Solving the Enterprise Security Challenge

Derek F Holt
Worldwide Sales Executive
Jazz, Security, Software Delivery Platform
dfholt@us.ibm.com

Rational. software

Online Risks Continue to Increase

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 contest**

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.

Breach Attempts Increase in Times of Economic Crisis

" In 2009, security products will remain stronger than other IT areas because of compliance and business requirements. In fact, a recent IDC economic meltdown study showed that **security was the least likely area to face cuts in response to the current economic crisis**. Many organizations will defer discretionary projects, freeze hiring, and actively look for savings from virtualization, hosted services, and automated security management."

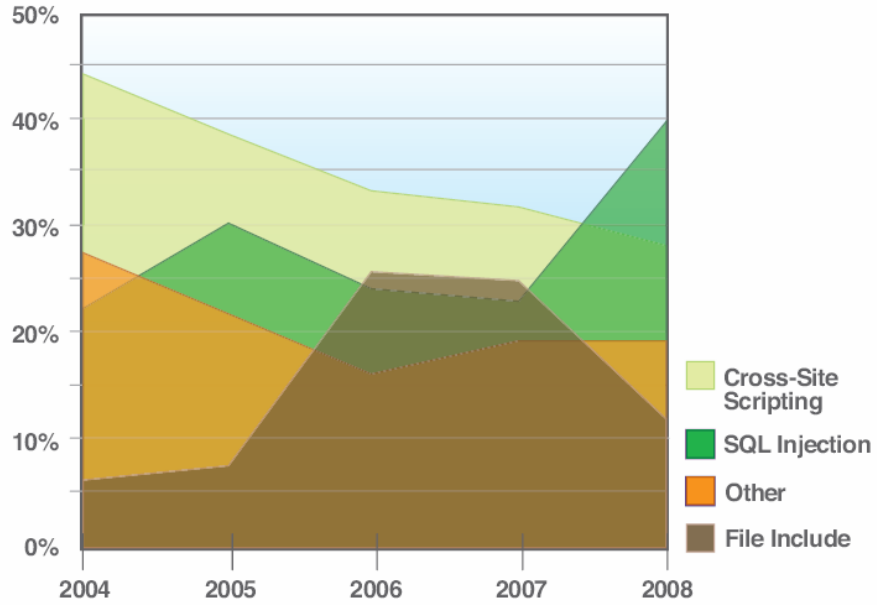
Source: December 2008, IDC #215745

"…just as street crime increases in times of financial stress, more attackers are likely to perform an online version of shoplifting and bank robbery ."

Source: October 2008, DarkReading

2008 Web Threats Take Center Stage

- Web application vulnerabilities
  - ***Web applications have become the Achilles heel of Corporate IT Security***
  - Represent largest category in vuln disclosures (55% in 2008)
  - *This number does not include custom-developed Web applications!*
  - 74% of Web application vulnerabilities disclosed in 2008 have no patch to fix them



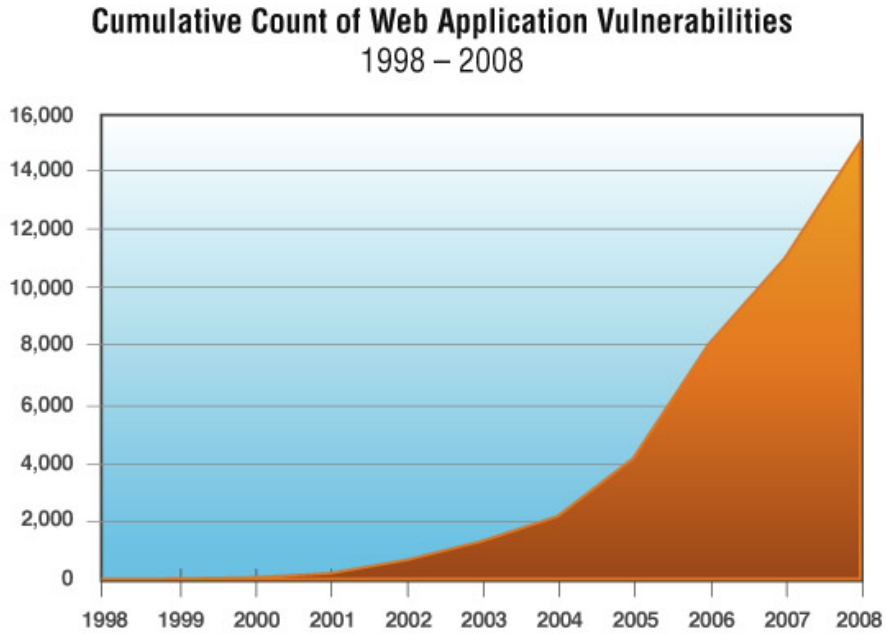
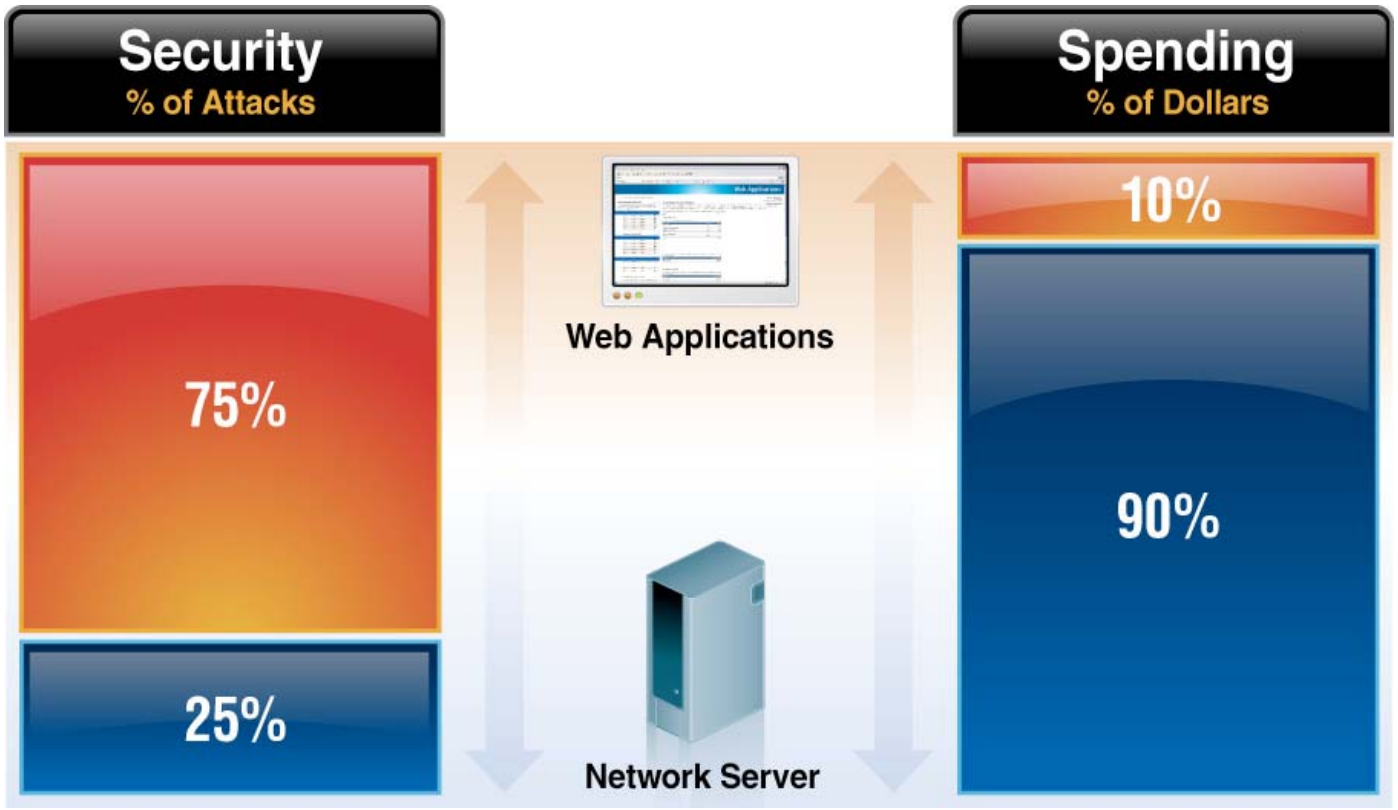


Figure 19: Web Application Vulnerabilities by Attack Technique, 2004 – 2008

source: IBM X-Force®

Reality: Most Attacks are Targeted at Web Apps



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

2/3 of All Web Applications are Vulnerable

***Gartner*

Changing Security Landscape of Today

"Webification" has changed everything

- Infrastructure is more abstract and less defined
- Everything needs a web interface
- Agents and heavy clients are no longer acceptable
- Traditional defenses no longer apply

Many Web Security Drivers

- Increase in vulnerabilities / disclosures
  - Application security has become the top threat
- Regulatory Compliance
  - Requirements such as PCI, HIPAA, GLBA, SOX, etc
- User demand
  - For rich applications is pushing development to advanced code techniques – Web 2.0 introducing more risks to threats
- Enterprise Modernization
  - Driving traditional applications to online world (SOA), increasing corporate risk
- Cost cutting in current economic climate
  - Demands increased efficiencies

Who Do We Need To Protect our Enterprise From?

- **Organized Crime**
  - What: Data & Identity Theft, Extortion
  - Why: Profit

- **Espionage (Nation State & Corporate)**
  - What: Data Theft & Intellectual Property
  - Why: Power

- **H4ck0rZ / Script Kiddies**
  - What: Defacement & Denial of Service
  - Why: Prestige

The Cost Of A Breach, Broken Out For Three Sample Companies

		Cost per record		
Category	**Description**	**Company A: Low-profile breach in a nonregulated industry**	**Company B: Low-profile breach in a regulated industry**	**Company C: High-profile breach in a highly regulated industry**
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	$50	$50	$50
Lost employee productivity	Employees diverted from other tasks	$20	$25	$30
Opportunity cost	Customer churn and difficulty in getting new customers	$20	$50	$100
Regulatory fines	FTC, PCI, SOX	$0	$25	$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	$0	$0	$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	$0	$5	$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	$0	$0	$25
Total cost per record		**$90**	**$155**	**$305**

September 2008 **"Confessions Of A QSA: The Inside Story Of PCI Compliance"**

Why Are Our Enterprises at Risk?

1. **Developers are not trained in security**
   - Most computer science curricula have no security courses
   - Focus is on developing features
   - Security vulnerability = BUG

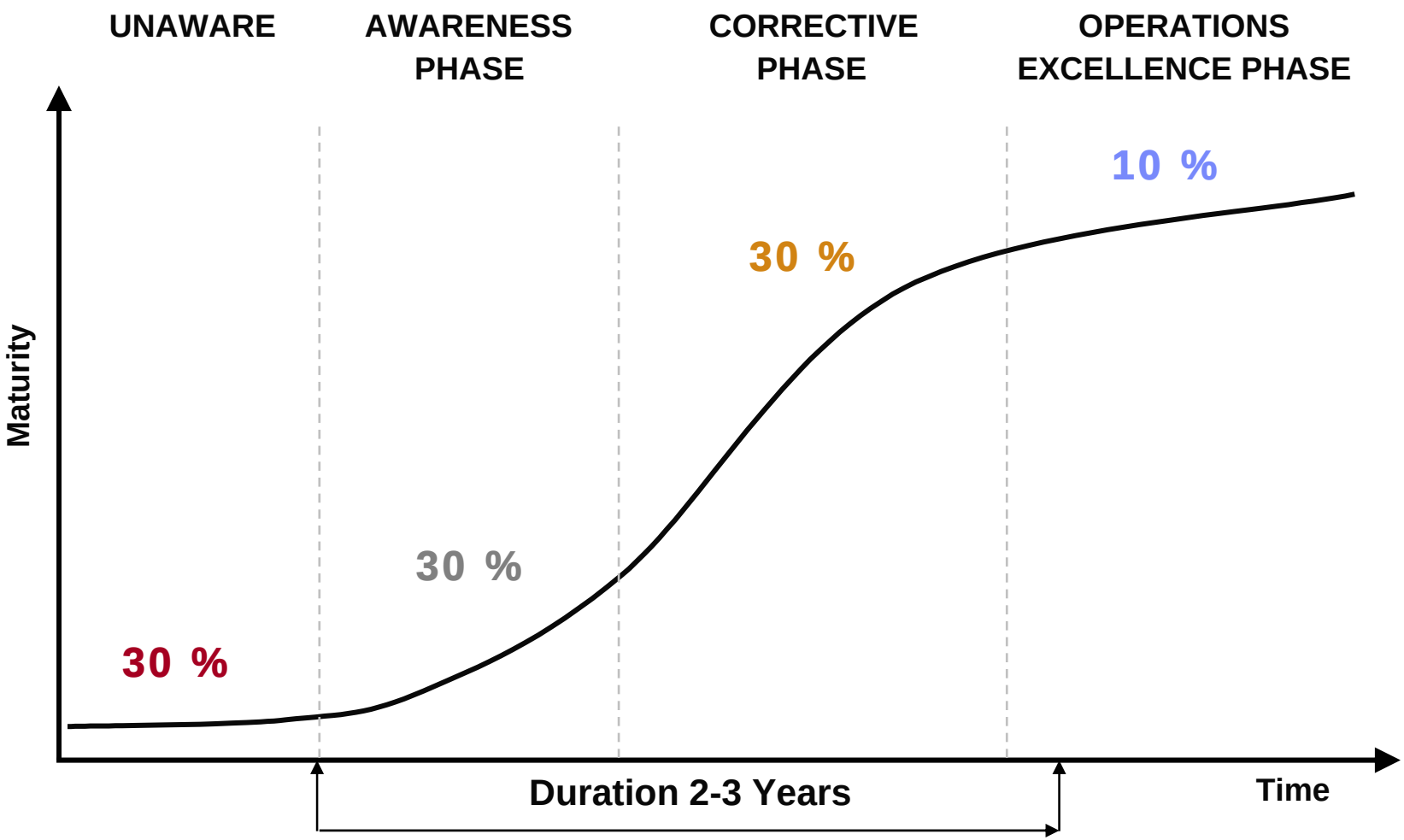
2. **Under investment from security teams**
   - Lack of tools, policies, processes, people

3. **Growth in complex, mission critical online applications**
   - Online banking, commerce,
   - Web 2.0, etc (AJAX, JSON, AMF, JavaScript, Adobe Flash, etc)

Organizations must mitigate their online risk!

- *Organizations need to mitigate the risk of a Web Application Security breach!*
  - They need to find and **remediate** vulnerabilities in their Web Applications before they are exploited by Hackers
  - They need to do this in a ***cost effective*** manner

Application Security Maturity Model



Addressing Web Application Security

Approaches for addressing Web Application Security

Strategic
- Enterprise-Wide
- Scalable Solution

Internal Tactical
- Manual Efforts, Desktop Audit Tools
- Internal Security Experts

Outsourced
- Consultants
- Pen Testing

Do Nothing

What is the cost of a defect?

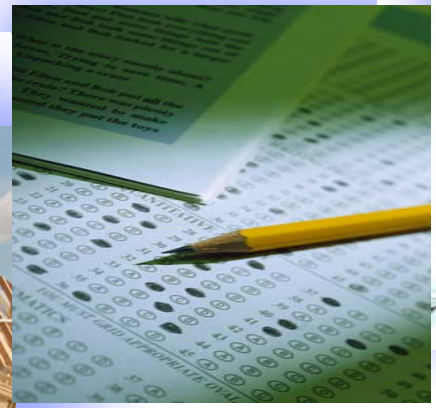
80% of development costs are spent **identifying and correcting defects**!

During the coding phase

$25/defect

During the build phase

$100/defect



During the QA/Testing phase

$450/defect

Once released as a product

$16,000/defect

The increasing costs of fixing a defect….

Enabling the Operationalization of Security Testing

Clients are addressing Web Application Security in three ways:

1 Outsource Security Testing (SaaS)

- Outsource web application security infrastructure or testing
- Enables immediate identification of sources of online risk without the necessary time and investment for in-house training and resources
- Fastest path to actionable information

2 Enable Security Specialists

- Requires web application security subject matter expertise
- Single-step security testing (no additional oversight required as expertise is built-in)
- Eliminates training requirements for non-security experts

3 Embed Security into Development

- Implement environment-specific security testing solution for select stakeholders
- Alleviates security testing bottleneck downstream
- Increases security awareness across the organization (code security improvement, vulnerability awareness)
- Enables a more efficient process for on-time and on-budget application development

Customers receive actionable reports (AppScan OnDemand)

Control, Monitor, Collaborate and Report Web Application Security Testing

Outsourced Testing: Case Study

An enterprise that has

- Many legacy and newly created web applications
- A small security team compared to the number of web applications requiring security testing
- Developers that are not that aware of security

The challenge

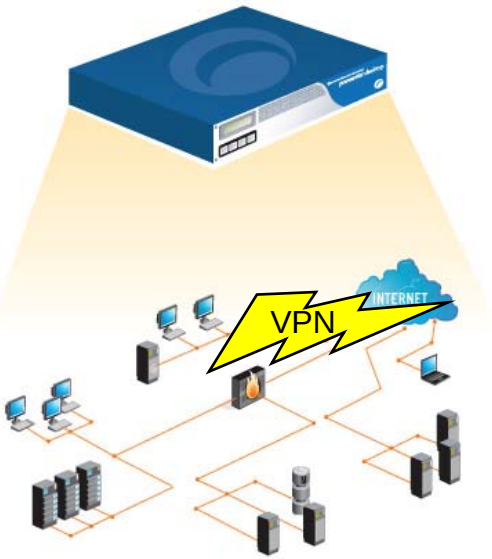
- Limited resources
- Need for detailed and actionable test results
- Need to test a large number of web applications

Outsourced Testing: AppScan OnDemand

- Hosting outsourced to IBM/Rational
  - Rational manages the setup, hardware, upgrades, maintenance, backups, etc.
- Administration outsourced to IBM/Rational
  - Rational creates scan configurations, job schedules, and organizes/prioritizes results – i.e. maximizes the product capabilities on your behalf
- Business/Security Analyst function outsourced to IBM/Rational experts via Solution Management
  - Client is trained on how to interpret and use the information resulting from AppScan and Policy Tester scans
- Client focuses only on issue remediation = customer success

AppScan OnDemand

Scan Web applications/sites



Analyze
(identify issues)

Virtual-SOC Portal

Report
(detailed & actionable)

PCI DSS Reporting

The Payment Card Industry Data Security Standard (PCI) Export Email

Last Updated: 14/04/2009 05:06:11

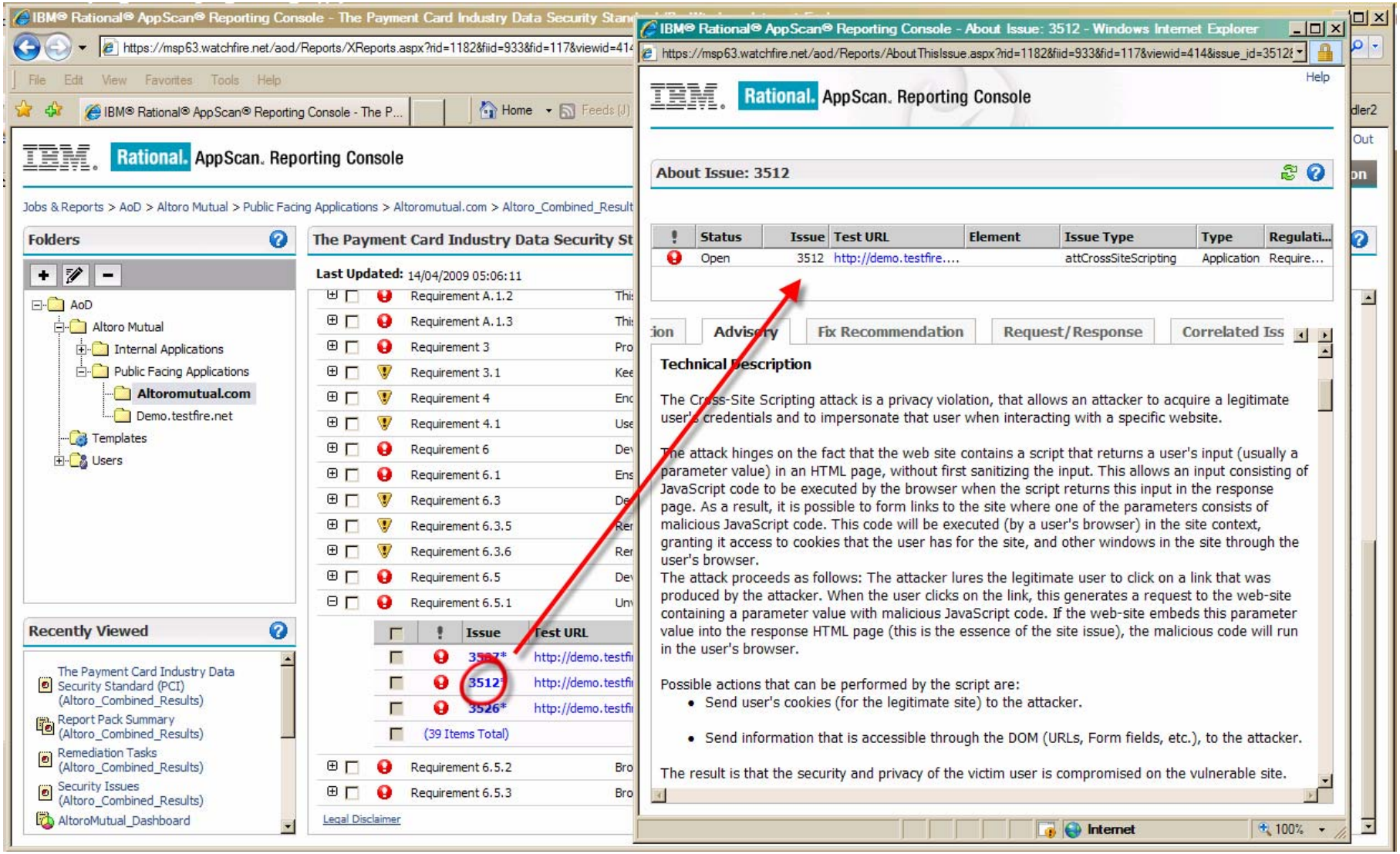
Requirement A.1.2	This section applies to hosting providers only - Protect each entity's (that is a merchant, service provider, or other ...	2
Requirement A.1.3	This section applies to hosting providers only - Protect each entity's (that is a merchant, service provider, or other ...	44
Requirement 3	Protect stored cardholder data	55
Requirement 3.1	Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storag...	2
Requirement 4	Encrypt transmission of cardholder and sensitive information across public networks.	2
Requirement 4.1	Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/ transport layer security (TLS)...	2
Requirement 6	Develop and maintain secure systems and applications.	78
Requirement 6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install...	18
Requirement 6.3	Develop software applications based on industry best practices and include information security throughout the so...	5
Requirement 6.3.5	Removal of test data and accounts before production systems become active.	5
Requirement 6.3.6	Removal of custom application accounts, usernames, and passwords before applications become active or are rele...	5
Requirement 6.5	Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project ...	78
Requirement 6.5.1	Unvalidated input	39

Issue	Test URL	Element	Issue Type	Type
3587*	http://demo.testfire.net/disclaimer.htm		DOMXSS1	Application
3512*	http://demo.testfire.net/comment.aspx		attCrossSiteScripting	Application
3526*	http://demo.testfire.net/comment.aspx	name	attCrossSiteScripting	Application
(39 Items Total)				

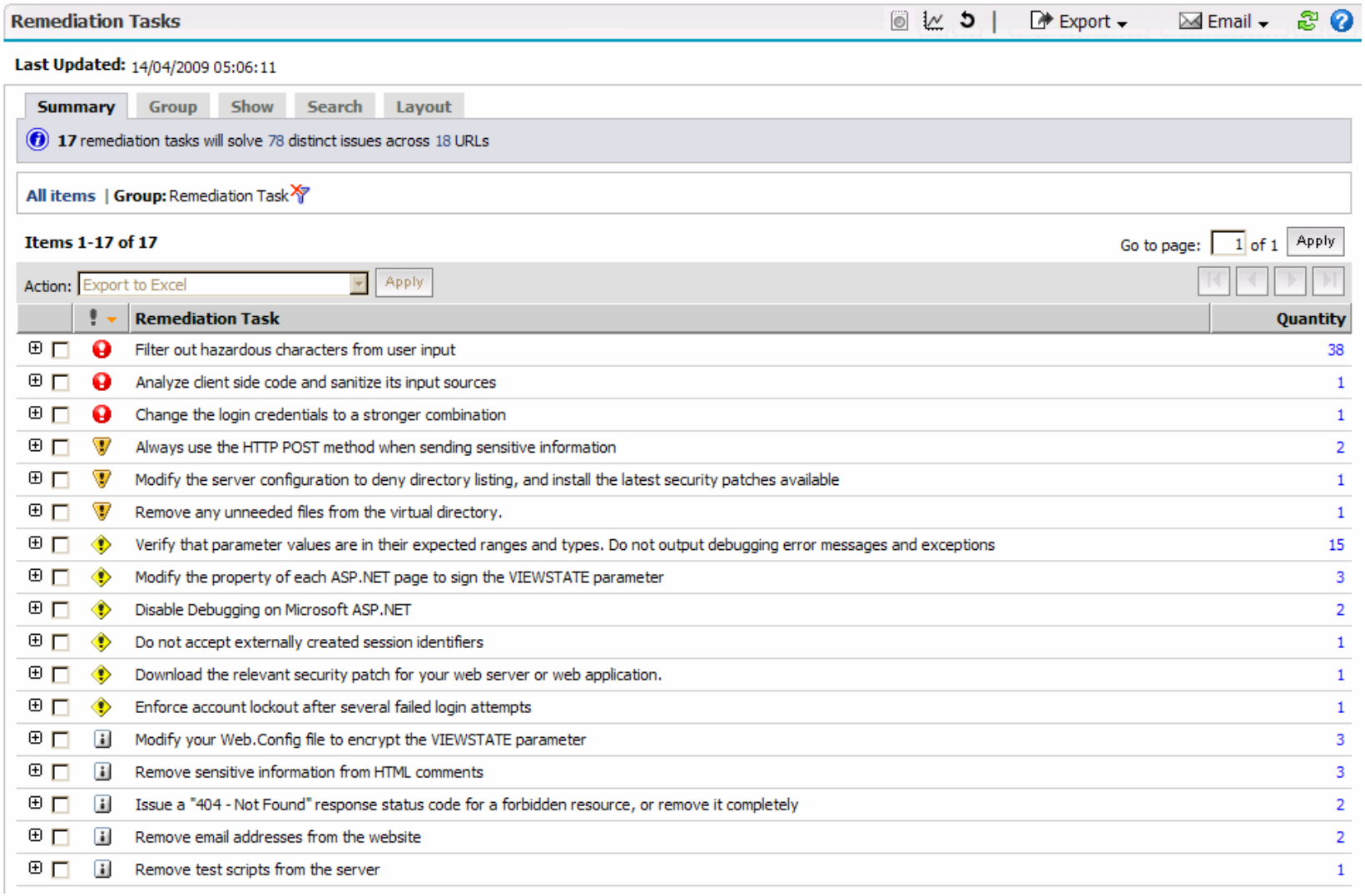
Requirement 6.5.2	Broken access control	4
Requirement 6.5.3	Broken authentication and session management	15

Legal Disclaimer

Findings Advisory and Details



Remediation Tasks – Action Plan



Remediation Tasks | Export | Email

Last Updated: 14/04/2009 05:06:11

Summary | Group | Show | Search | Layout

17 remediation tasks will solve 78 distinct issues across 18 URLs

All items | **Group:** Remediation Task

Items 1-17 of 17 — Go to page: 1 of 1 Apply

Action: Export to Excel Apply

Remediation Task	Quantity
Filter out hazardous characters from user input	38
Analyze client side code and sanitize its input sources	1
Change the login credentials to a stronger combination	1
Always use the HTTP POST method when sending sensitive information	2
Modify the server configuration to deny directory listing, and install the latest security patches available	1
Remove any unneeded files from the virtual directory.	1
Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	15
Modify the property of each ASP.NET page to sign the VIEWSTATE parameter	3
Disable Debugging on Microsoft ASP.NET	2
Do not accept externally created session identifiers	1
Download the relevant security patch for your web server or web application.	1
Enforce account lockout after several failed login attempts	1
Modify your Web.Config file to encrypt the VIEWSTATE parameter	3
Remove sensitive information from HTML comments	3
Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	2
Remove email addresses from the website	2
Remove test scripts from the server	1

Enabling the Operationalization of Security Testing

Clients are addressing Web Application Security in three ways:

1 Outsource Security Testing (SaaS)

- Outsource web application security infrastructure or testing
- Enables immediate identification of sources of online risk without the necessary time and investment for in-house training and resources
- Fastest path to actionable information

Customers receive actionable reports (AppScan OnDemand)

2 Enable Security Specialists

- Requires web application security subject matter expertise
- Single-step security testing (no additional oversight required as expertise is built-in)
- Eliminates training requirements for non-security experts

Security Team uses AppScan Standard Edition & AppScan Reporting Console

3 Embed Security into Development

- Implement environment-specific security testing solution for select stakeholders
- Alleviates security testing bottleneck downstream
- Increases security awareness across the organization (code security improvement, vulnerability awareness)
- Enables a more efficient process for on-time and on-budget application development

Control, Monitor, Collaborate and Report Web Application Security Testing

Enabling Security Team: Case Study

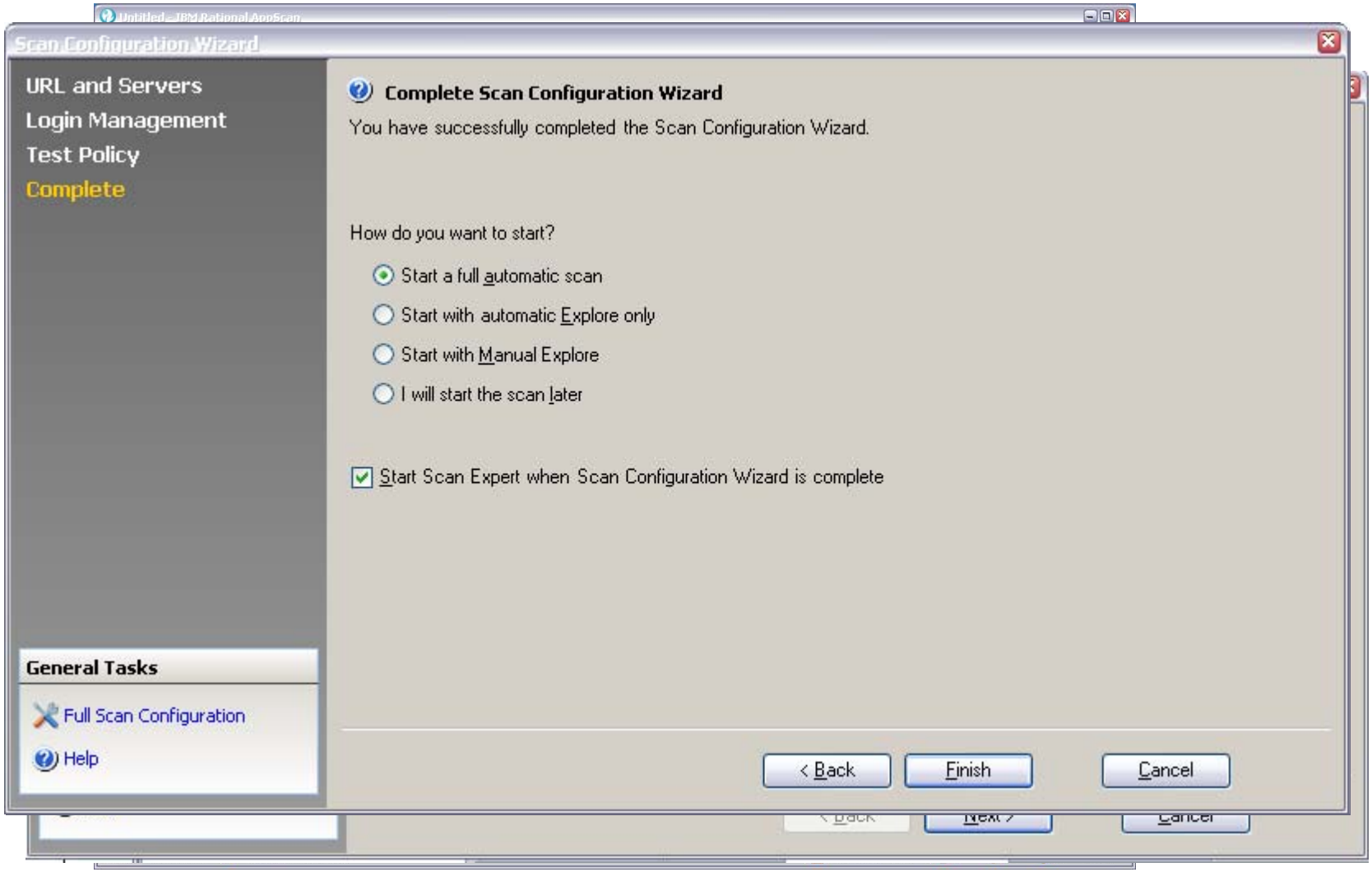
An enterprise that has

- Many web applications
- A policy requiring applications pass a security audit before going to production
- A security team in place to audit the applications
- A process for fixing security issues
  - Security issues found are sent back to developers
  - Developers communicate with the security team and implement the fix.
  - More rounds of auditing until the application passes the security audit

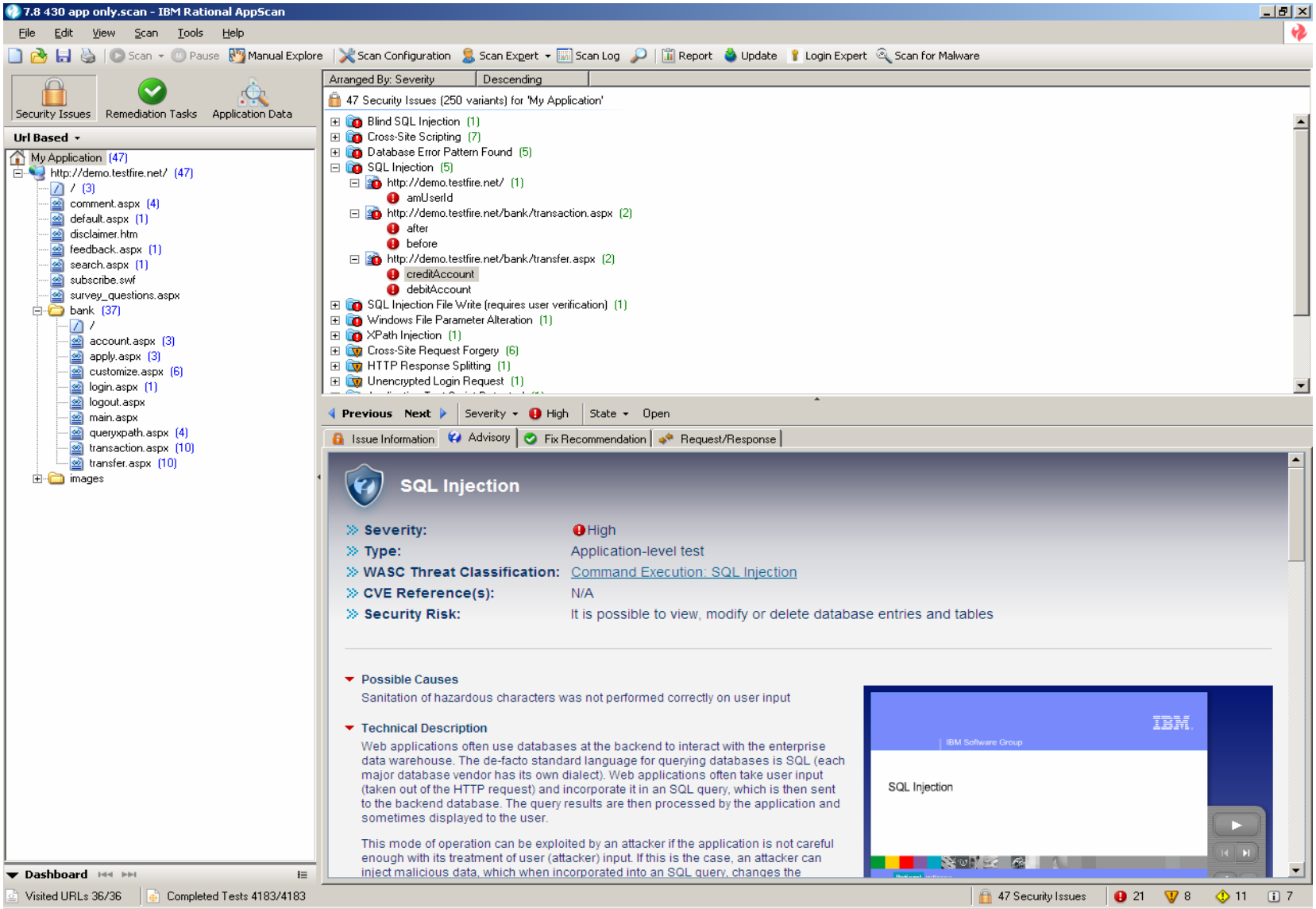
The challenge

- Security team's capacity is insufficient for the number of applications and security issues
- Developers need more detailed information and reproduction scenarios for the security issues detected
- How to securely get the results to the Developers and manage them

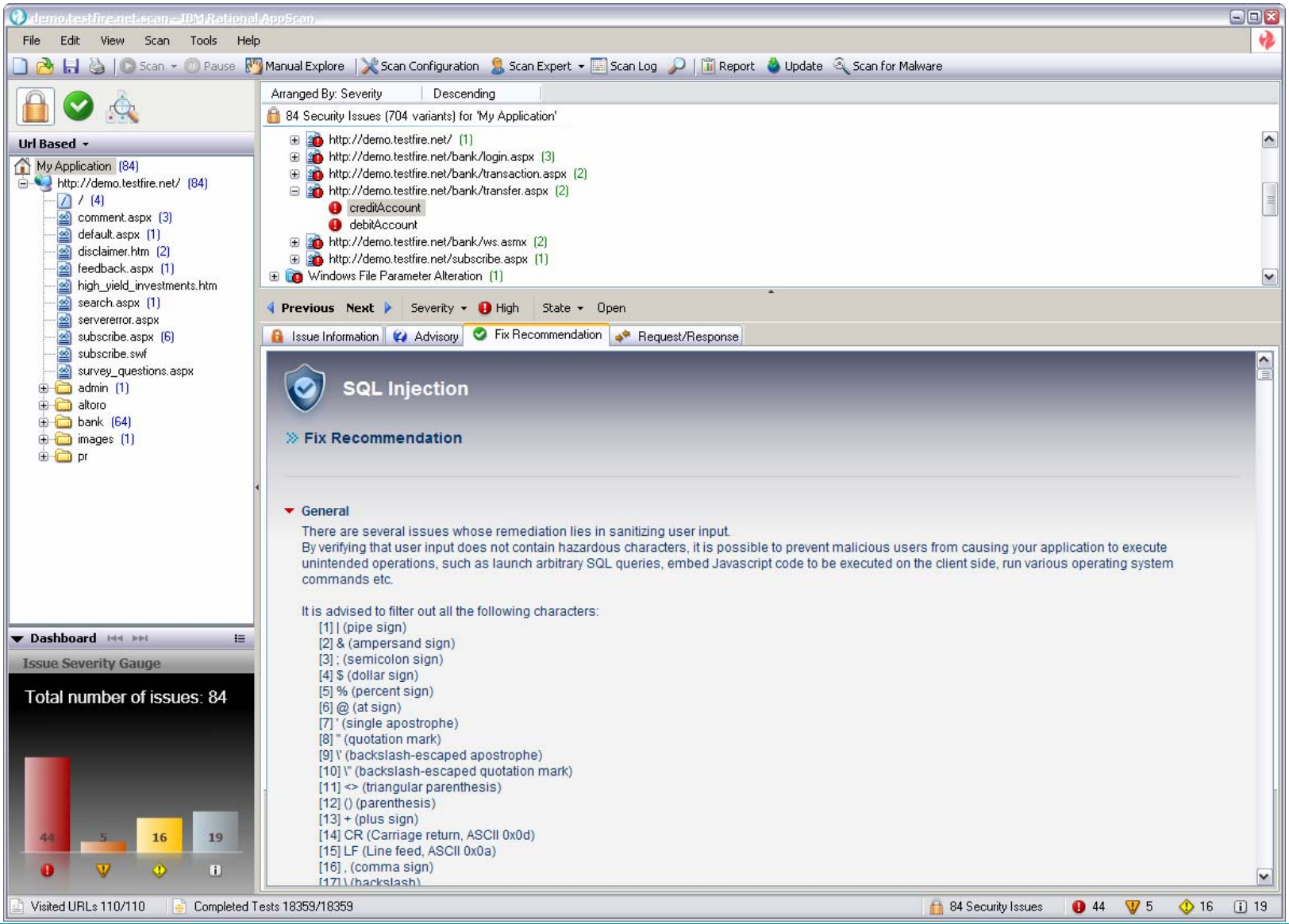
AppScan Standard Edition



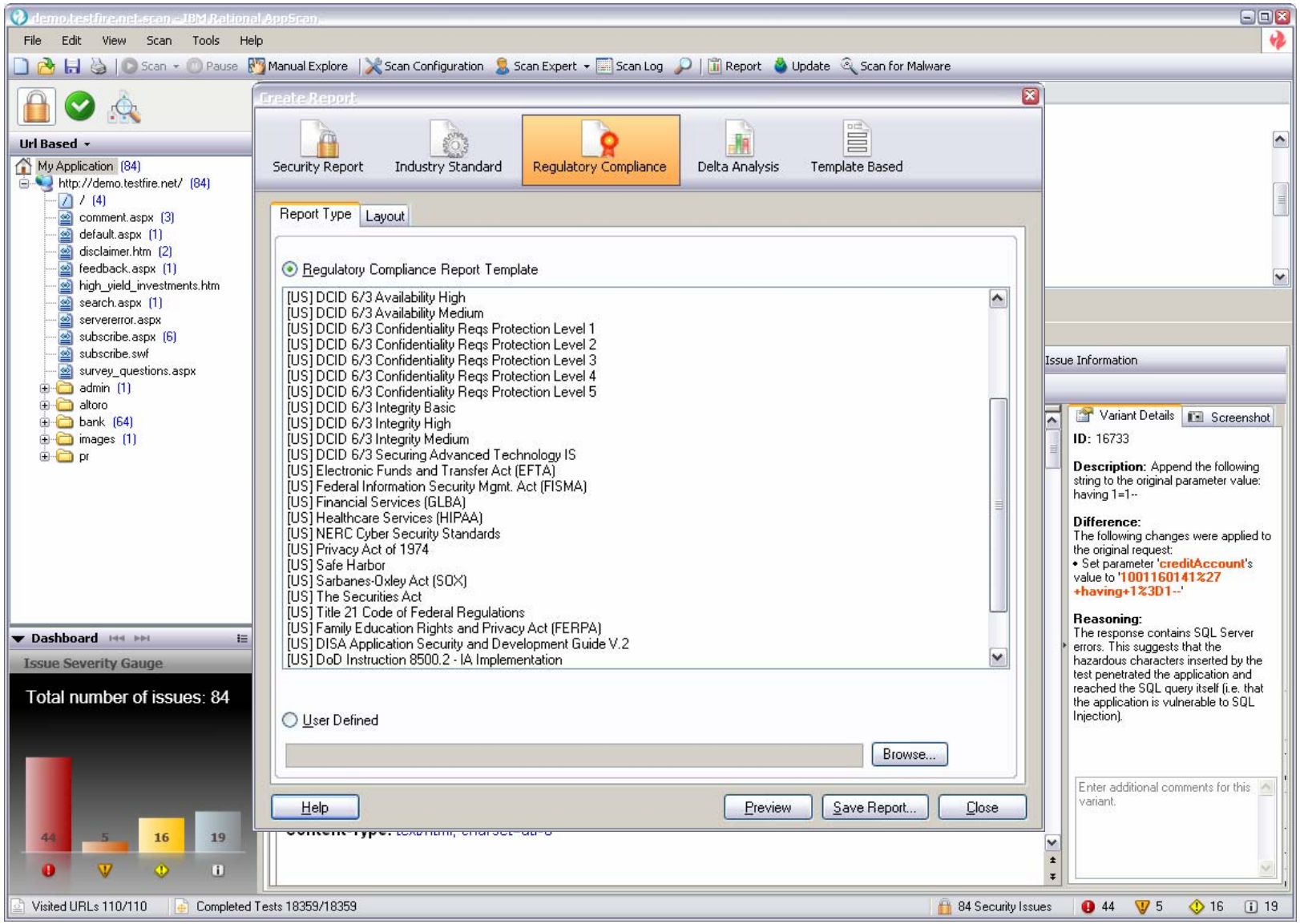
AppScan Standard Edition



AppScan Standard Edition



AppScan Standard Edition

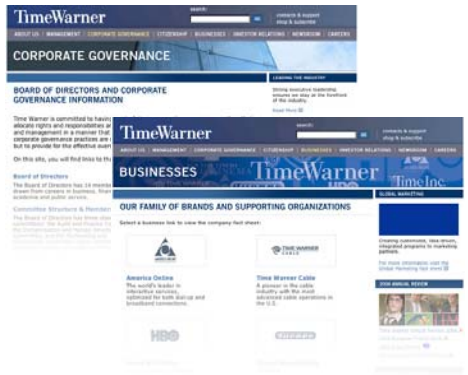


The Power of AppScan Reporting Console

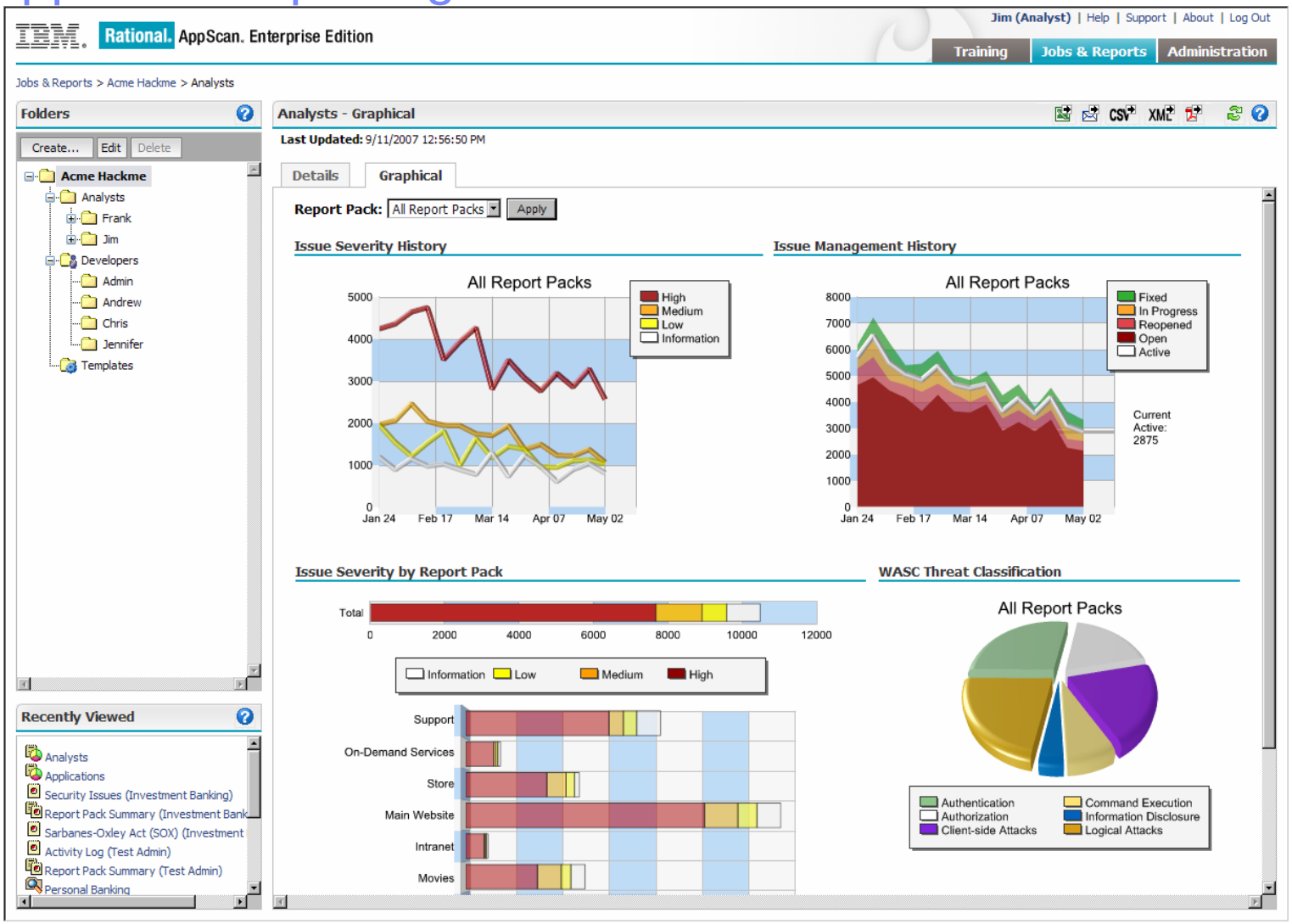
AppScan Reporting Console

VISIBILITY

CONTROL



AppScan Reporting Console – Dashboards and Metrics



Visibility

- Visibility of security issues
  - Sharing data to all stakeholders
  - Security people collaborating with developers to fix security issues
- Control of Who Can Access/Manage Results
  - Provides central control and oversight
- How it works:
  - Customer hosts AppScan Reporting Console
  - Developers provide application information to the security team
  - Security team tests the applications, compiles reports
  - Security team communicates security issues to development, by sending link to report within AppScan Reporting Console or by pushing defects into the defect tracking system
  - Once the issues are fixed, the tests are re-done and issues are managed

Enabling the Operationalization of Security Testing

Clients are addressing Web Application Security in three ways:

1 Outsource Security Testing (SaaS)

- Outsource web application security infrastructure or testing
- Enables immediate identification of sources of online risk without the necessary time and investment for in-house training and resources
- Fastest path to actionable information

Customers receive actionable reports (AppScan OnDemand)

2 Enable Security Specialists

- Requires web application security subject matter expertise
- Single-step security testing (no additional oversight required as expertise is built-in)
- Eliminates training requirements for non-security experts

Security Team uses AppScan Standard Edition & AppScan Reporting Console

3 Embed Security into Development

- Implement environment-specific security testing solution for select stakeholders
- Alleviates security testing bottleneck downstream
- Increases security awareness across the organization (code security improvement, vulnerability awareness)
- Enables a more efficient process for on-time and on-budget application development

Developers use AppScan Enterprise

Control, Monitor, Collaborate and Report Web Application Security Testing

Security in Development: Case Study

An enterprise that has

- Development teams who are aware of the security challenge and would like to fix security issues at an early in the development lifecycle for lower cost
- Developers that:
  - Incorporate security testing as part of the development work.
  - Test their changes to the application before delivering these changes to the source stream
  - Log defects or fix them immediately
- A security team that:
  - Oversees the applications' issues
  - Audit the applications before going to production

The challenge

- Enabling developers who are not security experts to perform security testing
- Enable security team to maintain control and oversight of the security testing

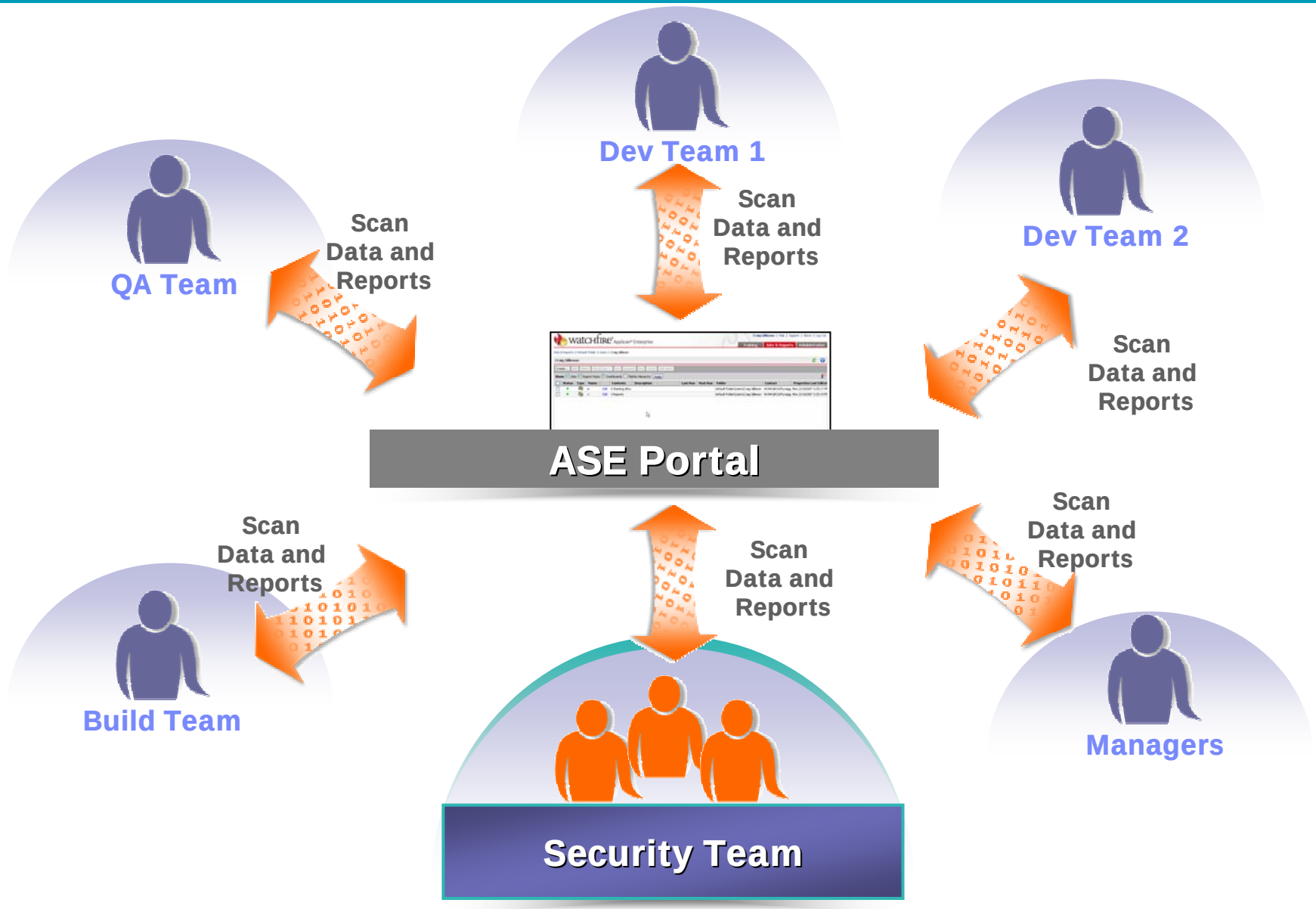
Security In Development: Scalability and Control

- Scalability
  - Scale up to large security scans
  - Scale out to different user communities
    - QuickScan UI enables non-security expert to do security scanning
- Control
  - Provides central control and oversight
  - Security team uses advanced view to see what scans have been done and results
  - Security team collaborates with developers to increase scope of testing

The Power of AppScan Enterprise

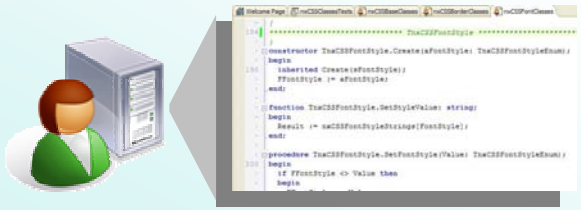
AppScan Enterprise Console

VISIBILITY | **SCALABILITY** | **CONTROL**

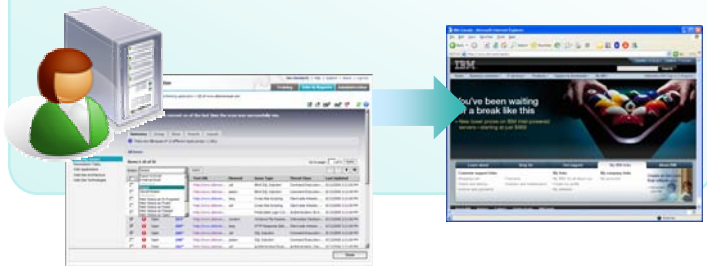

Dev Team 1
Scan
Data and
Reports
QA Team
Scan
Data and
Reports
Dev Team 2
Scan
Data and
Reports
ASE Portal
Scan
Data and
Reports
Scan
Data and
Reports
Scan
Data and
Reports
Build Team
Managers
Security Team

Security In Development: Workflow

1. Developer Writes Code

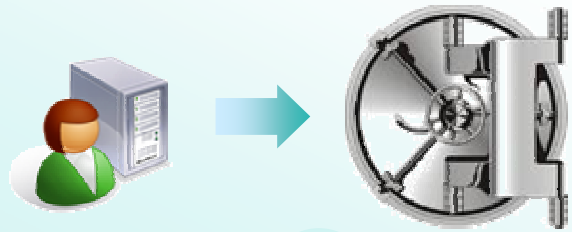


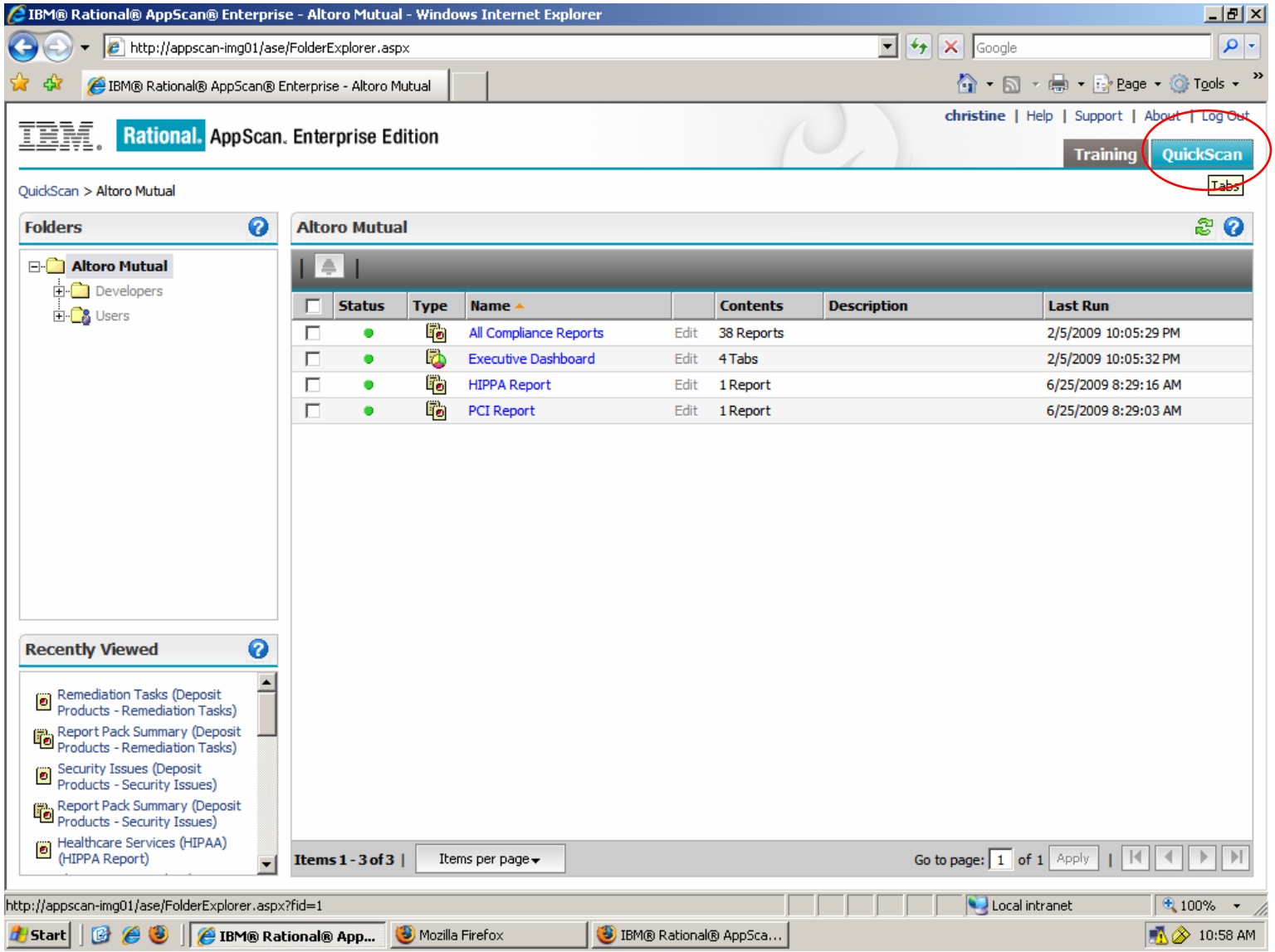
2. Developer compiles code locally to unit test changes using AppScan QuickScan

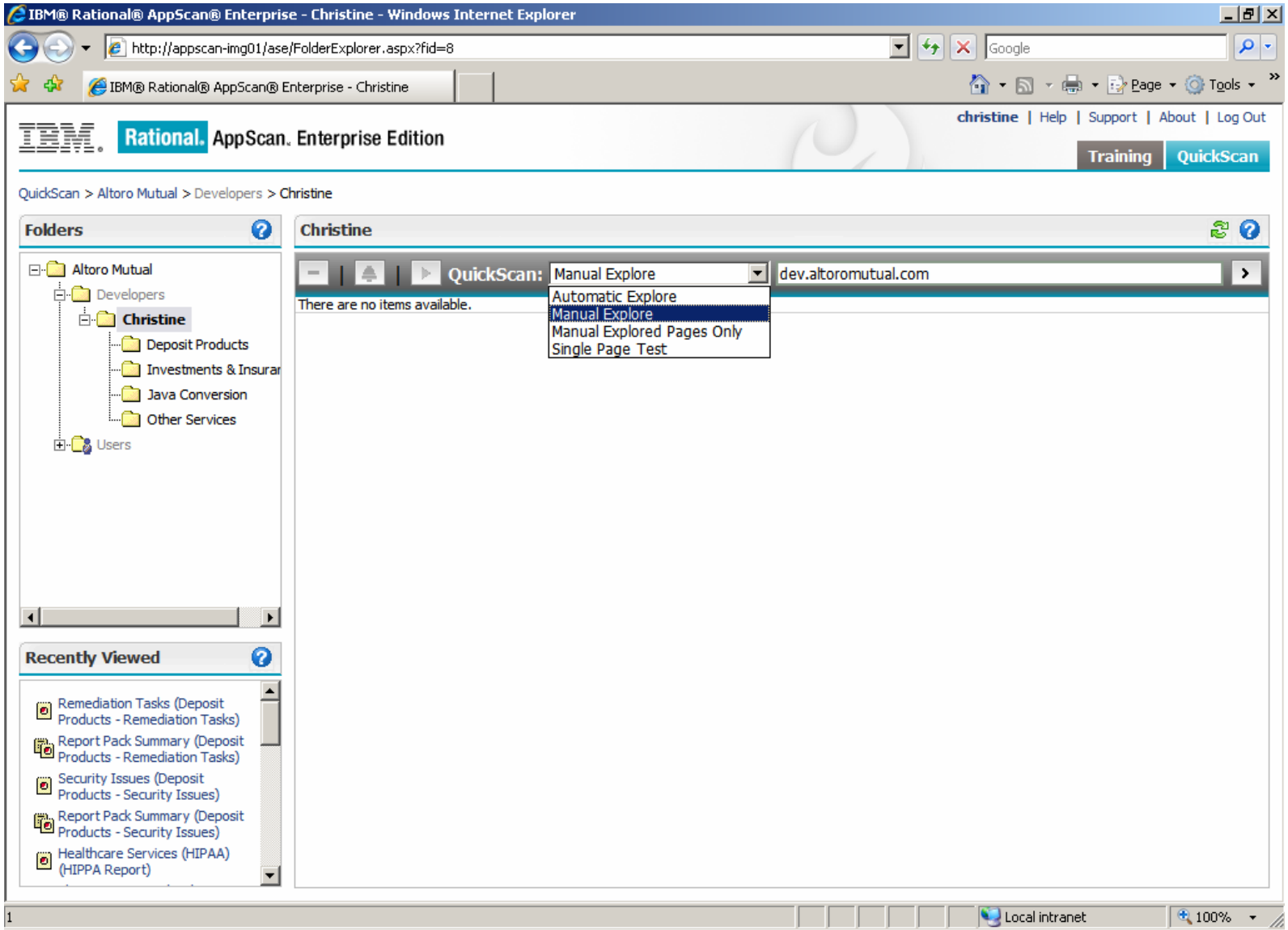


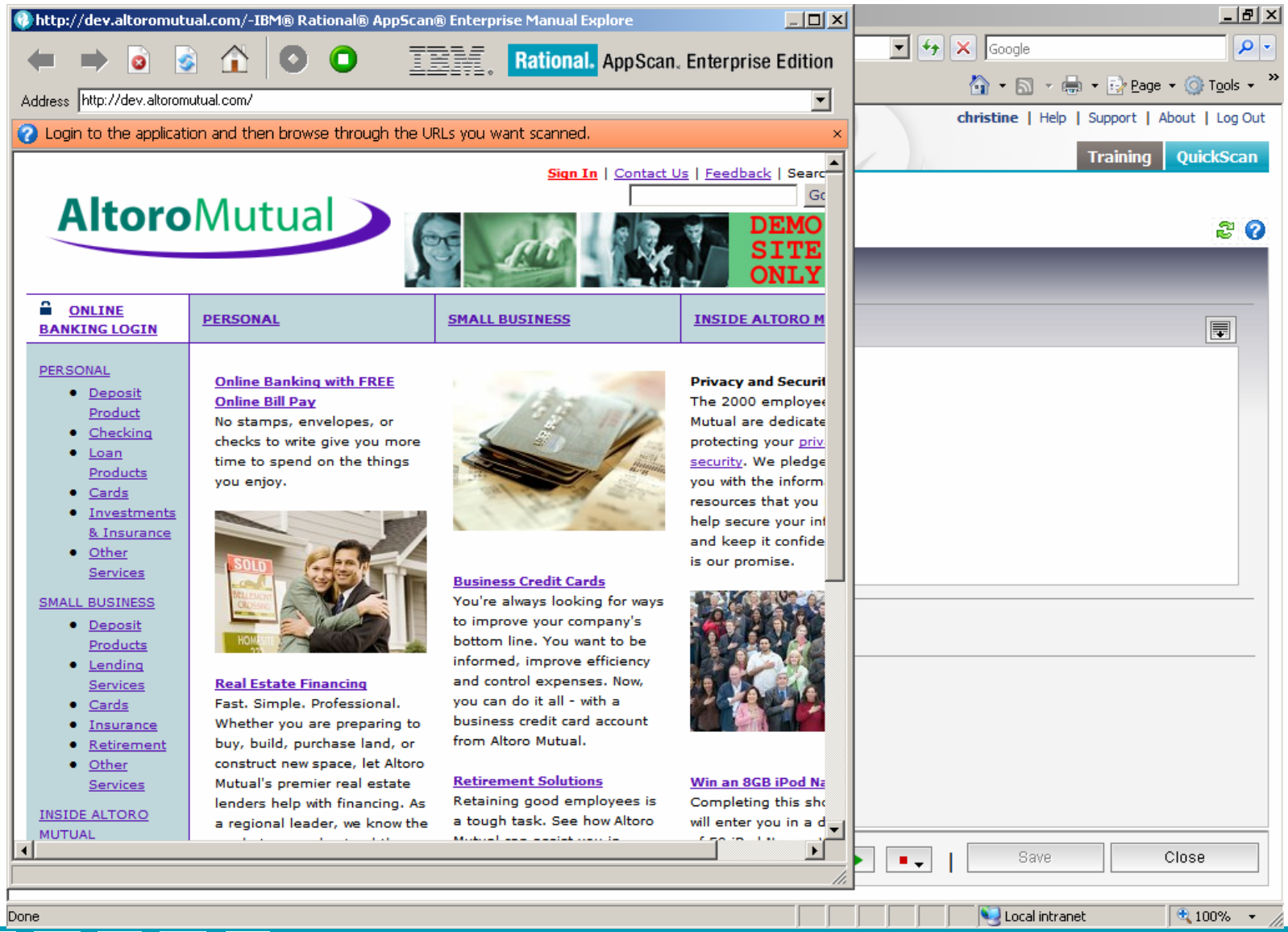
3. Developer Fixes or Logs Issues

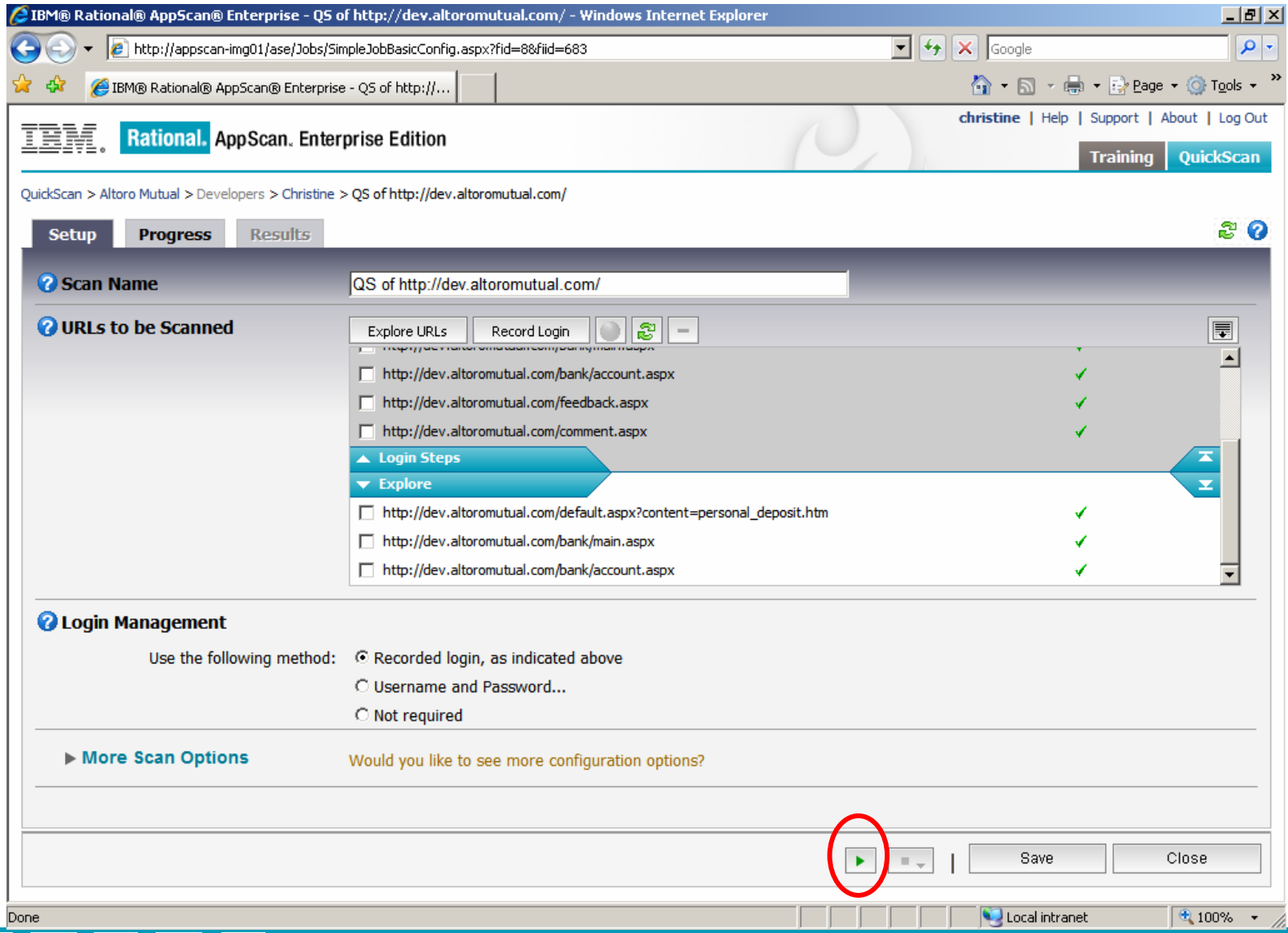
4. Developer Checks in Code

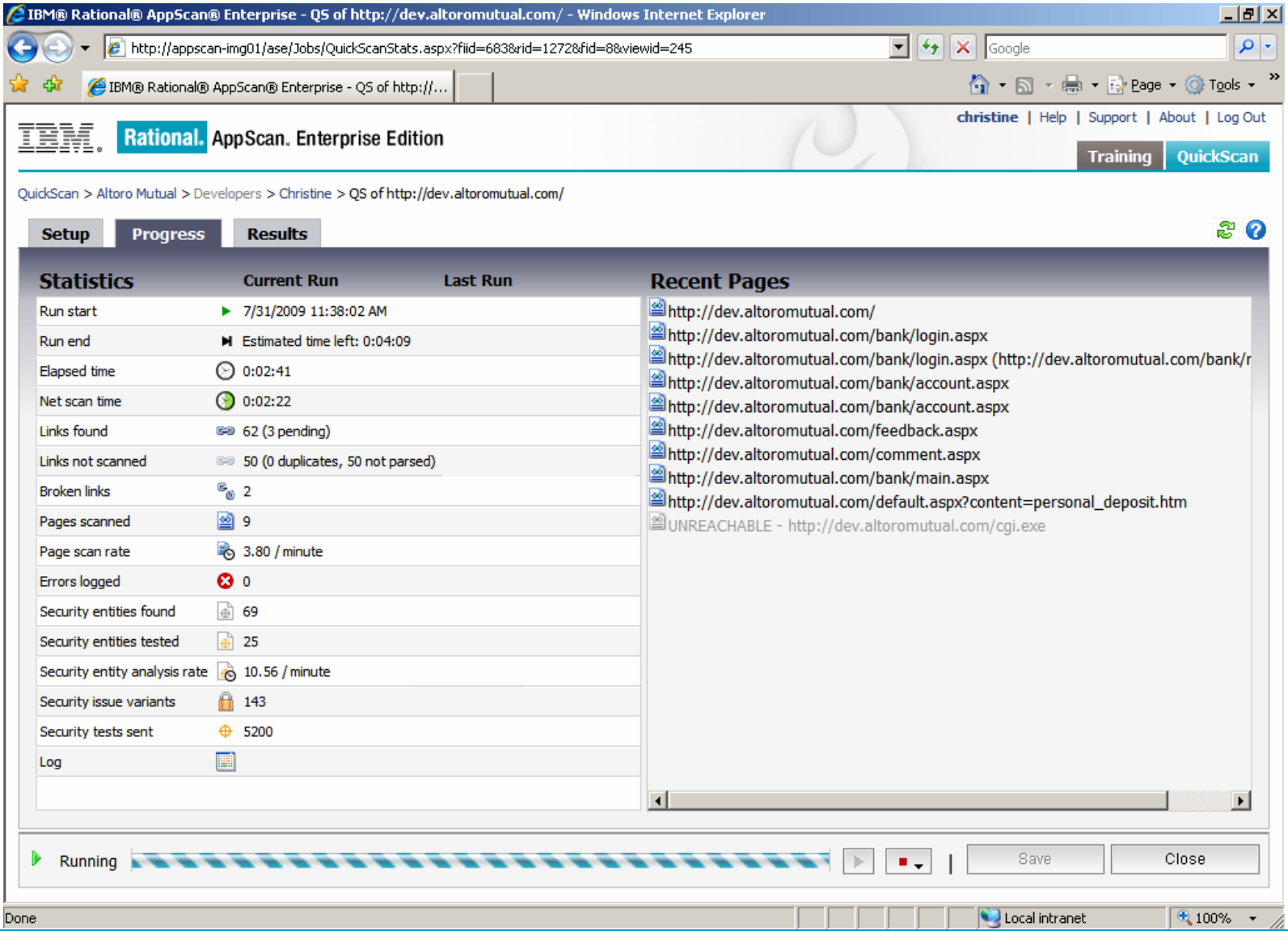


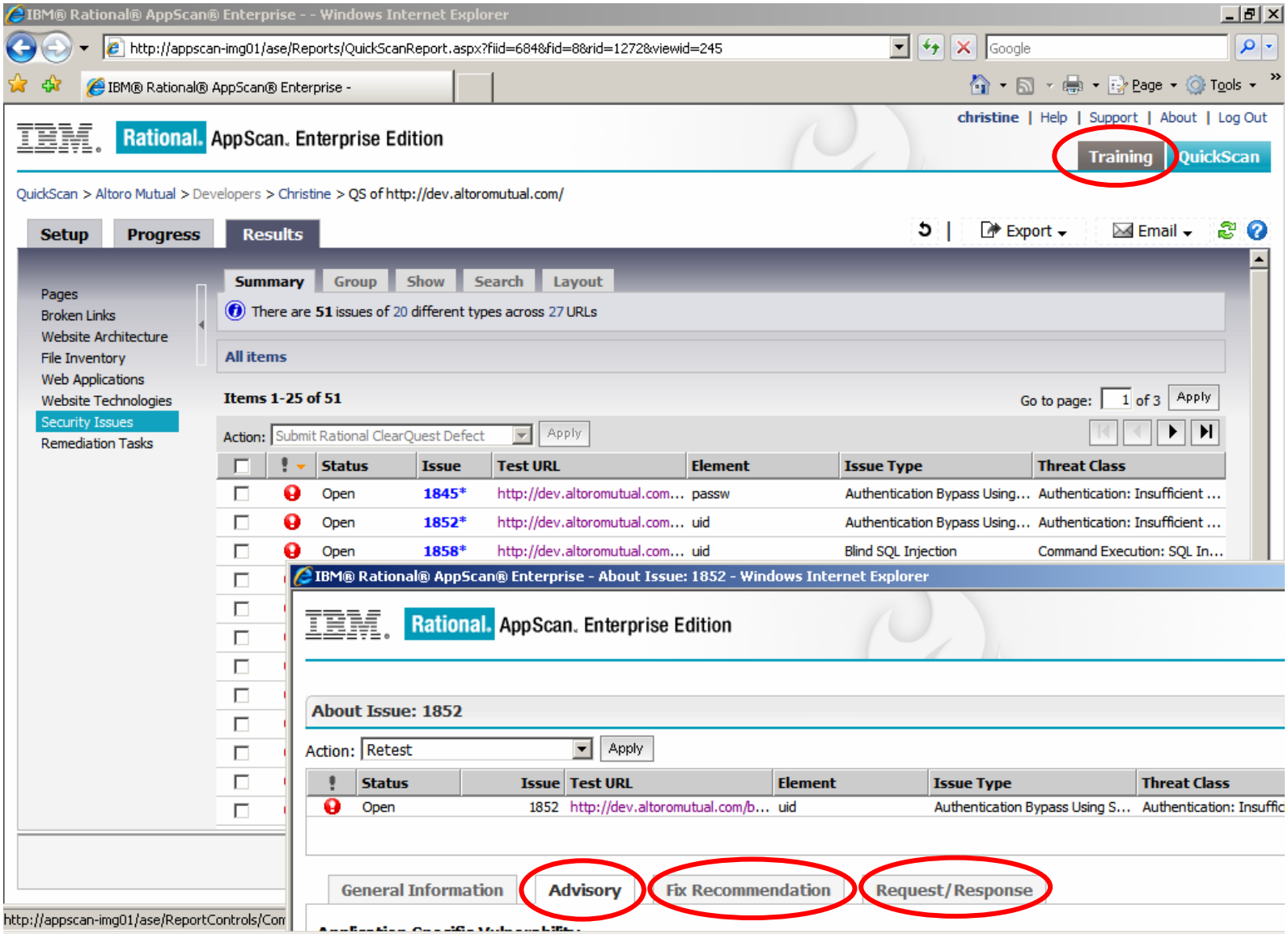

IBM® Rational® AppScan® Enterprise - Altoro Mutual - Windows Internet Explorer
http://appscan-img01/ase/FolderExplorer.aspx
IBM® Rational® AppScan® Enterprise - Altoro Mutual
christine | Help | Support | About | Log Out
Rational. AppScan. Enterprise Edition
Training
QuickScan
Tabs
QuickScan > Altoro Mutual
Folders
Altoro Mutual
Developers
Users
Altoro Mutual
Status
Type
Name
Contents
Description
Last Run
All Compliance Reports
Edit
38 Reports
2/5/2009 10:05:29 PM
Executive Dashboard
4 Tabs
2/5/2009 10:05:32 PM
HIPPA Report
1 Report
6/25/2009 8:29:16 AM
PCI Report
1 Report
6/25/2009 8:29:03 AM
Recently Viewed
Remediation Tasks (Deposit Products - Remediation Tasks)
Report Pack Summary (Deposit Products - Remediation Tasks)
Security Issues (Deposit Products - Security Issues)
Report Pack Summary (Deposit Products - Security Issues)
Healthcare Services (HIPAA) (HIPPA Report)
Items 1 - 3 of 3
Items per page
Go to page: 1 of 1 Apply
http://appscan-img01/ase/FolderExplorer.aspx?fid=1
Local intranet
100%
Start
IBM® Rational® App...
Mozilla Firefox
IBM® Rational® AppSca...
10:58 AM


IBM® Rational® AppScan® Enterprise - Christine - Windows Internet Explorer
http://appscan-img01/ase/FolderExplorer.aspx?fid=8
IBM® Rational® AppScan® Enterprise - Christine
christine | Help | Support | About | Log Out
Rational. AppScan. Enterprise Edition
Training
QuickScan
QuickScan > Altoro Mutual > Developers > Christine
Folders
Altoro Mutual
Developers
Christine
Deposit Products
Investments & Insurar
Java Conversion
Other Services
Users
Christine
QuickScan: Manual Explore
dev.altoromutual.com
There are no items available.
Automatic Explore
Manual Explore
Manual Explored Pages Only
Single Page Test
Recently Viewed
Remediation Tasks (Deposit Products - Remediation Tasks)
Report Pack Summary (Deposit Products - Remediation Tasks)
Security Issues (Deposit Products - Security Issues)
Report Pack Summary (Deposit Products - Security Issues)
Healthcare Services (HIPAA) (HIPPA Report)
Local intranet
100%


http://dev.altoromutual.com/-IBM® Rational® AppScan® Enterprise Manual Explore
Rational. AppScan. Enterprise Edition
Address http://dev.altoromutual.com/
Login to the application and then browse through the URLs you want scanned.
Sign In | Contact Us | Feedback | Search
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO M
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
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro
Privacy and Securit
The 2000 employee
Mutual are dedicate
protecting your priv
security. We pledge
you with the inform
resources that you
help secure your int
and keep it confide
is our promise.
Win an 8GB iPod Na
Completing this sho
will enter you in a d
Google
Page
Tools
christine | Help | Support | About | Log Out
Training
QuickScan
Save
Close
Done
Local intranet
100%


IBM® Rational® AppScan® Enterprise - QS of http://dev.altoromutual.com/ - Windows Internet Explorer
http://appscan-img01/ase/Jobs/SimpleJobBasicConfig.aspx?fid=8&fiid=683
IBM® Rational® AppScan® Enterprise - QS of http://...
christine | Help | Support | About | Log Out
Rational. AppScan. Enterprise Edition
Training
QuickScan
QuickScan > Altoro Mutual > Developers > Christine > QS of http://dev.altoromutual.com/
Setup
Progress
Results
Scan Name
QS of http://dev.altoromutual.com/
URLs to be Scanned
Explore URLs
Record Login
http://dev.altoromutual.com/bank/account.aspx
http://dev.altoromutual.com/feedback.aspx
http://dev.altoromutual.com/comment.aspx
Login Steps
Explore
http://dev.altoromutual.com/default.aspx?content=personal_deposit.htm
http://dev.altoromutual.com/bank/main.aspx
http://dev.altoromutual.com/bank/account.aspx
Login Management
Use the following method:
Recorded login, as indicated above
Username and Password...
Not required
More Scan Options
Would you like to see more configuration options?
Save
Close
Done
Local intranet
100%

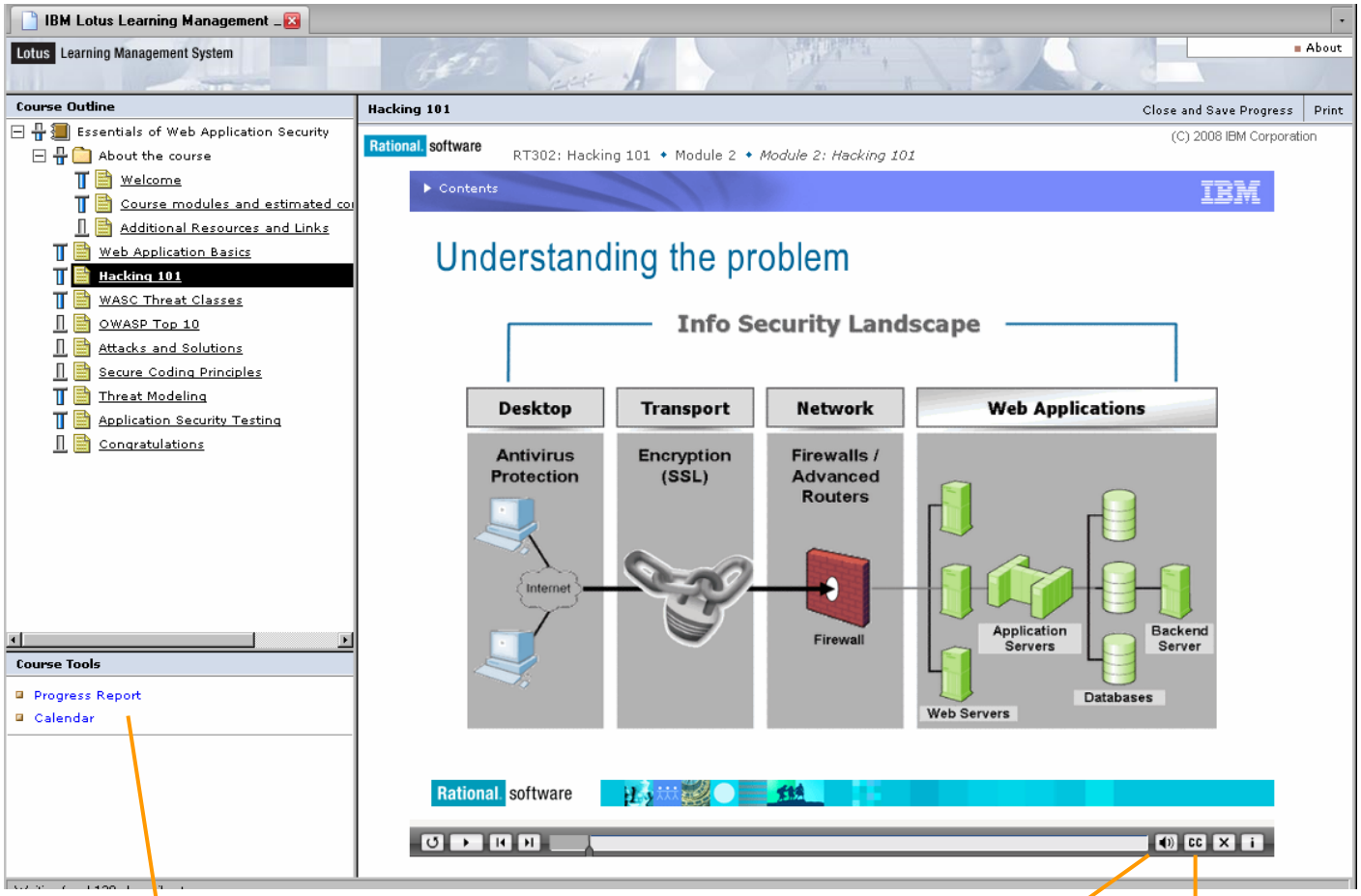

IBM® Rational® AppScan® Enterprise - QS of http://dev.altoromutual.com/ - Windows Internet Explorer
http://appscan-img01/ase/Jobs/QuickScanStats.aspx?fiid=683&rid=1272&fid=8&viewid=245
IBM® Rational® AppScan® Enterprise - QS of http://...
christine | Help | Support | About | Log Out
Rational. AppScan. Enterprise Edition
Training
QuickScan
QuickScan > Altoro Mutual > Developers > Christine > QS of http://dev.altoromutual.com/
Setup
Progress
Results
Statistics
Current Run
Last Run
Run start 7/31/2009 11:38:02 AM
Run end Estimated time left: 0:04:09
Elapsed time 0:02:41
Net scan time 0:02:22
Links found 62 (3 pending)
Links not scanned 50 (0 duplicates, 50 not parsed)
Broken links 2
Pages scanned 9
Page scan rate 3.80 / minute
Errors logged 0
Security entities found 69
Security entities tested 25
Security entity analysis rate 10.56 / minute
Security issue variants 143
Security tests sent 5200
Log
Recent Pages
http://dev.altoromutual.com/
http://dev.altoromutual.com/bank/login.aspx
http://dev.altoromutual.com/bank/login.aspx (http://dev.altoromutual.com/bank/r
http://dev.altoromutual.com/bank/account.aspx
http://dev.altoromutual.com/bank/account.aspx
http://dev.altoromutual.com/feedback.aspx
http://dev.altoromutual.com/comment.aspx
http://dev.altoromutual.com/bank/main.aspx
http://dev.altoromutual.com/default.aspx?content=personal_deposit.htm
UNREACHABLE - http://dev.altoromutual.com/cgi.exe
Running
Save
Close
Done
Local intranet
100%


IBM® Rational® AppScan® Enterprise - - Windows Internet Explorer
http://appscan-img01/ase/Reports/QuickScanReport.aspx?fiid=684&fid=8&rid=1272&viewid=245
IBM® Rational® AppScan® Enterprise -
Rational. AppScan. Enterprise Edition
christine | Help | Support | About | Log Out
Training
QuickScan
QuickScan > Altoro Mutual > Developers > Christine > QS of http://dev.altoromutual.com/
Setup
Progress
Results
Export
Email
Pages
Broken Links
Website Architecture
File Inventory
Web Applications
Website Technologies
Security Issues
Remediation Tasks
Summary
Group
Show
Search
Layout
There are 51 issues of 20 different types across 27 URLs
All items
Items 1-25 of 51
Go to page: 1 of 3 Apply
Action: Submit Rational ClearQuest Defect Apply
Status
Issue
Test URL
Element
Issue Type
Threat Class
Open 1845* http://dev.altoromutual.com... passw Authentication Bypass Using... Authentication: Insufficient ...
Open 1852* http://dev.altoromutual.com... uid Authentication Bypass Using... Authentication: Insufficient ...
Open 1858* http://dev.altoromutual.com... uid Blind SQL Injection Command Execution: SQL In...
IBM® Rational® AppScan® Enterprise - About Issue: 1852 - Windows Internet Explorer
Rational. AppScan. Enterprise Edition
About Issue: 1852
Action: Retest Apply
Status
Issue
Test URL
Element
Issue Type
Threat Class
Open 1852 http://dev.altoromutual.com/b... uid Authentication Bypass Using S... Authentication: Insuffic
General Information
Advisory
Fix Recommendation
Request/Response
http://appscan-img01/ase/ReportControls/Com

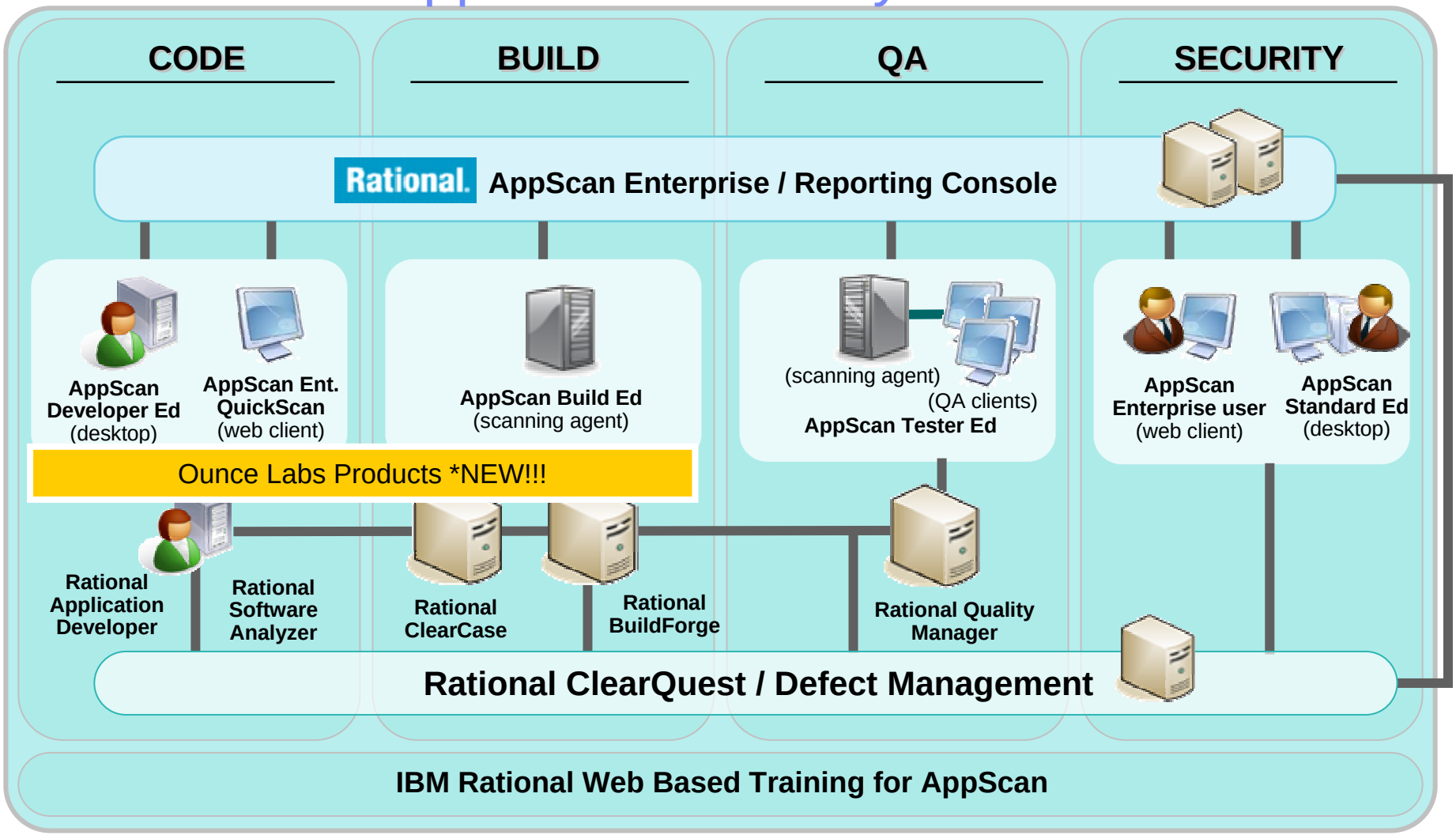
IBM Rational Web-Based Training

Key to adoption across the organization is education

- Informative
- Learn at your own pace
- Self-paced
- Engaging (narrated by experts)
- Accessible
- Localizable
- Compatible with other Learning Management Systems
- Easily embedded into Rational AppScan Enterprise and Policy Tester products



IBM Rational AppScan – Security in the SDLC



Build security testing into the IDE

Automate Security / Compliance testing in the Build Process

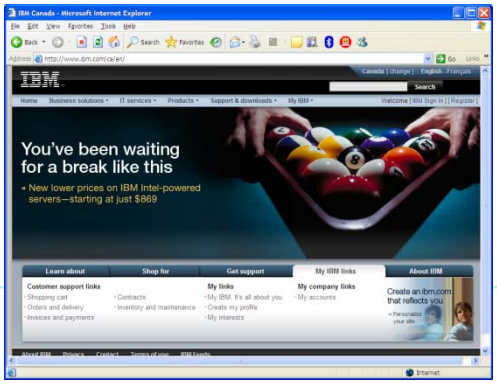
Security / compliance testing incorporated into testing & remediation workflows

Security & Compliance Testing, oversight, control, policy, audits

The Maturing Security Industry – Evolving Analysis Techniques

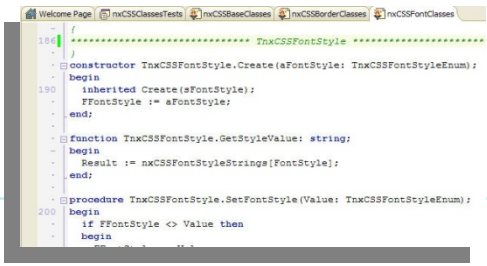
Dynamic Analysis <> Blackbox

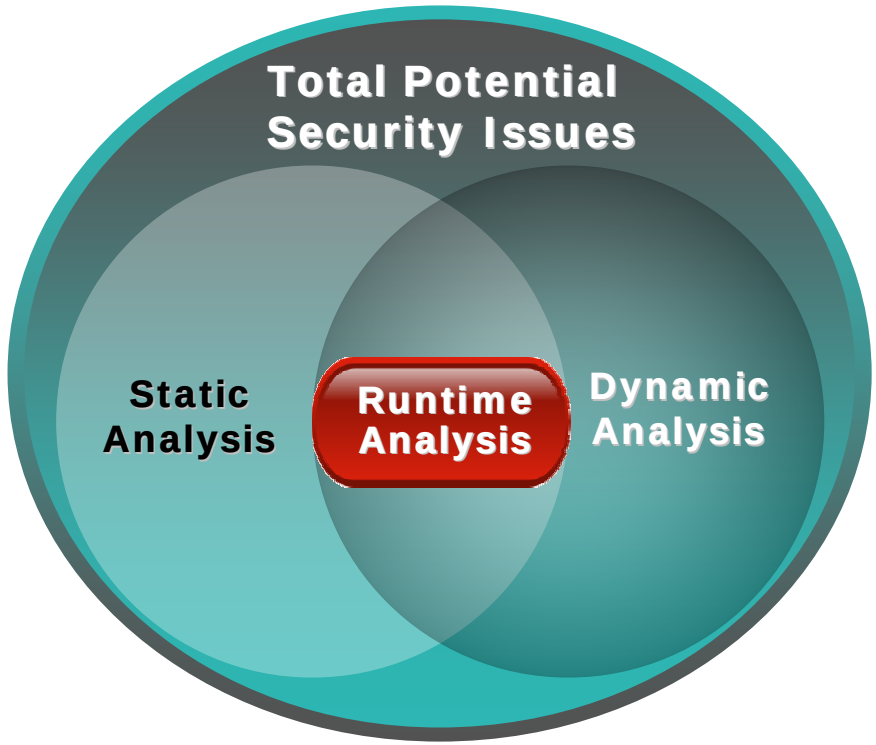
- Sending tests to a functioning application



Static Code Analysis <> Whitebox

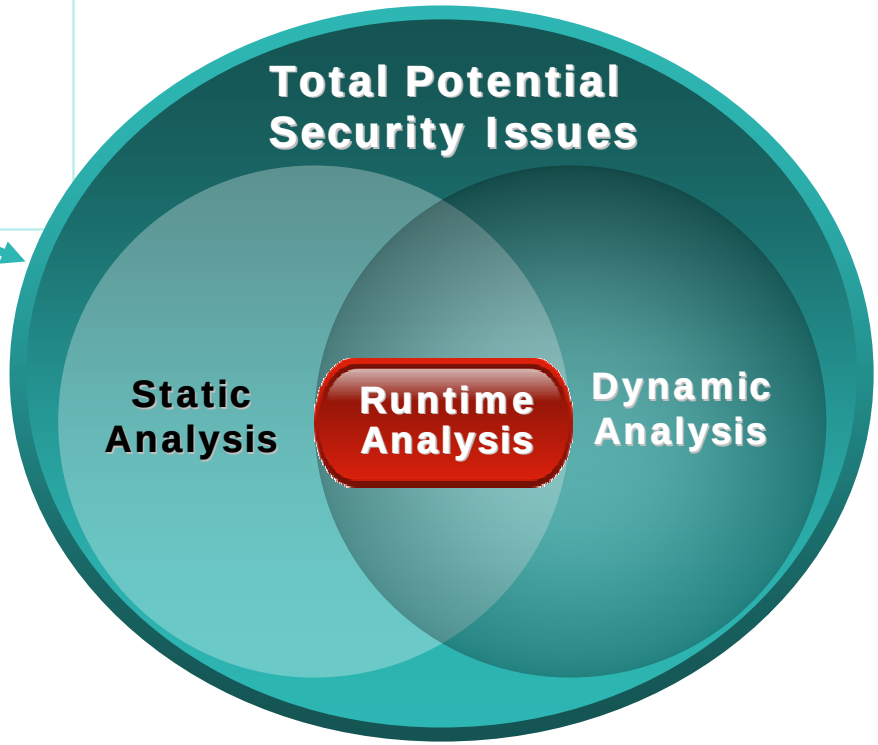
- Looking at the code for issues (code-level scanning)





Rational AppScan Development and Ounce Labs
An end to end security solution

- ***AppScan*** continues to be recognized as the leader in Dynamic Analysis Security Testing (DAST)
- With the addition of ***Ounce Labs*** (a recognized leader in Static Analysis Security Testing), IBM now has an unprecedented end to end security portfolio.



Business Outcome

- **Enable more people** to contribute to security testing coverage with solutions for specific use cases
- Use case offerings **facilitate the adoption of security with minimal disruption** to existing objectives


Questions