Achieve uncompromising levels of Web application security for your midsize businesses

Rational. software

IBM Rational AppScan Express Edition

Highlights

- ***Enables comprehensive and regular testing for Web vulnerabilities with limited resources***
- ***Dramatically reduces the need for manual testing, which can produce significant cost savings***
- ***Helps nonsecurity experts perform security scans and fix vulnerabilities at the source***
- ***Automatically scans complex Web applications using Web 2.0 technologies such as Adobe Flash, JavaScript and AJAX***
- ***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 vulnerabilities that hackers can use to gain access to confidential company information or customer data.

IBM Rational® AppScan® Express Edition software scans and tests for a wide range of Web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. IBM Rational AppScan Express Edition supports the latest Web 2.0 technologies; parsing and execution of JavaScript and Adobe® Flash applications; 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 Express Edition makes comprehensive Web vulnerability testing a reality for midsize organizations by delivering the core security features found in IBM Rational AppScan Standard Edition in a specially tailored, cost-effective solution. Rational AppScan Express Edition can significantly reduce the time and costs associated with manual vulnerability testing, enabling you to focus on other IT and security-related needs within your organization. Whether you currently outsource your vulnerability testing or perform tests in-house, Rational AppScan Express Edition can dramatically reduce the time needed to conduct a thorough vulnerability assessment of your applications. By allowing you to evaluate your Web security posture on an ongoing basis, as opposed to performing quarterly or yearly audits, the software can yield much higher levels of security and, at the same time, help dramatically reduce costs.

The patented Rational AppScan Express Edition scanning engine supports high levels of scan accuracy and 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 each individual application. Rational AppScan Express Edition learns the application down to the level of each specific parameter, adjusting to perform only the tests that are relevant. To help ensure protection from the latest threats, Rational AppScan Express Edition checks for attack signature updates from the IBM team of security research experts each time the software is launched.

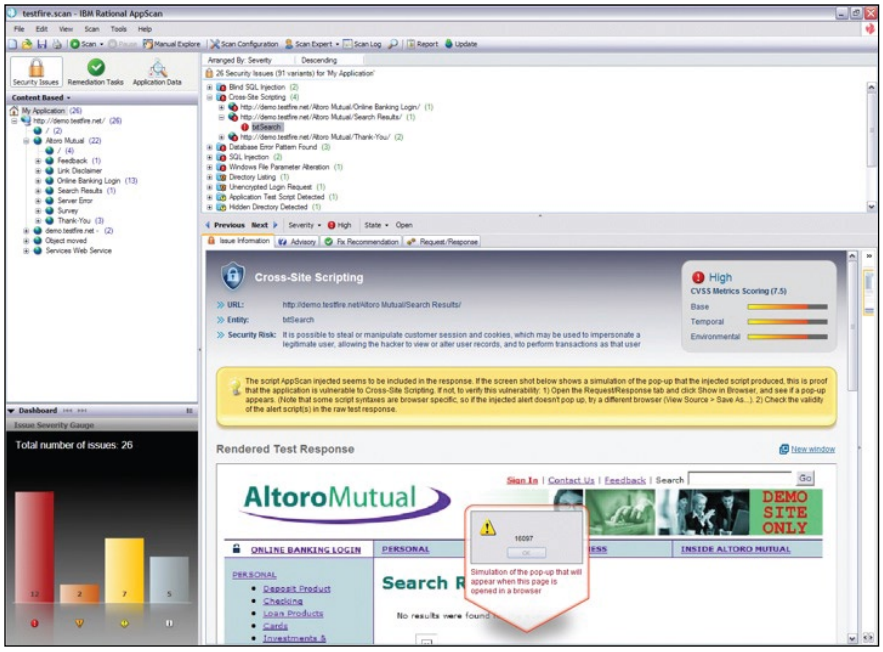
Rational AppScan Express Edition can also help organizations address critical compliance requirements such as Payment Card Industry Data Security Standards (PCI DSS) by providing a way to support an ongoing level of application security. IBM is an Approved Scanning Vendor (ASV) with its Rational AppScan Express Edition offering, making the software suited 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 Express Edition integrates several ease-of-use features to help make Web vulnerability scanning easy for nonsecurity experts. 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 Express 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 Express 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 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.



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

Gaining insight into key security and compliance issues

Rational AppScan Express 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, mapping 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, the Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA), the Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP).

For increased insight and visibility, organizations can easily add the IBM Rational AppScan Reporting Console to their existing Rational AppScan Express Edition deployment. The Rational AppScan Reporting Console uses a scalable enterprise architecture that provides role-based reporting access and aggregates scan data from multiple instances of Rational AppScan Express 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.

IBM Rational AppScan Express 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 (IDE):*** *Microsoft .NET Framework, version 2.0 (version 3.0 recommended), SP1*
- ***Flash Player****: Adobe Flash Player, version 9.0.124.0 or higher*

Customizing and extending your testing for greater control

Rational AppScan Express 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 Express Edition, from the execution of a long scan to the submission of an individual custom test. This platform enables easy integration into existing systems, supports advanced custom uses of the Rational AppScan engine and provides the foundation for IBM Rational AppScan eXtensions Framework and Pyscan applications.*
- *Rational AppScan eXtensions Framework is a flexible framework that can help users load software add-ons to extend the functionality of Rational AppScan Express Edition. The framework helps open up Rational AppScan Express 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 IBM developerWorks® site (www.ibm.com/developerworks/rational/products/appscan).*
- *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 Express Edition functionality when performing a manual audit. Rational AppScan Express Edition advanced session management capabilities can be used to establish and maintain login states, and an easily accessible repository of scanned application data and powerful reporting tools is readily available. Pyscan can dramatically increase the efficiency of the manual portion of an audit without eliminating the irreplaceable expertise of the auditor.*

For more information

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

ibm.com/software/awdtools/appscan/express

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

Produced in the United States of America
February 2009

RAD14020-USEN-01