Minimize your financial institution's risk with solutions from IBM

Web application security and compliance solutions to support your business objectives

Highlights

- Identify and remediate vulnerabilities in web applications and services before they are deployed
- Perform static analysis security testing to identify vulnerabilities within your source code as it's being developed
- Verify compliance with common financial services and industry regulations
- Automate to help improve web application scanning coverage and developer and tester productivity

It's a disaster waiting to happen

At a time when financial institutions are becoming more reliant on web technology to deliver innovative features and services to their customers, hackers are increasingly targeting web applications. According to a recent IBM® Internet Security Systems X-Force research and development team report, 49 percent of all vulnerabilities disclosed so far are web application vulnerabilities[1]

Undetected vulnerabilities in web applications or web services can leave financial institutions at risk of security breaches from external or even internal sources. The opportunity to introduce risk increases with the growing variety of devices allowing customers to access their financial data as well, And network security measures such as firewalls and intrusion detection systems don't address the risks presented by vulnerable web applications, which often expose valuable and confidential back-end resources, such as databases that contain confidential customer data.

Unfortunately, these aren't the only issues financial institutions are facing. Compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act can be a challenge. You need to find a cost-effective way to protect your systems, applications, private data and customer information while supporting compliance with applicable regulations. If you fail to protect your valuable data and adhere to regulations, the consequences to your bottom line and your brand can be devastating. The consequences range from heavy financial penalties and lost revenue to system outages that can and will most likely erode customer confidence and damage your institution's reputation.

To avoid these scenarios, you need to have a comprehensive security and compliance strategy in place. The IBM Rational® application security portfolio provides comprehensive security and compliance capabilities for complex web and networked applications that are imperative today.

"Despite the enormous number of attacks and despite widespread publicity about these vulnerabilities, most web site owners fail to scan effectively for common flaws and become unwitting tools used by criminals to infect the visitors who trusted those sites to provide a safe web experience."[2]

— The SANS Institute

This software suite scans and tests for common web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. IBM Rational AppScan® software shares 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 Adobe® Flash technology and advanced JavaScript™ languages, coupled with comprehensive support for the a synchronous JavaScript and XML (AJAX) programming language.

A comprehensive security and compliance solution for web and networked applications

IBM Rational AppScan Source Edition software provides static analysis security testing that enables you to identify vulnerabilities within your source code, review data flows and identify the threat exposure of each of your applications—during development. By managing your security policies, you'll have the ability to take action on priority vulnerabilities. By testing your applications as they're being developed, you can gain an understanding of your threat exposure at the executive level for audit and compliance purposes and throughout the software development life cycle. You can also address vulnerabilities earlier, which can help reduce costs. The Rational AppScan portfolio enables you to deploy application security testing—using both dynamic and static analysis techniques—that is integrated across the software delivery cycle.

Providing support for your compliance efforts

As web application security threats become both more prevalent and complex, many industry groups are acknowledging the need to comprehensively address this problem in order to protect sensitive data. Many industry standards now explicitly require organizations to protect their business critical web infrastructures including addressing web application vulnerabilities. The Rational AppScan family of solutions provides a cost effective, proactive solution to help organizations meet web application security requirements related to global compliance standards such as the Payment Card Industry Data Security.

Your institution can assess its compliance with key industry and regulatory requirements, including the PCI DSS, COPPA, GLBA, Sarbanes-Oxley Act, Freedom of Information and Protection of Privacy Act (FIPPA) and Payment Application Best Practices (PABP). Plus, users can produce custom security reports and select which data points should be included in each report, making it possible to address critical compliance requirements. Using these features, you can provide assurance to your customers that their valuable data is protected.

Enabling you to do more with less

Consumers expect the most convenient and innovative applications and services. To be able to deliver them—and deliver them quickly—you have to find a way to become more efficient. By automating your security and compliance testing, you can free your developers and testers for more value-generating tasks. Which means your organization will be better positioned to focus on innovation.

Reducing costs and improving scan coverage using automation

Your institution likely already has governance policies designed to ensure that your websites comply with relevant legislation. However, the size of today's websites—which can

include thousands of pages—combined with an increasing volume of rules and updates, makes manual compliance checking far too time consuming and expensive to be feasible. Nor can visual checks reveal all potential security flaws and vulnerabilities. Support from automated scanning tools that can quickly check and monitor complex websites is a necessity for those that need to reduce their exposure to security vulnerabilities. Automated support can yield other benefits as well, such as fewer technical support requests, fewer abandoned web sessions and greater consumer trust in your online channel. Collectively, these changes help boost confidence in your brand and improve customer retention.

Challenge: One company needed to create security-rich applications that could handle the clearance and settlement of more than US$1 quadrillion in securities transactions per year. With such a large amount of money at stake, the company needed to be able to implement rigorous security practices as part of its application development process.
Solution: The company educated its application developers on building security into the web application development life cycle, using Rational AppScan offerings to identify, analyze and remediate security issues from early development through live deployment.
Benefits: The company is now able to perform automated security, compliance and integration testing on its web-based applications, while adding roughly 225 new applications per year, improving its developer productivity and speeding time to market for new applications.

A market-leading suite of security and compliance solutions

The IBM Rational AppScan suite of market-leading web application security and compliance applications can help address the critical challenge of application security and compliance. All of the solutions provide scanning, reporting and fix recommendation functionalities. And they're all designed to be efficient and easy to use. So whether your people are just getting started with web application security or are advanced users who can create custom add ons to extend your company's testing capabilities, they'll be able to take advantage of the Rational AppScan portfolio.

End-to-end web application security made easier by IBM

You need an integrated solution from a trusted vendor that provides a holistic and cost-effective approach to IT security. IBM offers a security solution that can help you reduce risk for web-enabled applications, websites and web traffic, while protecting your service-oriented architecture (SOA) environments.

- Discover application vulnerabilities and how to fix them using Rational AppScan software.
- Help protect applications from potential attacks with IBM Proventia® web application security software.
- Protect XML and web services traffic, as well as SOA deployments, with the IBM WebSphere® DataPower® SOA Appliances.
- Help ensure that only authorized users have the appropriate access to web applications with IBM Tivoli® Access Manager software.

Your business is only as secure as the applications that support it. By combining software and hardware solutions with professional and managed services, IBM can help your institution adopt a comprehensive approach to web application security. The considerable benefits of web application security solutions from IBM can help your business:

- Reduce the risk of web application: Outage, defacement or data theft.
- Improve your ability to address compliance requirements.
- Protect your brand and reputation.
- Enhance your ability to integrate business-critical applications.
- Lower long-term security costs by focusing on building security features into application development and delivery, instead of retrofitting them after the fact.

IBM has highly skilled experts with broad knowledge and deep technical skills, including:

- Thousands of researchers, developers and SMEs on security initiatives (Data Security Steering Committee, Security Architecture Board, Secure Engineering Framework).
- Thousands of security & risk management patents.
- Hundreds of security customer references.
- Years of proven success securing the zSeries® environment.

For more information

To learn more about IBM Rational security and compliance solutions for the financial services industry, contact your IBM representative, or visit: **ibm.com**/software/rational/solutions/financial

To learn more about solutions for comprehensive application security from IBM, visit: **ibm.com**/security/application-process.html

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

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

Produced in the United States of America
August 2010

[1] IBM X-Force 2009 Trend and Risk Report http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[2] The SANS Institute, "The Top Cyber Security Risks," (http://www.sans.org/top-cyber-security-risks), September 2009.

Please Recycle

Rational. software

RAS14057-USEN-00