IBM Rational AppScan Standard Edition

■ *Facilitates accurate and auto-mated vulnerability scanning for complex Web applications and Web services including Adobe Flash, JavaScript and AJAX*

■ *Enables comprehensive appli-cation scanning coverage to identify vulnerabilities and generate detailed results to simplify remediation*

■ *Integrates Web-based training to provide insight into top security issues*

■ *Provides more than 40 out-of-the-box compliance reports to address regulatory requirements such as PCI, GLBA and HIPAA*

■ *Includes powerful manual testing features and the ability to record advanced test sequences*

■ *Assists in meeting key compliance standards such as PCI DSS*

Detecting Web application vulnerabilities and protecting sensitive data

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. Unfortunately, in the race to stay one step ahead of the competition, many organizations spend little to no effort to ensure that these applications are secure. Web-based systems can compromise the overall security of an organization by introducing vulner-abilities that hackers can use to gain access to confidential company infor-mation or customer data.

IBM Rational® AppScan® Standard Edition software scans and tests for a wide range of Web application vulnera-bilities, including those identified by the Web Application Security Consortium (WASC) threat classification. IBM Rational AppScan Standard Edition supports the latest Web 2.0 tech-nologies; parsing and execution of JavaScript and Adobe® Flash applica-tions; asynchronous JavaScript and

XML (AJAX) and Adobe Flex-related protocols such as JavaScript Object Notation (JSON), Action Message Format (AMF) and Simple Object Access Protocol (SOAP); elaborate service-oriented architecture (SOA) environments; and custom configuration and reporting capabilities for mashup- and process-driven applications.

Realizing cost savings using accurate, automated scanning

Rational AppScan Standard Edition significantly reduces the costs associ-ated with manual vulnerability testing. Whether you outsource your vulner-ability testing or perform it manually in-house, Rational AppScan Standard Edition dramatically reduces the time needed to perform a comprehensive vulnerability assessment of your applications. This enables you to evaluate your Web security posture on an ongoing basis, as opposed to performing quarterly or yearly audits, resulting in enhanced security levels and dramatically reduced costs.

The patented Rational AppScan Standard Edition scanning engine provides high levels of scan accuracy and dramatically limits false positives. To further improve accuracy and performance, it includes an adaptive test process that intelligently mimics human logic to adapt the testing phase to individual applications. Rational AppScan Standard Edition learns the application, down to the level of each specific parameter, and adjusts to perform only the tests that are relevant. To help ensure protection from the latest threats, Rational AppScan Standard Edition checks for attack signature updates from the IBM team of security research experts each time the software is launched.

Rational AppScan Standard Edition can also help organizations address critical compliance requirements such as Payment Card Industry Data Security Standard (PCI DSS) by providing a way to support an ongoing level of application security. IBM is an approved scanning vendor (ASV) with its Rational AppScan Standard Edition offering, making the software a perfect choice for addressing application security requirements around PCI DSS.

Providing quick results with features designed for ease of use

Not everyone is a security expert. That's why Rational AppScan Standard Edition integrates several ease-of-use features to help make Web vulnerability scanning easy for those who aren't. First, the scan configuration wizard walks each user through the process of setting up an initial scan: prompting for basic information such as a starting IP address or domain, querying which type of scanning profile should be used and soliciting any required login information. Next, the scan expert feature performs a settings check and makes any final configuration recommendations such as turning on Java™ parsing to support environments using JavaScript. Rational AppScan Standard Edition then begins the test phase and returns vulnerability results and remediation recommendations. The results expert runs and returns helpful tips and screenshots to clearly illustrate each issue. To increase the security knowledge of your organization, IBM offers Rational Web-based training modules that cover a variety of security topics.
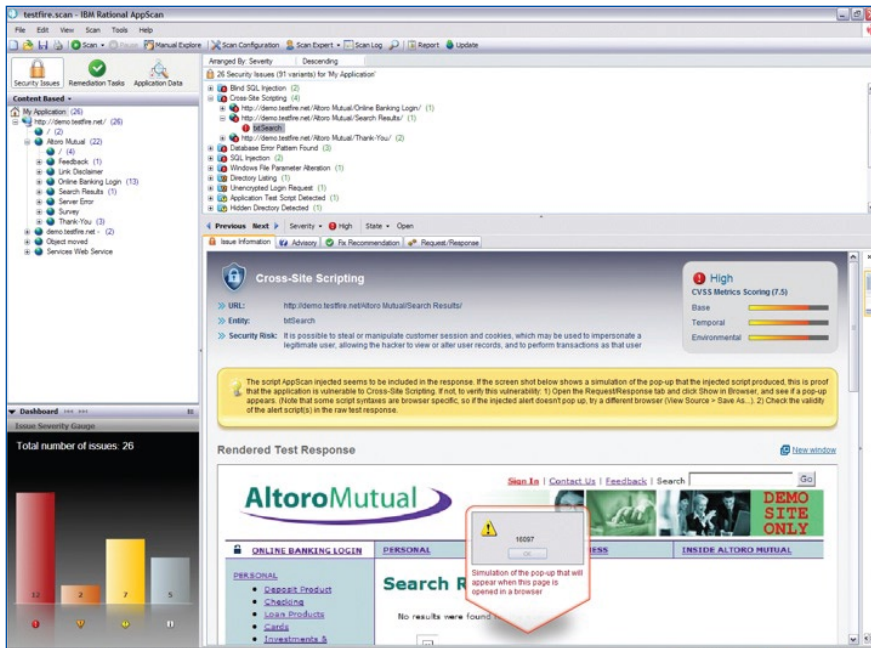
Streamlining remediation with prioritized results and fix recommendations

One of the most critical aspects of Web vulnerability scanning is the quick remediation of issues. Rational AppScan Standard Edition provides a fully prioritized list of the vulnerabilities found with each scan, which enables high-priority problems to be fixed first, helping organizations focus on what matters the most from a security perspective. Each vulnerability result includes a full description of how the vulnerability works and the potential causes. Integrated Web-based training provides short training modules directly from the user interface. The software's remediation view then explains the steps required to remediate the issue, including examples of both secure and insecure code.

Gaining insight into key security and compliance issues

Rational AppScan Standard Edition can produce custom security reports and includes the ability to select which data points should be included in each report. Users can also choose from more than 40 predefined reports and map scan results to key industry and regulatory compliance standards. These include National Institute of Standards and Technology Special Publication (NIST SP) 800-53 and the Open Web Application Security Project (OWASP) top 10, PCI DSS, Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP).

IBM Rational AppScan Standard Edition can help users quickly identify, understand and fix critical Web vulnerabilities.

For increased insight and visibility, organizations can easily add the IBM Rational AppScan Reporting Console to their existing Rational AppScan Standard Edition deployment. The Rational AppScan Reporting Console utilizes a scalable enterprise architecture that provides role-based reporting access and aggregates scan data from multiple instances of IBM Rational AppScan Standard Edition. By providing in-depth, yet easy-to-understand dashboards and flexible reporting views, the Rational AppScan Reporting Console provides enterprise-wide visibility into risks and continuous updates on remediation progress.

Customizing and extending your testing for greater control

Rational AppScan Standard Edition includes a set of powerful customization features for greater control over Web vulnerability testing in your environment.

- *IBM Rational AppScan software development kit (SDK) offers a powerful set of interfaces that enable customizable invocation of each action in Rational AppScan Standard Edition, from the execution of a long scan to the submission of an individual custom test. This platform enables easy integrations into existing systems, supports advanced custom uses of the Rational AppScan engine and provides the foundation for the Rational AppScan eXtensions Framework and Pyscan.*

- *IBM Rational AppScan eXtensions Framework is a flexible framework that can help users load software add-ons to extend the functionality of Rational AppScan Standard Edition. The framework helps open up Rational AppScan Standard Edition, enabling users to customize and enhance existing functionality to fit their own processes, automate in-house activities and receive a large number of additional features and functionality by downloading open source extensions from the Rational AppScan eXtensions community portal (ibm.com/ developerworks/rational/downloads/ 08/appscan_ext_framework).*

- *The Pyscan Web application security testing platform is built on Rational AppScan and the Python scripting language. Pyscan can help an auditor better utilize Rational AppScan Standard Edition functionality when performing a manual audit. Rational AppScan Standard Edition advanced session management capabilities can be used to establish and maintain login state, and an easily accessible repository of scanned application data and powerful reporting abilities is readily available. Pyscan can dramatically increase the efficiency of the manual portion of an audit without eliminating the irreplaceable expertise of the auditor.*

IBM Rational AppScan Standard Edition system requirements

Processor	
Intel® Pentium® P4 processor, 2.4GHz	
Memory	
1GB RAM	
Free disk space	
10GB	
Network	
One network interface controller (NIC) with 100Mbps	
Operating system	
• Microsoft® Windows® XP Professional edition, Service Pack 2 (SP2) and SP3	
• Microsoft Windows Vista Ultimate and Enterprise editions, SP2	
• Microsoft Windows 2003 Enterprise edition, SP2	
Web browser	
Microsoft Internet Explorer 6.0 or higher	
Integrated development environment	
Microsoft .NET Framework, version 2.0 (version 3.0 recommended), SP1	
Flash Player	
Adobe Flash Player, version 9.0.124.0 or higher	

For more information

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

ibm.com/software/awdtools/appscan/standard