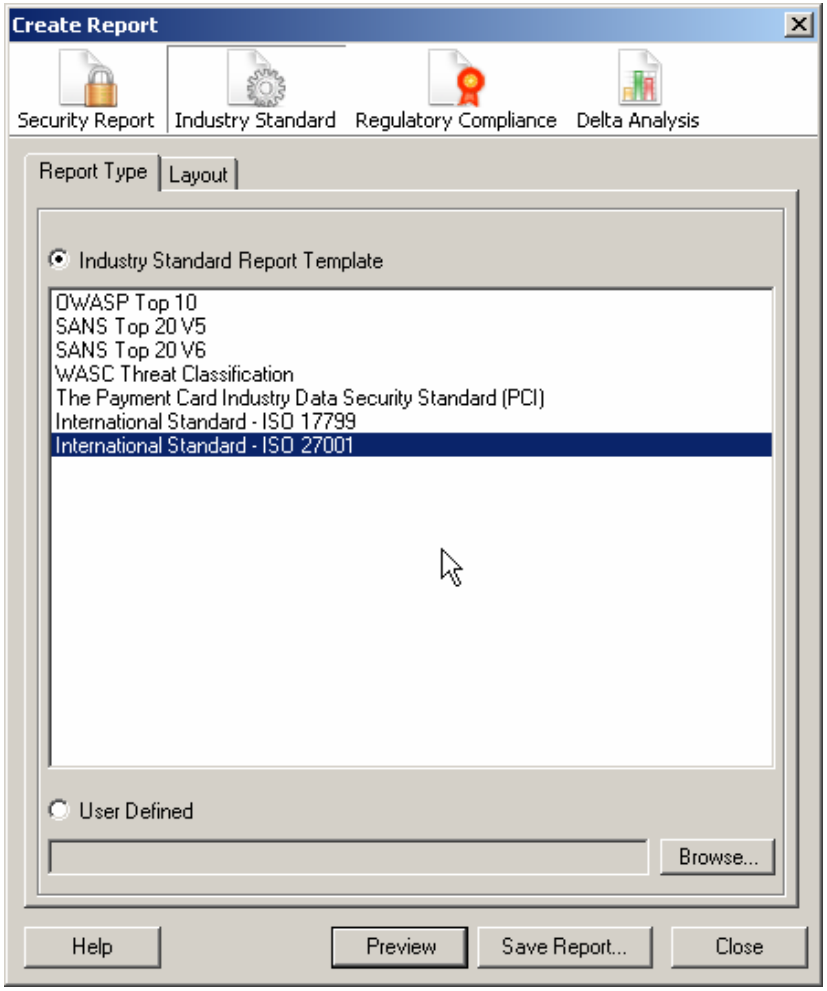


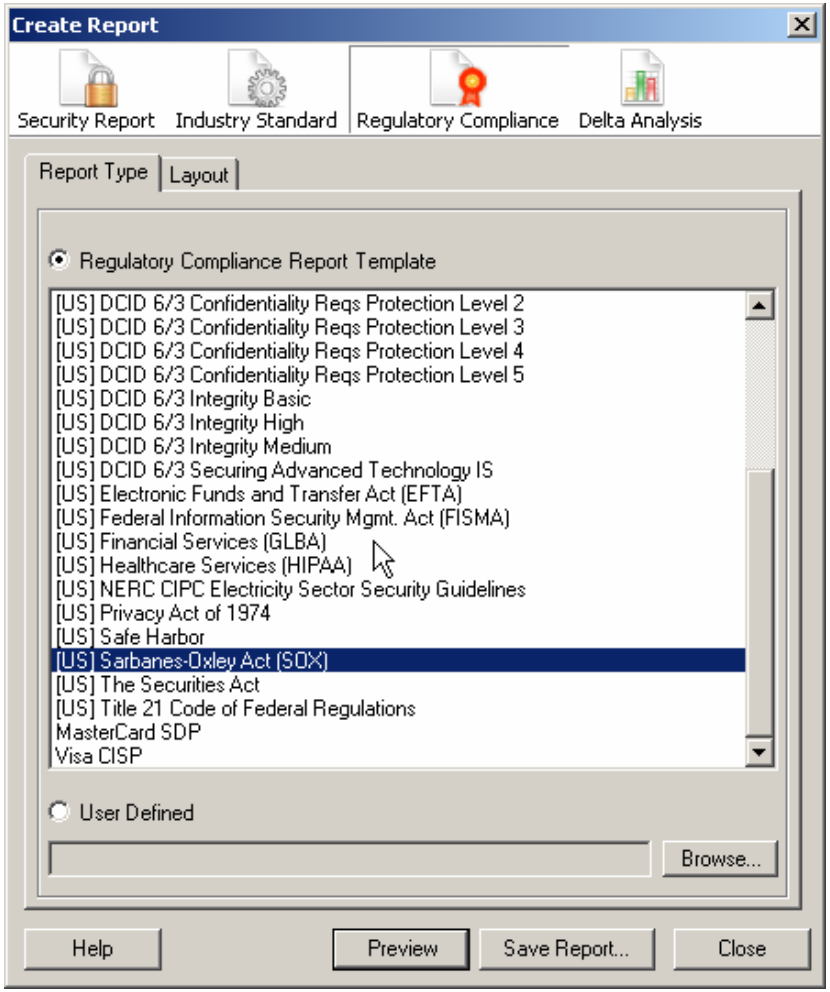
灵活的报表


Create Report
Report Type
Layout
Select Report Type:
Security Report
Industry Standard
Regulatory Compliance
Template:
Developer
Executive Summary
Issues
Include User Comments
Include Requests
Include Advisory and Fix Recommendations
General
.Net
J2EE
Minimum Severity Filter:
Informational
Remediation
Application Data
Visited URLs
Help
Preview
Save Report...
Cancel

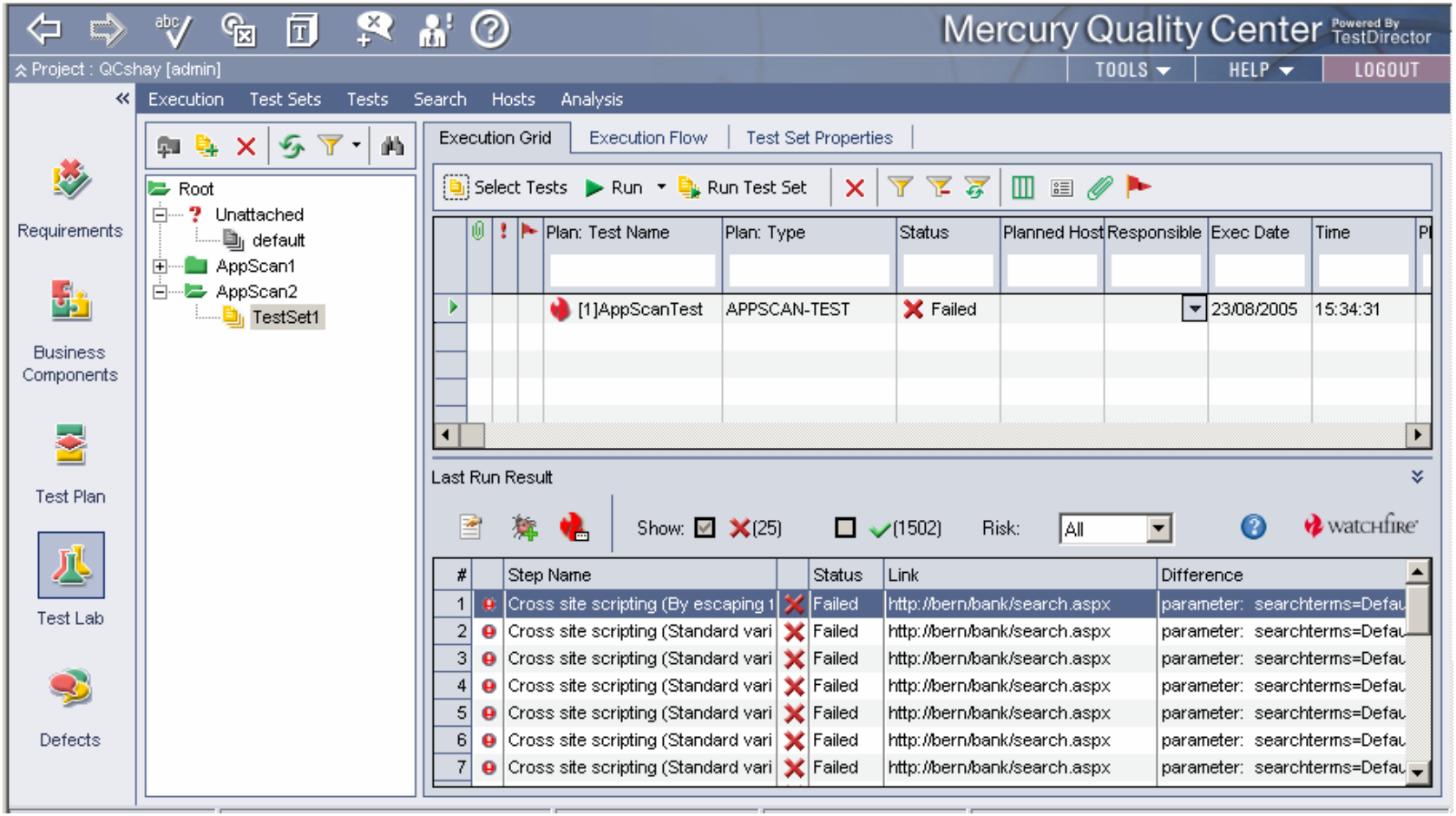

Create Report
Security Report
Industry Standard
Regulatory Compliance
Delta Analysis
Report Type
Layout
Scans for Analysis
Base Scan
Current Scan
Saved Scan:
E:\ACW\Projects\Bankofshanghai_Testi
Browse...
Target Scan
Current Scan
Saved Scan:
Browse...
Report Content
Compare the following elements:
Application URLs
Security Issues
Help
Preview
Save Report...
Close

与安全标准的依从


Create Report
Security Report
Industry Standard
Regulatory Compliance
Delta Analysis
Report Type
Layout
Industry Standard Report Template
OWASP Top 10
SANS Top 20 V5
SANS Top 20 V6
WASC Threat Classification
The Payment Card Industry Data Security Standard (PCI)
International Standard - ISO 17799
International Standard - ISO 27001
User Defined
Browse...
Help
Preview
Save Report...
Close


Create Report
Security Report
Industry Standard
Regulatory Compliance
Delta Analysis
Report Type
Layout
Regulatory Compliance Report Template
[US] DCID 6/3 Confidentiality Reqs Protection Level 2
[US] DCID 6/3 Confidentiality Reqs Protection Level 3
[US] DCID 6/3 Confidentiality Reqs Protection Level 4
[US] DCID 6/3 Confidentiality Reqs Protection Level 5
[US] DCID 6/3 Integrity Basic
[US] DCID 6/3 Integrity High
[US] DCID 6/3 Integrity Medium
[US] DCID 6/3 Securing Advanced Technology IS
[US] Electronic Funds and Transfer Act (EFTA)
[US] Federal Information Security Mgmt. Act (FISMA)
[US] Financial Services (GLBA)
[US] Healthcare Services (HIPAA)
[US] NERC CIPC Electricity Sector Security Guidelines
[US] Privacy Act of 1974
[US] Safe Harbor
[US] Sarbanes-Oxley Act (SOX)
[US] The Securities Act
[US] Title 21 Code of Federal Regulations
MasterCard SDP
Visa CISP
User Defined
Browse...
Help
Preview
Save Report...
Close

AppScan QA---测试阶段集成



技术优势

- 直观的图形界面
- 及时的更新
- 详细的漏洞修复建议
- 灵活的报表功能
- 全面覆盖SDLC（软件生命周期）的工具

产品定位

- 世界第一的创造者:
  - 自动的 **Web** 应用安全测试工具 (AppScan)*
  - 自动的 **SQL** 注入 和 **XSS** 测试
  - 完全支持 **SDLC** 的开发, 质量评估, 审计和生产
  - 与缺陷跟踪系统 **(ClearQuest)** 的整合
- 在应用安全漏洞评估管理的市场份额世界第一

有用链接

- OWASP
  - http://www.owasp.org
  - Top 10
  - Web 应用开发安全
- Web Application Security Consortium
  - http://www.webappsec.org
  - Web应用安全弱点分类
  - Web攻击事件库


Thank
You