IBM Security AppScan Standard

Enhance web application security by identifying and remediating web application vulnerabilities

Highlights

- Simplify remediation by identifying vulnerabilities and generating results through comprehensive scanning coverage
- Scan complex web applications, including those that utilize Adobe Flash, JavaScript, Ajax and Simple Object Access Protocol (SOAP) web services
- Combine advanced dynamic and innovative hybrid analyses of glass-box testing (runtime analysis) with static taint analysis for superior accuracy
- Identify the latest threats, including full coverage of the Open Web Application Security Project (OWASP) Top 10 web application vulnerabilities
- Manage regulatory requirements such as PCI, GLBA and HIPAA

Today, most organizations depend on web-based software and systems to run their business processes, conduct transactions with suppliers and deliver sophisticated services to customers. Unfortunately, in the race to stay one step ahead of the competition, many organizations invest little to no effort in ensuring that those applications are secure. Web-based systems can compromise the overall security of organizations by introducing vulnerabilities that hackers can use to gain access to confidential company information or customer data.

The IBM® Security AppScan® portfolio of solutions helps organizations address web application vulnerabilities through a *secure-by-design* approach. This approach embeds security testing into the software development lifecycle, providing organizations with the tools they require to develop more secure code.

Designed to help security teams test and audit web applications in development and production, IBM Security AppScan Standard software scans and tests for the latest threats with a desktop solution that offers:

- Broad coverage of emerging threats, including Web 2.0 application vulnerabilities
- Advanced dynamic application security testing, also referred to as *black-box analysis*
- Glass-box testing, also referred to as *runtime analysis* or *integrated application security testing*

- Cross-Site Scripting (XSS) Analyzer for cutting-edge XSS detection and exploitation
- JavaScript Security Analyzer for static taint analysis of client-side security issues
- Customizable product extensions for greater control over web vulnerability testing
- Ease-of-use, particularly when implementing an automated security testing program
- Convenient identification of security issues, along with beneficial remediation guidance
- More than 40 out-of-the-box compliance reports to help facilitate an organization's compliance initiatives
- Support for industry-standard Transport Layer Security (TLS) protocol 1.2

To download a free trial of IBM Security AppScan today, please click here:

Sign up for free AppScan trial

Generating cost savings with accurate, automated scanning

Security AppScan Standard software can help significantly reduce the costs associated with manual vulnerability testing. Whether an organization outsources its vulnerability testing or performs it manually in-house, Security AppScan Standard software can help reduce the time required to perform comprehensive application vulnerability assessments. It permits organizations to evaluate their web security postures on an ongoing basis—as opposed to quarterly or yearly audits—which can help enhance security levels and reduce costs.

The patented Security AppScan Standard software scanning engine is designed to provide high levels of scan accuracy and limit false positives. To further improve accuracy and performance, it includes an adaptive test process that intelligently mimics human logic to adapt its testing phase to individual applications. Security AppScan Standard software learns the application down to the level of each specific parameter and adjusts to perform only the tests that are relevant. To help ensure protection from the latest threats, Security AppScan Standard software checks for attack-rule updates from the IBM X-Force® team of security research experts each time the software is launched.

Providing quick results with features designed for ease of use

Not everyone is a security expert. Security AppScan Standard software integrates many ease-of-use features to help make web vulnerability scanning easier for those who aren't:

- The scan configuration wizard guides each user to set up an initial scan by prompting for basic information such as a starting URL or IP address, querying which type of scanning profile should be used and soliciting required login information.
- The scan expert feature performs a settings check and makes any final modifications, such as turning on JavaScript or Adobe Flash parsing and execution, to support environments that utilize client-side logic.
- After the scan configuration is complete, Security AppScan Standard explores the application and extracts information about web pages, HTML forms, parameters, cookies and so on. This information is later used to build thousands of test cases.
- Security AppScan Standard software then begins the test phase and returns vulnerability results and remediation recommendations. The results offer helpful tips and screenshots to clearly illustrate each issue.

Streamlining remediation with prioritized results and fix recommendations

One of the most critical aspects of web vulnerability scanning is the quick remediation of issues. Security AppScan Standard software provides a fully prioritized list of vulnerabilities that are found with each scan, which enables the highest-priority problems to be fixed first—helping organizations focus on what matters the most from a security perspective. Each vulnerability result includes a full description of how the vulnerability works and its potential causes. When deploying glass-box scanning (runtime analysis) agents during a scan, the software reports the actual location in the application's code where the vulnerability took place, such as the name of the Java class and the vulnerable line number. Integrated modules provide convenient training sessions directly from the user interface. The remediation view then explains the steps required to remediate the issue, including examples of both secure and insecure code. To assign and manage remediation, results can be integrated into multiple defect tracking systems.

Managing compliance and gaining insight into key security issues

Many organizations face key compliance demands associated with their web applications. Security AppScan Standard software helps them manage these critical compliance requirements by facilitating ongoing application security.

Security AppScan Standard software can also produce custom security reports and has the ability to select which data points should be included in each report. Users can also choose from more than 40 predefined reports and map scan results to key industry and regulatory compliance standards, including:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53
- OWASP Top 10
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act
- Family Educational Rights and Privacy Act
- Freedom of Information and Protection of Privacy Act
- Payment Application Best Practices

For increased insight and visibility, organizations can add an IBM Security AppScan Enterprise server to their existing Security AppScan Standard software deployment. Security AppScan Enterprise servers provide role-based reporting access and aggregate scan data from multiple instances of Security AppScan Standard software. By providing in-depth, yet easy-to-analyze dashboards and flexible reporting views—including enterprise-wide visibility into risks and continuous updates on remediation progress—Security AppScan Enterprise servers provide platforms for application security testing and risk management.

Detecting and exploiting cross-site scripting with XSS Analyzer

Recent research performed by IBM showed that more than half of all web application vulnerabilities were comprised of XSS vulnerabilities.[1] XSS has been a known vulnerability type for more than 10 years. Even so, it still appears on the OWASP Top 10 2013 web application vulnerabilities list based on its prevalence.[2]

Security AppScan Standard software has the innovative ability to detect and exploit XSS vulnerabilities. XSS Analyzer delivers some of the most advanced technology available for XSS testing, drawing from a knowledge base of hundreds of millions of exploits. The analyzer substantially reduces scan time by applying a smart learning system that mimics human behavior to find threats precisely and efficiently. With XSS Analyzer, Security AppScan Standard software is able to quickly find and remediate this important vulnerability.

Performing dynamic analysis with glass-box testing

Security AppScan Standard software offers glass-box testing, a form of integrated application security testing (IAST). Glass-box security testing is the latest evolution of hybrid analysis that combines dynamic (black box) analysis to simulate security attacks with an internal agent that monitors application behavior during the attack. With glass-box testing, Security AppScan Standard software provides more accurate test results and identifies vulnerabilities that traditional dynamic testing cannot detect. Through the powerful combination of security research and glass-box testing, the software delivers full coverage of OWASP Top 10 vulnerabilities and can identify non-reflected vulnerabilities, such as command execution, SQL injection, file inclusion, Lightweight Directory Access Protocol (LDAP) injection, log forging and more.

Glass-box testing also helps security teams collaborate with development organizations by providing precise information about vulnerabilities. With glass-box testing, Security AppScan Standard software identifies specific lines of code and provides details on how the application performs during attacks, which helps facilitate remediation. For this reason, many leading

developers are deploying glass-box testing earlier in their development cycles for a new level of precise testing not available with traditional dynamic or static analysis.

Performing hybrid analysis with JavaScript Security Analyzer

The adoption of Web 2.0 technologies in today's rich Internet applications expands the role of JavaScript as technologies such as Ajax, JavaScript Frameworks and HTML5 continue to proliferate. Most web applications make heavy use of client-side JavaScript code, which increases the likelihood of associated client-side vulnerabilities. Recent IBM research performed showed that several new Java-based, zero-day vulnerabilities were exploited in the first half of 2013.[1]

To address the latest risks, Security AppScan Standard software includes JavaScript Security Analyzer for static taint analysis of JavaScript code. JavaScript Security Analyzer detects a range of client-side security issues, such as Document Object Module (DOM)-based XSS, client-side open redirect, client-side SQL injection and many other HTML5-related security issues. Additionally, Security AppScan software is one of the first scanners to apply dynamic and static application security testing in the same scan for hybrid analysis.

Customizing and extending web vulnerability testing

Security AppScan Standard software includes a set of powerful customization features to provide greater control over web vulnerability testing:

- **IBM Security AppScan software development kit** offers a powerful set of interfaces that enable customizable invocation of each action in Security AppScan Standard software, from the execution of long scans to the submission of individualized custom tests.
- **IBM Security AppScan eXtensions Framework** permits users to develop and utilize add-ons to extend the functionality of Security AppScan Standard software. This framework enables users to customize and enhance existing functionality to fit their own processes, automate in-house activities and receive a large number of additional features and functionality by downloading open-source extensions from Security AppScan Standard eXtensions Framework.[3]
- **Pyscan web application security testing platform** helps auditors better utilize Security AppScan Standard software functionality when performing manual audits. Using the Python interface, users can easily establish and maintain a login state, access the Security AppScan Standard repository of scanned application data and generate compliance reports.

Why IBM?

IBM delivers a comprehensive portfolio of application security and risk management solutions. With advanced security testing and a platform for managing application risk, the Security AppScan portfolio delivers both the security expertise and the critical integrations with application lifecycle management that help organizations to not just identify vulnerabilities, but also reduce overall application risk. The Security AppScan software portfolio is complemented by Software-as-a-Service delivery options and robust professional service offerings including application security assessments, deployment services, advanced application security training, product training and more.

For more information

To learn more about IBM Security AppScan Standard software, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/appscan-standard/

For complete system requirements, please visit: **ibm.com**/support/docview.wss?uid=swg27024155

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2013

Please Recycle

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

[1] IBM X-Force, "IBM X-Force 2013 Mid-Year Trend and Risk Report," September 2013. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov16986&S_TACT=102PW63W

[2] Open Web Application Security Project (OWASP) 2013 Top 10 web application vulnerabilities: https://www.owasp.org/index.php/Top_10_2013-Top_10

[3] Access IBM Security AppScan Standard eXtensions Framework here: http://www.ibm.com/developerworks/rational/downloads/08/appscan_ext_framework/