IBM Rational Software
Development Conference
2008

WHERE TEAMS ARE R-HEROES

Our Vision for Application Security

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

Rational. software

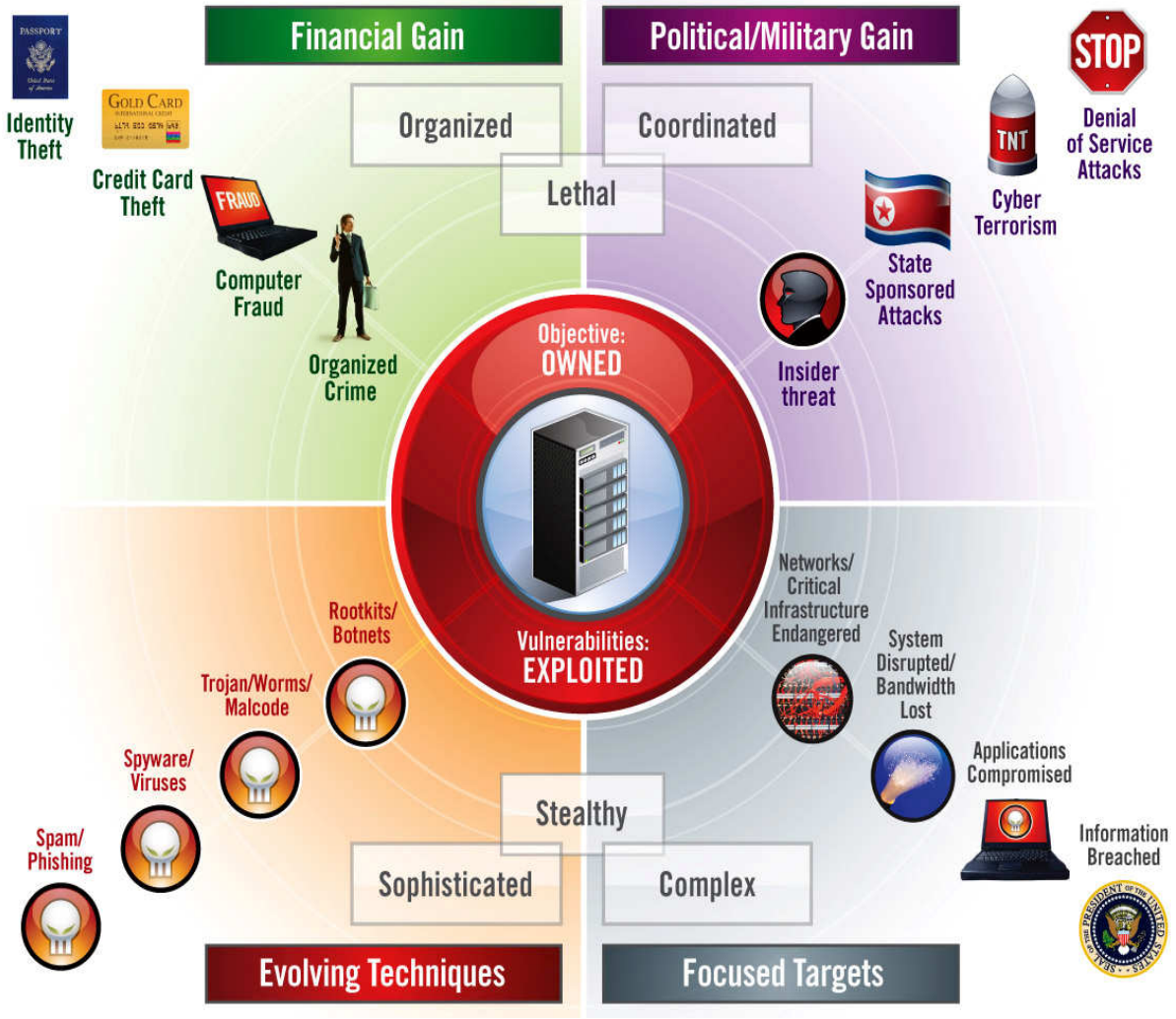
Go to IBM

© 2008 IBM Corporation

Agenda

- Application Security Defined
- Hacking Example
- Trends and Best Practices
- IBM Vision and Roadmap for Application Security

Evolving Threats



The Myth: "Our Site Is Safe"

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Audit It Once a Quarter with Pen Testers

Applications are constantly changing

We Use Network Vulnerability Scanners

Neglect the security of the software on the network/web server

We Use SSL Encryption

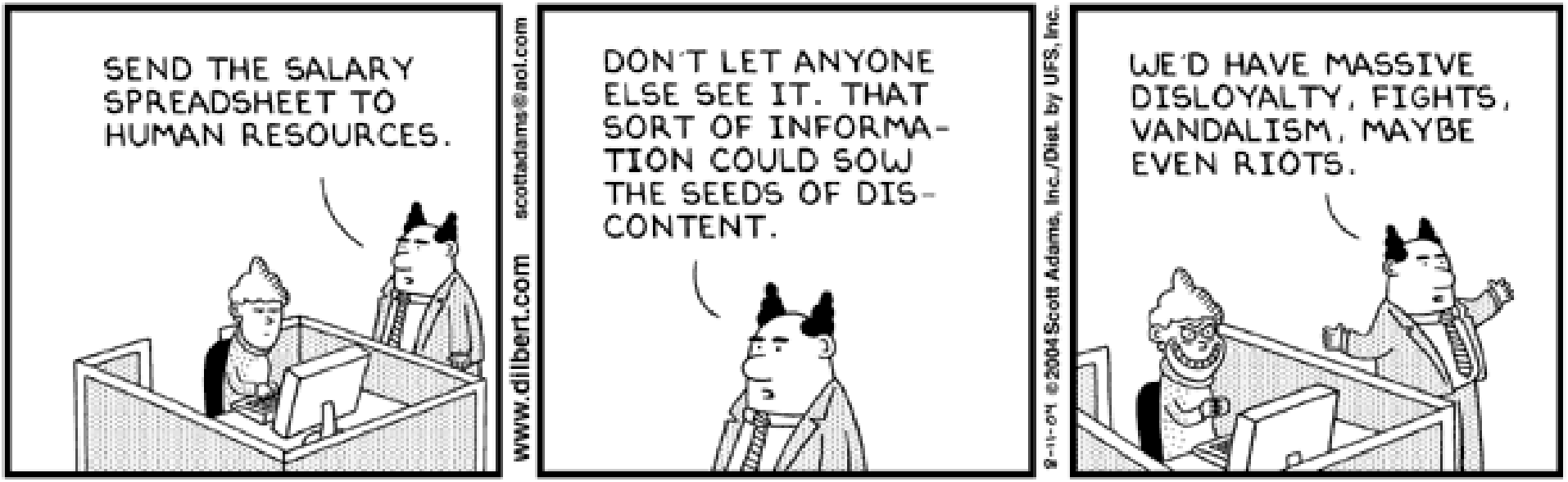
Only protects data between site and user not the web application itself

Regulation & Compliance SARBANES-OXLEY, HIPAA, BASEL II …

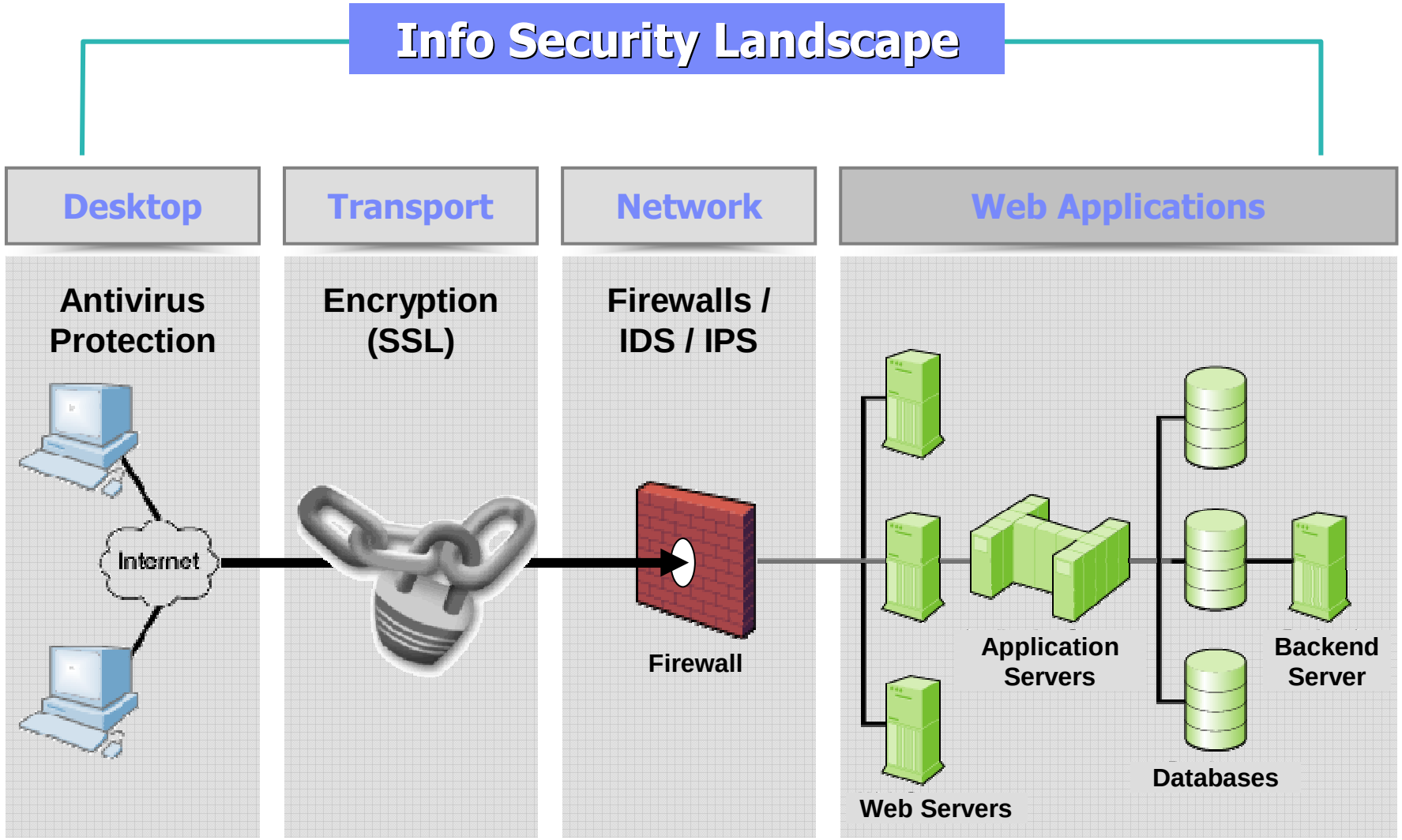
- **It is part of doing business**
- **Business Continuity**
- **An environment of TRUST**
  - **For doing business**
  - **Ensure Orderliness in Internet world**
  - **Promote Economic growth**

- More than just Confidentiality, Integrity and Availability
- **Privacy**

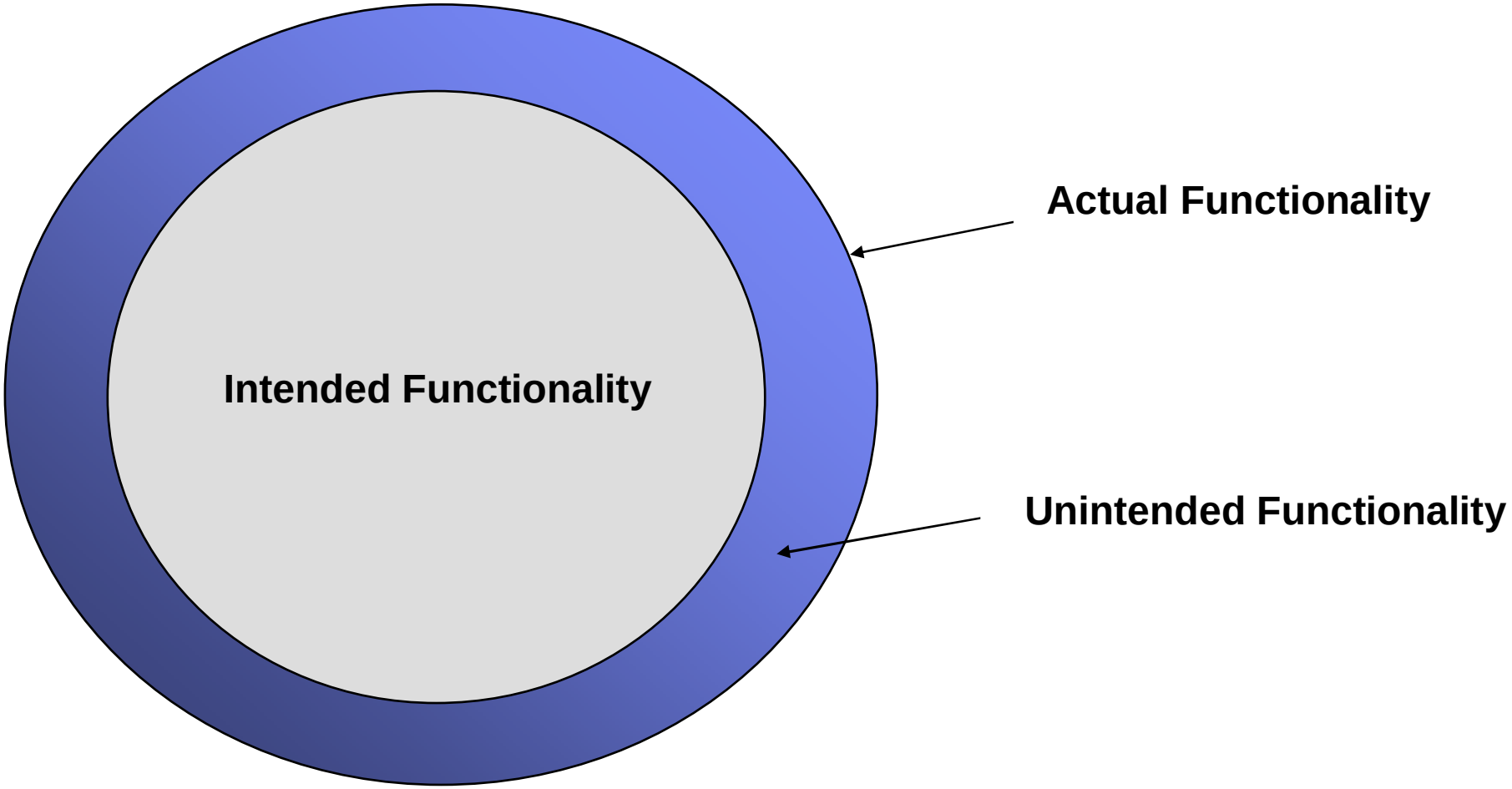
3rd Party Customer Data



Application Security - Understanding the Problem



Hackers Exploit Unintended Functionality to Attack Apps



IBM Rational Software
Development Conference
2008

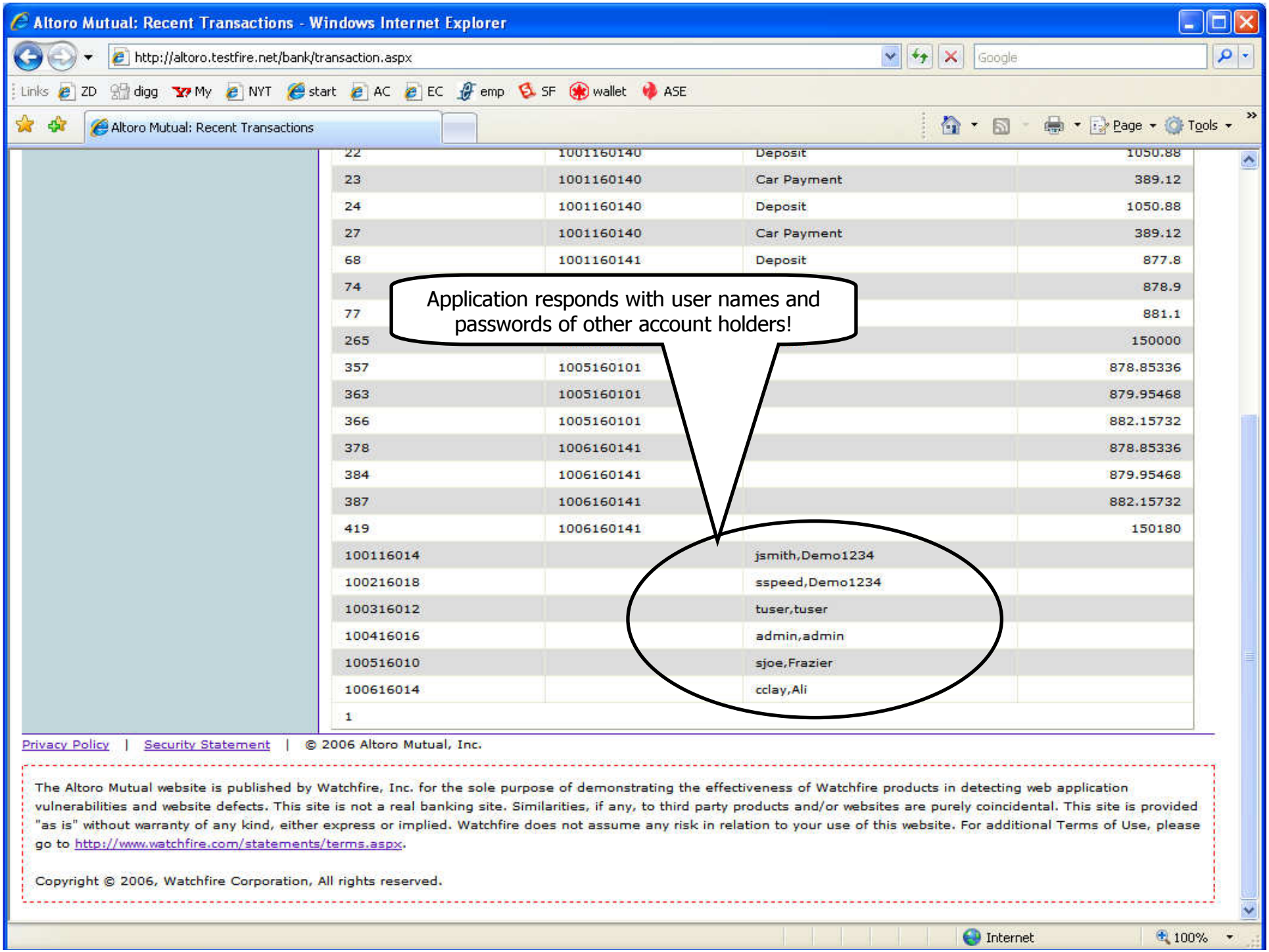
WHERE TEAMS ARE R-HEROES

Application Security Hacking Example

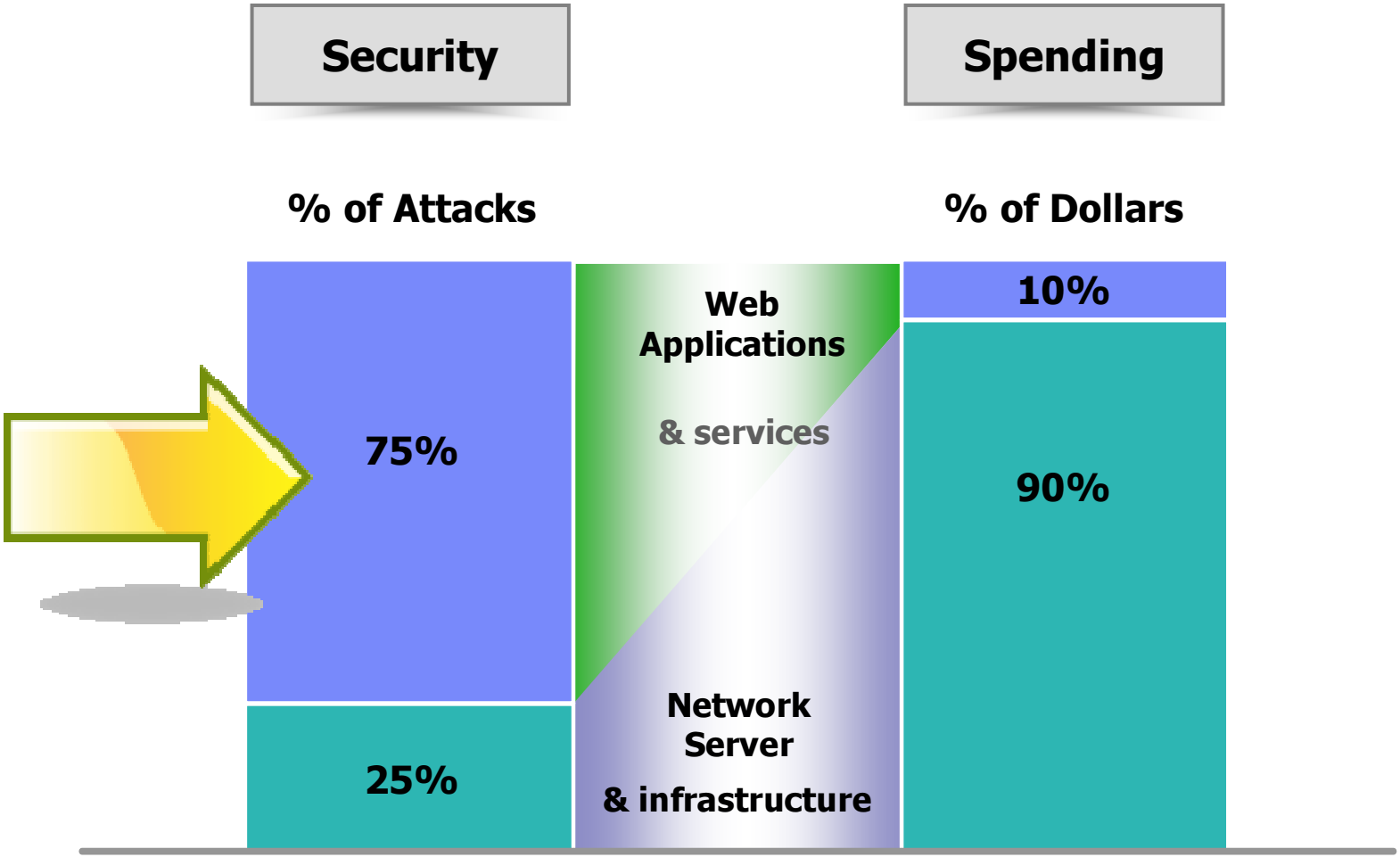
Rational. software

Go to IBM

© 2008 IBM Corporation


Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Altoro Mutual: Recent Transactions
Application responds with user names and passwords of other account holders!
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
74 878.9
77 881.1
265 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%

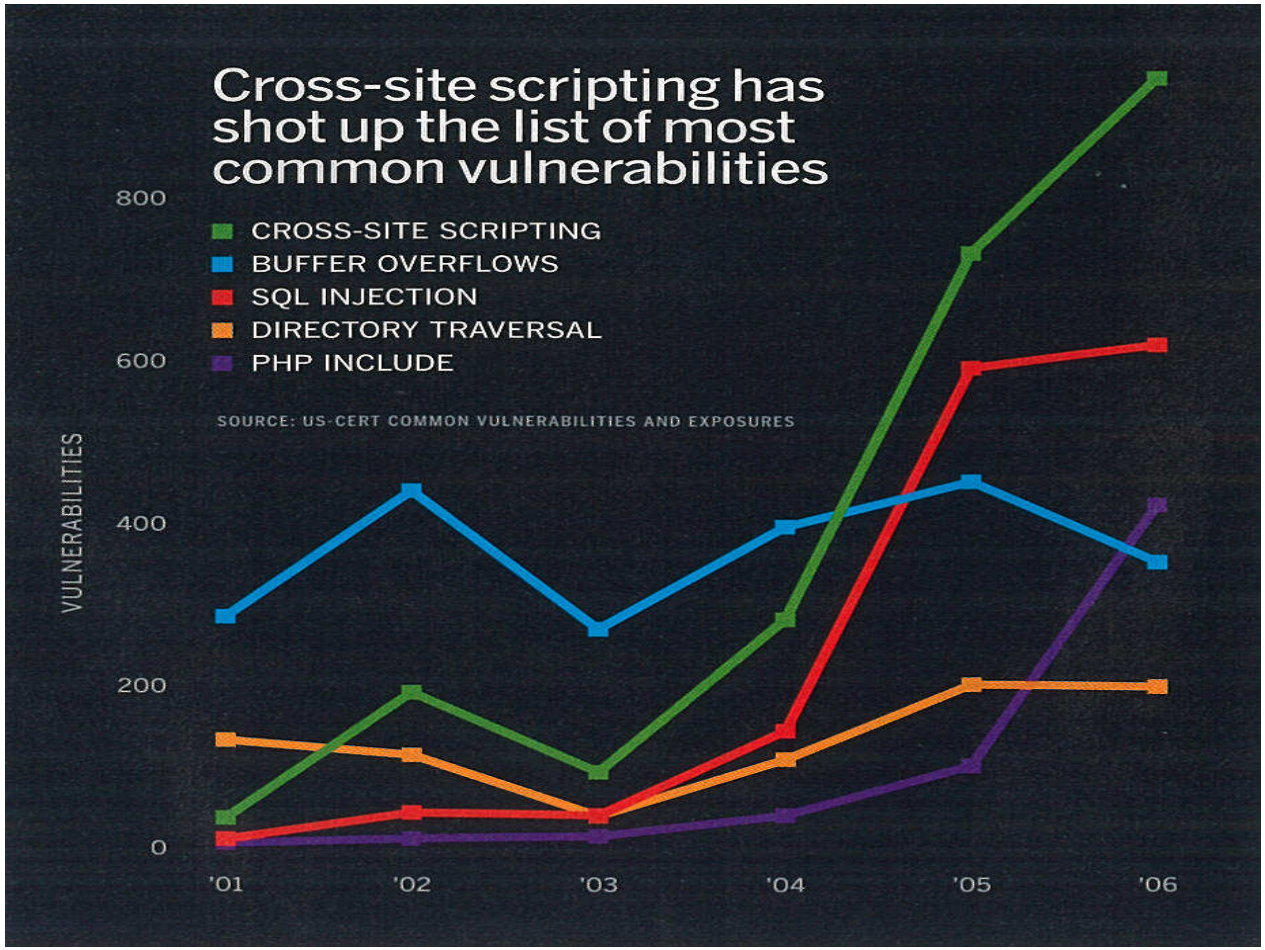
The Fact: Attacks targeted at a new area



In an organization, IT Security people and developers are poles apart

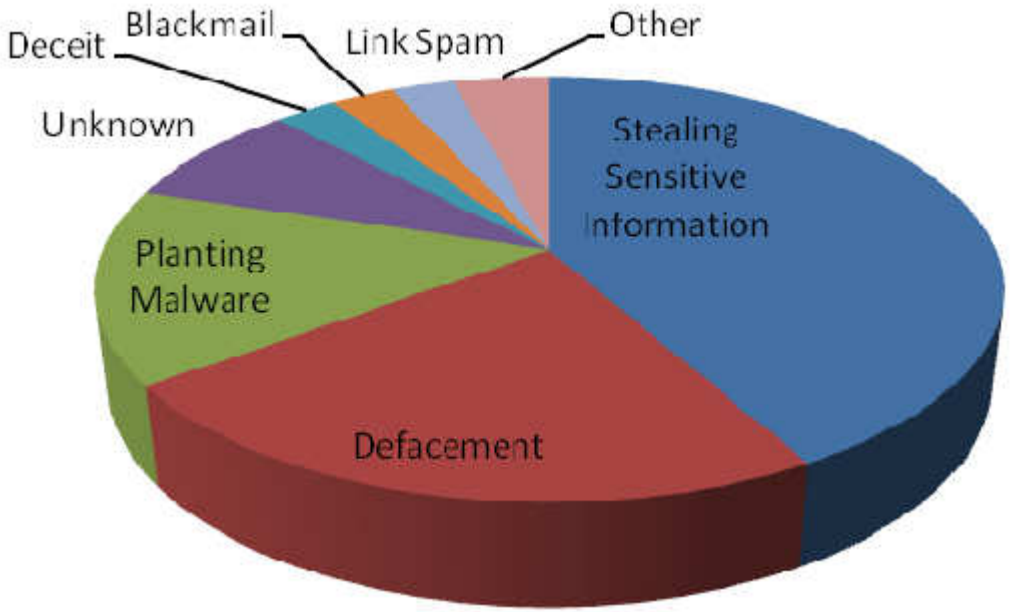
Sources: Gartner, IDC, Watchfire

How Common Are These Problems?



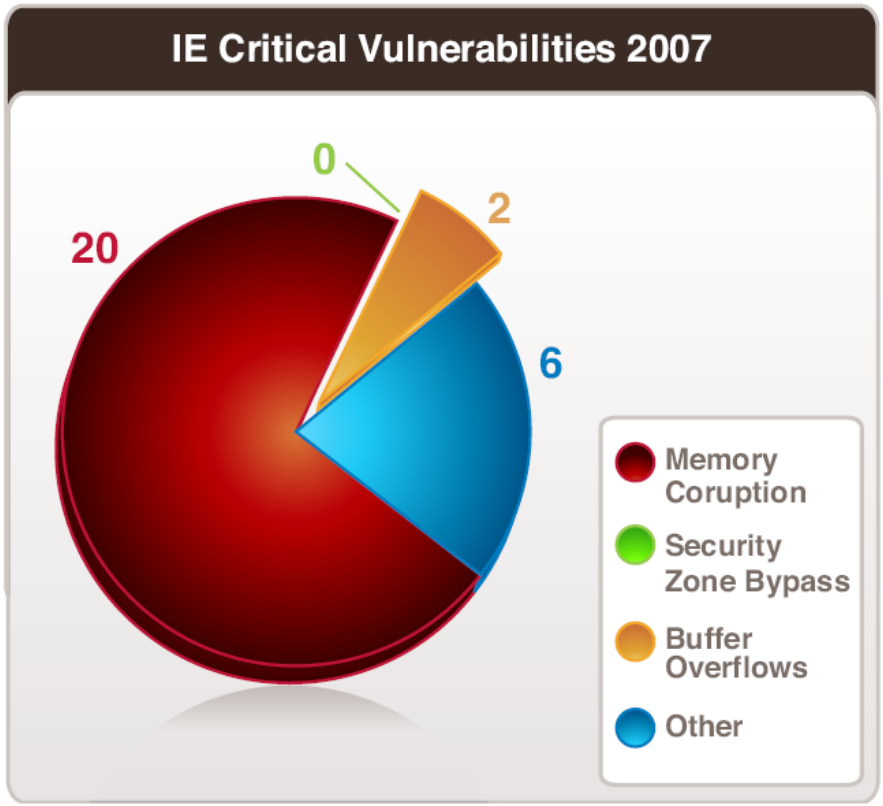
80% of Websites and applications are vulnerable to these attacks – Watchfire Research

Motives Behind Application Hacking Incidents



Source: Breach/WASC 2007 Web Hacking Incident Annual Report

Growth In Browser Vulnerabilities



Source: IBM Xforce 2007 Annual Report

What is the Root Cause?

1. Developers not trained in security
   - Most computer science curricula have no security courses
2. Under investment from security teams
   - Lack of tools, policies, process, etc.
3. Growth in complex, mission critical online applications
   - Online banking, commerce, Web 2.0, etc
4. Number one focus by hackers
   - 75% of attacks focused on applications - Gartner

Result: Application security incidents and lost data on the rise

Where Do These Problems Exist?

Type:

- Customer facing services
- Partner portals
- Employee intranets

Source:

1. Applications you buy – e.g. COTS
2. Applications you build internally
3. Applications you outsource

Building Security Into the Development Process

Define/Design

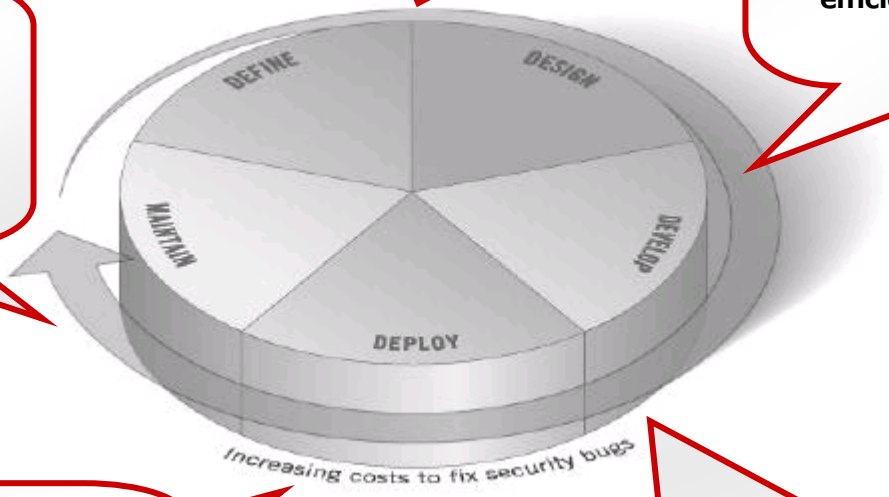
- Continuous security education of architects, developers etc. on Web Application Security

Development

- Test apps for security issues in Development identifying issues at their earliest point
- Realize optimum security testing efficiencies (cost reduction)

Production

- Test existing deployed apps
- Eliminate security exposure in live applications



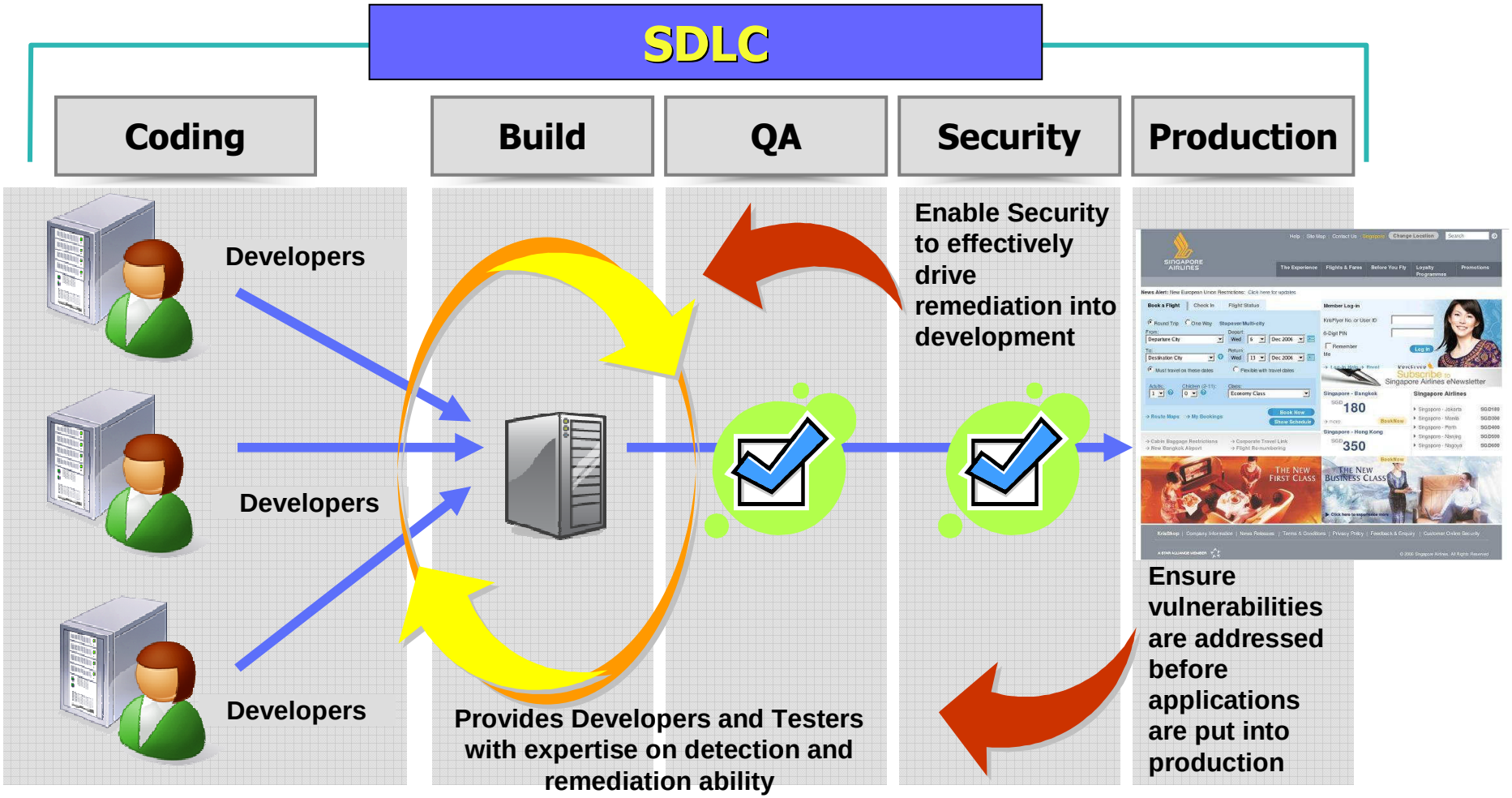
Deploy

- Test apps before going to production
- Deploy secure web applications

Test

- Test apps for security issues in QA organization along with performance and functional testing
- Reduce costs of security testing

*Graphics from OWASP.com


SDLC
Coding
Build
QA
Security
Production
Developers
Developers
Developers
Enable Security to effectively drive remediation into development
Provides Developers and Testers with expertise on detection and remediation ability
Ensure vulnerabilities are addressed before applications are put into production

IBM Rational Software
Development Conference
2008

WHERE TEAMS ARE R-HEROES

IBM Vision and Roadmap for Application Security

Rational. software

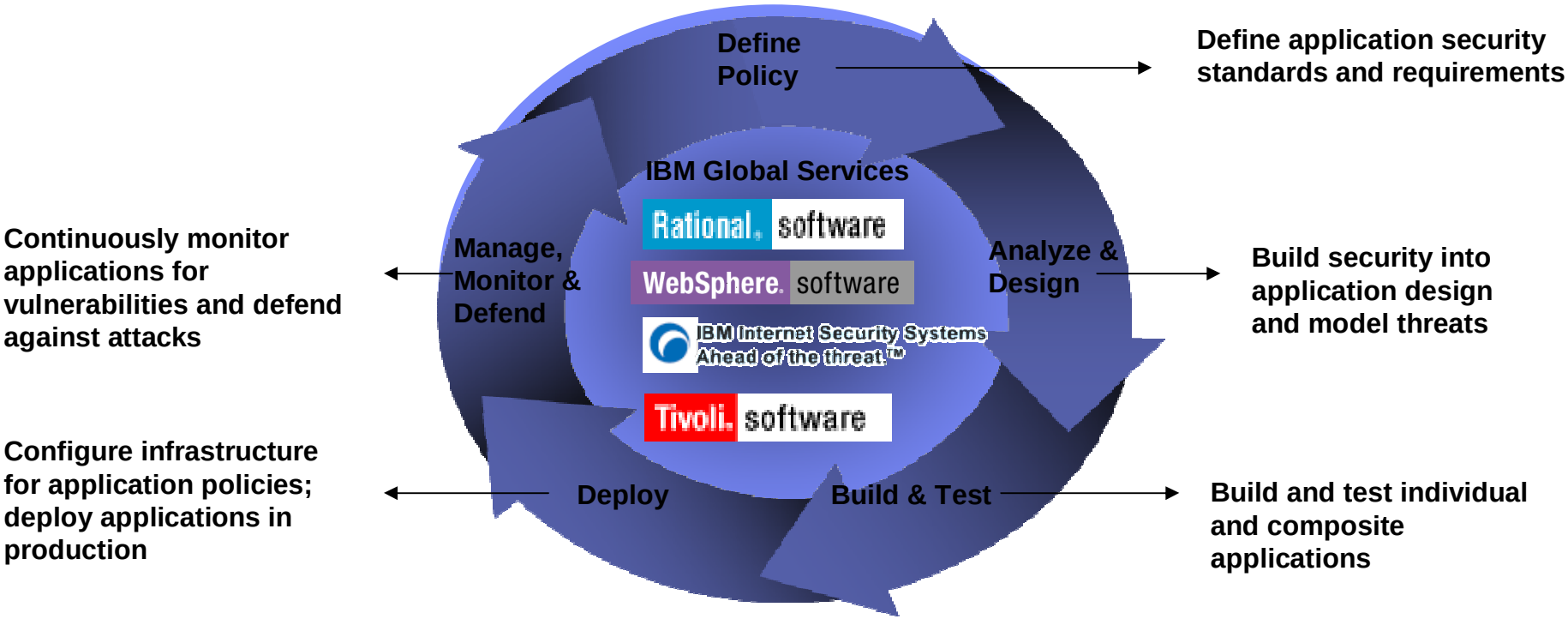
Go to IBM

© 2008 IBM Corporation

IBM is laying the foundation for end-to-end application security

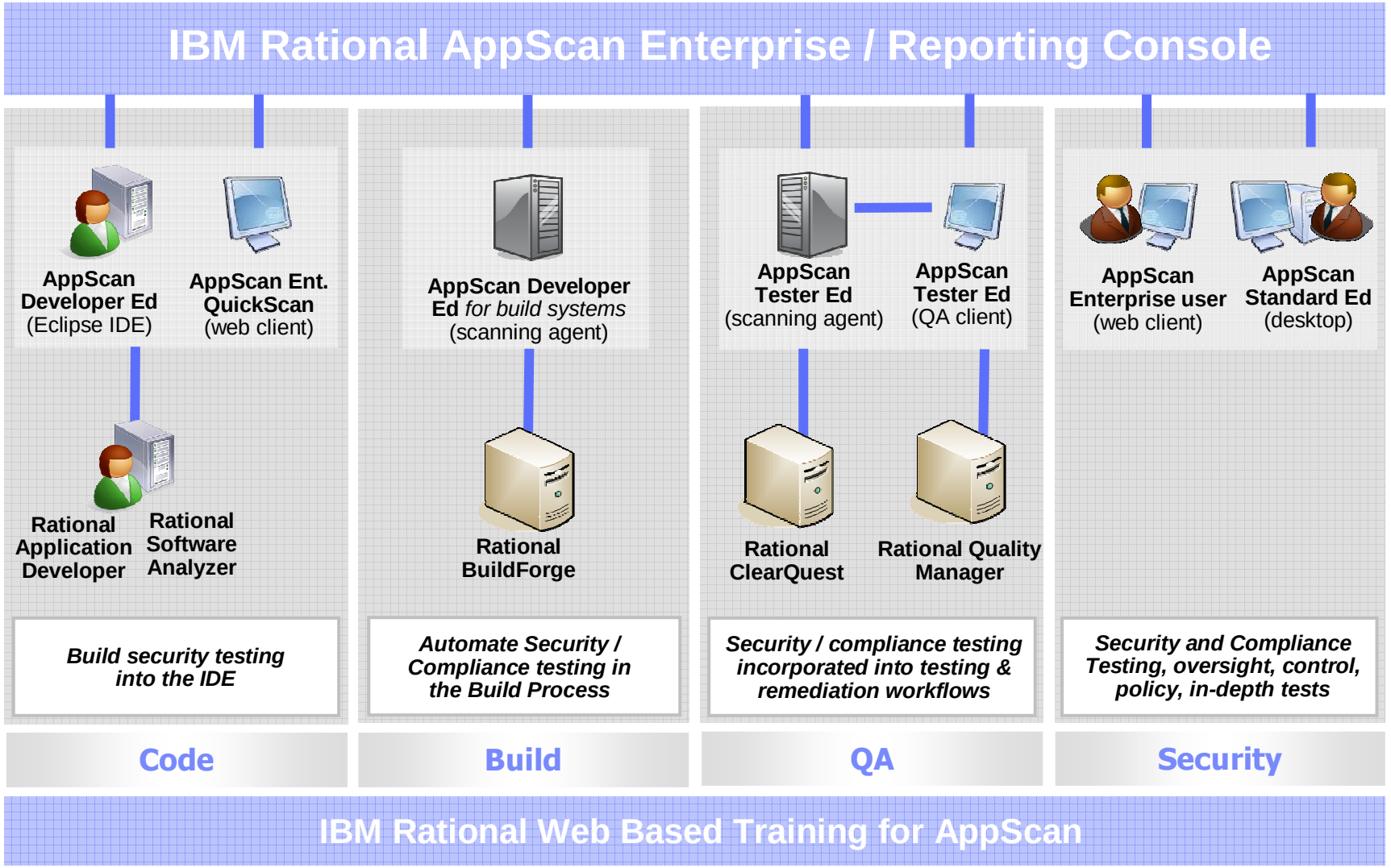
- IBM Global Services **– security risk assessments helping define policies and processes**
- Rational **– automated vulnerability testing for web applications/web services across the development cycle**
- IBM Technology Services/ISS **– managed services for network and application vulnerability assessment**
- Tivoli **– access control and security information and event management to web applications/web services**
- DataPower **– provides SOA security solutions**
- IBM Research **– static analysis technology**

Application Security Management Lifecycle

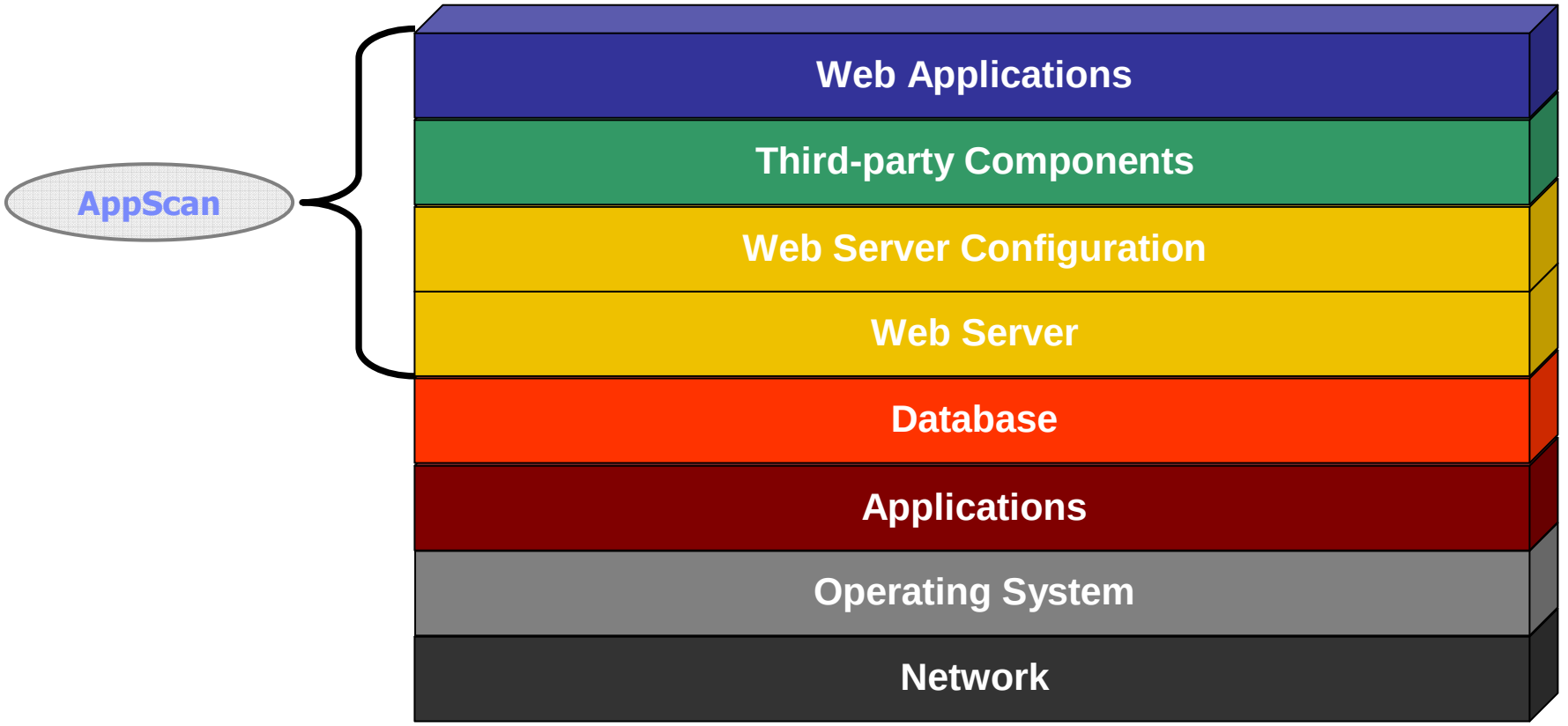


IBM Rational AppScan SDLC Ecosystem

Includes Fall 2008 Releases

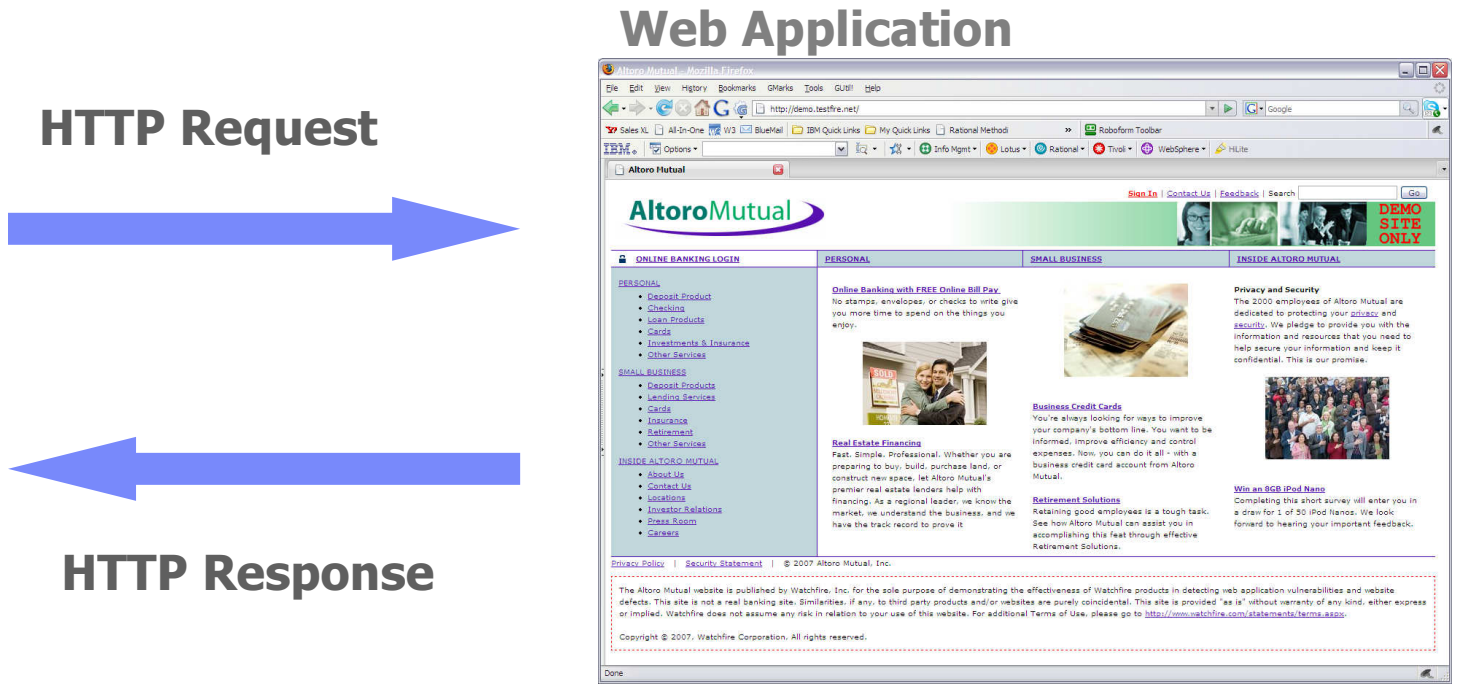


What does AppScan test for?

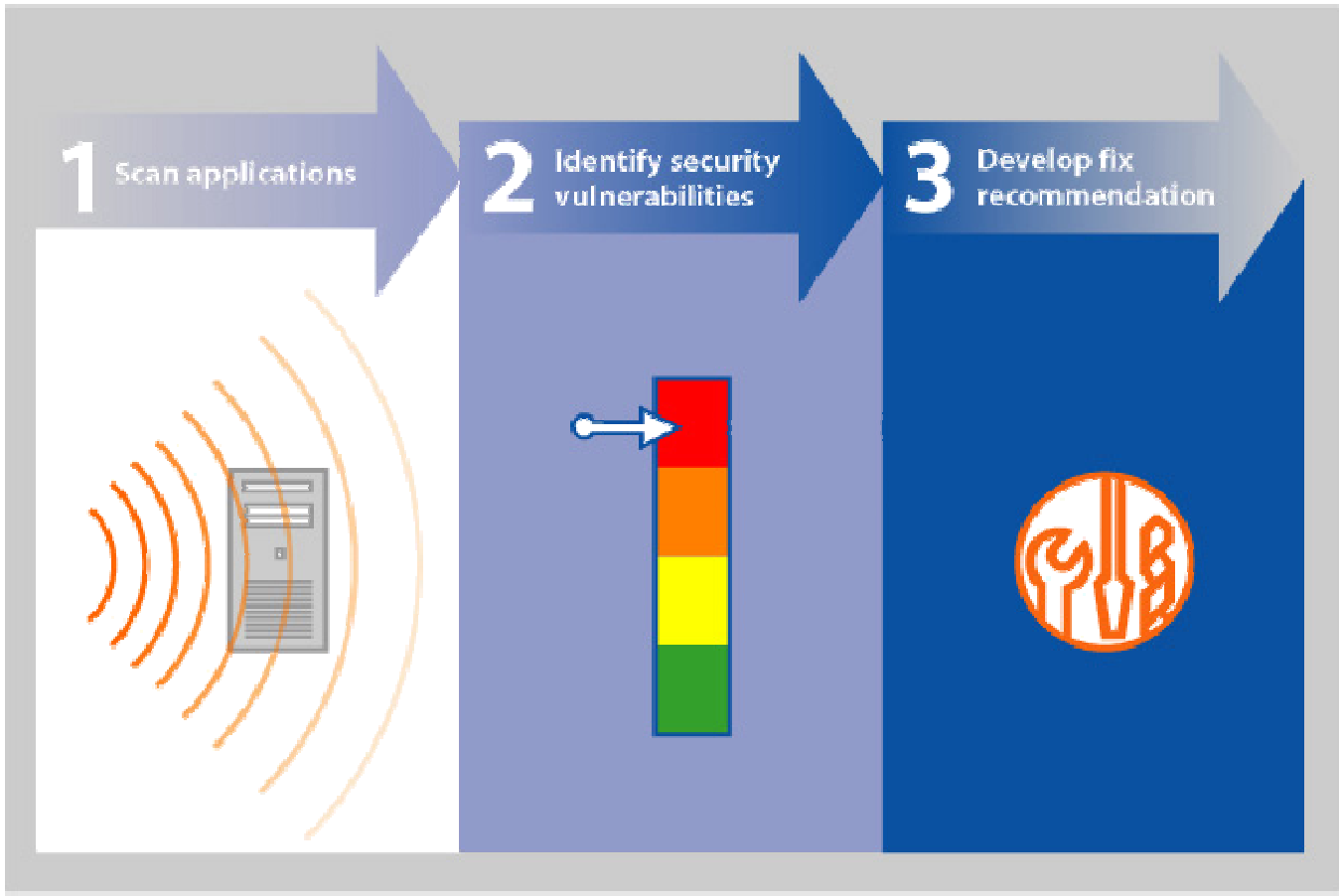


How does AppScan work?

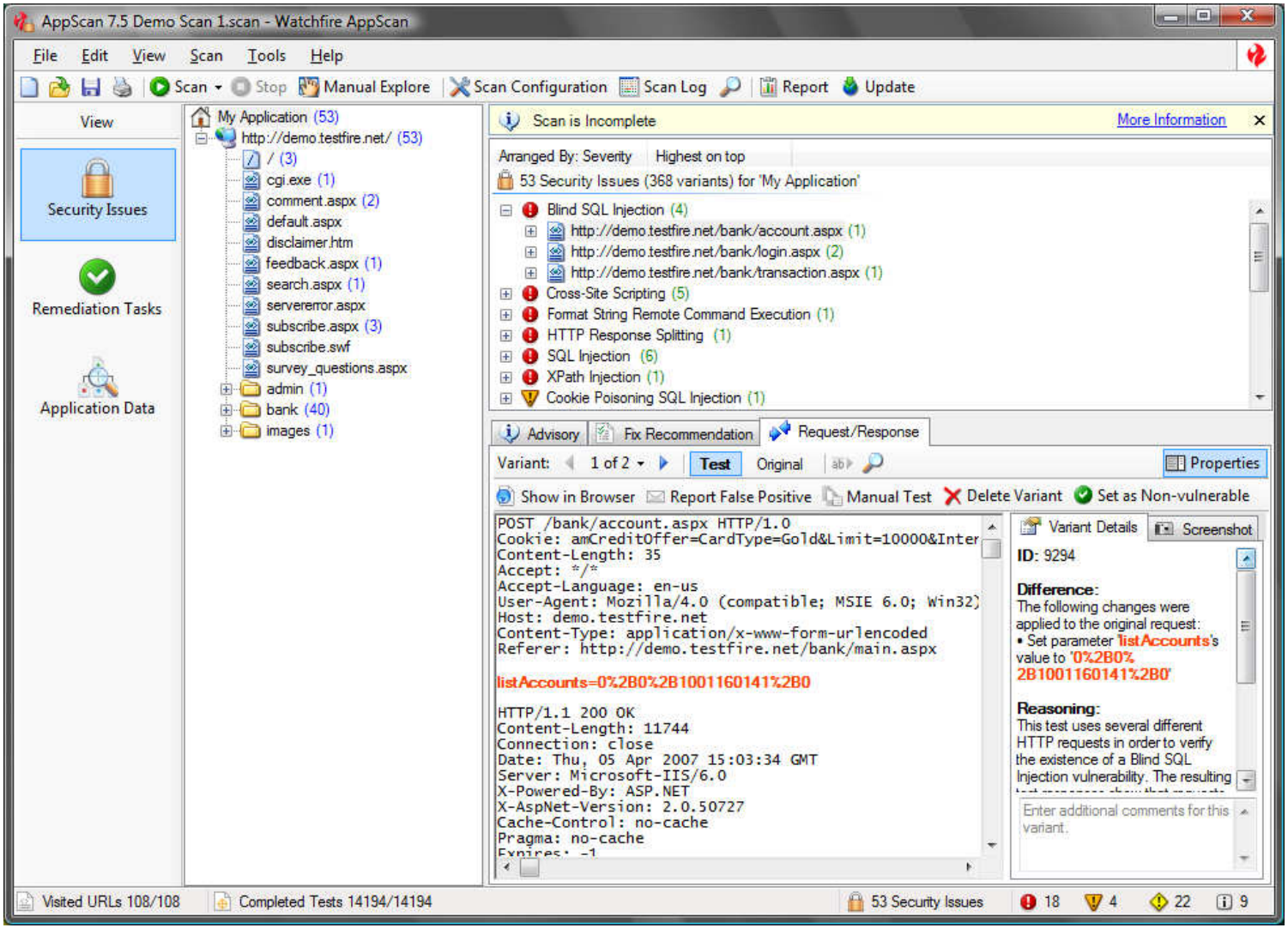
- **Approaches an application as a black-box**
- **Traverses a web application and builds the site model**
- **Determines the attack vectors based on the selected Test policy**
- **Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules**



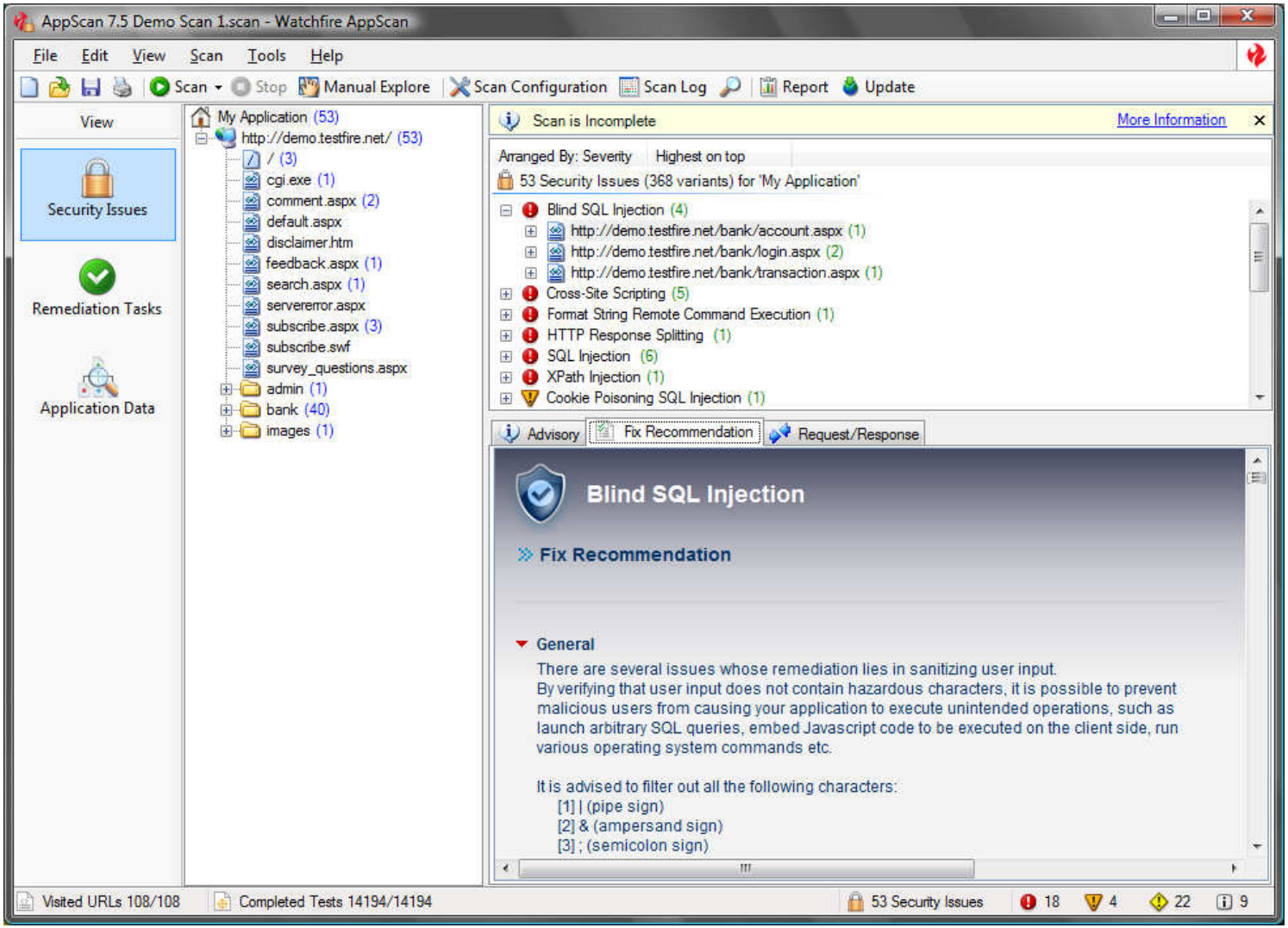
Rational AppScan: Find and fix web application security and compliance issues



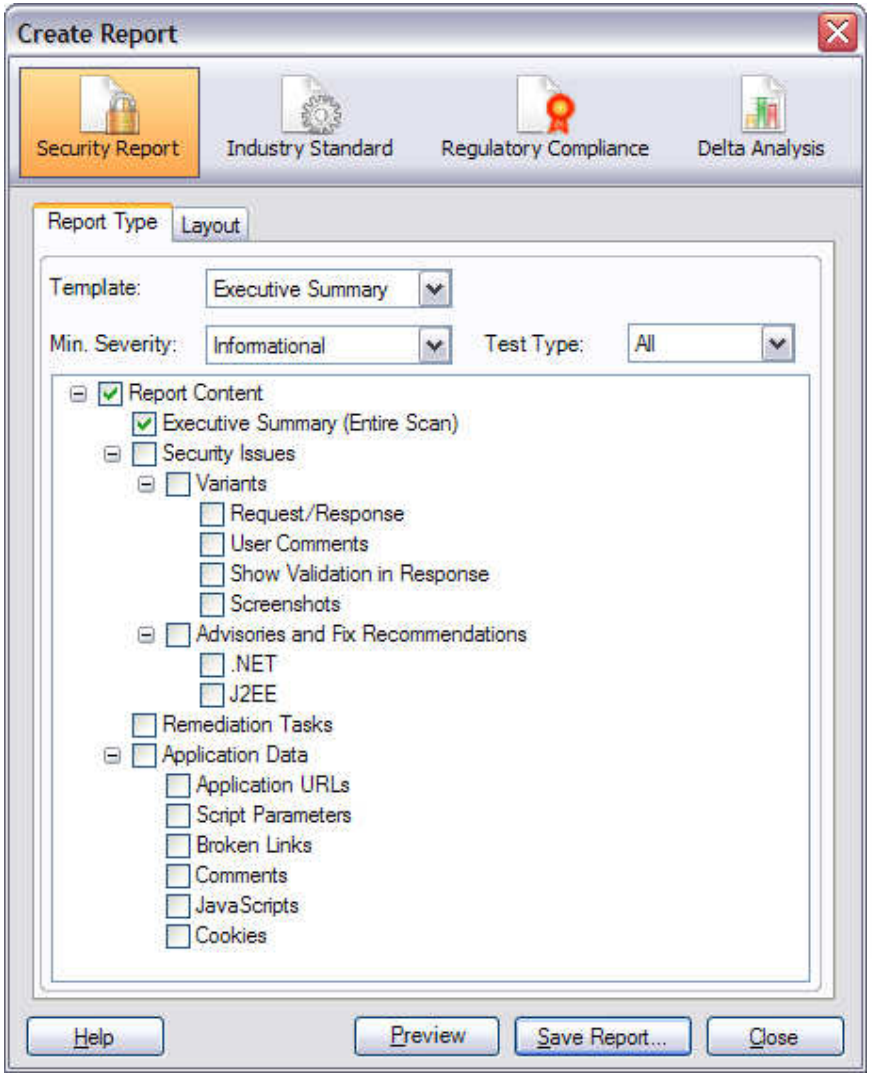
Identify Vulnerabilities

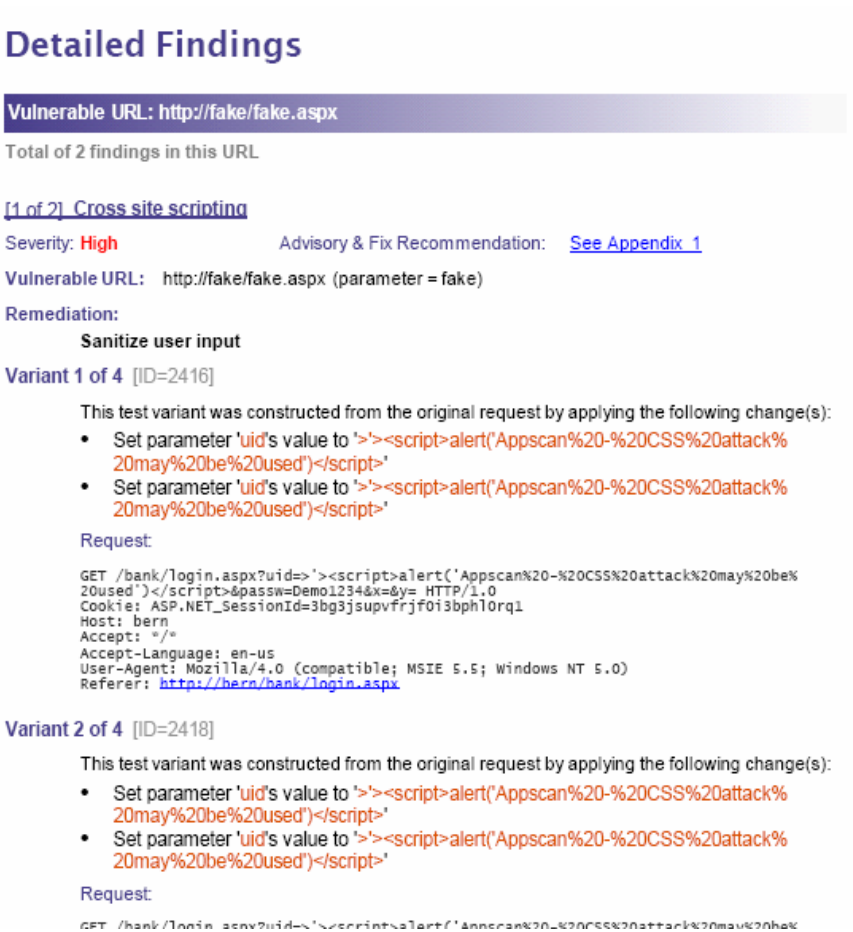


Actionable Fix Recommendations

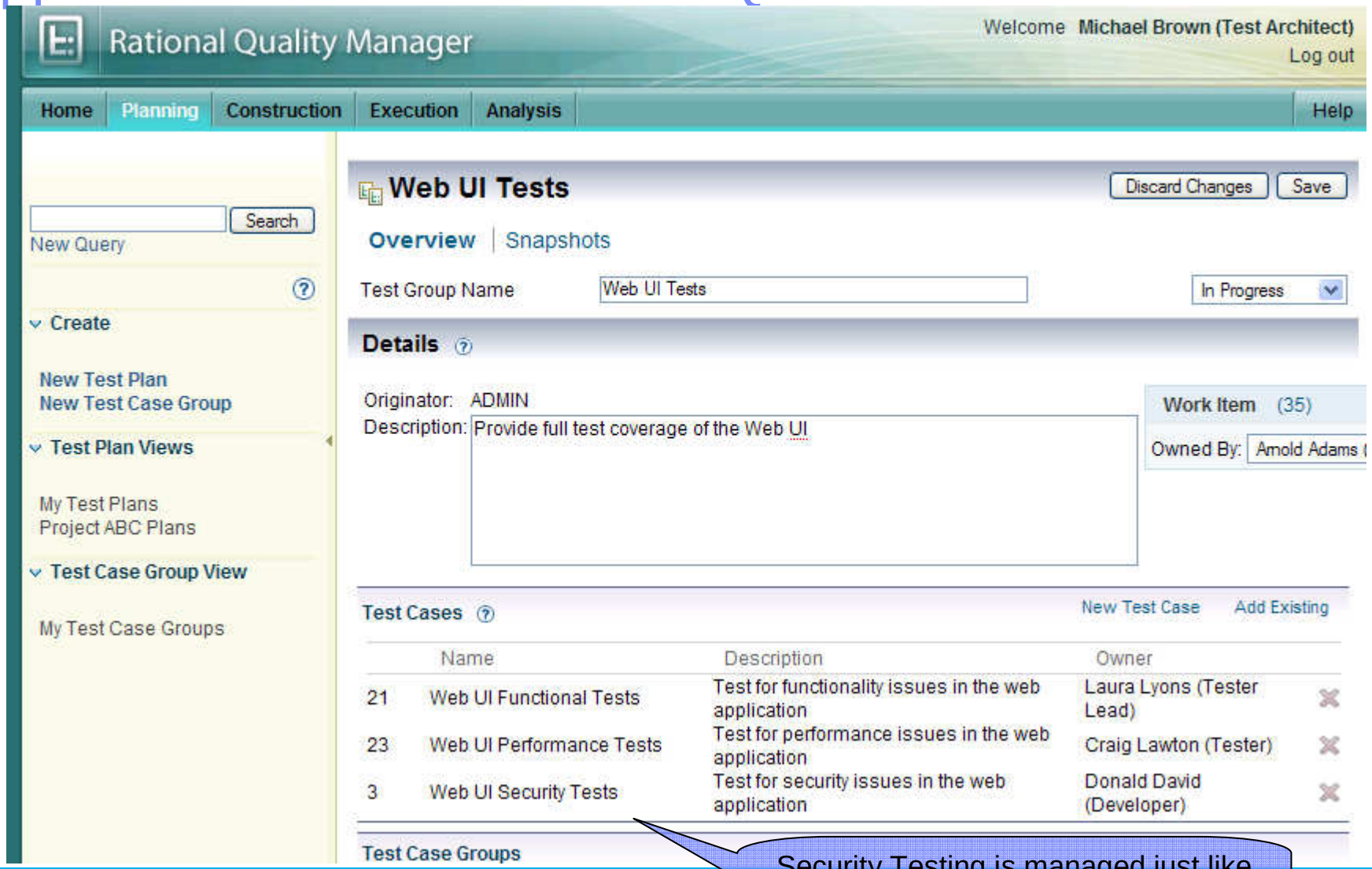


Report


Create Report
Security Report
Industry Standard
Regulatory Compliance
Delta Analysis
Report Type
Layout
Template:
Executive Summary
Min. Severity:
Informational
Test Type:
All
Report Content
Executive Summary (Entire Scan)
Security Issues
Variants
Request/Response
User Comments
Show Validation in Response
Screenshots
Advisories and Fix Recommendations
.NET
J2EE
Remediation Tasks
Application Data
Application URLs
Script Parameters
Broken Links
Comments
JavaScripts
Cookies
Help
Preview
Save Report...
Close

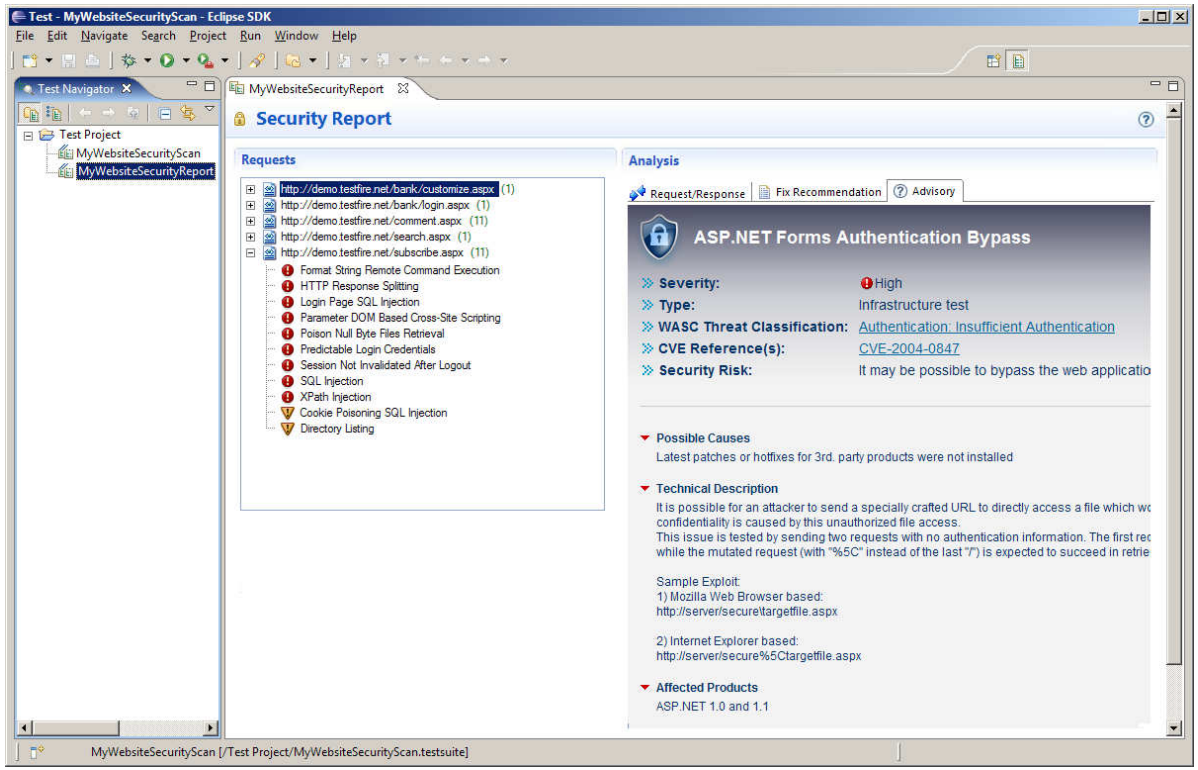

Detailed Findings
Vulnerable URL: http://fake/fake.aspx
Total of 2 findings in this URL
[1 of 2] Cross site scripting
Severity: High
Advisory & Fix Recommendation: See Appendix 1
Vulnerable URL: http://fake/fake.aspx (parameter = fake)
Remediation:
Sanitize user input
Variant 1 of 4 [ID=2416]
This test variant was constructed from the original request by applying the following change(s):
Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
Request:
GET /bank/login.aspx?uid=><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bphl0rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/login.aspx
Variant 2 of 4 [ID=2418]
This test variant was constructed from the original request by applying the following change(s):
Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
Request:

AppScan Tester Edition for RQM

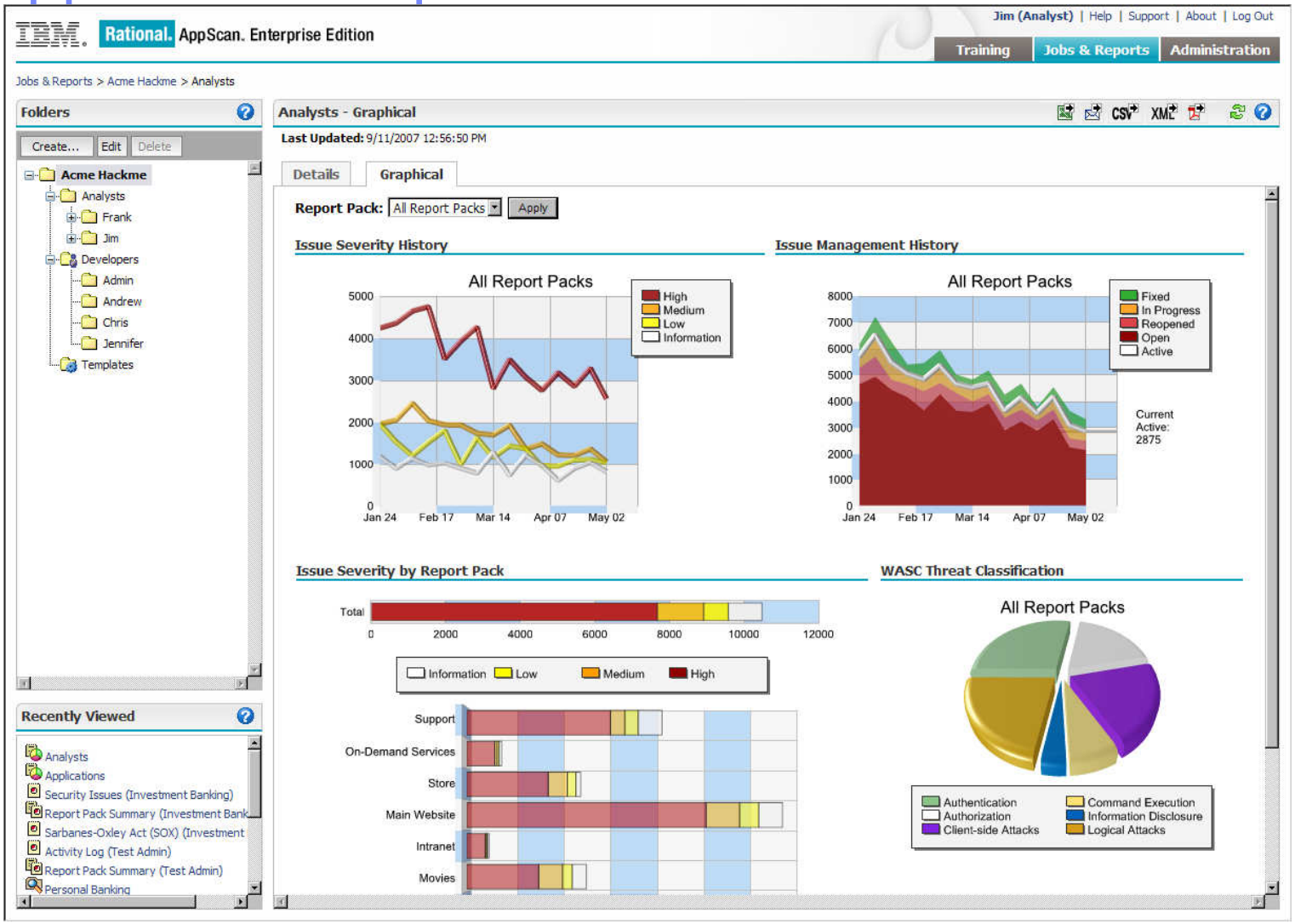


Forthcoming AppScan DE

- Security Testing in your Development Environment (Architect, RAD or Eclipse)
- Integration with source code, WebSphere, ClearQuest
- Can interoperate with AppScan Enterprise for central licensing, permissions and oversight

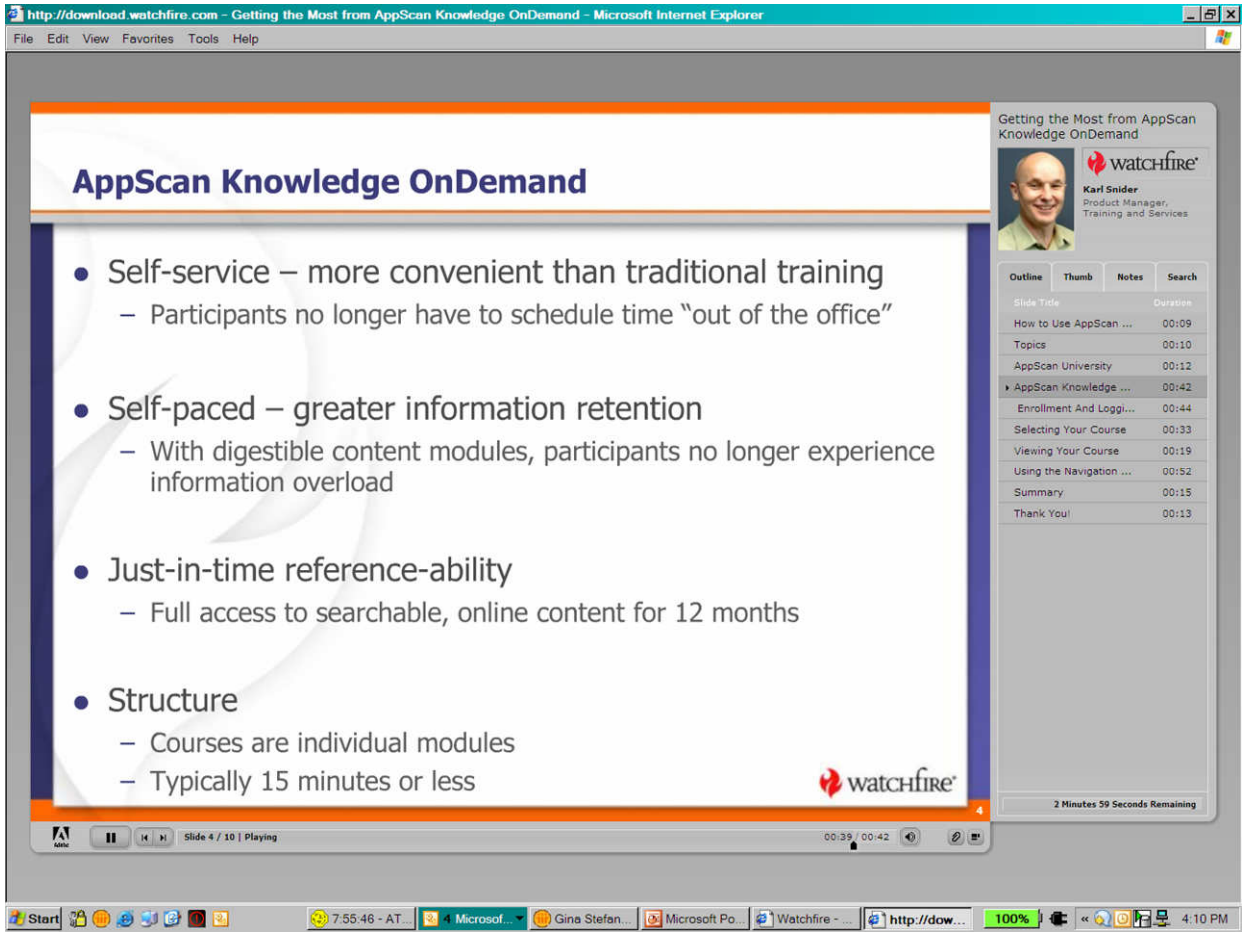


AppScan Enterprise – Dashboards and Metrics



Integrated Computer Based Training

Key to adoption across the organization is education



800+ Companies Depend On Watchfire

9 of the Top 10 Banks

HSBC
JPMorganChase
citi
AXA Financial Protection
Fidelity
SunTrust
Liberty Mutual
Sovereign Bank

8 of the Top 10 Technology Companies

Microsoft
Cisco Systems
intel
DELL
IBM
SONY
Adobe
Analog Devices

7 of the Top 10 Pharma / Clinical Companies

Wyeth
Novartis
AstraZeneca
Abbott Laboratories
Aventis
Roche
Genentech
In Business For Life

Telecommunication Companies

AT&T
Bell
cingular raising the bar
Lucent Technologies Bell Labs Innovations
ROGERS
Sprint Together with NEXTEL
verizon

Multiple Large Government Agencies

Department of Veterans Affairs
Social Security Administration USA
Department of the Navy
United States Postal Service

For More Information

- Product information
  - See our booth on the show floor for information on AppScan and AppScan Enterprise
- Rational labs pedestals
  - AppScan Developer Edition
  - AppScan Tester Edition for Quality Manager
- Hands on workshops
  - Hacking 101

QUESTIONS

THANK YOU

Terry Goldman - goldmant@sg.ibm.com

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

© **Copyright IBM Corporation 2008. 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, the on-demand business logo, Rational, the Rational 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.