QM05

Building a Secure Application Development Process with the Rational AppScan Family

John Smith
Senior Security Architect, IBM Rational
johnsmith@uk.ibm.com

IBM Rational Software Development Conference 2008

WHERE TEAMS ARE R-HEROES

IBM

Rational. software

Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
  - People
  - Tools
  - Process/Governance
- Rational solutions
  - Education
  - Software
  - Services

Avoiding the Headlines…

Associated Press

Visa, Amex Cut Ties with CardSystems

July 19, 2005 -- Visa USA Inc. and American Express Co. are cutting ties with the payment-processing company that left 40 million credit and debit card accounts vulnerable to hackers in one of the biggest breaches of consumer data

CSO
The Resource for Security Executives

Jan 18, 2007
Massive Security Breach Reveals Credit Card Data

The TJX Companies, a large retailer that operates more than 2,000 retail stores under brands such as Bob's Stores, HomeGoods, Marshalls, T.J. Maxx and A.J. Wright, said on Wednesday that it suffered a massive computer breach on a portion of its network that handles credit card, debit card, check and merchandise transactions in the United States and abroad.

THE WALL STREET JOURNAL.

BJ's Settles Case with FTC over Customer Data

FTC alleges weak security at wholesale club led to fraudulent sales valued in the millions

JUNE 17, 2005 -- After credit card data for thousands of customers was used to make fraudulent purchases in other stores, BJ's Wholesale Club Inc. has agreed

The McGraw-Hill Companies
BusinessWeek

CNBC's Easy Money

BusinessWeek **uncovers that the cable channel's own design flaw may be behind the investigation into its million-dollar stock-picking co**

AXcess News
News for the X generation

USDA admits data breach, thousands of social security numbers revealed

Thursday, 17 April 2007

(AXcess News) Washington - The US Department of Agriculture (USDA) admitted that a security breach allowed social security and other personal information of over 63,000 recipients of federal farm loans be made available on a public website in violation of Federal privacy laws.

Motivations for Secure Applications

Web applications are the #1 focus of hackers:

- XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)

Most sites are vulnerable:

- 90% of sites have security issues (IBM)
- 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)

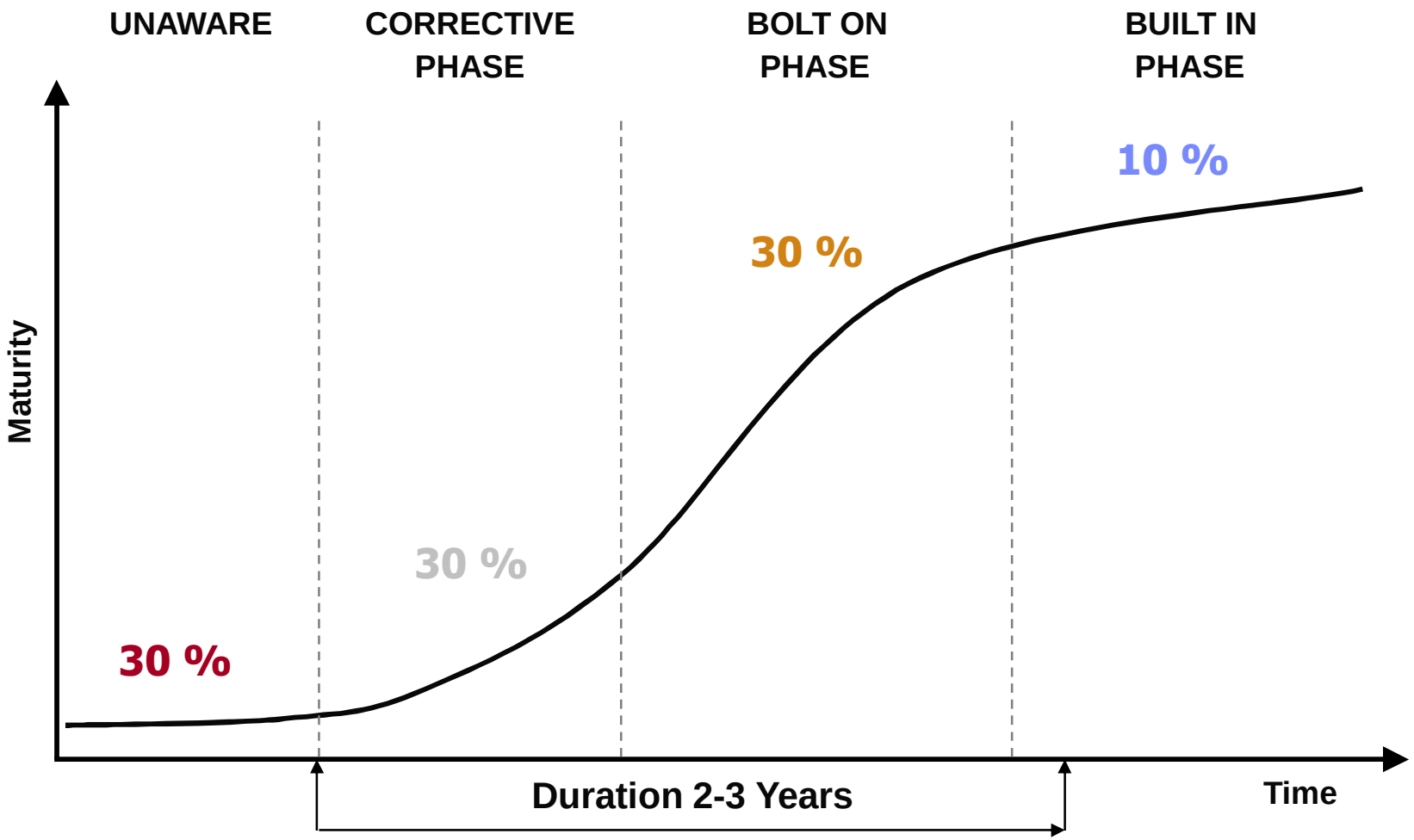
Web applications are high value targets for hackers:

- Customer data, credit cards, ID theft, fraud, site defacement, etc

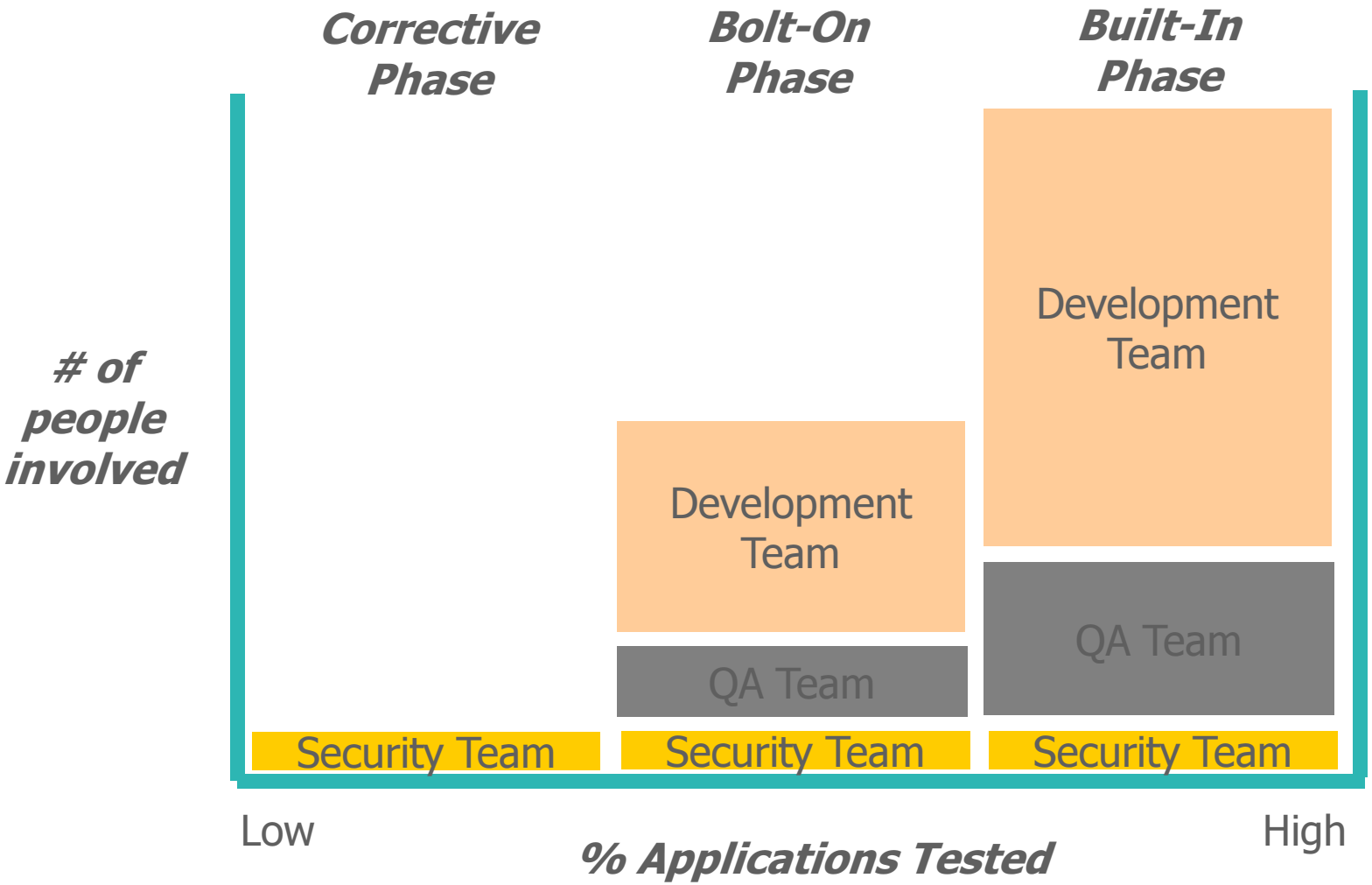
Compliance requirements:

- Payment Card Industry (PCI) Standards, Sox/EuroSox, Basel II etc.

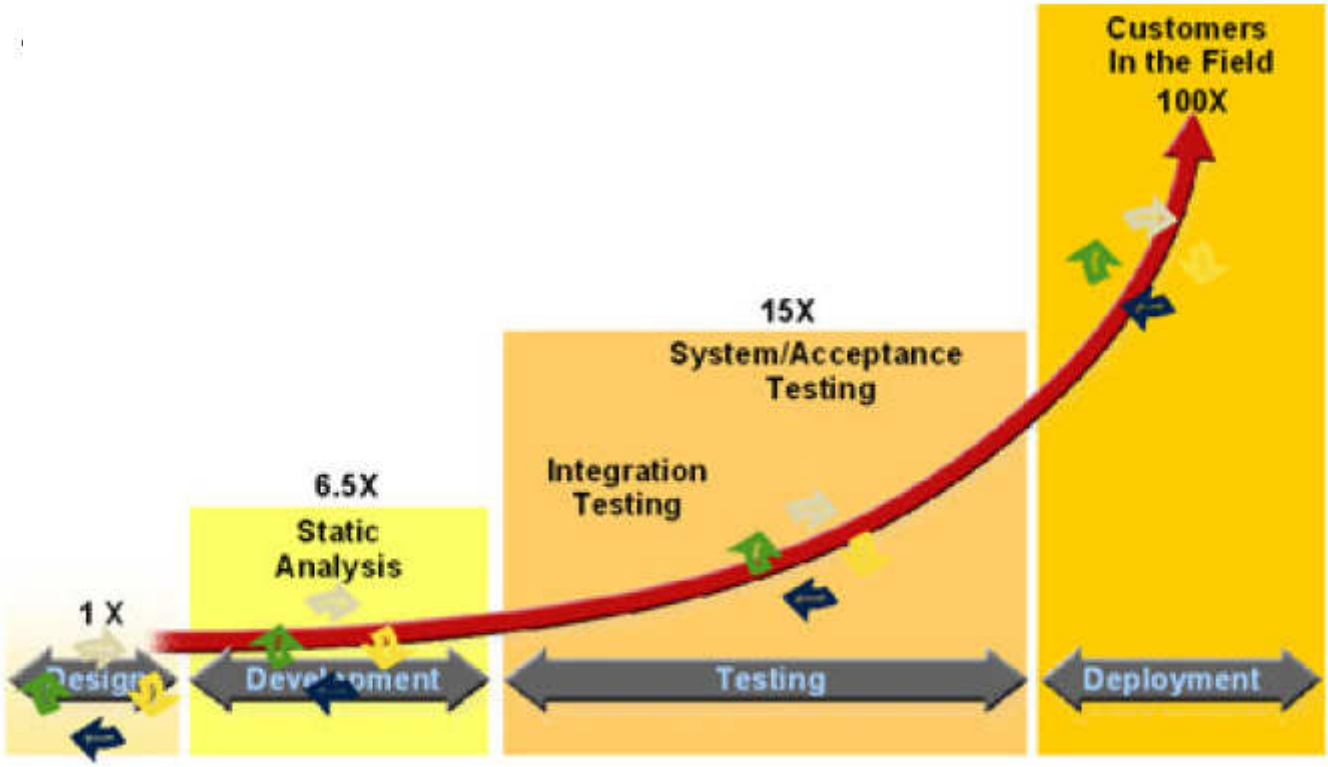
Phases of Application Security Maturity



The need to scale



Cost Benefits of Early Detection



Source: IBM Systems Sciences Institute

Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
  - People
  - Tools
  - Process/Governance
- Rational solutions
  - Education
  - Software
  - Services

Ingredients

- People
- Tools
- Process/Governance

People

- Many different stakeholders in Application Lifecycle
  - Business Owners
  - Architects
  - Developers
  - Testers
  - ...
- Education is the Key
  - Understanding the Vulnerabilities
  - Secure Coding Principles
  - Corporate Security Policy
  - ...

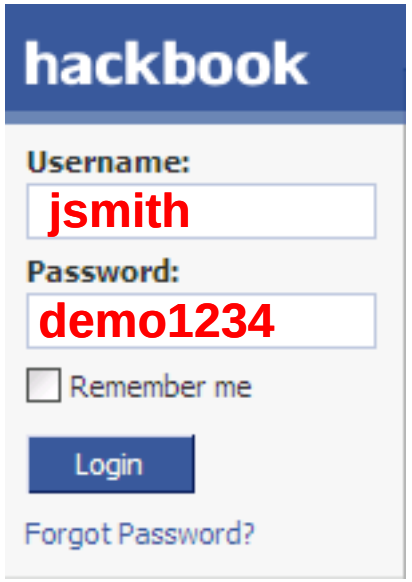
Tools

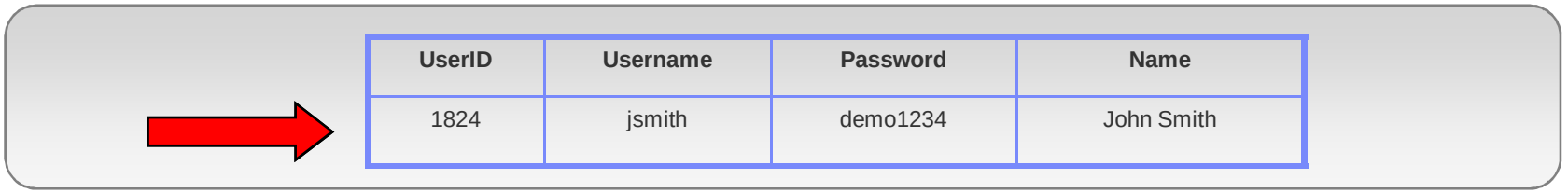
- Security is a Quality problem
  - Defect Management
  - Test Management
  - Test Automation
- Security Testing Tools based on 2 complimentary approaches:
  - Black-Box Testing
  - White-Box Testing
- Lets look at an example...

SQL Injection

User input is embedded as-is in predefined SQL statements:

```
query = "SELECT * from tUsers where
        userid='" +  iUserID  + "' AND
        password='" +  iPassword  + "'";
```

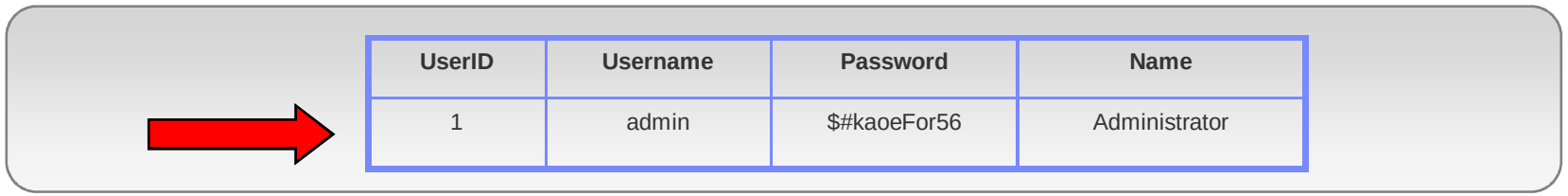




UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

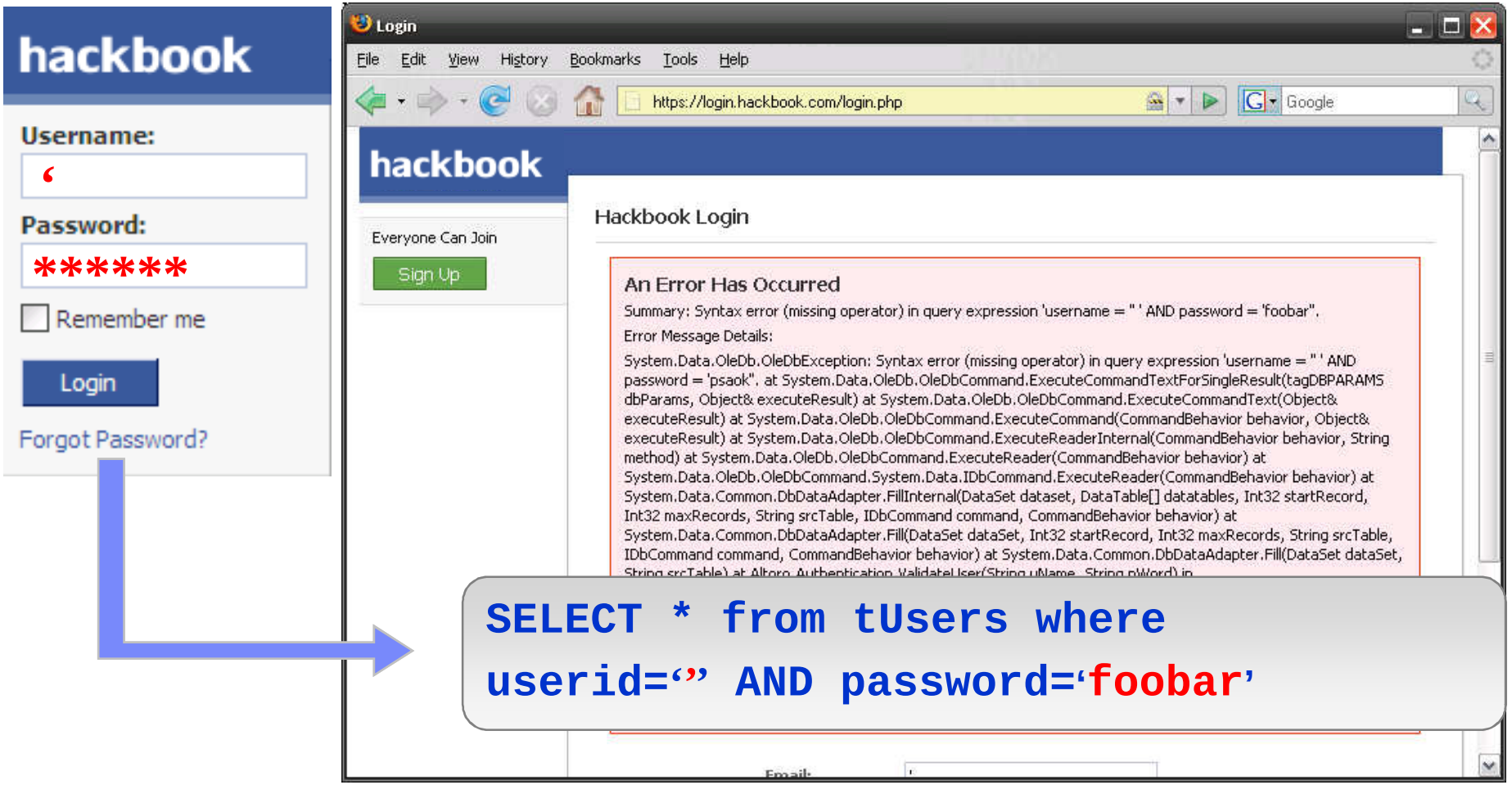
Hacker supplies input that modifies the original SQL statement, for example:

```
iUserID = ' or 1=1 --
```



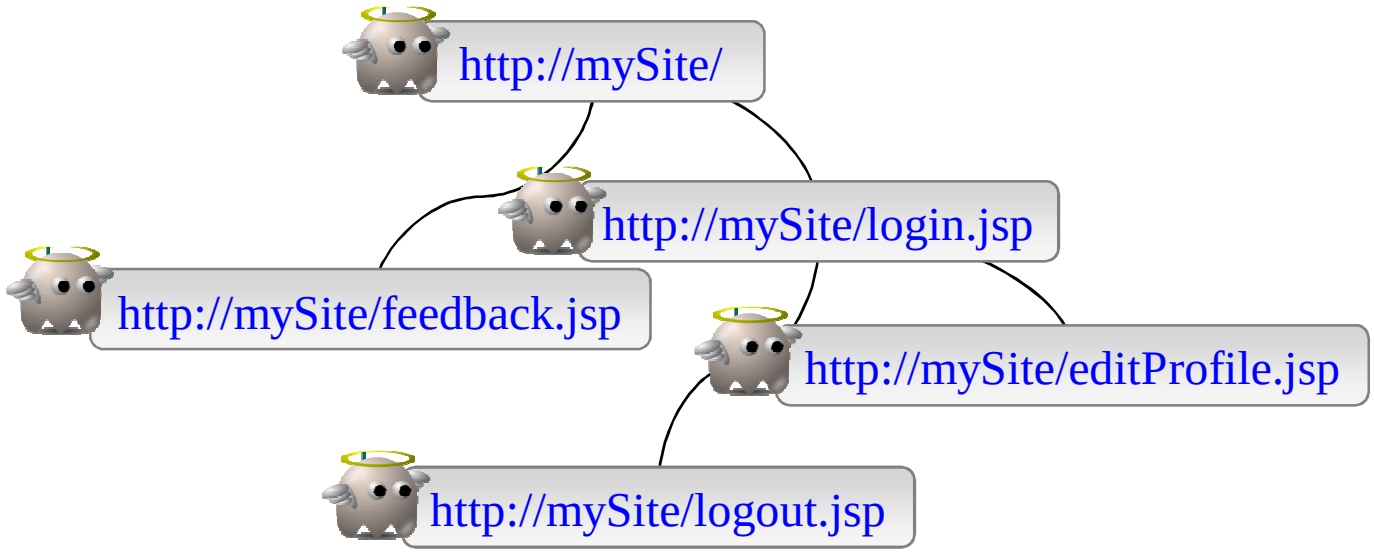
UserID	Username	Password	Name
1	admin	$#kaoeFor56	Administrator

How Black-Box Scanners Work



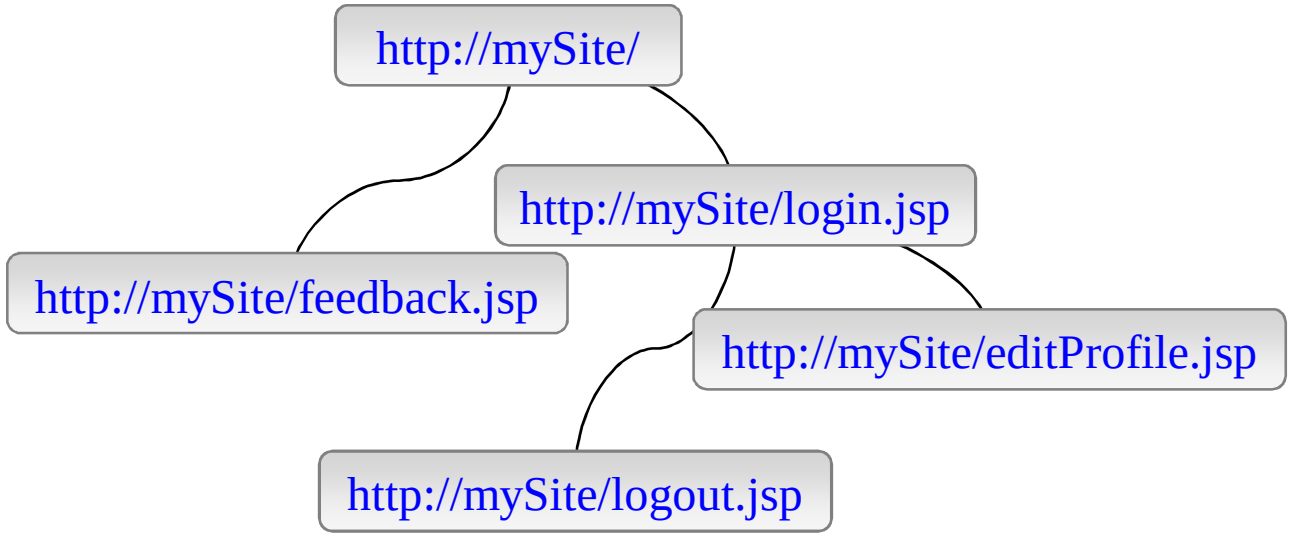
How Black-Box Scanners Work

Stage 1: Crawling as an honest user



How Black-Box Scanners Work

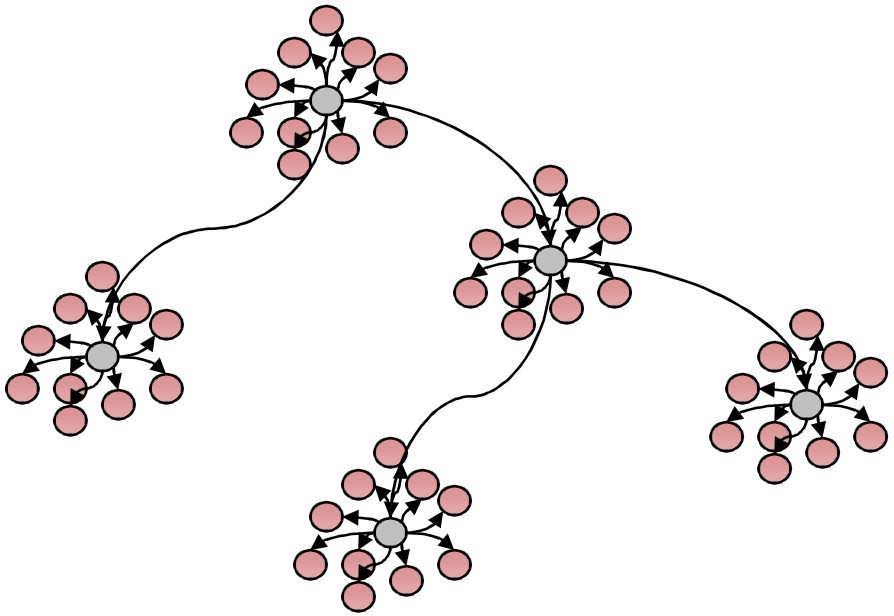
Stage 1: Crawling as an honest user



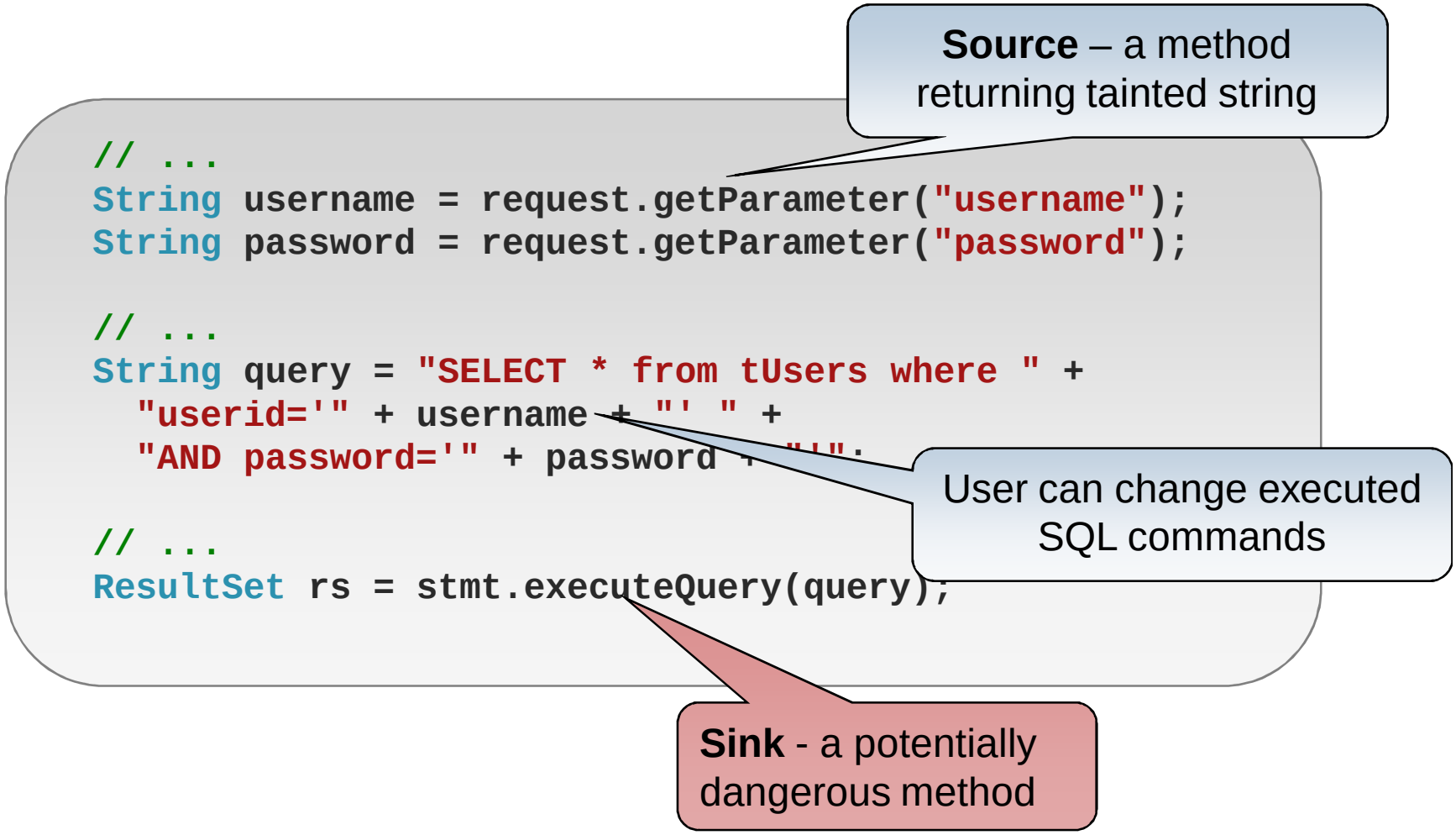
How Black-Box Scanners Work

Stage 1: Crawling as an honest user

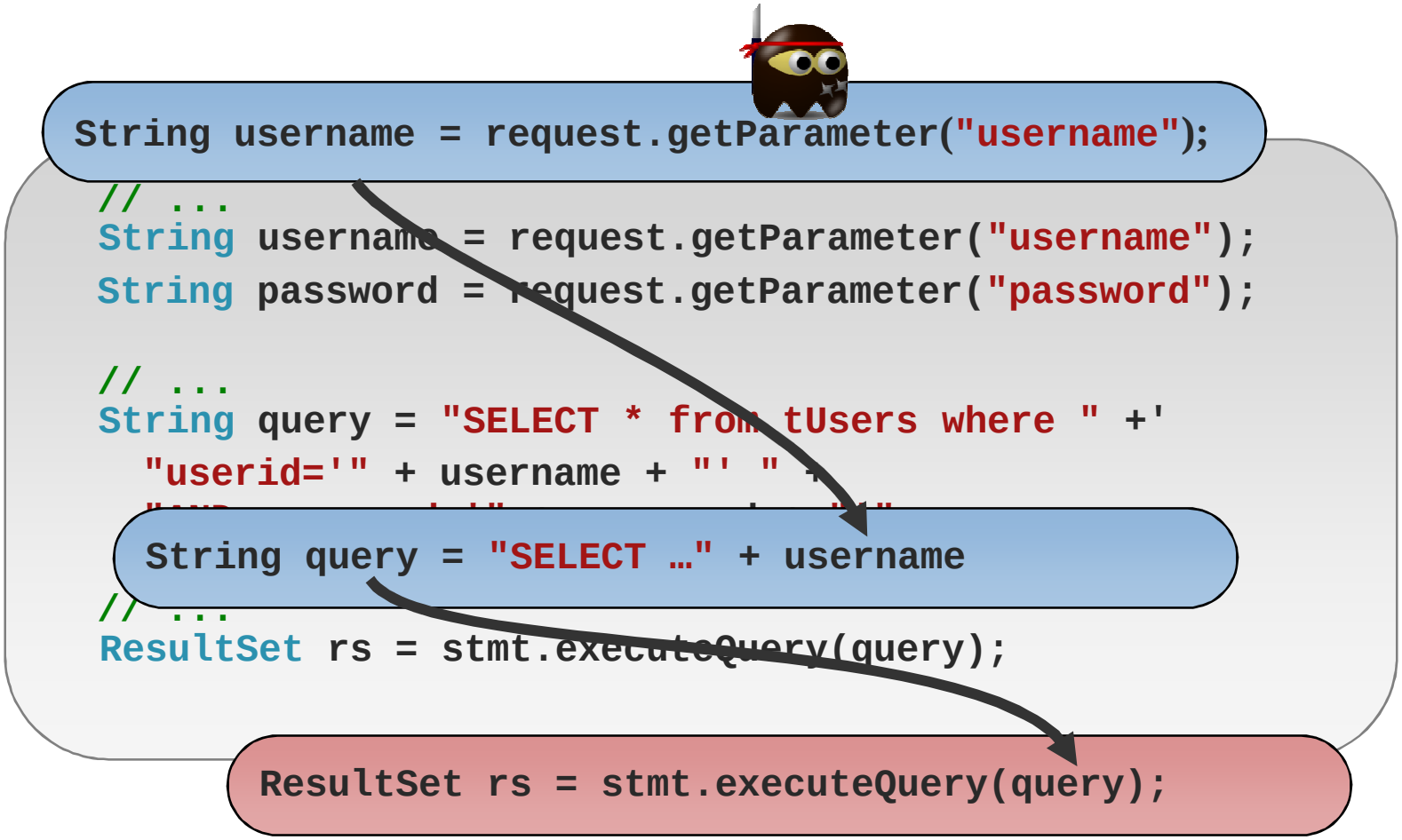
Stage 2: Testing by tampering requests



How White-Box Scanners Work



How White-Box Scanners Work



A Common Fix (not the best one...)

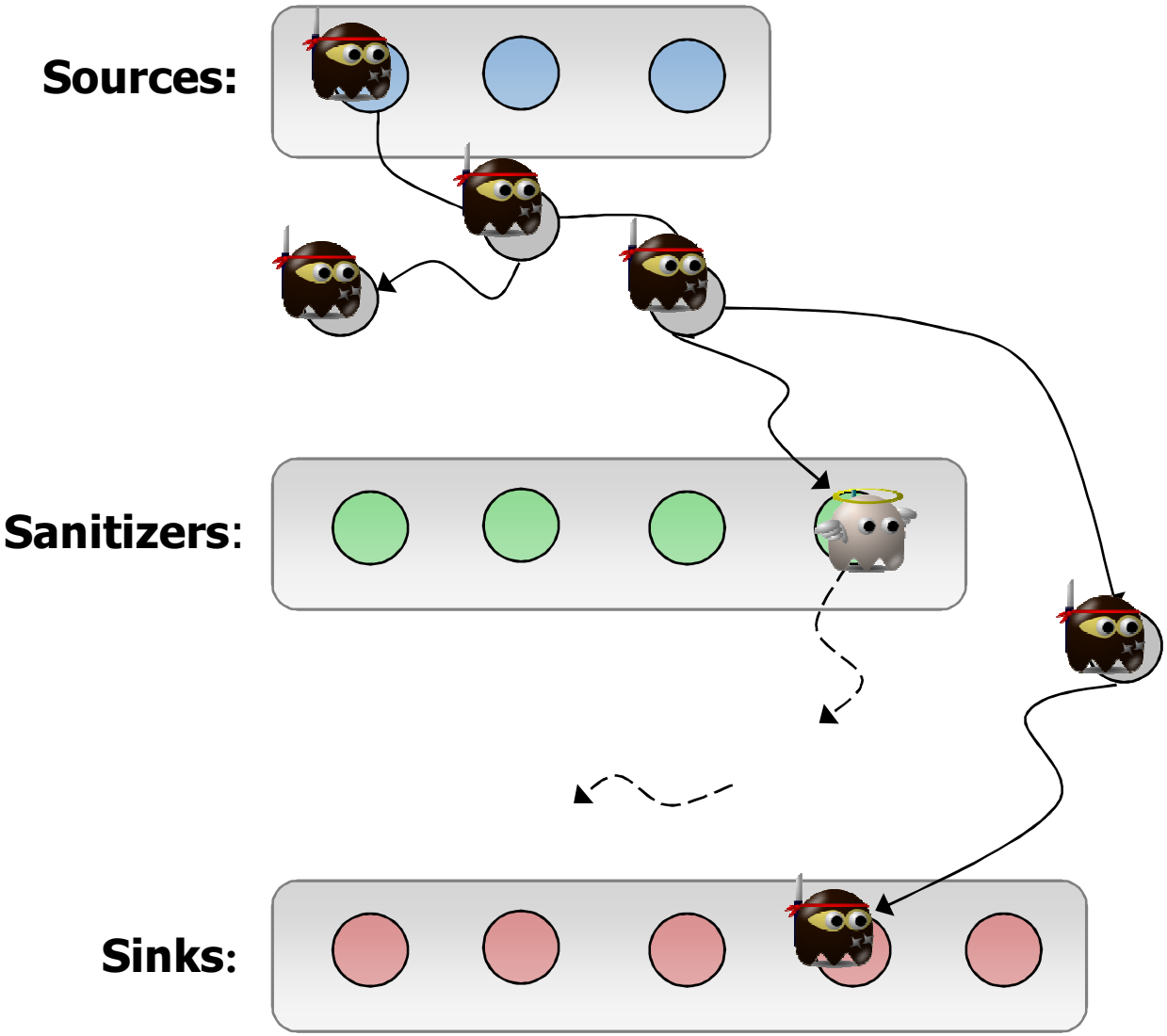
```
// ...
String username = request.getParameter("username");
String password = request.getParameter("password");

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

// ...
ResultSet rs = s        ecuteQuery(query);
```

Sanitizer:
a method returning
a non-tainted string

How WB Scanners Work



Processes/Governance

"We are what we repeatedly do.
Excellence, then, is not an act but a habit"

Ralph Waldo Emerson

- Well defined and understood processes allow Habits of Excellence to be formed
- Strong governance ensures that Habits of Excellence are formed consistently throughout the organisation

Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
  - People
  - Tools
  - Process/Governance
- Rational solutions
  - Education
  - Software
  - Services

Rational Education

- Web Based Training
  - Comprehensive Curricula
    - Product Training
    - Security Training
    - Secure Coding Principles
  - Customisable
- Immersion Training
  - Onsite, working within your infrastructure
  - Tailored to your needs

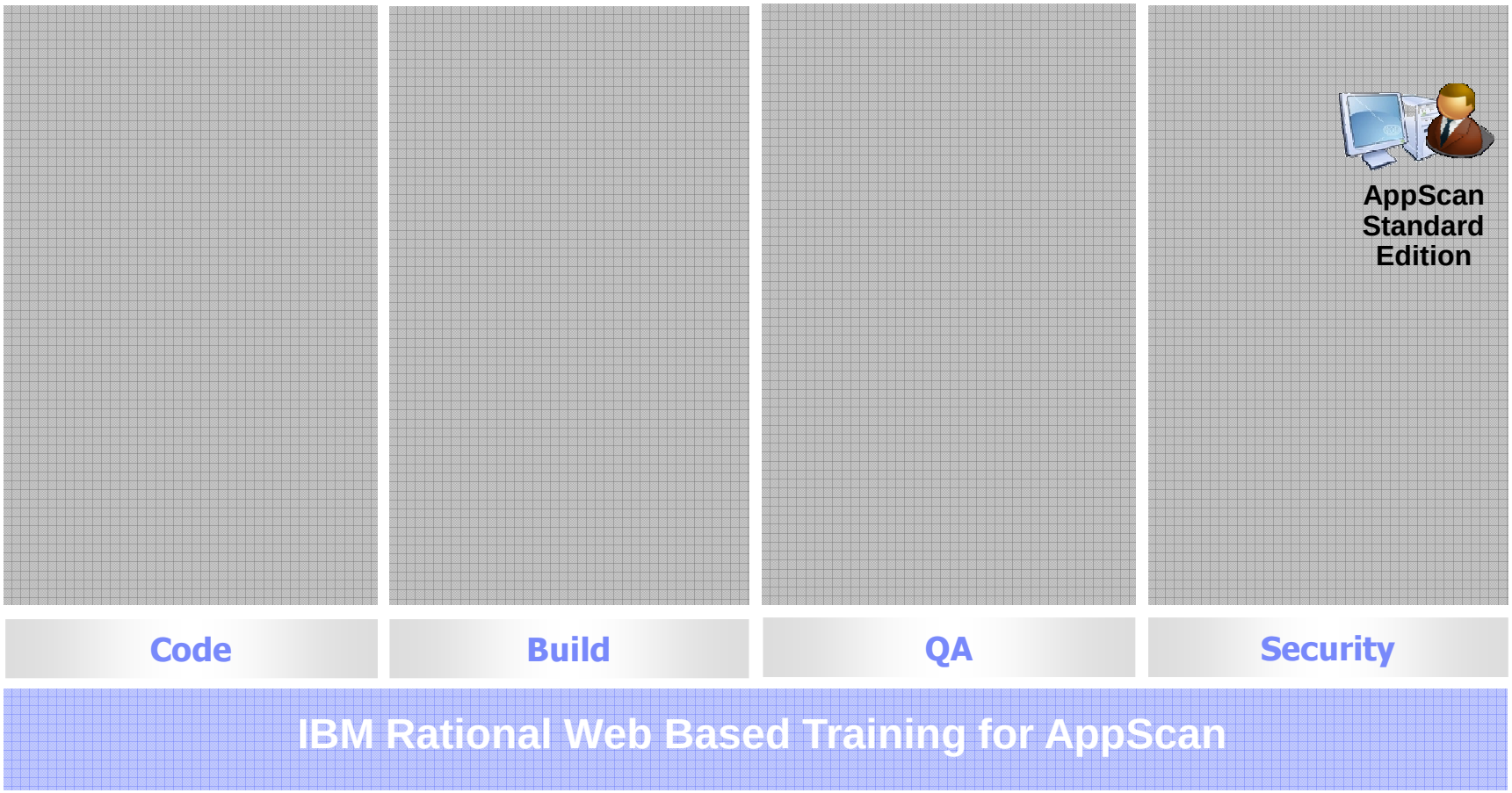
Rational Services

- Software as a Service
  - AppScan On Demand
  - Managed Services
- Deployment Services
  - Ease the deployment path
  - Integration with your infrastructure
- Consultancy
  - Help you find a path to security

Rational Software

- Complete Quality Management Solution
  - Rational Quality Manager
  - Rational Clearquest
  - Rational Functional Tester
  - Rational Performance Tester
  - ...
- Specific Toolset for Application Security
  - AppScan Product Family

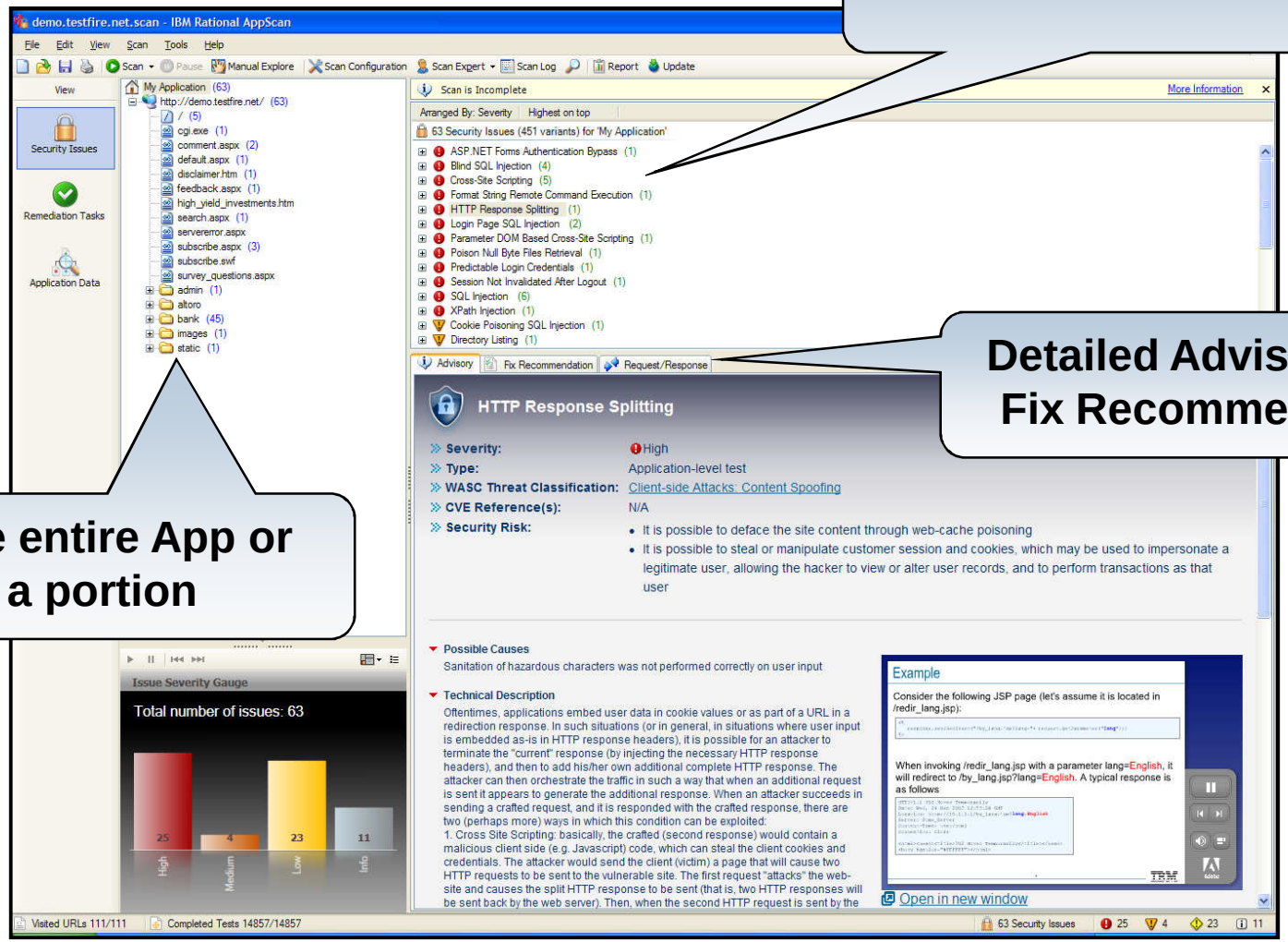
IBM Rational AppScan SDLC Ecosystem



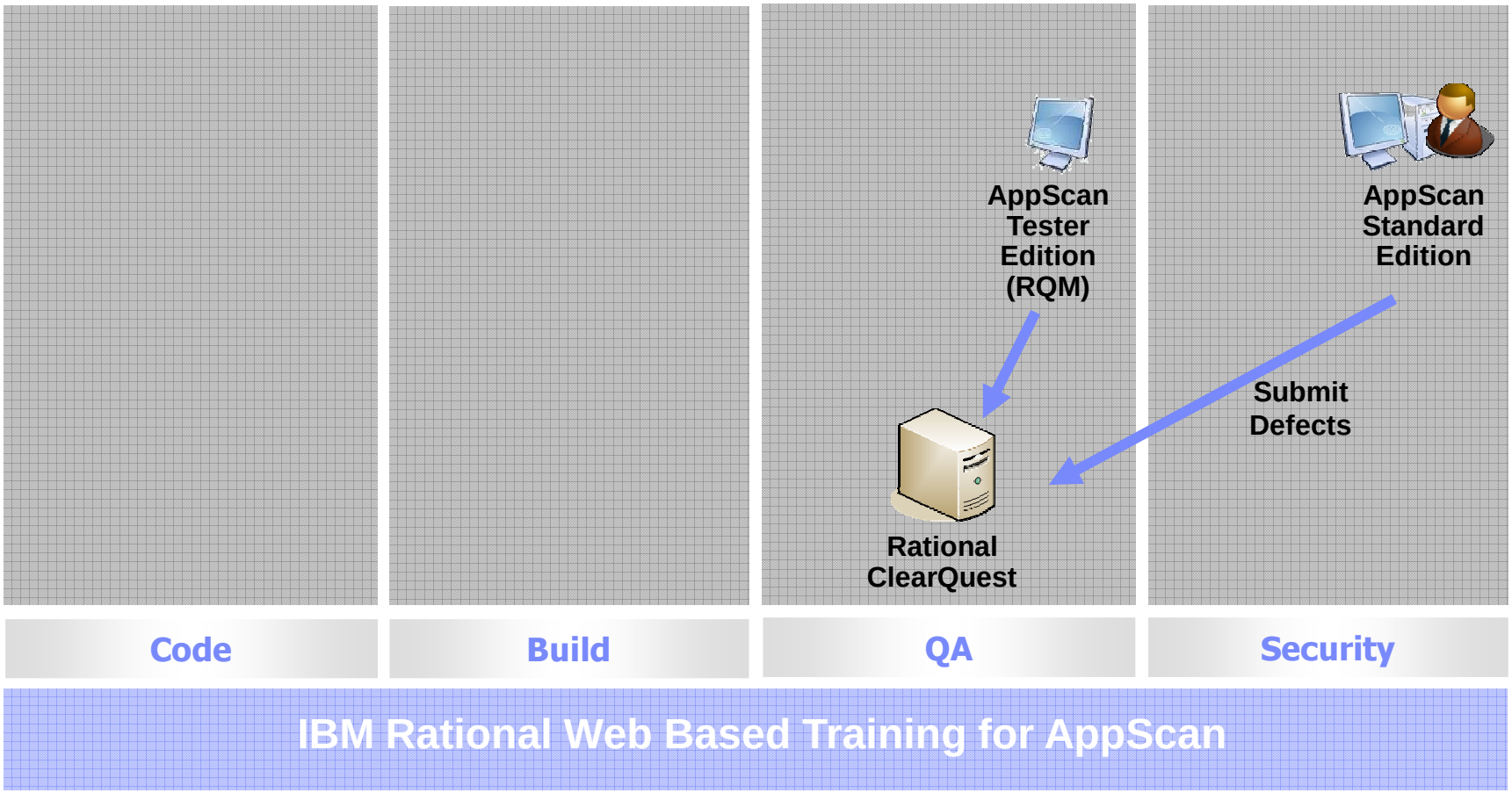
AppScan Standard Edition

- Best in class Black-Box Testing
  - AJAX Support
  - Multi-Step Process Support
  - Advanced Login Management
- Extensible Plug-in Architecture
  - Integrate with systems and processes
- Easy to use, drives Education process
  - Scan Expert for configuration assistance
  - Integrated WBT Modules

AppScan Standard Edition



IBM Rational AppScan SDLC Ecosystem



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

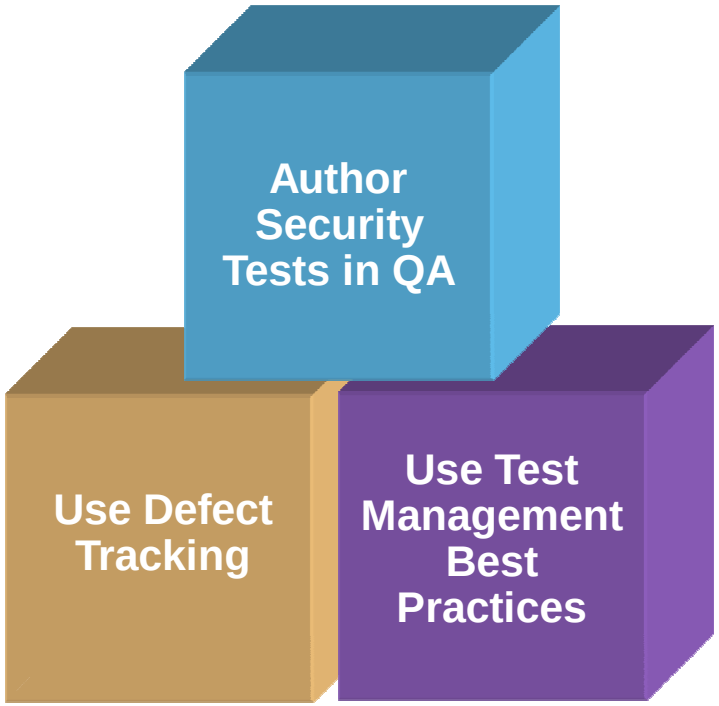
Triages and manages defects

Scales testing effort across a large team

Already part of the development process

Phased adoption of security testing in QA

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



Tracking security defects like other defects is the first building block

- Benefit to have the bugs tracked properly
- Begins to bring security into the normal dev process
- QA Team gains awareness/begins to learn about security
- Security Auditors benefit from having the issue they find tracked properly
- Can prioritize security work against other work, triage

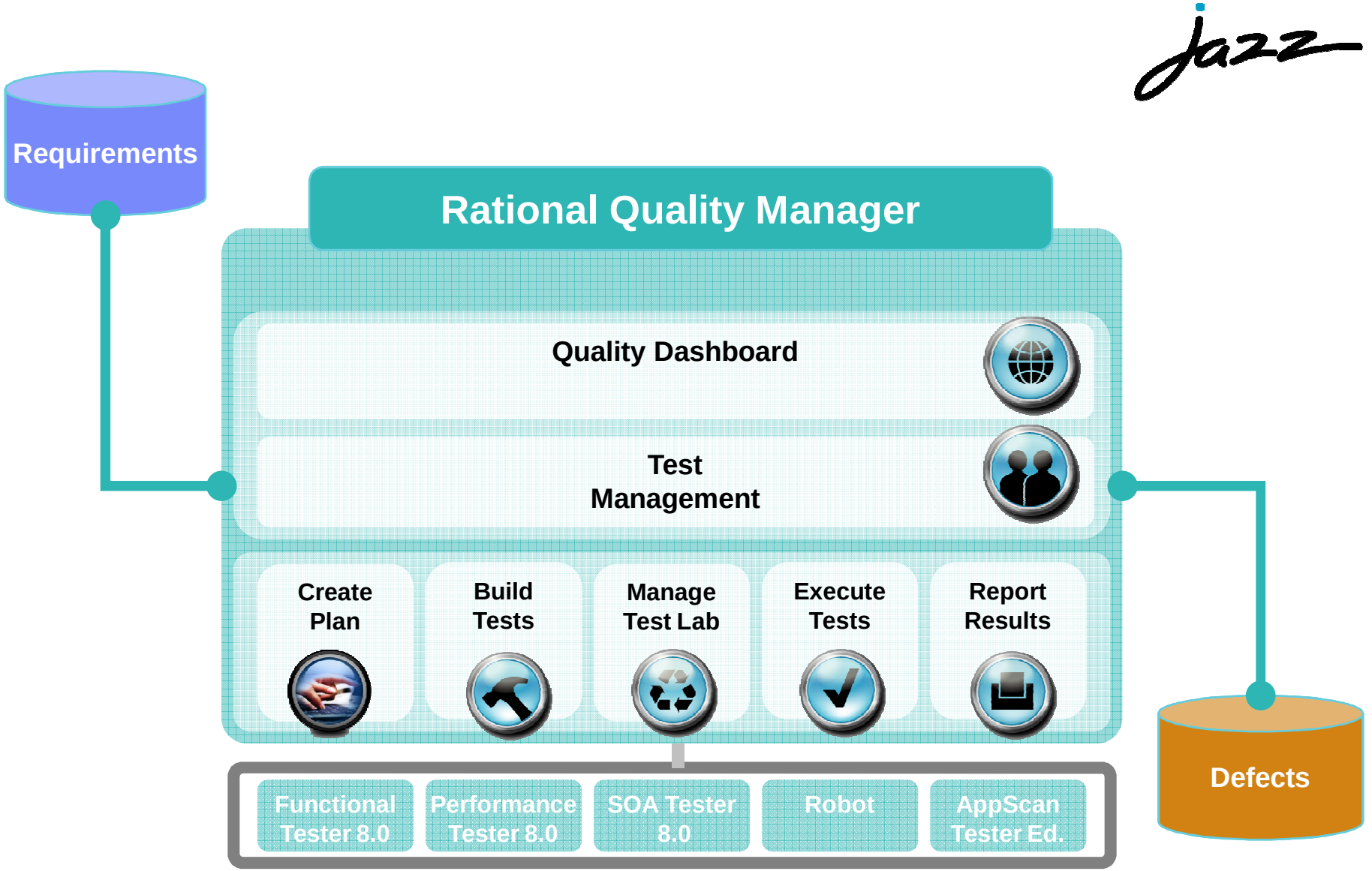
Manage your security testing like other types of testing

- 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

Enable your testers to create security tests

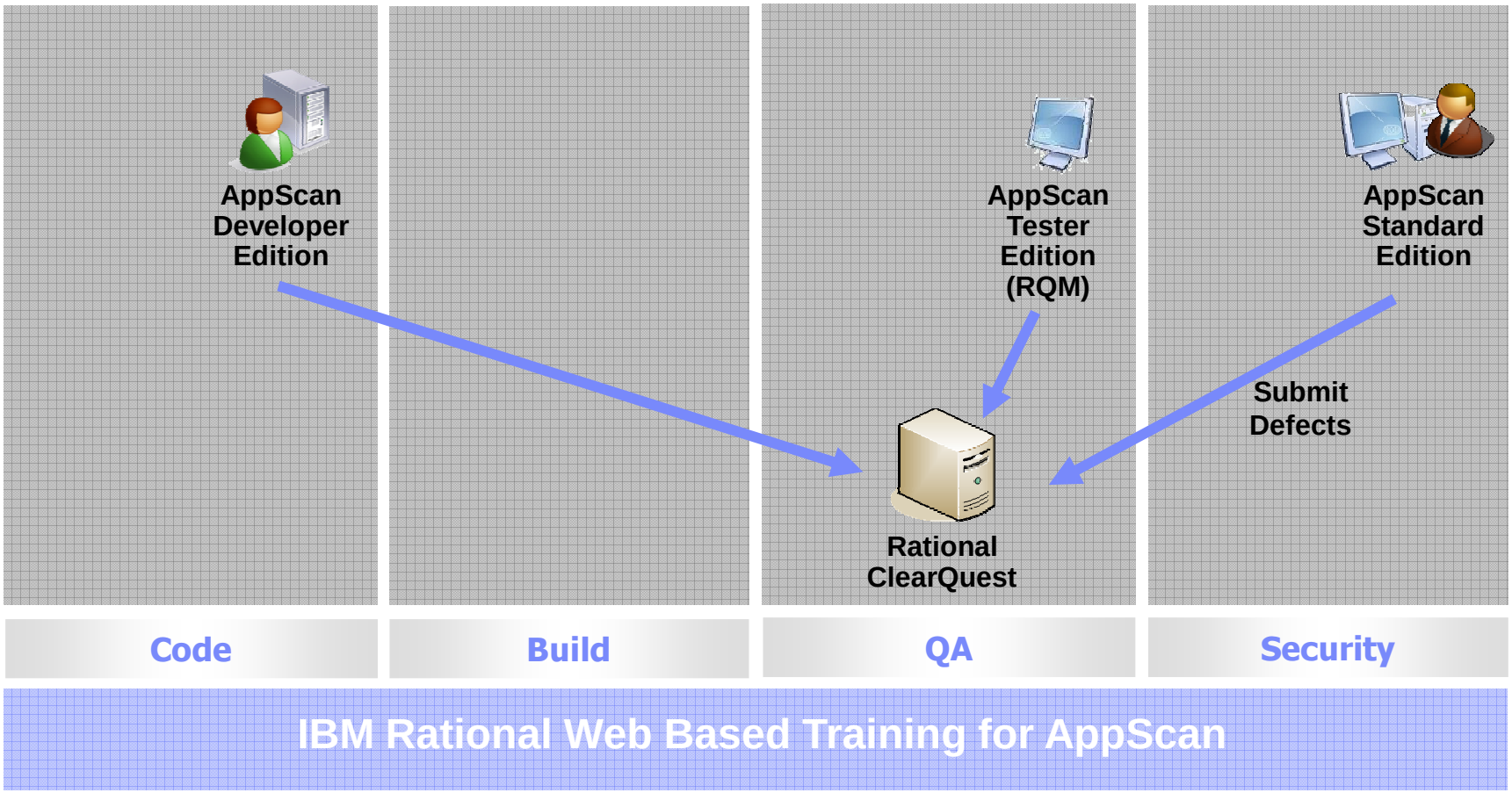
- QA begins writing their own security tests
- By now have acquired some security knowledge in the team
- Leverage skills of experts to scale out testing to more junior testers
  - Templates to capture expert knowledge, making it easy for more junior testers
- Authoring a simple Security Test can be as easy as making a recording
  - Familiar if they are using Rational Functional Tester or Rational Performance Tester


Jazz
Requirements
Rational Quality Manager
Quality Dashboard
Test Management
Create Plan
Build Tests
Manage Test Lab
Execute Tests
Report Results
Functional Tester 8.0
Performance Tester 8.0
SOA Tester 8.0
Robot
AppScan Tester Ed.
Defects

AppScan Tester Edition

- Black-Box Testing Technology
- Integrate Security Testing into well governed QA Process
  - Leverage RQM Test Management Platform
  - Delegate security testing

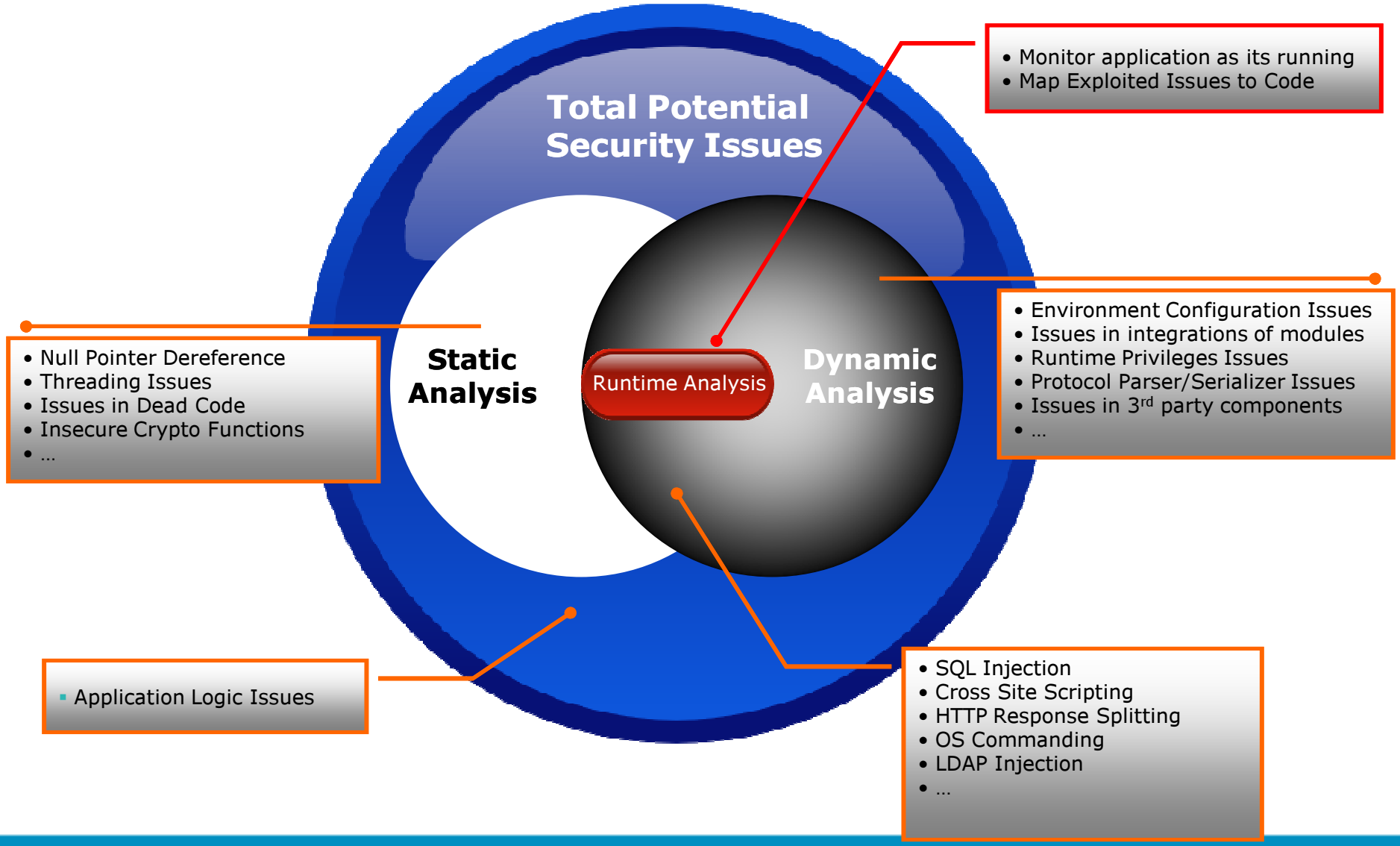
IBM Rational AppScan SDLC Ecosystem



AppScan Developer Edition

- Includes White-Box, Black-Box & Runtime Analysis
  - Side-by-side, gain the strengths of all techniques
- Uses Composite Analysis , merging the different ways
  - CA overcomes the weaknesses of each technique, such as:
    - Theoretical White-Box issues confirmed by Black-Box
    - Black-Box Coverage measured with Runtime Analysis
- Extreme Emphasis on Accuracy & Actionable Results
  - Innovative Static String Analysis dramatically improves accuracy
  - Runtime Analysis maps Black-Box issues to code
  - Correlated Black-Box & White-Box results practically guaranteed

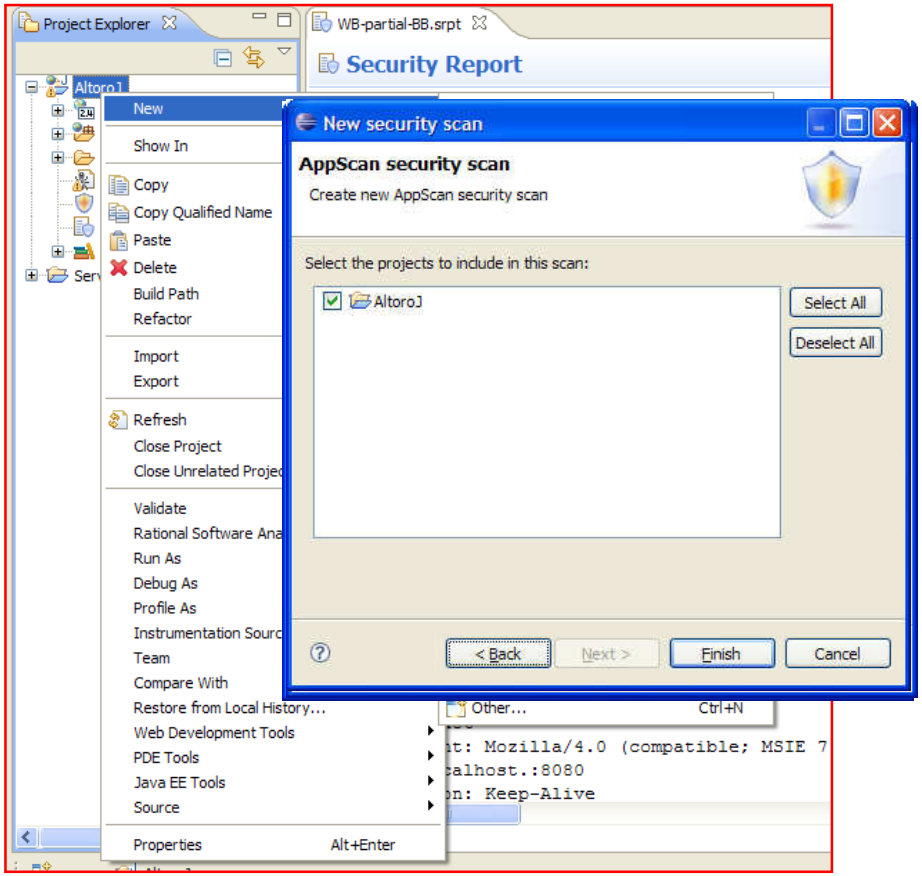
Security Issues Coverage

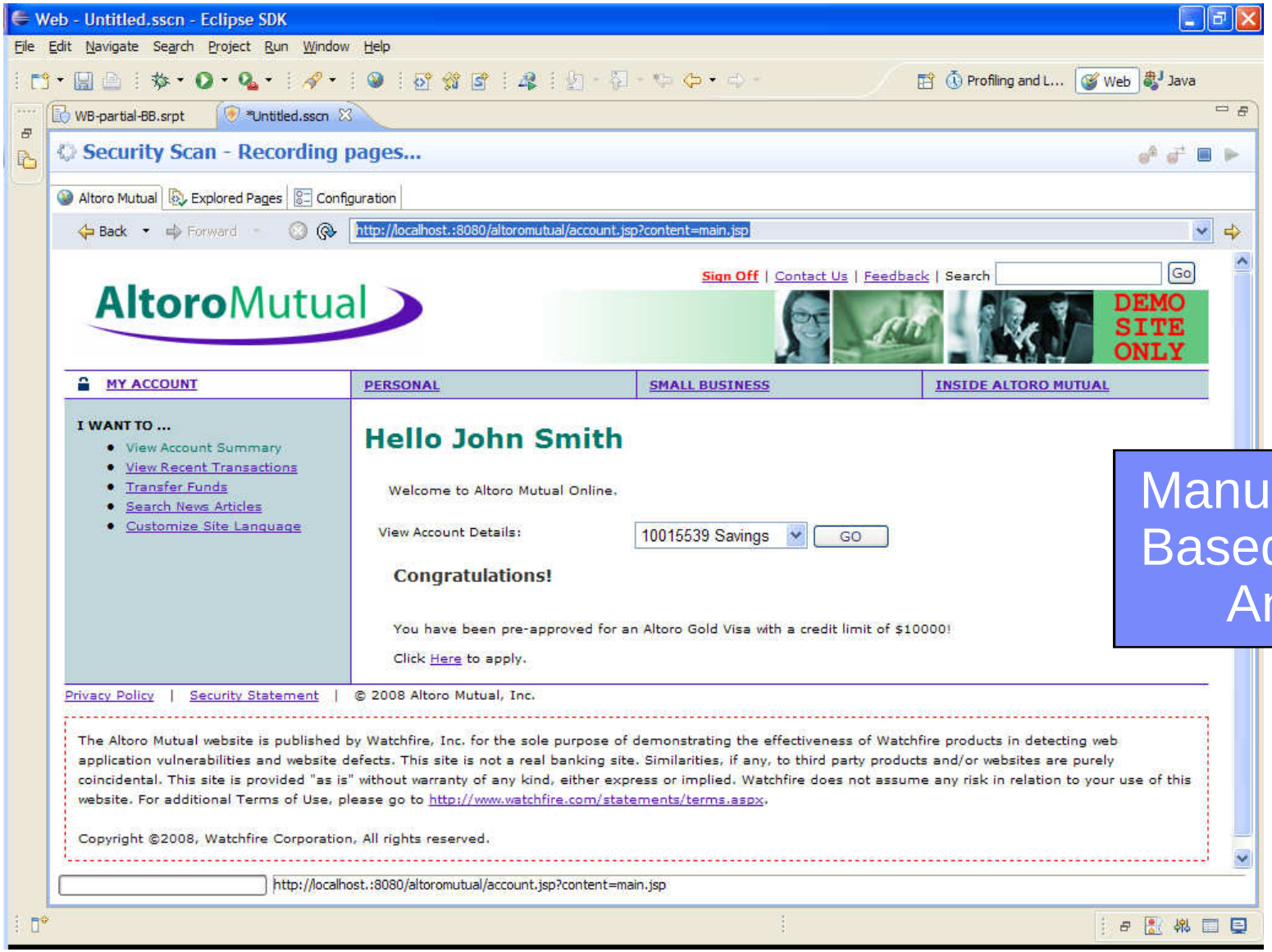


Self-Serve Security Testing for Developers

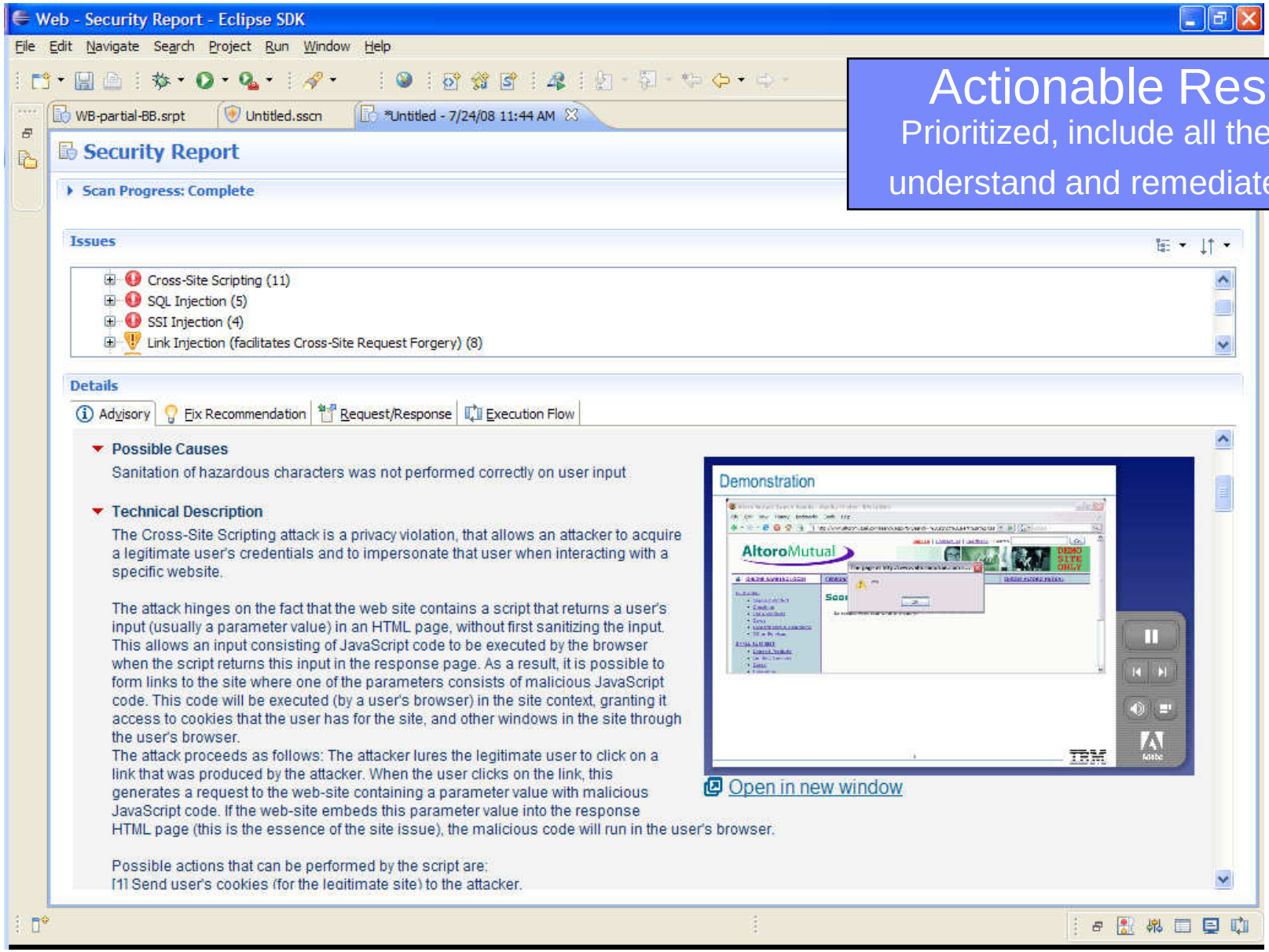
- Detailed results include all you need to know
  - Comprehensive information about each security issue and its impact
  - Clear prioritization account for security risk and exploitability
- Remediation view turns risk into tasks
  - Look at the problems from a development tasks perspective
  - Risk manifested in task priority
- Detailed Fix Recommendations clarify needed action
  - Complete with platform-specific code examples
  - Retest capabilities enable verifying the fix works
- Built in and accompanying training supports self-serve
  - Issue-specific flash-based training built into product
  - Product & Security Web-Based Training will be available at GA

Wizard-based Scan Creation





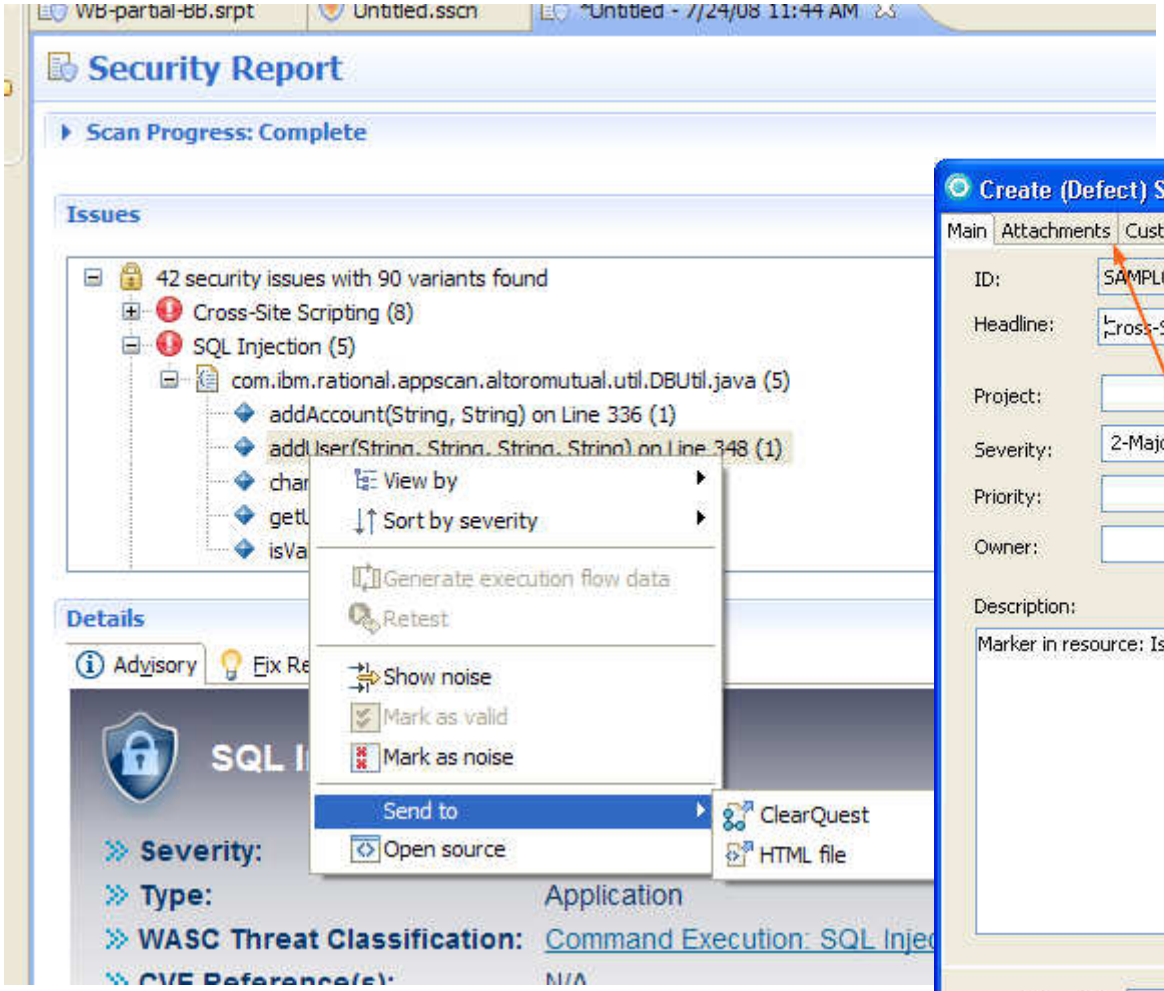
Manual-Explore Based Dynamic Analysis

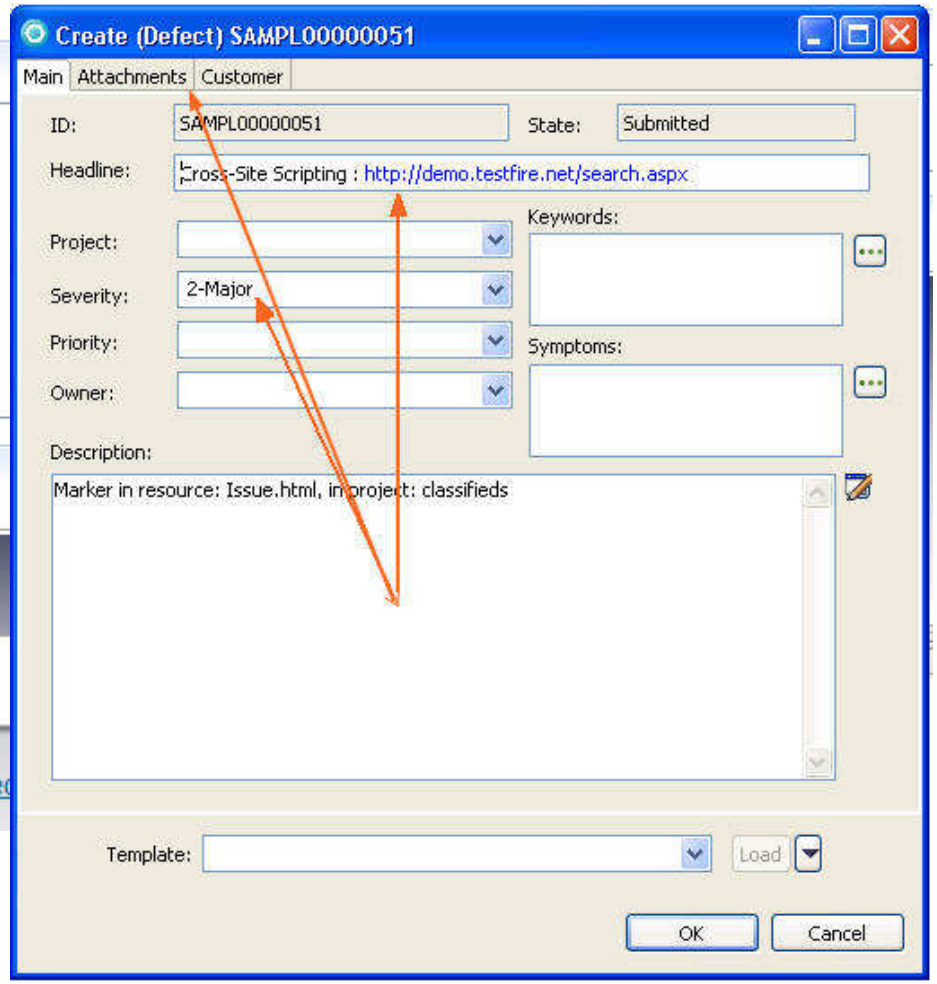


Actionable Results

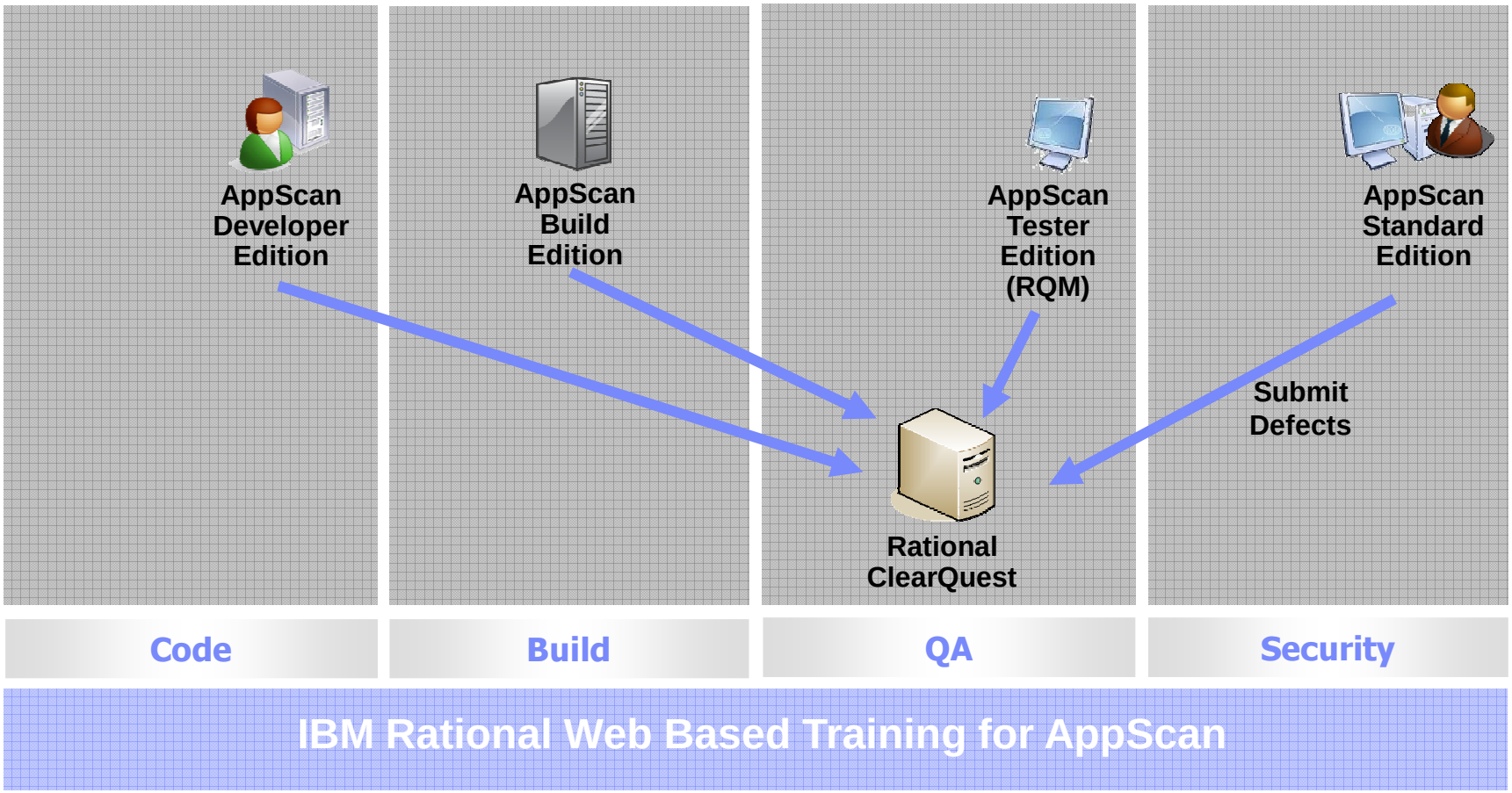
Prioritized, include all the info to understand and remediate issues

Built-in Export to ClearQuest





IBM Rational AppScan SDLC Ecosystem

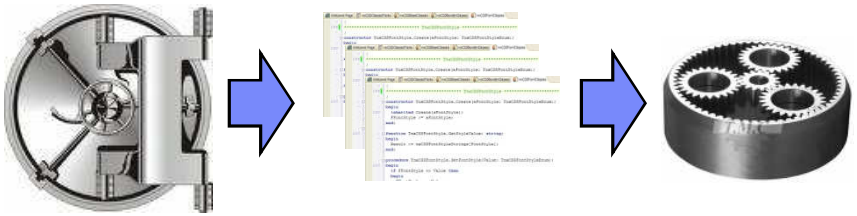


AppScan Build Edition

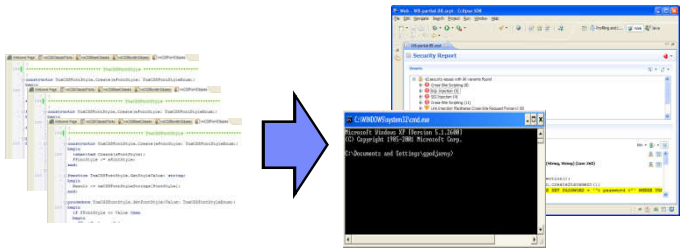
- Allows scans created by either AppScan Standard or Developer Edition to be processed in a non-UI / scriptable mode
- Provides generic command line support for integration into any build environment
- Provides a BuildForge Adaptor so that integrating AppScan testing is an experience that should be familiar/expected for a BuildForge practitioner

AppScan Build Edition Use-Case

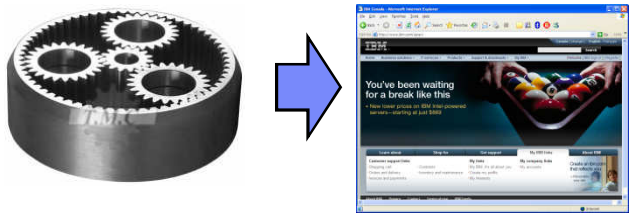
1. Build System compiles code



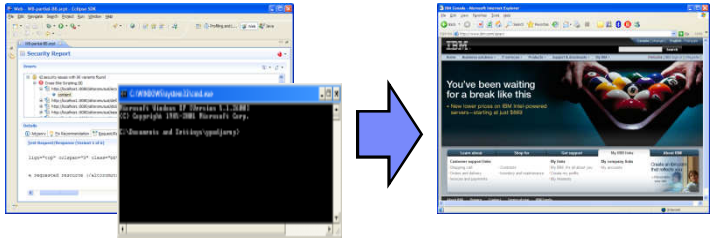
2. RASBE Static Analysis Invoked



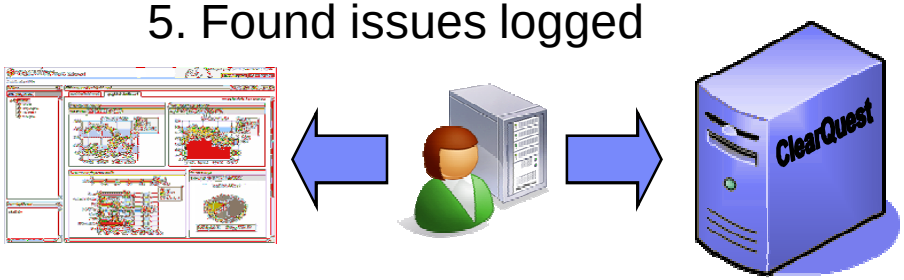
3. Application auto-deployed



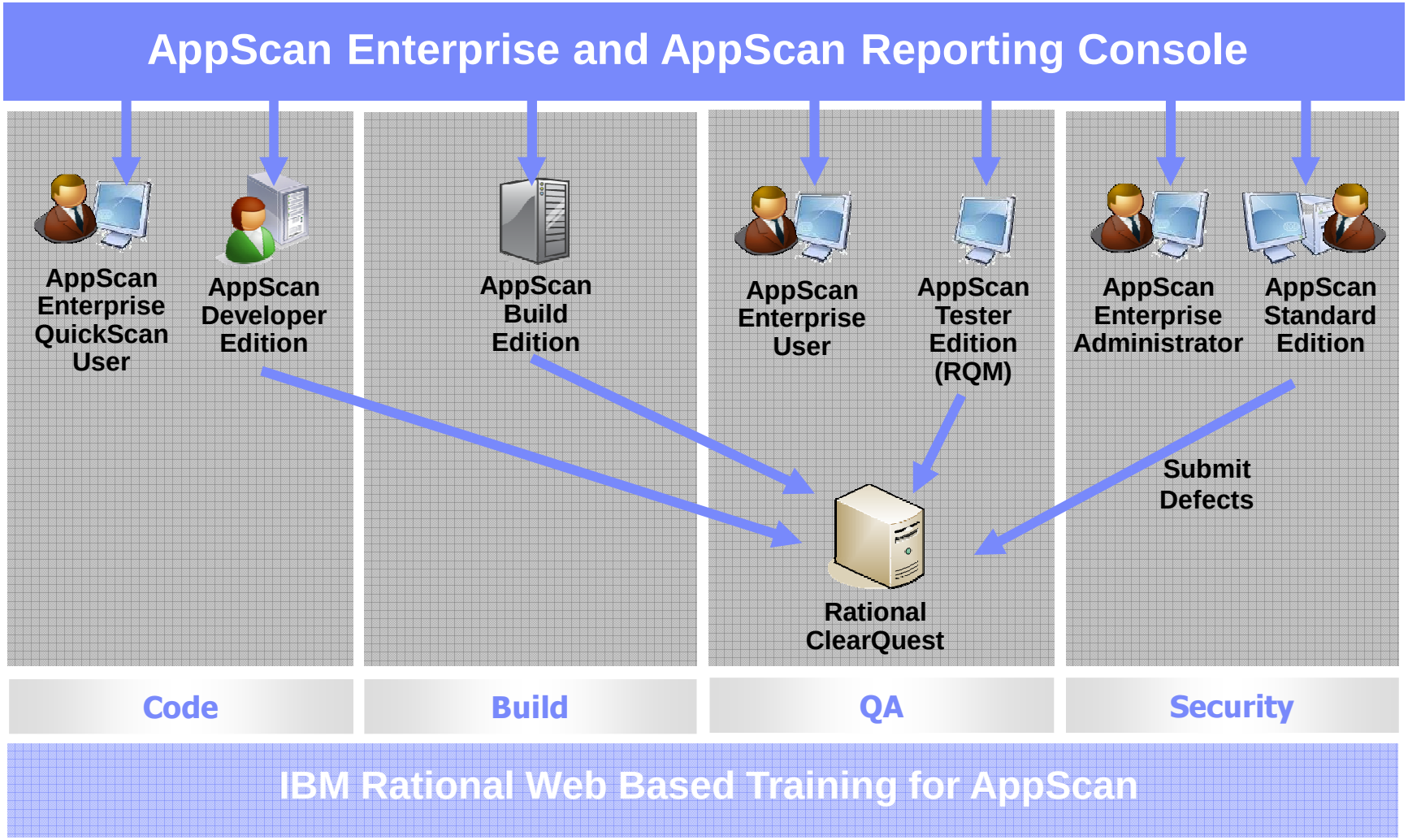
4. RASBE Dynamic Analysis Invoked



5. Found issues logged

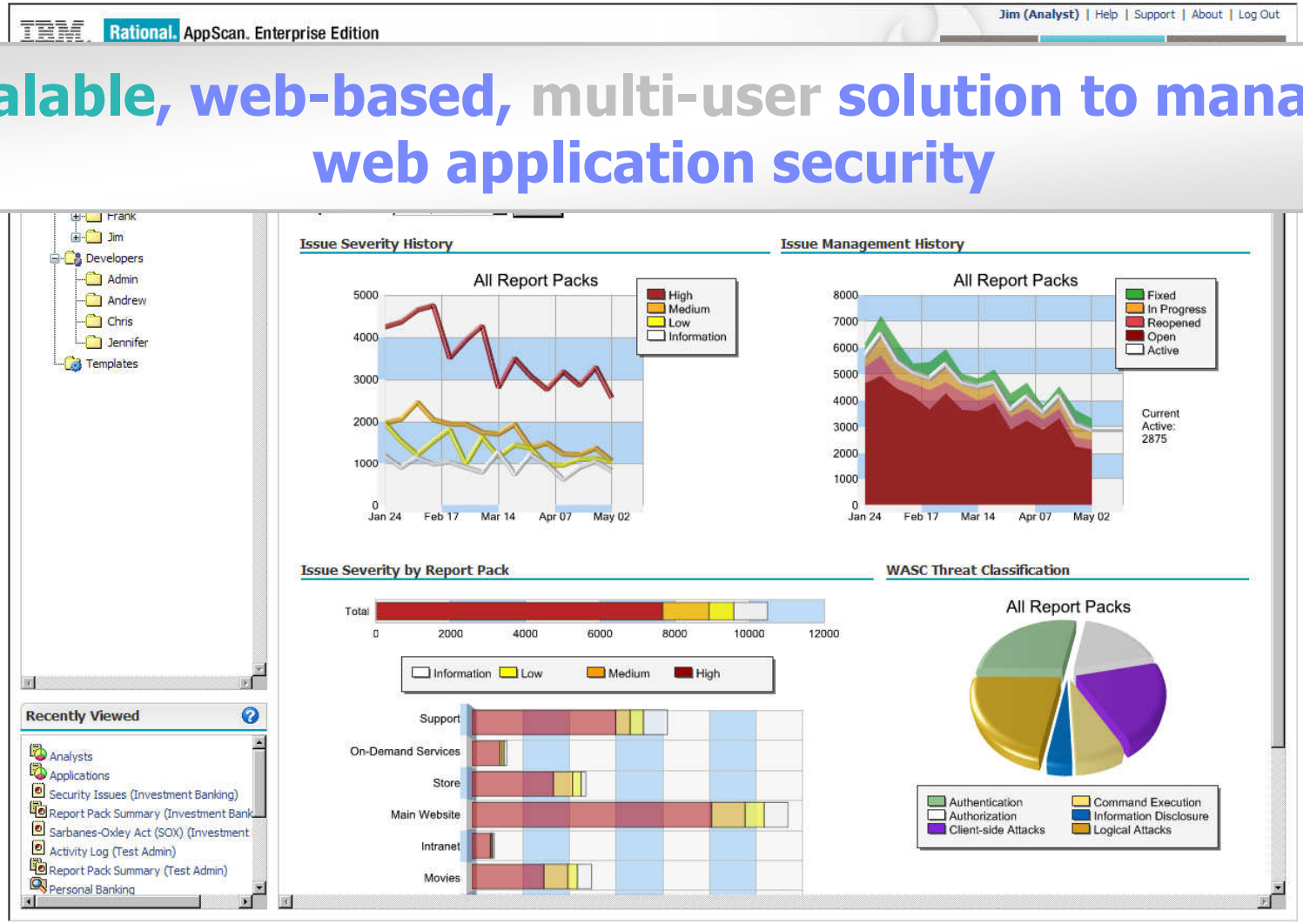


IBM Rational AppScan SDLC Ecosystem

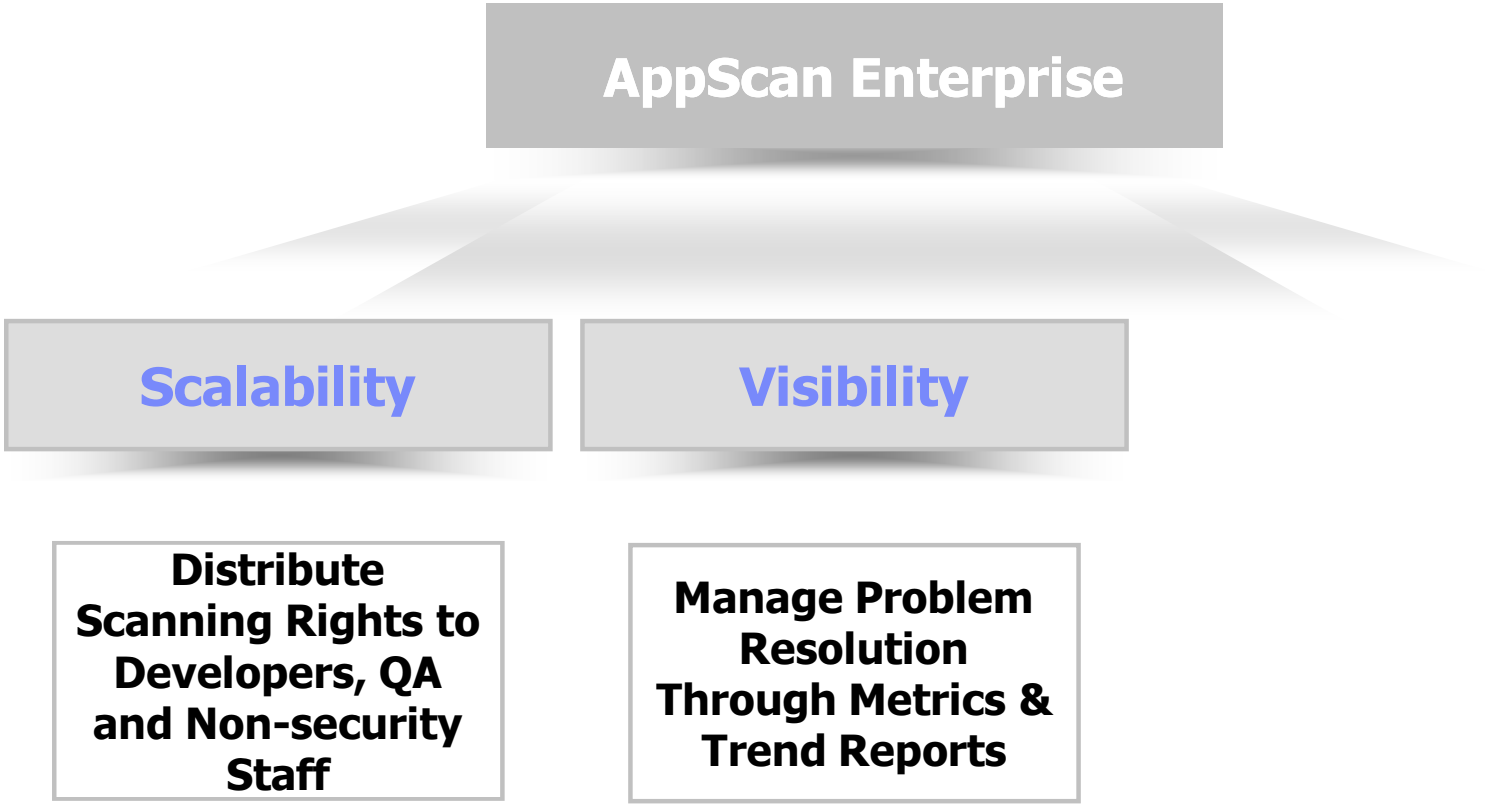


AppScan Enterprise Edition

scalable, web-based, multi-user solution to manage web application security



The Power of AppScan Enterprise



Visibility throughout the Enterprise

Dashboards | **Reports**

CSO / CIO | Divisions | Applications | Compliance Officers | Developers

Entire Organization

Group Portal

Berkshire Life

Individual Markets

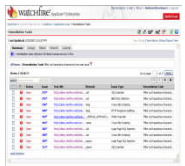
Equity Investments

EFORMS

Application 1

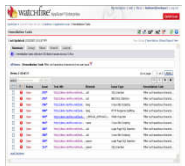
Application 2

Security Issues



PCI

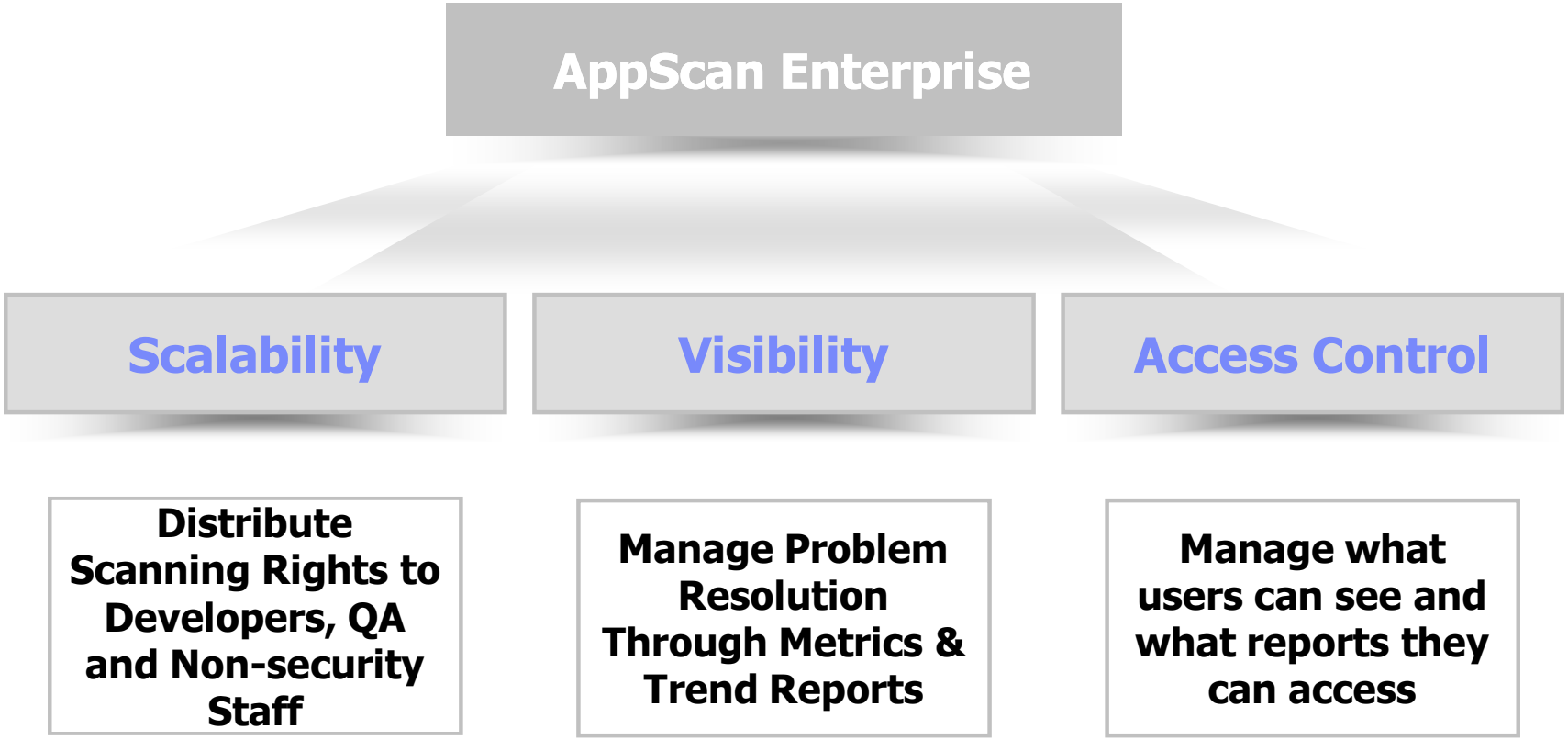
ISO 17799



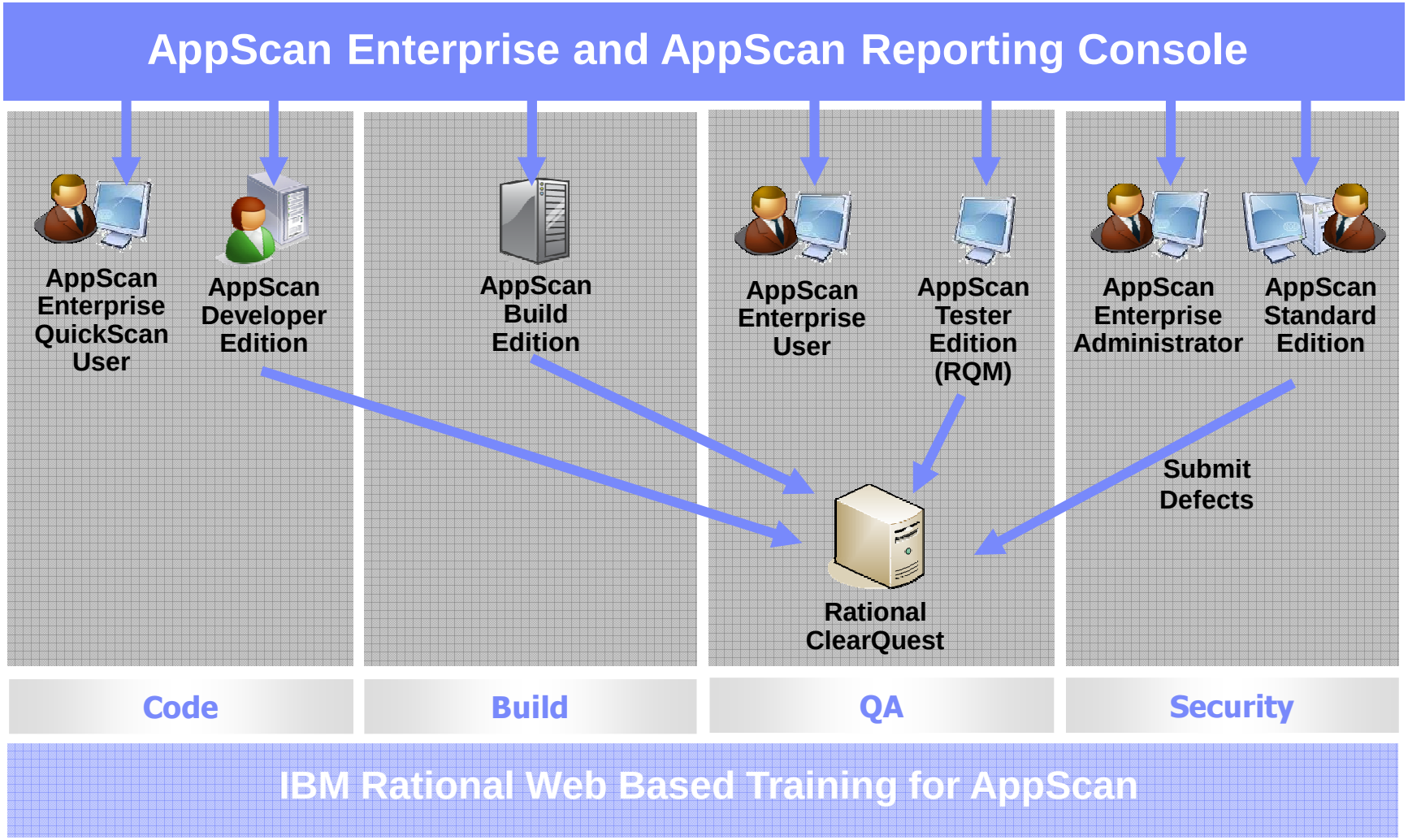
Remediation Report

Trending Report

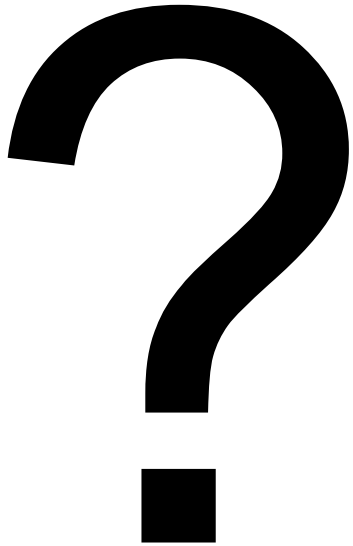
The Power of AppScan Enterprise



IBM Rational AppScan SDLC Ecosystem



Questions



QuickScan – What Is It?

- QuickScan gives developers black box scanning capability from a simple, self-service web portal
- QuickScan leverages administrator-defined Scan Templates, so running a scan is as simple as clicking a button
  - Shields developers from the complexity of configuring a scan
  - Keeps control in the hands of the security team