Rational. software

IBM Rational AppScan Source Edition

Highlights

- ***Enables you to identify vulnerabilities within your source code, review data flows and identify the threat exposure of each of your applications***
- ***Allows you to scan static code early in the development cycle, review applications that are already in use, or perform quality checks on outsourced applications or components***
- ***Integrates with many application development and security applications you may already have, protecting your existing investments***
- ***Enables you to set, push and enforce consistent policies that can be used throughout your enterprise***

Interconnected, instrumented and intelligent products are flooding the marketplace. Made up of embedded software along with mechanical and electrical components, these smart products generate an increasing amount of data. And as a result, we have all become more dependent upon the software that powers these products and processes this information. Eager to take advantage of opportunities in the marketplace, companies are developing these smarter products at an increasingly rapid rate. But in the race to stay ahead, many companies fail to give application security the attention and priority it needs.

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 security strategy in place.

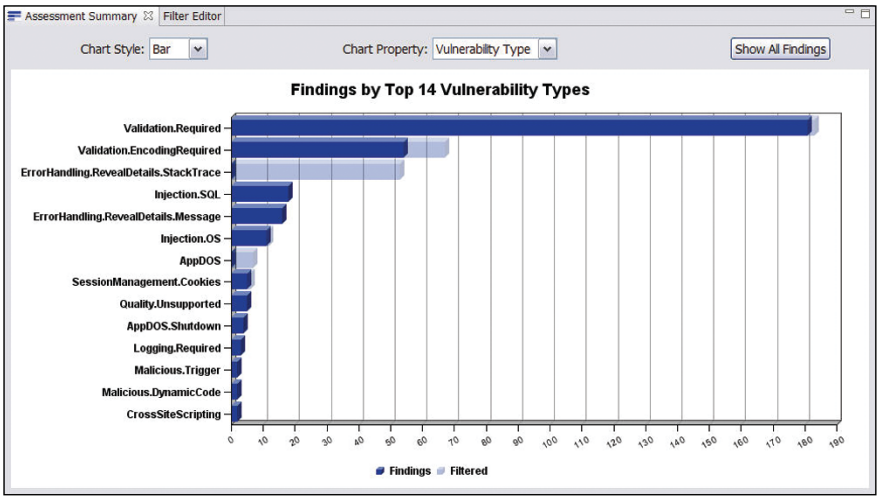
Identifying vulnerabilities within your source code

IBM Rational® AppScan® Source Edition software* is a static analysis security testing application that enables you to identify vulnerabilities within your source code, review data flows and identify the threat exposure of each of your applications. Deployed during development, Rational AppScan Source Edition software makes it easier for you to understand your threat exposure at the executive level for audit and compliance purposes and throughout the software development lifecycle (SDLC). 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 SDLC

Rational AppScan Source Edition software provides a comprehensive approach to source code analysis, delivering fast scans of more than 1 million lines of code an hour, enabling you to scan even the most complex enterprise applications. It also provides actionable, prioritized information—down to the line of vulnerable code. This enables you to use the application to find and address vulnerable code early in the development cycle, to review applications that are already in use, or to perform 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.

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. 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. Take action on your most critical vulnerabilities using an advanced source code analysis technology.



Rational AppScan Source Edition software provides assessment summaries that give you insight into the vulnerabilities affecting your applications.

Combining the source code testing capabilities of Rational AppScan Source Edition with the Web application security scanning provided by other offerings in the Rational AppScan portfolio helps to ensure the most comprehensive coverage for addressing vulnerabilities in your applications. You can also achieve centralized reporting of static and dynamic analysis results with IBM Rational AppScan Reporting Console or IBM Rational AppScan Enterprise Edition software.

Protecting your existing investments

Rational AppScan Source Edition software is built on an open architecture, so it enables you to continue working the way you always have. It integrates easily with applications you may already have, protecting your investments in your existing enterprise SDLC tools and security infrastructure. It can integrate with:

- ***Defect tracking systems (DTSs).*** *Rational AppScan Source Edition software provides a DTS integration framework that enables you to seamlessly integrate its findings with your existing DTS. The framework enables you to dispatch Rational AppScan Source Edition issues in conjunction with your existing processes, using your existing priority and severity nomenclature, and your existing workflows.*

- *Software configuration management (SCM) and build management tools. The Rational AppScan Source Edition for Automation server works with a wide range of build applications, including IBM Rational Build Forge®, CruiseControl, Apache Continuum and Microsoft® MSBuild software.*
- *Dynamic analysis tools and Web application firewalls. Rational AppScan Source Edition software includes an open API to the assessment database, enabling you to manipulate data for integration with other security systems. Correlate data from a penetration test to pinpoint issues at the line of code and identify the source of an exploit. Use the results of your Rational AppScan Source Edition scan to better tune your firewall to protect assets while you work to fix vulnerabilities.*

Improving efficiency using automation

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 enables you to set, push and enforce consistent policies that can be used throughout your enterprise. Plus, it provides enterprise-wide metrics and reporting with a centralized policy and assessment database. By using one set of policies and one set of data, you can implement a more consistent, efficient and effective enterprise testing platform. Assessment results are stored centrally with reports and remediation information, so your teams can use dashboards. Stakeholders can also monitor project progress through the Rational AppScan Source Edition online portfolio. You can even keep outside teams—including partners and suppliers—in the loop by publishing customized compliance results and remediation lists.

Providing comprehensive and scalable testing capabilities

Rational AppScan Source Edition software is based on a patented design that enables it to accommodate a comprehensive portfolio of the largest and most complex applications across 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.

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.

Delivering value to just about every team in your organization

Rational AppScan Source Edition software has been designed to deliver excellent value with available components to support every security stakeholder within your organization. It includes:

- *Rational AppScan Source Edition for Core — A security knowledge base and multiapplication assessment database.*
- *Rational AppScan Source Edition for Security — A workbench to manage security policies, and to configure, scan and take action on priority vulnerabilities.*
- *Rational AppScan Source Edition for Automation — A server component to seamlessly integrate scanning, publishing and reporting into build environments.*
- *Rational AppScan Source Edition for Developer — An integrated development environment (IDE) module with the ability to scan source code and to understand and address critical vulnerabilities at the line of code.*
- *Rational AppScan Source Edition for Remediation — An IDE module with the ability to process and address critical vulnerabilities at the line of code.*

For more information

To learn more about IBM Rational AppScan Source Edition software, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/software/rational/products/appscan/source

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

Produced in the United States of America
November 2009

* Formerly Ounce 6 software from Ounce Labs.

RAD14105-USEN-00