Strategic protection for Web applications
To support your business objectives

Rational software

IBM Rational AppScan: enhancing Web application security and regulatory compliance.

Are untested Web 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. Unfortunately, in the race to meet deadlines and stay ahead of the competition, many businesses fail to perform adequate security testing or take the time to make sure applications are in compliance with industry and regulatory standards. The result is that many companies may unwittingly expose corporate or personal data to cybercriminals who can exploit these vulnerabilities for fun and profit—placing the entire business at risk. And since many regulatory requirements mandate a degree of application security, these organizations also run the risk of failing to meet compliance audit requirements, which can result in fines and customer backlash. To help protect your company's valuable assets, it's important to test Web applications throughout their entire lifecycle—as they're being developed and after they're put into production.

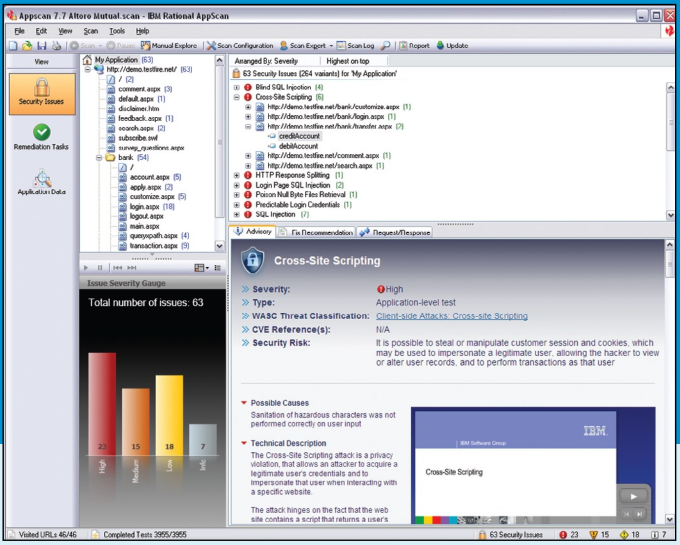
IBM Rational® AppScan® software is a suite of marketplace-leading Web application security and compliance solutions that can help address the critical challenge of application security and compliance. The suite includes:

- 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 Reporting Console
- IBM Rational AppScan OnDemand
- IBM Rational AppScan OnDemand Production Site Monitoring
- IBM Rational Web Based Training for AppScan

All of the solutions provide scanning, reporting and fix recommendation functionality. 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

Protect your 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. Plus, each time a user launches a Rational AppScan application, the software downloads notifications on the latest security threats, so you have up-to-date information from IBM.



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)

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)

Total number of issues: 63

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

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

The IBM Rational AppScan security advisory view

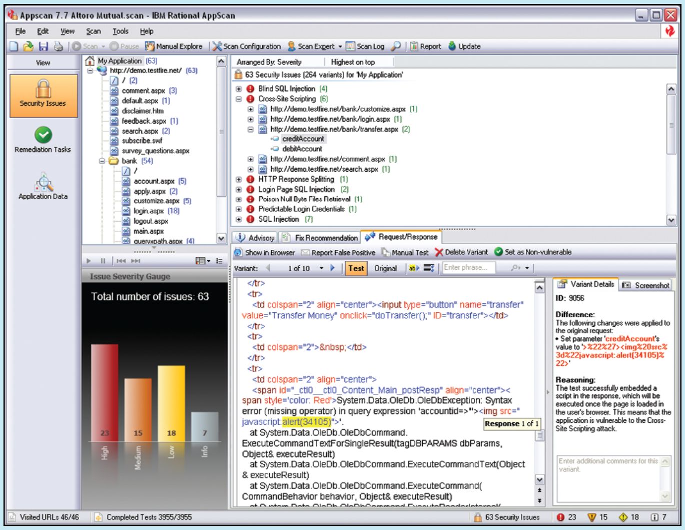
Stay on top of compliance issues

The Rational AppScan offerings include compliance reports to help your company track its compliance with key industry and regulatory requirements, including National Institute of Standards and Technology Special Publication (NIST SP) 800-53 and the Open Web Application Security Project (OWASP) top 10, Payment Card Industry Data Security Standard (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). 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.

Rational AppScan Standard Edition: Conduct security audits and production monitoring

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 includes features designed to support moderate and power users. Features include:

- The scan expert, a wizard-based 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.
- 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)

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)

```
  </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)
```

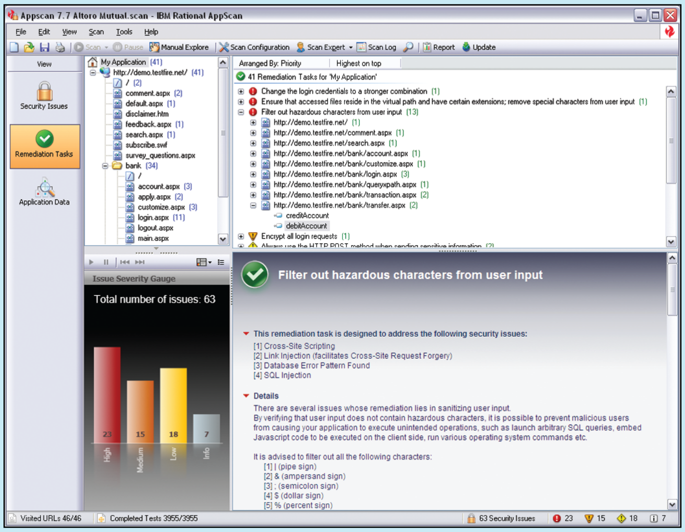
ID: 9056

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.

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

The IBM Rational AppScan security issues view


Appscan 7.7 Altoro Mutual.scan - IBM Rational AppScan
File Edit View Scan Tools Help
Scan Pause Manual Explore Scan Configuration Scan Expert Scan Log Report Update
View
Security Issues
Remediation Tasks
Application Data
Issue Severity Gauge
Total number of issues: 63
23
15
18
7
High
Medium
Low
Info

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

Arranged By: Priority | Highest on top

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)

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

The IBM Rational AppScan remediation view

Rational AppScan Express Edition: Gain robust Web application security features at an attractive price point

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.

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

Rational AppScan Tester Edition, available as a desktop application, offers capabilities to help quality assurance (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.

Rational AppScan Developer Edition: Embed security testing in your development environment

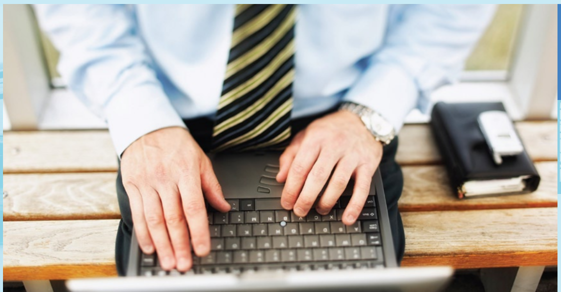
The most efficient way to stay ahead of application security vulnerabilities is to build software securely from the ground up. The challenge is that most developers are not security experts, and writing secure code is not always their top priority. So the best way to engage development in the process 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.

Rational AppScan Build Edition: Integrate security analysis in the build environment

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.



Rational AppScan Enterprise Edition: Scale application security testing across the enterprise

With its Web-based architecture, Rational AppScan Enterprise Edition is designed to help organizations distribute responsibility for security testing among multiple stakeholders.

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.

Rational AppScan Reporting Console: Access centralized reporting on Web application vulnerability data

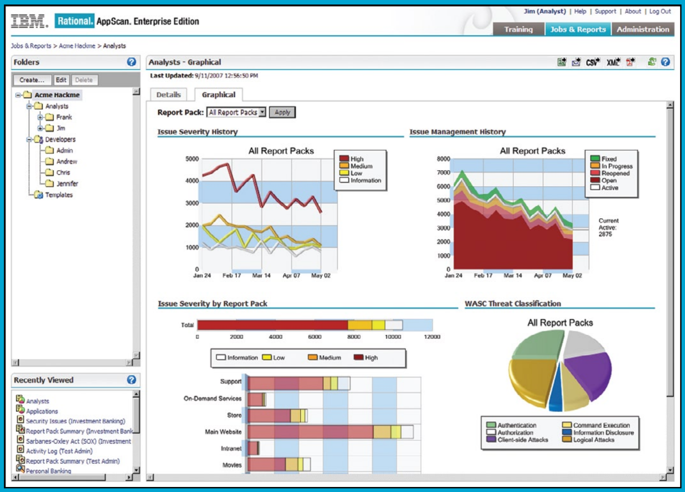
IBM Rational AppScan Reporting Console is a powerful Web-based management and reporting application. Fully integrated with Rational AppScan Standard Edition, Rational AppScan Reporting Console is backed by an enterprise-class database that allows you to consolidate scan results from multiple Rational 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.

Rational AppScan OnDemand: Manage Web application security without up-front investments

The IBM Rational AppScan OnDemand offering is a SaaS solution that allows you to manage Web application security without the up-front investments. Delivering actionable results fast, the service utilizes IBM Rational AppScan Enterprise Edition software and is hosted and run by an experienced team of security and compliance experts from IBM. Rational AppScan OnDemand provides monthly application security scanning, data consolidation and reporting, remediation capabilities, executive dashboards, and compliance reporting for preproduction Web applications in the QA and security test phases. The offering provides an outsourced Web application security testing solution with a cost-effective startup cost, rapid time to value and competitive total cost of ownership.

Rational AppScan OnDemand Production Site Monitoring: Maintain Web application security after applications are launched

The IBM Rational AppScan OnDemand Production Site Monitoring offering is a SaaS product that uses a noninvasive subset of the IBM Rational AppScan Enterprise Edition test policy to monitor production applications for vulnerabilities that may be introduced after the applications go live. If your marketing, e-business or Web teams update, change or push out new content to your Web applications, they can introduce new vulnerabilities that can put your organization's confidential information at risk. Plus, we all know that major application releases necessitate hot fixes, support for service interruptions (break fixes) and structural changes that can provide new soft spots for hackers to attack. To maintain security-rich Web applications, you must continually monitor your Web sites for vulnerabilities, long after their go-live dates.



The IBM Rational AppScan Enterprise Edition dashboard view

A state-of-the-art security testing environment

Both Rational AppScan OnDemand and Rational AppScan OnDemand Production Site Monitoring are run in a scalable, private hosting environment with advanced data center security services to help ensure the integrity of your data. Managed by experienced engineers and security specialists who are dedicated to data and systems protection, the hosting environment has achieved the Statement on Auditing Standards (SAS) No. 70 Type II certification. IBM continually evaluates emerging security developments and threats, deploying proven, up-to-date technologies to help ensure that your sensitive information is protected.

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 how you can take advantage of IBM Rational AppScan products to make your Web applications more security-rich and compliant, 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
April 2009

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

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.