

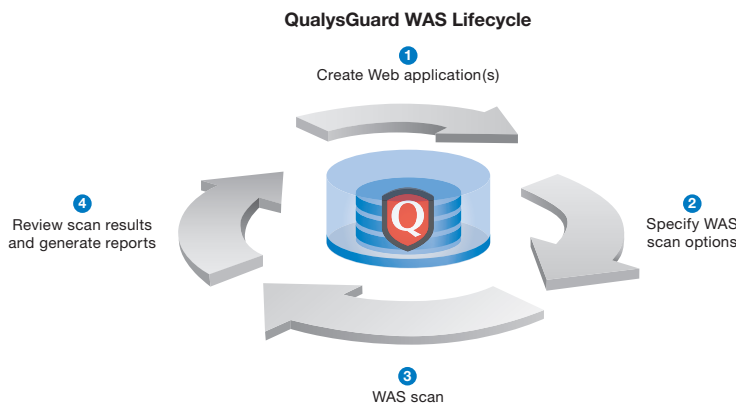
WEB APPLICATION SECURITY THAT SCALES TO UNLIMITED NUMBER OF WEB SITES – ON DEMAND

Vulnerabilities in web applications are now the largest vector of enterprise security attacks. Stories about exploits that compromise sensitive data frequently mention culprits such as “cross-site scripting,” “SQL injection,” and “web site misconfigurations.” Vulnerabilities like these fall often outside the traditional expertise of network security managers. The relative obscurity of web application vulnerabilities thus makes them useful for attacks. As many organizations have discovered, these attacks will evade traditional enterprise network defenses unless new precautions are put into action.

Web application security vulnerabilities usually stem from misconfigurations or programming errors with a web application programming language (e.g., Java, .NET, PHP, Python, Perl, Ruby), a code library, design pattern, or architecture. These vulnerabilities can be complex and may occur under many different circumstances.

Introducing QualysGuard® Web Application Scanning

To help customers assess and track web application vulnerabilities, Qualys® is introducing a new member to the QualysGuard® Security and Compliance Suite – QualysGuard Web Application Scanning (WAS) 1.0. The new service, delivered on demand, provides automated crawling and testing for custom web applications to identify most vulnerabilities such as those in the OWASP Top 10 and WASC Threat Classification, including SQL Injection and Cross-Site Scripting. Users can manage web applications, launch scans and generate reports using the familiar QualysGuard UI.



QualysGuard WAS Benefits

- Lowers total cost of operations by automating repeatable testing processes
- Identifies vulnerabilities of syntax and semantics in custom web applications
- Profiles the target application and performs authenticated crawling and auditing
- Improves accuracy and reduces false positives through profiling of web site
- Scales to scan any number of web applications, internal or external in production or development environments, using the QualysGuard Software-as-a-Service (SaaS) platform

“Enterprise-class web application scanning solutions are broader, and should include a wide range of tests for major web application vulnerability classes, such as SQL injection, cross-site scripting, and directory traversals. An enterprise solution should also be capable of scanning multiple applications, tracking results over time, providing robust reporting (especially compliance reports), and providing reports customized for local requirements.”

Building a Web Application Security Program Whitepaper
Securosis.com

“The number of vulnerabilities affecting Web applications has grown at a staggering rate. In 2008, vulnerabilities affecting Web server applications accounted for 54 percent of all vulnerability disclosures and were one of the primary factors in the overall growth of vulnerability disclosures during the year.”

IBM X-Force® 2008 Trend & Risk Report

QualysGuard WAS Features:

Crawling & Link Discovery — Embedded web crawler parses HTML and some JavaScript to extract links. Automatically balances breadth and depth of discovered links to crawl up to 5,000 links per web application.

Authentication — HTTP Basic, Digest and NTLM server-based authentication. Simple form authentication.

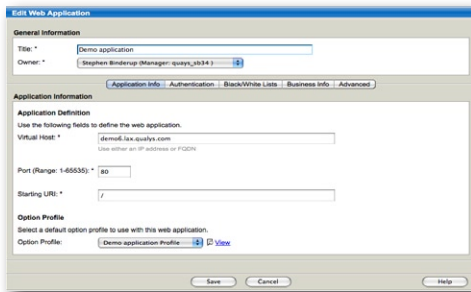
Black List — Prevents the crawler from visiting certain links in a web application.

White List — Instructs the crawler to only visit links explicitly defined in this list.

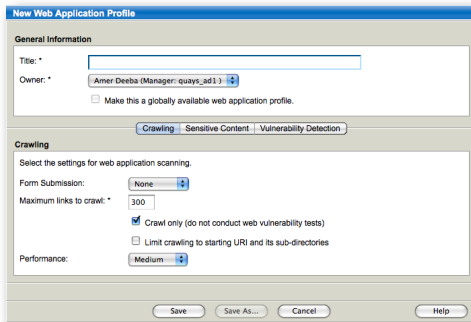
Performance Tuning — User-determined bandwidth level for parallel scanning to control impact on application performance.

Sensitive Content — Enables automated expression search for content in HTML, such as Social Security Number.

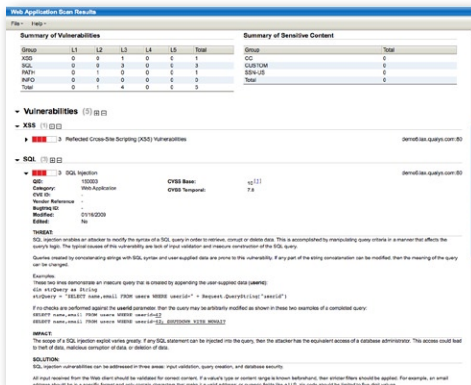
Workflows for Defining Scans and Reviewing Reports — Logical workflows provided for each web application. Reports provide deep visibility on vulnerabilities.



Create Web Application(s)



WAS Scan Options



Summary of Vulnerabilities						Summary of Sensitive Content	
Severity	L1	L2	L3	L4	L5	Total	Count
Info	0	0	1	0	0	1	0
Low	0	0	0	0	0	0	0
Med	0	1	0	0	0	1	0
High	0	0	0	0	0	0	0
Total	0	1	1	0	0	2	0

Severity	Count
Info	0
Low	0
Med	0
High	0
Total	0

WAS Scan Results

How QualysGuard WAS Works:

Crawler Phase

The sophisticated scanning engine features several techniques to effectively crawl a web site. Given only a user name and password, the crawler automatically identifies an HTML form login page, profiles the authentication process, and monitors the session state to ensure an authenticated scan remains authenticated throughout the crawl. The crawler attempts to cover as much of the target web site's functionality as possible by balancing the breadth and depth of the crawl in addition to avoiding redundant or recursive links. Also, the crawler profiles custom behaviors of the target web site, such as the appearance of default error pages, and uses the profile information to reduce false positives during the test phase.

Assessment Phase

The test phase of WAS searches for common vulnerabilities such as SQL injection, cross-site scripting, source disclosure, and directory traversal. The test engine relies on a mix of signatures and site profiling to accurately determine the presence of vulnerabilities. The tests currently focus on fault injection problems and distinguish between exploitable problems and simple information disclosure whenever possible.

Review and Reporting

The reporting engine breaks down problems into types of vulnerabilities such as cross-site scripting or SQL injection for a single web site, and it also generates summary vulnerability information across groups of web applications. Additionally, QualysGuard WAS introduces a new mechanism for managing user access to individual web application scans in order to accommodate different workflows for remediation and testing.

Pricing and Availability:

QualysGuard WAS is available as part of the QualysGuard Security and Compliance Suite. QualysGuard WAS annual subscriptions are licensed by number of Web Application(s), include an unlimited number of WAS scans and 24x7 support and updates.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • PO Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

