



IBM Rational Software Conference 2009
As Real as It Gets!



Securing Your Web Applications Using IBM® Rational® AppScan Standard Edition

Danny Allan
Director of Security Research, IBM Rational
dallan@us.ibm.com

Rational. software

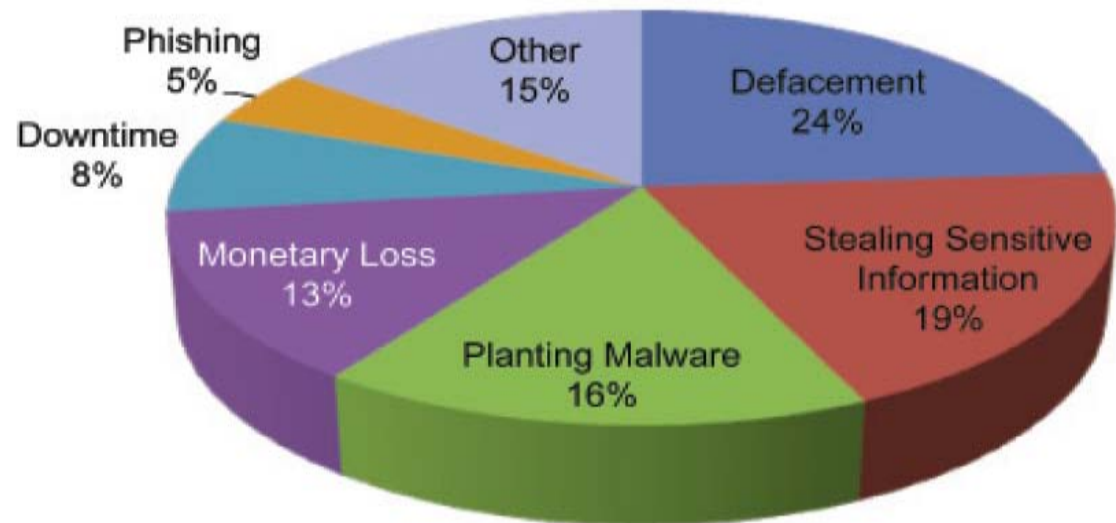
Agenda

- Quick Intro
 - ▶ 2009 reported Web Application Security Incidents

- IBM Rational AppScan
 - ▶ Overview
 - ▶ Demo
 - ▶ Wrap up

Drivers for Web Application Attacks*

Attack Goal	%
Defacement	24%
Stealing Sensitive Information	19%
Planting Malware	16%
Monetary Loss	13%
Downtime	8%
Phishing	5%
Deceit	2%
Worm	1%
Link Spam	1%
Information Warfare	1%



Web Applications hacks have replaced email as the preferred delivery method of Malware (viruses, root kits and trojans)

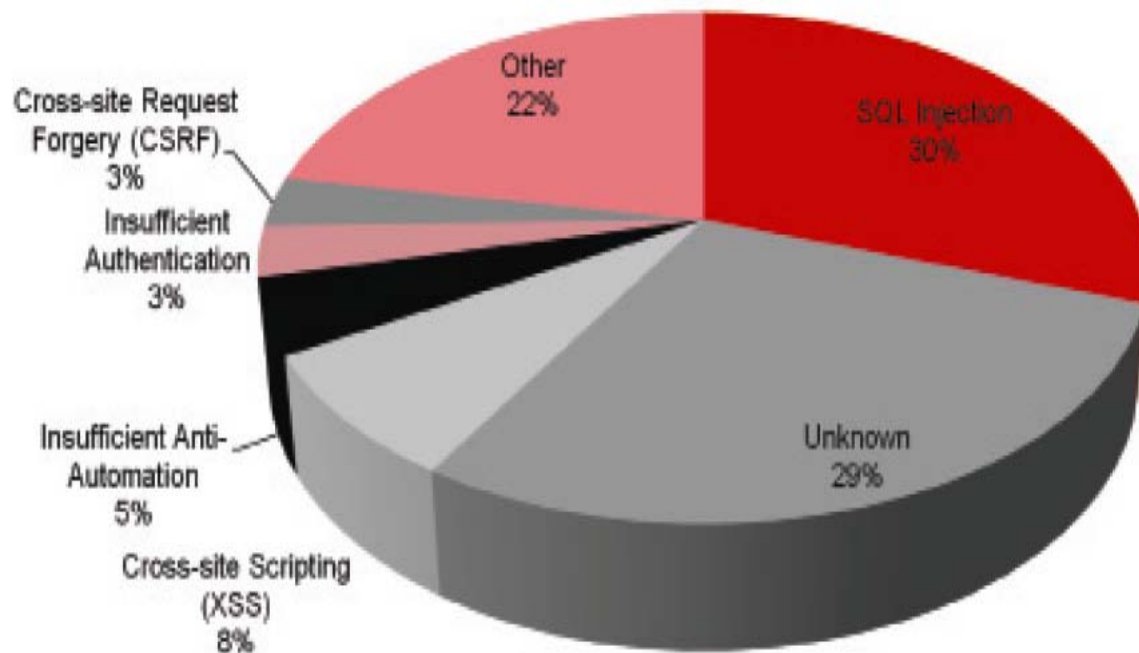
*From Web Hacking Incidents Database 2008

SQL injection vector used to plant malware

- Over 500,000 Web Sites compromised via SQL injection
 - ▶ Done via automated attack which altered contents of back end database and injected malicious script
 - ▶ Turned legitimate Web Sites into Malware distribution centres

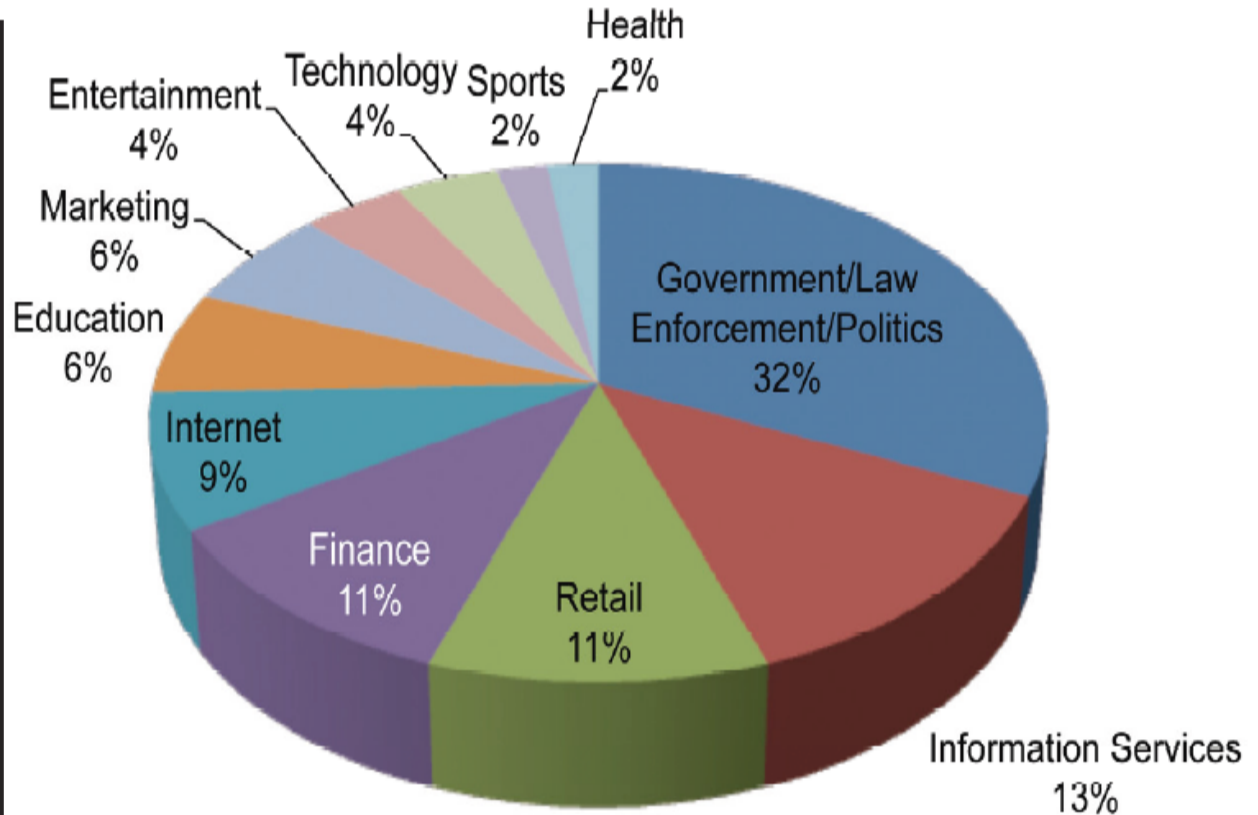
Incident by Attack Type (2008)

Attack / Vulnerability Used	%
SQL Injection	30%
Unknown	29%
Cross-Site Scripting (XSS)	8%
Insufficient Anti-Automation	5%
Insufficient Authentication	3%
Cross-Site Request Forgery (CSRF)	3%
OS Commanding	3%
Denial of Service	3%
Drive By Pharming	3%
Known Vulnerability	2%
Brute Force	2%
Credential / Session	2%



Incident by Organization Type

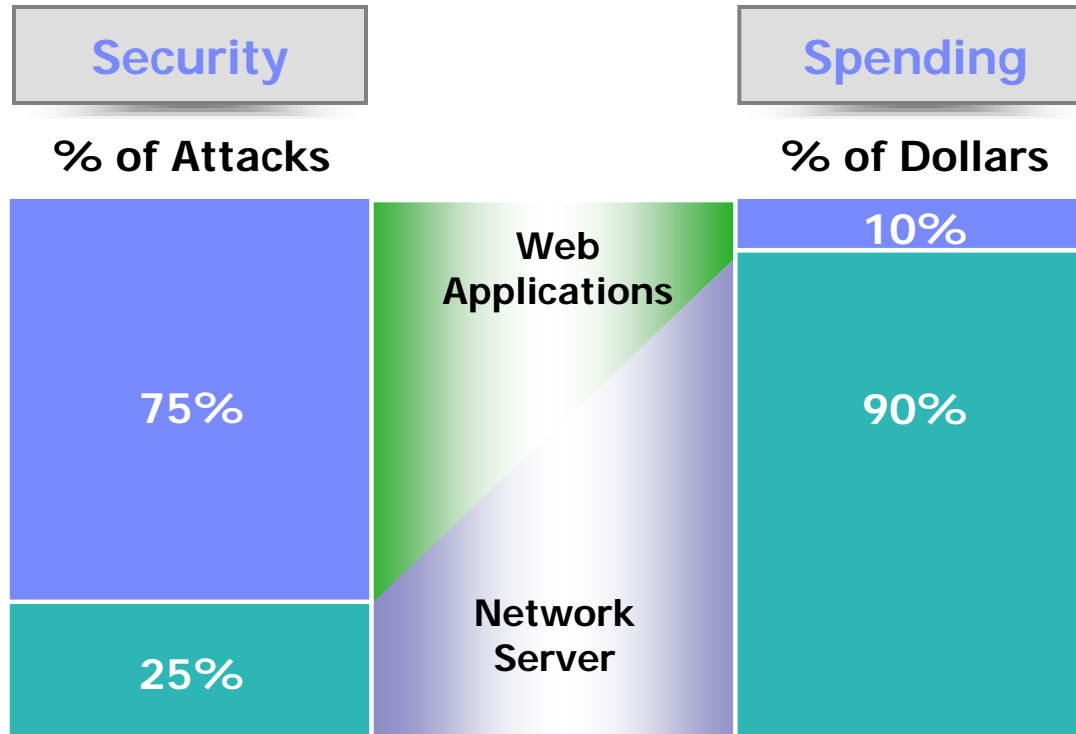
Vertical	%
Government, Security and Law Enforcement	32%
Information Services	13%
Retail	11%
Internet	9%
Education	6%
Marketing	6%
Entertainment	4%
Technology	4%
Sports	2%
Health	2%





Security

The Challenge for Organizations



75% of All Attacks on Information Security Are Directed to the Web Application Layer

Cost of an Application Security Breach

- Media attention/ Brand damage
- Sharp decline in Stock Prices
- Communication/Monitoring Service Costs
- Legal Fees (Reported \$3-4 million/incident)
- FTC Penalties (Fines can range up to 15 million/incident)
- Additional 3rd party Audits
- New Security Spending
- Customer Lawsuits
- Customer Loss

TJ Maxx's Application Security Breach cost them over 200 million dollars!!

Why Application Security is a High Priority

- **Web applications are the #1 focus of hackers:**
 - ▶ 75% of attacks at Application layer (Gartner)
 - ▶ XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)

- **Most sites are vulnerable:**
 - ▶ 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
 - ▶ 80% of organizations will experience an application security incident by 2010 (Gartner)
 - ▶ 90% of sites are vulnerable to application attacks (Watchfire)

- **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, GLBA, HIPPA, FISMA,

Organizations must mitigate the risk!

- They need to find and remediate vulnerabilities in Web applications before they are exploited by Hackers
- IBM Rational AppScan can help you do this!

Web App Security Issue Example: SQL Injection

Altoro Mutual: Online Banking Login - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks Tools Help

http://www.althoromutual.com/bank/login.aspx

Sign Off | Contact Us | Feedback | Search [] Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT

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

ADMINISTRATION

- [View Application Values](#)
- [Edit Users](#)

PERSONAL | **SMALL BUSINESS** | **INSIDE ALTORO MUTUAL**

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: [] GO

Privacy Policy | Security Statement | © 2008 Altoro Mutual, Inc.

SELECT true FROM users

WHERE username = ' AND password = '

IBM Rational AppScan

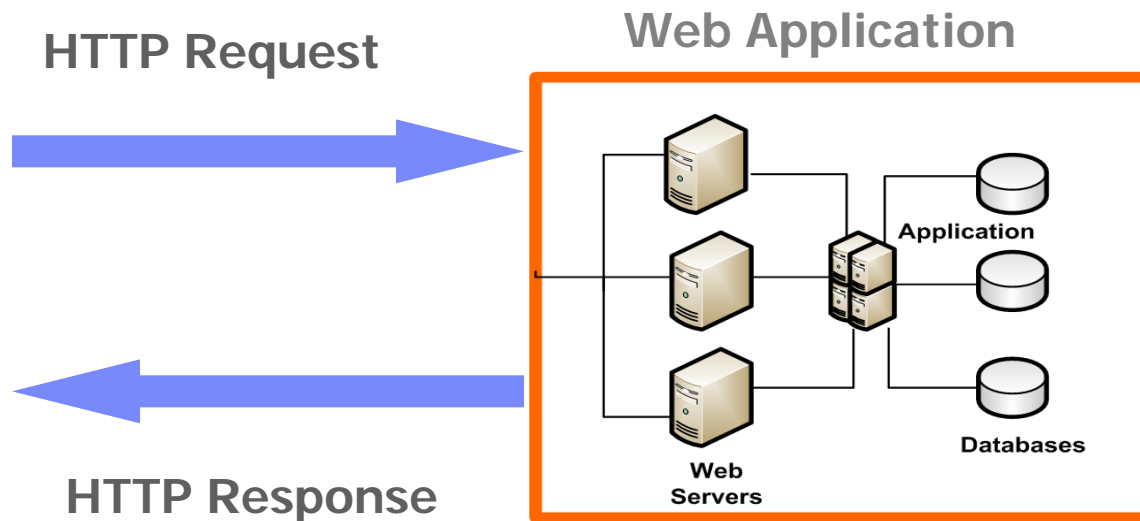
- IBM Rational AppScan: A Web Application Security Scanner
 - ▶ Helps users find and remediate application-layer security issues in their web applications & web services

- IBM Rational AppScan Standard Edition
 - ▶ A standalone desktop application

- Who uses it?
 - ▶ Security Auditors - To bring automation to their audits
 - ▶ IT Security Teams - To reach beyond network security
 - ▶ QA engineers - To add Security to Functionality & Performance testing
 - ▶ Developers (to a lesser extent) – Wanting to be proactive about security

How does AppScan work?

- Approaches an application as a black-box
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected Test policy
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules



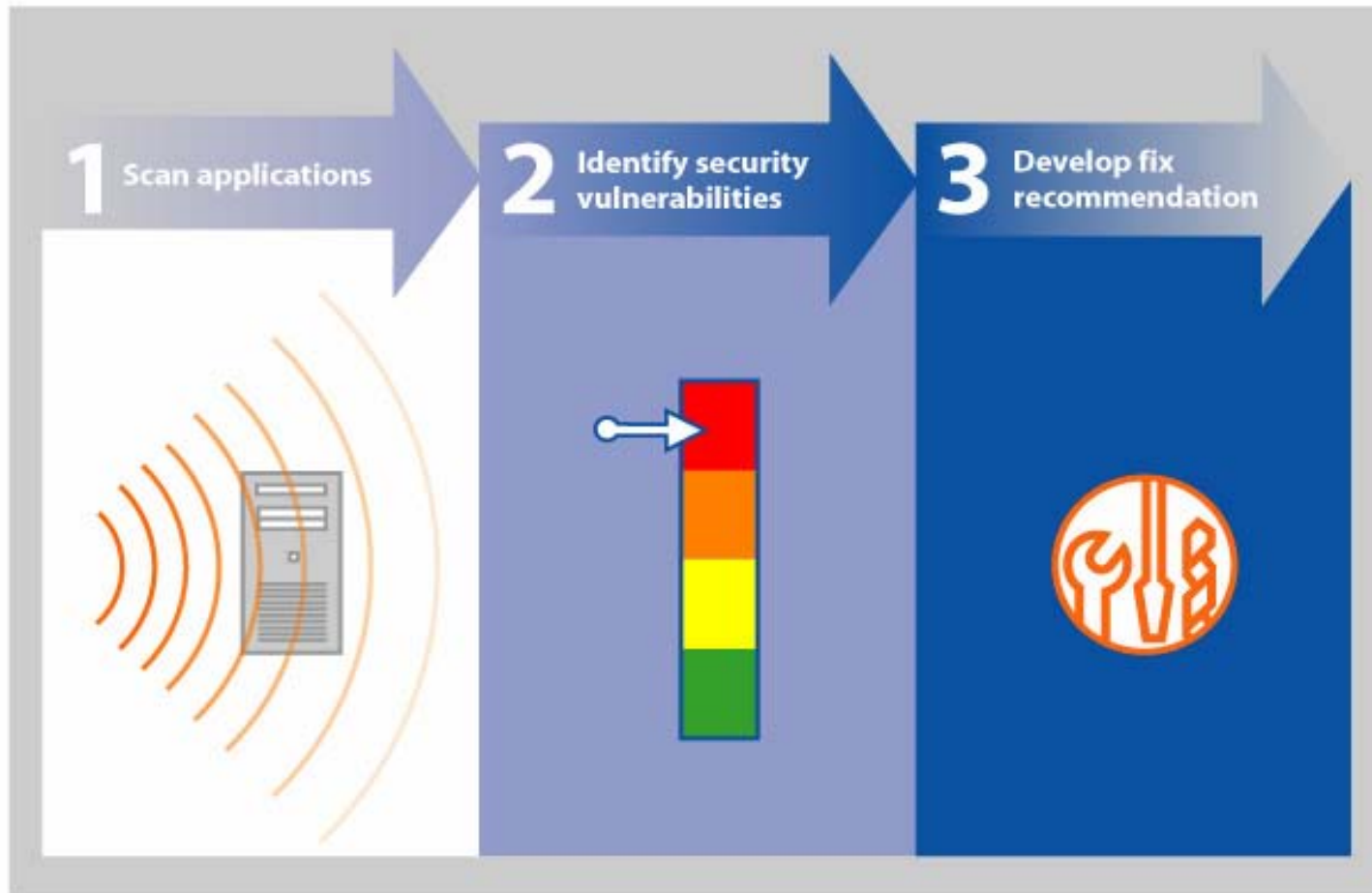
AppScan's Active Testing

- AppScan doesn't rely on metadata to flag issues
 - ▶ Such as saying "Apache version X.X is known to be vulnerable to Y"
- AppScan's tests actively look for the existence of a vulnerability
 - ▶ Mutate the inputs and logic of the application, as learned during the Explore
 - ▶ Assess if the application is vulnerable based on the resulting HTTP activity

SQL Injection Test Examples:

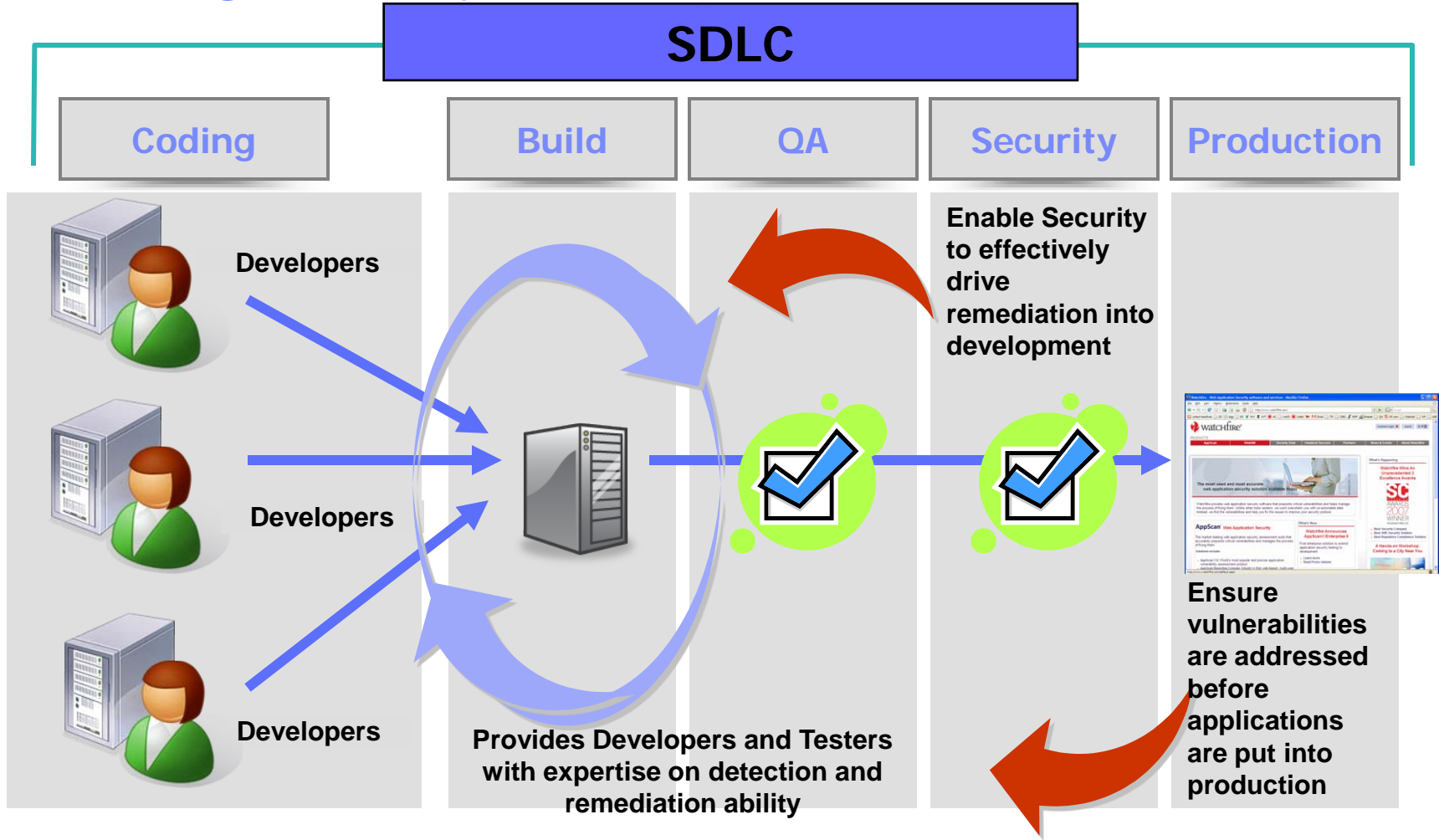
- Original Request: `http://server/page.jsp?param=value`
- Test Requests:
 - `http://server/page.jsp?param=' or 1=1 or ''='`
 - `http://server/page.jsp?param=" or 1=1 or ""="`
 - `http://server/page.jsp?param=' --`
 - `http://server/page.jsp?param=+1+1+1`
 - ...

AppScan Goes Beyond Pointing out Problems

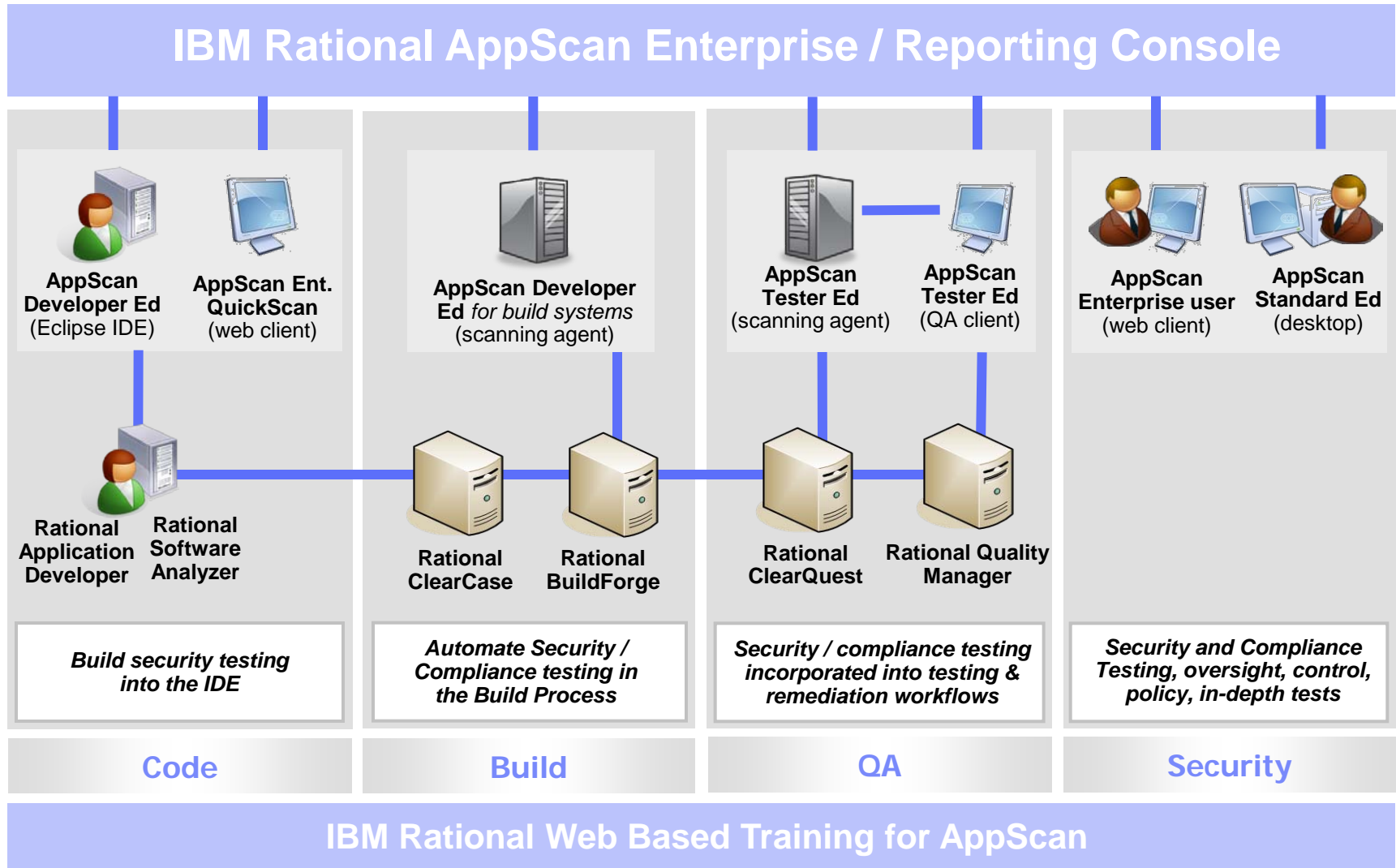


DEMO

Building Security & Compliance into the SDLC



IBM Rational AppScan SDLC Ecosystem



QUESTIONS

Thank You

© Copyright IBM Corporation 2009. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.