



IBM Software Group

Qualitymanagement Lösungen für innovative Softwareentwicklung

Quality Driven Software Delivery

Rational. software

[→ Go to IBM](#)

Edgar Boehm
edgar.boehm@de.ibm.com

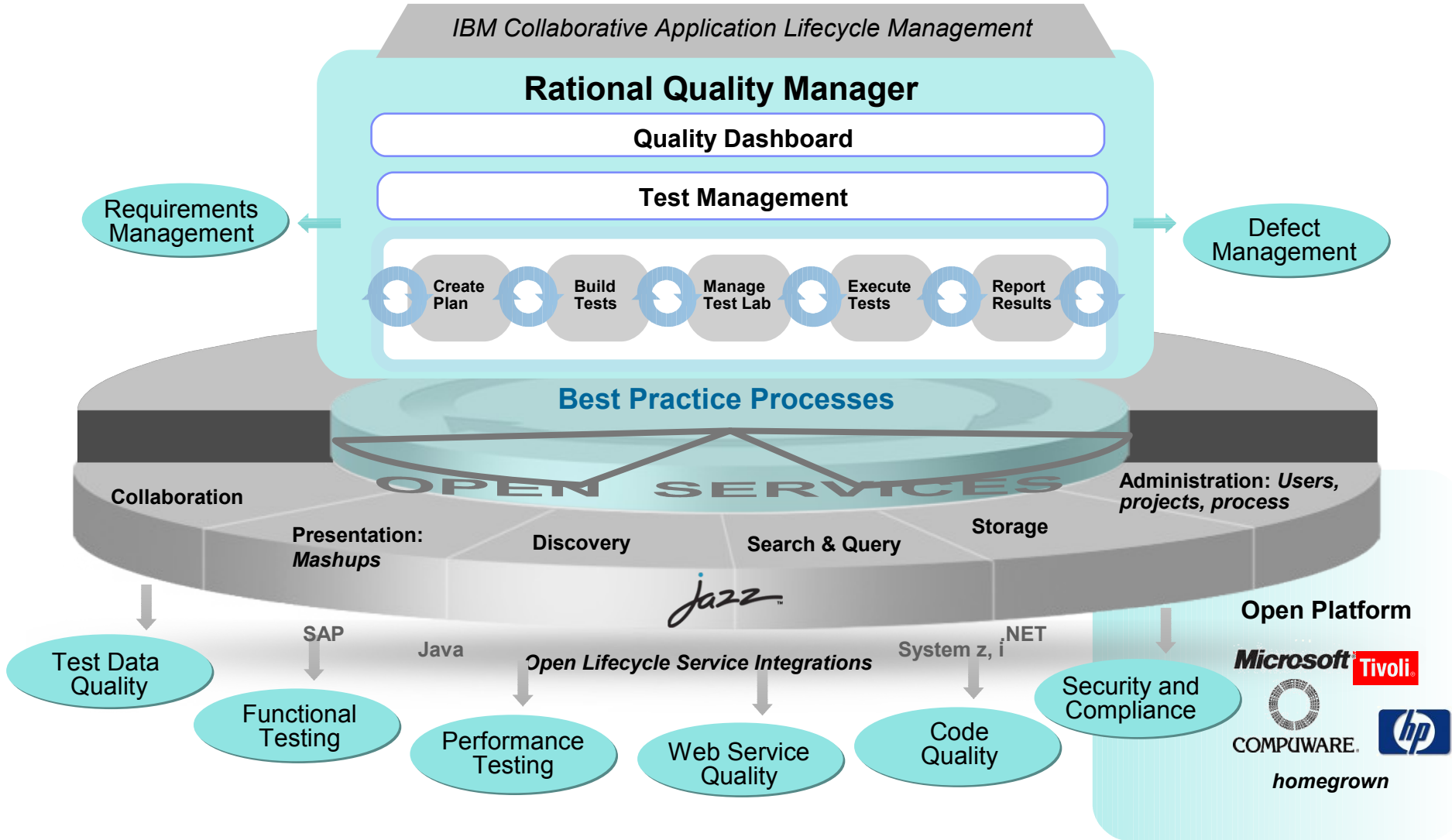
IBM Rational Quality Management

Quality Driven Software Delivery

- IBM Rational Quality Management
- Rational Functional Testing
- Rational Performance Tester
- Rational IT Web Security



Collaborative Application Lifecycle Management



E2E Integration Testing of SAP Solutions

Test Process embedded in the SAP Application Lifecycle

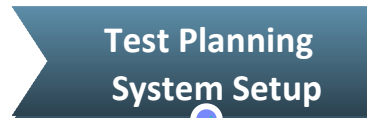
Type of Change

Test Scope Identification



- Implementation of new SAP Solution

- Business Blueprint Design
- Solution Configuration



- SAP Support Packages
- SAP Legal Change Packages
- SAP Enhancement Packages
- Customizing changes
- Custom Code
- Interface changes

- Business Blueprint Update
- Identification of Business Processes affected by SAP Solution Updates
- Recommendation of business processes for regression tests

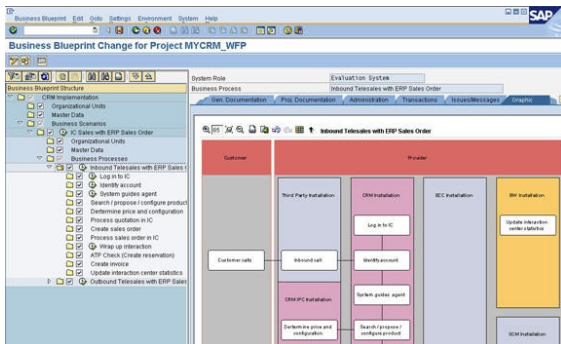
- Development of Test Cases
- Test Plan setup
- Compilation of Test Packages
- Assignment of Testers
- Setup of Test System
- Creation of Test Data

- Manual tests
- Automated tests
- Integration Validation
- Incident Management
- Performance tests
- Test status and progress reporting
- Test sign-off

- Deployment of changes through transports from Test to Production system
- SAP Support packages, Legal Change Packages, Enhancement Packages

Rational Software and SAP Solution Manager for Testing

Rational software and SAP Solution Manager for testing integrates application lifecycle management capabilities of SAP Solution Manager with test planning and test execution capabilities of Rational software

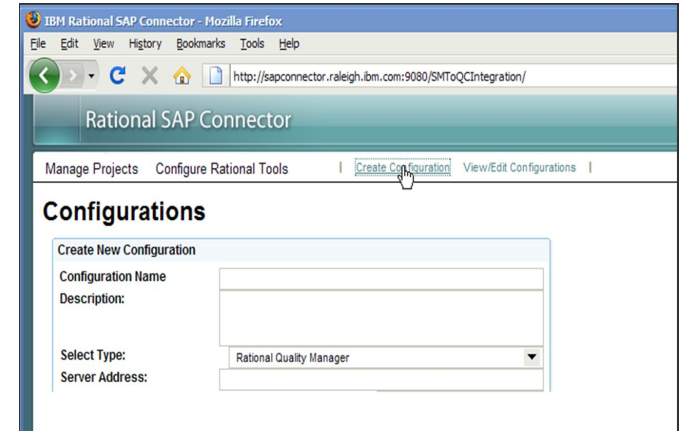


Outbound

- Business Blueprint
- Bus. Requirements
- Test Objects
- Documents
- Incidents

Inbound

- Test Results
- Incidents



Integrated Manual test authoring and execution

Step	Description	Expected Results
1	Start Classics Application	This window should appear.
2	Select a CD. User browses to Schubert and selects String Quarter	
3	Order the selected CD. Press the Place Order Button. The Place Order Window appears with Schubert as a selected item.	
4	Insert CC Number	
5	Validate Trent Cuplit	
6	Press the	
7	Press the OK Button	
8	OK Button	

#	Type	Result	Description	Attachment
1	Step	Passed	Select a cd and click Order button	
2	Step	Passed	Verify the login window displays	
3	Step	Passed	Select new customer radio button and select OK button	

- Manual test author and execute
 - ▶ Step by step capture and execution of manual tests
 - ▶ Assisted data entry
 - ▶ Keyword support for integrated manual and automated testing
 - ▶ Rich defect capture during execution, including screenshot and attachments
 - ▶ Simple intuitive interface for quick test execution

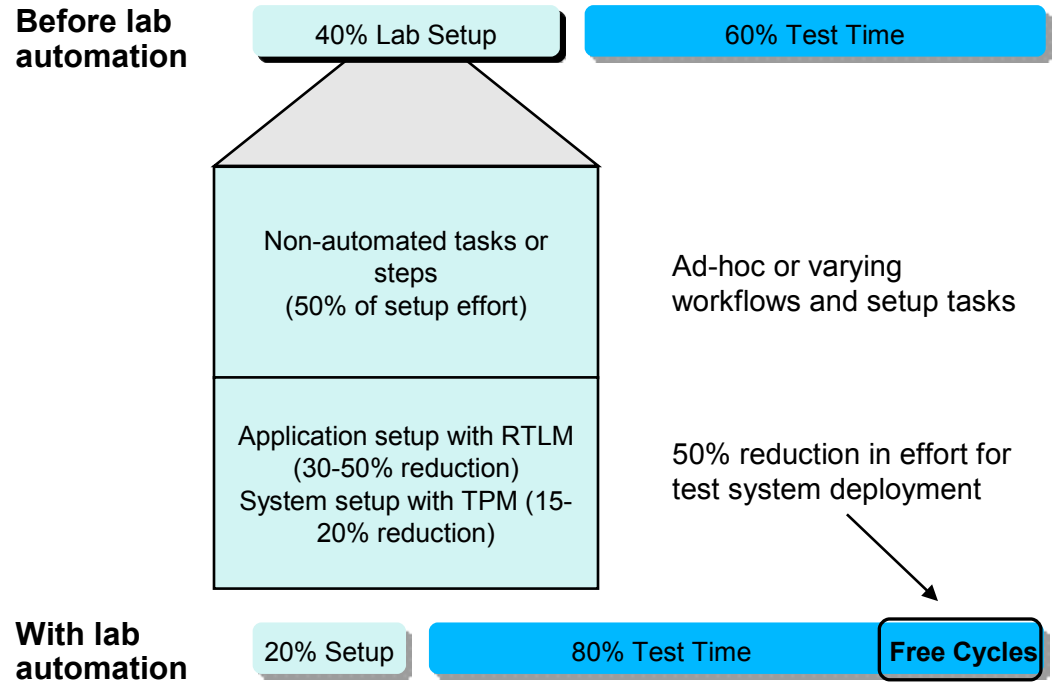
Maximizing efficiency of manual testing



Test lab automation and management

Insight and control over the test lab

- Manage
 - ▶ Verify that I have the resources required to fulfill my test plan
- Deploy
 - ▶ Deliver the configurations my teams require for test
- Optimize
 - ▶ Analyze patterns to minimize cost and maximize utilization



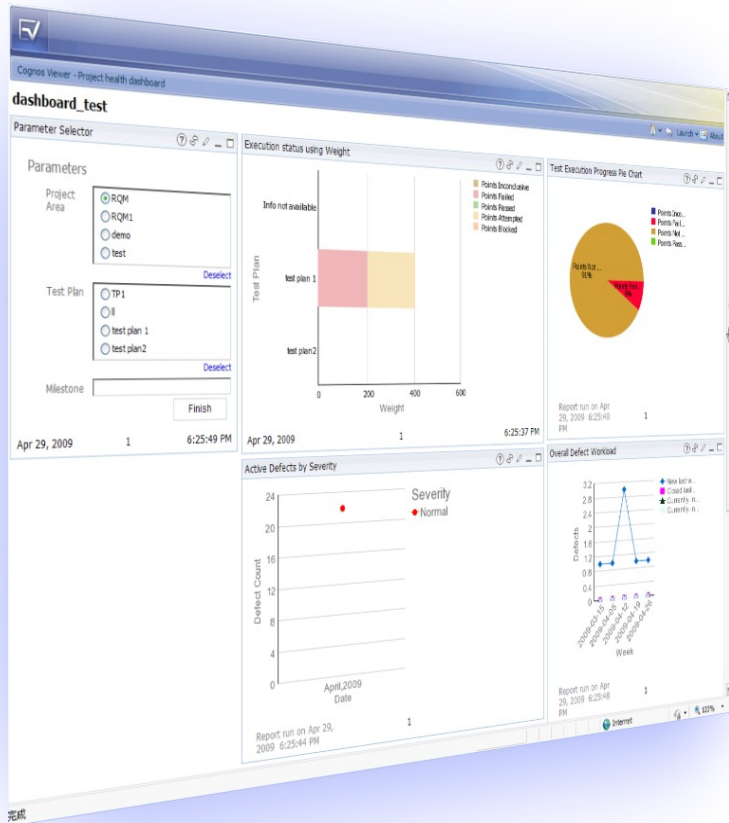
Source: IBM

Work smarter, save on test lab overhead, infrastructure and duration costs



Make confident decisions with effortless reporting

Closed Loop Analysis & Reporting



- Customizable reports and dashboards
 - ▶ Reduce escalating cost of information gathering
 - ▶ Reduce risk by identifying trends before they become issues
 - ▶ Raise enterprise visibility and transparency to reduce costs and risk
 - ▶ Measures the effectiveness of processes and practices to improve organizational and business outcomes

Make the right decisions at the right time



Rational Quality Manager Open Ecosystem Today

Rational. software



Tivoli. software

Automated Testing

- Rational Functional Tester
- Rational Performance Tester
- Rational Service Tester for SOA Quality
- Rational AppScan Tester Edition
- Test RealTime
- Rational Robot
- Rational Rhapsody

Builds, WorkItems and Defects

- Rational ClearQuest
- Rational Team Concert
- Rational BuildForge

Reporting

- Rational Insight

Requirements

- Rational Requirements Composer
- Rational ReqPro
- Rational DOORS

Provisioning

- Tivoli Provisioning Manager (TPM)
- Tivoli Service Request Manager
- TADDM



RapidRep



Supporting bidirectional integration with the Jira change management system



DeviceAnywhere™
by Mobile Complete

Managing mobile applications testing across a global handset test environment



Accelerating test cycles with virtual machine management and execution



Quick Test Professional LoadRunner



TMAP Process



Enabling greater quality and productivity with automated SOA governance support



Quality Management Portfolio Update

Team based, business driven software quality

- IBM Rational Quality Management
- Rational Functional Testing
- Rational Performance Tester
- Rational IT Web Security



Maximize your investment in test automation

With IBM Rational Functional Tester

- Achieve success quickly and minimize maintenance
 - ▶ Simplified natural language scripting with Storyboard testing
 - ▶ Eclipse based or Visual Studio .net
 - ▶ Easy to learn
 - ▶ Maximize reuse

- Complete test coverage
 - ▶ Supports testing for Java, Web, Visual Basic .Net, SAP, Siebel, Web 2.0, Power Builder and Terminal Based applications
 - ▶ Ability to support custom controls

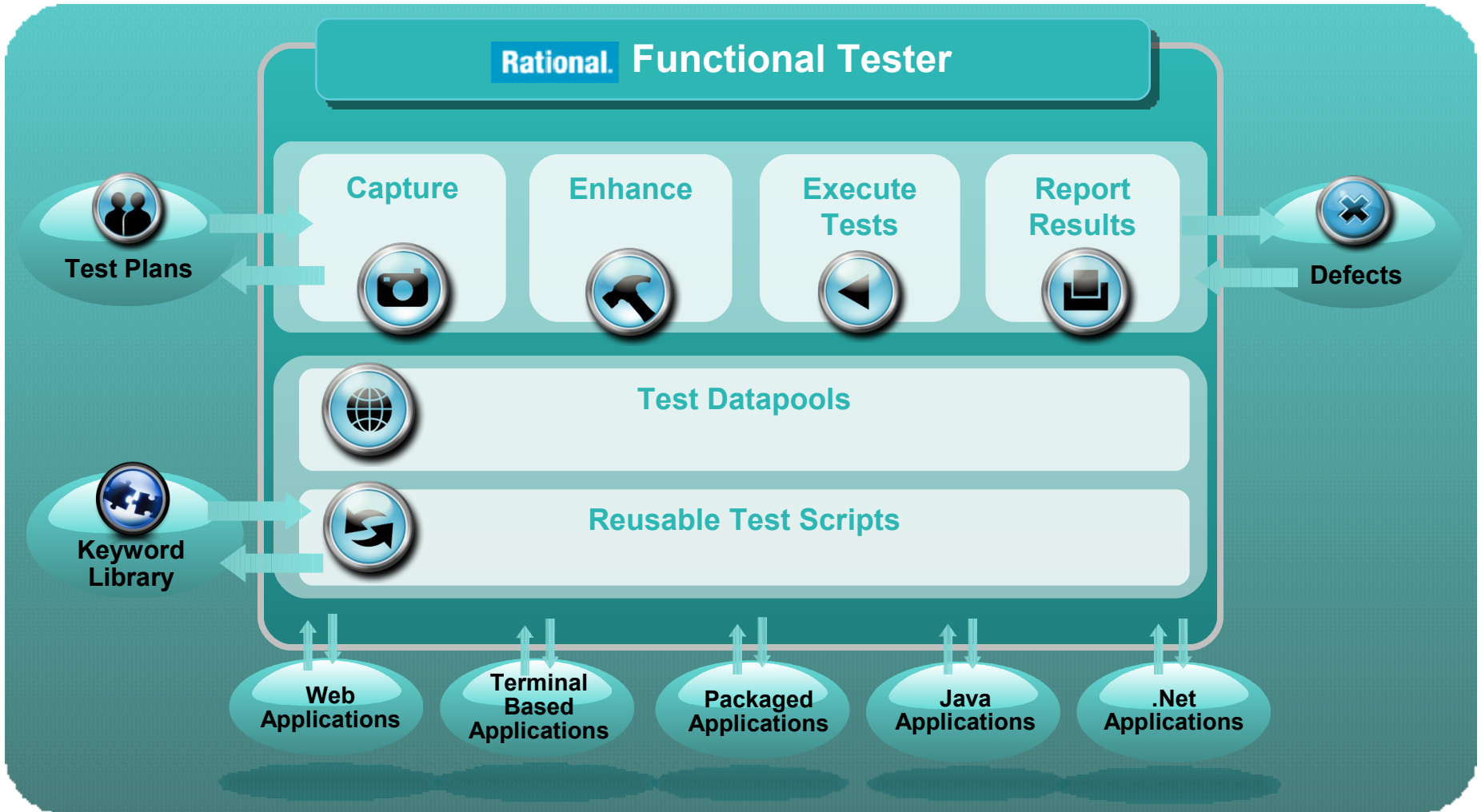


System z

System i



Rational Functional Tester 8.1

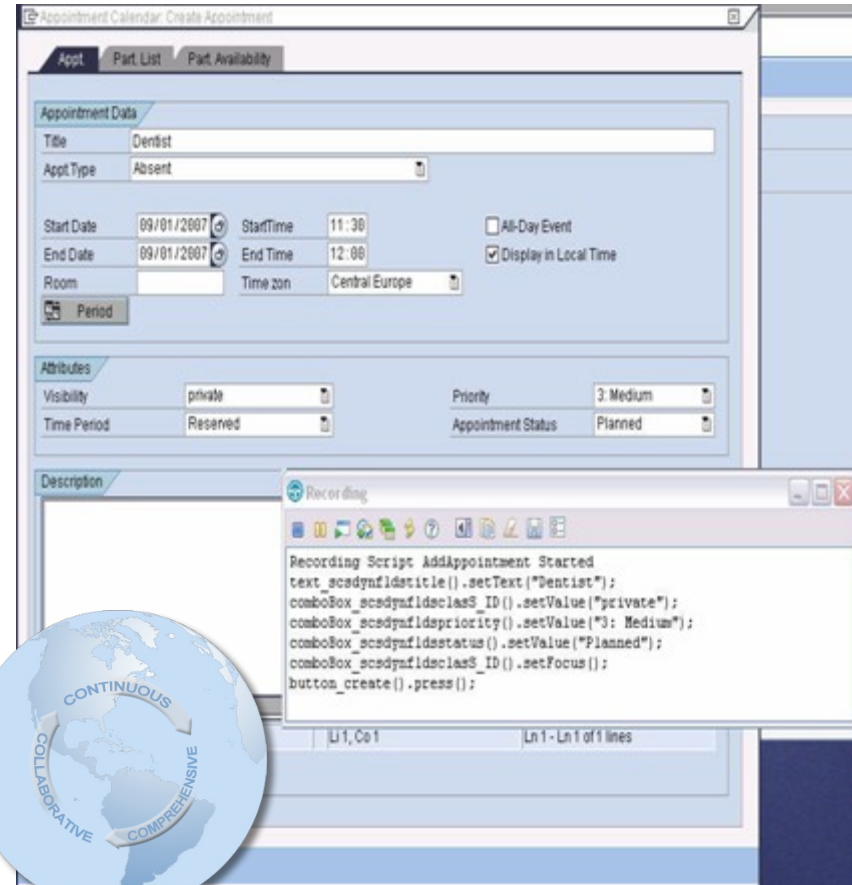


IBM Rational Functional Testing in SAP® deployments

Test SAP® customizations before they go live

- SAP® certified solution for SAP R/3 and SAP NetWeaver applications (BC-TEST-GUI 6.40)
- Integrates with the SAP® NetWeaver platform to exchange critical data with instances of the SAP Business Suite family of applications.
- Minimize test maintenance with scripts resilient to application changes
- Wizard enhanced automation to speed test creation for the new user
- Powerful scripting language and IDE integration for the professional tester provides a consistent, integrated environment for functional and performance testing
- Supports team oriented parallel development

SAP® Certified Integration



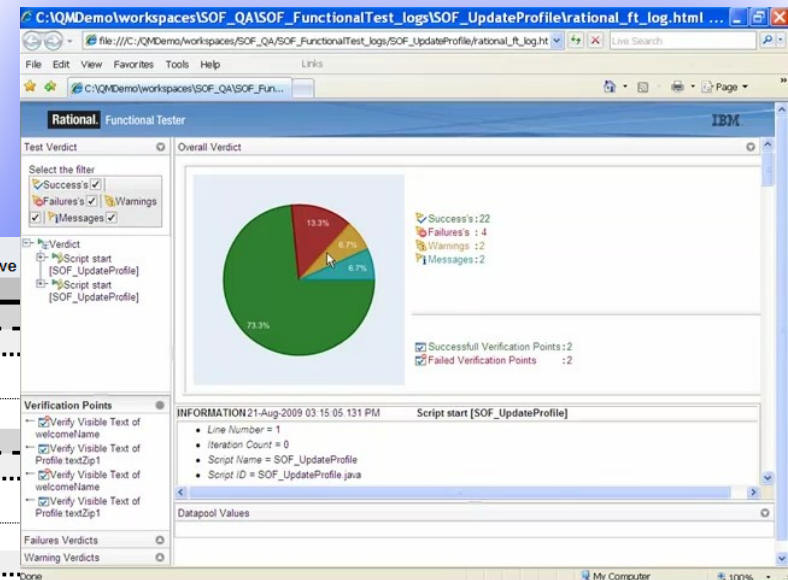


Executing Scripts

Reporting fits your organization's needs

- Following execution results can be viewed and stored in many ways:
 - Viewed and stored in an XML or HTML format
 - Centralized in Rational Quality Manager
 - Adobe® PDF 7 and 8 documents

Functional Tester XML



Rational Quality Manager

Test Iteration	Tester	Configuration	Test case	EWI ID	Weight	Points Passed	Points Failed	Points Blocked	Points Inconclusive
M0					320	160	0	0	0
	ADMIN	SAMPLE_AMDx86_WinXP_IE	Accessibility Web UI Test 3	3	95	95	0	0	0
	donald	SAMPLE_Intelx86_WinXP_Firefox	Performance Web Services Test 2	2	45	0	0	0	0
		SAMPLE_x86_Linux_Firefox	Accessibility Web UI Test 4	4	20	0	0	0	0
	larry	SAMPLE_Intelx86_WinXP_Firefox	Functionality Security Test 8	8	65	65	0	0	5



IBM Rational Quality Management

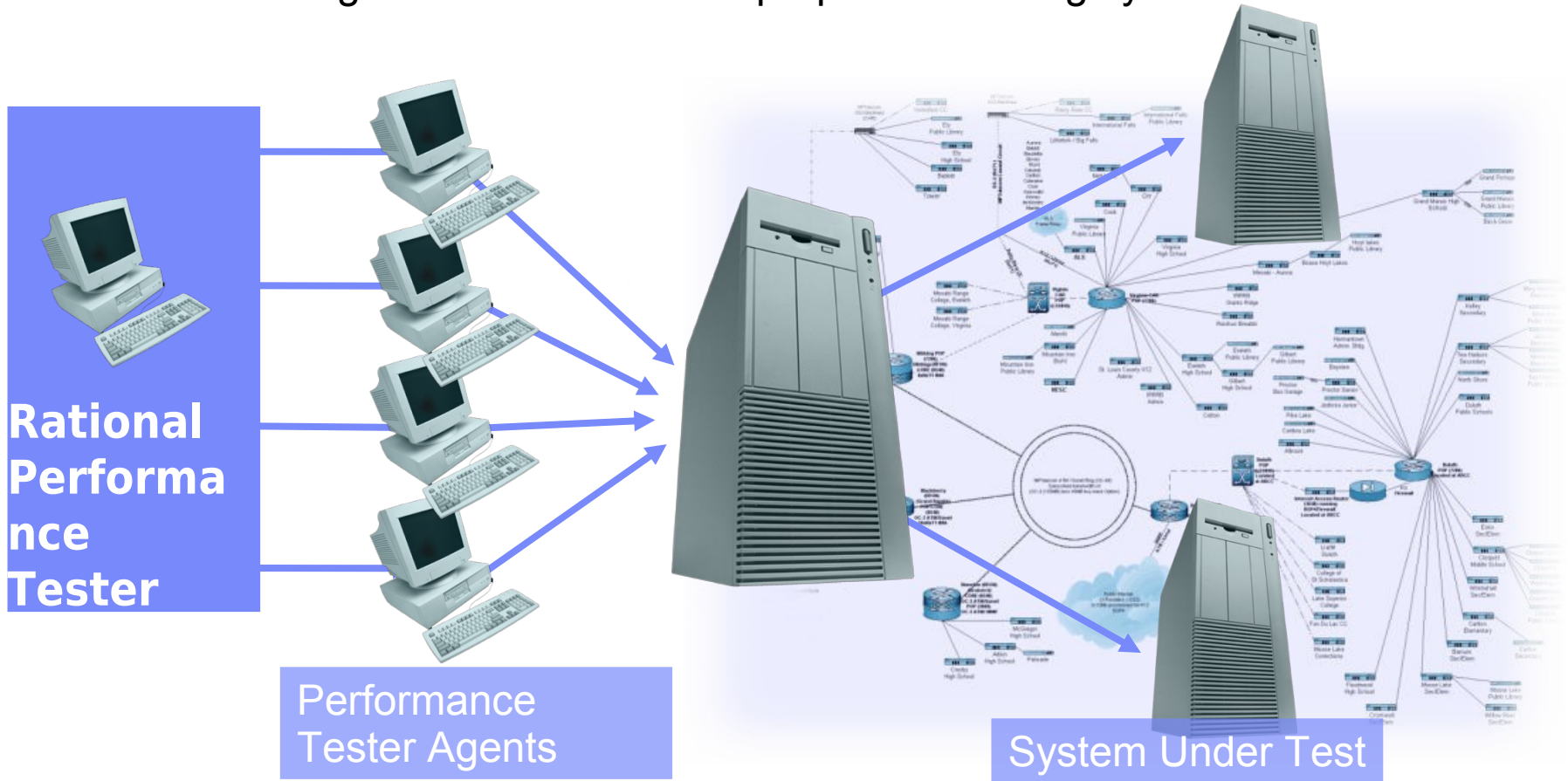
Quality Driven Software Delivery

- IBM Rational Quality Management
- Rational Functional Testing
- Rational Performance Tester
- Rational IT Web Security
- Summary



What Is Performance Testing?

- The process of exercising an application by emulating actual users with a load generation tool for the purpose of finding system bottlenecks



Performance Testing with IBM Rational Performance Tester

Test automation for the novice and the professional



■ IBM Rational Performance Tester

- ▶ Performance problem identification and diagnosis for Web, SAP, Siebel, Oracle and Citrix based applications

■ Performance test automation

- ▶ **Built for Day 1 Productivity**
 - Mask complexity to get the job done
- ▶ **Advanced Data Access & Manipulation**
 - Automated data variation and synchronization
- ▶ **Root Cause Analysis**
 - Identifies location and **root cause** of performance problem in hardware and software

Creating a Performance Test

Creating a performance test is a three step process



Build Scripts

Schedule Workload

Execute & Analyze

§ **Script Creation Considerations**

- 4 Visual test editor, varying input data & correlating server responses

§ **Scheduling Considerations**

- 4 Accurately representing a true user workload

§ **Execute and Analyze Considerations**

- 4 Validating responses & finding the bottleneck

IBM Rational Performance Testing for SAP®

Maximize the performance and scalability of business-critical applications

SAP® Recorder

Enables users to easily capture all SAP transactions using SAPGUI

Provides full visibility into all SAP activities

SAP® Protocol Browser

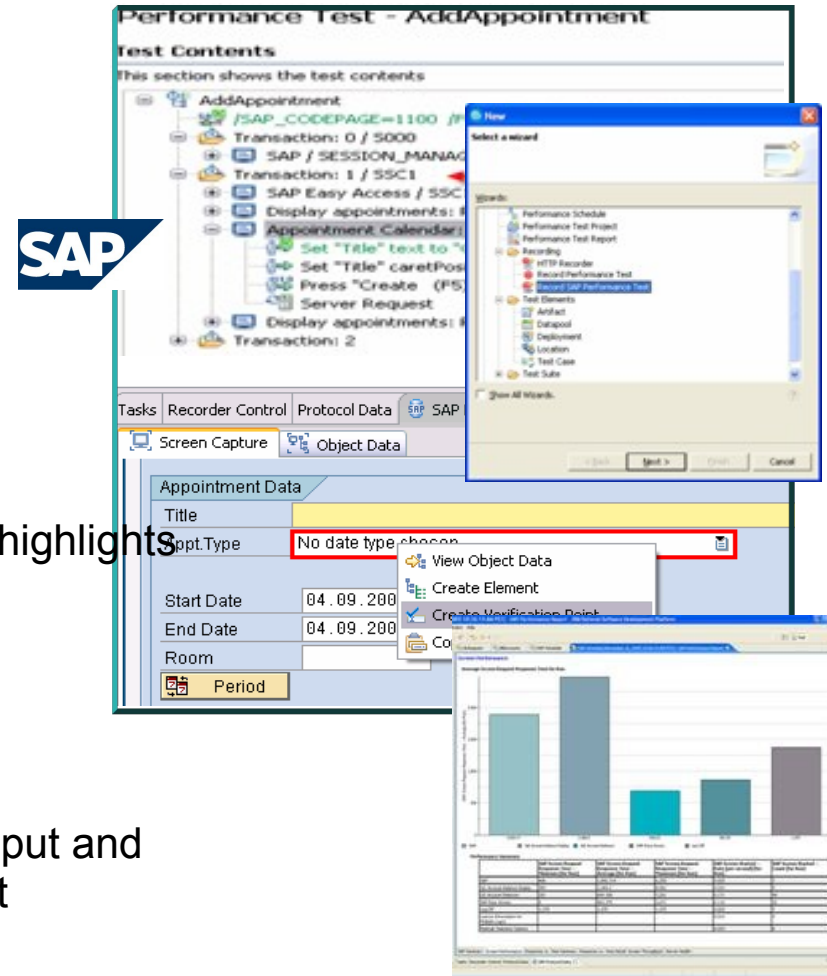
Enables users to easily read and edit tests

Shows a screenshot of SAP screen being tested and highlights the individual objects that are acted upon

SAP® Performance Reports

Enables users to quickly pinpoint bottlenecks

Reports on slow pages, server health, screen throughput and response times for all pages throughout the entire test



IBM Rational Performance Testing for SAP® Portal

Maximize the performance and scalability of business-critical applications

New and Enhanced!

Resource Management

Welcome

Request has been Copied to a new Request.

Choose

- [Overview](#)
- [Requests](#)
- [Roles](#)
- [SP Worklist](#)

- [Create FS Request](#)
- [Create Corp request](#)
- [Open Request/Role](#)

- [My Profile](#)
- [My View](#)
- [CM View](#)
- [RM View](#)

Request

Save
Broadcast Req
Check
Submit Req
Email

Req. Type	Project	Req-ing Country	Brazil	Customer Name		Status	
Req. Name	Load-Test 2008-12-01-001	Req-ing SRegion		Requester Name			
Created	01.12.2008	RO-Header Group		RO-Header Name			

Request Header

Roles

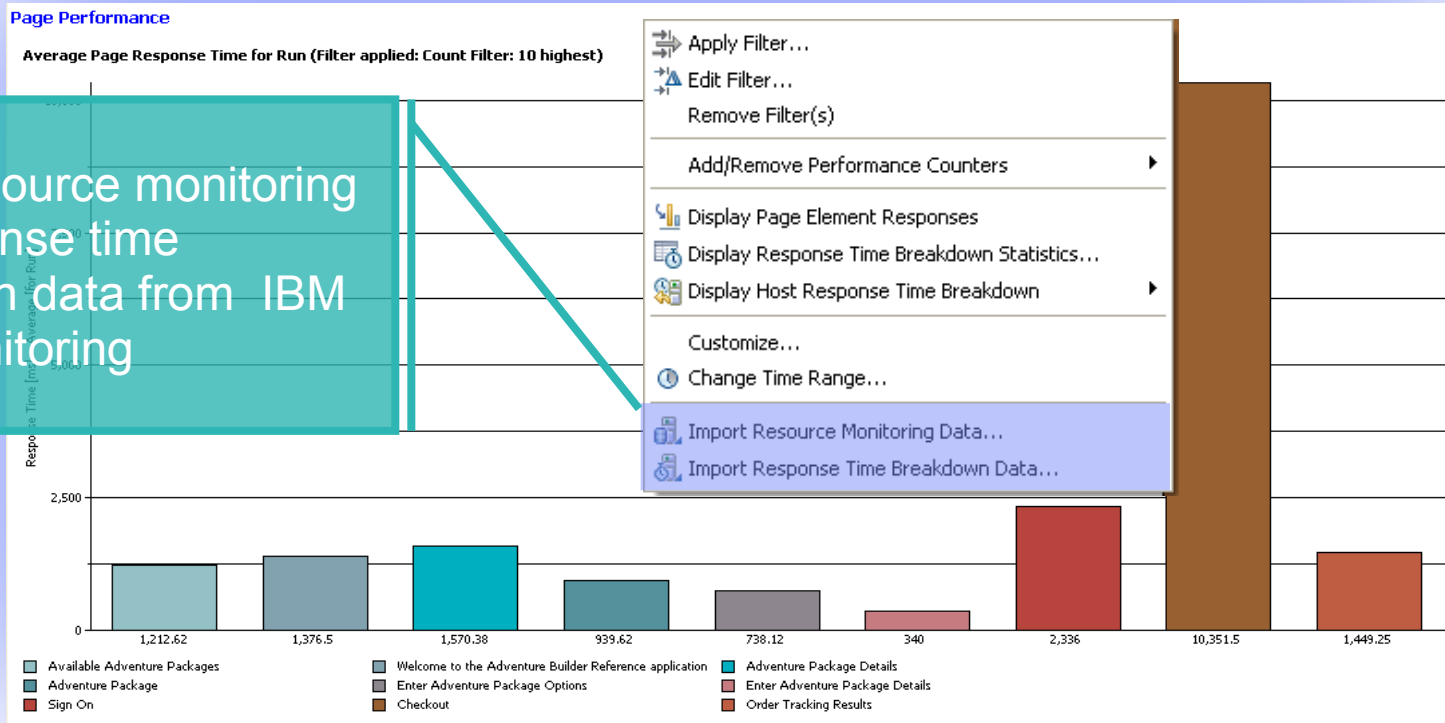
Request Details

Req Type: *	Project	Req. Name: *	Load-Test 2008-12-18_001	Request Status:	
Requester Name: *	00001181	Req. Priority:	Standard	Resp/ RM Org: *	Consulting
Requesting LOB:	FS- Consulting	PTC(Header):		RO-Header Name:	
Req-ing Country: *	Brazil	Origin of Request:		Services Sales Org:	

- Improved Support for SAP Netweaver Portal applications
- Supports full automatic data correlation for Java and ABAP Webdynpro
- Reduces test development time

IBM Tivoli Monitoring Import

Resource Monitoring data import from IBM Tivoli Monitoring



§ Additional data can be imported from IBM Tivoli Monitoring tools

- Gain insight for problem diagnosis of WAS, DB2, MQSeries, SNMP (MIB-II only), zOS, Oracle DB, Citrix

IBM Rational Quality Management

Quality Driven Software Delivery

- IBM Rational Quality Management
- Rational Functional Testing
- Rational Performance Tester
- Rational IT Web Security
- Summary



Warum ist Anwendungssicherheit wichtig?

- **Web Applikationen stehen an erster Stelle der Hacker Attacken**
 - ▶ 75% aller Attacken betreffen die Applikationsschicht (Gartner)
 - ▶ “XSS” und “SQL Injection” stehen an erster und zweiter Stelle der Attacken
- **Die meisten Seiten sind angreifbar**
 - ▶ 90% aller Seiten sind angreifbar durch Applikations-Attacken (Watchfire)
 - ▶ 78% der einfach anwendbaren Attacken betreffen Web Applikationen (Symantec)
 - ▶ 80% aller Unternehmen werden bis 2010 mit Sicherheitsvorfällen konfrontiert werden (Gartner)
- **Web Applikationen sind für Hacker höchst interessant**
 - ▶ Zugriff auf persönliche Daten, Kundendaten, Unternehmensdaten, Kreditkarten usw.
- **Compliance Anforderungen werden verletzt**
 - ▶ Basel II, Datenschutzgesetze, SOX, Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA.



Kosten fehlender Security

Hackers breach LexisNexis, grab info on 32,000 people

By [Paul Roberts](#)

IDG News Service, 03/09/05

Hackers have compromised databases belonging to LexisNexis and stolen information on at least 32,000 people, according to a statement Wednesday from LexisNexis' parent company, Reed Elsevier PLC.

The hackers stole passwords, names, addresses, Social Security and drivers license numbers of legitimate customers of the company's Seisint division. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis identified the incidents in a review of security procedures and warned that there may be more incidents of data theft, Reed Elsevier said. The incident is eerily familiar to recent revelations about similar compromises at Seisint competitor ChoicePoint, which [acknowledged](#) in February that hackers had access to data on 145,000 people.

Reed Elsevier did not immediately respond to requests for comment.

LexisNexis, which acquired Seisint of Boca Raton, Fla., in September for \$775 million, expressed regret for the incident and said it is notifying the individuals whose information may have been accessed and will provide them with credit monitoring services.

The U.S. Secret Service is actively involved in an investigation of the incident, but declined to give any details about the case through spokesman Jonathan Cherry.

Like ChoicePoint, Seisint
Security numbers, credit
"Multistate Anti-Terrorism



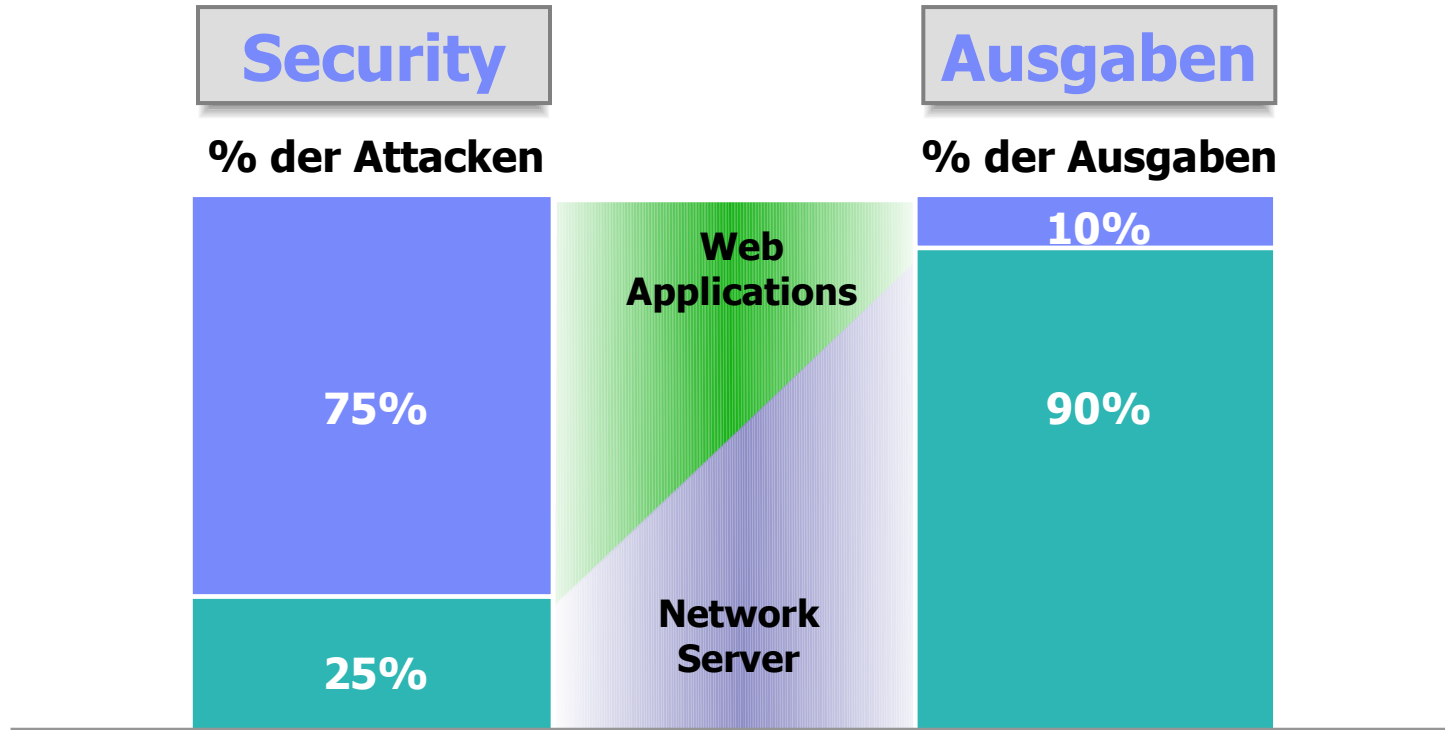
Social
behind the
and public



- Mediale Aufmerksamkeit
- Beschädigung der Marke
- Stark sinkende Aktienkurse
- Hohe Kommunikationskosten
- Gesetzliche Strafen
- Verstärkte Audits
- Klagewelle von Kunden
- Verlust von Kunden



Ausgabenverteilung für Security



75% aller Attacken auf Informationssicherheit finden im Web Application Layer statt

2/3 aller Webanwendungen sind gefährdet.

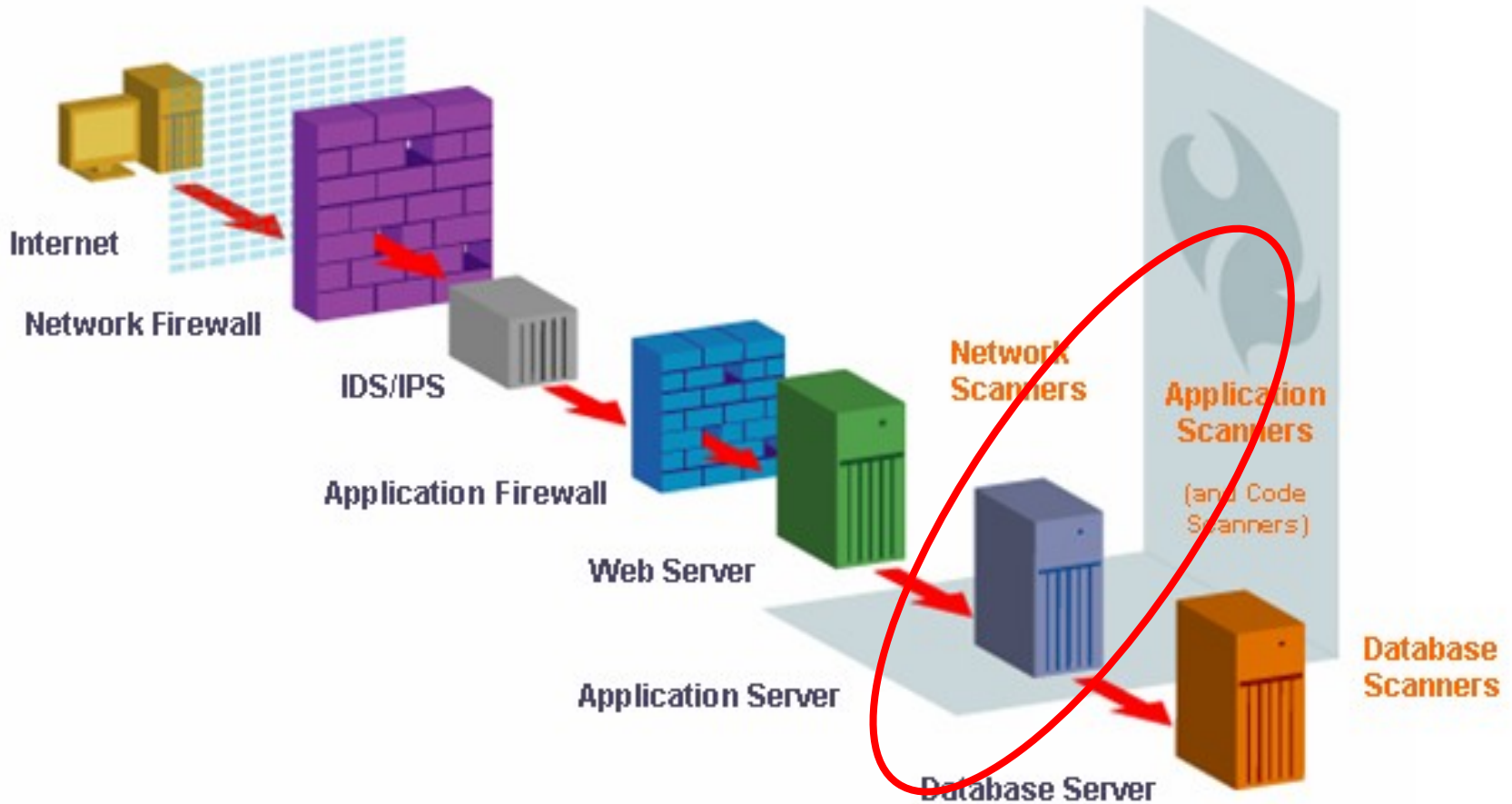
Gartner

Sources: Gartner, Watchfire

Warum ist Anwendungssicherheit wichtig?

- **Seit dem 1. September 2009 gilt ein neues Bundesdatenschutzgesetz!**
 - *"...Gehen beispielsweise personenbezogene Daten verloren, verschaffen sich Unbefugte Zugriff darauf oder werden sie unrechtmäßig an Dritte weitergegeben, **müssen** Unternehmen und Behörden dies künftig **veröffentlichen** (Novelle II des Bundesdatenschutzgesetzes BDSG, §42a). Festgelegt ist auch, dass Unternehmen die von den Datensicherheitsverletzungen **Betroffenen informieren** müssen. Dies kann schlimmstenfalls bedeuten, dass sie sich an Millionen von Betroffenen beispielsweise über Anzeigen in Tageszeitungen wenden müssen..."*
- **Web Applikationen sind für Hacker höchst interessant**
 - Zugriff auf persönliche Daten, Kundendaten, Unternehmensdaten, Kreditkarten usw.
- **Compliance Anforderungen werden verletzt**
 - Basel II, Datenschutzgesetze, SOX, Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA.

Einordnung von Webanwendungssicherheit



(IDS=Intrusion Detection System, IPS=Intrusion Prevention System)

... und die Security Lücken

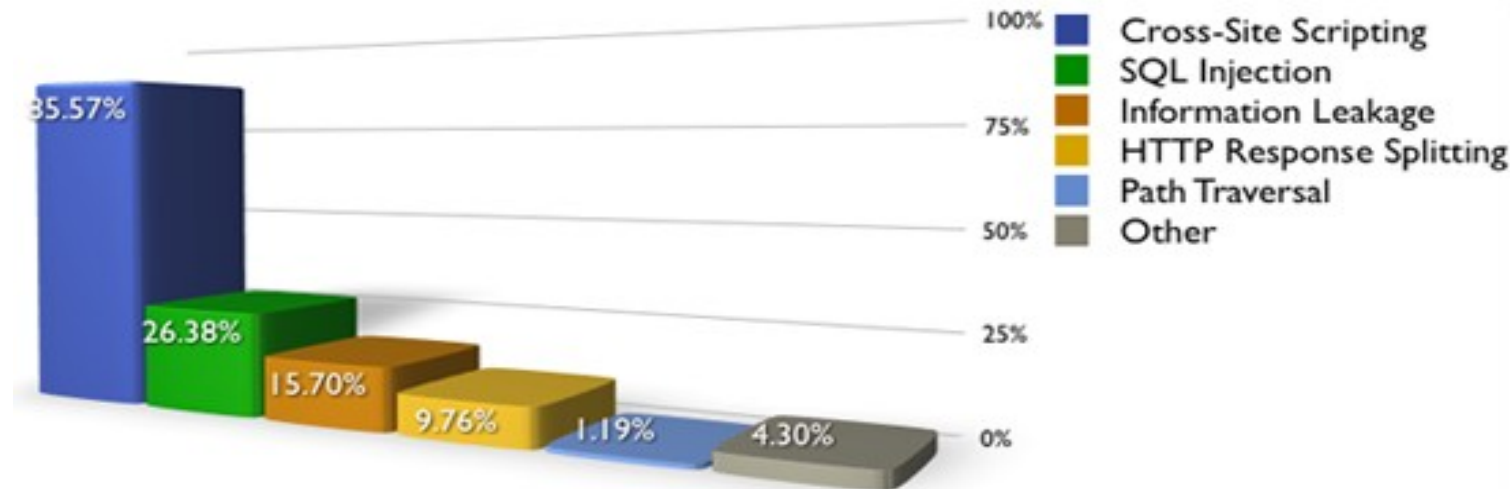
1. **“Cross-Site Scripting” (XSS)**
2. “Injection Flaws”
3. Verstecktes Ausführen einer Datei
4. Unsichere “Direct Object Reference”
5. Verfälschung eines “Cross-Site Requests”

Top Ten des “Open Web Application Security Project” (OWASP)

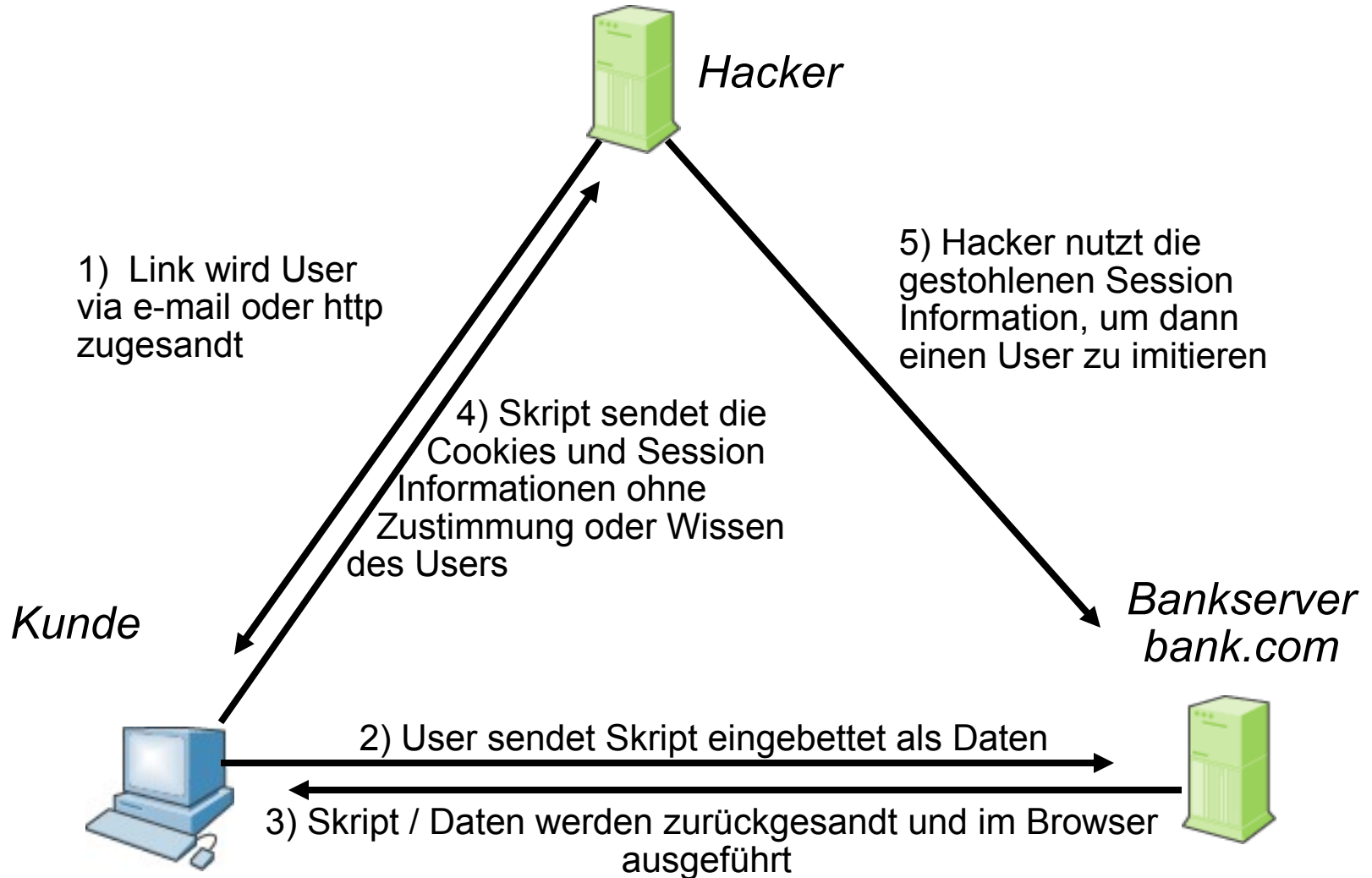
1. Informationsverlust und unsaubere Fehlerbehandlung
2. Broken Authentication & Session Management
3. Unsichere Kryptografie Speicherung
4. Unsichere Kommunikation
5. Fehlerhafte Abwehr von URL Zugriffen

Schwachstellen Statistik
(31.373 Seiten)

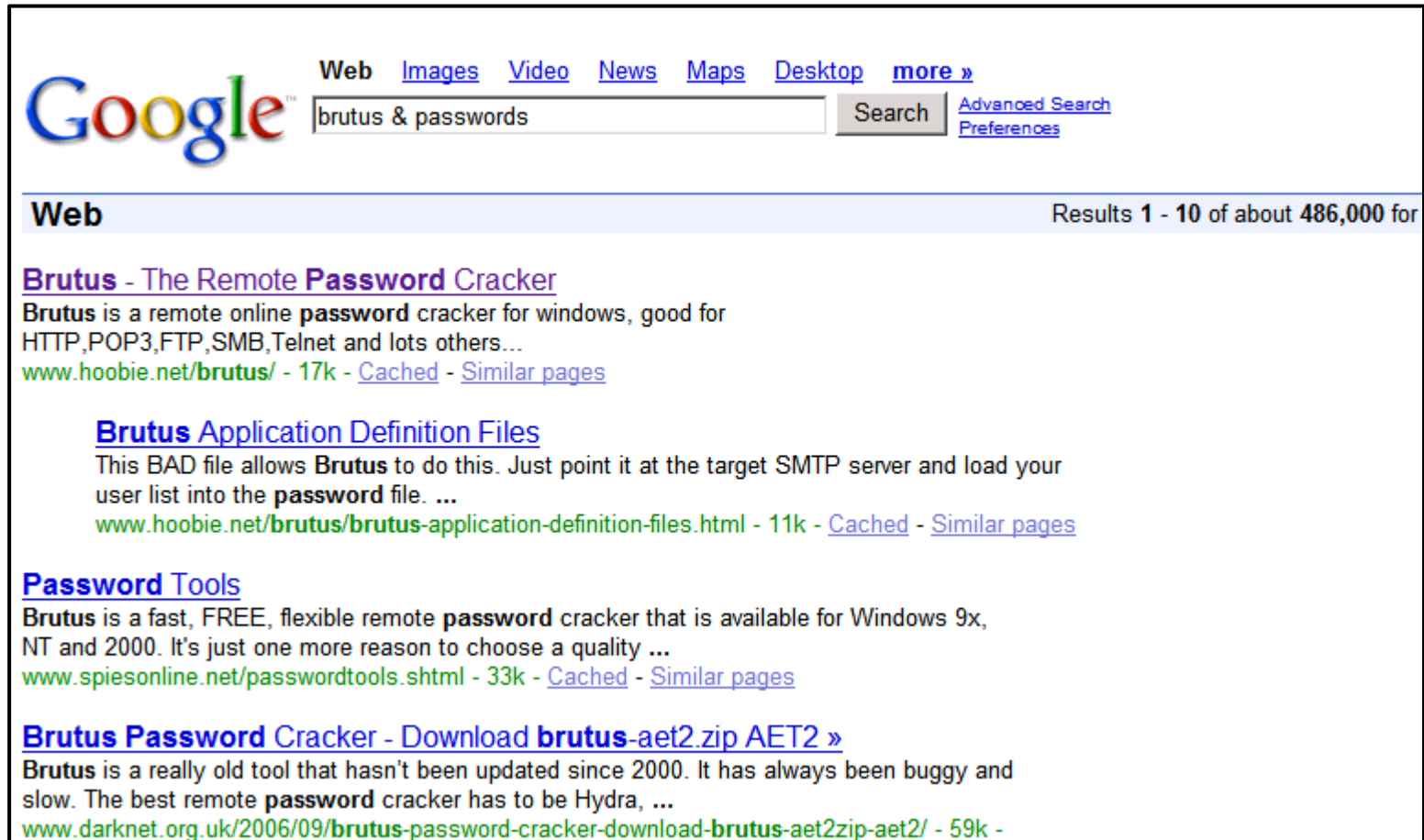
Percentage of websites vulnerable by class (Top 5)



XSS – Beispiel Bankanwendung - Prozess



Brute Force Tools sind einfach zu finden...



Google [Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [Desktop](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

Web Results 1 - 10 of about 486,000 for

[Brutus - The Remote Password Cracker](#)
Brutus is a remote online **password** cracker for windows, good for HTTP,POP3,FTP,SMB,Telnet and lots others...
www.hoobie.net/brutus/ - 17k - [Cached](#) - [Similar pages](#)

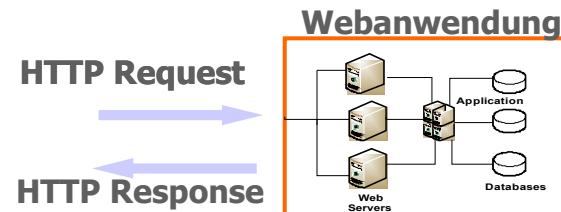
[Brutus Application Definition Files](#)
This BAD file allows Brutus to do this. Just point it at the target SMTP server and load your user list into the **password** file. ...
www.hoobie.net/brutus/brutus-application-definition-files.html - 11k - [Cached](#) - [Similar pages](#)

[Password Tools](#)
Brutus is a fast, FREE, flexible remote **password** cracker that is available for Windows 9x, NT and 2000. It's just one more reason to choose a quality ...
www.spiesonline.net/passwordtools.shtml - 33k - [Cached](#) - [Similar pages](#)

[Brutus Password Cracker - Download brutus-aet2.zip AET2 »](#)
Brutus is a really old tool that hasn't been updated since 2000. It has always been buggy and slow. The best remote **password** cracker has to be Hydra, ...
www.darknet.org.uk/2006/09/brutus-password-cracker-download-brutus-aet2zip-aet2/ - 59k -

Was ist IBM Rational AppScan?

- Ein automatisiertes Testtool zum Aufdecken von Sicherheitslücken in Webanwendungen
- Zweistufiges Vorgehen:
 1. „Auslesen“ der URL-Struktur und Scan der Seiten, um potentielle Angriffspunkte zu finden und zu listen.
 2. Test der gefundenen Angriffspunkte.
- Mehr als 2000 vordefinierte Sicherheits- und Compliantetests werden automatisiert durchgeführt
- Ein Expertenteam beobachtet laufend bekannte und neue Angriffsarten. Entwickelt neue und aktualisiert bestehende Tests und stellt diese per Update zur Verfügung.
- Ausführliche, konfigurierbare Reports zu den durchgeführten Tests. Zu den gefundenen Schwachstellen werden Maßnahmen zur Abhilfe vorgeschlagen.



Rational AppScan Standard Edition

The screenshot displays the IBM Rational AppScan Standard Edition interface. The main window title is "altoro_jsmith.scan - IBM Rational AppScan". The interface includes a menu bar (File, Edit, View, Scan, Tools, Help) and a toolbar with icons for Scan, Pause, Manual Explore, Scan Configuration, Scan Expert, Scan Log, Report, and Update.

On the left, there are three tabs: Security Issues (active), Remediation Tasks, and Application Data. Below these is a "Url Based" tree view showing the scan results for "My Application" (105 issues). The tree includes a root folder "http://www.althoromutual.com/" (105) and several sub-folders: "/" (4), "comment.aspx" (4), "default.aspx" (2), "disclaimer.htm" (2), "feedback.aspx" (1), "high_yield_investments.htm", "privacypolicy.aspx", "retirement.htm", "search.aspx" (1), "servererror.aspx", "subscribe.aspx" (9), "subscribe.swf" (1), "survey_questions.aspx", "admin" (4), "altoro" (1), "bank" (74), and "c:".

The main pane shows a list of security issues arranged by severity in descending order. The top issue is "Cross-Site Scripting (6)", which is expanded to show details for the "txtSearch" entity. The issue list includes:

- 105 Security Issues (741 variants) for 'My Application'
- Authentication Bypass Using SQL Injection (2)
- Cross-Site Scripting (6)
 - http://www.althoromutual.com/bank/customize.aspx (2)
 - http://www.althoromutual.com/comment.aspx (2)
 - http://www.althoromutual.com/search.aspx (1)
 - txtSearch
 - http://www.althoromutual.com/subscribe.aspx (1)
- Database Error Pattern Found (10)
- DOM Based Cross-Site Scripting (2)
- Inadequate Account Lockout (1)
- Predictable Login Credentials (1)
- Privilege Escalation using a Non-Authenticated User (8)
- Privilege Escalation using an Under-Privileged User (4)
- Session Identifier Not Updated (1)
- SQL Injection (6)
- SQL Injection File Write (requires user verification) (1)

Below the list, there are navigation buttons (Previous, Next) and dropdown menus for Severity (High) and State (Open). The "Issue Information" tab is active, showing details for the selected "Cross-Site Scripting" issue:

- Issue Information:** Cross-Site Scripting
- Severity:** High
- CVSS Metri... (7.5):** Base (High), Temporal (Medium), Environmental (Medium)
- URL:** http://www.althoromutual.com/search.aspx
- Entity:** txtSearch
- Security Risk:** It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.

At the bottom of the interface, there is a "Dashboard" section with an "Issue Severity Gauge" showing "Total number of issues: 105". A bar chart displays the distribution of issues by severity: 45 Critical (red), 13 High (orange), 19 Medium (yellow), and 28 Low (grey). The status bar at the bottom shows "Visited URLs 166/166", "Completed Tests 25355/25355", and a summary of "105 Security Issues" with counts for each severity level: 45 High, 13 Medium, 19 Low, and 28 Informational.

Rational AppScan Enterprise Edition

Rational. AppScan. Enterprise Edition
Jim (Analyst) | Help | Support | About | Log Out

Training
Jobs & Reports
Administration

Jobs & Reports > Acme Hackme > Analysts

Folders

Create... Edit Delete

- Acme Hackme
 - Analysts
 - Frank
 - Jim
 - Developers
 - Admin
 - Andrew
 - Chris
 - Jennifer
 - Templates

Analysts - Graphical

Last Updated: 9/11/2007 12:56:50 PM

Details Graphical

Report Pack: All Report Packs Apply

Issue Severity History

Issue Management History

Current Active: 2875

Issue Severity by Report Pack

WASC Threat Classification

Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank)
- Sarbanes-Oxley Act (SOX) (Investment)
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

Webanwendungssicherheit mit Ra

33

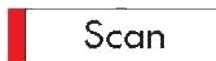
Basisoperationen der Rational AppScan Source Edition



Security Anforderungen: Ein Manager oder Sicherheits-
experte definiert Schwachstellen und wie diese beurteilt werden



Konfigurieren: Der Project Configuration Wizard hilft
Anwendungsscans aufzusetzen



Scannen: Code wird untersucht und Ergebnisse werden
geliefert.



Triage: Separieren von echten und potenziellen
Sicherheitslücken, um kritische Schwachstellen sofort beheben
zu können



Beheben: Eliminieren von Schwachstellen durch Code
Änderungen oder Hinzufügen von Sicherheitsfunktionen



Überprüfen: Rescan des Codes um sicherzustellen, dass die
Schwachstellen entfernt wurden

Eine Erfolgsstory mit mehr als 800 Referenzen

9 der Top 10 größten US Banken



8 der Top 10 Technologie Unternehmen



7 der Top 10 Pharma Unternehmen



Grosse Öffentliche Kunden



Referenzen in Deutschland:



THANK YOU

