Staying Ahead of Cybercrime:
The Importance of Web Application Security

With your real host:
Adrian John Lim
Quality Management

Rational. software

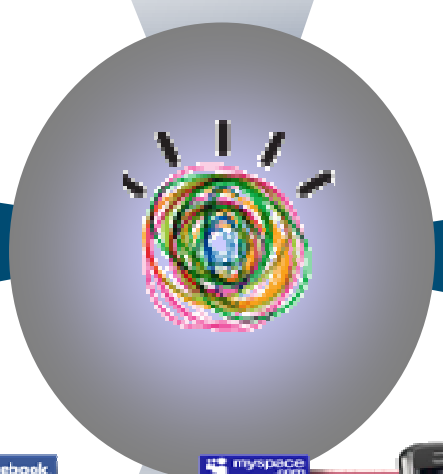
ASC02

Go to IBM

Welcome to the smarter planet

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



Access to streams of information in the Real Time

New Forms of Collaboration

New possibilities.
New complexities.
New risks.

Smarter planet opportunities driven by Web-enabled applications

The Security Equation Has Changed

- How businesses look at security has changed
  - Security is now business driven not technology driven
  - Security is now defined through risk management and compliance disciplines instead of threat and technology disciplines
- The threat landscape has changed
  - Traditional operating system and native client application security risks have become somewhat passé
  - Client threats are now all about the browser environment
  - Server threats are now all about web applications

The Security Landscape of Old

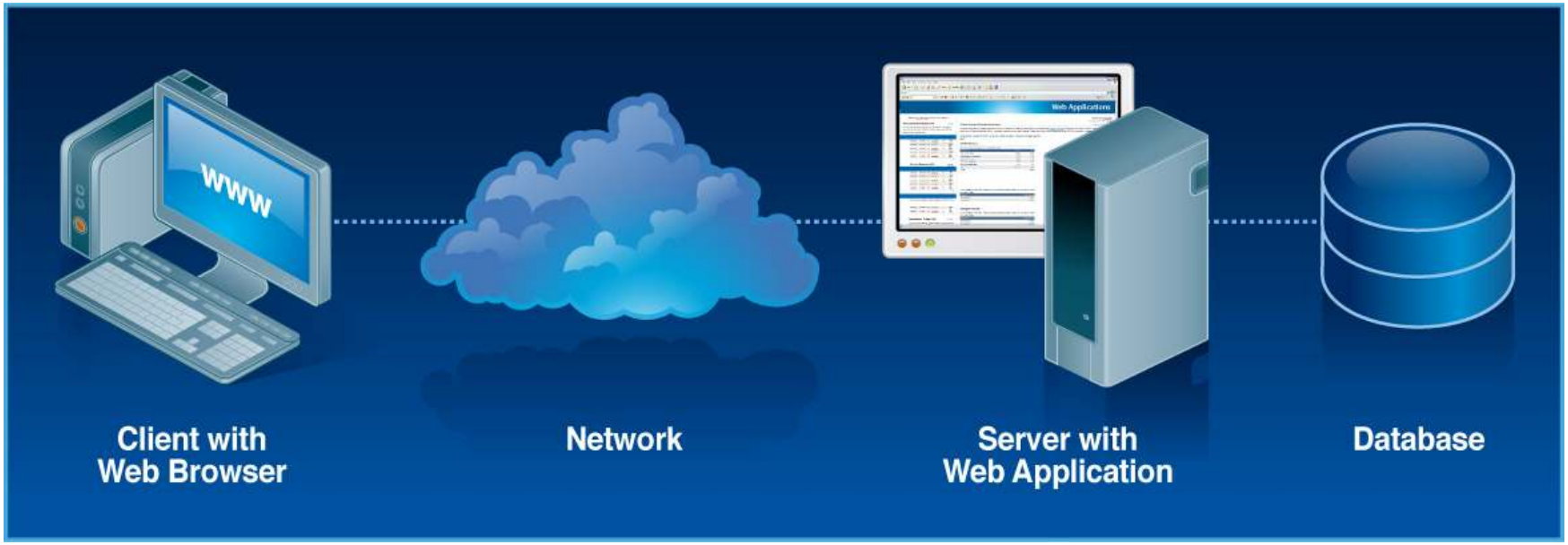
- **Traditional Infrastructure was easier to protect . . .**
- Concrete entities that were easy to understand
- Attack surface and vectors were very well-defined
- Application footprint very static
- Perimeter defense was king

Changing Security Landscape of Today

"Webification" has changed everything ...

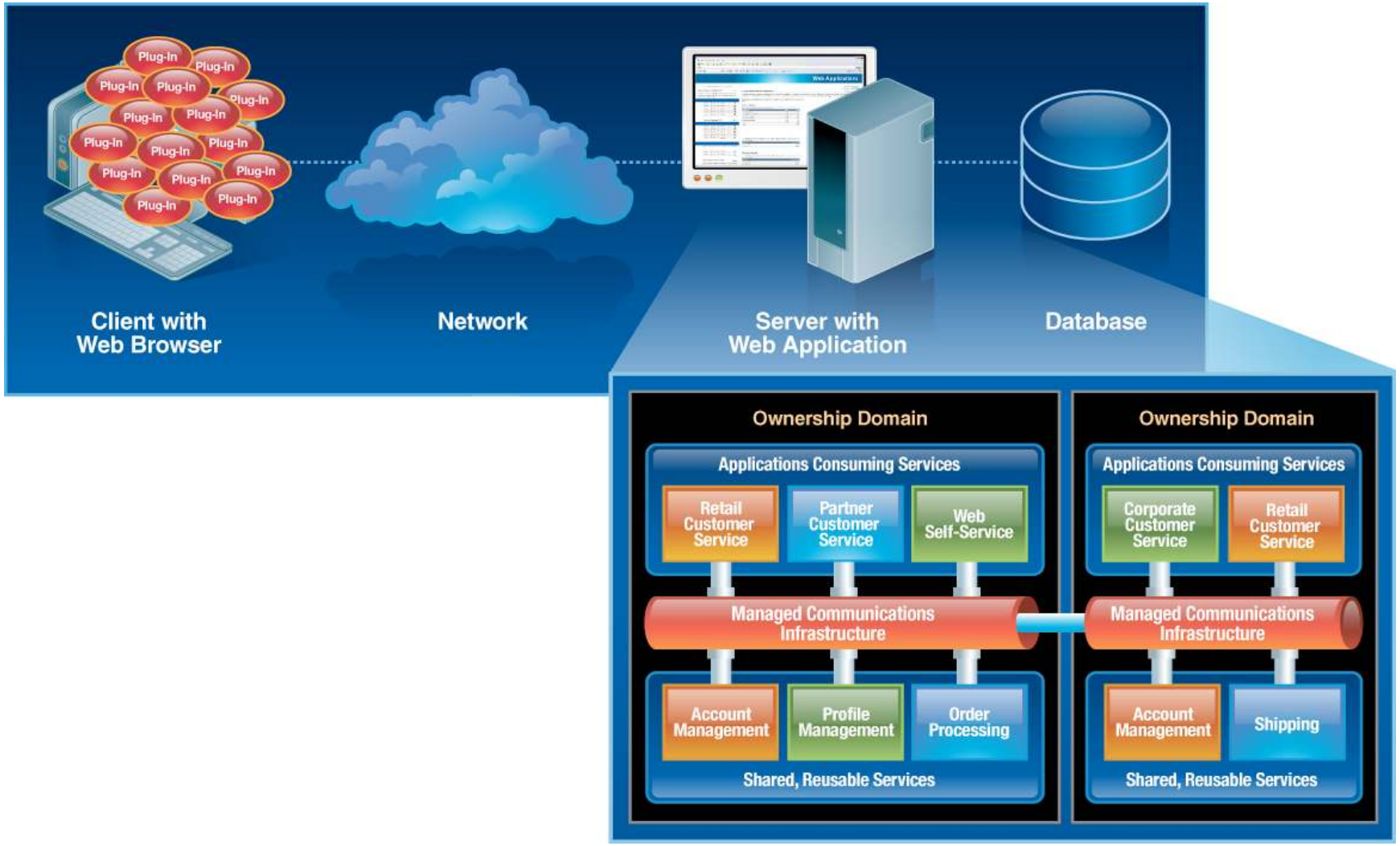
- Infrastructure is more abstract and less defined
- Everything needs a web interface
- Agents and heavy clients are no longer acceptable
- Traditional defenses no longer apply

The Web Ecosystem (simple view)

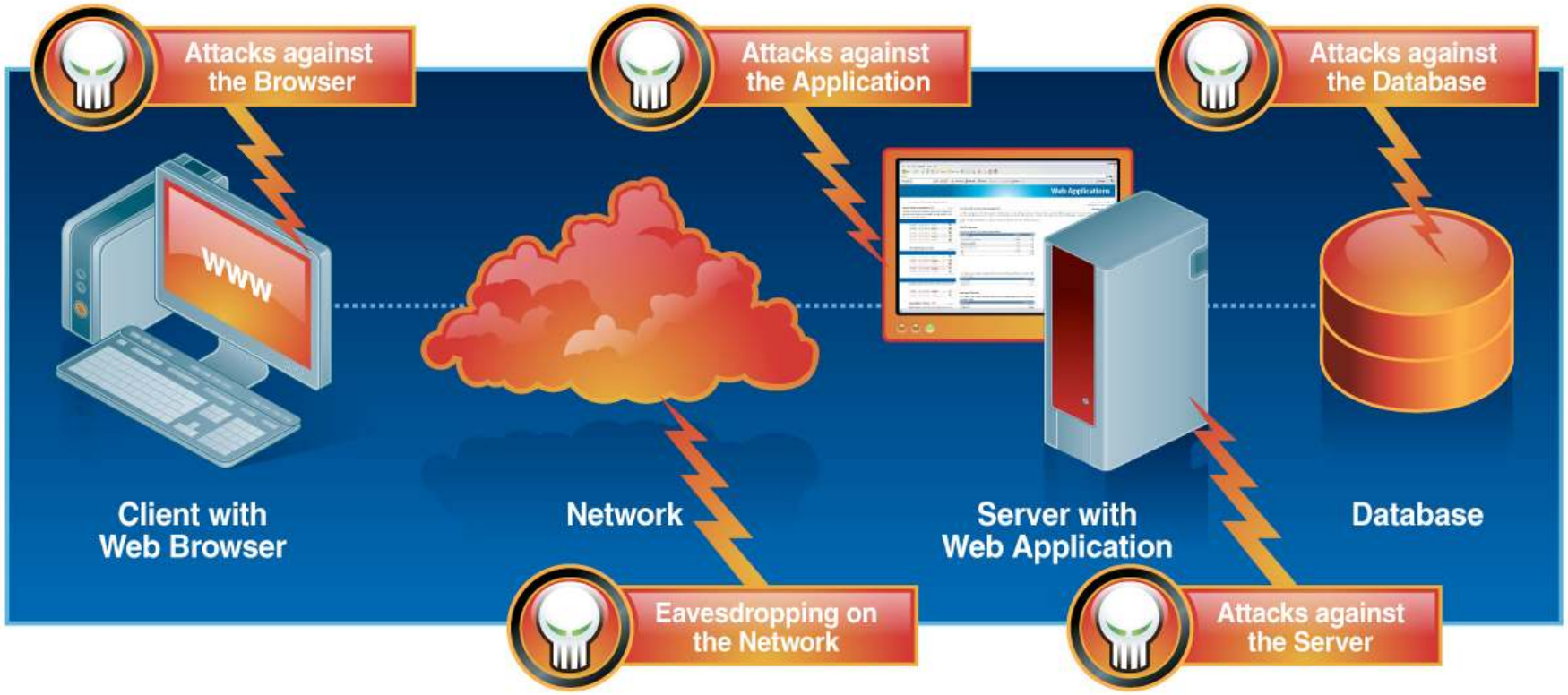


- Client with a web browser renders the content for a user
- Network transports content between the server and the client
- Server with the web application performs the required action
- Database stores information

The Web Ecosystem (complex view)



Attack Vectors



2008 Web Threats Take Center Stage

- Web application vulnerabilities
  - Represent largest category in vuln disclosures (55% in 2008)
  - 74% of Web application vulnerabilities disclosed in 2008 have no patch to fix them

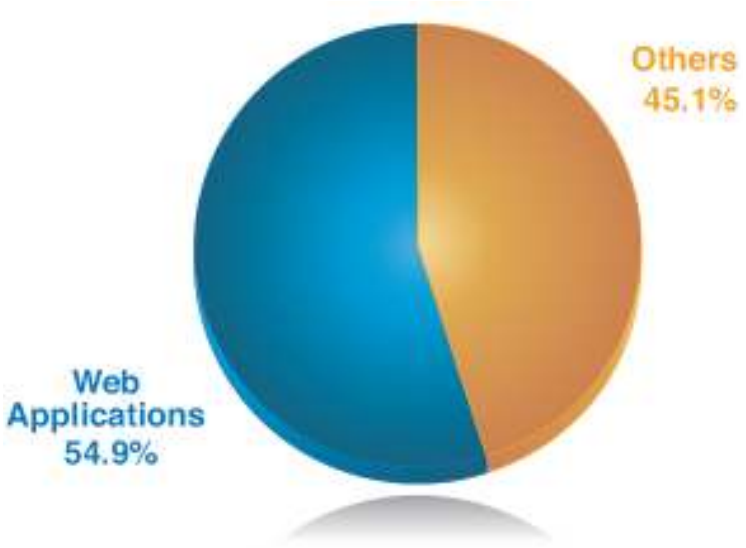


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

Attack Techniques are Plentiful and Trivial

- SQL injection and cross-site scripting are the two largest categories of Web application vulnerabilities
- SQL injection is fastest growing category (up 134% in 2008)

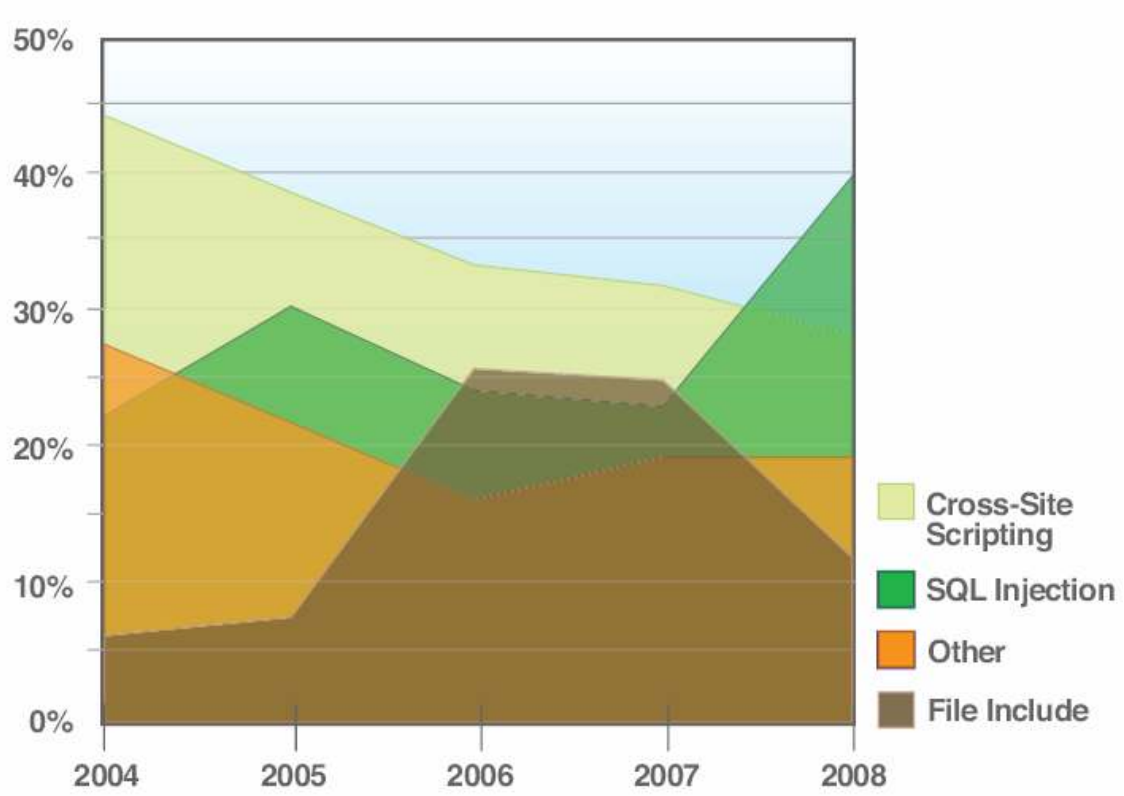


Figure 19: Web Application Vulnerabilities by Attack Technique, 2004 – 2008

Exploitation is Rampant

- Exploitation of SQL injection skyrocketed in 2008
  - Increased by 30x from the midyear to the end of 2008

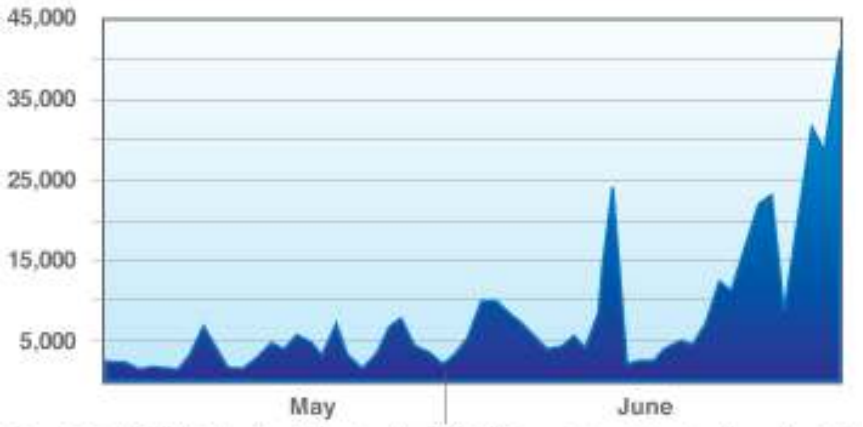


Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

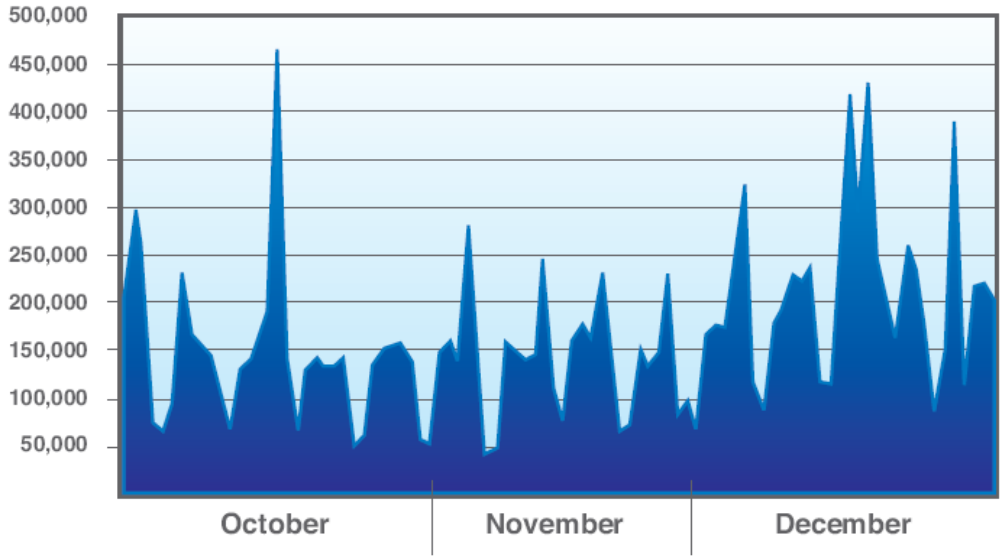
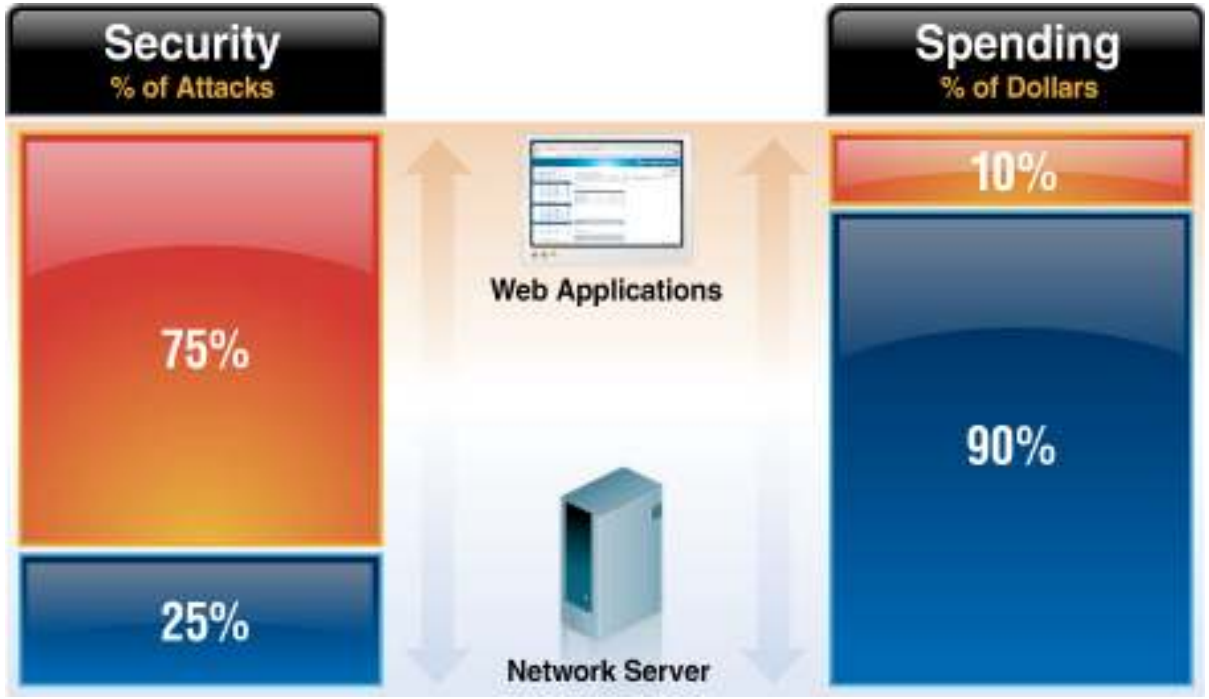


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Reality: Security and Spending Are Unbalanced



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

2/3 **of All Web Applications are Vulnerable** ***Gartner**

The Conundrum

- How security professionals and businesses prioritize risk and threats haven't changed with the overall landscape
- Businesses and professionals still tend to prioritize risk against an outdated traditional infrastructure viewpoint
- Businesses and professionals still tend to implement security solutions that focus on traditional threats and vectors
- Big blind spots
  - Browsers and web applications are still largely ignored or prioritized below other infrastructure from a security perspective

Web Threats Will Become Increasingly Complex

- Web becoming main application delivery interface and ecosystem
- Popularization of new web technologies (Web 2.0) growing attack surface
- New techniques and scenarios for targeting web infrastructure

Web Protection Does Not Have To Be …

1. Cross-Site Scripting (XSS)

- What is it?
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context
- What are the implications?
  - Steal your cookies for the domain you're browsing
  - Completely modify the content of any page you see on this domain
  - Track every action you do in that browser from now on
  - Redirect you to a Phishing site
  - Exploit browser vulnerabilities to take over machine

2. Injection Flaws

- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.
- Many kinds of injection flaws
  - LDAP, XPath, SSI, MX (Mail)…
  - HTML Injection (Cross Site Scripting)
  - HTTP Injection (HTTP Response Splitting)
- What are the implications?
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands / access sensitive data
  - LDAP Injection – Bypass authentication

The Strategy

- **Reduce Cost and Time to Market**
  - **Find the issues earlier in the SDLC**
  - **Automate the process**
  - **Use less security savvy employees by leveraging tools**
- **Mitigate Risk and increase quality**
  - **Increase coverage**
  - **Involve more people in the process: Developers / QA**
- **Increase Visibility**
  - **Distribute reports to different levels**
  - **Dashboards**
- **Increase Productivity**
  - **Build the knowledge**
  - **Prevent of doing the same mistake**

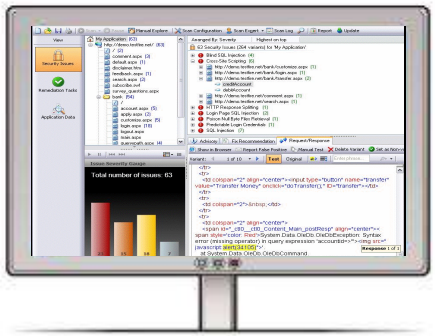
How does Application Security Testing work?

1

Explore source code and/or web site to detect structure

2

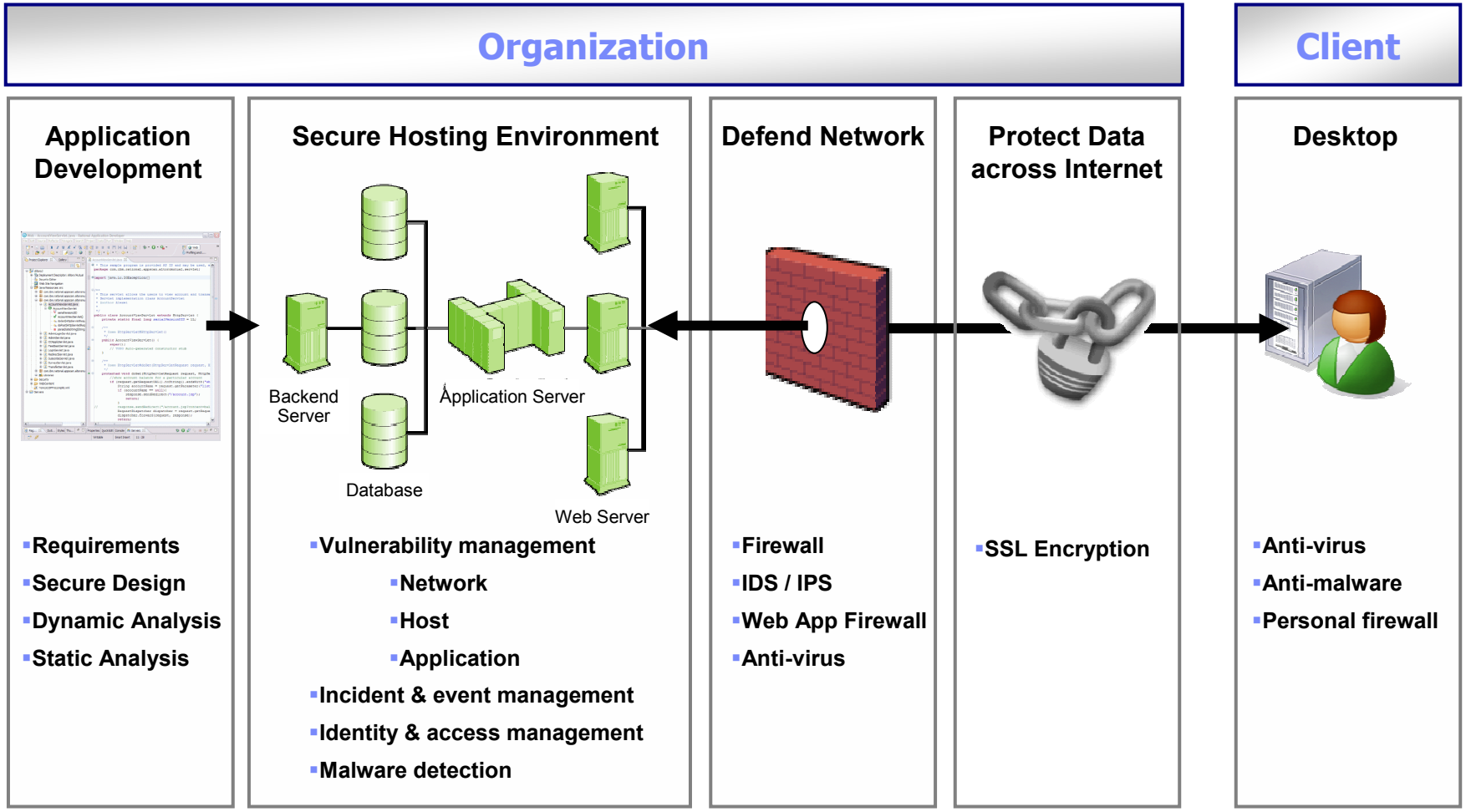
Identify Vulnerabilities ranked after severity and show how it was identified



3

Advanced remediation, fix recommendations and security enablement

Secure Web Applications: Who is responsible?

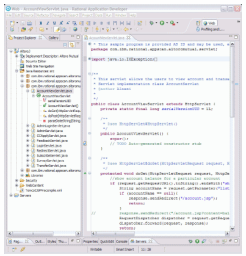


Secure Application Development

- Challenge
  - Ensure the creation of high quality, secure and compliant software
  - Ensure effective management of secure requirements, design and testing
  - Lifecycle management of vulnerabilities
  - Application Lifecycle Management (ALM)
- IBM Solutions
  - IBM Rational AppScan
    - Dynamic Analysis
    - Static Analysis
    - Runtime Analysis

Rational. AppScan.

Application Development

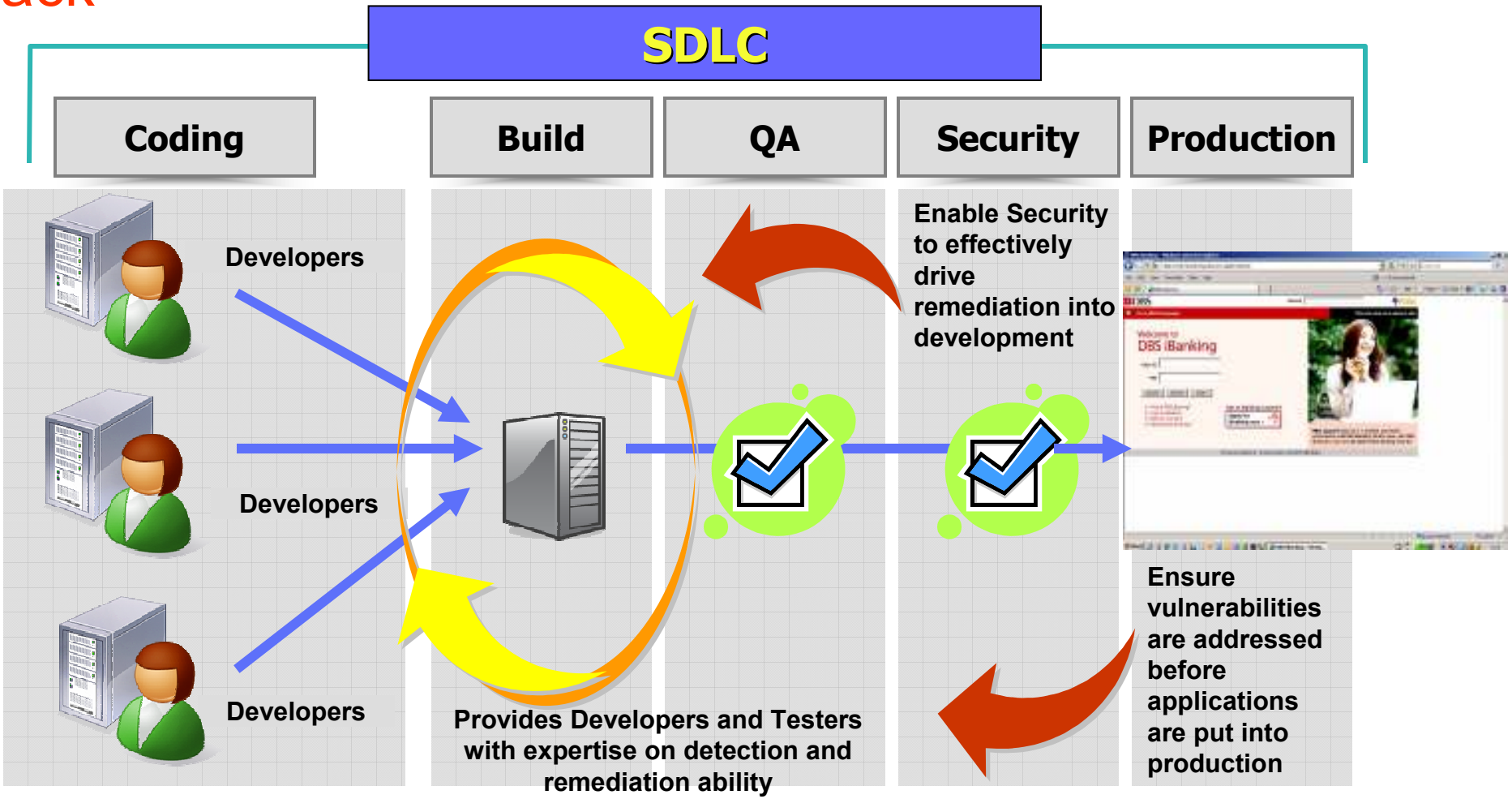


- **Requirements**
- **Secure Design**
- **Dynamic Analysis**
- **Static Analysis**

Required Technologies for Securing the SDLC

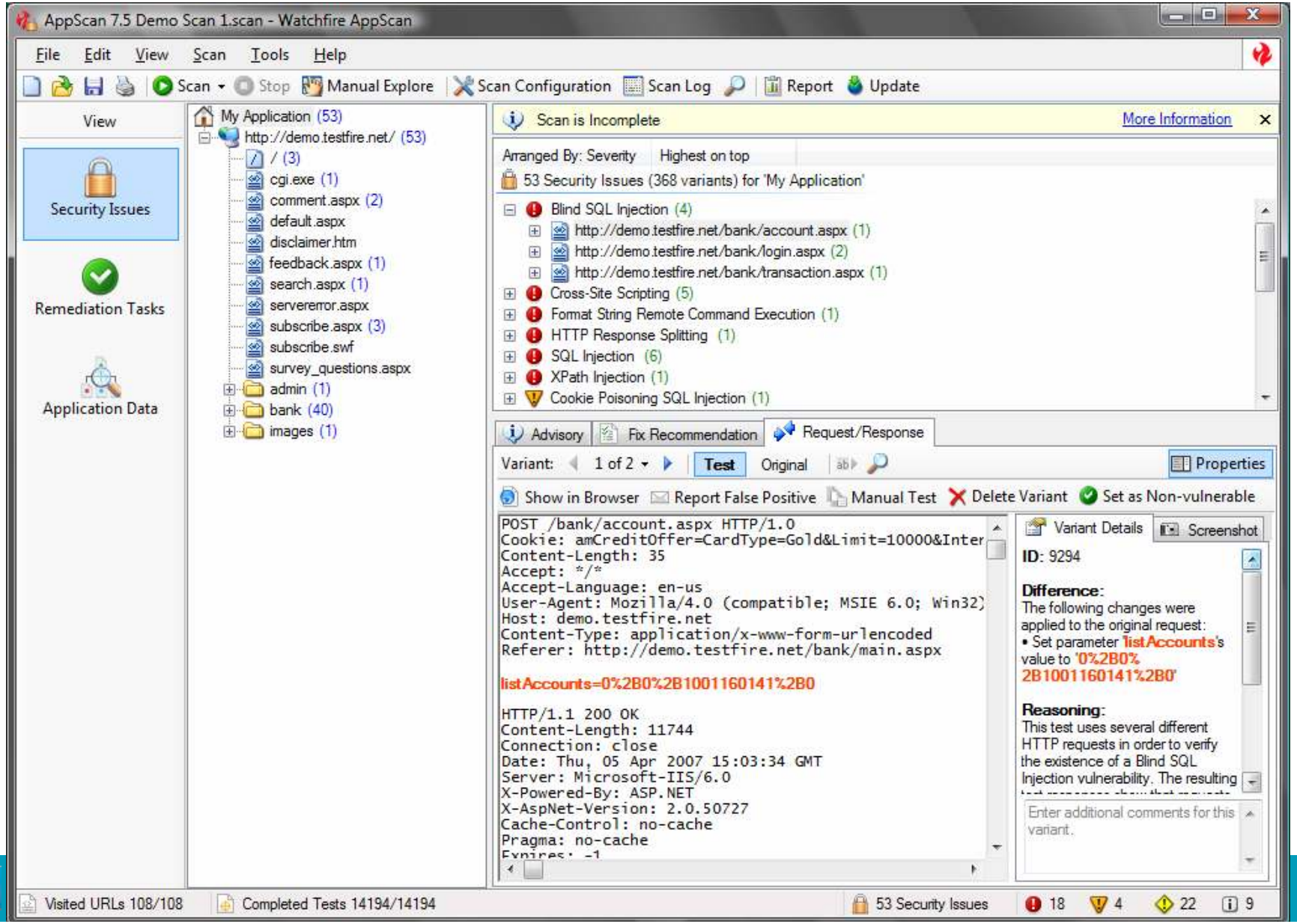
- Tier 1: Source Control & Change Request Management
  - Rational ClearQuest / Change
  - Rational ClearCase / Synergy
- Tier 2: Requirements & Test Management
  - Rational RequisitePro / Doors
  - Rational AppScan
  - Rational Quality Manager
- Tier 3: Build Management
  - Rational Build Forge
- Tier 4: Architectural & Asset Management
  - Rational Asset Manager
  - Rational Software Architect

Building security & compliance into the SDLC – further back



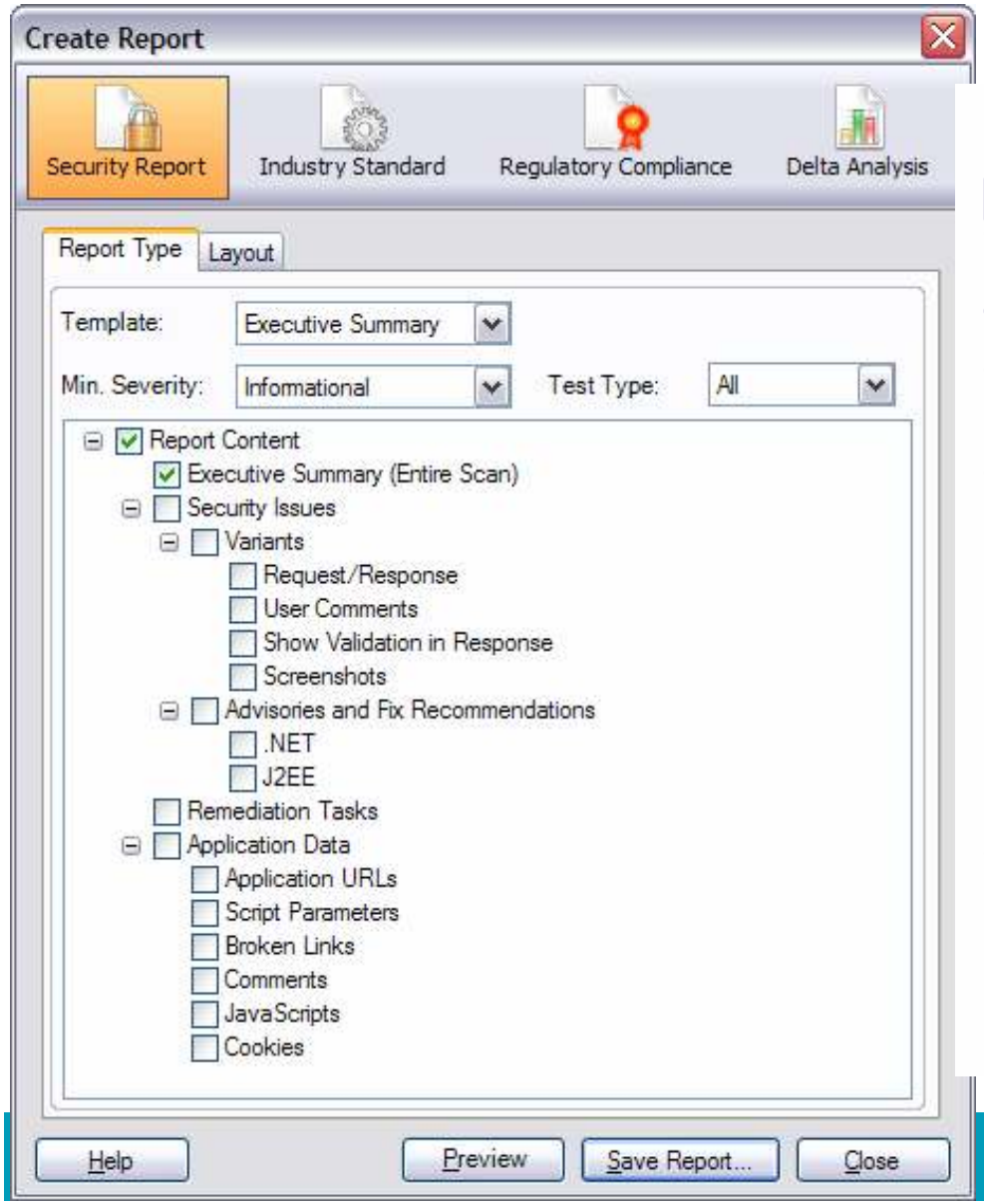
You need a professional solution to

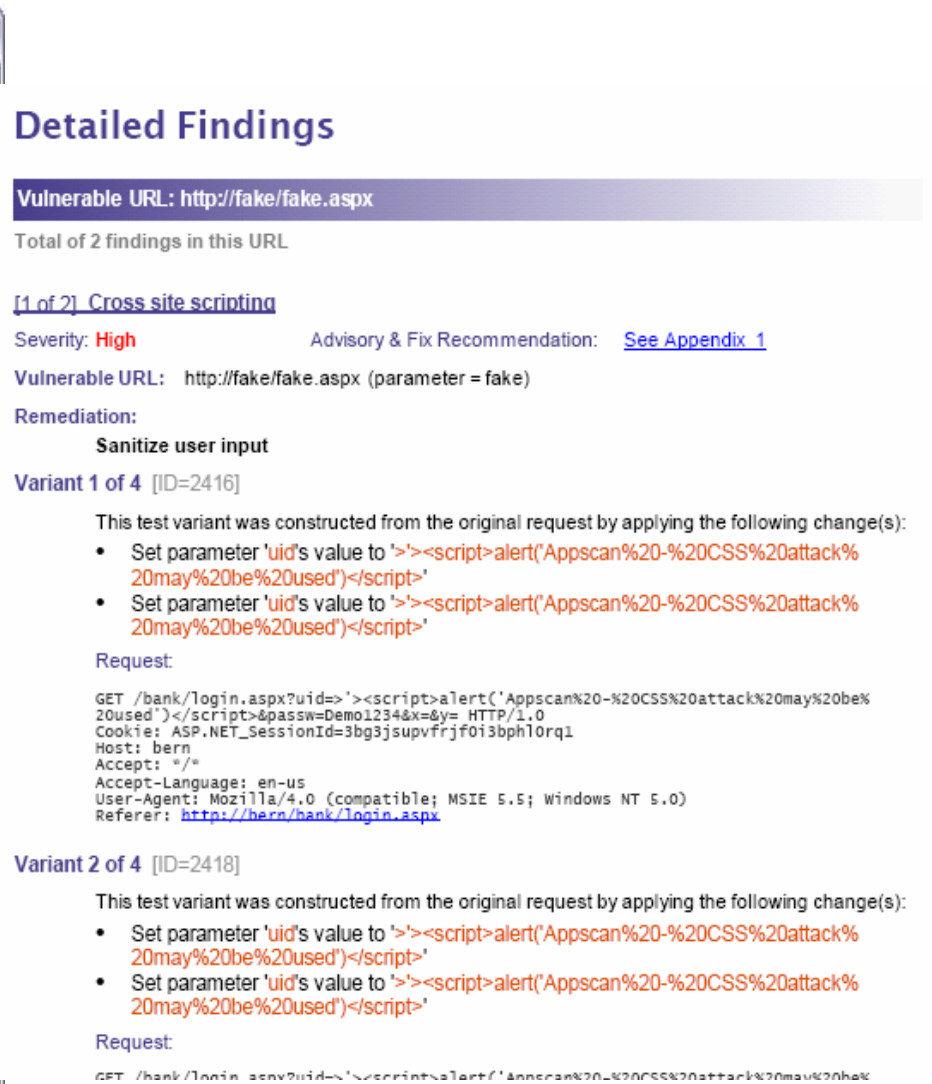
Identify Vulnerabilities



With Rich Report Options

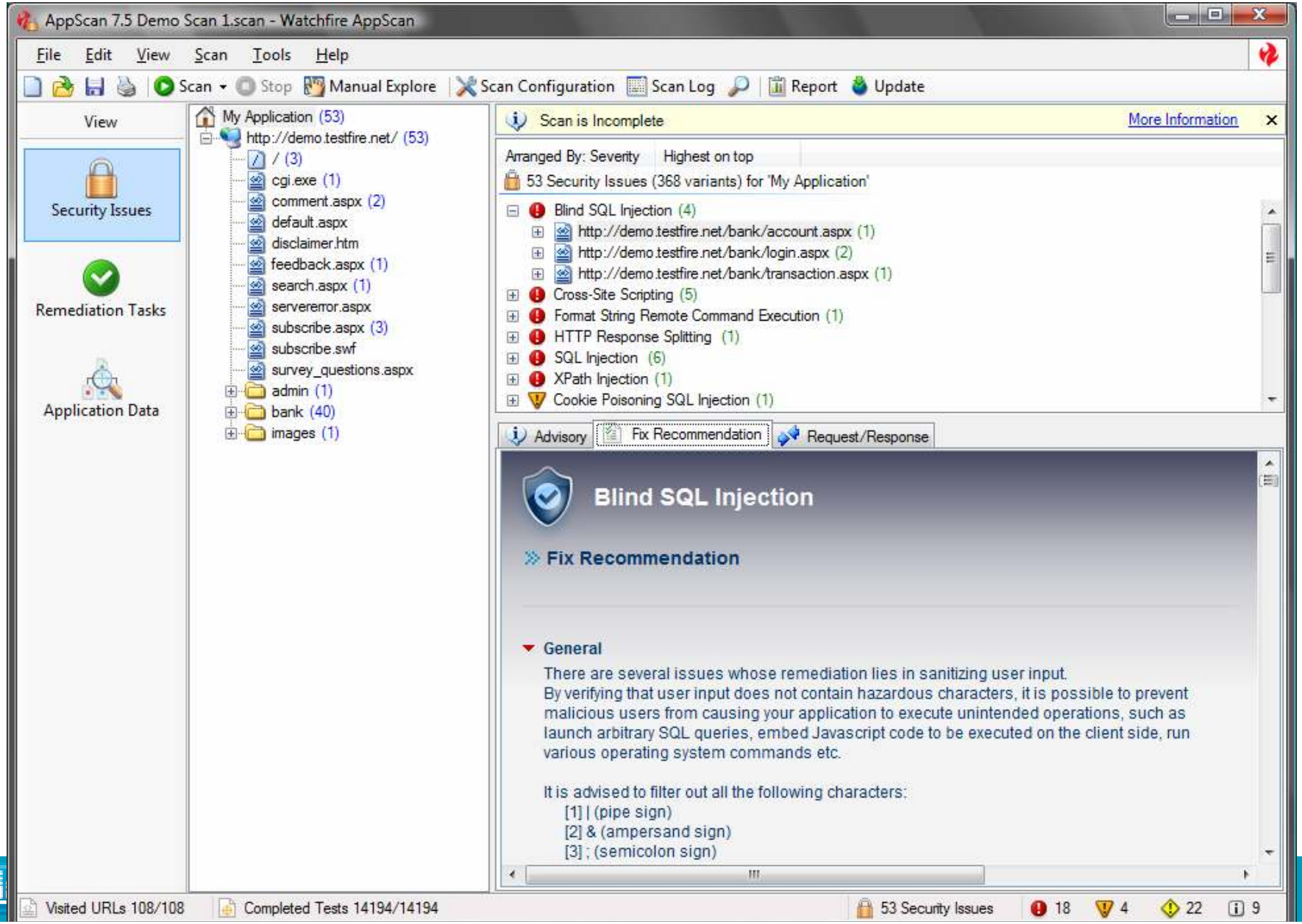
44 Regulatory Compliance Standards, for Executive, Security, Developers.



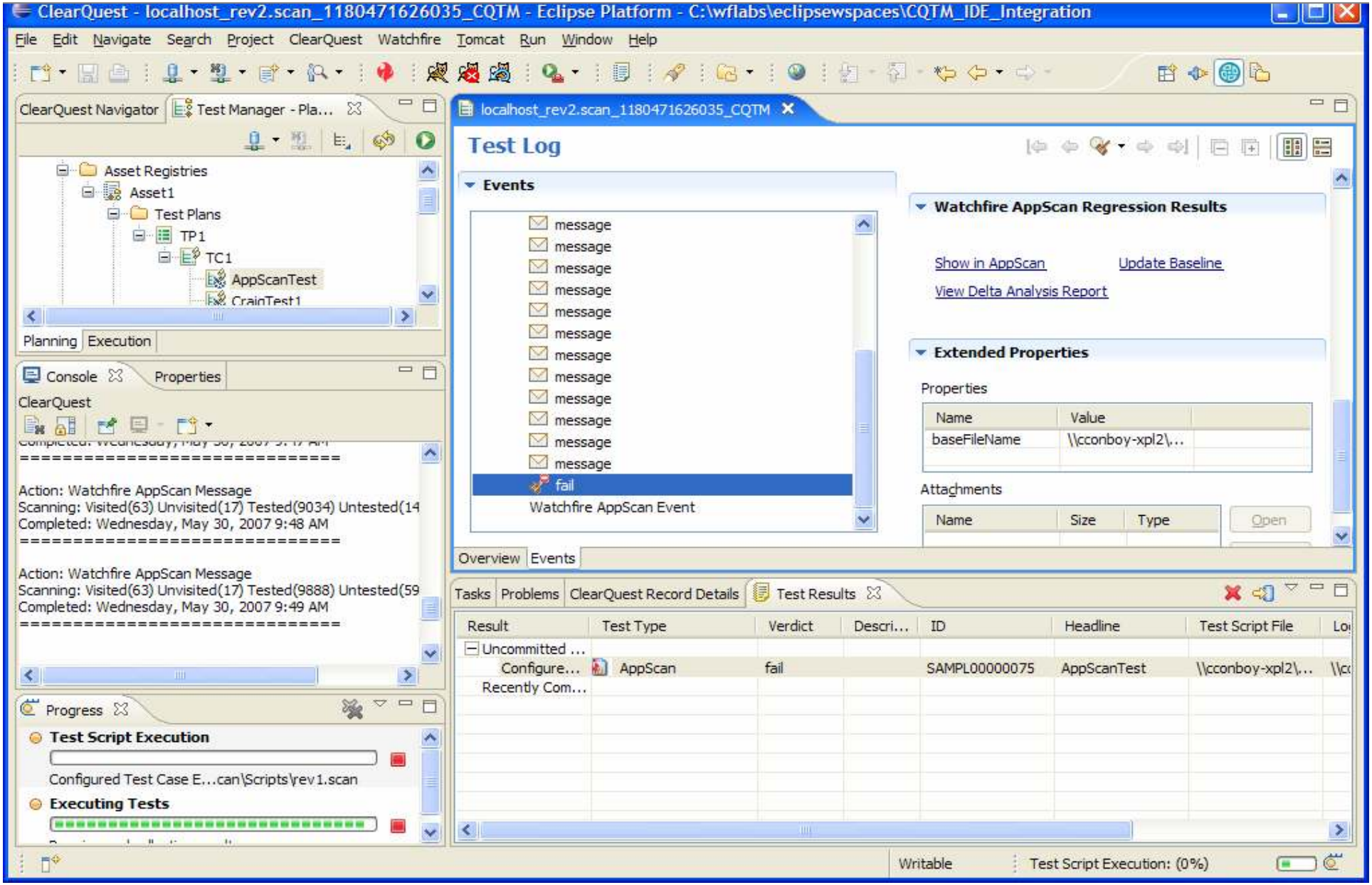


And Most Important :

Actionable Fix Recommendations



AppScan - CQTM & RQM Integration *Protect Your Investment*



Executive Summary - IBM acquires Ounce

- Today's smart products are increasingly interconnected, instrumented and intelligent. Software makes products smarter but has the potential to introduce risk from cyber-attack and regulatory non-compliance
- Application security is one of the top security issues
- The cost and lack of coverage of reactive security is driving companies towards proactive measures – building security into the application development process
- Traditional approaches make it unlikely that development will support security testing due to schedule risks and potential project failure

- **IBM is acquiring Ounce Labs to expand its market leading web application security portfolio.**
- **By combining Ounce Labs source code testing with IBM Rational AppScan's application security testing we are the only provider of a true end-to-end application security solution for managing security compliance across all stages of the development process – from coding to production.**

Delivering greater value
from your investments in software

Who is Ounce Labs?

- Ounce Labs is a proven leader in Static Code Analysis Security
  - Named "leader" in Gartner's 1st Magic Quadrant for SAST (Static Application Security Testing)
  - Software developer founded 2002
  - Headquarters: Waltham, MA
  - Source code security experts

Products

- **Identifies** security vulnerabilities in application source code
- **Automates and integrates** security analysis in the SDLC
- **Connects** source code analysis to enterprise security and GRC platforms

Technology

- 4 **granted** source code security patents, 3 pending
- **Superior** architecture for scalable enterprise deployments
- **Community leadership**: Multiple solutions released into open source, senior-level contributions to PCI, SANS, CWE, OWASP, and more

Customers

- 150+ customers; 98% renewal rate
- **Marquee** financial, government, retail and e-commerce customers
- Solution of choice for security SIs and consultant community

Why has IBM acquired Ounce Labs?

*Ounce Labs provides application source code testing tools to help enterprises **reduce risk and cost** associated with online security and compliance breaches.*

- Application security is the largest category of vulnerability disclosures (55% in 2008)
- Rational acquired Watchfire in 2007 to address customers' Application Security Testing needs
  - AppScan continues to be recognized as the leader in Dynamic Analysis Security Testing (DAST)
  - Avanti is a recognized leader in Static Analysis Security Testing (SAST)
- Application security markets are converging
  - The combination of these two industry leading technologies provides the most accurate solution in the market
  - Avanti's technology enables Rational to fulfill our vision of moving testing earlier in the development process
- Continues to add to our competitive advantage in the application security testing segment
  - Only vendor to offer complete solutions for both SAST & DAST
  - Only vendor to offer complete integration across the software delivery lifecycle
  - Only vendor to offer a complete IT security solution across all major domains (IBM Security Framework)
- Ounce Labs is a good fit
  - Mature technology that supports all key development technologies and languages (Java, .NET, C/C++)
  - Excellent integrations with Rational SDLC products and for the developer – Rational's traditional user base

Ounce Labs & IBM Customer Value

*The addition of Ounce Labs technology and expertise will build on IBM's broad security and compliance product and services offerings to help enterprises **reduce risk and cost** associated with application security breaches*

Key to Business Integrity is Application Security - a top of mind issue for businesses and governments Worldwide

- ✓ *75% of the cyber attacks today are at the application level*[(1)] **, where personal, customer, credit card and other high value data resides.**

This is a complex problem that requires comprehensive technology

- ✓ **The complexity of today's systems, coupled with the sophistication of attackers *requires equally sophisticated technology* to combat these challenges without the expense of developing or employing specialized expertise.**

IBM Provides the complete solution to Application Security

- ✓ **By *integrating Ounce labs Static Code Analysis with IBM Rational AppScan's Dynamic analysis,* IBM is the *only provider of a true end-to-end application security solution for managing security compliance across all stages of the development process* – from coding to production.**
- ✓ ***Remediation of vulnerabilities before applications go live significantly improves business integrity and dramatically reduces cost.***

Rational Security & Compliance–with Ounce Labs

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Req'ts Definition (security templates)	**AppScan Developer** (desktop)	**AppScan Build** (scanning agent)	**AppScan Tester** (scan agent & clients)	**AppScan Standard** (desktop)	**AppScan OnDemand** (SaaS)
Security requirements defined before design & implementation	**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**	**Outsourced testing for security audits & production site monitoring**

Ounce Labs Products

AppScan Enterprise / Reporting Console
(enterprise-wide scanning and reporting)

Application Security Best Practices

Address security from the start

Security audit solutions for IT Security

Security for the development lifecycle

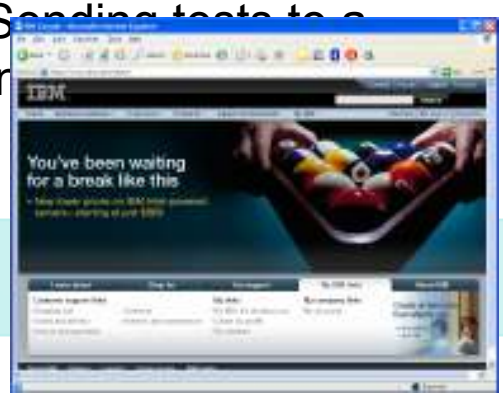
Security Testing Technologies Primer

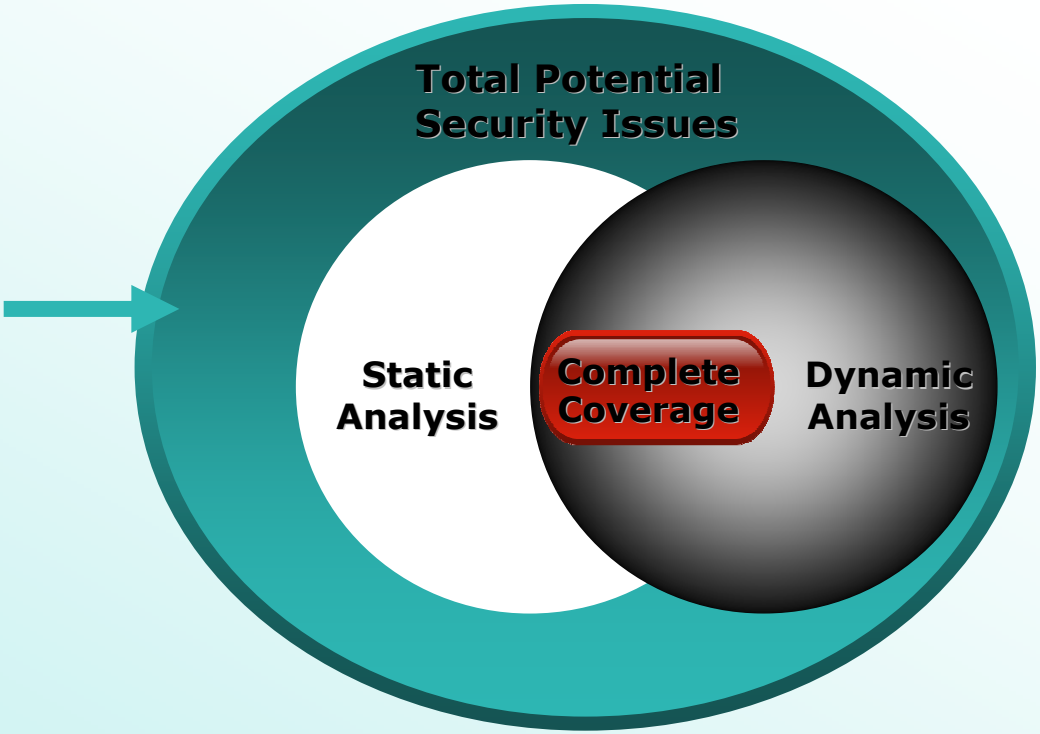
Static Code Analysis = Whitebox

- Looking at the code for se el sc

Dynamic Analysis = Blackbox

- S
fur





Why Choose IBM Rational Security & Compliance

- Broadest suite of offerings to support security testing across the development lifecycle
- **IBM is the only company to offer a complete IT security framework across all major security domains**
- Only web application security testing solution to provide combined code, dynamic, runtime and string analysis
  - Only vendor to offer complete solutions for both SAST & DAST
  - Only vendor to offer complete integration across the software delivery lifecycle
- Broadest set of security compliance reporting
- R&D backed by IBM's $1.5B annual investment in security
- Best Application Security Analysis - Includes multiple analysis techniques to leverage strengths of all techniques & overcomes weaknesses
- Naturally fits into the SDLC process
  - Minimize disruption
  - Scale to large number of users
  - Support collaboration within development
  - Integrate with development tools