



Rational software

Proactively detect, remediate and report Web application security vulnerabilities with Rational AppScan software.

Highlights

- **Enables agencies and departments to more easily meet OMB FISMA compliance**
- **Helps federal agencies better understand exposure to security threats**
- **Provides detailed, actionable security vulnerability information through a standard Web browser**
- **Measures assessment processes to remediate defects**

Reporting and remediating security risk

As foreign countries and global cyber villains became more persistent and sophisticated in their ability to attack government networks, the United States House and Senate passed the Federal Information Security Management Act (FISMA). Part of the E-Government Act of 2002, FISMA initially focused on network security for government agencies and departments, requiring them to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

In 2006, FISMA was rewritten to include privacy compliance mandates that require agencies to conduct reviews of how personally identifiable information (PII) about individuals is handled when IT is used to collect it.

Today, two security reports are required—FISMA and National Institute of Standards and Technology (NIST) 800-53A. As stipulated in Section 208 of the Privacy Impact Assessment (PIA), four privacy reports are required: privacy statement, collection of PII (detailing how users are being tracked), Platform for Privacy Preferences (P3P) project and persistent cookies.

A significant challenge facing departments and agencies is the ability to meet Office of Management and Budget (OMB) FISMA Plan of Action and Milestone (POAM) reporting in consistent OMB formats. Quarterly, FISMA reports must be filed with the OMB. These reports are used by oversight committees to grade the filing agencies. Based on the results of the audits, consequent budget allocations

may be determined. Recently, FISMA began requiring agencies to report to the OMB the tools and technologies they are using for incident detection, which means you, like many other IT heads at government agencies, are even more challenged by the lengthy, stringent identification and compliance reporting process. Ensuring that your own Web applications are secure from common vulnerabilities requires vigilance, technology and time. But now you have to meet OMB reporting guidelines that require labor-intensive, time-consuming and tedious paper-based processes.

Providing agency-wide visibility and control for Web applications

IBM Rational® AppScan® Enterprise Edition software is designed to identify Web application security vulnerabilities and enable you to take a proactive approach to online risk management. Rational AppScan Enterprise Edition analyzes Web sites by running thousands of platform- and application-specific tests to detect hundreds of types of vulnerabilities. It combines sophisticated security algorithms with enterprise scanning, reporting and trending capabilities.

Rational AppScan Enterprise Edition is one of the only products in the marketplace that can help you meet FISMA reporting requirements at the application layer. Competitors' solutions enable security and vulnerability reporting, but they do not presently have privacy compliance reporting; or they offer compliance reporting, but not security reporting.

The Rational AppScan Enterprise Edition solution provides three levels of FISMA reporting:

- **Security vulnerabilities.** *Rational AppScan Enterprise Edition identifies weaknesses such as cross-site scripting and structured query language (SQL) injection that can expose your agency to online security risk.*
- **Worst-case scenarios.** *The Rational software provides a textual description of what a hacker could do with the information made available by the online security vulnerability.*

- **Custom security standards.** *Rational AppScan Enterprise Edition enables you to map to internal security standards as well as FISMA, NIST 800-53A, Director of Central Intelligence Directive (DCID) 6/3 Information Assurance, and Security Content Automation Protocol (SCAP).*

IBM Rational AppScan Enterprise Edition simplifies the FISMA process by automating Web application security auditing and POAM reporting in consistent OMB formats. Following is a list of some of the FISMA reports that Rational AppScan Enterprise Edition can help you produce:

- *Authentication reports that address authentication points, unsecured login forms, unprotected resources, weak passwords, exposed passwords in URLs and exposed passwords in forms*
- *Session management reports that address session token length, session tokens in persistent cookies, session token reuse over Secure Sockets Layer (SSL) and non-SSL*
- *Input validation reports that address SQL injection and cross-site scripting*
- *Parameter manipulation reports that address exposed server-side code, hidden field manipulation and cookie manipulation*

Meeting the challenges of

FISMA compliance

Using Rational AppScan Enterprise Edition, you can automate the processes of identifying Web security vulnerabilities and addressing FISMA compliance guidelines. The Rational software provides a framework that can enhance the efficiency and effectiveness of information security in the federal government by automatically scanning for exposure points at the Web server and application layers as part of the application development process. Rational AppScan Enterprise Edition can also detect and identify resources to accurately perform risk and compliance audits. And, since various stakeholders in the development lifecycle require different types of data, Rational AppScan intelligent management dashboards—as well as detailed reports available via a Web browser—are designed to communicate exposures, FISMA

defects and actionable information. Rational AppScan Enterprise Edition drives FISMA compliance reporting in a number of ways:

- *Measure your assessment process/FISMA defect remediation.*
 - *Analyze exposure from individual assessments and compare results across the cycle.*
 - *Validate success and maintain accountability.*
 - *Implement system auditing to address reporting requirements.*
- *Contain costs through automation.*
 - *Automatically check potentially millions of Web pages for hundreds of issues with sophisticated scanning technology.*
- *Address e-government policies regarding information privacy.*
 - *Populate POAM reports appropriate for OMB.*
 - *Improve government auditing scores by enhancing your implementation of the Federal Enterprise Architecture (FEA).*

Experience that gets results

The skilled consultants at IBM offer best practices expertise and will work with you to determine your Web site architecture and FISMA audit and development practices to create FISMA reports that best meet the OMB reporting guidelines for compliance. Certified information systems security personnel (CISSP) and certified information privacy professional/government (CIPP/G) professionals, Rational AppScan consultants can help you manage the security and privacy issues that are most important to your organization, as well as increase users' confidence and trust in your online channel.

For more information

To learn more about addressing FISMA compliance guidance with IBM Rational AppScan Enterprise Edition software, contact your IBM sales representative or IBM Business Partner, or visit:

ibm.com/software/awdtools/appscan/enterprise



© Copyright IBM Corporation 2009

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

Produced in the United States of America
January 2009
All rights reserved

IBM, the IBM logo, ibm.com, Rational, and AppScan are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.