IBM Rational AppScan Source Edition

Secure applications and build secure software with static application security testing

Highlights

- Identify vulnerabilities in your source code, review data and call flows and identify the threat exposure of each of your applications
- Scan source code early in the development cycle to simplify the adoption of security testing by development
- Integrate security testing with application development tools and the IBM Rational Collaborative Lifecycle Management solution
- Create, push and enforce consistent policies that can be used throughout your enterprise

Today's economy depends upon interconnected, instrumented and intelligent systems with custom software and web applications. These smart products and applications generate or interact with vast amounts of data. Eager to take advantage of opportunities in the marketplace, companies are developing these smarter products and applications at an increasingly rapid rate. But in the race to stay ahead, many companies fail to give application security the attention and priority it requires.

Unfortunately, the headlines have made one thing clear: If you don't take the appropriate measures to protect your company's systems, applications, private data and customer information, the consequences to your bottom line and your brand can be devastating. They range from heavy financial penalties and lost revenue to system outages that erode customer confidence and damage your company's reputation. Can your company weather that kind of storm? Not many can. That's why it's essential to have a comprehensive application security strategy in place.

Identifying vulnerabilities in your source code

To address the wide range of application risks, IBM offers the IBM® Rational® AppScan® portfolio of application security testing and risk management solutions. As a key component of the portfolio, IBM Rational AppScan Source Edition software is a static analysis security testing solution that helps you identify vulnerabilities in your source

code, review data and call flows, and identify the threat exposure of each of your applications. Deployed throughout the software development life cycle, Rational AppScan Source Edition software makes it easier for you to understand your threat exposure for audit and compliance purposes. Rational AppScan Source Edition software also helps facilitate a partnership between development and security teams by providing both groups with the information they need, when they need it.

Reducing vulnerabilities early in the development life cycle

Rational AppScan Source Edition software provides a comprehensive approach to source code analysis. It is designed to deliver fast scans of more than one million lines of code in an hour, allowing you to scan complex enterprise applications. It also provides actionable, prioritized information—down to the line of vulnerable code. This helps you find and address vulnerable code early in the development cycle, review applications that are already in use and perform security and quality checks on applications or components that you have outsourced for development. For example, you can build security requirements into your outsourcing contracts, and use Rational AppScan Source Edition software to help ensure that your acceptance criteria have been met.

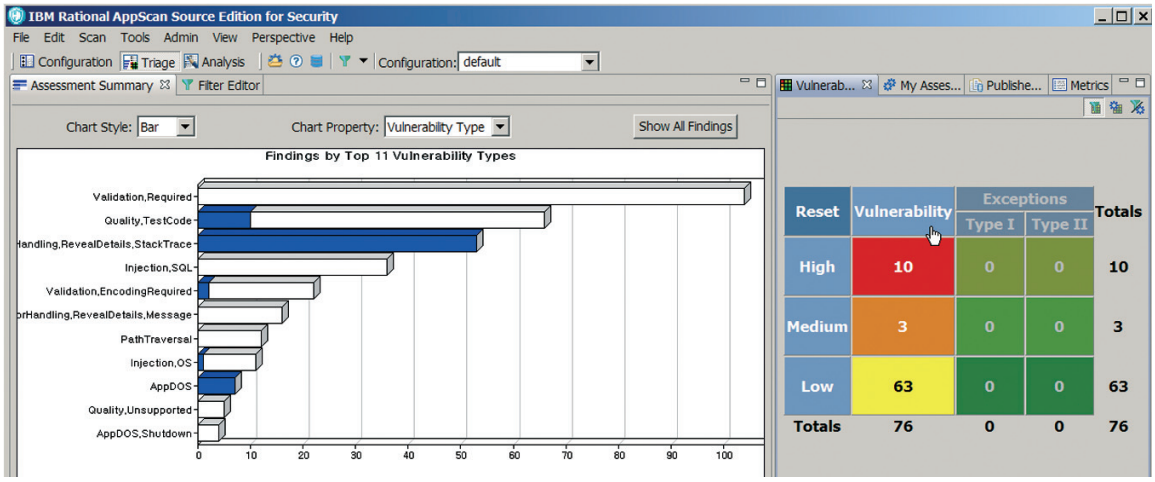

Figure 1: Rational AppScan Source Edition software provides assessment summaries that map to application risk and give you insight into the vulnerabilities affecting your applications.

Right out of the box, Rational AppScan Source Edition software provides report cards, detailed metrics and the remediation advice you need to find and eliminate the vulnerabilities in your applications. However, merely identifying buffer overflows or Structured Query Language (SQL) injections does not secure an application. Improper implementation of other security mechanisms, including access controls, authentication and encryption, can pose an even greater risk to your organization.

Rational AppScan Source Edition allows you to take action on your most critical vulnerabilities by integrating with the Rational Collaborative Lifecycle Management solution 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).

Improving efficiency using automated security testing

Manually testing your software applications can result in late releases or inconsistent test results. An automated solution can help your team test software more thoroughly and more quickly, while freeing your testers for more value-generating tasks. Plus, Rational AppScan Source Edition software prioritizes the results you need to eliminate the coding errors and design flaws that put your data at risk. The application is easy to install and configure, so you can implement it quickly and begin to automate your workflows with minimal disruption to your existing processes.

Facilitating consistency with centralized policies, processes and reporting

Rational AppScan Source Edition software helps you set, push and enforce consistent policies that can be used throughout your enterprise. The solution supports deployment options that allow non-security experts to execute automated test scripts configured by the security team to identify common vulnerabilities.

Security analysts use the **AppScan Source for Security** client to manage all static testing, execute advanced source code scans and build the test scripts that can be executed in either build systems or by developers in their integrated development environment (IDE). **AppScan Source for Automation** software

works with a wide range of build applications, including IBM Rational Build Forge® software, CruiseControl, Apache Continuum and Microsoft MSBuild software, to automatically trigger source code scans as new code is checked into the build system.

Rational AppScan Source Edition software can be used by developers to scan their code, remediate vulnerabilities and resolve assigned work items in their IDE. For developers to scan their own code, IBM offers **AppScan Source for Developer** software as an IDE module or plug-in. For developers who just want to analyze results from scans executed in the build system and work on issues assigned by security analysts, **AppScan Source for Remediation** software delivers the IDE module without the scanning capability. Both IDE options offer robust support for resolving vulnerabilities with detailed explanations of the defect and recommended code corrections.

All test results are centrally managed with **Rational AppScan Enterprise** server, a component of AppScan Source Edition software deployments. The server provides the centralized platform for application security testing and risk management. Rational AppScan Enterprise server:

- Aggregates both dynamic and static tests
- Correlates results for hybrid analysis
- Provides executive level dashboards with key performance indicators
- Integrates with the Rational application lifecycle m anagement suite
- Includes more than 40 out-of-the-box compliance reports for regulations such as PCI, HIPAA, EU Data Protection Directive, Security Control Standard (ISO 27001) and more

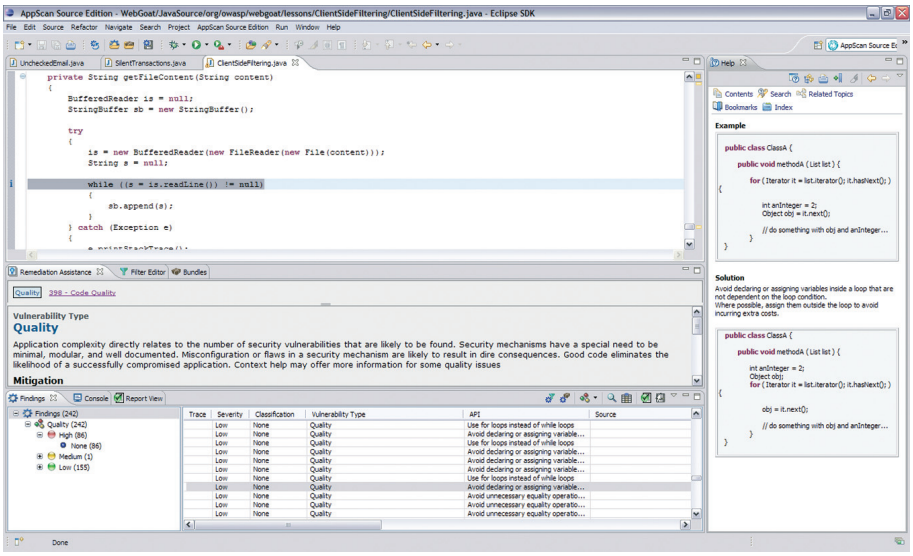

Figure 2: Rational AppScan Source Edition software includes options to scan from the IDE or simply access results from the IDE with details about the defect, explanation of the risk and guidance on how the defect can be corrected.

Providing comprehensive and scalable testing capabilities

Rational AppScan Source Edition software is based on a patented design that allows it to accommodate a comprehensive portfolio of the largest and most complex applications for a wide range of languages. Plus, it identifies a wide range of security vulnerabilities, pinpointing the coding flaws and design errors that put data and operations at risk. Its in-depth, cross-modular analysis is able to isolate confirmed vulnerabilities to immediately target the most critical security flaws. Of course, in order to be able to identify security flaws the analysis software must be able to test against a range of languages and application frameworks. Rational AppScan Source Edition's unique Extensible Web Application Framework provides the ability to gain greater visibility and data flow analysis into commercial, open source, and in-house custom developed web application frameworks.

Customizing analysis, reporting and workflows

With Rational AppScan Source Edition software, you can customize the analysis to fit your policies and critical security concerns. Add vulnerabilities specific to your organization, adjust the severity of existing vulnerabilities and adjust the priority of those most critical to you. Rational AppScan Source Edition software provides flexible and customizable reporting that enables you to decide how the information is selected, grouped and represented for remediation, compliance and risk management reporting. The application also delivers flexible triage and remediation configurations, so you can automate the flow of information between security and development teams, using the workflow that best suits your organization.

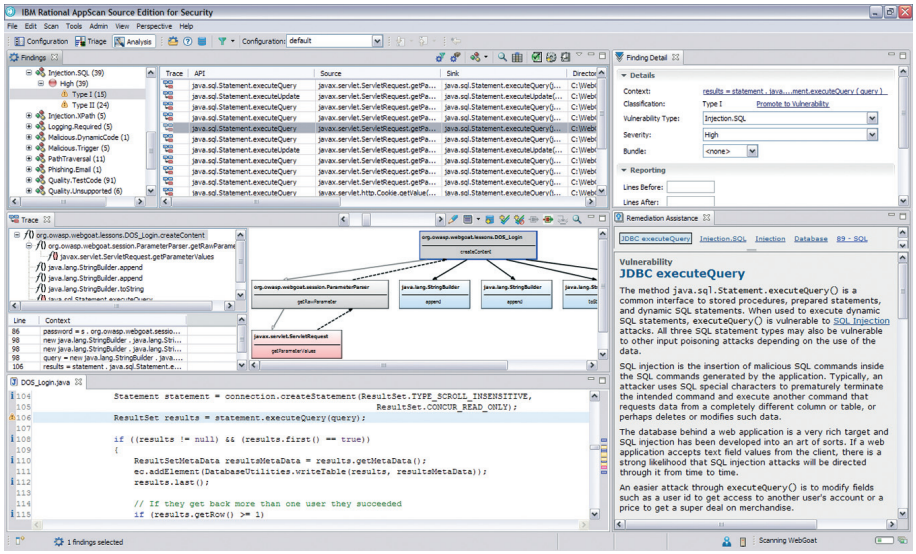

Figure 3: Rational AppScan Source Edition software provides details for every vulnerability including line of code and source-to-sink function flow.

Rational AppScan Source Edition software integrates with defect tracking systems (DTS) with a framework that helps you dispatch Rational AppScan Source Edition software issues in conjunction with your existing processes, using your existing priority and severity nomenclature and your existing workflows.

Managing the risk in enterprise modernization

Enterprise modernization of legacy applications can also be a source for application risk. COBOL still accounts for nearly 80 percent of the world's actively used code[1], and web interfaces for these legacy applications open them to threats that did not exist when the code was written 20 - 40 years ago.

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

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

Extend static testing to include code quality

Many leading enterprises integrate security with their software development processes by making security an element of quality management. As security and quality converge, the static code analysis capability of Rational AppScan Source Edition software is extended to include identification of quality defects. Rational AppScan Source Edition software now also includes the capabilities that are offered by IBM Rational Software Analyzer software to:

- Identify code-level quality defects at the time of coding, helping save both time and money
- Improve overall code quality and predictability by identifying and resolving potential coding errors
- Provide KPIs to help developers learn best practices
- Enhance project visibility and more effectively manage governance and compliance using customizable and out-of-the-box reporting
- Automate code quality analysis as part of the build process for a centralized software code scan solution

Rational AppScan Source Edition software provides options for executing quality testing from the IDE with AppScan Source Edition for Developer software and AppScan Source Edition for Remediation software or in the build system with AppScan Source Edition for Automation software. By extending static analysis to include quality testing, Rational AppScan Source Edition software can help clients continuously enforce code quality best practices for faster time to market and higher customer satisfaction.

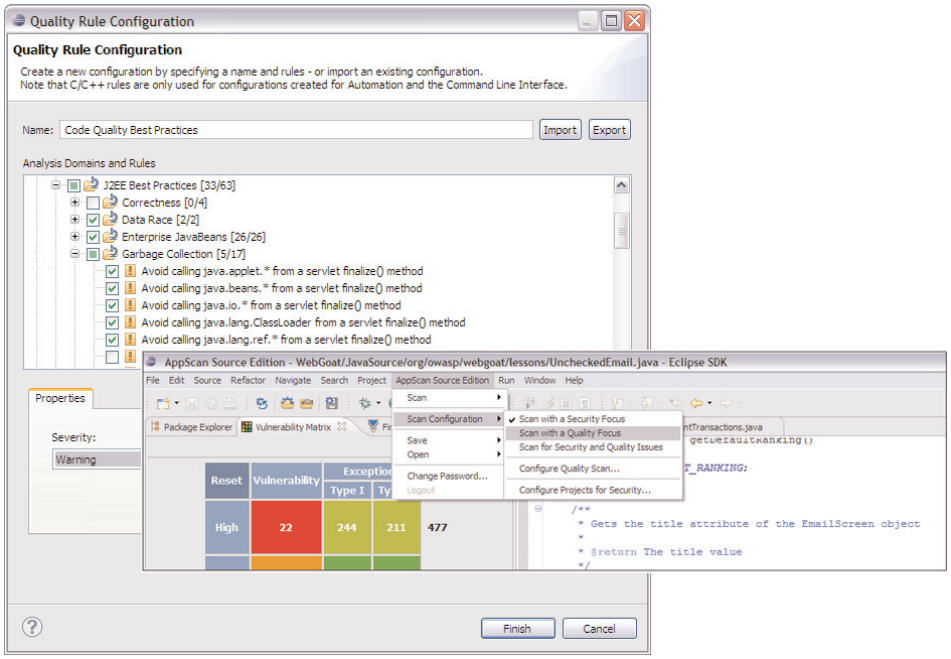

Figure 4: Rational AppScan Source Edition software includes code quality analysis that is executed from the IDE or in the build system just like security tests.

Solution components	Features and benefits
AppScan Enterprise Server (required)	• Centralized platform for managing application security testing and risk management for 100s or 1000s of applications • Drive collaboration between security, development and testing teams to remediate vulnerabilities and reduce risk • Enterprise-wide view of application security and compliance risk with more than 40 out-of-the-box report templates for measuring compliance, trending and key performance indicators • Correlate and triage security testing results from dynamic (black box) and static (white box) scans • Integrate with IBM Proventia® Management SiteProtector software, IBM Security Network IPS software and IBM Security Server Protection software to block attacks that target vulnerabilities identified by AppScan software.
AppScan Source for Security (required for static analysis)	• Workbench to manage static (white box) analysis security testing policies–configure and scan • Triage results from static testing and take action to remediate vulnerabilities
AppScan Source for Automation (optional)	• Seamlessly integrate static (white box) analysis security, publishing and reporting into build environments • Automate code quality analysis as part of the build process
AppScan Source for Developer (optional)	• Integrated development environment (IDE) module with the ability to scan source code and to understand and address critical vulnerabilities at the line of code. • Remediate security vulnerabilities from the IDE with detailed explanations of the issue and recommended source code corrections • Identify and remediate non-security software code-level quality defects
AppScan Source for Remediation (optional)	• IDE module with the ability to process and address critical vulnerabilities at the line of code • Remediate security vulnerabilities from the IDE with detailed explanations of the issue and recommended source code corrections • Identify and remediate non-security software code-level quality defects
AppScan Enterprise Dynamic Analysis Scanner (optional)	• Adds advanced application security testing applying dynamic (black box) analysis
AppScan Enterprise Reporting User (optional)	• Web-based user to triage testing results, collaborate with development teams, create reports and drive application risk management
Virtual Forge CodeProfiler for AppScan Source (optional)	• Extends static code analysis for SAP ABAP applications to identify and remediate security vulnerabilities and performance issues

Rational AppScan Source Edition at a glance

System requirements:

- Processor: Intel Pentium P4, 3.0 GHz or faster
- Memory: 2 GB RAM minimum
- Disk Space: Windows 1 GB (2 GB required for installation); Linux 1.1 GB (2 GB required for installation)
- Network: 1 NIC 10 Mbps for network communication with configured TCP/IP (100 Mbps recommended)
- Drives: CD-ROM or DVD-ROM drive

Operating systems:

- Microsoft Windows 7 Professional, Enterprise and Ultimate 32 and 64-bit (in 32-bit mode)
- Microsoft Windows XP Professional (SP2, and higher)
- Microsoft Windows Vista Business, Enterprise and Ultimate (SP1) 32 and 64-bit (in 32-bit mode)
- Microsoft Windows Server 2003 Enterprise (SP2, and higher)
- Microsoft Windows Server 2008 Enterprise
- Microsoft Windows Server 2008 R2 Enterprise (in 32-bit mode)
- RedHat Enterprise Linux 4.0 Workstation and Server
- RedHat Enterprise Linux 5.0 and 6.0 Workstation and Server 32 and 64-bit (in 32-bit mode)
- Solaris 9 (IBM Rational AppScan Source Edition for Automation only)
- Solaris 10 (IBM Rational AppScan Source Edition for Automation only)

Rational AppScan Source Edition at a glance

Project Files:

- Visual Studio 2005, Visual Studio 2008, Visual Studio 2010 (excluding C and C++), WebSphere Studio, Application Developer 5.1, Eclipse 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 and 3.7, IBM Rational Application Developer V6.0, V7.0, V7.5, V8.0, and V8.0.1

Compilers:

- GNU compiler Collection (gcc), Visual Studio.NET (V7, Visual Studio .NET 2003 (V7.1), Visual Studio 2005 (V8) for Windows, Visual Studio 2008, Visual Studio 2010 (excluding C and C++), Sun Studio C and C++ Compilers for Linux and Solaris

Language Support for Security:

- Java, ClientSide JavaScript, JSP, ColdFusion, C, C++, .NET (C#, ASP.NET, and VB.NET), Classic ASP, (JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL, and COBOL

Language Support for Quality Testing:

- Java, C, C++ (Microsoft Windows, Red Hat Enterprise Linux only)

IDE Plug-inSupport:

- Eclipse versions 3.3, 3.4, 3.5 and 3.6; IBM Rational Application Developer (RAD) V7.0, V7.5, V7.5.0.3, V8.0, and V8.0.1; Visual Studio 2005, Visual Studio 2008, and Visual Studio 2010 (excluding C and C++); RAD and Eclipse supports Java, Visual Studio supports C#, ASP.NET, and VB.NET

Defect Tracking System Support:

- IBM Rational ClearQuest® V7.0, V7.1.1, 7.1.2 and 8.0; HP Quality Center 9.2, 10.0; Rational Team Concert 2.0.0.2, 3.0 and 3.0.1; Microsoft Team Foundation Server 2008 and 2010

External Database Support:

- Oracle 10g and Oracle 11g

Why IBM for application security and risk management

IBM delivers a comprehensive 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 enable enterprises to not just identify vulnerabilities, but to 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 how Rational AppScan Source Edition software can help you identify vulnerabilities in your source code and identify threat exposures, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/rational/products/appscan/source

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] http://www.bankingtech.com/bankingtech/article.do?articleid=20000168221

Please Recycle

RAD14105-USEN-02