November 2011

IBM Rational AppScan: Application security and risk management

Identify, prioritize, track and remediate critical security vulnerabilities and compliance demands

IBM

Comprehensive application vulnerability management

Enterprises today rely on software applications to drive essential business processes, from online transactions to advanced services for customers, business partners and employees. The critical nature of these processes—and the data they collect—make these applications a top target for attacks and the number one source of data breaches. For this reason, enterprises require solutions specific to the challenges of application security that go beyond basic security testing to manage application risk.

The greatest source of application risk comes from security vulnerabilities that create the opportunity for attacks that compromise the integrity of business processes and may allow an attacker to access, create, change or delete data without authorization. But application risk also includes compliance demands that require businesses and public entities to secure sensitive data, ensure the privacy of client data or make services accessible to those with disabilities. To stay ahead of these threats, applications must be *secure by design*.

IBM Secure by Design is the IBM philosophy that security and privacy must be fully considered and prioritized throughout the life cycle of your applications, systems, networks and business processes. When applied to the specific risks and demands of applications, IBM Secure by Design integrates security throughout the software development life cycle. To address the wide range of application risk, the IBM Rational® AppScan® portfolio integrates into the application life-cycle management processes to identify risk, facilitate timely remediation and monitor the state of application security and risk over time.

With a rich history of innovative application security research, the Rational AppScan portfolio combines advanced security testing with the strengths of the Rational application life-cycle management suite to enhance productivity through automation and accelerate better decision making throughout the development organization. Quite simply, Rational AppScan enables you to deliver applications that are secure by design.

Application security: A shared responsibility

Application security has traditionally been the responsibility of security teams that conduct preproduction tests before applications launch. While some vulnerabilities can be corrected, too often these enterprises face a difficult decision when a security defect is identified just before launch. They can:

1. Add development cycles that may delay the launch and increase project costs.
2. Accept the risk of data loss from targeted attacks, application downtime or compliance penalties by launching the application with the security vulnerabilities and compliance issues.

The Rational AppScan portfolio includes solutions for both security teams and development organizations to collectively address application security by identifying and remediating vulnerabilities early in the software development life cycle, when they are easier and cheaper to correct. IBM research drives Rational AppScan solutions to identify the latest threats with advanced security testing for application security analysts. With more than a decade of application security experience, Rational AppScan solutions deliver some of the most advanced testing features that combine expert analysis with ease of use.

The Rational AppScan portfolio includes solutions specifically designed for non-security experts to execute automated test scripts configured by the security team to identify common vulnerabilities, such as SQL Injection and cross-site scripting (XSS). By enabling developers, quality assurance professionals and other nonexperts to address application security as part of their normal processes, security teams can then dedicate their efforts on the more advanced testing to identify sophisticated threats like client-side JavaScript vulnerabilities.

"We turned to IBM Rational because they offered both the technology leadership and the deep security expertise required to help us implement an analysis strategy that could be embedded in our existing development process. By doing so we have been able to vastly improve the security of our software while reducing costs by finding vulnerabilities earlier where they are less costly to repair."

—Marek Hlávka, Chief Security Officer, S'koda Auto

Integrate security into application life-cycle management

Security vulnerabilities are just like quality defects because they occur naturally in any application development process. Enterprises require tools and solutions that empower them to identify and remediate these vulnerabilities as part of their standard practices for application life-cycle management.

By applying the principles of IBM Secure by Design, the Rational AppScan portfolio leverages the strengths of the IBM Rational Collaborative Lifecycle Management Solution to integrate security throughout the application life cycle and enable enterprises to:

- *Collaborate* among and between business, development and test teams with dynamic process- and activity-based workflows for test planning and execution.
- *Automate* labor-intensive security testing and audits to catch security issues early, reduce time to market, cut project costs and mitigate business risk.
- *Empower* non-security experts, such as developers and quality professionals, to execute security tests, identify vulnerabilities and remediate their code.
- *Report* prioritized metrics tailored for individuals and teams, facilitating greater visibility, enabling decision makers to act with confidence and documenting compliance.
- *Deliver* greater predictability by mapping successful deployment patterns to operational key performance indicators (KPIs).

From requirements, through design and code, security testing and into production, Rational AppScan software helps to ensure that critical security vulnerabilities and compliance issues are identified, prioritized, tracked and remediated across the application life cycle. In short, Rational AppScan software helps you to design security into your application infrastructure.

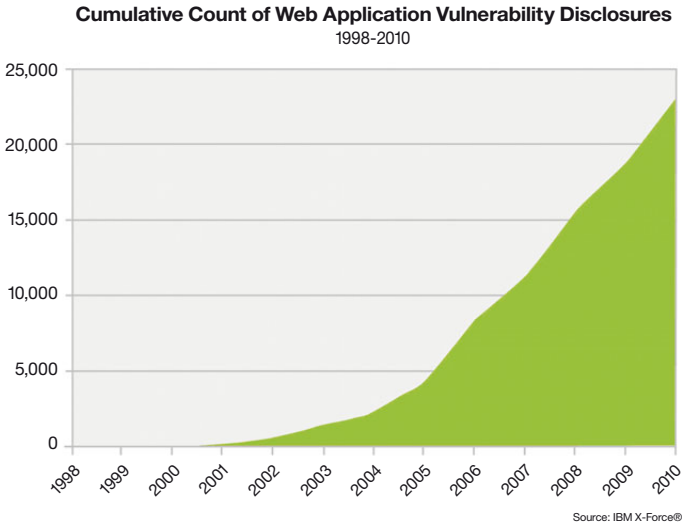

Figure 1: Every year, nearly 4,000 new application vulnerabilities are discovered. This data from the 2010 IBM X-Force® Trend and Risk Report shows the cumulative count of web-application vulnerability disclosures from 1998 to 2010.

Security starts with requirements and design

Just like quality standards, application security is not limited simply to security testing. Security starts by building applications that are secure by design. For this reason, the security experts who built Rational AppScan provide templates for application security requirements. By including security requirements early in development, project teams can write use cases that reflect security risks, reduce project rework and improve the overall security of the application.

Write secure code

Once security is identified as a high-priority requirement for application development, development organizations can then implement secure development practices by empowering developers to identify and remediate security vulnerabilities—while measuring the group's progress at meeting the objectives of secure applications.

The Rational AppScan portfolio delivers the solutions that empower these non-security experts to analyze their code and compiled applications for security vulnerabilities, then take action to remediate the issue. IBM Rational AppScan Source Edition includes plug-ins into the integrated development environment (IDE) to analyze the source code with static (white box) technology and pinpoint the precise line of code that contains the vulnerability.

IBM Rational AppScan Enterprise Edition includes options for dynamic (black box) analysis that tests compiled applications. With its Quick Scan web interface designed for non-security experts, Rational AppScan Enterprise Edition enables developers to easily execute predefined test scripts to identify vulnerabilities by simulating security attacks against the application. With both static and dynamic testing, the Rational AppScan solutions include detailed vulnerability descriptions that explain the risk, and recommended code corrections that give the developers the information to remediate the issue.

Tools like IDE integrations and Quick Scan provide developers with information on improper coding practices to reduce the costs of remediation and help prevent similar security defects from being introduced as they develop additional code.

Integrate security testing with build verification

Security testing is a natural extension to build-acceptance tests. Before a build is released to the test team, development organizations can run static and dynamic tests against the build to identify and remediate known vulnerabilities. Rational AppScan Source Edition includes options for automatically triggering security static scans of the source code with each build. Through their IDE plug-in, developers then access the results to view issues in their code—as well as the detailed descriptions of risk and recommended remediation.

By automating attacks against the compiled application, dynamic testing from Rational AppScan Enterprise Edition or Rational AppScan Standard Edition provides powerful analysis of how the application withstands security attacks while providing the detailed vulnerabilities that should be addressed before releasing the build.

Testing: Make security an element of quality

When application security is integrated into test planning, QA managers can build and execute test plans that map to security requirements. With these test plans in place, QA can then use dynamic (black box) analysis security testing from Rational AppScan Enterprise Edition or Rational AppScan Tester Edition that automates test scripts predefined by the security team. Both Rational AppScan Enterprise Edition and Rational AppScan Tester Edition integrate with IBM Rational Quality Manager software to execute and manage security tests within the familiar testing environment.

Rational AppScan offering	Integrations with Rational Application Lifecycle Management solutions
AppScan Enterprise Edition	• IBM Rational ClearQuest® • IBM Rational Quality Manager • IBM Rational Team Concert™
AppScan Source Edition	• IBM Rational Application Developer • IBM Rational ClearQuest • IBM Rational Quality Manager • IBM Rational Build Forge®
AppScan Standard Edition	• IBM Rational ClearQuest
AppScan Tester Edition	• IBM Rational Quality Manager

Advanced security testing before launch

With common security vulnerabilities identified and corrected in the development, build and testing stages of the process, security teams can now focus on advanced security testing. The Rational AppScan portfolio has a deep history of innovation to deliver broad coverage of application risk with precise results. The Rational AppScan software's advanced security testing delivers:

- Scanning of rich internet applications that use Adobe Flash, JavaScript, AJAX and more.
- Coverage for top threats as ranked by the Open Web Application Security Project (OWASP) and Web Application Security Consortium (WASC).
- Advanced testing for Simple Object Access Protocol (SOAP) web services.
- Static taint analysis of client-side JavaScript.
- Innovative glass-box testing that combines dynamic (black box) analysis with an internal agent that monitors application behavior during a simulated attack to provide more accurate test results, identify specific lines of code and that includes details that help facilitate remediation.

Security of production applications

Every year, nearly 4,000 new application vulnerabilities are discovered.[1] To keep up with the new threats and meet compliance requirements, security teams must routinely scan their critical applications and remediate new vulnerabilities identified in their production applications. Advanced application security research at IBM drives regular content updates to the Rational AppScan portfolio, so clients can be confident that they are keeping up with the latest threats.

Enterprises expand beyond security testing into application risk management when they apply the centralized management features of Rational AppScan Enterprise Edition to:

- Schedule routine scans of production applications—and execute the scans concurrently.
- Measure results over time and multiple scans for each application to track improvement and recognize areas of concern.
- Monitor aggregate risk throughout all applications for executive-level views with KPIs.
- Integrate with defect tracking systems and the greater Rational portfolio for collaborative life-cycle management.
- Deliver more than 40 ready-to-use-without-modification compliance reports for global regulations, including PCI, HIPAA, EU Data Protection Directive, Security Control Standard (ISO 27001) and more.

IBM Rational AppScan portfolio summary

Rational AppScan offering	Description
AppScan Enterprise Edition	• Enterprise platform for managing application security and risk management • Identify application risk with advanced security testing • Mitigate risk by collaborating with developers to remediate security vulnerabilities • Measure, monitor and drive risk reduction with reporting, issue tracking, KPIs and trending • Empower security teams to drive security testing throughout the software development life cycle (SDLC) • Collaborate with developers to remediate security vulnerabilities • Integrate with web-application firewalls to provide custom tuning based on actual vulnerabilities • Plan and execute dynamic (black box) tests against applications in development and production • Integrates with Rational Quality Manager software for QA teams to use in test scripts, and can conduct security checks within their familiar testing environments
AppScan Source Edition	• Adds source code analysis to Rational AppScan Enterprise Edition to identify the latest security threats with static (white box) analysis • Enables quick analysis and recommended corrections, all within the IDE • Automated security testing within build environments
AppScan Standard Edition	• Desktop application for security analysts and penetration testers • Advanced security testing based primarily on dynamic (black box) analysis, but also includes static analysis for client-side JavaScript • Glass-box testing with run-time analysis that applies an internal agent to monitor application behavior during a dynamic test, provide more accurate test results and identify specific lines of code • Coverage of the latest rich-Internet applications and web technologies (web services, SOAP, Flash, Ajax and more • Designed for ease of use
AppScan Tester Edition	• Server and web interface solution designed for QA teams to integrate security testing into existing quality management processes • Integrates with Rational Quality Manager for QA teams to use in test scripts, and can conduct security checks within their familiar testing environments
AppScan Policy Tester	• Online compliance solution to assess quality, privacy and accessibility-compliance issues for corporate web properties

Risk management for privacy and accessibility

Application risk includes more than just security vulnerabilities, and the Rational AppScan portfolio includes solutions to address the risks associated with privacy and accessibility. IBM Rational Policy Tester addresses website privacy by:

- Identifying and documenting where in your application you collect data from users.
- Cataloging the types of data your application collects.
- Highlighting data that could potentially be exposed.

Accessibility risks include the potential for web users with disabilities to be denied full access to the website—and the potential law suits that could arise from denying them full access. To maintain accessibility, websites must support assistive technologies, such as screen readers and voice-activated devices. Optimizing web pages for these technologies is critical to serving all users, maintaining compliance with regulations that require full accessibility and avoiding litigation.

IBM Rational Policy Tester Accessibility Edition software scans web applications and content by executing hundreds of comprehensive accessibility checks, as well as testing for compliance-related issues concerning US government regulations and widely accepted nongovernmental organization (NGO) standards.

Managing the risk in enterprise modernization

Enterprise modernization of mature applications can also be a source for application risk. COBOL still represents nearly 80 percent of the world's actively used code, and web interfaces for these legacy applications expose them to threats that did not exist when the code was written 20 - 40 years ago.

The Rational AppScan portfolio delivers complete security coverage for enterprise modernization projects to secure the web interfaces and analyze the heritage-application code to identify security vulnerabilities. With extensive language support that includes COBOL and C++ and robust integration with IDEs, Rational AppScan Source Edition helps manage security risk and protect heritage assets by proactively securing the applications. Key benefits include:

- Cost-effectively manage risk with proactive remediation of application vulnerabilities
- Protect heritage assets by securing applications early in the application life cycle
- Identify vulnerabilities and risks associated with multiple languages, including COBOL, Java and .NET (Microsoft Visual C#, VB.NET, ASP.NET)

Why IBM for application security and risk management

IBM delivers the most complete portfolio of application-security and risk-management solutions. With advanced security testing and a platform managing application risk, the IBM Rational AppScan portfolio delivers the security expertise and critical integrations to application life-cycle management that empower enterprises to not just identify vulnerabilities, but also reduce overall application risk. The IBM Rational AppScan portfolio includes advanced static (white box) and dynamic (black box) analysis—as well as innovative technologies like glass-box testing and run-time analysis that keep up with the latest threats and drive precise, actionable results.

Application security is a core component of the IBM Security framework. The software portfolio of Rational AppScan is complemented by software-as-a-service (SaaS) delivery options and robust professional service offerings, including application security assessments, deployment services, advanced application security training, product training and more. In addition to application security testing, IBM Security Systems delivers application security solutions that protect against attacks and securely manage identity and access for application users.

For more information

To learn more about IBM Rational AppScan solutions for application security, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/software/awdtools/appscan/

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2011

[1] IBM X-Force 2010 Risk and Trend Report

Please Recycle