Retina Web Security Scanner

powered by Acunetix

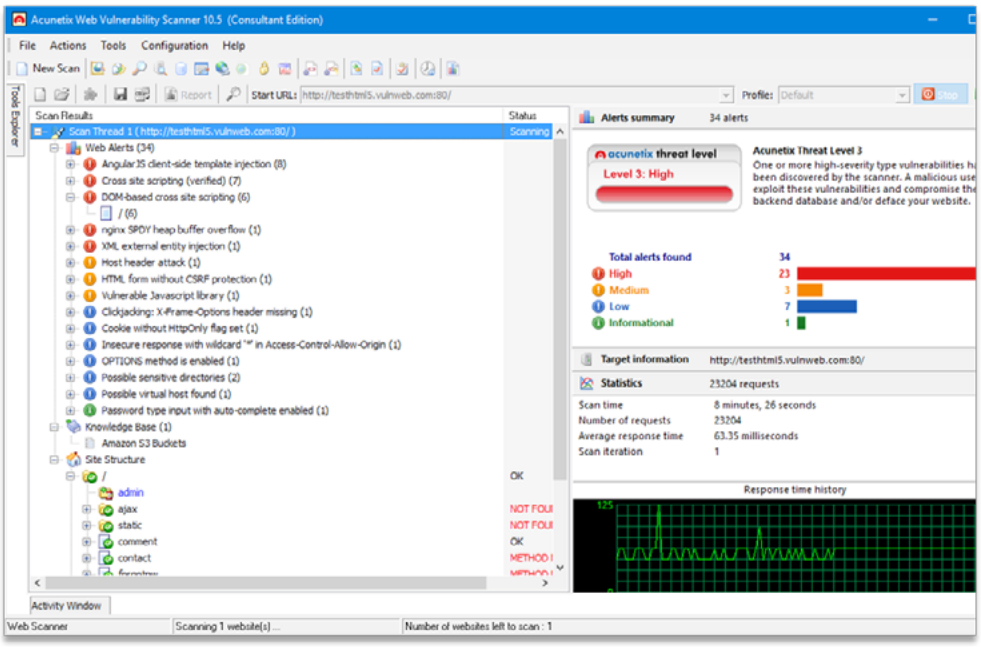
Comprehensive Vulnerability Scanning for Dynamic Web Applications

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

Websites and web-based applications are favored targets of today's advanced cyber attacks. And while web applications can be mission-critical for many organizations, they may have not been designed that way. Often developed internally from a combination of third-party platforms, tools and services – these types of applications pose a unique risk. Since they are custom built, most web applications will contain distinct vulnerabilities, including those that are implementation and not code-related, requiring assessment and remediation techniques that go beyond traditional network vulnerability management.

Crawl and scan for over 3,000 web vulnerabilities & misconfigurations.

Retina Web Security Scanner is a comprehensive application security testing solution designed for modern web and mobile applications that are built on technologies such as AJAX, SOAP, WADL, XML, JSON, GWT, and CRUD operations. With Retina Web Security Scanner, you get comprehensive application coverage against the most sophisticated attack vectors, backed by one of the lowest false positive and false negative rates in the industry. Lock out hackers at the front door and stop your web applications from providing an easy way into critical systems and information.



Retina Web application vulnerability scan results.

Key Capabilities

DEEPSCAN TECHNOLOGY

HTML5 crawling and scanning engine that fully replicates user interactions inside of a browser.

- Integrate with WebKit, the world's most widely used browser engine
- Crawl and scan HTML5 web applications, and execute JavaScript like a real browser
- Scan complex client-side web applications leveraging AngularJS, ReactJS, EmberJS, and more
- Detect advanced DOM-based Cross-site Scripting
- Scan for malicious URLs and test popular CMSs such as WordPress, Drupal, Joomla!, and others
- Support for CRUD requests, JSON, XML, GWT, AJAX, WSDL/SOAP, WCF/SOAP, and WADL/REST

ACUMONITOR TECHNOLOGY

Set-it-and-forget-it service that allows the scanner to detect out-of-band vulnerabilities, including:

- Blind Cross-site Scripting
- XML External Entity Injection
- Server-Side Request Forgery
- Out-of-Band SQL Injection
- Out-of-Band Remote Code Execution (OOB RCE)
- Host Header Injection
- Email Header Injection
- Password Reset Poisoning

Key Capabilities (cont...)

ACUSENSOR TECHNOLOGY

Unique capability that performs gray-box scans to inspect web app source code, while the application is running.

- Shows vulnerable source code line number and stack trace
- Shows vulnerable SQL queries
- 100% backend crawl coverage
- 100% verification of 12+ high-severity vulnerabilities
- Analyze server configuration for critical weaknesses

ACTIONABLE REPORTS

- Compare scan data to identify trends and progress
- Customize granular details on scans, server configs, alerts, external links, and more
- Respond quickly with remediation examples and recommendations
- Export XML data for integration with third-party systems
- Meet compliance reporting requirements for ISO, PCI, FISMA, OWASP, SOX, HIPAA, and more

ADVANCED FEATURES

- Flexible scan settings
- Easily customize scan scope
- Schedule scans with ease
- Import crawl data from third-party tools
- Dynamic crawl pre-seeding
- Test business logic with Selenium IDE
- Virtually patch application firewalls

Comprehensive Application Security Testing for Identifying Complex Website and Web Application Vulnerabilities

Retina Web Application Security Scanner automatically crawls and scans off-the-shelf and custom-built websites and web applications for SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and over 3,000 other web vulnerabilities.

- Crawl web pages that include technologies such as AJAX, SOAP/WDSL, SOAP/ WCF, REST/WADL, XML, JSON, Google Web Toolkit (GWT), and CRUD operations.
- Cover the OWASP Top 10 most critical web application security risks, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and more.
- Automatically crawl and scan complex password protected areas, including multi-step Single Sign-On, CAPTCHAs and multi-factor with an included login recorder.
- Audit web applications against a database of more than 1,200 known WordPress core, theme, and plugin vulnerabilities.
- Scan hundreds of thousands of web pages and applications without interruption, using Retina's multi-threaded architecture.

Advanced Protection for Custom Web Applications

Today's modern web applications are custom-built with unique site structures, parameter names and responses. Therefore, rather than checking for known vulnerabilities, Retina Web Security Scanner employs pen testing tools, heuristics, and behavioral analysis techniques to discover unknown threats that fly under the radar of signature-based scans.

- **DeepScan Technology:** Accurately crawl most content such as full HTML5, JavaScript, and AJAX-heavy client-side Single Page Applications (SPAs).
- **AcuMonitor Technology:** Discover out-of-band and blind vulnerabilities including SQLi, XSS, XXE, SSRF, and more.
- **AcuSensor Technology:** Increase vulnerability detection while significantly limiting the number of false positives.
- **Login Sequence Recorder:** Automatically crawl and test web applications that require complex authentication.
- **Advanced Penetration Tools:** Create and automate custom attack scenarios just like an attacker.

CONTACT

North America
Tel: 800.234.9072 or 480.405.9131
info@beyondtrust.com

EMEA
Tel: +44 (0)1133 970445
emeainfo@beyondtrust.com

APAC
Tel: +65 6701 8267
apacinfo@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com