Strategic protection for Web applications
To support your business objectives

Rational software

IBM Rational AppScan: enhancing Web application security.

Are vulnerable applications putting your business at risk?

Many organizations depend on Web-based software to run their business processes, conduct transactions and deliver increasingly sophisticated services to customers. Every application destined for online deployment should address security issues as an integral part of the software delivery process. Unfortunately, in the race to meet deadlines and stay ahead of the competition, many businesses have failed to perform adequate security testing, and the resulting vulnerabilities have provided ample opportunity for hackers to access or steal corporate or personal data—placing the entire business at risk.

A suite of marketplace-leading Web application security solutions, IBM Rational® AppScan software is used across an organization's software development lifecycle to increase visibility and control—helping to address the critical challenge of application security. The suite includes the following software:

- IBM Rational AppScan Standard Edition
- IBM Rational AppScan Express Edition
- IBM Rational AppScan Tester Edition
- IBM Rational AppScan Developer Edition
- IBM Rational AppScan Build Edition
- IBM Rational AppScan Enterprise Edition
- IBM Rational AppScan SaaS solutions
- IBM Rational AppScan Reporting Console
- IBM Rational Web Based Training for AppScan

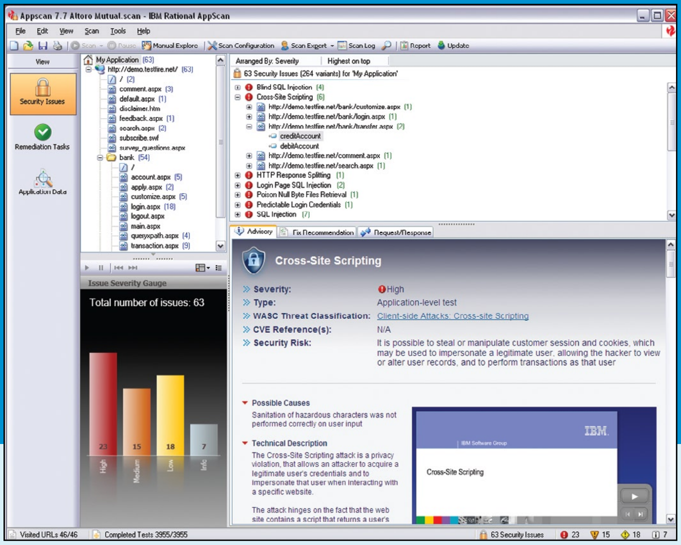
Each of these solutions provides scanning, reporting and fix recommendation functionality, and each is designed for a variety of users, including information security managers, penetration testers, security auditors, application developers, build managers and quality assurance (QA) teams.

Protect critical Web-based business assets

Offering comprehensive security capabilities for complex Web applications, the Rational AppScan software suite scans and tests for common Web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. 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 Adobe® Flash technology and advanced JavaScript languages, coupled with comprehensive support for the Asynchronous JavaScript and XML (AJAX) programming language.

Rational AppScan core features for scanning efficiency and ease of use

- The user interface provides a view selector for the application tree, along with hierarchical security issues results lists, developer remediation views and details panes.
- An adaptive test process enables users to analyze application parameters and select only relevant tests that do not impede the development process.
- Complex authentication support enables testing for multistep authentication procedures.



Appscan 7.7 Altoro Mutual.scan - IBM Rational AppScan

My Application (63)
http://demo.testfire.net/ (63)
/ (2)
comment.aspx (3)
default.aspx (1)
disclaimer.htm
feedback.aspx (1)
search.aspx (2)
subscribe.swf
survey_questions.aspx
bank (54)
/
account.aspx (5)
apply.aspx (2)
customize.aspx (5)
login.aspx (18)
logout.aspx
main.aspx
queryxpath.aspx (4)
transaction.aspx (9)

Total number of issues: 63

Arranged By: Severity | Highest on top

63 Security Issues (264 variants) for 'My Application'

Blind SQL Injection (4)
Cross-Site Scripting (6)
http://demo.testfire.net/bank/customize.aspx (1)
http://demo.testfire.net/bank/login.aspx (1)
http://demo.testfire.net/bank/transfer.aspx (2)
creditAccount
debitAccount
http://demo.testfire.net/comment.aspx (1)
http://demo.testfire.net/search.aspx (1)
HTTP Response Splitting (1)
Login Page SQL Injection (2)
Poison Null Byte Files Retrieval (1)
Predictable Login Credentials (1)
SQL Injection (7)

Cross-Site Scripting

Severity: High
Type: Application-level test
WASC Threat Classification: Client-side Attacks: Cross-site Scripting
CVE Reference(s): N/A
Security Risk: It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Possible Causes
Sanitation of hazardous characters was not performed correctly on user input

Technical Description
The Cross-Site Scripting attack is a privacy violation, that allows an attacker to acquire a legitimate user's credentials and to impersonate that user when interacting with a specific website.

The attack hinges on the fact that the web site contains a script that returns a user's

IBM. | IBM Software Group
Cross-Site Scripting

Visited URLs 46/46 | Completed Tests 3955/3955 | 63 Security Issues | 23 | 15 | 18 | 7

The IBM Rational AppScan security advisory view

- Advanced session management performs automatic re-logins when required.
- Realtime results views enable users to act on issues before a scan is complete.
- Prebuilt pattern search rules facilitate security testing around credit card, social security or other numerical sequences.

Rational AppScan core features for customization and control

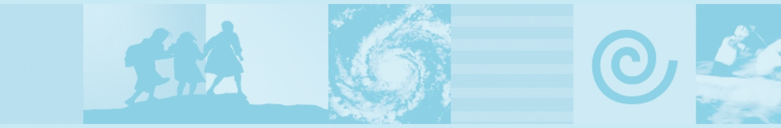
- IBM Rational AppScan eXtensions Framework technology helps users create, share and load powerful add-ons that extend testing capabilities.
- Pyscan, which couples Rational AppScan software with the capabilities of Python scripts, lets users leverage scanning capabilities without the limitations of a user interface.
- Rational AppScan software development kit (SDK) helps users 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

- Coverage for global validation analyzes test responses for inadvertently triggered issues, Secure Sockets Layer (SSL) certificate testing and cross-site request forgery (CSRF) testing.
- Hacker simulations aid in the search for current, known vulnerabilities.
- Notifications on the latest threats are delivered automatically when users launch a Rational AppScan application.
- A bundled utility suite helps penetration testers and security consultants develop, test and debug Web applications.

Rational AppScan core features for reporting and remediation

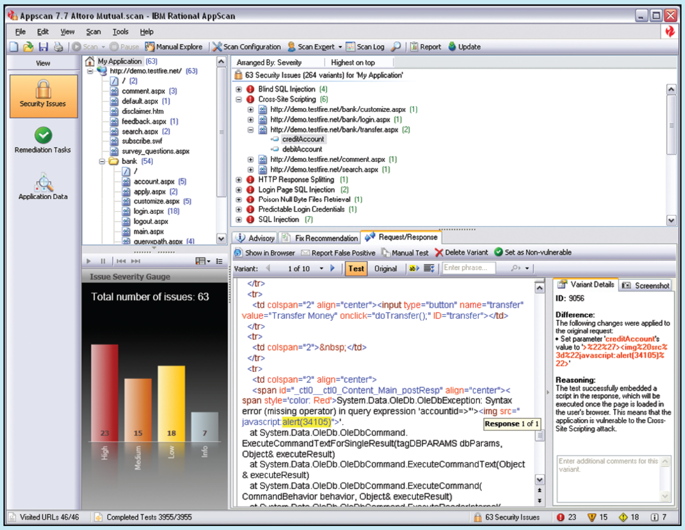
- Tests are related to more than 40 global regulatory compliance issues and standards.
- Validation highlighting pinpoints HTML code containing vulnerabilities, explains the issue and suggests modified HTML code to eliminate it.
- Remediation reports include Hypertext Preprocessor (PHP) fix recommendations and developer task lists. These reports also enable users 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 list items such as sensitive data in HTML comments, as well as HTTP activity around suspicious content.
- Test descriptions include identifications for common vulnerabilities and exposures (CVEs) from the vulnerability database maintained by IBM.
- The software can incorporate screenshots from the internal browser into reports, and it can extract, compress and encrypt information from specific tests for sending via e-mail.
- The software submits reports of false positive (or negative) incidents to the IBM Rational AppScan security research team, helping to continually improve the product.



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

Automating Web application testing processes to help security auditors and penetration testers quickly and efficiently do their jobs requires sophisticated and intelligent scanning technologies. Rational AppScan Standard Edition, available as a desktop application or as software as a service (SaaS), includes features designed to support moderate and power users. Features include:

- The scan expert, a wizard tool that 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 carts and order 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.
- Embedded Web-based training modules that help explain issues and demonstrate exploits.



My Application (63)
http://demo.testfire.net/ (63)
/ (2)
comment.aspx (3)
default.aspx (1)
disclaimer.htm
feedback.aspx (1)
search.aspx (2)
subscribe.swf
survey_questions.aspx
bank (54)
/
account.aspx (5)
apply.aspx (2)
customize.aspx (5)
login.aspx (18)
logout.aspx
main.aspx
queryxpath.aspx (4)

63 Security Issues (264 variants) for 'My Application'
Blind SQL Injection (4)
Cross-Site Scripting (6)
http://demo.testfire.net/bank/customize.aspx (1)
http://demo.testfire.net/bank/login.aspx (1)
http://demo.testfire.net/bank/transfer.aspx (2)
creditAccount
debitAccount
http://demo.testfire.net/comment.aspx (1)
http://demo.testfire.net/search.aspx (1)
HTTP Response Splitting (1)
Login Page SQL Injection (2)
Poison Null Byte Files Retrieval (1)
Predictable Login Credentials (1)
SQL Injection (7)

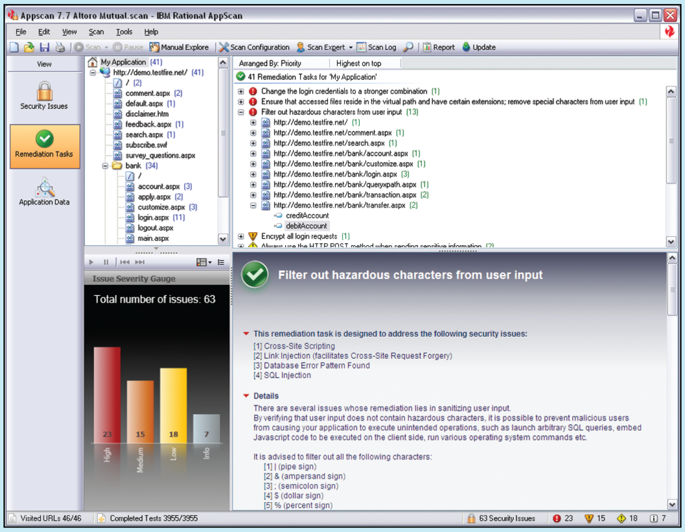
```
  </tr>
  <tr>
    <td colspan="2" align="center"><input type="button" name="transfer"
value="Transfer Money" onclick="doTransfer();" ID="transfer"></td>
  </tr>
  <tr>
    <td colspan="2">&nbsp;</td>
  </tr>
  <tr>
    <td colspan="2" align="center">
    <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><
span style='color: Red'>System.Data.OleDb.OleDbException: Syntax
error (missing operator) in query expression 'accountid=>"'><img src="
javascript:alert(34105)">'.
   at System.Data.OleDb.OleDbCommand.
ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams,
Object& executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object
& executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(
CommandBehavior behavior, Object& executeResult)
```

ID: 9056

Difference:
The following changes were applied to the original request:
- Set parameter 'creditAccount''s value to '>%22%27><img%20src%3d%22javascript:alert(34105)%22>'

Reasoning:
The test successfully embedded a script in the response, which will be executed once the page is loaded in the user's browser. This means that the application is vulnerable to the Cross-Site Scripting attack.

The IBM Rational AppScan security issues view



My Application (41)
http://demo.testfire.net/ (41)
/ (2)
comment.aspx (2)
default.aspx (1)
disclaimer.htm
feedback.aspx (1)
search.aspx (1)
subscribe.swf
survey_questions.aspx
bank (34)
/
account.aspx (3)
apply.aspx (2)
customize.aspx (3)
login.aspx (11)
logout.aspx
main.aspx

41 Remediation Tasks for 'My Application'
Change the login credentials to a stronger combination (1)
Ensure that accessed files reside in the virtual path and have certain extensions; remove special characters from user input (1)
Filter out hazardous characters from user input (13)
http://demo.testfire.net/ (1)
http://demo.testfire.net/comment.aspx (1)
http://demo.testfire.net/search.aspx (1)
http://demo.testfire.net/bank/account.aspx (1)
http://demo.testfire.net/bank/customize.aspx (1)
http://demo.testfire.net/bank/login.aspx (3)
http://demo.testfire.net/bank/queryxpath.aspx (1)
http://demo.testfire.net/bank/transaction.aspx (2)
http://demo.testfire.net/bank/transfer.aspx (2)
creditAccount
debitAccount
Encrypt all login requests (1)
Always use the HTTP POST method when sending sensitive information (2)

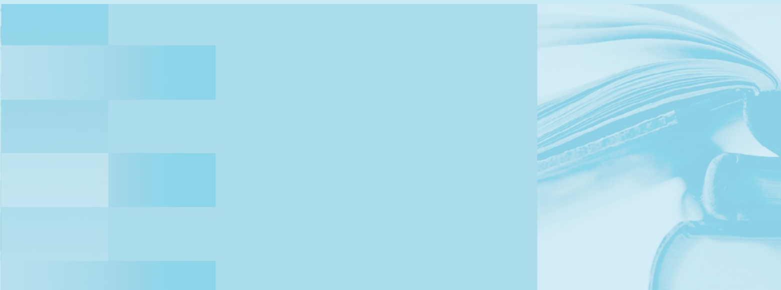
Filter out hazardous characters from user input

This remediation task is designed to address the following security issues:
[1] Cross-Site Scripting
[2] Link Injection (facilitates Cross-Site Request Forgery)
[3] Database Error Pattern Found
[4] SQL Injection

Details
There are several issues whose remediation lies in sanitizing user input.
By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:
[1] | (pipe sign)
[2] & (ampersand sign)
[3] ; (semicolon sign)
[4] $ (dollar sign)
[5] % (percent sign)

The IBM Rational AppScan remediation view



Gain robust Web application security features with Rational AppScan Express Edition software

Organizations with small or limited application development teams also need to consider security testing as part of the development lifecycle. Yet these organizations often have to sacrifice functionality for affordability. Rational AppScan Express Edition meets the requirements of midsize organizations by delivering the uncompromising security testing functionality found in IBM Rational AppScan Standard Edition at an attractive price point. Designed for ease of deployment, Rational AppScan Express Edition significantly reduces the time and costs associated with manual vulnerability testing, allowing your teams to focus on other IT and security-related needs within your organization.

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

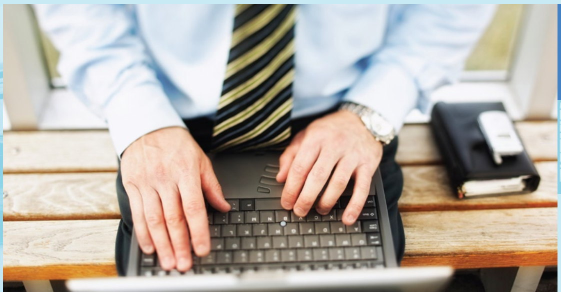
Rational AppScan Tester Edition, available as a desktop application, offers capabilities to help QA teams integrate security testing into existing quality management processes, thereby easing the burden on security professionals. Because Rational AppScan Tester Edition integrates with leading testing systems, QA professionals can use its functionality in test scripts and can conduct security checks within their familiar testing environments, facilitating the adoption of security testing along with functional and performance testing.

Embed security testing seamlessly into your development environment with Rational AppScan Developer Edition software

The most efficient way to stay ahead of application security vulnerabilities is to build software securely from the ground up. The challenge is that most developers are not security experts, and writing security-rich code is not always their top priority. So the best way to engage development in the process of application security is to provide them with tools that work in their environment and that generate results in languages they understand.

Rational AppScan Developer Edition is designed to empower developers to invoke Web application security testing right from within their development environment. It enables the development organization to address the volume of security issues that can be introduced in code, streamlining the development lifecycle workflow and helping to reduce costly security testing bottlenecks that can occur at the end of the release cycle.

Rational AppScan Developer Edition uses a range of analysis techniques to accurately pinpoint security issues in your Web applications, including static code analysis, dynamic analysis, run-time analysis and IBM patent-pending string analysis.



Automate security testing with Rational AppScan Build Edition software

Rational AppScan Build Edition supports automated security testing at the build stage of the software development lifecycle. By integrating with multiple build management systems, such as IBM Rational Build Forge® software, it provides security testing coverage for scheduled builds. It also routes the results back to development though defect-tracking solutions such as IBM Rational ClearQuest® software, or through security reporting solutions such as Rational AppScan Enterprise Edition or Rational AppScan Reporting Console.

Rational AppScan Build Edition includes the same set of analysis techniques as the Rational AppScan Developer Edition, providing a high level of accuracy plus code coverage that helps you identify which code has been tested.

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

With its Web-based architecture, Rational AppScan Enterprise Edition is designed to help organizations distribute responsibility for security testing among multiple stakeholders. The software is also available as SaaS, allowing you to easily add users as needed, as well as gain better control of costs.

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

- The ability to scan and test thousands of applications simultaneously on a complex Web site and retest them frequently, following changes.
- A 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.
- A Web-based reporting console that provides role-based access to security reports and facilitates communication across the organization.
- Executive dashboards and delta analysis reports that 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 Web-based training modules that help explain issues and demonstrate exploits.

Access centralized reporting on Web application vulnerability data with IBM Rational AppScan Reporting Console software

IBM Rational AppScan Reporting Console is a powerful Web-based management and reporting application. Fully integrated with Rational AppScan Standard Edition, Rational AppScan Reporting Console is backed by an enterprise-class database that allows you to consolidate scan results from multiple Rational AppScan clients to create a centralized application vulnerability repository. Scan results can be easily distributed to QA and development teams without having to install additional desktop licenses, helping to simplify the remediation process and integrate vulnerability analysis across the software development lifecycle. Rational AppScan Reporting Console enables you to create multiple dashboards for multiple users, giving individuals the ability to segment security data by application, business unit, geography or third-party provider.

Leverage Rational AppScan Standard Edition and Rational AppScan Enterprise Edition 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.

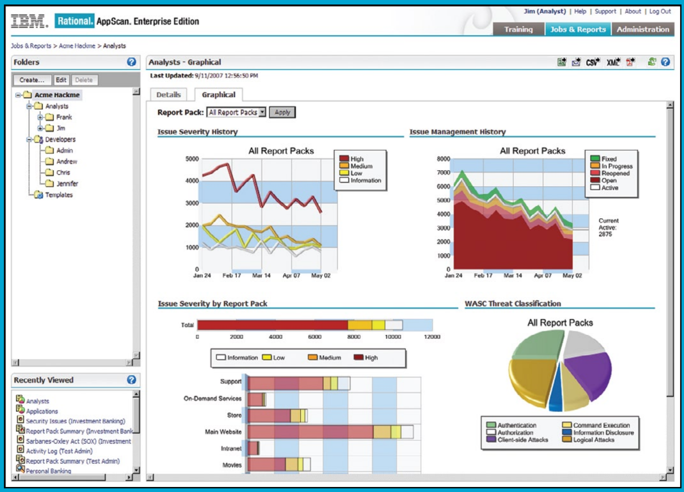
A state-of-the-art security testing environment

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

Dedicated security and compliance assistance from IBM professionals

Rational AppScan Standard Edition or Rational AppScan Enterprise Edition SaaS customers can engage an IBM security analyst to help:

- Configure and tune scans to potentially ensure comprehensive coverage for each application.
- Review and analyze results to help eliminate false positives, identify patterns, prioritize issues and highlight remediation tasks.
- Track remediation progress by maintaining trend data, tracking resolution from scan to scan, and reporting on remediation effectiveness.



Last Updated: 9/11/2007 12:56:50 PM

Report Pack: All Report Packs

The IBM Rational AppScan Enterprise Edition dashboard view

Help prevent security and compliance management issues with Web-based training

IBM offers Web-based application security training, delivered online and in 15-minute intervals. In addition to basic product instruction, the training service provides targeted advice for developers, QA teams and security professionals.

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 Rational AppScan Enterprise Edition.

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
August 2008
All Rights Reserved

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 customerís business and any actions the customer may need to take to comply with such laws.