watchfire®
an IBM company

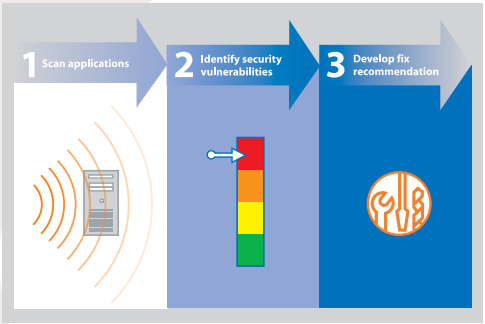
Watchfire AppScan, Version 7.6

Leverage comprehensive results and customizable features for Web application security scanning

In the race to push more business services online, Web applications frequently suffer from a lack of built-in security. The resulting vulnerabilities represent an easy path for hackers to access or steal corporate or personal data and information. Web application vulnerability scanning represents the best way for security auditors to defend against such targeted attacks.

Watchfire® AppScan®, a worldwide marketshare-leading Web application security scanner is trusted by security and development teams to provide the visibility and control necessary to address this critical challenge. AppScan offers a solution for all types of security testing — outsourced, desktop-user and enterprise-wide analysis — and for all types of users — application developers, quality assurance (QA) teams, penetration testers, security auditors and senior management.

The AppScan patented scan engine continuously audits Web applications, tests for security and compliance issues and provides actionable reports with fix recommendations. Seamless integration with leading QA tools, including Mercury Quality Center; development environments, such as JBuilder and Microsoft® Visual Studio; and code scanning devices like Fortify, further simplifies security testing and remediation throughout the software development process.



AppScan, Version 7.6 overview

AppScan, Version 7.6 helps ensure the security and compliance of Web applications throughout the software development lifecycle. It's designed for the broadest range of users — from nonsecurity professionals to advanced power users who can utilize the added tools and extensions to create a customized scanning environment. AppScan, Version 7.6 handles more complex Web environments and extends its scanning accuracy with its adaptive test process and enhanced Ajax support.

Web application scanning

The latest version of AppScan software features new offerings to improve your ability to effectively scan Web applications and test for security issues:

- A fast and comprehensive patented scan engine.
- A configuration wizard to assist in scan setup.
- A user interface that includes an application tree, view selector, hierarchical security issues results list, remediation view and details pane.
- An adaptive test process that intelligently mimics human logic to adapt the testing phase to each application. AppScan can learn the application down to specific parameters, adjusting to perform only relevant tests, helping to improve scan performance and accuracy.
- A developer essentials test policy that automates security testing of the most critical issues in a format that can optimize and simplify the process for development.
- Concurrent scanning that lets you simultaneously run multiple instances of AppScan. This can be used to perform concurrent scans on high-end machines; review results of one scan while performing another; or run any combination of the broad functions AppScan offers.

BENEFITS

- Helps enable productivity gains from greater transparency and automation
- Enables user customization through the AppScan SDK with AppScan eXtensions Framework and Pyscan
- Provides coverage for more modern and complex sites
- Features advanced remediation and fix recommendations for unmatched accuracy and efficiency

- Enhanced Ajax support that can improve the ability of AppScan to automatically crawl and test Ajax-based applications. The improvements include various Java™ technology JavaScript execution improvements, dedicated testing of JavaScript Object Notation (JSON) protocol parameters, better handling of ActiveX objects used by JavaScript technology, and more.
- Complex authentication support that enables multi-step authentication procedures in Web applications. If AppScan detects that a complex authentication is required, it will suspend the scan and prompt you to complete the authentication process. Supported authentication methods include Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), stepped authentication, multifactor authentication, one-time passwords, Universal Serial Bus (USB) keys, smartcards and mutual authentication.
- Privilege escalation testing that tests the authorization model in AppScan by detecting protected resources that could be accessed by users with insufficient access permissions.
- Advanced session management that actively checks that you remain logged in, and automatically refreshes your login when required.
- Pattern search rules that look for strings and regular expressions in the original responses. This facilitates, for example, security testing around credit card or social security sequence.
- Integrated Web services scanning that understands application-to-application interactions and comes with a wide range of advanced Simple Object Access Protocol (SOAP) tests, resulting in broad coverage of the scanned application.
- A real-time view of results that lets you start examining and acting on the issues that have been found before the scan is completed — which is useful for large scans and for auditors or penetration testers with limited time for application testing.
- An enhanced view of issues, which provides greater control over the way issues are displayed. You can increase and decrease the request/response font, choose between two viewing modes — word wrap and regular view — perform searches and print the information pages presented by AppScan.

Customization and control

Also new in the 7.6 version of AppScan software are enhanced customization and control extensions:

- AppScan SDK offers a powerful set of interfaces that allows you to invoke every action in AppScan — from the execution of a long scan to the submission of an individual custom test. This strong platform helps enable easy integrations into existing systems; supports advanced custom uses of the AppScan engine; and provides the foundation for the AppScan eXtensions Framework and Pyscan (discussed below).
- The AppScan eXtensions Framework lets you load add-ons to extend AppScan functionality. The framework allows you to customize and enhance AppScan to fit your own processes, automate in-house activities using AppScan as a powerful supporting layer, and receive additional features and functionality by downloading open source extensions from the AppScan eXtensions community portal.
- The SQL Injection Exploiter, which is available as part of the AppScan eXtensions framework, automatically attempts to exploit a structured query language (SQL) injection vulnerability by trying to extract database tables.
- Pyscan — a Web application security testing platform built on AppScan and Python software — lets auditors enjoy the benefits of AppScan extensive functionality while performing manual audits. Features such as AppScan advanced session management (used to establish and maintain login state), an easily accessed repository of scanned application data, and powerful reporting abilities are all readily available. Pyscan can dramatically increase the efficiency of the manual portion of an audit — without losing the irreplaceable expertise of the auditor.
- Predefined scan templates are installed in AppScan software and include Watchfire's demonstration Web site, Hacme Bank and WebGoat V4.
- Advanced configuration options, including AppScan registry settings and advanced controls over AppScan behavior, are now accessible through the *Advanced* tab in the *Options* dialog box.
- The *View Non-Vulnerable* feature allows you to opt to keep all tests submitted by AppScan. This gives you broader visibility into granular choices and

actions performed by AppScan, allowing manual review of sampled issues supported by strong searching and sorting tools.

- The ability to report false positives and false negatives allows you to send information packs with an encryption option back to Watchfire's Security Research Team for analysis. Any necessary changes to the security tests are made available through AppScan's daily updates.

Vulnerability detection

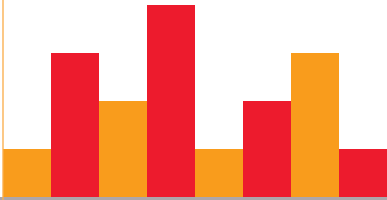
Also new in the latest release of AppScan, robust additional vulnerability detection features:

- AppScan can run simulated hacker attacks such as cross-site scripting, HTTP response splitting, parameter tampering, hidden field manipulation, backdoor/debug options, stealth commanding, forceful browsing, application buffer overflow, cookie poisoning, third-party misconfiguration, known vulnerabilities, HTTP attacks, SQL injections, suspicious content, XML/SOAP tests, content spoofing, Lightweight Directory Access Protocol (LDAP) injection, XPath injection and session fixation.
- Maps to Open Web Application Security Project's (OWASP's) top 10 and System Administration, Networking and Security (SANS) Institute's top 20 vulnerabilities are included in the 7.6 version.
- Zero-day vulnerability updates are provided daily on the latest security vulnerabilities, and AppScan checks for updates automatically when it's launched, or on demand by the user.
- The Watchfire PowerTools utility suite is bundled with AppScan to assist those who develop, test and debug Web applications — such as penetration testers and security consultants — complementing manual testing and providing greater power, automation and efficiency.

Reporting and remediation

To assist in reporting and remediation activities, AppScan, Version 7.6 provides the following capabilities:

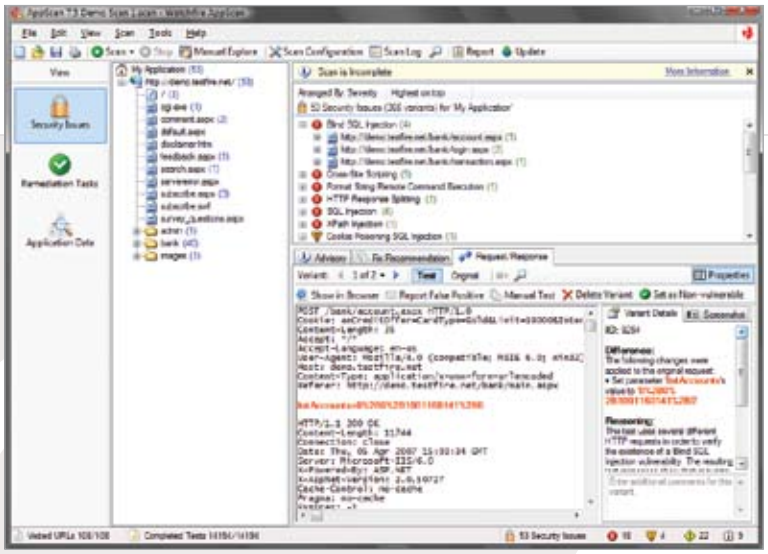
- Delta analysis reports, which tell you what changes have occurred from one scan to the next. The reported information includes what has been fixed, what has not and what new security issues have been introduced since the initial scan.
- Validation highlighting and reasoning, which can be used to determine vulnerability. During a test, AppScan can highlight the HTML code that appears to be causing the vulnerability. Then, AppScan can provide reasoning text in natural language to explain the logic of the test and why an issue was identified. Additionally, the AppScan *Difference* feature can display the HTML code that has been modified from the original response to provide greater clarity for the user.
- Customizable advisories and fix recommendations, which can be used to add a note about company policy or provide custom explanations of specific issues. This ability enables you to adapt AppScan to your process, saving the time required for changes or repeats.
- PHP Hypertext Preprocessor (PHP) fix recommendations.
- Individual variant control, which allows you to delete individual variants or mark them as "not vulnerable" for later review in the *View Non-Vulnerable* screen.
- Identification of suspicious content — such as sensitive data in HTML comments and full information about the HTTP activity — which AppScan can present to users.
- Regulatory compliance reporting, which has been added for National Institute of Standards and Technology (NIST) 800-53 and the latest OWASP top 10, updated in 2007. AppScan now provides a total of 41 global regulatory compliance and standards reports.
- Common Vulnerabilities and Exposures (CVE) IDs from the vulnerability database, which are now included in each test description.
- Customizable reports for management, developers, QA engineers, system managers and security professionals, which provide you with full control of content and layout.
- URL-based reports that are more concise and actionable.
- Industry-standard reports, including the OWASP top 10, SANS top 20 and the Web Application Security Consortium (WASC) standards.
- The industry's most comprehensive compliance reporting solution, which generates 41 out-of-the-box regulatory compliance templates and reports including California Assembly Bill No. 1950, Children's Online Privacy Protection Act (COPPA); Director of Central Intelligence Directive (DCID) 6/3; Electronic Funds Transfer



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

Produced in the United States of America
07-07

RAD11041-USEN-00



AppScan provides full details to show how vulnerabilities are exposed

Act (EFTA); Exchange and Securities Act; Federal Information Security Management Act (FISMA); Gramm-Leach Bliley; Health Insurance Portability and Accountability Act (HIPAA); MasterCard Site Data Protection (MasterCard SDP) program; North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) security guidelines for the electricity sector; Payment Card Industry (PCI) Data Security Standards; Privacy Act of 1974; Sarbanes-Oxley; Title 21 Code of Federal Regulations; Visa Cardholder Information Security Program (Visa CISP), Basel Committee on Banking Supervision banking laws and regulations (BASEL II), International Standards Organization (ISO) 17799 and ISO 27001 standards.

- Reporting filter, which lets you choose to report on application-related issues, infrastructure issues or both.
- Report screenshots, which can be taken of the AppScan internal browser to include in AppScan reports. This is useful for communicating scan results to developers or system administrators who require proof of vulnerability.
- False positive reporting, which lets you select specific tests from which AppScan can extract, zip and encrypt nonproprietary information for e-mailing. This offers a quick and easy way to send Watchfire feedback about tests you believe are false positives (i.e., AppScan records a positive test result indicating a security issue where you believe the result should have been negative). Additionally, this feature allows you to easily send test information for review to the application developers or system managers.
- Remediation view, which shows a comprehensive list of tasks necessary to fix the security issues found by the scan. This view shows tasks either for the whole application or for specific folders, easing assignment of remediation to application developers and system managers.

Why IBM and Watchfire?

A leading provider of Web application security software, Watchfire, an IBM company, offers clients a complete solution that includes intelligent fix recommendations to evaluate, understand and resolve their security issues. More than 800 enterprises and government agencies — including global financial services, communications and high-tech companies — rely on Watchfire products to help them identify, report and remediate security vulnerabilities.

For more information

To learn more about Watchfire AppScan, Version 7.6 software, contact your IBM Watchfire representative or visit:

www.watchfire.com/products/appscan/appscan.aspx

System requirements

Processor Intel® Pentium® P4, 1.5 GHz (2.4GHz recommended)
Memory 512MB RAM (1GB recommended for scanning large sites)
Free disk space 1GB (10GB recommended for scanning large sites)
Network 1NIC 10Mbps for network communication with configured TCP/IP (100 Mbps recommended)
Operating system Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
Browser Microsoft Internet Explorer 5.5 or higher (IE 6.0 or higher recommended)
Software development platforms and environments Microsoft .NET Framework 2.0 or higher Java Runtime Environment 5.0 (for Watchfire HTTP proxy only)