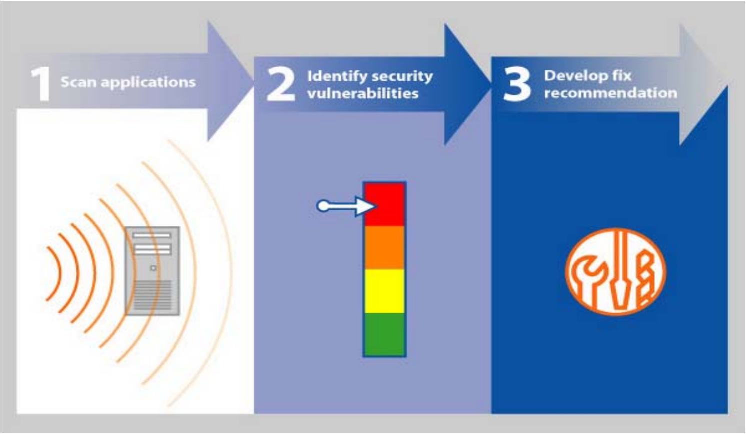
Watchfire® AppScan® 7.5

Web Application Security Scanning: Comprehensive results and customizable features

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®, the worldwide market-share leading (Gartner and IDC,[1]) web application security scanner with more than a third of the global market share, is trusted by more security professionals 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 teams, penetration testers, security auditors and senior management.

AppScan's 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 Visual Studio, and Fortify's Code Scanner further simplifies security testing and remediation throughout the software development process.


1 Scan applications
2 Identify security vulnerabilities
3 Develop fix recommendation

[1] Source: Gartner Dataquest, "Market Share: Application Development and Project and Portfolio Management, Worldwide, 2005, Table 2-1," Laurie F. Wurster and Fabrizio Biscotti, 18 May, 2006 and IDC, "Worldwide Security and Vulnerability Management Software 2005-2009 Forecast and Analysis: Taking Control of the Security Environment, Doc #34604," December 20, 2005.

<front page callout>

Benefits

- Productivity gains from greater transparency and automation
- User customization through the AppScan SDKwith AppScan eXtensions Framework and Pyscan
- Coverage for more modern and complex sites
- Advanced remediation and fix recommendations for unmatched accuracy and efficiency

AppScan 7.5 Overview

AppScan 7.5 helps ensure the security and compliance of web applications throughout the software development lifecycle. It's designed for the broadest range of users – from non-security professionals to advanced power users who can utilize the added tools and eXtensions to create a customized scanning environment.

Web Application Scanning

- Patented scan engine is the industry's fastest and most comprehensive
- Configuration Wizard to assist in scan set-up
- User Interface that includes an Application Tree, View Selector, hierarchical Security Issues results list, Remediation View and Details Pane to ease navigation
- **Adaptive Test Process: (New in 7.5!)** intelligently mimics human logic to adapt the testing phase to each individual application. AppScan learns the application, down to the level of each specific parameter, adjusting to perform only those tests relevant to greatly improve scan performance and accuracy.
- **Concurrent Scanning: (New in 7.5!)** lets the user run multiple instances of AppScan at the same time. This can be used to perform concurrent scans on high-end machines, review results of one scan while performing another, or any other combination of the broad functions AppScan offers.
- **Enhanced AJAX Support: (New in 7.5!)** further enhances AppScan's ability to automatically crawl and test AJAX-based applications. The improvements include various JavaScript execution improvements, dedicated testing of JSON protocol parameters, better handling of ActiveX objects used by JavaScript and more.
- Complex Authentication Support: to enable multi-step authentication procedures in web applications. If AppScan detects that a complex authentication is required it will suspend the scan and prompt the user to complete the authentication process. Supported authentication methods include CAPTCHA, stepped authentication, multi-factor authentication, one-time passwords, USB keys, smartcards and mutual authentication
- Privilege Escalation Testing: AppScan tests the application's authorization model by detecting protected resources that could be accessed by users with insufficient access permissions.
- Advanced Session Management: to actively check that the user remains logged in, and will automatically re-login when required.

- Pattern Search Rules: to 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: to understand application-to-application interactions and comes with the widest range of advanced SOAP tests resulting in broad coverage of the scanned application
- Real-time View of Results: lets users 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
- Enhanced View of Issues: providing greater control over the way issues are displayed. Users can increase and decrease the request/response font, choose between two viewing modes – word wrap and regular view – and perform search on and print the information pages presented by AppScan.

Customization and Control

- **AppScan SDK: (New in 7.5!)** Offers a powerful set of interfaces allowing custom invoking of every single action in AppScan, from the execution of a long scan to the submission of an individual custom test. This strong platform allows easy integrations into existing systems, supports advanced custom uses of the AppScan engine and provides the foundation for the AppScan eXtensions Framework and Pyscan.

- **AppScan eXtensions Framework (AXF): (New in 7.5!)** AXF is a flexible framework letting the user load add-ons to extend AppScan's functionality. AppScan eXtensions open up AppScan, letting users customize and enhance AppScan to fit their own processes, automate in-house activities using AppScan as a powerful supporting layer and receive a plethora of additional features and functionality by downloading open-source extensions from the AppScan eXtensions community portal (http://axf.watchfire.com)

- **Pyscan: (New in 7.5!)** Pyscan is a web application security testing platform built on AppScan and Python. Pyscan lets an auditor enjoy the benefits of AppScan's extensive functionality while performing a manual audit. Abilities such as the Advanced Session Management of AppScan (used to establish and maintain login state), easily accessed repository of scanned application data and powerful reporting abilities are all readily available. Pyscan dramatically increases the efficiency of the manual portion of an audit – without losing the irreplaceable expertise of the auditor.

- **Predefined Scan Templates: (New in 7.5!)** AppScan is installed with predefined scan templates including Watchfire's demonstration web site, Hacme Bank and WebGoat v4.

- **Advanced Configuration Options: (New in 7.5!)** All of AppScan's registry settings, holding advanced controls over AppScan behavior, are now accessible through the Advanced tab in the Options dialog box.

- **View Non-Vulnerable: (New in 7.5!)** Feature allows the user to opt to keep all tests submitted by AppScan. This gives the user broader visibility into granular choices and actions performed by AppScan, allowing manual review of sampled issues supported by strong searching and sorting tools.

- **Report False Positives & Report False Negatives: (New in 7.5!)** Users can report on suspected False Positives or False Negatives. An information pack can be sent, with an encryption option, back to Watchfire's Security Research Team for analysis. Any necessary changes the security tests are made available through AppScan's Daily Updates.

Vulnerability Detection

- Security vulnerability detection by simulating hacker attacks such as Cross-Site Scripting; HTTP Response Splitting; Parameter Tampering; Hidden Field Manipulation; Backdoors/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; LDAP Injection; XPath Injection; Session Fixation
- Maps to Open Web Application Security Project's (OWASP) Top 10 and SANS Top 20 vulnerabilities
- **Zero-Day Vulnerability Updates:** AppScan provides daily security updates on the latest security vulnerabilities and checks for updates automatically when AppScan is launched, or on demand by the user.
- **Watchfire PowerTools:** the 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

- Delta Analysis: AppScan's Delta Analysis report provides you with the changes that have occurred from one scan to the next. The reported information includes what has been fixed, what has not and new security issues that have been introduced since the initial scan.
- Validation Highlighting & Reasoning: During a test, AppScan highlights the offending HTML code that is determined to cause the vulnerability. Reasoning text is provided in natural language to explain the logic of the test and why an issue was identified. Additionally, a *Difference* feature displays the HTML code that has been modified from the original response to provide greater clarity for the user.
- **Customizable Advisories & Fix Recommendations: (New in 7.5!)** AppScan 7.5 allows users to modify AppScan's detailed advisories & fix recommendations to their own needs. Allowing anything from adding a note about company policy to adding custom explanations of the specific issue, this ability enables adapting AppScan to your process, saving the time required for changes or repeats.
- Individual Variant Control: AppScan allows the user to delete individual variants, or mark them as not vulnerable for later review in the Non-Vulnerable screen.

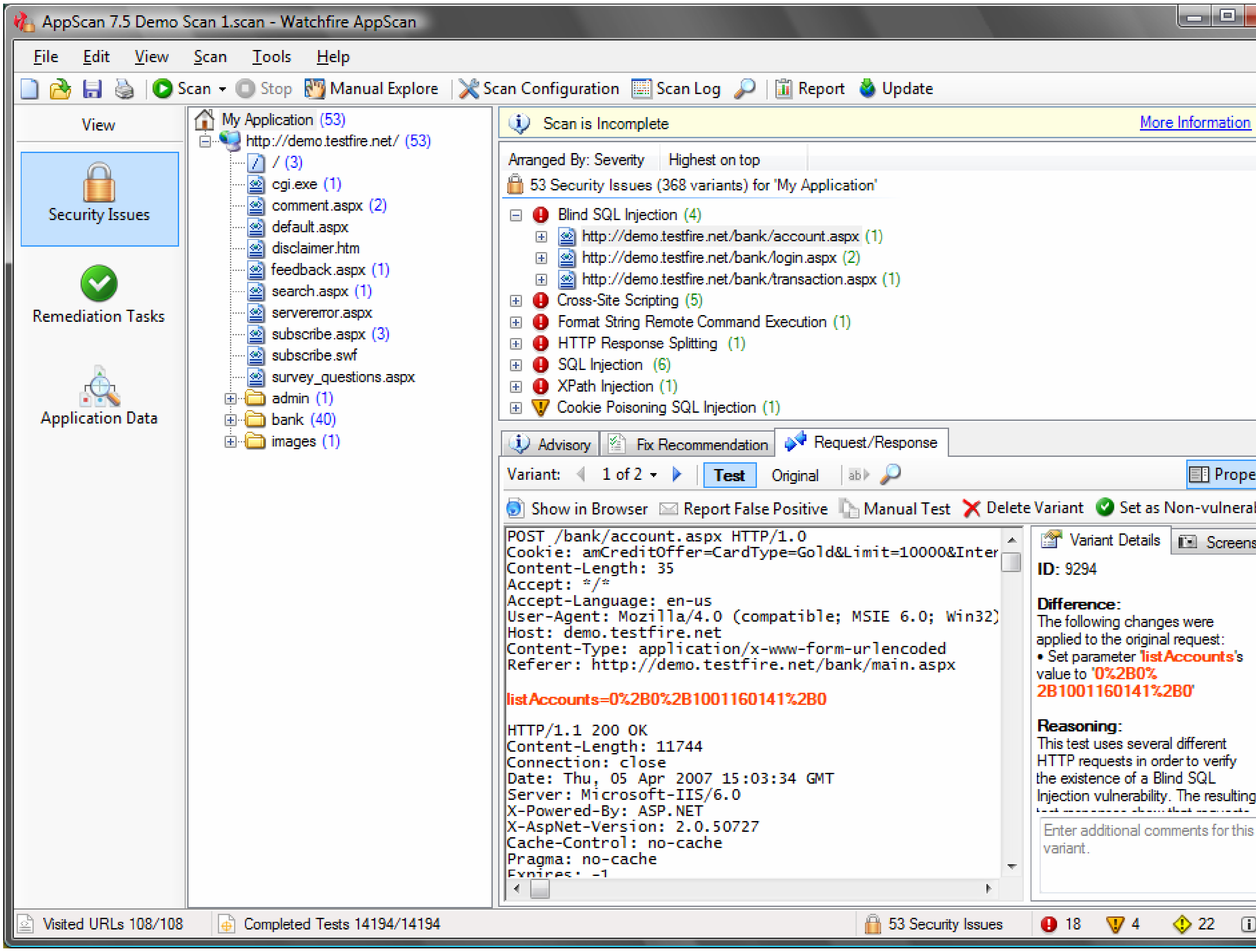
- **Detailed Suspicious Content: (New in 7.5!)** In addition to issues found by sending test requests to the site, AppScan also identifies suspicious content found on the application, such as sensitive data in HTML comments. AppScan 7.5 now presents the full information about the HTTP activity which shows the suspicious content.

- **Regulatory compliance reporting: (New reports in 7.5!)** New compliance reports have been added for NERC and BASEL II. AppScan now provides a total of 40 global regulatory compliance and standards reports.

- CVE Referencing: The CVE IDs from the vulnerability database are now included in each test description.
- Customizable reports for management, developers, QA engineers, system managers and security professionals, providing users full control of content and layout.
- Streamlined reporting: 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: generates 34 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 DCID 6/3; Electronic Fund and Transfer Act (EFTA); Exchange and Securities Act; Federal Information Security Management Act (FISMA); Gramm-Leach-Bliley (GLBA); Health Insurance Portability & Accountability Act (HIPAA); MasterCard® Site Data Protection Program (MasterCard SDDP); NERC CIPC 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 (CISP), ISO 17799 and ISO 27001standards
- Reporting Filter lets you choose to report on application-related issues, infrastructure issues, or both
- Screenshots in Report: lets users take a screenshot of AppScan's internal browser to include in AppScan reports. This is useful for communicating scan results to developers or system administrators who require "proof" of vulnerability

- Report False Positive: lets you select specific tests from which it will extract, zip and encrypt non-proprietary 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: 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.



Scan is Incomplete

Arranged By: Severity Highest on top

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

```
POST /bank/account.aspx HTTP/1.0
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter
Content-Length: 35
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.testfire.net/bank/main.aspx

listAccounts=0%2B0%2B1001160141%2B0

HTTP/1.1 200 OK
Content-Length: 11744
Connection: close
Date: Thu, 05 Apr 2007 15:03:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
```

ID: 9294

Difference:
The following changes were applied to the original request:
- Set parameter 'listAccounts's value to '0%2B0%2B1001160141%2B0'

Reasoning:
This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting

Enter additional comments for this variant.

Visited URLs 108/108 Completed Tests 14194/14194 53 Security Issues 18 4 22

AppScan provides full details showing how vulnerabilities are exposed

System Requirements

- Processor: Pentium P4, 1.5 GHz (2.4GHz recommended)
- Memory: 512 MB RAM (1 GB recommended for scanning large sites)
- Free Disk Space: 1 GB (10GB recommended for scanning large sites)
- Network: 1 NIC 10 MBPS for network communication with configured TCP/IP (100 Mbps recommended)
- Operating System: Windows XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
- Microsoft Internet Explorer 5.5 or higher (IE 6.0 or higher recommended)
- Microsoft .Net Framework version 2.0 or higher
- JRE 5.0 (for Watchfire HTTP Proxy only)

About Watchfire

Watchfire is the leading provider of web application security software and the only company to offer an end-to-end solution including intelligent fix recommendations to evaluate, understand and resolve issues. More than 800 enterprises and government agencies, including AXA Financial, SunTrust, HSBC, Vodafone, Veterans Affairs and Dell rely on Watchfire to identify, report and help remediate security vulnerabilities. Watchfire has been the recipient of several industry honors including: winning an unprecedented three out of five 2007 *SC Magazine* Excellence Awards (including Best Security Company); the HP/IAPP Privacy Innovation Award; *Computerworld's* Innovative Technology Award; winner of the *Dr. Dobb's* 2007 Jolt Product Excellence Awards; and "Recommended" rating by *Computer Reseller News*. For two years in a row, Watchfire has been named by IDC as the worldwide market share leader in web application vulnerability assessment software. Watchfire's partners include IBM Global Services, Fortify, PricewaterhouseCoopers, Sapient, Microsoft, Interwoven, EMC Documentum and Mercury. Watchfire is headquartered in Waltham, MA. For more information, please visit www.watchfire.com.