

IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**



Enabling Security Testing across the Software Development Lifecycle with IBM® Rational® AppScan Enterprise Edition

Terry Goldman
Technical Evangelist,
Rational ASEAN
goldmant@sg.ibm.com

Security is Quality



The Myth: “Our Site is Safe”

**We Have Firewalls
in Place**

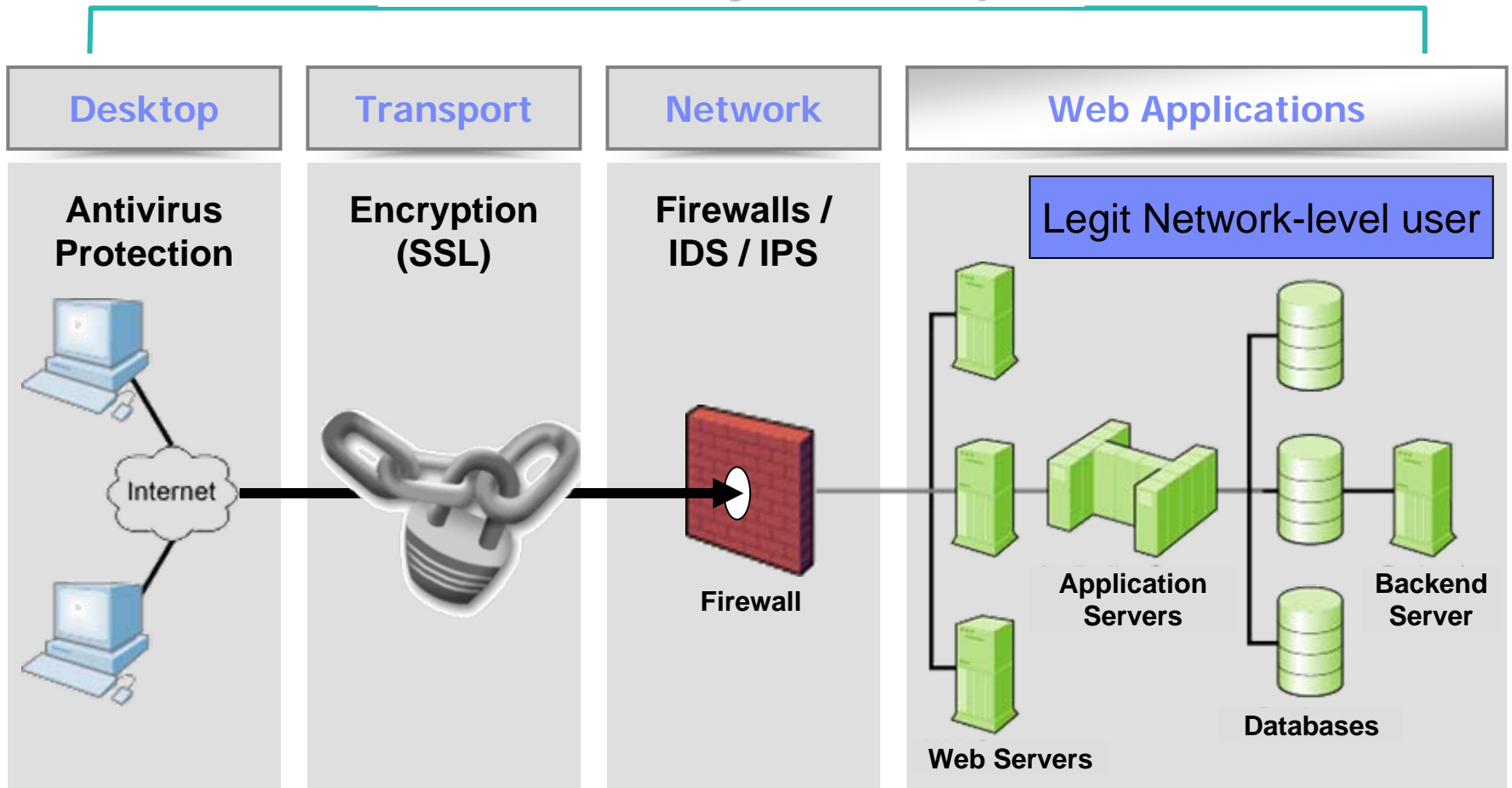
**We Audit It Once a
Quarter with Pen Testers**

**We Use Network
Vulnerability Scanners**



Each layer of the application requires its own security measures

Info Security Landscape



Web application security defects are common and serious

Growing Threat

- Past customer spending focused on Network security – yet 75% of attacks come through web applications – market is now focusing on spending on web application security
- Mitre group indicates that application issues (XSS and SQL Injection) are the top 2 hacks
- Most websites are vulnerable (Watchfire/Gartner)

Analyst Views

“Gartner estimates that **90 percent of externally-accessible applications today are web-enabled, and that two-thirds of them have exploitable vulnerabilities.**”

“**64% of developers are not confident in their ability to write secure applications**”

Microsoft Developer Research

Cost of Application Security Breach

- **Security Breach**
 - Every lost record costs \$138 to the organization who lost it
 - Media Attention > Brand Damage > Sharp Decline in Stock Prices



Regulatory requirements in many industries require you to develop and test to ensure system security



Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security



There are several types of web application security defects

Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, ...	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Execute shell commands on server, up to full control	Site modified to transfer all interactions to the hacker.
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Web application returns contents of sensitive file (instead of harmless one)
Cross-Site Request Forgery	Attacker can invoke "blind" actions on web applications, impersonating as a trusted user	Blind requests to bank account transfer money to hacker
Information Leakage and Improper Error Handling	Attackers can gain detailed system information	Malicious system reconnaissance may assist in developing further attacks
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly	Hacker can "force" session token on victim; session tokens can be stolen after logout
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted credentials "sniffed" and used by hacker to impersonate user
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access a page past the login page



For example, Injection Flaws are an important type of security defect that result from flaws in the application

- What is it?
 - ▶ User-supplied data is sent to an interpreter as part of a command, query or data.

- What are the implications?
 - ▶ SQL Injection – Access/modify data in DB
 - ▶ SSI Injection – Execute commands on server and access sensitive data
 - ▶ LDAP Injection – Bypass authentication



Altoro Mutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



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:

[Privacy Policy](#) | [Security Statement](#) | © 2006 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.

Altoro Mutual

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



[MY ACCOUNT](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details:

1001160140 Checking

Congratulations!

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

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | © 2006 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.



MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Recent Transactions

After Before

mm/dd/yyyy mm/dd/yyyy

TransactionID	AccountID	Description	Amount
20	1001160140	Rent	1100
21	1001160140	Deposit	1050.88
22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141	Deposit	878.9
77	1001160141	Deposit	881.1
1			

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.



DEMO

01/01/2006 union select userid,null,username+', '+password,null from users--

MY ACCOUNT

PERSONAL

INSIDE ALTORO MUTUAL

- I WANT TO ...
- View Account Summary
 - View Recent Transactions
 - Transfer Funds
 - Search News Articles
 - Customize Site Language

Recent Transactions

After Before

mm/dd/yyyy *mm/dd/yyyy*

TransactionID	AccountID	Description	Amount
20	1001160140	Rent	1100
21	1001160140	Deposit	1050.88
22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141	Deposit	878.9
77	1001160141	Deposit	881.1
1			

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74	1001160141	Deposit	878.9
77	1001160141	Deposit	881.1
265	1003160121	Deposit	150000
357	1005160101		878.85336
363	1005160101		879.95468
366	1005160101		882.15732
378	1006160141		878.85336
384	1006160141		879.95468
387	1006160141		882.15732
419	1006160141		150180
100116014		jsmith,Demo1234	
100216018		sspeed,Demo1234	
100316012		tuser,tuser	
100416016		admin,admin	
100516010		sjoe,Frazier	
100616014		cclay,Ali	
1			

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



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:

[Privacy Policy](#) | [Security Statement](#) | © 2006 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.



[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



[MY ACCOUNT](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Hello, Smoking Joe

Welcome to Altoro Mutual Online.

View Account Details:

1005160100 Checking

Congratulations!

You have been pre-approved for an Altoro Platinum Visa with a credit limit of \$12000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | © 2006 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.

A bug in the web application code causes this SQL Injection security defect

```
string sAfter = Request.Form["after"];  
string sBefore = Request.Form["before"];
```

Evil input comes in

```
string sSQL = "SELECT t.transid, t.accountid, t.description, t.amount  
FROM transactions t  
INNER JOIN accounts a ON t.accountid = a.accountid  
where t.trans_date >= " + sAfter + " and t.trans_date <= " + sBefore;
```

```
myTransactions = new OleDbDataAdapter(sSQL, myConnection);
```

Evil input gets concatenated into SQL Statement

SQL statement containing evil input gets executed. The result may not be what the developer intended.



The security defects we are talking about are bugs in the application itself

- What causes a security defect?
 - ▶ A coding problem in the application

- How do you fix a security defect?
 - ▶ Need to fix the bug

- Why are security defects so prevalent?
 - ▶ Human Gap: bugs happen
 - ▶ Knowledge Gap: many developers are just getting up to speed on security
 - ▶ Process Gap: security hasn't been part of the development process

- Why wouldn't we apply our best Quality Management practices to security defects?



Security Auditors and Quality Assurance Specialists have complimentary skills and responsibilities



- Knows security in-depth
- Knows corporate and industry standards
- Can exploit security defects to prove impact
- Is responsible for the security of application

- Makes testing repeatable
- Reports on test coverage, release readiness
- Triage and manages defects
- Scales testing effort across a large team
- Already part of the development process

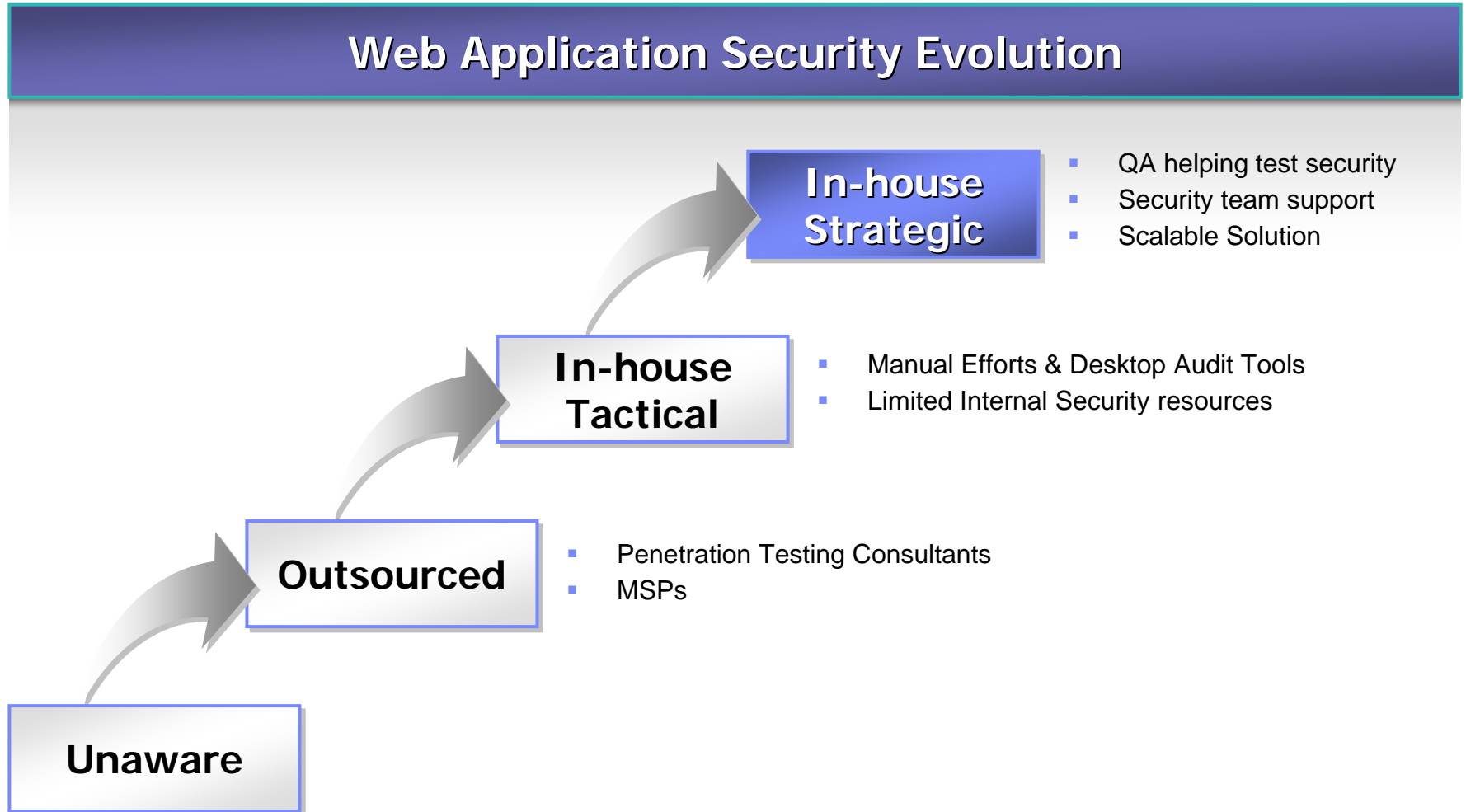


Web application security testing is about finding security defects, but it is also important to understand the issues and how they are fixed

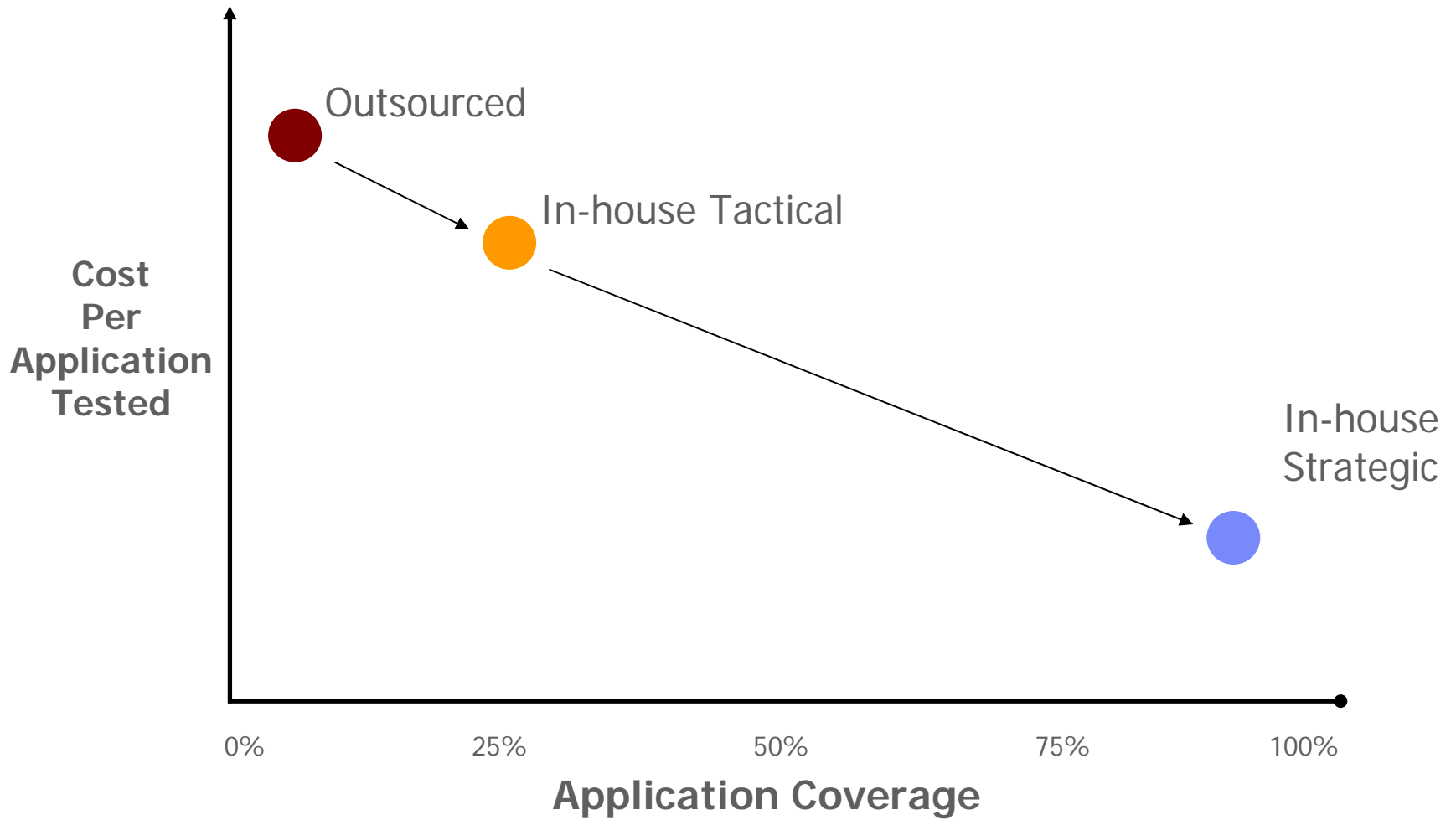
- Web Application Security (WAS) testing is the process of:
 - ▶ Identifying how a web application is vulnerable to being hacked, and
 - ▶ Providing fix recommendations to remediate the security issues



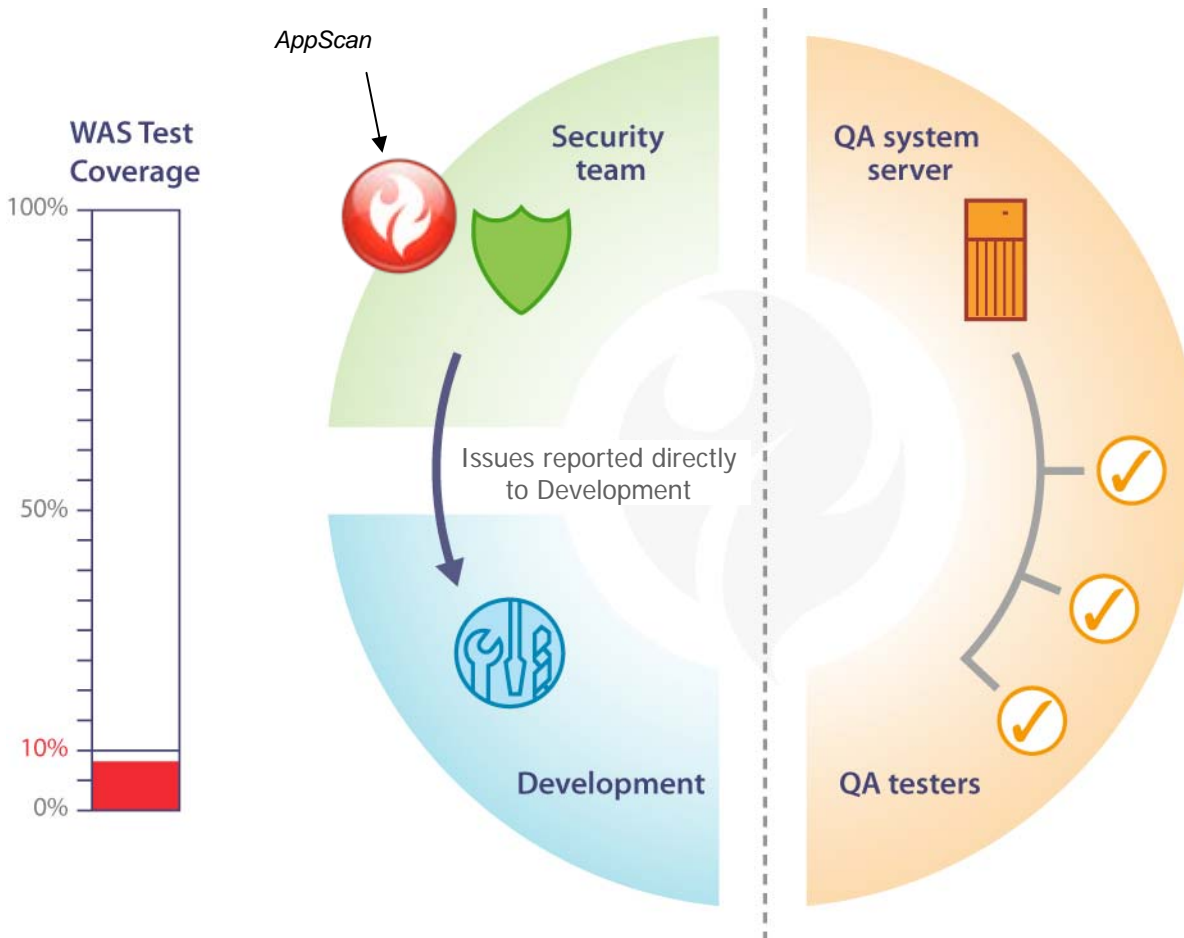
Many organizations move through a maturity model as they adopt web application security testing



The goal is to reduce cost of testing per application so that you can increase test coverage



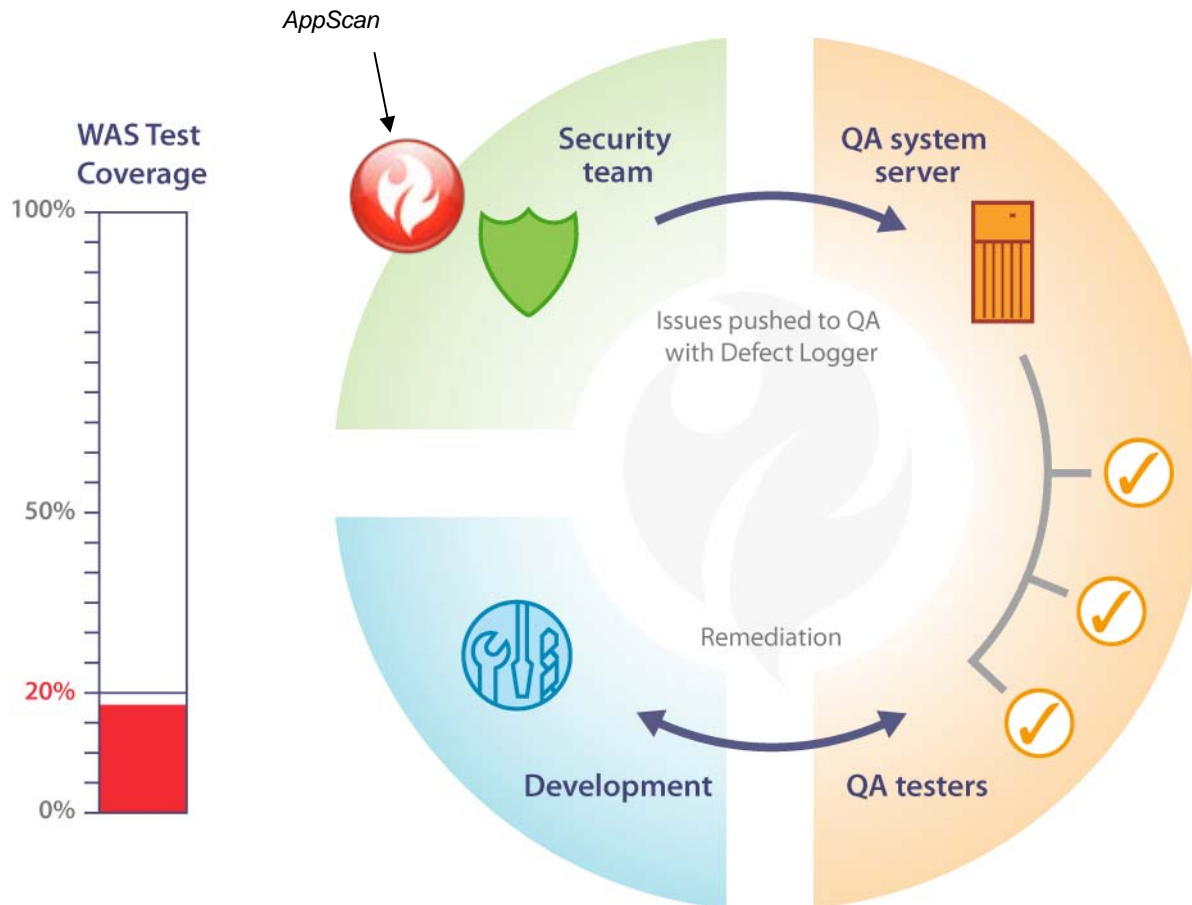
At first, there is little or no QA involvement in security testing and little test coverage is achieved



- No communication between Security & QA teams



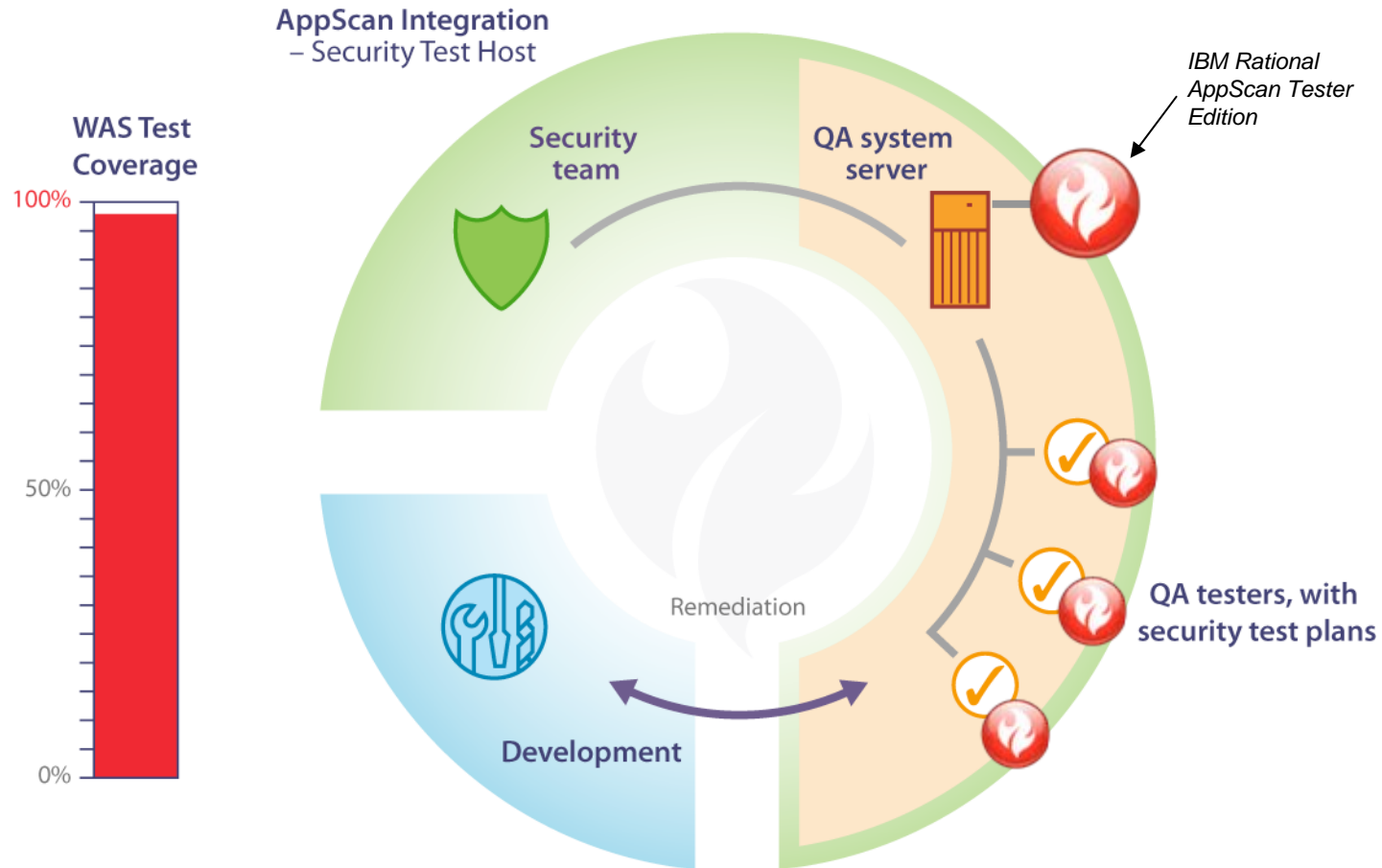
Later, QA becomes more involved in security testing and test coverage increases



- QA Introduced to WAS; process not yet formalized



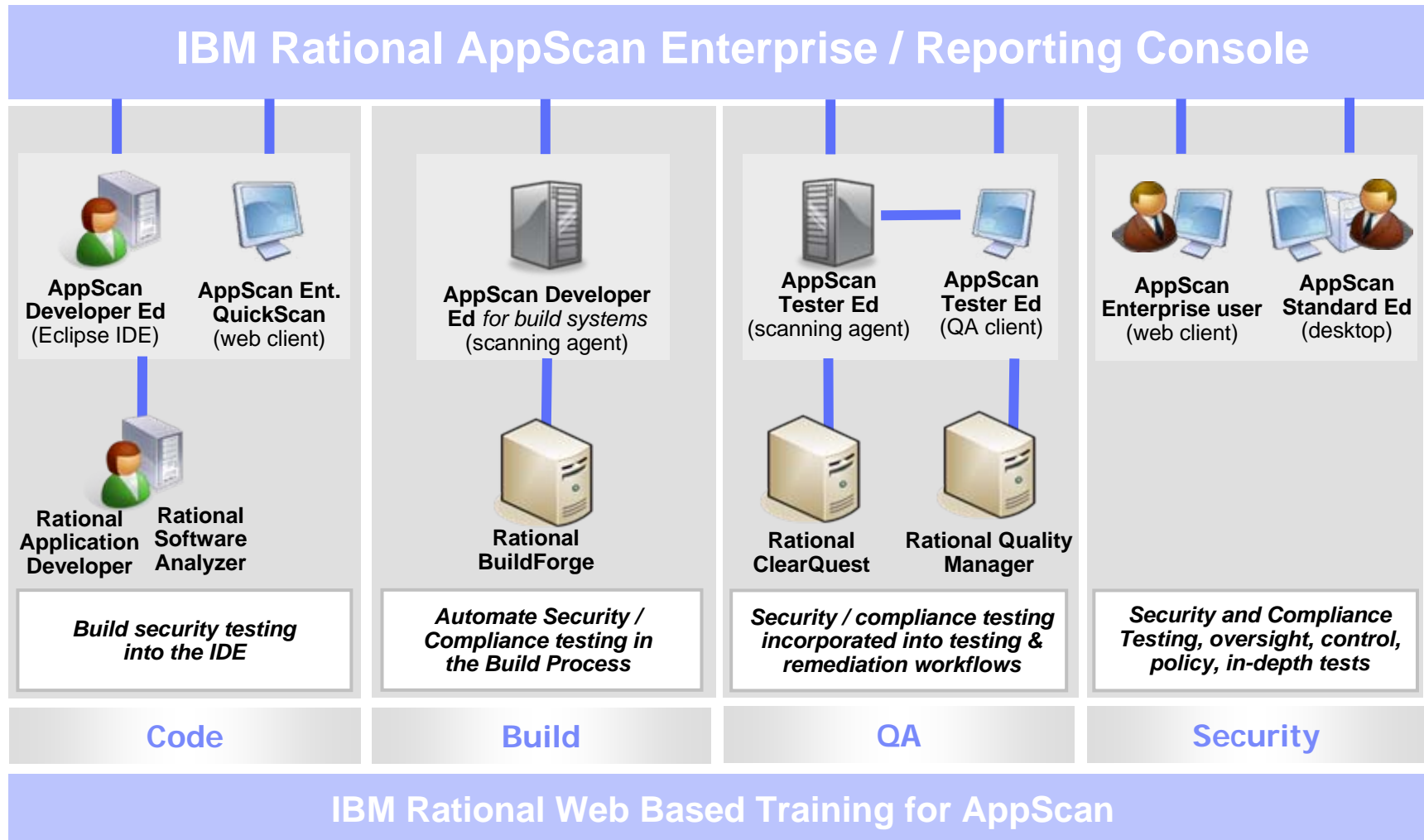
Finally, QA is fully engaged in security testing and test coverage approaches 100%



- QA responsible for WAS

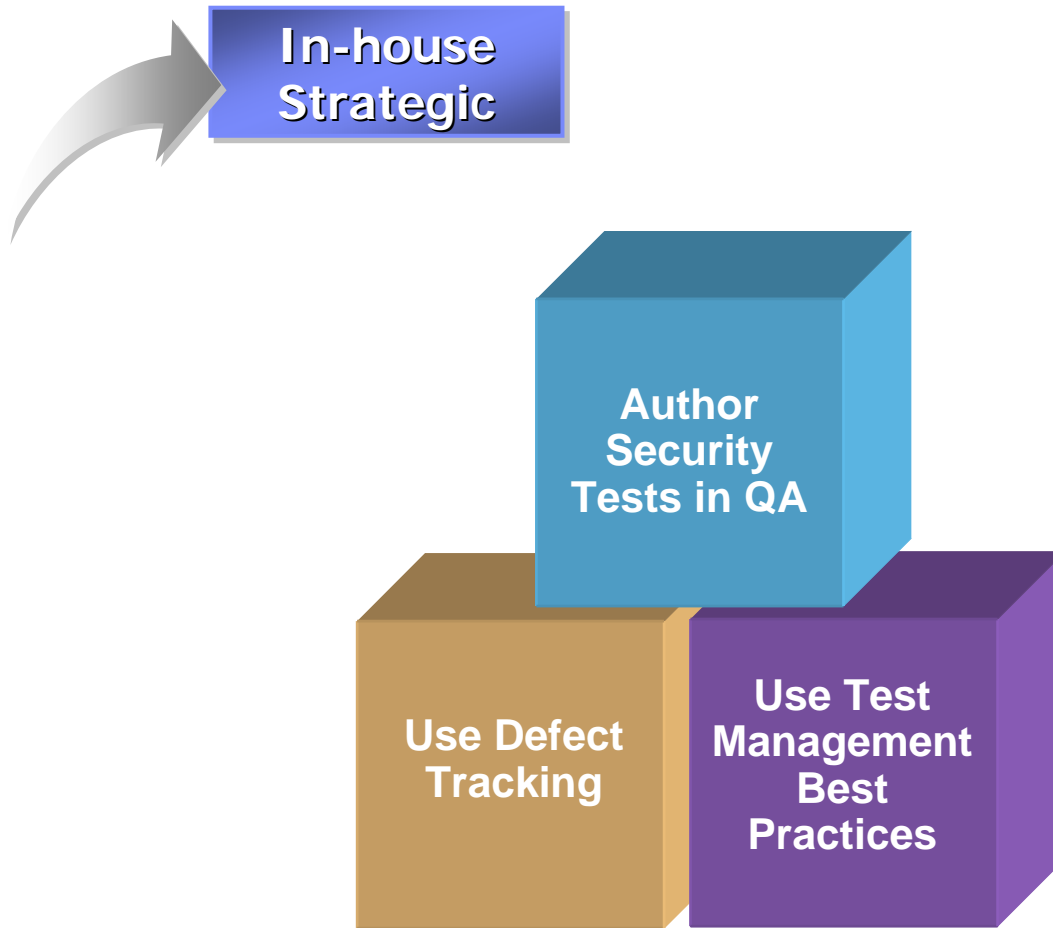


Security needs attention across the software development lifecycle



Phased Adoption of Security Testing in QA

Engaging your QA team in security testing, one step at a time



Using Rational AppScan Standard Edition with ClearQuest



The screenshot displays the Rational AppScan Standard Edition interface. The main window shows a scan of 'My Application' (54) at 'http://demo.testfire.net/'. A list of security issues is shown, including Blind SQL Injection (4), Cross-Site Scripting (5), Format String P, HTTP Respons, Session Not Inv, SQL Injection, XPath Injection, Cookie Poisoning, Directory Listing, Predictable Log, Unencrypted L, and Application Error. A context menu is open over the 'Cross-Site Scripting' issue, with the 'Log Defect to ClearQuest' option highlighted. An arrow points from this menu to the 'Defect Details' dialog box.

The 'Defect Details' dialog box contains the following information:

- Credentials:** Username: admin, Password: [redacted]
- Defect Details:** Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)
- Project:** [dropdown]
- Severity:** 1-Critical
- Priority:** solve Immediately (dropdown menu open showing: 1-Resolve Immediately, 2-Give High Attention, 3-Normal Queue, 4-Low Priority)
- State:** [dropdown]
- Keywords:** [dropdown]
- Symptoms:** [dropdown]
- Owner:** engineer
- Description:** SQL Injection, Application-level test, WASC Threat Classification: Command Execution: SQL Injection, Security Risk: It is possible to view, modify or delete database entries and tables
- Attachments:** Advisory.html, FixRec.html, Variant1-Ori..., Variant1-Tes..., Variant2-Ori..., Variant2-Tes..., Variant3-Ori...

At the bottom of the dialog, there are 'Cancel' and 'Log Defect' buttons.

Using Rational AppScan Tester Edition with Rational Team Concert

Use
Defect
Tracking

Rational AppScan Tester Edition

Welcome **Craig Conboy** Admin

Security Issues

Last Updated: 5/12/2008 10:33:51 AM

Summary Group Show Search Layout

There are **68** issues of 24 different types across 21 URLs

All items

Items 1-25 of 68

Go to page: 1 of 3 Apply

Action: Submit Rational Quality Manager Defect Apply

<input type="checkbox"/>		Status	Issue	Work It	Test URL	Element	Issue Type	Threat Class	Last Updated
<input type="checkbox"/>		Open	299*		http://qadcore1.otta	before	Blind SQL Injection	Command Execution:	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	300*		http://qadcore1.otta	uid	Blind SQL Injection	Command Execution:	5/12/2008 2:33:00 P
<input checked="" type="checkbox"/>		Open	301*		http://qadcore1.otta	passw	Blind SQL Injection	Command Execution:	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	305*		http://qadcore1.otta	_ctl0%3A_ctl0	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	306*		http://qadcore1.otta	creditAccount	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	307*		http://qadcore1.otta	debitAccount	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	308*		http://qadcore1.otta	txtSearch	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	309*		http://qadcore1.otta	lang	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P
<input type="checkbox"/>		Open	310*		http://qadcore1.otta	uid	Cross-Site Scripting	Client-side Attacks: C	5/12/2008 2:33:00 P



Using Rational AppScan Developer Edition with ClearQuest

The screenshot displays the Rational AppScan Developer Edition interface. On the left, the Project Explorer shows a project named 'tomchat' with various files and folders. The main window displays a 'Security Report' for 'MyScan - 07-05-08 14_19_35 PM.srpt'. The report lists several issues, with 'Cross-Site Scripting (1)' highlighted. The details for this issue are shown below, including severity, type, WASC Threat Classification, CVE Reference(s), and Security Risk. A 'Possible Causes' section indicates that 'Sanitization of hazardous characters was not performed correctly on user input'.

Overlaid on the report is a 'Create (Defect) SAMPL0000076' dialog box. The dialog has tabs for 'Main', 'Attachments', and 'Customer'. The 'Main' tab is active, showing the following fields:

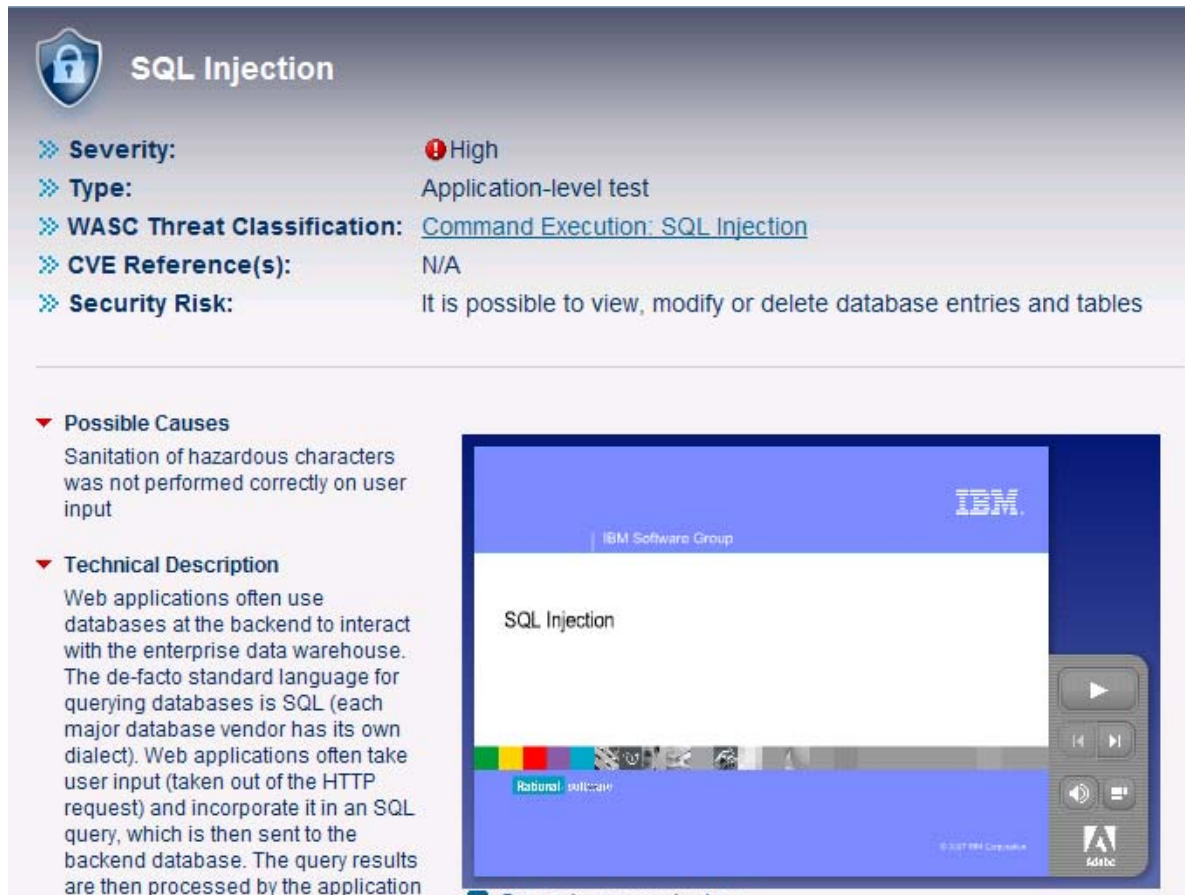
- ID: SAMPL0000076
- State: Submitted
- Headline: Cross-Site Scripting : http://localhost:8080/tomchat/login.jsp
- Project: [Dropdown]
- Severity: 2-Major
- Priority: [Dropdown]
- Owner: [Dropdown]
- Description: See attached Issue.html for more information.
- Template: [Dropdown]

Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog.



Use
Defect
Tracking

Detailed information about the security issue provides QA Managers with the information needed to triage defects




SQL Injection

- ❖ **Severity:** High
- ❖ **Type:** Application-level test
- ❖ **WASC Threat Classification:** [Command Execution: SQL Injection](#)
- ❖ **CVE Reference(s):** N/A
- ❖ **Security Risk:** It is possible to view, modify or delete database entries and tables

▼ **Possible Causes**
Sanitation of hazardous characters was not performed correctly on user input

▼ **Technical Description**
Web applications often use databases at the backend to interact with the enterprise data warehouse. The de-facto standard language for querying databases is SQL (each major database vendor has its own dialect). Web applications often take user input (taken out of the HTTP request) and incorporate it in an SQL query, which is then sent to the backend database. The query results are then processed by the application



The video player shows a presentation slide with the IBM logo at the top right, the text 'IBM Software Group' below it, and the title 'SQL Injection' in the center. The slide also features a footer with the Rational logo and '© 2007 IBM Corporation'. The video player interface includes standard playback controls like play, stop, and volume.





The security community has methodologies you can use to assign a severity rating to an issue

Score	0 - 2	3 - 4	5 - 6	7 - 8	9 - 10
D amage Potential	Trivial information about the target disclosed. Trivial cost associated with impact	Significant information about the target architecture and/or application disclosed. Limited cost associated with impact	Extended or increased functional control of the application and/or underlying system. Moderate cost associated with impact	Full control of the application and/or the ability to view underlying network or database infrastructure. Large cost associated with impact	Full compromise of Network or Database Infrastructure. Extensive cost associated with impact
R eproducibility	Very difficult to reproduce (more than 24 hours)	Difficult to reproduce (within 24 hours)	Moderately difficult to reproduce (within 2 hours)	Easy to reproduce (within 5 minutes)	Very easy to reproduce (30 seconds or less)
E xploitability	Seasoned security skills and/or specialised tools required	Extensive skills and tools required	Moderate skills and tools required	limited skills and tools required	no skill or tools required
A ffected Users	Very small limited user group (under 100)	Small user group (100 - 1,000)	Moderate user group (between 1,000 - 5,000)	Large user group, Open to the entire Company Network (between 5,000 - 20,000)	Open to the general internet with no authentication or very large group requiring authentication (20,000++)
D iscoverability	Very difficult to find (over 24 hours)	Difficult to find (within 24 hours)	Moderate effort required to find (within 4 hours)	Easily found (within 2 hour)	Very easily found (within 1 hour)

$$\text{Risk Rating} = (D + R + E + A + D) / 5$$

Risk Rating	Threat
0.1 - 4.0	Low Risk
4.1 - 8.0	Medium Risk
8.1 - 10.0	High Risk





Use Test
Mgmt
Best
Practices

Manage your security testing like other types of testing

- QA teams know how to manage testing
 - ▶ What are we going to test?
 - ▶ How are we going to test it?
 - ▶ Who is going to do the work?
 - ▶ How frequently are we going to retest?
 - ▶ What hardware and software are required for the test?
 - ▶ How much of the application has been tested?

- Test Plan, Test Cases, Test Scripts
 - ▶ Include security tests
 - ▶ Monitor and report on test coverage



Manage security test as you manage other tests

Use Test Mgmt Best Practices

Rational Quality Manager | GUEST | Log in | Jazz Project 1

Home | All Test Plans | Test Plan

Table Of Contents

- Summary
- Business Objectives
- Test Objectives
- Review and Approvals
- Requirements
- Application Security
- Test Iterations
- Sizing
- Environments
- Test Team
- Quality Goals
- Entry Criteria
- Exit Criteria
- Test Cases**
- Attachments

Show All Sections

Java PetStore Test Plan | Test Plan Overview | View Snapshots

State: Draft

Provide full test coverage for Java PetStore Test Plan

Test Cases

Owned By: Tony (Tester) | Status: New | Authoring 1

Lists the test cases associated with a given plan. You can add and remove associations to test documents and create and associate a new test case. Removing a test case will remove the association to this test plan but not delete the test case.

Group By: Ungrouped | Type Filter Text

Show All | Items per page | Previous | 1 - 9 of 9 | Next

	Id	Name	State	Theme	Category	Function	Weight	Modified
<input type="checkbox"/>		Shopping Cart Security Tests	Draft	Security	Security	Editors	90	1 minute ago
<input type="checkbox"/>	8	Rich Client UI Execution Test 8	Draft	Functionality	Rich Client UI	Execution	55	5 hours ago



Report on test execution status and trend

Use Test Mgmt Best Practices

Rational Quality Manager Michael Brown (Test Architect) | Log Jazz Project 1

Home | Preferences | Help

My Reports

Shared Reports

- ▼ Admin
 - Overall Execution Status
 - Plan Summary
- ▼ Execution
 - Execution Status
 - Execution Status by Owner
 - Execution Status by Plan
 - Execution Trend
- ▼ Requirements
 - Plan Requirements Coverage
 - Plan Requirements Coverage Detail
 - Plan Requirements Execution

Overall Execution Status

Parameters

Team Area: (No selection) Category: (No selection)

Interval: (No selection) Type: (No selection)

Save As... Save

Execution status per Plan

Plan Name	Passed	Failed	Blocked	Incomplete	Not Start
Java PetStore Test Plan	200	60	0	0	110
null	0	0	0	0	5

State Legend:

- Passed
- Failed
- Blocked
- Incomplete
- Not Start

Apr 28, 2008 11:13 AM





Enable your testers to create security tests

- Training
- Templates
 - ▶ Test policy
 - ▶ Scan configuration
- Record tests
- Advanced stuff later



Define Test Policies for all testers to use

Author
Security
Tests in
QA

The screenshot shows the Rational Quality Manager web interface. The main content area displays the configuration for a "Java PetStore Test Plan". The state is set to "Draft". A section titled "Application Security" is highlighted, showing a list of available test policies:

Name	Description
Developer_Essentials	This policy includes a selection of Application tests that have a high probability of success. This can be useful for developers who wish to quickly evaluate their application.
Invasive	This policy includes all invasive tests (tests which might affect the server's stability).
The_Vital_Few	This policy includes a selection of tests that have a high probability of success. This can be useful for evaluating a site when time is limited.
Default	This policy includes all tests except invasive and port listener tests.

The interface also includes a sidebar with navigation options: Planning, Construction, Lab Management, Execution, Reports, Defects, and Administration. The "Table Of Contents" for the test plan is visible on the left, listing sections like Summary, Business Objectives, Test Objectives, Review and Approvals, Requirements, Application Security (selected), Test Iterations, Sizing, Environments, Test Team, Quality Goals, Entry Criteria, Exit Criteria, Test Cases, and Attachments.





Create AppScan Tester Edition tests from Rational Quality Manager

Rational Quality Manager ADMIN | Log Out
Jazz Project 1

Type to Search Home | Preferences | Help | About

Home | New Test Case | New Test Script

Shopping Cart Automated Security Test New / Not Yet Saved
 Test Script

Originator: ADMIN
 Owner:
 Type:
 Description: Tests the shopping cart functionality of the application for security defects

Rational AppScan Tester Edition
 Rational AppScan Tester Edition will scan your web application for security vulnerabilities.

Template
 Select the template type to use while creating the scan. Once the scan has been created, this information can no longer be modified.
 Type:

Verdict Strategy
 The verdict strategy determines the criteria that must be met for a related execution work item to pass or fail.
 Severity Threshold

- High
- Medium
- Low
- Information

Planning

Construction

Lab Management

Execution

Reports

Defects

Administration





Provide a template for configuring the test to make it easy

- QuickScan UI simplifies test creation



Summary and Call To Action

- Security is Important
 - Security is Quality
 - Security is Testable; you can make a difference
-
- Make application security part of what your QA team does!





QUESTIONS





THANK YOU

Learn more at:

Terry Goldman - goldmant@sg.ibm.com

- [IBM Rational software](#)
- [IBM Rational Software Delivery Platform](#)
- [Process and portfolio management](#)
- [Change and release management](#)
- [Quality management](#)
- [Architecture management](#)
- [Rational trial downloads](#)
- [Leading Innovation Web site](#)
- [developerWorks Rational](#)
- [IBM Rational TV](#)
- [IBM Rational Business Partners](#)

