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

Kedar Walimbe.
Technical Sales Manager ,IBM Rational
kedar@sg.ibm.com

AS07

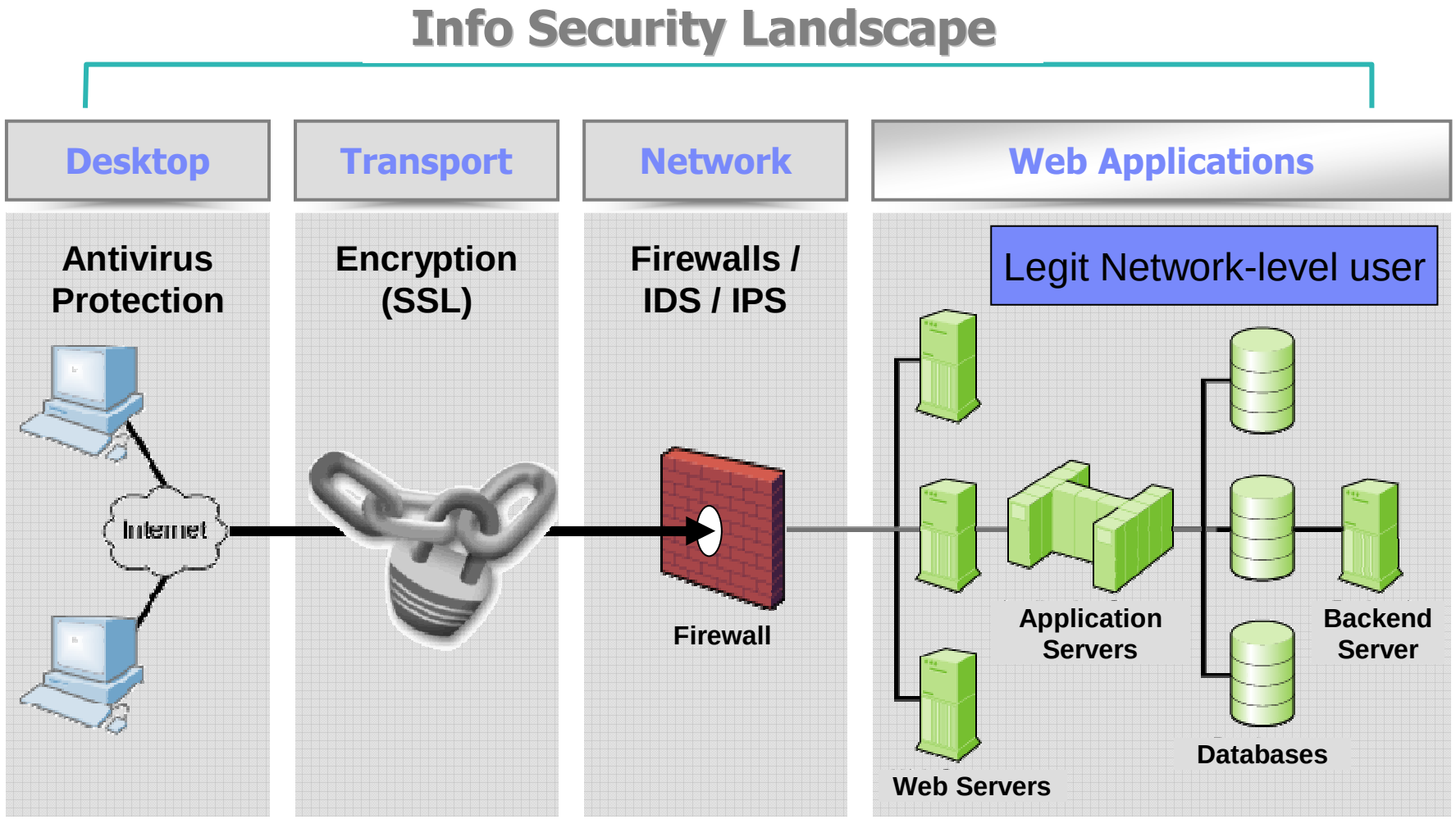
Rational. software

Go to IBM

Security is Quality

The Myth: “Our Site is Safe”

Each layer of the application requires its own security measures



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

PCI Security Standards Council

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

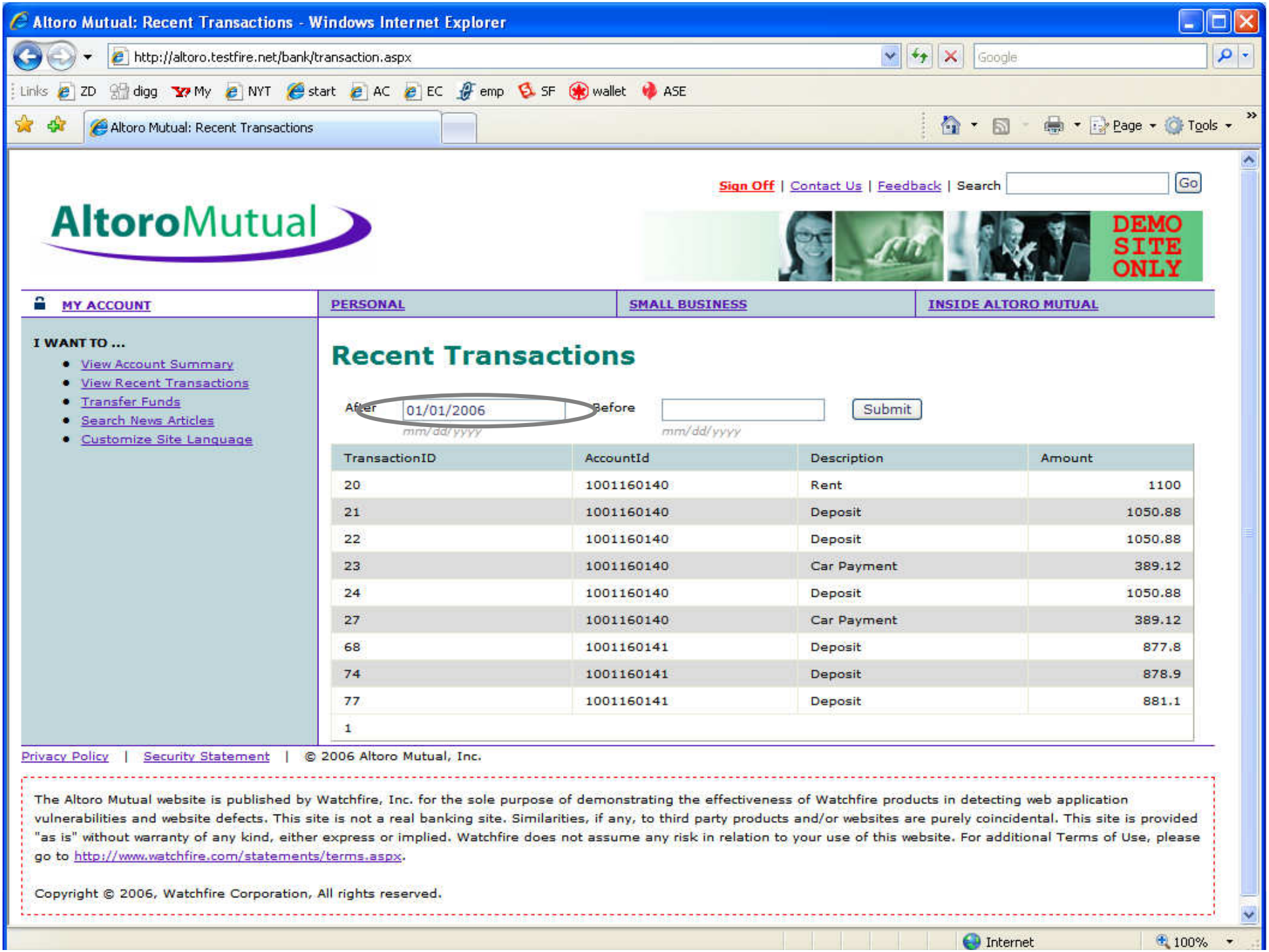
Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database 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

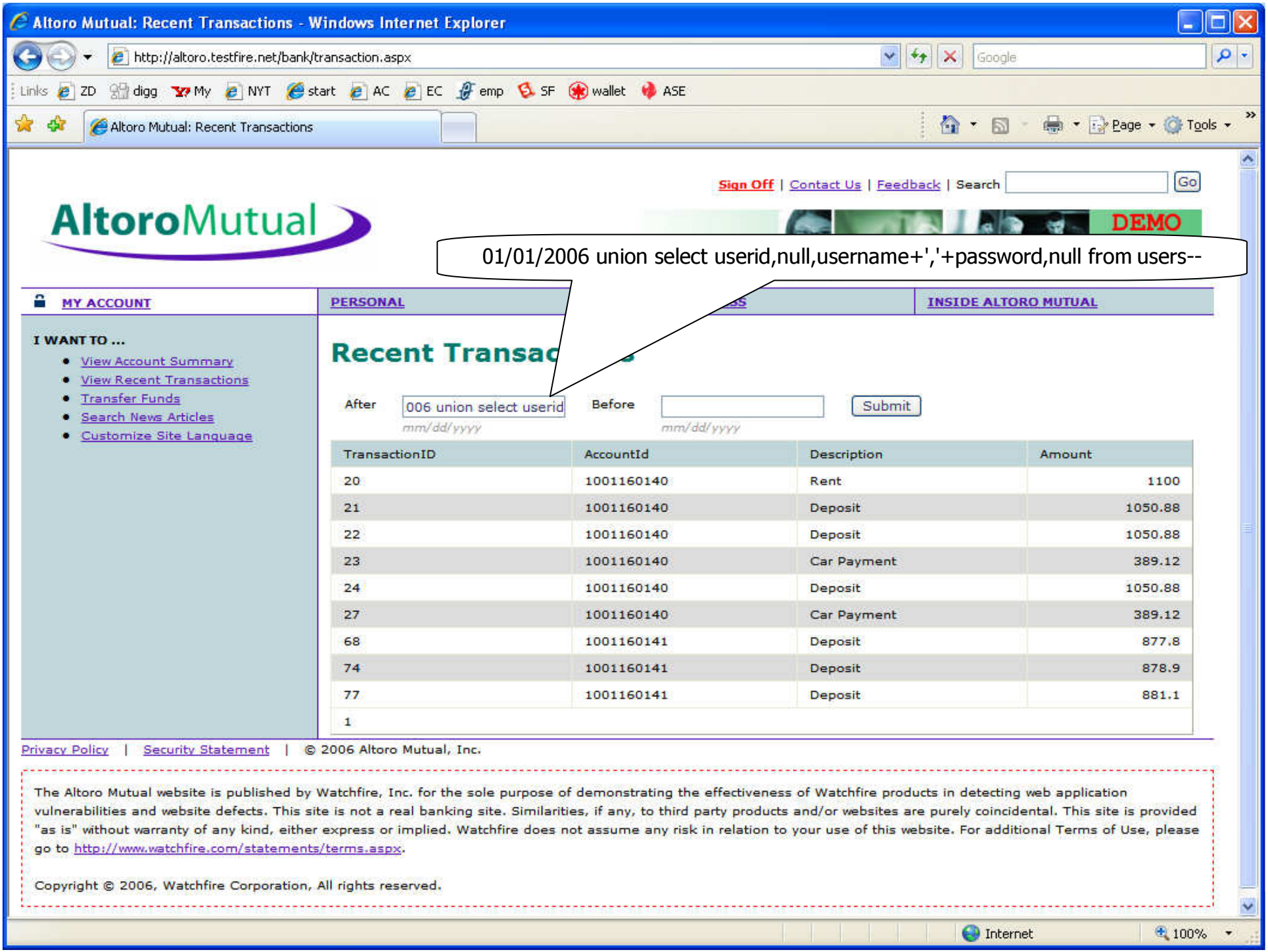
For example, Injection Flaws are an important type of security defect that result from flaws in the application

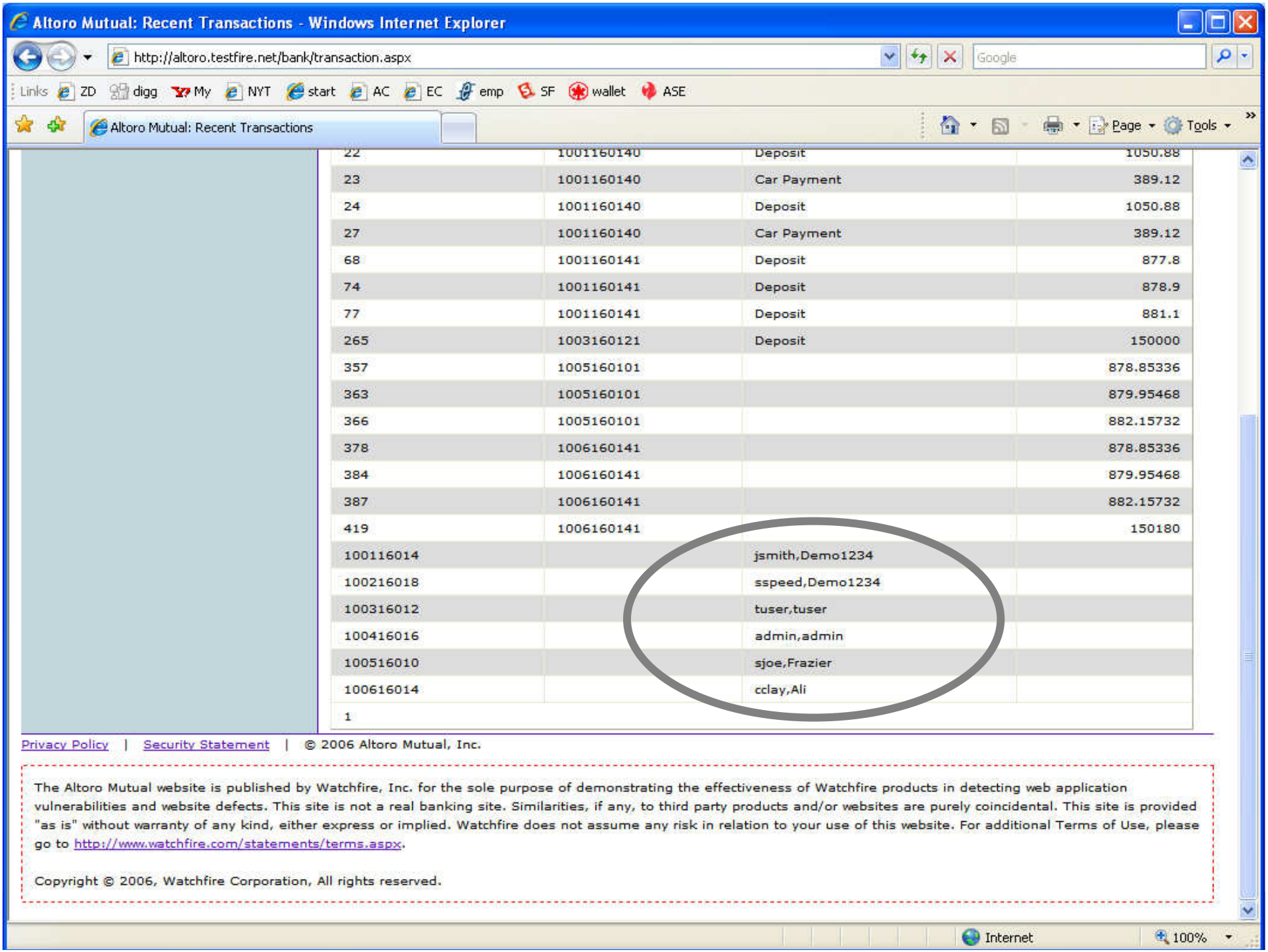
- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.
- What are the implications?
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands on server and access sensitive data
  - LDAP Injection – Bypass authentication


Altoro Mutual: Online Banking Login - Windows Internet Explorer
http://altoro.testfire.net/bank/login.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Online Banking Login
Page Tools
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: jsmith
Password: ••••••••
Login
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.
Internet
100%

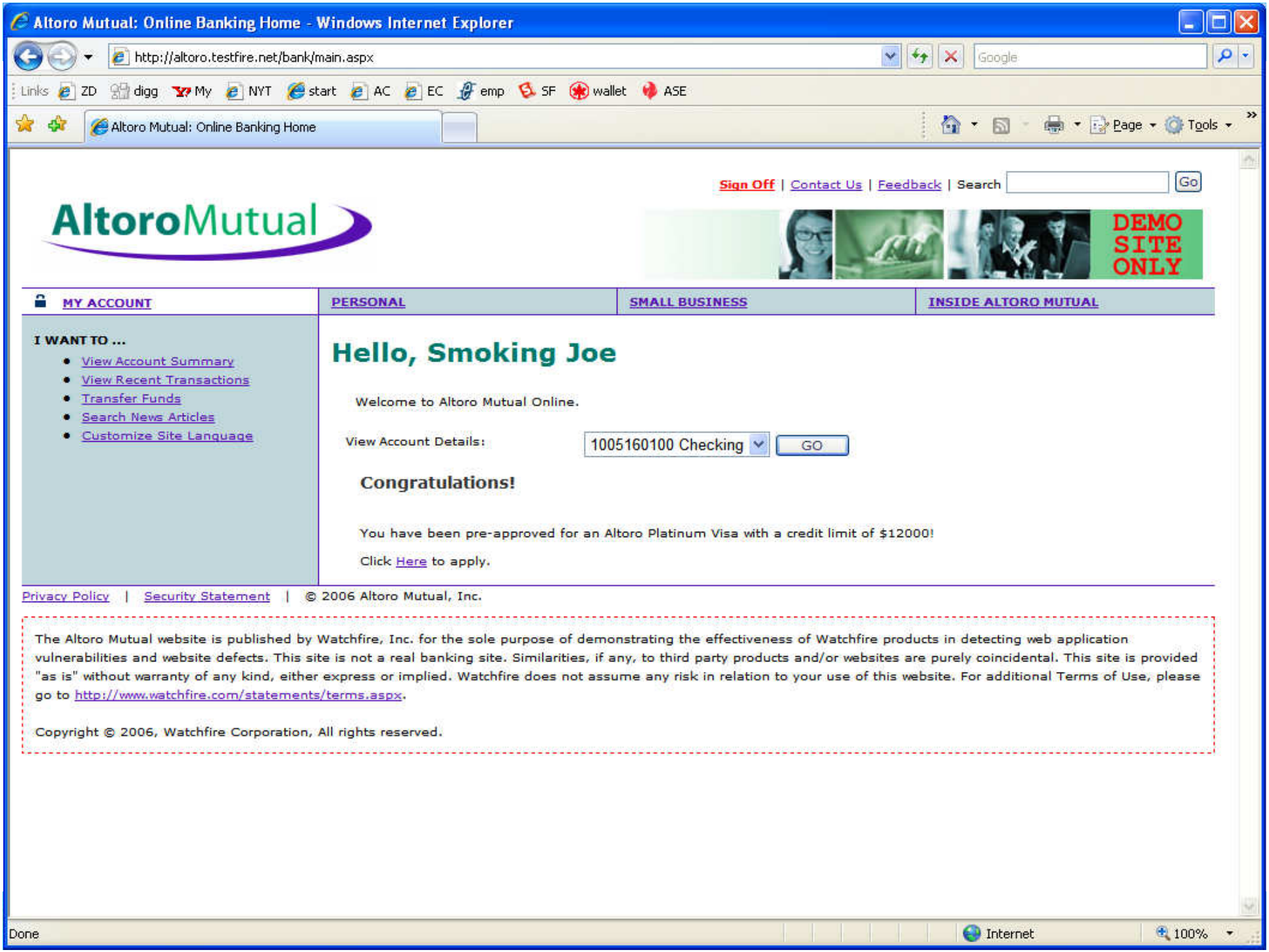

Altoro Mutual: Online Banking Home - Windows Internet Explorer
http://altoro.testfire.net/bank/main.aspx
Gmail - Inbox (73)
eWEEK.com - Enterprise Tec...
Altoro Mutual: Online Ban...
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO 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
GO
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.
Internet
100%


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Altoro Mutual: Recent Transactions
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
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 01/01/2006 mm/dd/yyyy
Before mm/dd/yyyy
Submit
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
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.
Internet
100%


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Altoro Mutual: Recent Transactions
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
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 Transac
After
006 union select userid
mm/dd/yyyy
Before
mm/dd/yyyy
Submit
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
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.
Internet
100%


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Recent Transactions
Page Tools
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
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.
Internet
100%


Altoro Mutual: Online Banking Login - Windows Internet Explorer
http://altoro.testfire.net/bank/login.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Online Banking Login
Page Tools
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: sjoe
Password: •••••••
Login
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.
Internet
100%


Altoro Mutual: Online Banking Home - Windows Internet Explorer
http://altoro.testfire.net/bank/main.aspx
Google
Links ZD digg My NYT start AC EC emp SF wallet ASE
Altoro Mutual: Online Banking Home
Page Tools
Sign Off | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
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 GO
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.
Done
Internet
100%

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

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

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 comes in

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

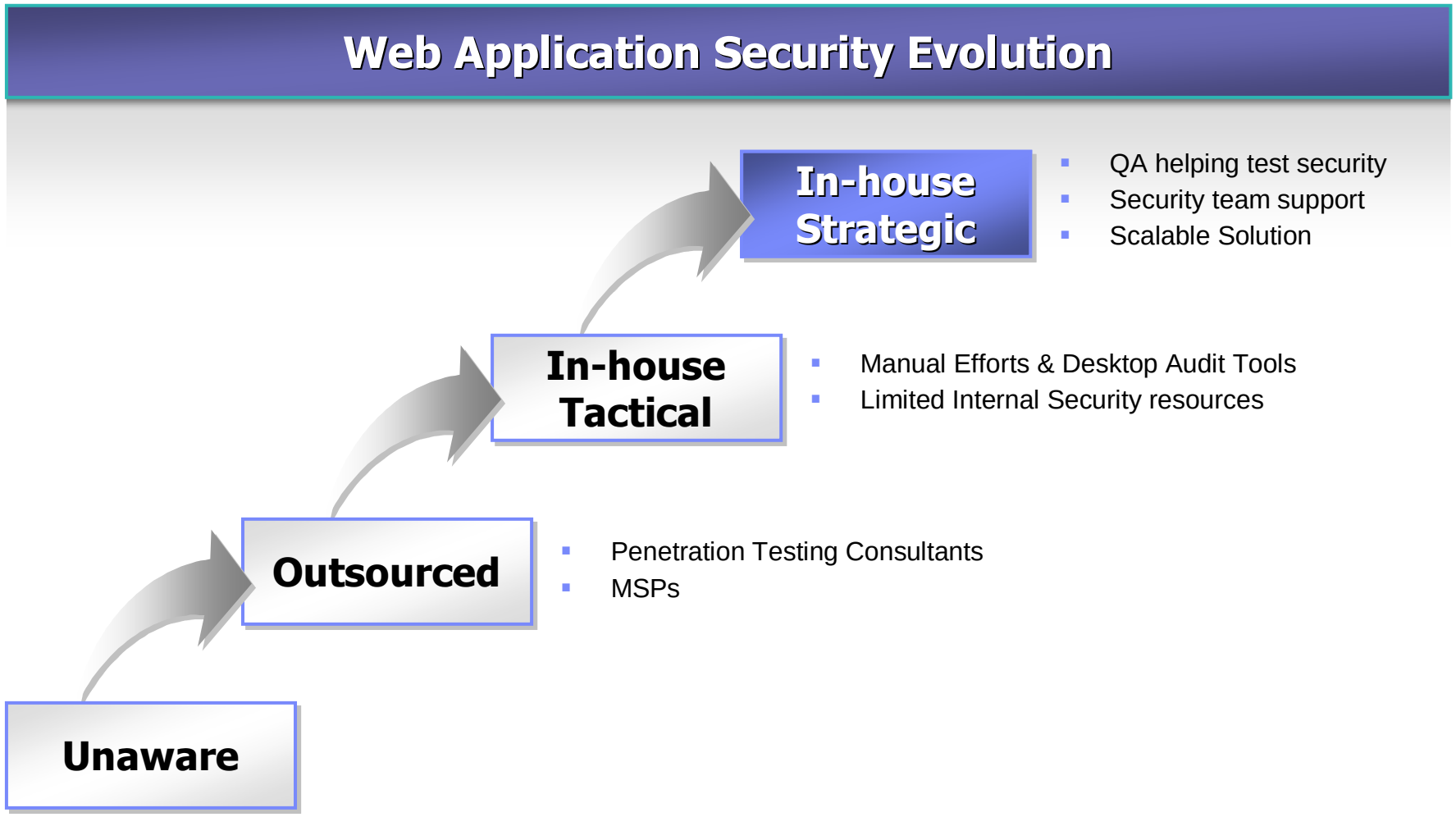
- Knows security in-depth
- Knows corporate and industry standards
- Can exploit security defects to prove impact
- Is responsible for the security of application

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

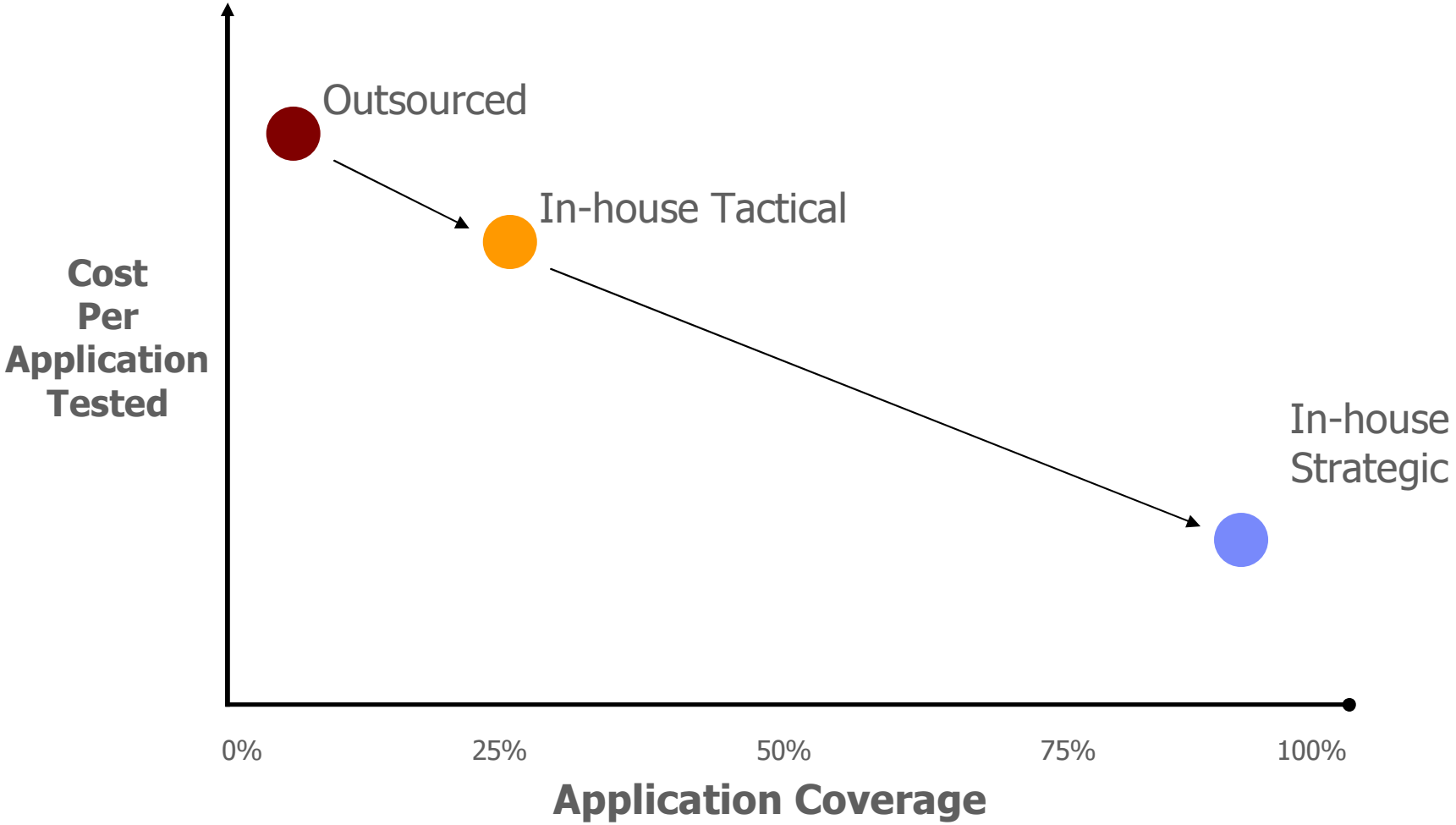
Web application security testing is about finding security defects, but it is also important to understand the issues and how they are fixed

- 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

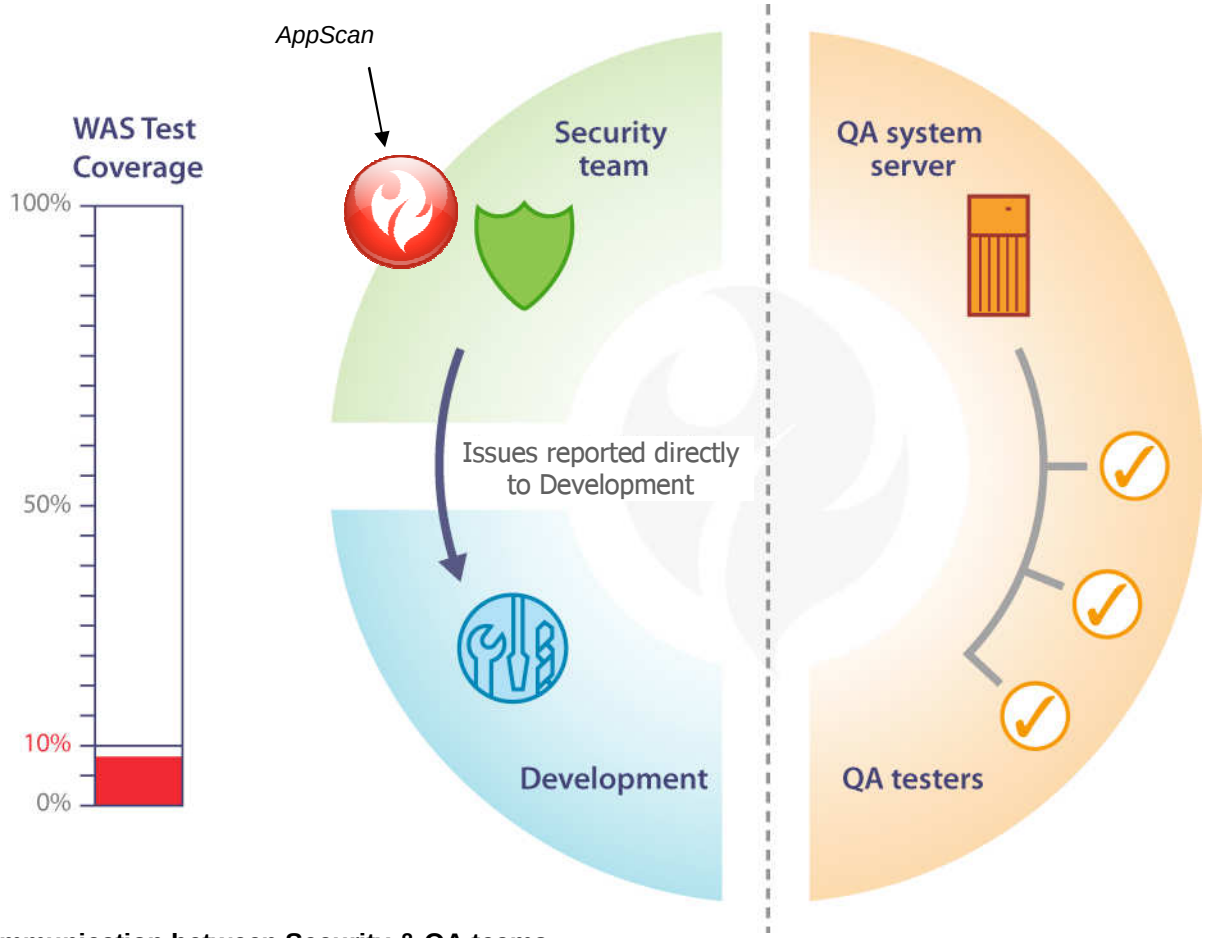
Many organizations move through a maturity model as they adopt web application security testing



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

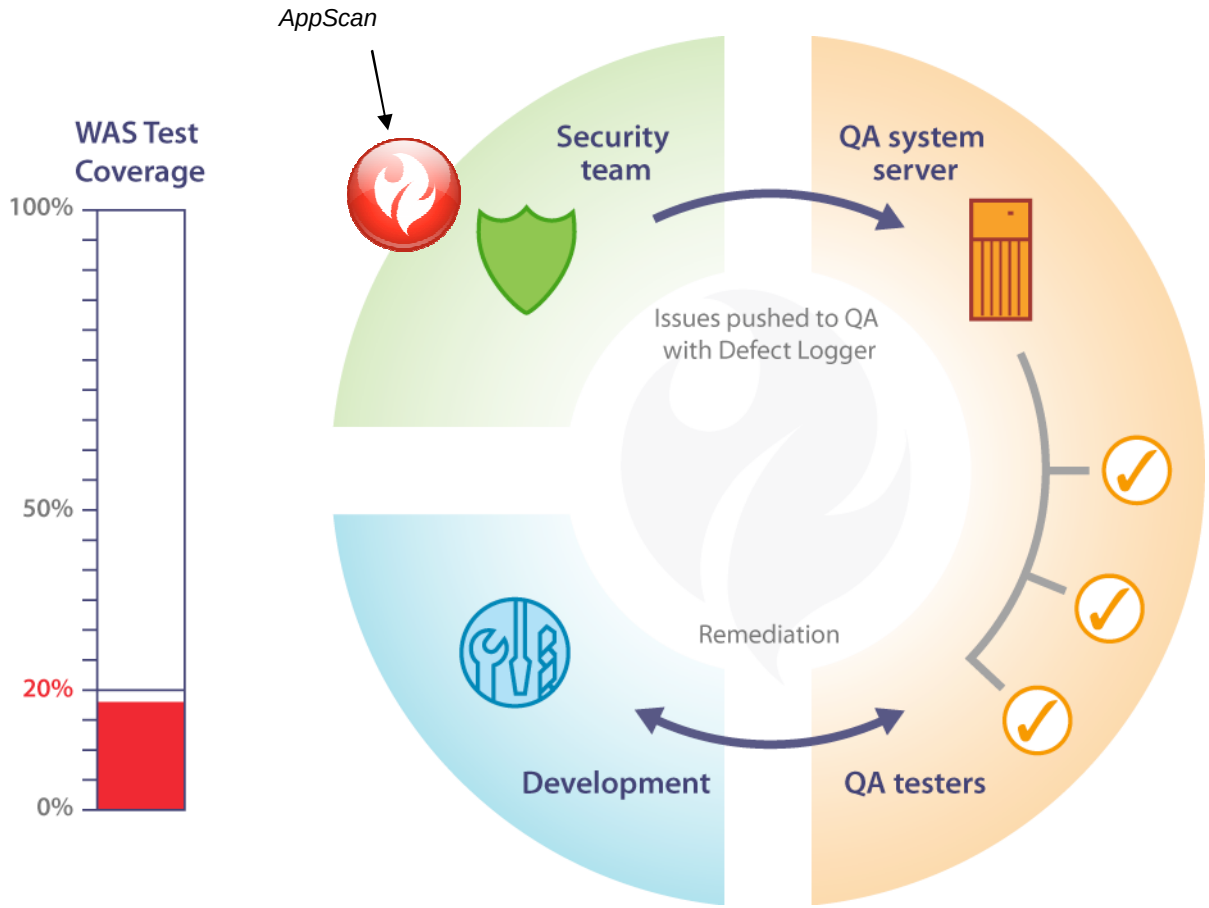


At first, there is little or no QA involvement in security testing and little test coverage is achieved



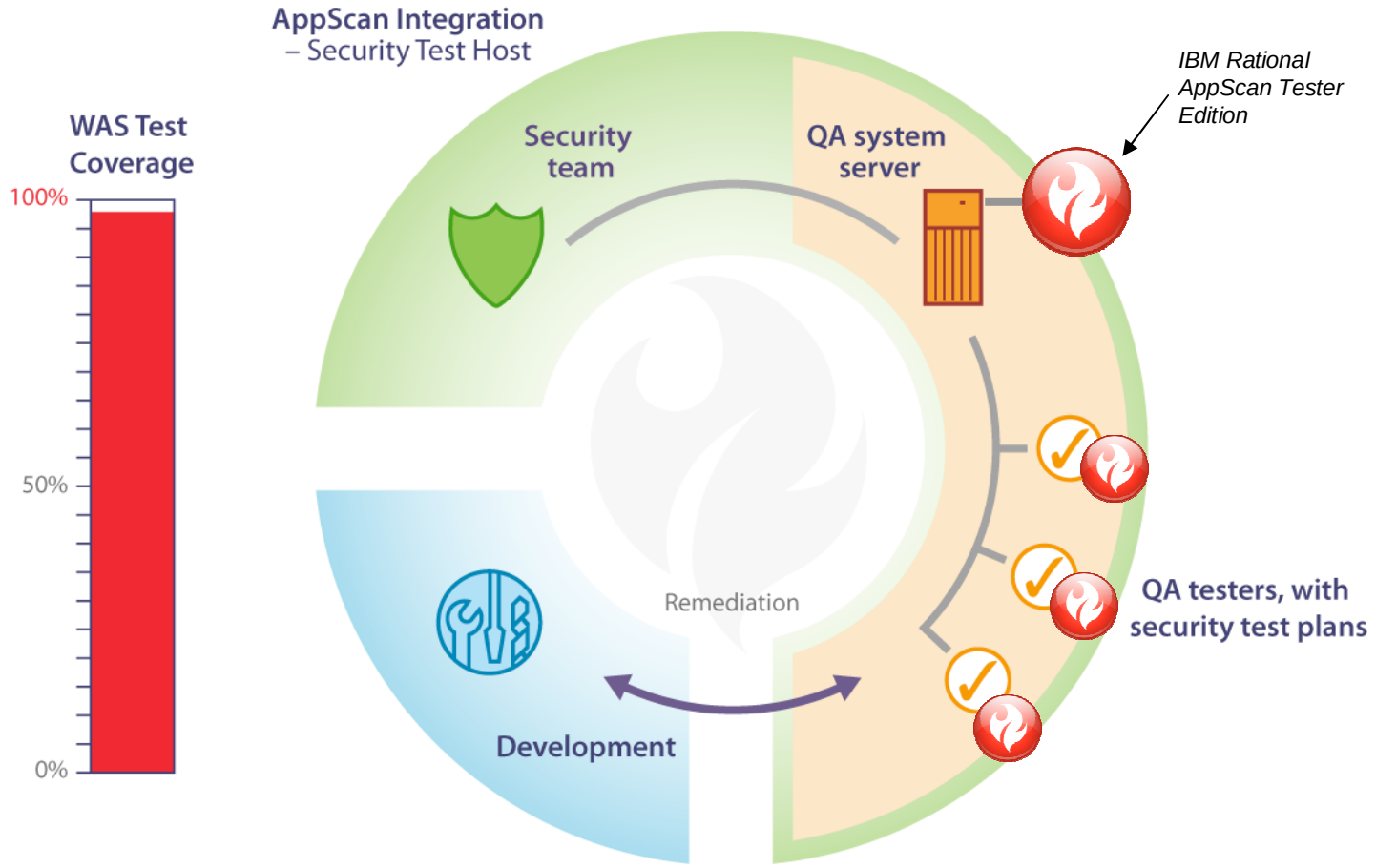
- **No communication between Security & QA teams**

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



- **QA Introduced to WAS; process not yet formalized**

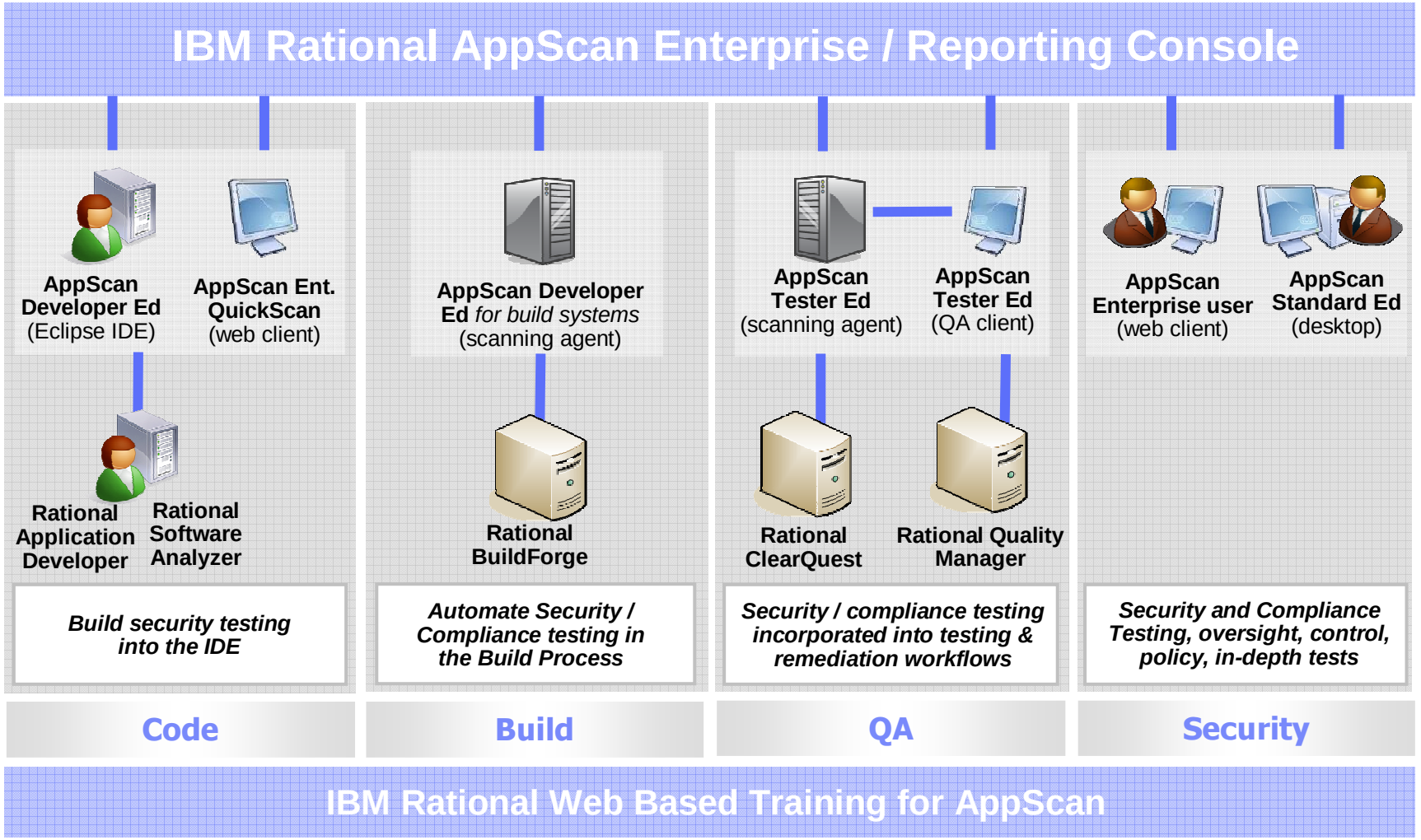
Finally, QA is fully engaged in security testing and test coverage approaches 100%



- **QA responsible for WAS**

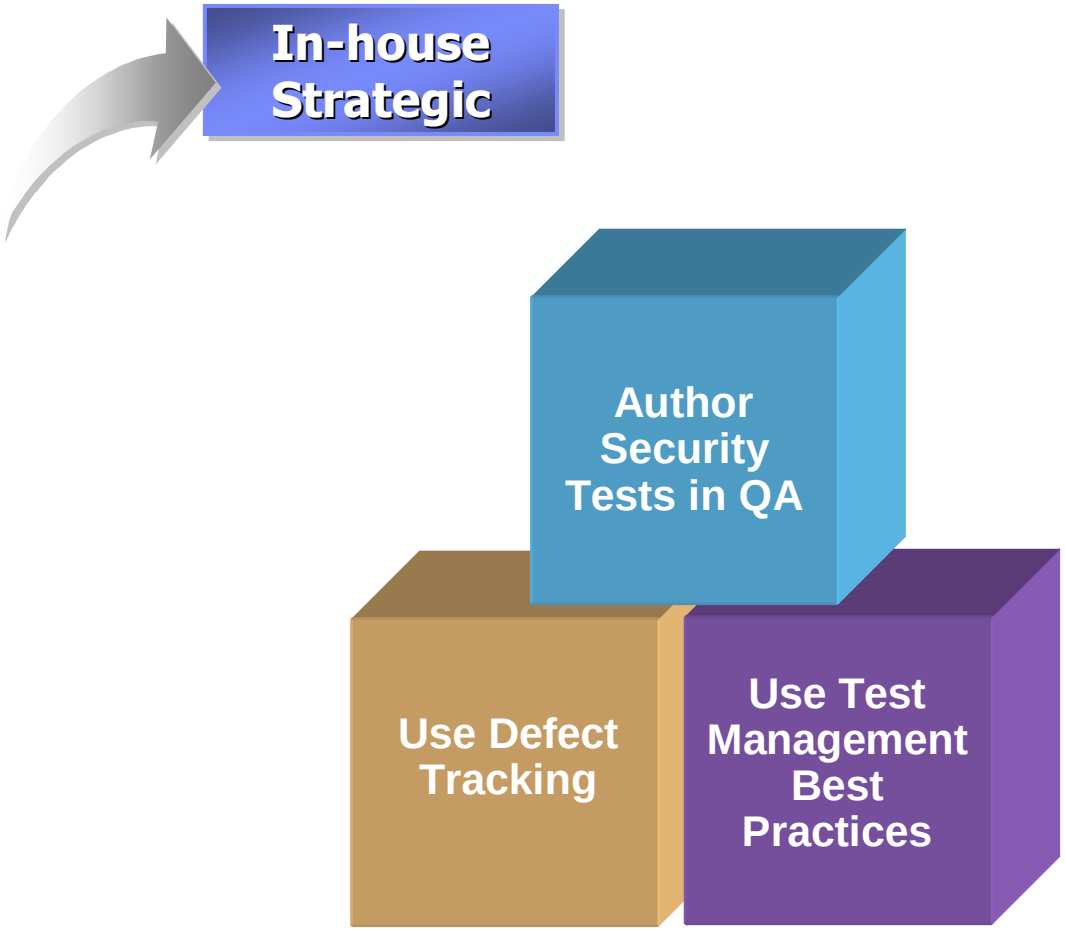
Includes Fall 2008 Releases

Security needs attention across the software development lifecycle

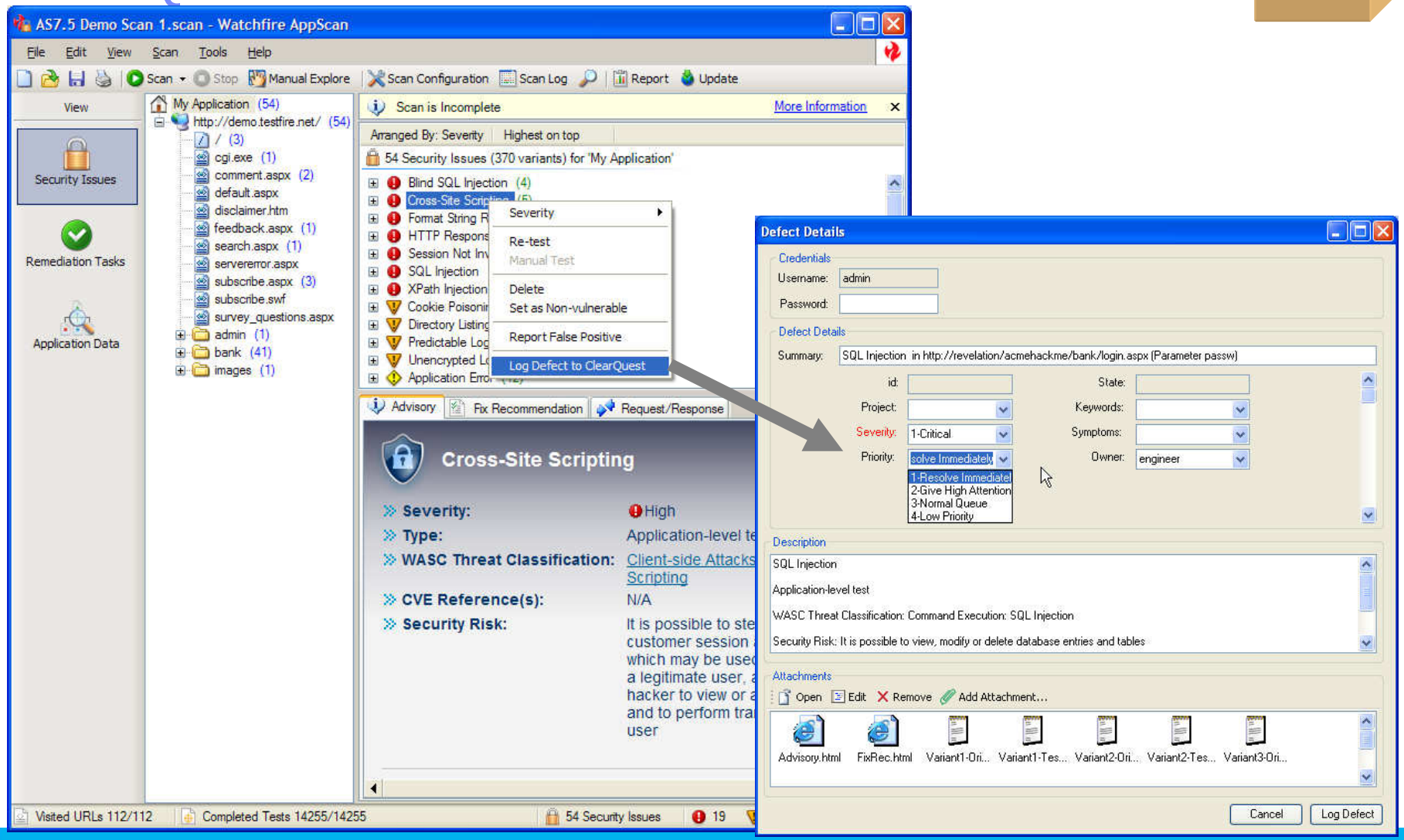


Phased Adoption of Security Testing in QA

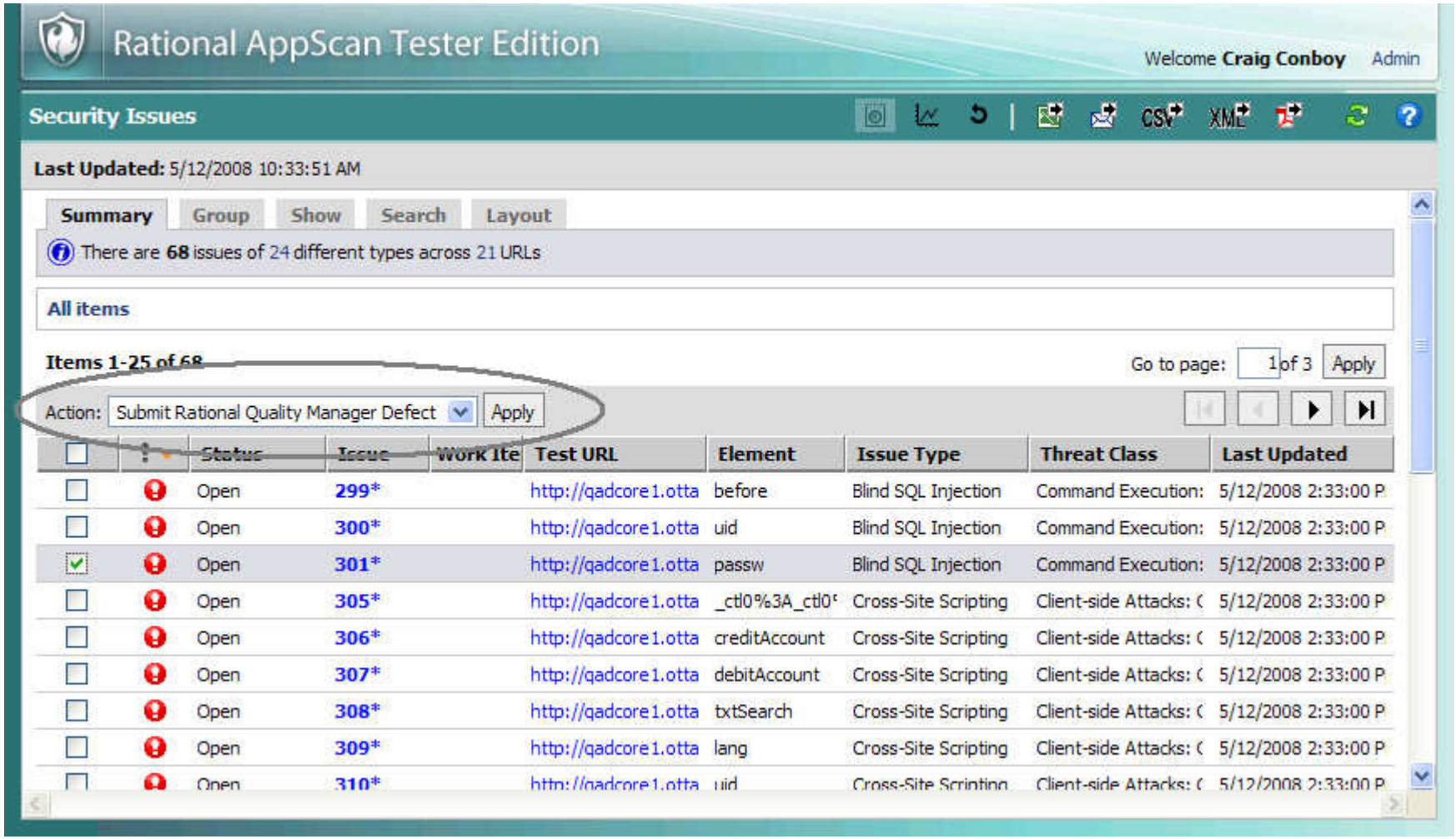
Engaging your QA team in security testing, one step at a time



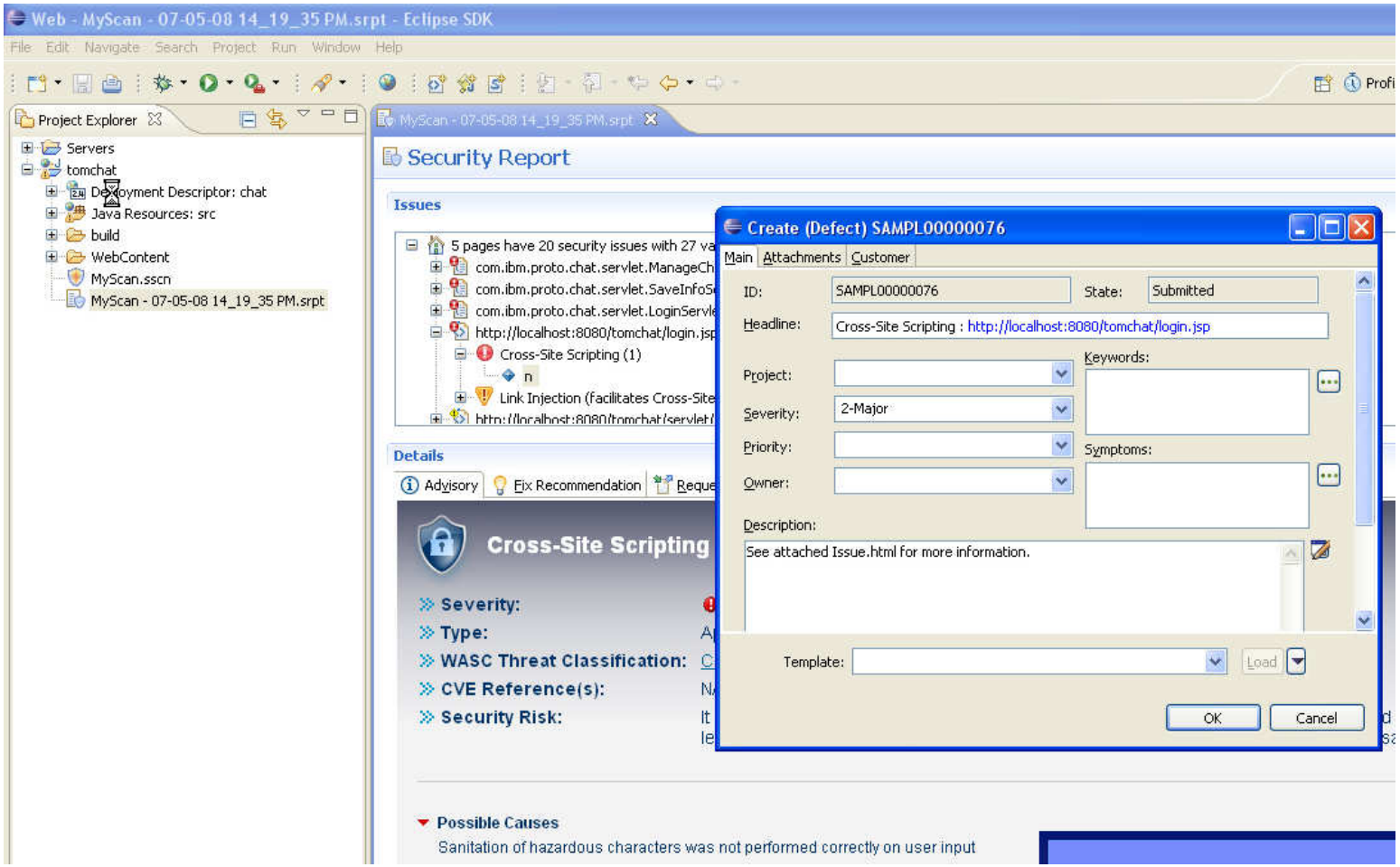
Using Rational AppScan Standard Edition with ClearQuest



Using Rational AppScan Tester Edition with Rational Team Concert



Using Rational AppScan Developer Edition with ClearQuest



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

SQL Injection

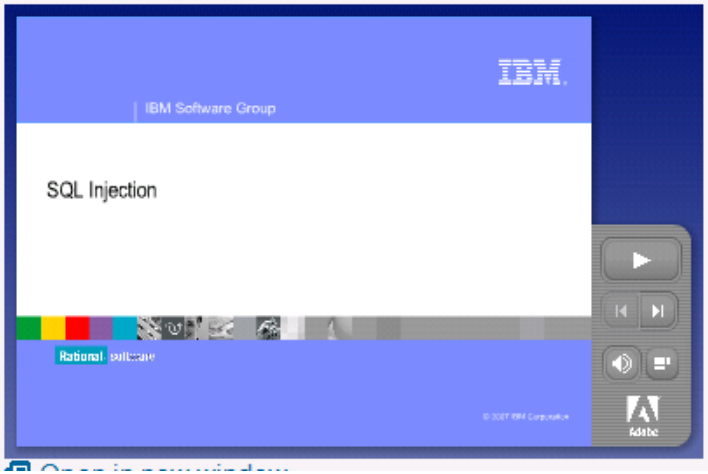
- **Severity:** High
- **Type:** Application-level test
- **WASC Threat Classification:** Command Execution: SQL Injection
- **CVE Reference(s):** N/A
- **Security Risk:** It is possible to view, modify or delete database entries and tables

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 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
Damage 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 contol of the application and/or the ability to view underlying network or database infrastucture. Large cost associated with impact	Full compromise of Network or Database Infrastucture. Extensive cost associated with impact
Reproducibility	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)
Exploitability	Seasoned securtiy skills and/or speacialised tools required	Extensive skills and tools required	Moderate skills and tools required	limited skills and tools required	no skill or tools required
Affected 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++)
Discoverability	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)

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

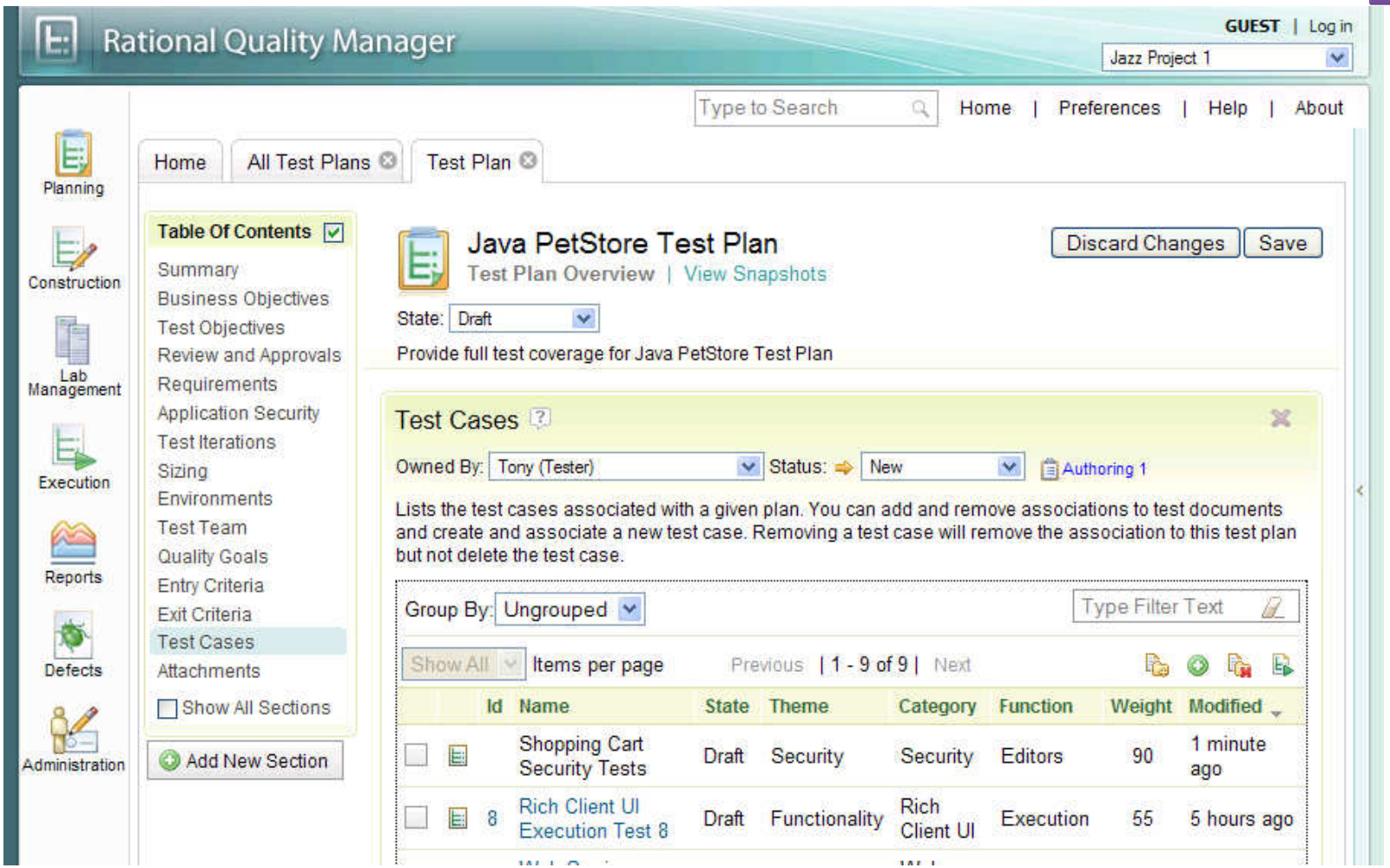
Manage your security testing like other types of testing

- 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



Execute your security tests

Report on test execution status and trend

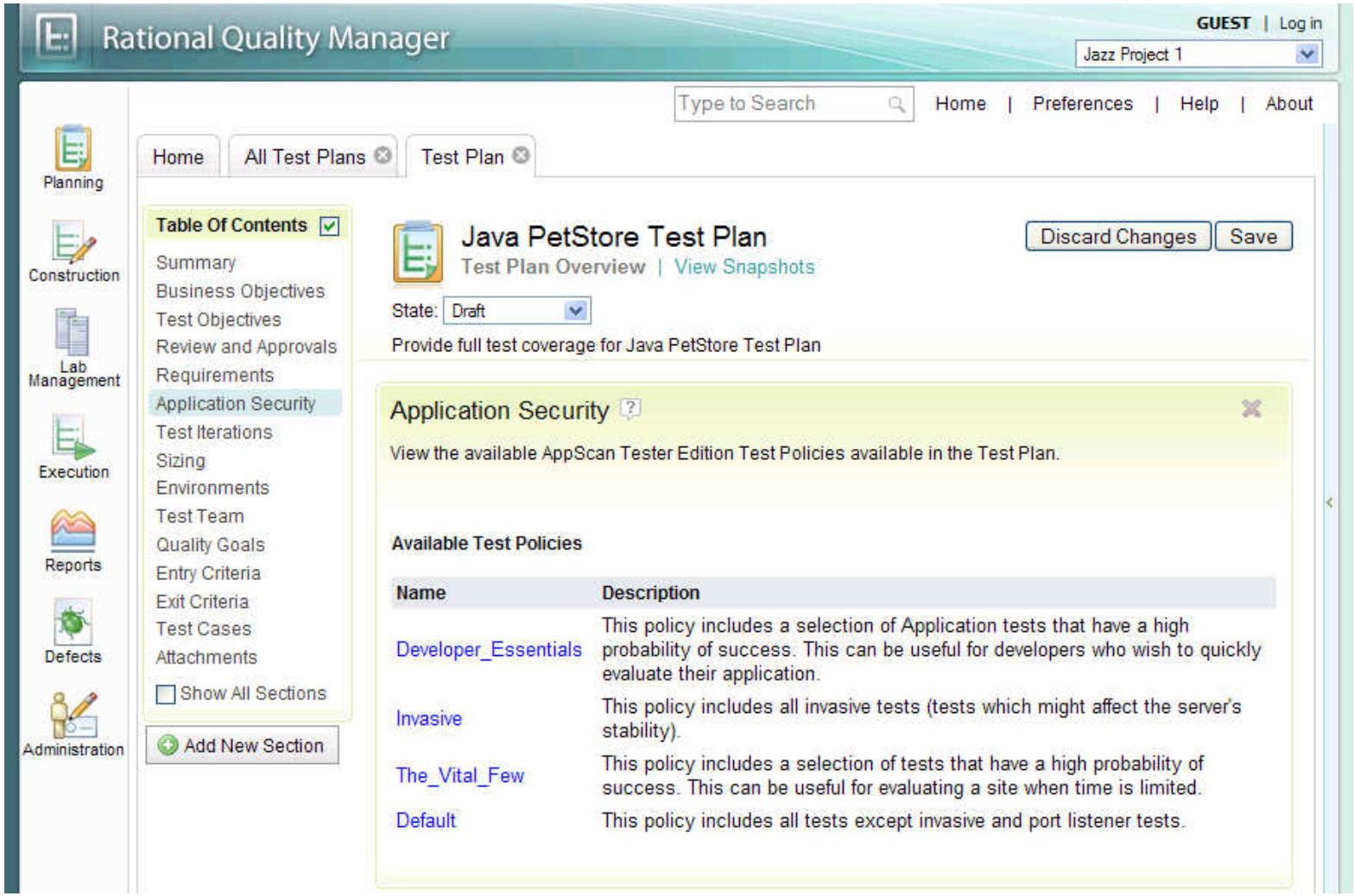
Use Test Mgmt Best Practices

Enable your testers to create security tests

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

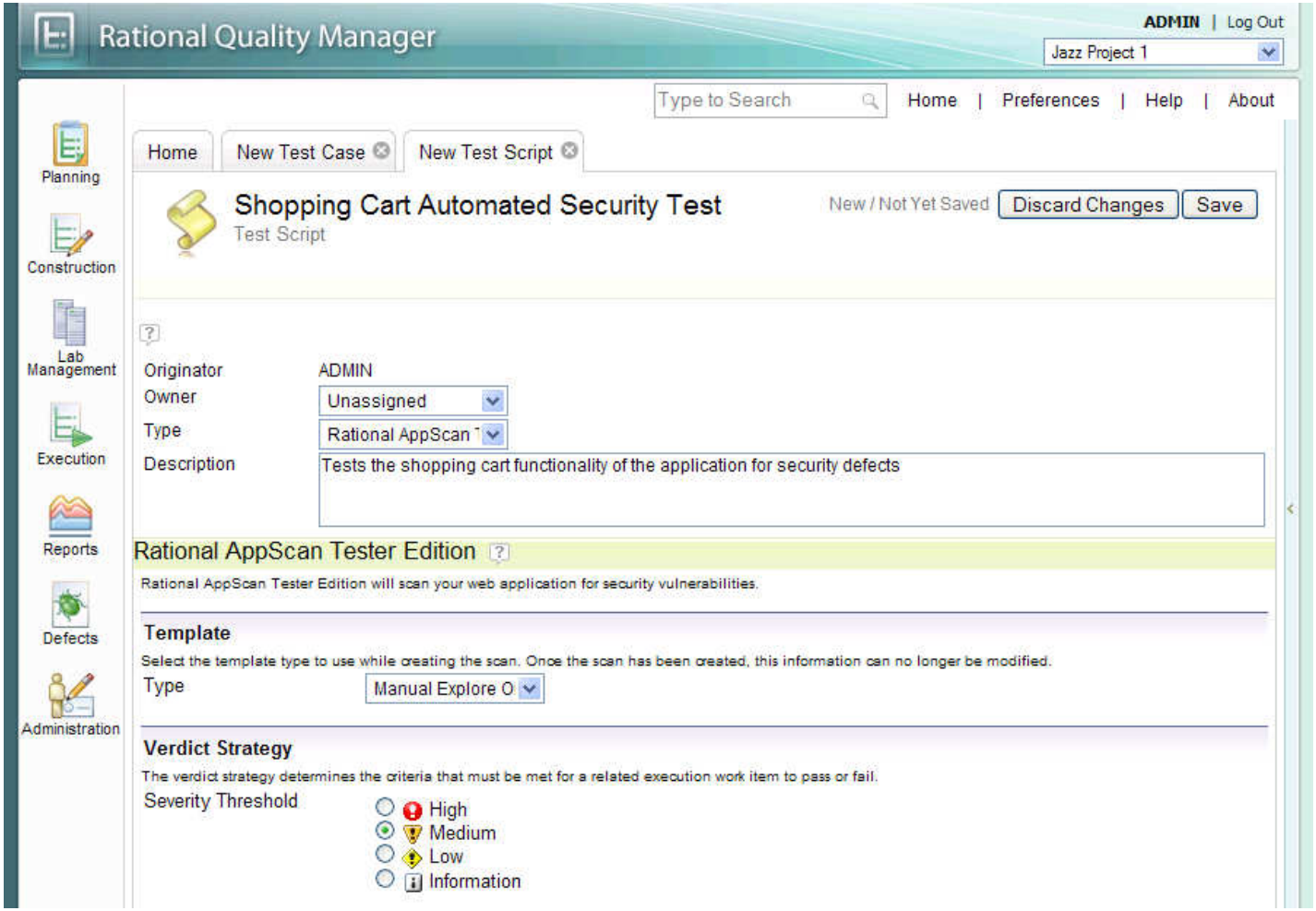
Define Test Policies for all testers to use

Author Security Tests in QA



Create AppScan Tester Edition tests from Rational Quality Manager

Author Security Tests in QA



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:

- 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