



IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**



Our Vision for Application Security

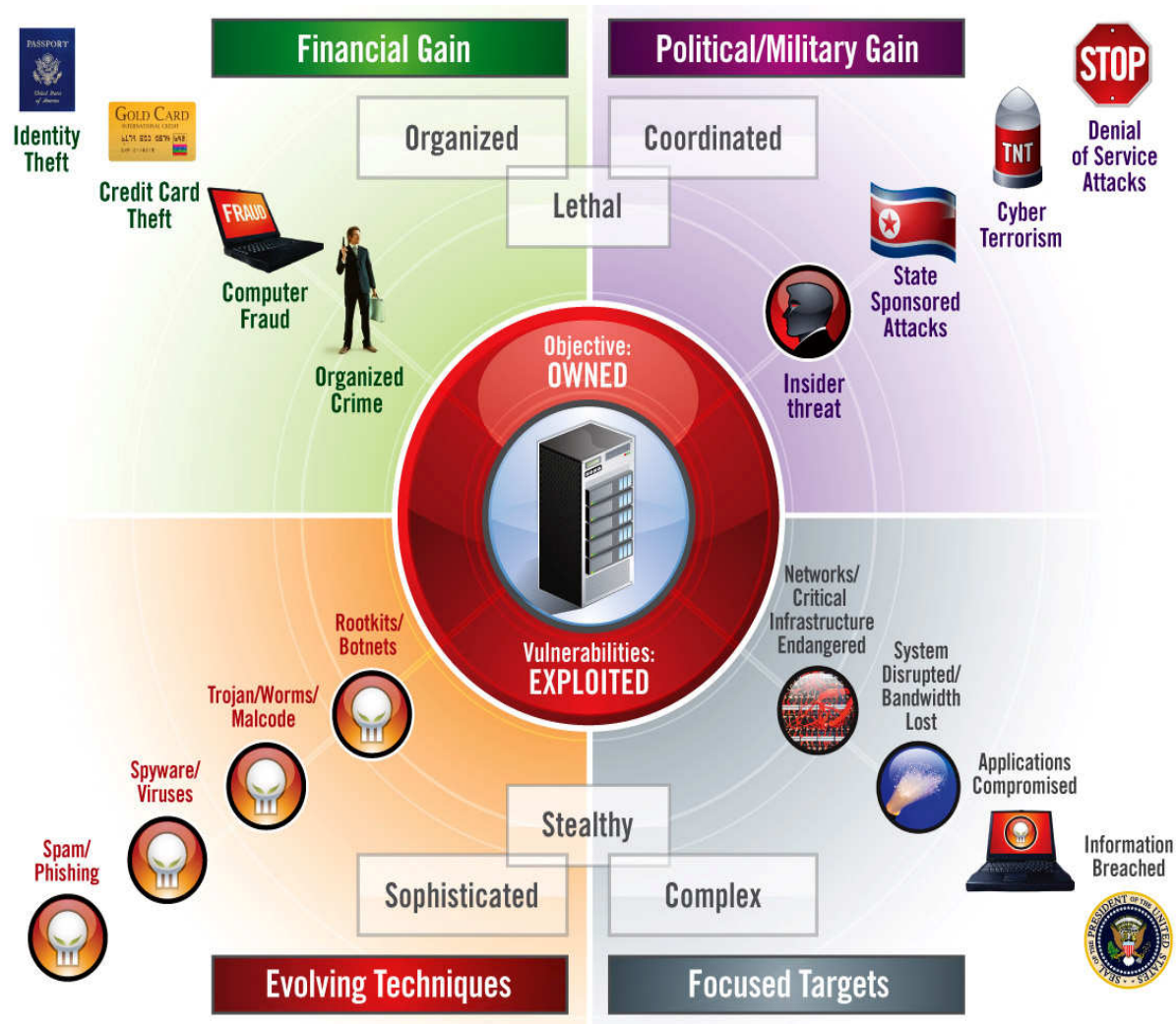
Terry Goldman
Technical Evangelist,
Rational ASEAN
goldmant@sg.ibm.com

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



www.dilbert.com scottadams@aol.com

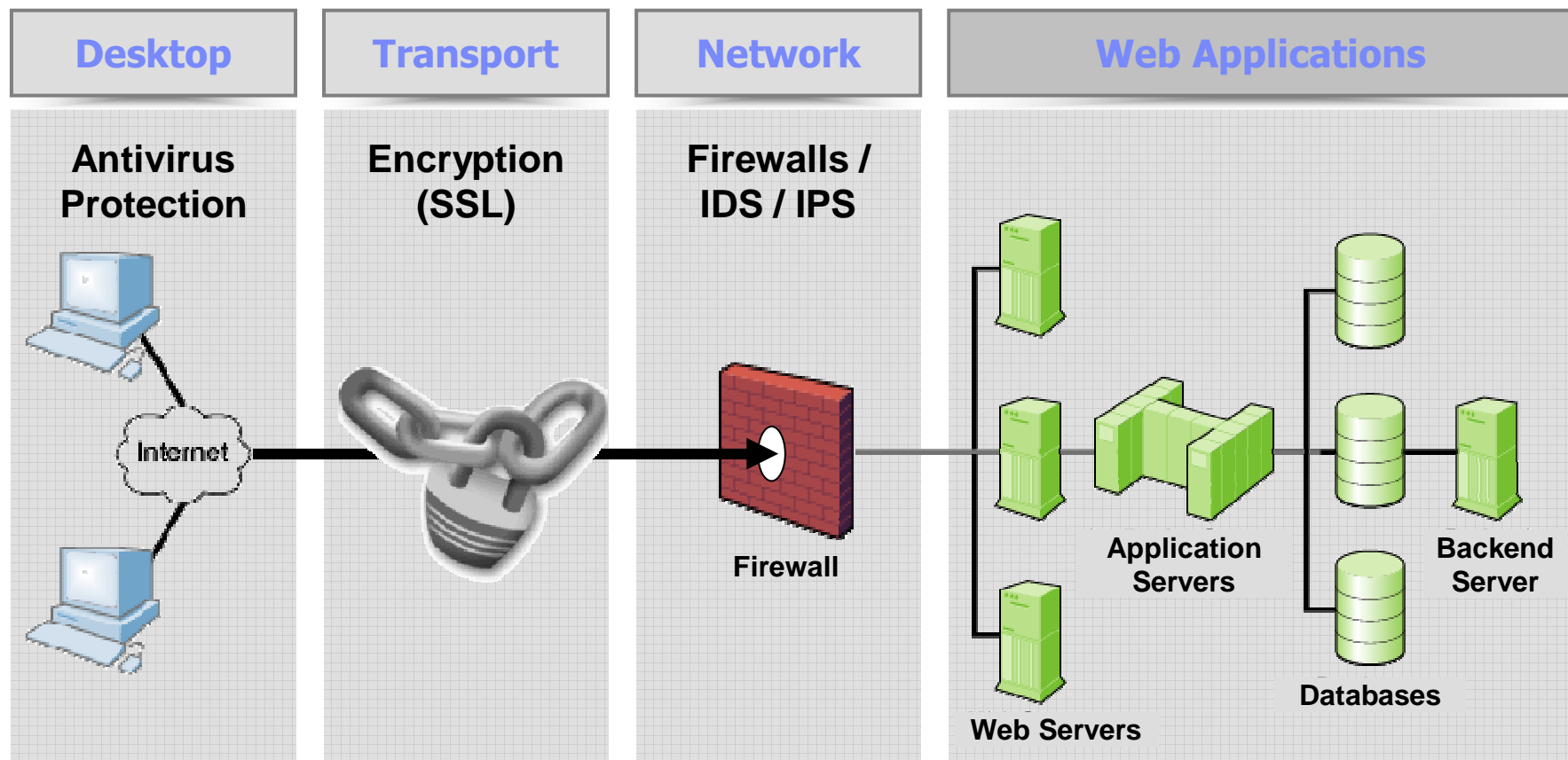


9-11-04 © 2004 Scott Adams, Inc./Dist. by UFS, Inc.

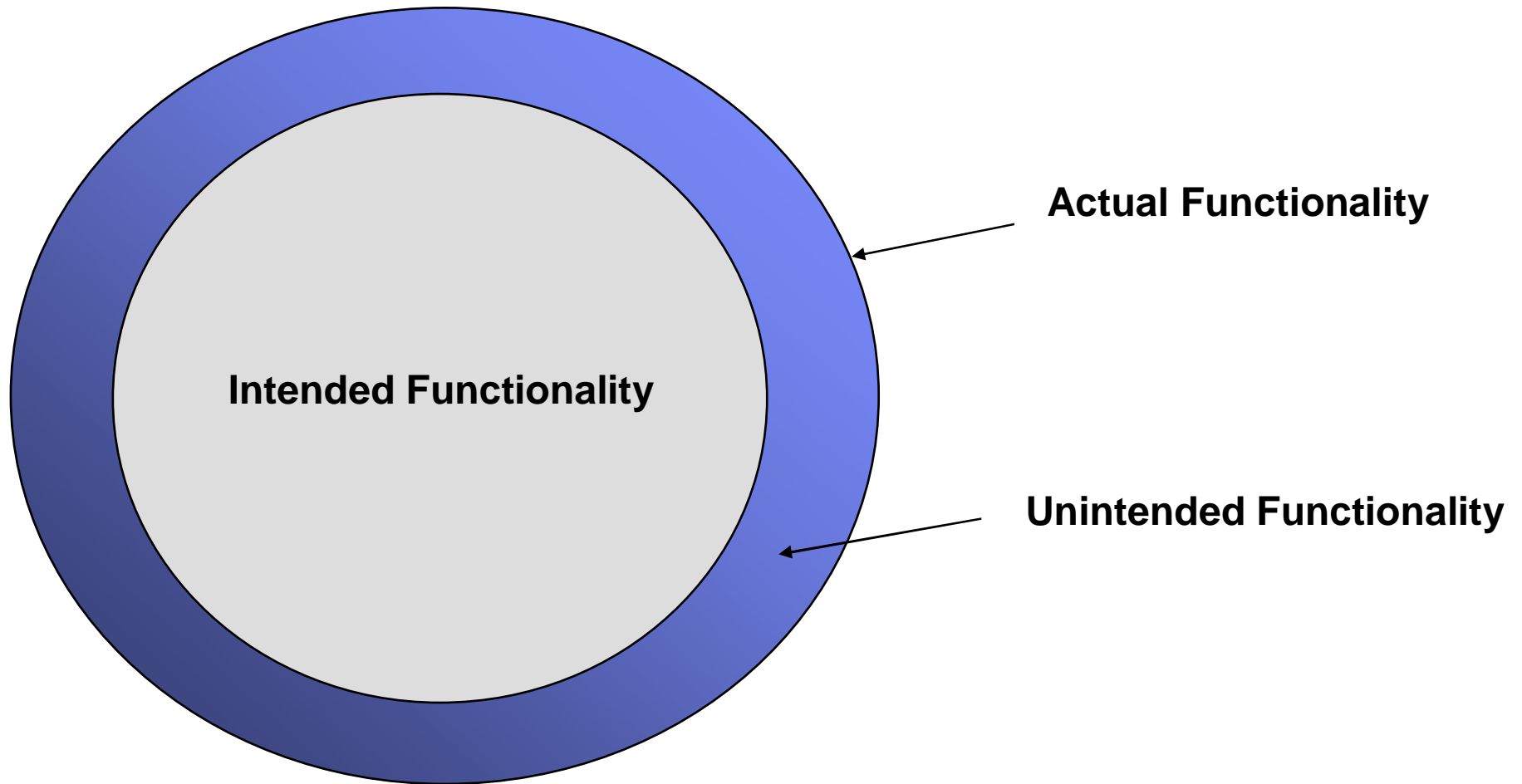


Application Security - Understanding the Problem

Info Security Landscape



Hackers Exploit Unintended Functionality to Attack Apps





IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**



Application Security Hacking Example

Altoro Mutual: Recent Transactions - Windows Internet Explorer

http://altoro.testfire.net/bank/transaction.aspx

Links ZD digg My NYT start AC EC emp SF wallet ASE

Altoro Mutual: Recent Transactions

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			

Application responds with user names and passwords of other account holders!

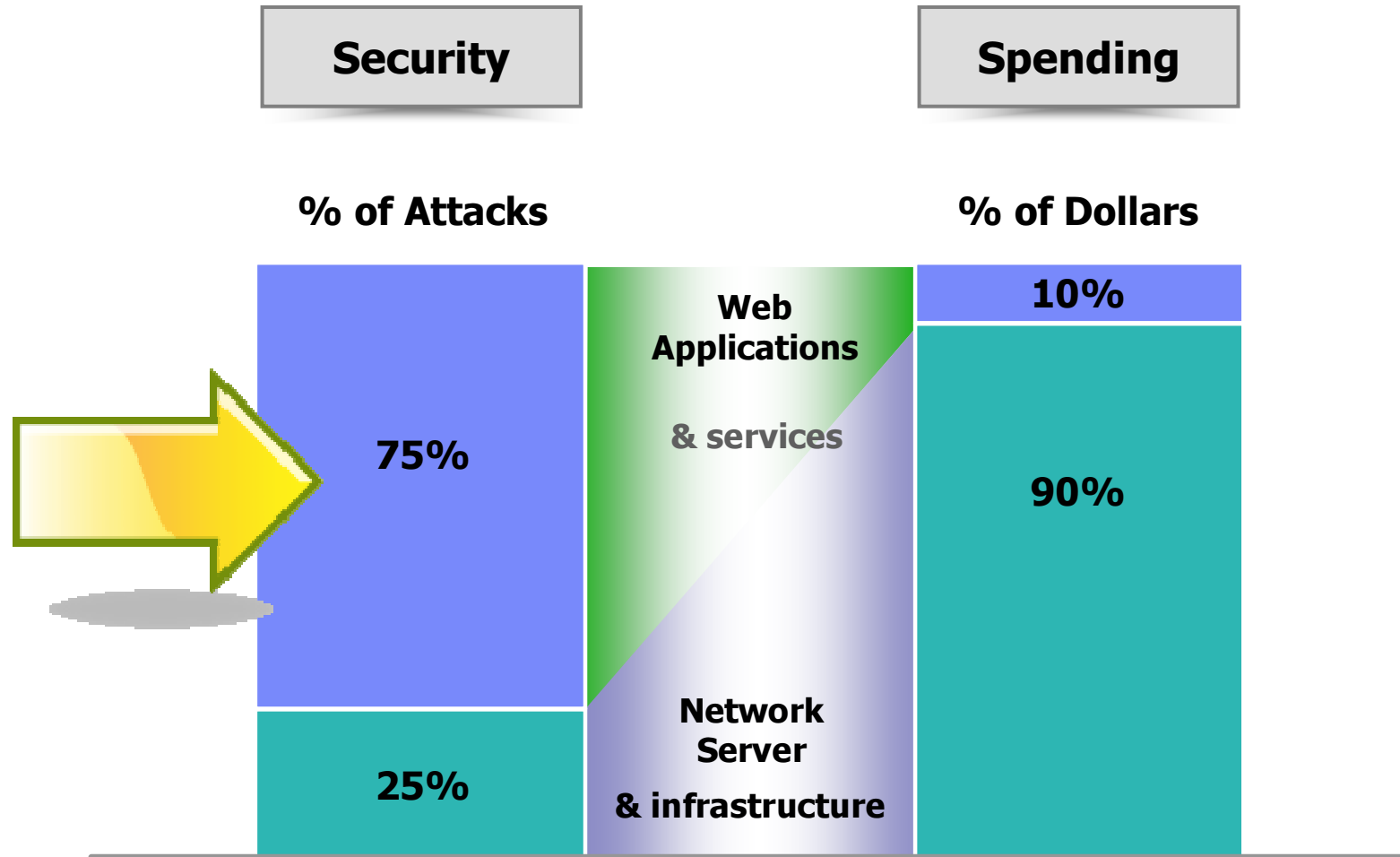
Privacy Policy | Security Statement | © 2006 Altoro Mutual, Inc.

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%

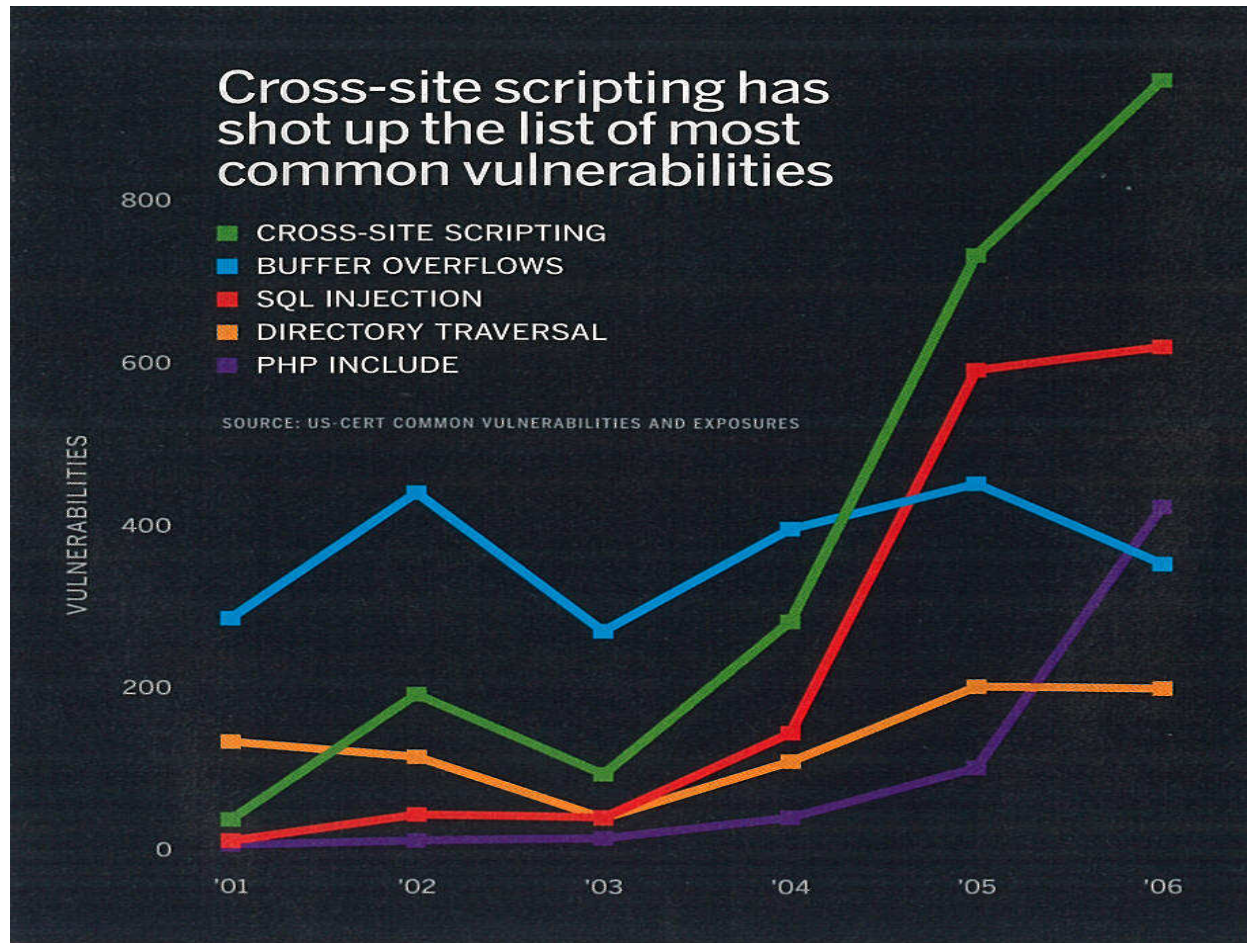
The Fact: Attacks targeted at a new area



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



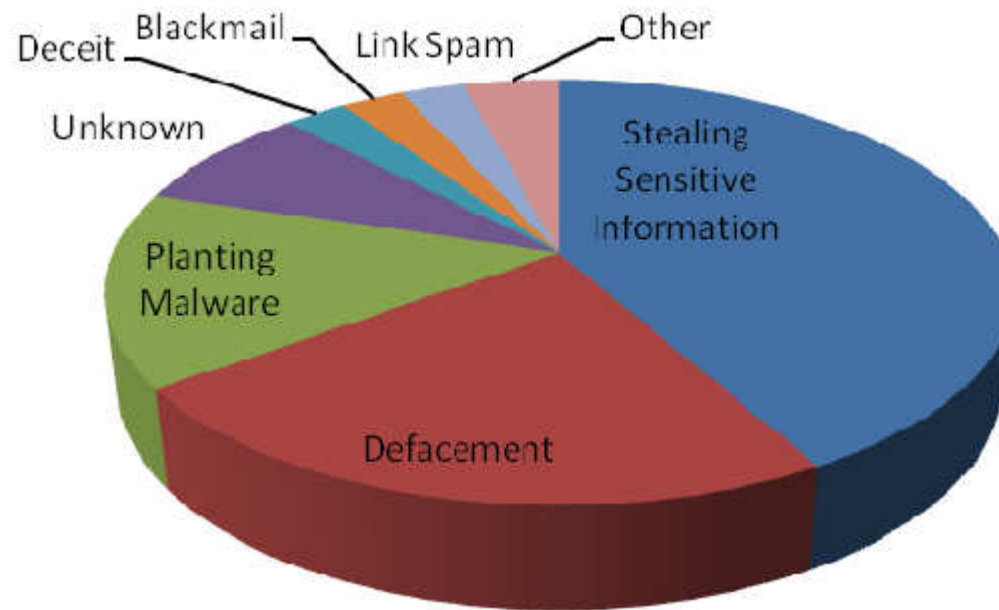
How Common Are These Problems?



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



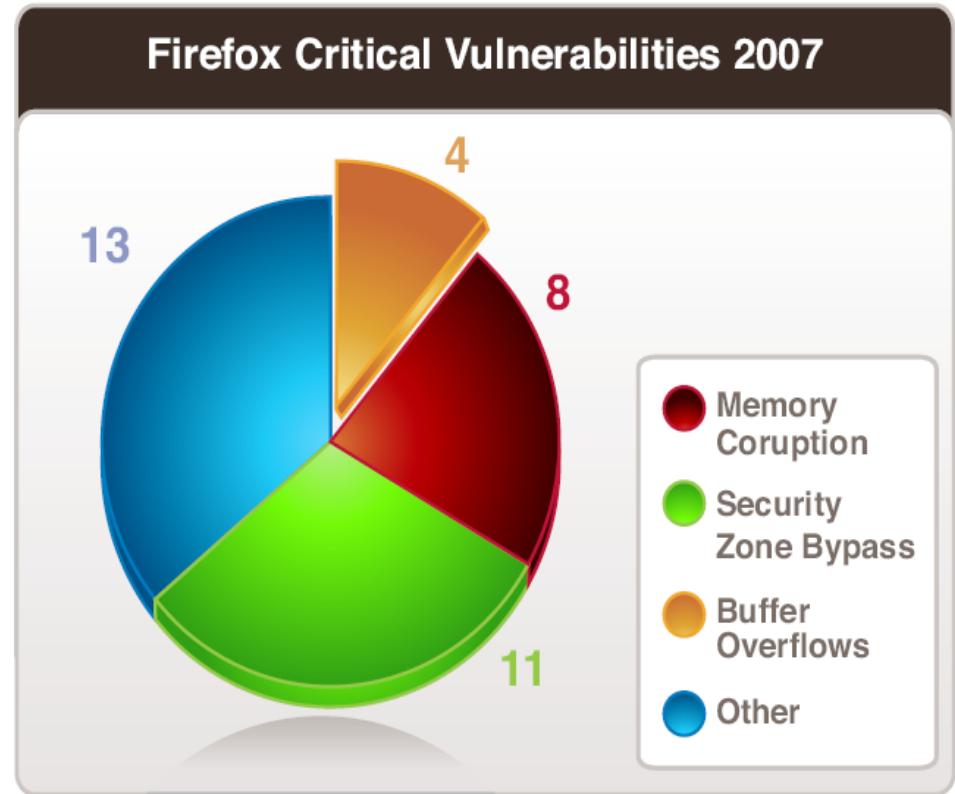
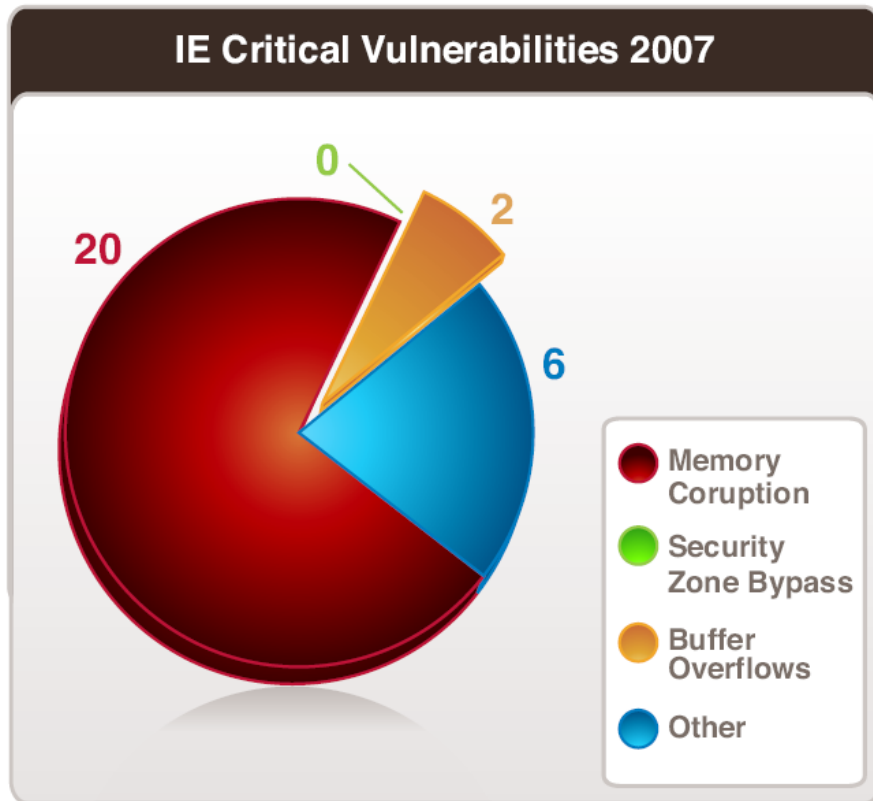
Motives Behind Application Hacking Incidents



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:

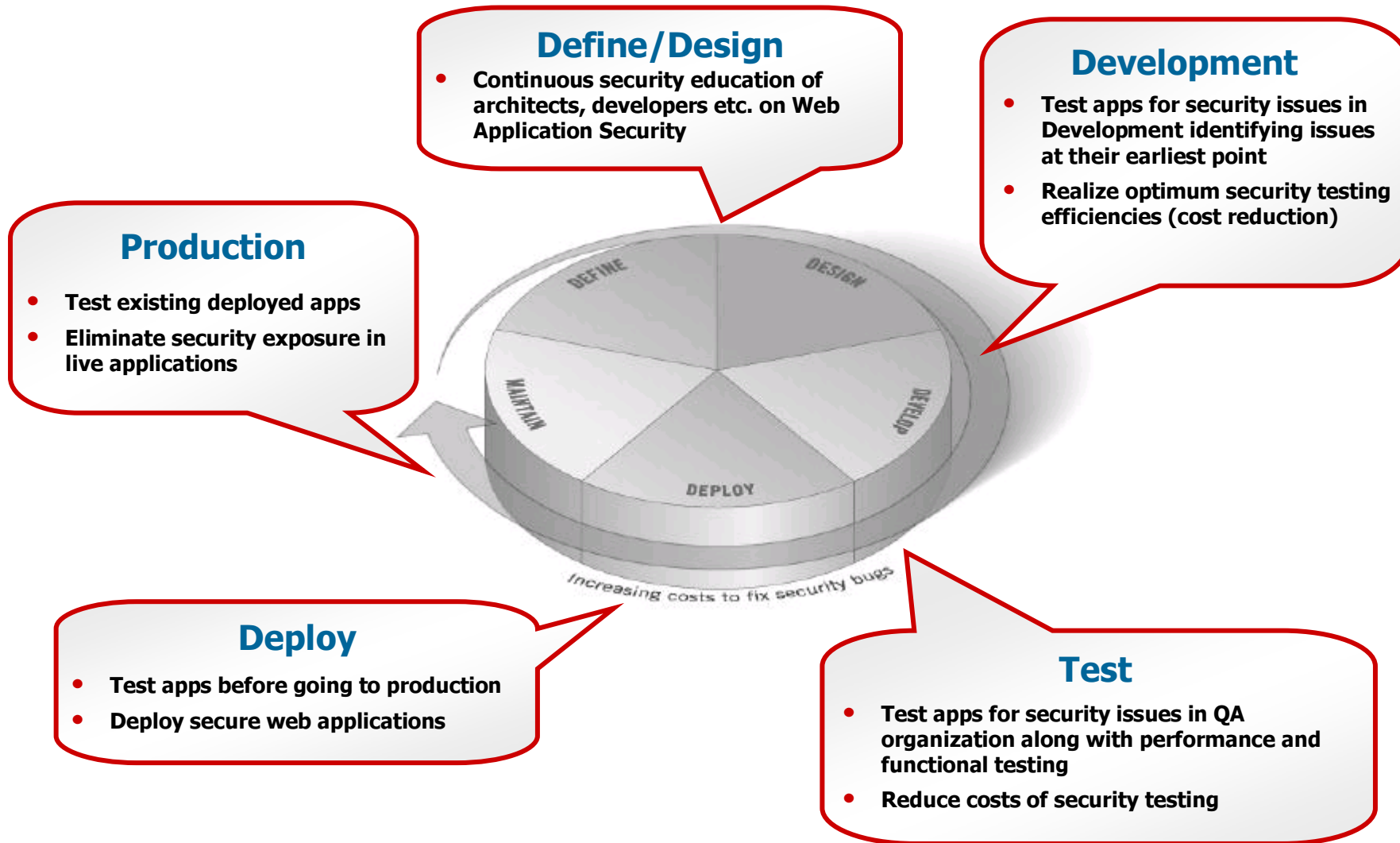
- Customer facing services
- Partner portals
- Employee intranets

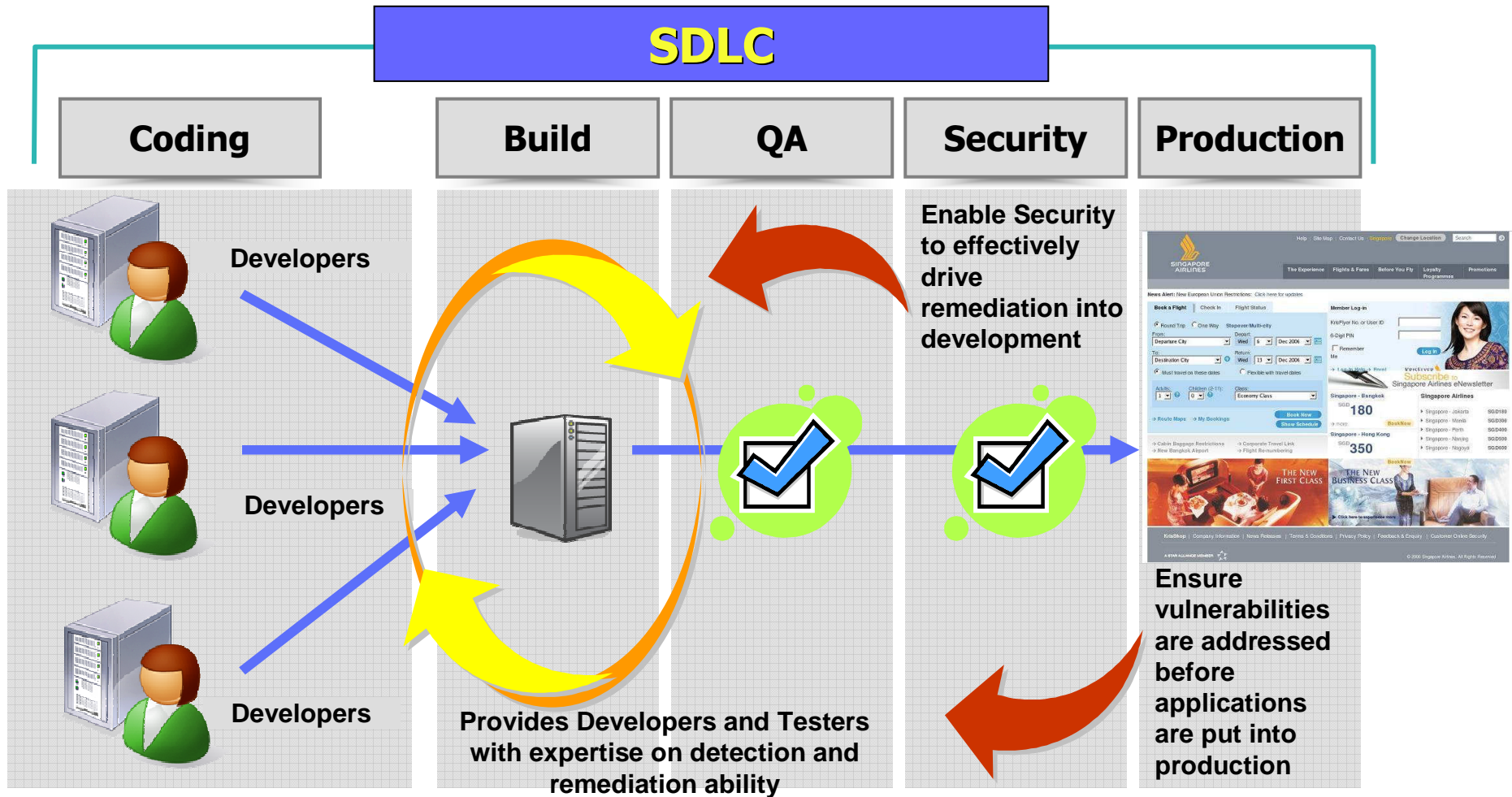
Source:

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



Building Security Into the Development Process







IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**

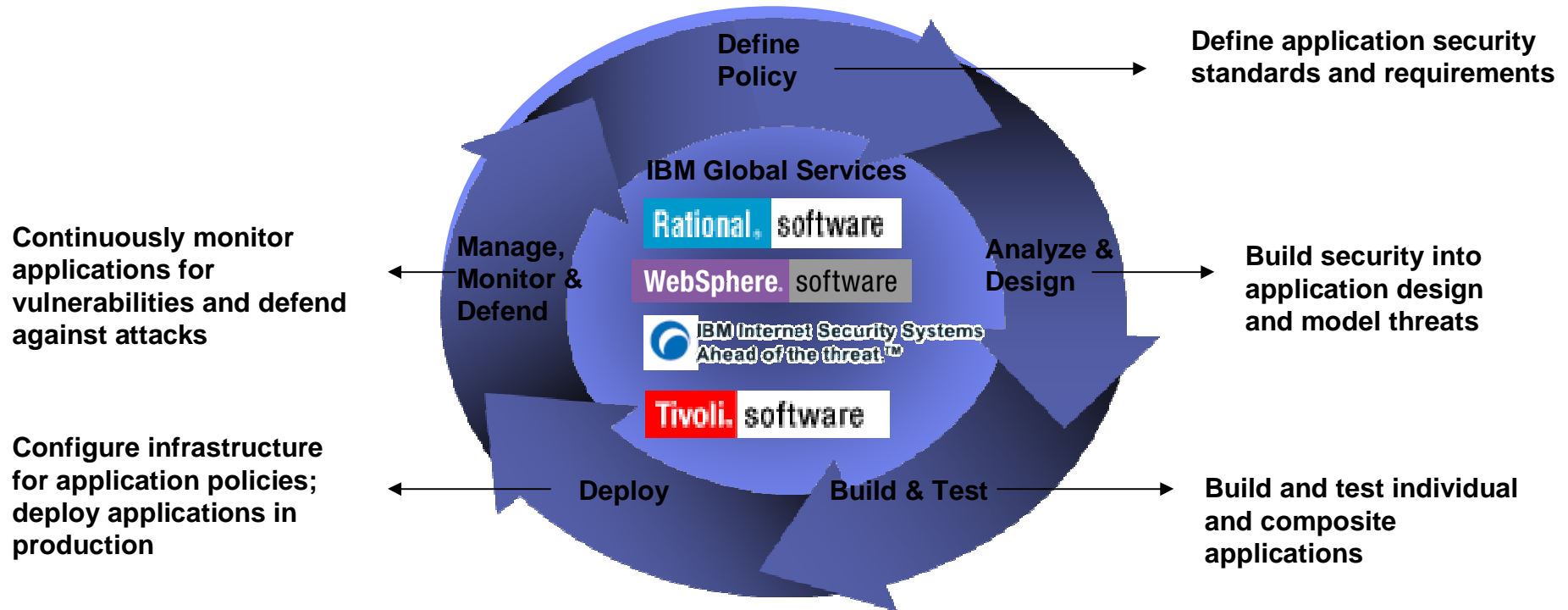


IBM Vision and Roadmap for Application Security

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

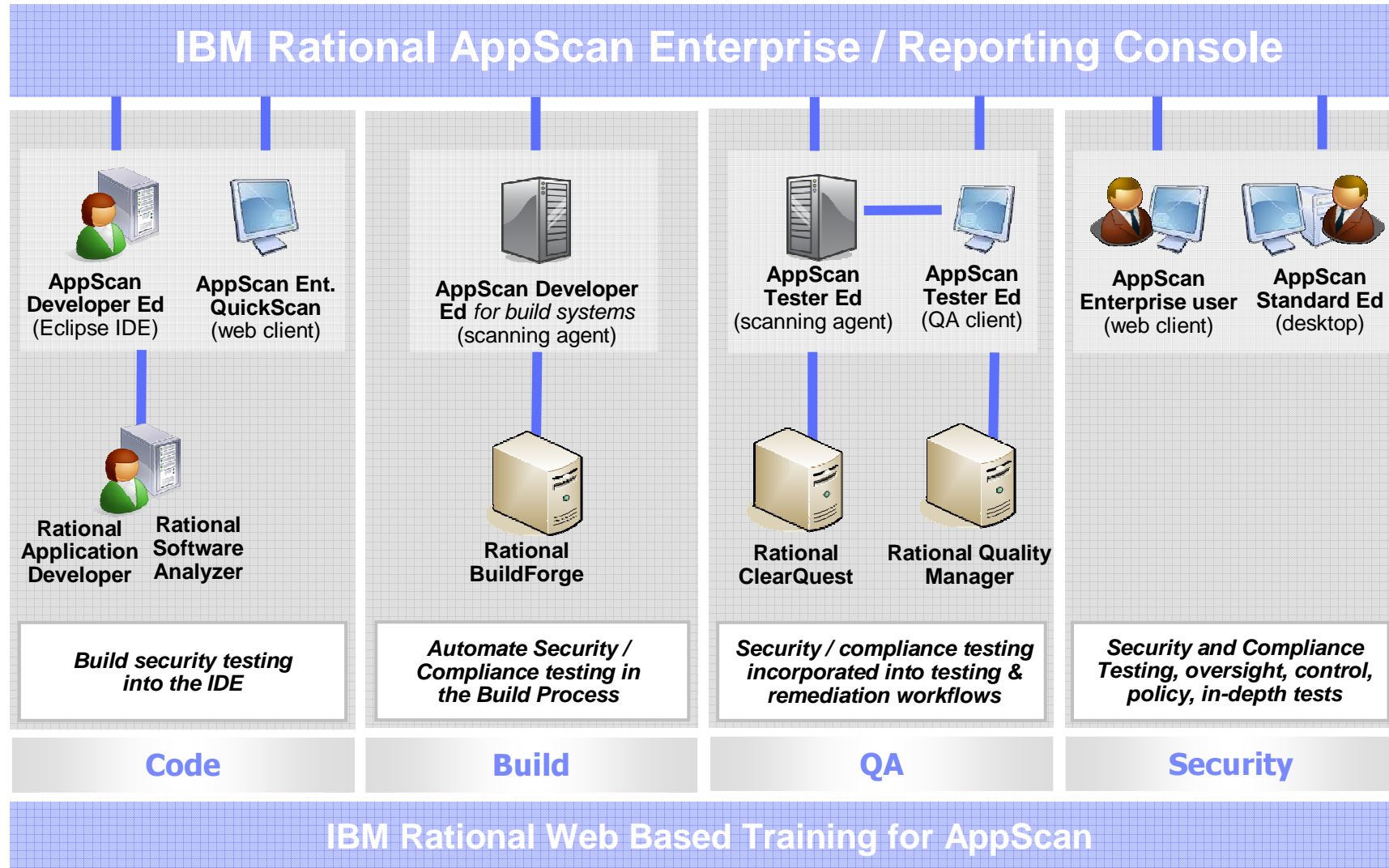
- IBM Global Services – **security risk assessments** helping define policies and processes
- Rational – **automated vulnerability testing** for web applications/web services across the development cycle
- IBM Technology Services/ISS – **managed services** for network and application vulnerability assessment
- 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

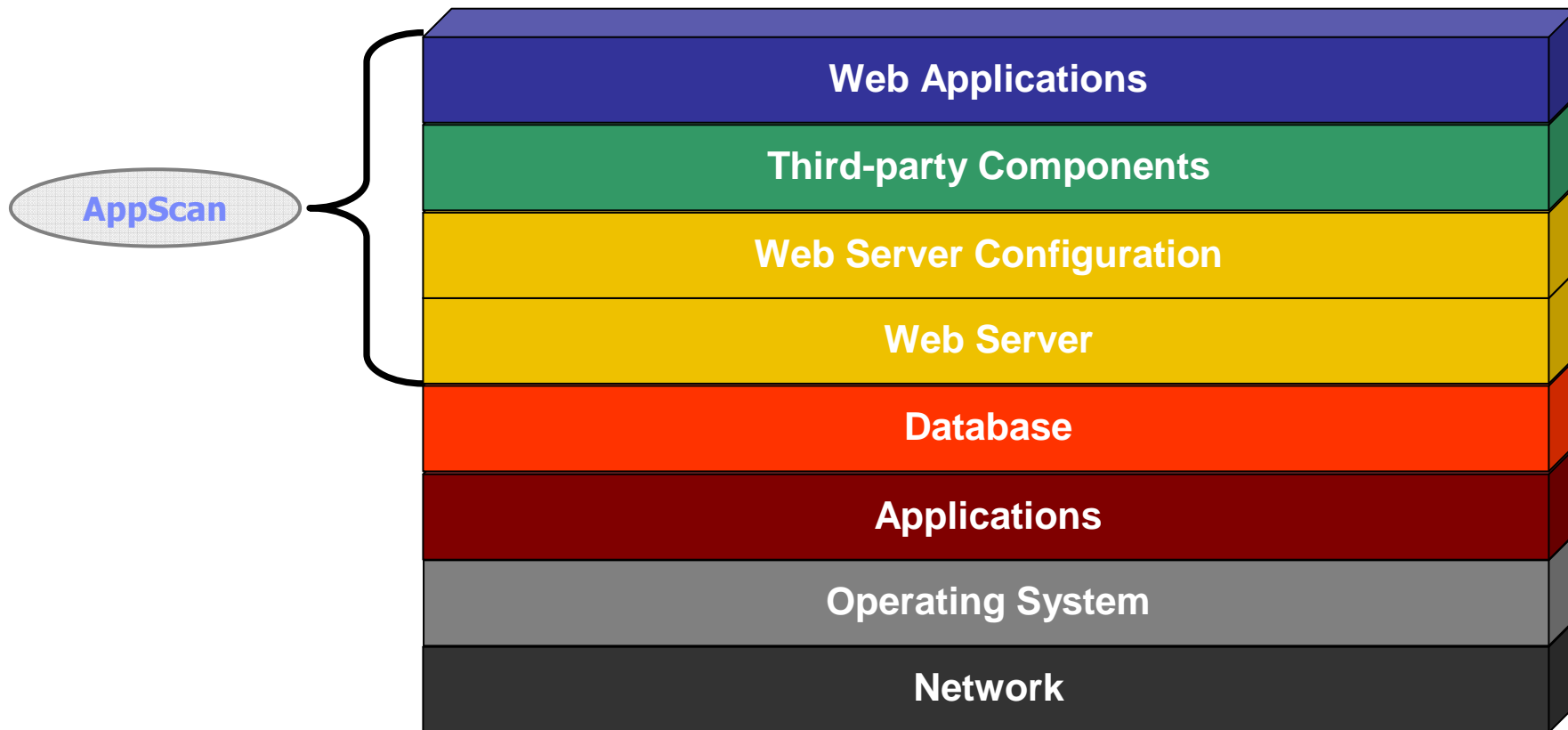


Includes Fall
2008 Releases

IBM Rational AppScan SDLC Ecosystem



What does AppScan test for?



How does AppScan work?

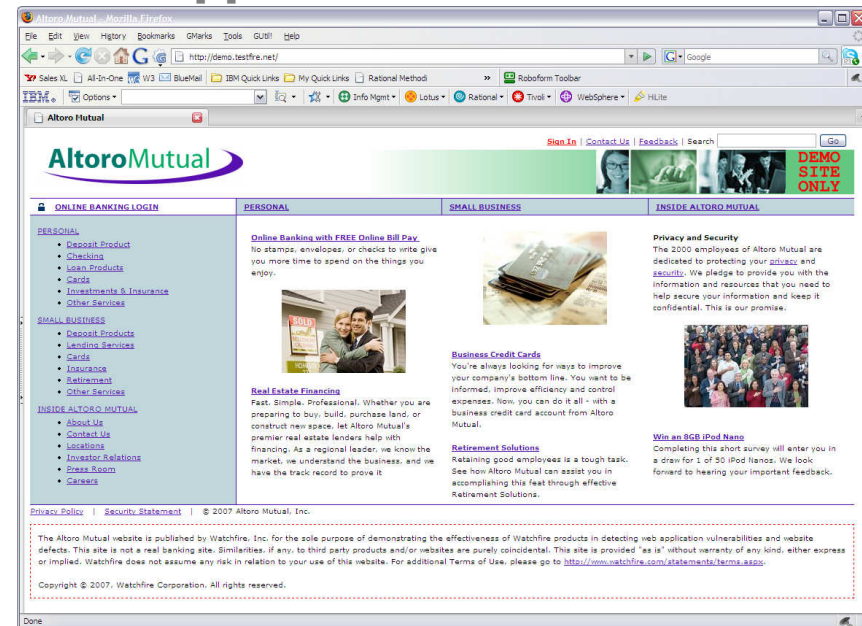
- Approaches an application as a black-box
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected Test policy
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules

HTTP Request

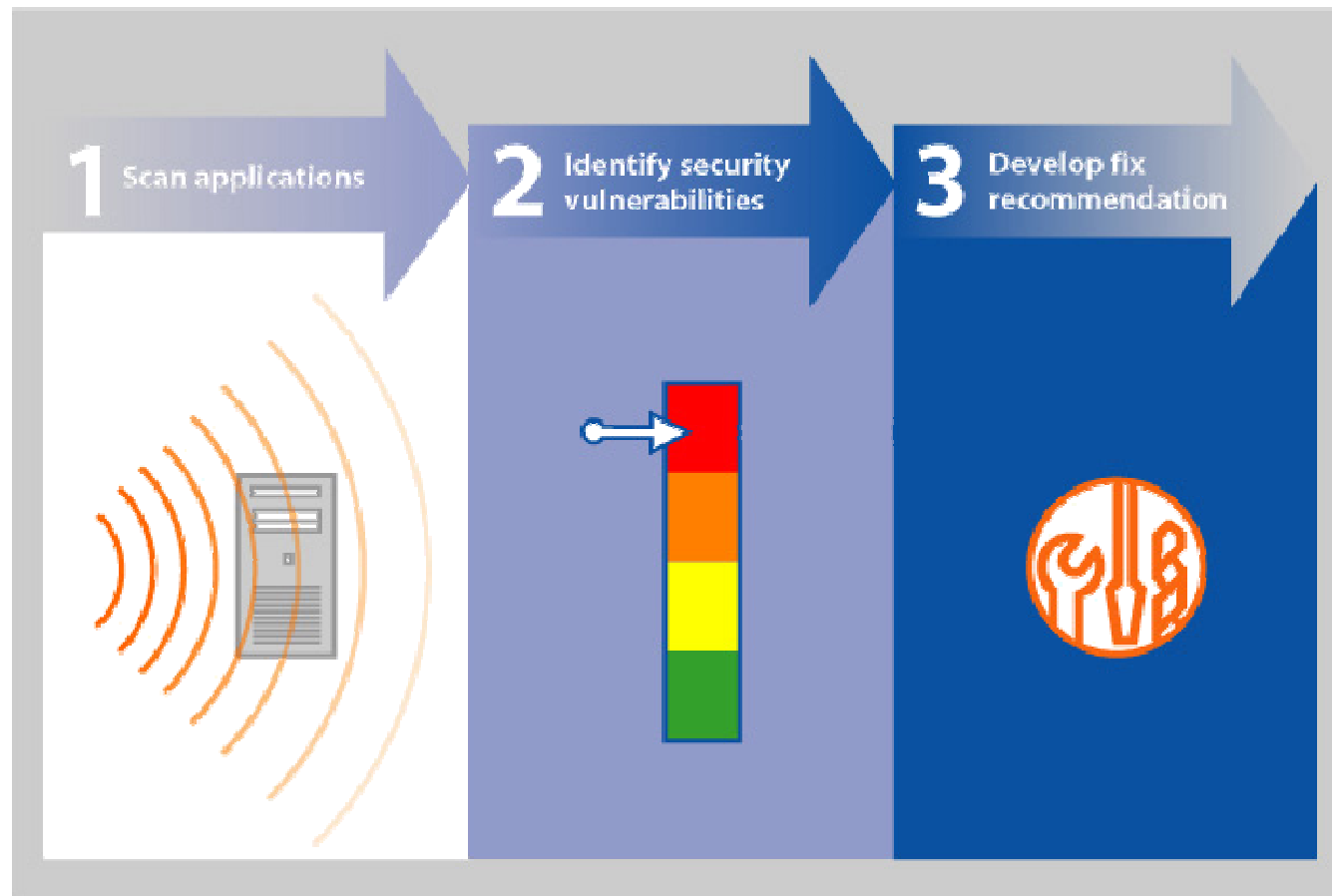


HTTP Response

Web Application



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



Identify Vulnerabilities

The screenshot displays the AppScan 7.5 interface. The main window title is "AppScan 7.5 Demo Scan 1.scan - Watchfire AppScan". The interface is divided into several sections:

- Navigation Pane (Left):** Shows a tree view of the scanned application "My Application (53)" with sub-items like "http://demo.testfire.net/ (53)", "cgi.exe (1)", "comment.aspx (2)", "default.aspx", "disclaimer.htm", "feedback.aspx (1)", "search.aspx (1)", "servererror.aspx", "subscribe.aspx (3)", "subscribe.swf", "survey_questions.aspx", "admin (1)", "bank (40)", and "images (1)".
- Summary (Top Right):** A yellow banner indicates "Scan is Incomplete". Below it, a summary shows "53 Security Issues (368 variants) for 'My Application'".
- Issue List (Middle Right):** A list of vulnerabilities is shown, including:
 - Blind SQL Injection (4)
 - Cross-Site Scripting (5)
 - Format String Remote Command Execution (1)
 - HTTP Response Splitting (1)
 - SQL Injection (6)
 - XPath Injection (1)
 - Cookie Poisoning SQL Injection (1)
- Detailed View (Bottom):** The "Request/Response" tab is active, showing a "Test" variant. The request is a POST to "/bank/account.aspx" with a "Cookie" and "listAccounts" parameter. The response is an "HTTP/1.1 200 OK".
- Variant Details (Right):** Shows "ID: 9294" and a "Difference" section stating: "The following changes were applied to the original request: Set parameter listAccounts's value to '0%2B0%2B1001160141%2B0%2B1001160141%2B0'".
- Reasoning (Right):** Explains: "This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting..."
- Status Bar (Bottom):** Shows "Visited URLs 108/108", "Completed Tests 14194/14194", and "53 Security Issues" (18 Critical, 4 High, 22 Medium, 9 Low).



Actionable Fix Recommendations

The screenshot displays the AppScan 7.5 interface. The left sidebar contains navigation options: Security Issues, Remediation Tasks, and Application Data. The main area shows a scan of 'My Application' at 'http://demo.testfire.net/'. A list of files is shown, including 'cgi.exe', 'comment.aspx', 'default.aspx', 'disclaimer.htm', 'feedback.aspx', 'search.aspx', 'servererror.aspx', 'subscribe.aspx', 'subscribe.swf', 'survey_questions.aspx', 'admin', 'bank', and 'images'. A 'Scan is Incomplete' notification is present at the top right. Below it, a list of security issues is shown, arranged by severity (Highest on top). The issues include: Blind SQL Injection (4), Cross-Site Scripting (5), Format String Remote Command Execution (1), HTTP Response Splitting (1), SQL Injection (5), XPath Injection (1), and Cookie Poisoning SQL Injection (1). The 'Blind SQL Injection' issue is selected, and the 'Fix Recommendation' tab is active. The fix recommendation details are as follows:

Blind SQL Injection

Fix Recommendation

General

There are several issues whose remediation lies in sanitizing user input. By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

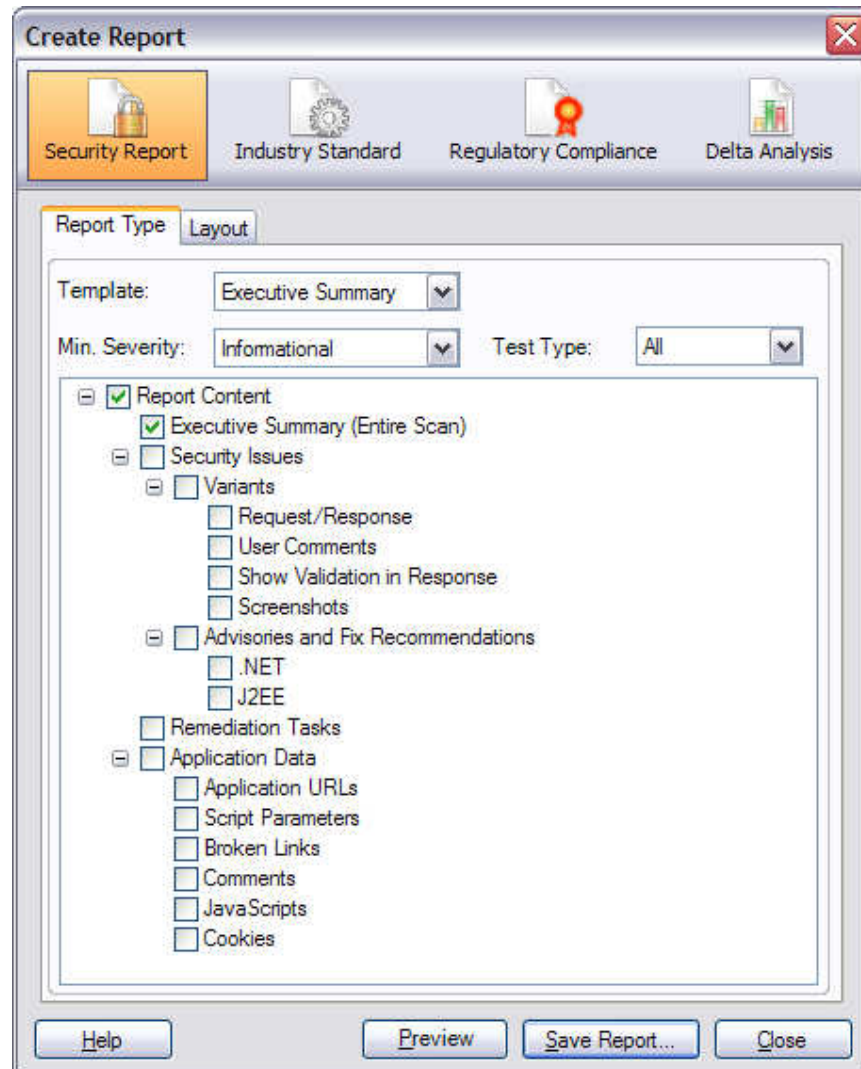
It is advised to filter out all the following characters:

- [1] | (pipe sign)
- [2] & (ampersand sign)
- [3] ; (semicolon sign)

The status bar at the bottom indicates: Visited URLs 108/108, Completed Tests 14194/14194, 53 Security Issues, 18 Critical, 4 High, 22 Medium, and 9 Low severity issues.



Report



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>&pass=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph1orq1
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:

```
GET /bank/login.aspx?uid=>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&pass=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph1orq1
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
```



AppScan Tester Edition for RQM

The screenshot shows the Rational Quality Manager (RQM) interface. The top navigation bar includes 'Home', 'Planning', 'Construction', 'Execution', 'Analysis', and 'Help'. The user is logged in as Michael Brown (Test Architect). The main content area is titled 'Web UI Tests' and shows the 'Overview' tab. The 'Test Group Name' is 'Web UI Tests' and the status is 'In Progress'. The 'Details' section shows the originator as 'ADMIN' and the description as 'Provide full test coverage of the Web UI'. A 'Work Item' summary shows 35 items owned by Arnold Adams. Below this is a table of 'Test Cases' with columns for Name, Description, and Owner.

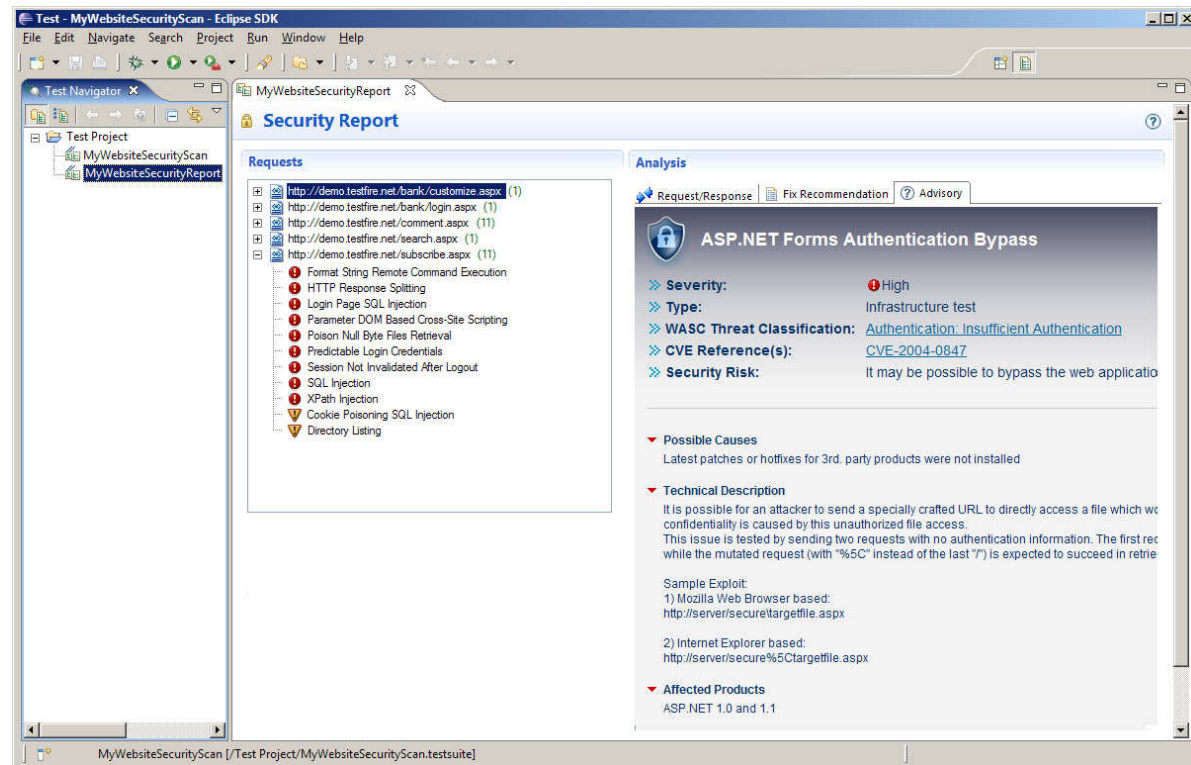
Name	Description	Owner
21 Web UI Functional Tests	Test for functionality issues in the web application	Laura Lyons (Tester Lead)
23 Web UI Performance Tests	Test for performance issues in the web application	Craig Lawton (Tester)
3 Web UI Security Tests	Test for security issues in the web application	Donald David (Developer)

Security Testing is managed just like other types of testing



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

IBM Rational AppScan Enterprise Edition

Jim (Analyst) | Help | Support | About | Log Out

Training | Jobs & Reports | Administration

Jobs & Reports > Acme Hackme > Analysts

Analysts - Graphical
Last Updated: 9/11/2007 12:56:50 PM

Report Pack: All Report Packs [Apply]

Folders

- Acme Hackme
 - Analysts
 - Frank
 - Jim
 - Developers
 - Admin
 - Andrew
 - Chris
 - Jennifer
 - Templates

Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank)
- Sarbanes-Oxley Act (SOX) (Investment)
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

Issue Severity History

Issue Management History

Issue Severity by Report Pack

WASC Threat Classification

Support

Category	High	Medium	Low	Information
Support	~4000	~1000	~500	~1000
On-Demand Services	~1000	~200	~100	~100
Store	~1000	~500	~200	~100
Main Website	~8000	~1000	~500	~1000
Intranet	~1000	~200	~100	~100
Movies	~1000	~500	~200	~100



Integrated Computer Based Training

Key to adoption across the organization is education

The screenshot shows a Microsoft Internet Explorer browser window displaying a training slide titled "AppScan Knowledge OnDemand". The slide content is as follows:

- Self-service – more convenient than traditional training
 - Participants no longer have to schedule time “out of the office”
- Self-paced – greater information retention
 - With digestible content modules, participants no longer experience information overload
- Just-in-time reference-ability
 - Full access to searchable, online content for 12 months
- Structure
 - Courses are individual modules
 - Typically 15 minutes or less

The slide also features the Watchfire logo in the bottom right corner. The browser's address bar shows the URL: <http://download.watchfire.com> - Getting the Most from AppScan Knowledge OnDemand - Microsoft Internet Explorer. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. On the right side of the slide, there is a sidebar with a profile for Karl Snider, Product Manager, Training and Services, and a table of contents:

Outline	Thumb	Notes	Search
Slide Title			Duration
How to Use AppScan ...			00:09
Topics			00:10
AppScan University			00:12
AppScan Knowledge ...			00:42
Enrollment And Loggi...			00:44
Selecting Your Course			00:33
Viewing Your Course			00:19
Using the Navigation ...			00:52
Summary			00:15
Thank You!			00:13

At the bottom of the slide, a progress bar indicates "2 Minutes 59 Seconds Remaining". The browser's taskbar at the bottom shows the Start button, several application icons, and the system tray with the time 4:10 PM.



800+ Companies Depend On Watchfire

9 of the Top 10 Banks	8 of the Top 10 Technology Companies	7 of the Top 10 Pharma / Clinical Companies	Telecommunication Companies
<p>Multiple Large Government Agencies</p>			



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.

