QUALYS®
ON DEMAND SECURITY

Discovering Vulnerable Web Applications

Vulnerabilities in web applications are a major vector for cybercrime. In large organizations, vulnerable web applications comprised 54% of all hacking breaches and led to 39% of compromised records, according to the *2012 Data Breach Investigation Report* by Verizon Business. In response, most enterprises have established an application security team and deployed some technology to minimize these vulnerabilities. But based on the statistics from Verizon, the processes and technologies used to manage risks in web applications generally are not robust and need to improve. The culprit is not having a reliable and complete catalog of all web applications in the enterprise, coupled with the inability to automatically scan hundreds and thousands of web applications for vulnerabilities.

This paper describes how large enterprises can effectively discover, catalog and scan web applications to control this major risk vector as part of their organization's overall vulnerability management program.

CONTENTS

A Wake-Up Call for Web Application Security

The vulnerability of web applications in large enterprises poses an enormous risk. As documented in the most recent data breach study by Verizon Business, 54% of successful exploits leveraged a web application vulnerability to capture 39% of compromised records.[1] Criminals are targeting web applications partly because enterprises have successfully shut down many traditional exploits with robust perimeter defenses. The study noted: "The inherent need for many web applications to be Internet-visible makes them a logical target; the potential to use them as an entry point into a corporate database makes them an attractive one."

The Verizon study found that web/application servers and database servers constituted the largest category of compromised assets in larger organizations – 33% of all breaches for both, with 82% and 98% of all records, respectively.[2] Once they've used a vulnerable web application to enter an organization's network, criminals can cause major damage to connected assets.

The danger is a false sense of security for enterprises that have established an application security team and deployed rudimentary controls to address the web application threat vector. Such organizations may think they are secure from web application exploits, but the data from Verizon suggest existing measures may not be adequately robust.

[1] Verizon Business, *2012 Data Breach Investigations Report*, pp. 32-33 at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
[2] Verizon Business, *2012 Data Breach Investigations Report*, pp. 39.

SCANNER USABILITY IS CRUCIAL FOR LARGE ENTERPRISES

Usability issues in other scanners can cripple their effectiveness:

- **Complex setup** allows a well-trained engineer to scan only 50-100 apps per year.
- **Siloed datasets** for each app resist integration into an enterprise-wide view.
- **No integration** with enterprise vulnerability management scanning data.
- **Single-workstation hosting** for a scanner limits scalability for concurrently scanning thousands of distributed web apps.
- **Internally hosted scanners** prevent real-world external scans and may inhibit code testing by developers.
- **Extensive training** required for complex scan setups.
- **Complex licensing and updates** inhibits scanning thousands of apps.
- **Weak support** inhibits effective programmatic scanning.

Factors Preventing Effective Web App Security

The strategy for reducing vulnerable web applications is to scan the apps and identify which have insecure code, then fix the code in each app to eliminate the respective vulnerability. Attacks are often based on fault injection, which exploits vulnerabilities in a web application's syntax and semantics. Examples of these include SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF). These attacks insert characters or scripts into request to alter logical workflow – and trigger an exploit. A Dynamic Application Security Testing (DAST) scanner is the fastest way to locate these vulnerabilities. Other vulnerabilities may require line-by-line review of application source code, reviewing and reconfiguring application or system settings, or re-architecting a solution. There is no silver bullet to discover all web application vulnerabilities, but using a good DAST scanner can quickly detect major issues and put your application security team on the path to remediation.

One factor that can jeopardize success is relying on a scanner with mediocre vulnerability detection capabilities. It's crucial for your scanner to accurately identify critical vulnerabilities such as SQL injection and XSS, and to continuously update signatures as threats evolve.

Another negative factor is using a scanner that cannot support the complexity and scale required by large enterprises with hundreds or thousands of web applications. A scanner's specifications may look good on paper, but if it falls short on enterprise-grade usability, relying on that tool places your organization in a severely vulnerable position. The sidebar describes eight limiting factors for enterprise usability.

Perhaps the biggest factor is more fundamental: many large enterprises do not have a catalog of all of their web applications. You can't point your scanner at an application if it's off the security team's radar.

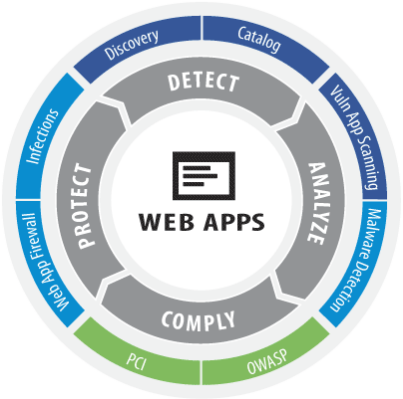
BEST PRACTICES FOR WEB APPLICATION SECURITY

Challenge	Tactic
1. Acknowledging the critical need for web application security.	• Organization must commit to place higher priority on eradicating web site vulnerabilities. • Devise and implement better processes and preventive technology.
2. Measuring potential fallout of a breach to justify a comprehensive program.	• Consider customers switching to competitors, lost sales, fewer people using your online store due to fear of a breach, fines for non-compliance, legal judgments, losing ability to accept payment cards.
3. Establishing an enterprise-grade web application security program.	• Address everything it takes to develop, deploy and maintain secure web applications. • Focus on obtaining enterprise-wide visibility, scale and results.
4. Using automation to discover and catalog web application services.	• Scanner should automate discovery and cataloging, which otherwise will overwhelm manual review.
5. Adding web application scanning to vulnerability management.	• Web application security is not just a footnote – it requires scalable processes and technology to address all web

	applications in context enterprise vulnerability management.
6. Weighing criteria to choose the right web site scanner.	• Quickly and effectively discover all web applications in the enterprise. • Catalog and organize all web apps. • Quickly and effectively scan all web applications for vulnerabilities. • Provide comprehensive reporting with an enterprise-wide view of web application security.
7. Being aware of top vulnerabilities and scanner capabilities.	• Technology must track top vulnerabilities (e.g. CWE/SANS Top 25, OWASP Top 10, Web Application Security Consortium Threat).
8. Scaling to support complex enterprise requirements without requiring extensive infrastructure, staff and support.	• Use a cloud solution. • Technology should support roles-based operation. • Technology should leverage existing vulnerability management processes.

Robust Web App Discovery and Cataloging With QualysGuard WAS

Automated web application discovery is a major new function of QualysGuard WAS, a cloud service fully integrated with the QualysGuard Cloud Platform and suite of security and compliance solutions. Discovery is the first step of the Web Application Scanning Lifecycle – and is a vital step because it establishes the baseline for enterprise-wide control of web application security.



QualysGuard WAS also scans your network to identify all HTTP services listening for web application activity. These services are automatically entered into your Web Application Catalog with the status "New." These applications can then be reviewed and organized by assigning a status such as "Rogue," "Approved" or "Ignored." Administrators can reference these statuses when determining which web applications should be added to the subscription for scanning. Once added, web applications have an "In Subscription" status within the Catalog.

The goal of web application service discovery is to populate an enterprise catalog with status and technical details for each web application. An example is shown below.

FEATURES OF QUALYSGUARD WAS

Unified Dashboard. Provides comprehensive view of scans, results and reports.

Discover, Catalog and Scan Web Applications. Ensures comprehensive scanning coverage and application management for large enterprises.

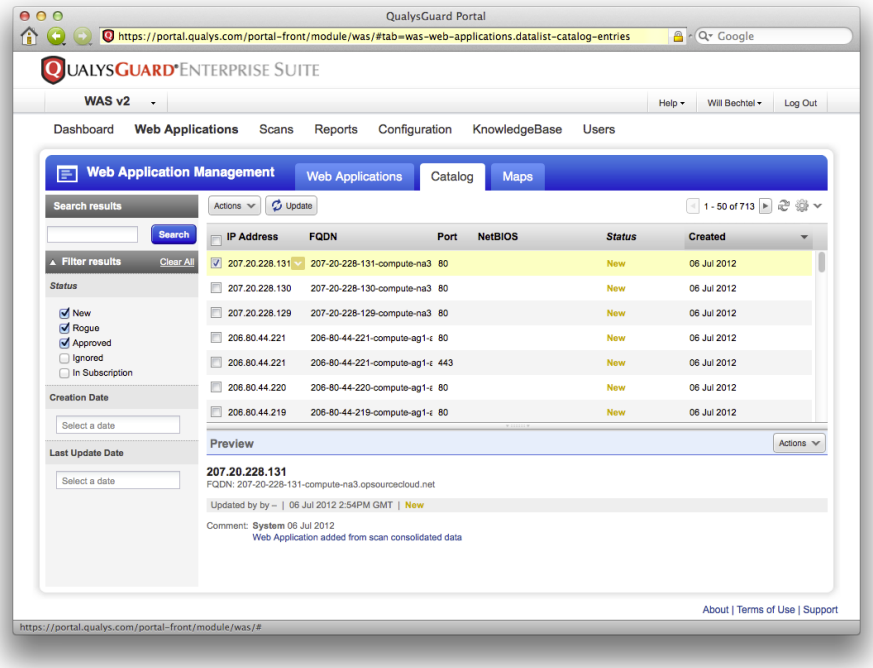
Interactive Reporting. Supports powerful analysis and secure distribution of scan results.

Selenium Integration. Enables complex authentication sequences and expands workflow crawl coverage.

Authenticated Scanning. Web crawler automatically identifies HTML form login page(s) and monitors the session state to ensure an authenticated scan remains authenticated throughout the crawl.

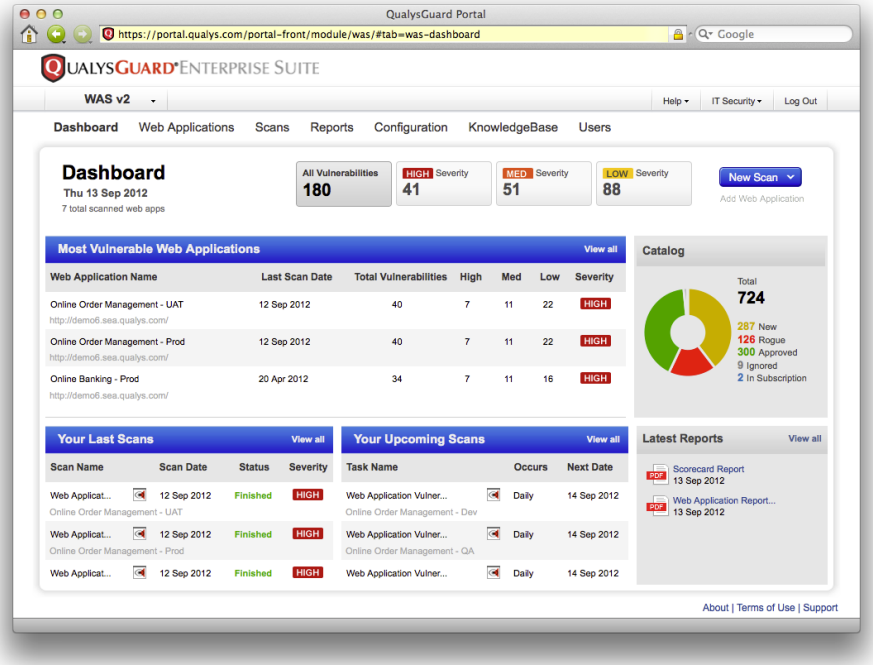
Targeted Scan Profiles. Analyzes the security of your web applications and identifies detected vulnerabilities, sensitive content data and information gathered data.

Scan Options. Robust options support enterprise requirements.



Large enterprises may also benefit from a customizable asset tagging mechanism, which enables user-defined hierarchical partitioning of web applications, scan data and reporting. Tagging can be used to limit user access to only those assets that they share a tag with.

A dashboard provides convenient access to all security data for web applications, scans, reports, configurations, users and a KnowledgeBase for vulnerability remediation. Details are accessed by drilling down from the dashboard. An example is shown below.



Benefits of QualysGuard WAS. Use the power and scalability of the cloud to identify web application risks throughout your enterprise.

- **Complete.** Discovers, catalogs and manages all web applications to ensure comprehensive coverage.
- **Productive.** Provides intuitive user interface and highly automated processes to increase productivity.
- **Economical.** Offers unlimited web application scanning that delivers the most cost-effective solution.
- **Scalable.** Enables automated scanning of thousands of web applications with centralized management for an organized approach that leverages cooperation in a large enterprise.

LEARN MORE

Learn more about how QualysGuard Web Application Scanning can help your enterprise to discover, catalog, scan and control these risks with a scalable cloud solution. For details, contact your Qualys sales representative and visit http://www.qualys.com/enterprises/web-applications/

About QualysGuard WAS

QualysGuard Web Application Scanning, or QualysGuard WAS, uses the scalability of the QualysGuard Cloud Platform to allow customers to discover, catalog and scan a large number of web applications. QualysGuard WAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass access controls. These web applications are often the main attack vectors for cyber attackers.

About QualysGuard Cloud Platform

Qualys' flagship product, QualysGuard Cloud Platform and its integrated suite of security and compliance solutions provides organizations of all sizes with a global view of their security and compliance posture, while drastically reducing their total cost of ownership. The QualysGuard solutions, including vulnerability management, policy compliance, web application scanning, malware detection and Qualys SECURE service for security testing of web sites, are used today by more than 5,800 organizations in 85 countries and perform more than 650 million IP audits per year.

QUALYS® ON DEMAND SECURITY

Qualys, Inc. – Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T: 1 (800) 745 4355

Qualys is global company with offices around the world.
To find an office near you, visit, **http://www.qualys.com**