Strategic protection for Web assets
To support your business objectives

Rational. software

IBM

The IBM Rational AppScan lifecycle solution: building Web application security into software and systems delivery.

Are online vulnerabilities putting your business at risk?

Today, many organizations depend on Web-based software and systems to run their business processes, conduct transactions with suppliers and deliver ever more sophisticated services to customers. Building security into every application destined for online deployment should be an integral part of the business processes for software and systems delivery within a well-governed organization. Unfortunately, in the race to stay one step ahead of the competition, many companies give short shrift to these concerns as they hasten to speed new offerings to market. And the resulting vulnerabilities can provide ample opportunity for hackers to access or steal corporate or personal data—potentially placing the entire business at risk.

IBM Rational® AppScan® is a suite of marketplace-leading Web application security solutions that gives organizations the necessary visibility and control to address this critical challenge. The suite includes:

- **IBM Rational AppScan Standard Edition** (available as a desktop application or as software as a service [SaaS]).
- **IBM Rational AppScan Tester Edition** (available as a desktop application).
- **IBM Rational AppScan Enterprise Edition** (available as a Web-based solution or SaaS).

Each of these comprehensive solutions provides scanning, reporting and fix recommendations and is suitable for all types of security testing by a variety of users, including application developers, quality assurance (QA) teams, penetration testers, security auditors and senior managers.

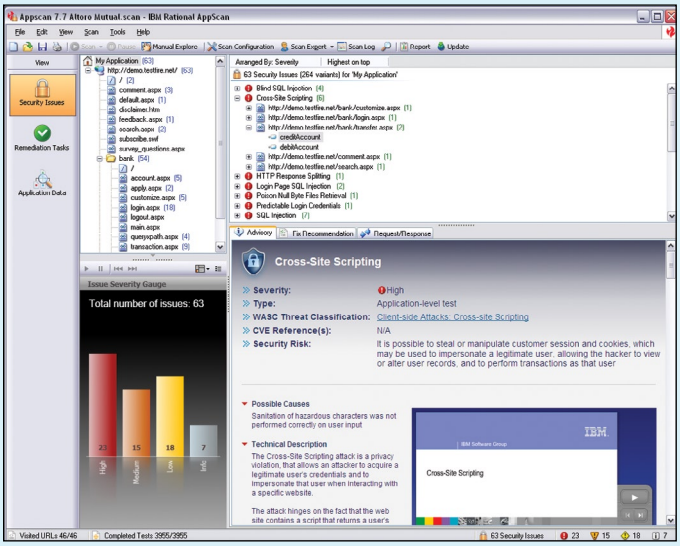
Like other lifecycle solutions in the IBM Rational Software Delivery Platform, Rational AppScan products allow users to work within a familiar technology environment, offering virtually seamless integration with leading QA tools and integrated development environments (IDEs). And the applications enable you to perform continuous security auditing, helping software delivery teams build security into Web applications from the ground up, and helping to mitigate business risk before you even deploy your applications.

Protecting your critical Web-based business assets

Offering comprehensive security coverage for complex Web sites, the Rational AppScan Standard, Rational AppScan Tester and Rational AppScan Enterprise solutions scan and test for common Web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. The Rational AppScan solutions share an extensive range of powerful, flexible core features to provide robust application scanning coverage for the latest Web 2.0 technologies, including enhanced support for Flash and advanced Java™ Script languages, coupled with comprehensive support for the Ajax programming language (including dedicated tests for JavaScript Object Notation [JSON] and Web services parameters).

Rational AppScan core features for scanning efficiency and ease of use include:

- A user interface with a view selector for the application tree, hierarchical security issues results lists, developer remediation views and details panes.
- An adaptive test process that enables you to analyze application parameters and select only relevant tests that do not impede the development process.
- Complex authentication support that enables testing for multi-step authentication procedures in Web applications, including Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) stepped authentication, multifactor authentication, one-time passwords, Universal Serial Bus (USB) keys, smart cards and mutual authentication.
- Advanced session management that performs automatic relogins when required.
- Realtime results views that enable users to act on issues before a scan is complete.
- Pattern search rules that facilitate security testing around credit card, social security or other numerical sequences.



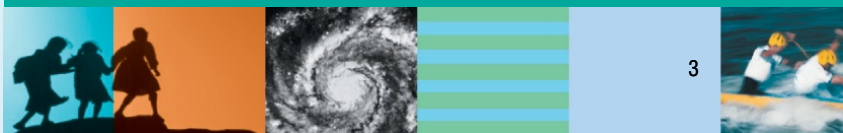
IBM Rational AppScan security advisory view

Rational AppScan core features for customization and control include:

- Rational AppScan eXtensions Framework technology, which enables users to create, share and load powerful add-ons that extend testing capabilities.
- Pyscan, which couples Rational AppScan with the capabilities of Python scripts to enable users to leverage scanning capabilities without the limitations of a user interface. The result is a level of customization previously unavailable to security professionals and penetration testers.
- Rational AppScan software development kit (SDK), which provides the ability to invoke actions, from executing a long scan to submitting a custom test. The SDK interfaces are designed to ease integrations and support customized use of the scan engine, along with Rational AppScan eXtensions Framework and Pyscan options.

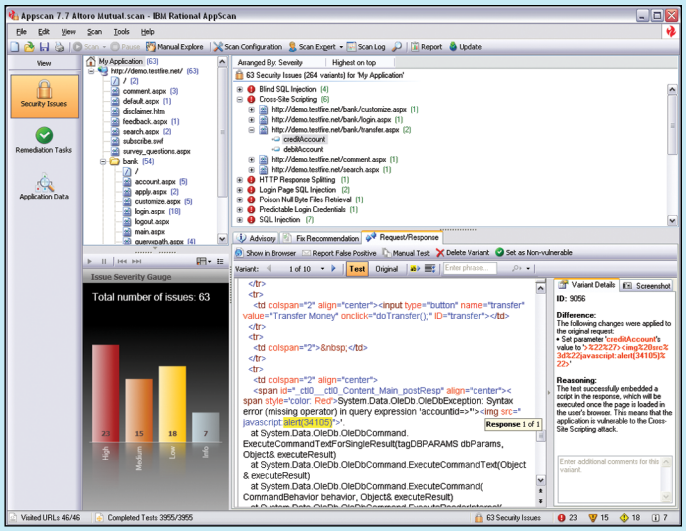
Rational AppScan core features for vulnerability detection include:

- Coverage for global validation that analyzes test responses for inadvertently triggered issues, Secure Sockets Layer (SSL) test (to test SSL certificate validity) and cross-site request forgery (CSRF) testing.
- Hacker simulations covering the Open Web Application Security Project's (OWASP's) top 10 and the System Administration, Networking, and Security Institute's (SANS's) top 20 vulnerabilities.
- Information on the latest threats, updated automatically when you launch a Rational AppScan product.
- A bundled utility suite to help penetration testers and security consultants develop, test and debug Web applications.

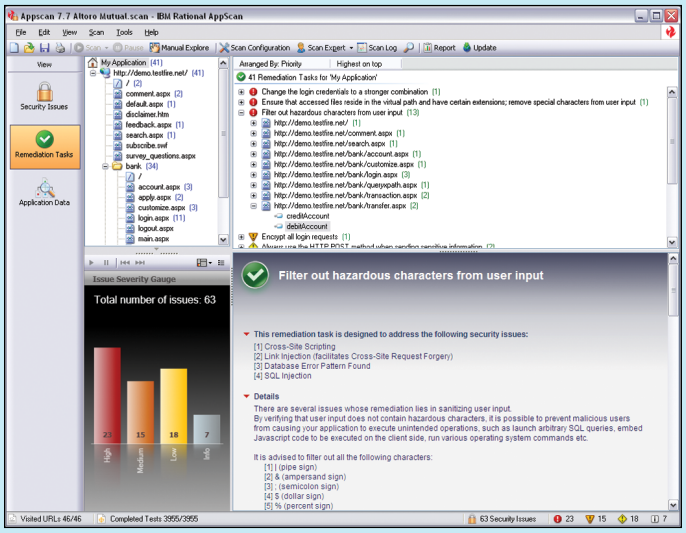


Rational AppScan core features for reporting and remediation include:

- Tests related to more than 40 global regulatory compliance issues and standards, including National Institute of Standards and Technology Special Publication (NIST SP) 800-53 and the OWASP top 10 (updated in 2007). Rational AppScan, Version 7.7 also includes coverage for the Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP).
- Validation highlighting that pinpoints HTML code containing vulnerabilities and explains the issue. A difference feature displays modified HTML code.
- Remediation reports that include Hypertext Preprocessor (PHP) fix recommendations and developer task lists. These reports also enable you to view application-related issues, infrastructure issues or both, and to delete variants or mark them as *not vulnerable* for later review.
- Detailed suspicious content reports that list items such as sensitive data in HTML comments, as well as HTTP activity around suspicious content.
- Test descriptions that include IDs for common vulnerabilities and exposures (CVEs) from the vulnerability database.
- The ability to incorporate screen shots from the Rational AppScan internal browser into reports, and to extract, compress and encrypt nonproprietary information from specific tests for e-mailing. The Rational AppScan software also allows you to report false positive (or negative) incidents to the IBM Rational AppScan security research team, which helps to continually improve the accuracy of the product.



IBM Rational AppScan security issues view



IBM Rational AppScan remediation view

Conduct security audits and production monitoring with Rational AppScan Standard Edition software

Automating Web application testing for security auditors and penetration testers requires sophisticated and intelligent scanning technologies. Rational AppScan Standard Edition includes specific features designed to support moderate users and power users. Features include:

- The scan expert, which offers guidance for scan creation and setup based on best practices, including the use of additional tools. Users can authorize a prescan that profiles the target application and recommends actions required for a successful scan.
- The state inducer, which scans and tests complex business processes, such as multistep online shopping and tracking, and maintains parameter values and cookies throughout.
- Predefined scan templates that enable users to quickly choose and launch configuration options.
- A rapid scan configuration wizard that guides users through important settings as well as conditional steps for proxy/platform authentication and in-session detection information.
- New request/response tabs that offer syntax highlighting, request/response, collapse/expand, as-you-type search and additional right-click options.
- Microsoft® Word template–based reporting for designing custom formats that conform to corporate standards. Templates feature a table of contents, scan start and end times, and graphics.
- Embedded Web-based training (WBT) modules that help explain issues and demonstrate the exploit, along with results verification to help facilitate understanding and communication of the vulnerabilities.

Make security testing part of your quality management program with Rational AppScan Tester Edition software

Rational AppScan Tester Edition offers capabilities to help QA teams integrate security testing into existing quality management processes, thereby easing the burden on security professionals.

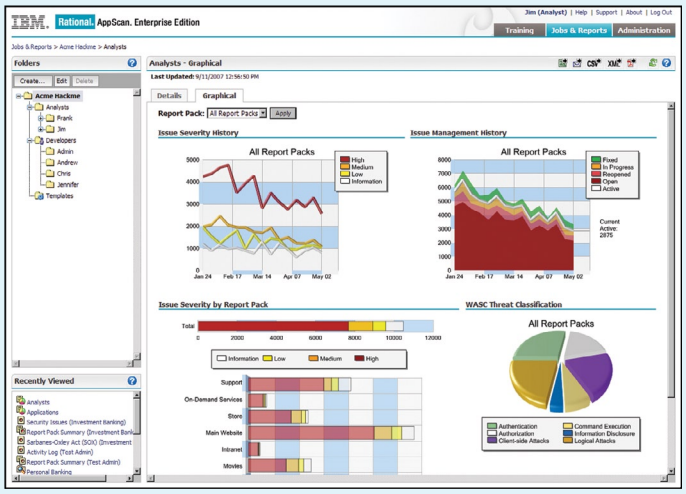
Because it integrates with leading testing systems, QA professionals can use Rational AppScan functionality in test scripts and conduct security checks within their familiar testing environments, facilitating the adoption of security testing along with functional and performance testing.

Scale application security testing across the enterprise with Rational AppScan Enterprise Edition software

With its Web-based architecture, Rational AppScan Enterprise Edition software is designed to help organizations distribute responsibility for security testing among multiple stakeholders and to help users uncover vulnerabilities early in the Web application delivery lifecycle—when they're easy and cost-efficient to fix.

In addition to the convenience and extensibility of centralized administration, the Rational AppScan Enterprise Edition offers:

- The ability to scan and test thousands of applications simultaneously on a complex Web site and retest them frequently, following changes.
- A simple quick-scan testing tool to execute administrator-defined scan templates for developers and other nonsecurity professionals, without desktop installation or configuration.
- A central data repository that automatically stores and aggregates test results for enterprise-wide access and multiple views. Users can segment and trend vulnerabilities by business unit, geography or third-party provider.
- A Web-based reporting console that provides role-based access to security reports and facilitates communication across the organization. Users can filter and prioritize issues and specify their status: open, in progress or closed.
- Executive dashboards and delta analysis reports highlight changes from one scan to the next, including fixed, pending and new security issues.
- Centralized controls for monitoring and controlling Web application vulnerability testing across the organization.
- Embedded WBT modules that explain issues and demonstrate the exploit, along with results verification to help facilitate understanding and communication of the vulnerabilities.



IBM Rational AppScan Enterprise Edition dashboard view

Rational AppScan Standard and Rational AppScan Enterprise capabilities available as SaaS

By accessing Rational AppScan capabilities as a managed service, you can take advantage of product benefits without the costs of adding staff or hardware.

A state-of-the-art security environment

With a focus on protecting your operating environment, these services are built with sophisticated security tools and techniques.

Your own dedicated security and compliance expert

As a Rational AppScan Standard or Rational AppScan Enterprise customer, you can engage an IBM Rational security analyst to help you:

- Configure and tune scans to help ensure coverage for each application.
- Review and analyze results to help eliminate false positives and negatives, identify patterns, prioritize key issues and highlight key remediation tasks.
- Track remediation progress by maintaining trend data, tracking resolution of key issues from scan to scan and reporting on remediation effectiveness.
- Train your QA staff to use Rational AppScan throughout the Web application delivery lifecycle and help build security and compliance management into your applications from the ground up.

Address organizational security and compliance management issues with Web-based training

The IBM Rational AppScan product family includes Web-based training, an online, self-paced training curriculum based on a decade of expertise, and best practices gleaned from hands-on customer deployments in challenging and complex Web environments. In addition to basic product instruction, the service provides targeted advice for developers, QA teams and security professionals.

Delivered online at 15-minute intervals and then archived, the service modules are accessible to users from any location, at any time. During special expert lab hours, users can also access realtime guidance from Rational AppScan security experts.

Online testing for three levels of product knowledge certification is available throughout the instructional process, and managers can track employee progress via a management dashboard available online and in the Rational AppScan Enterprise Edition.

System requirements

Processor	Intel® Pentium® P4, 1.5GHz (2.4GHz recommended)
Memory	512MB RAM (1GB recommended for scanning large sites)
Free disk space	1GB (10GB recommended for scanning large sites)
Network	One 10Mbps Network Interface Card)NIC) for network communication with configured TCP/IP (100 Mbps recommended)
Operating system	Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
Web browser	Microsoft Internet Explorer 5.5 or higher (6.0 or higher recommended)
	Microsoft .NET framework 2.0 or higher
	Java Runtime Environment (JRE) 5.0 (for Rational AppScan HTTP proxy only)

For more information

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

ibm.com/software/rational/offerings/testing/webapplicationsecurity

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

Produced in the United States of America
12-07

RAB14001-USEN-00