DATASHEET

OpsMx

OpsMx DAST Powered by OWASP ZAP

Discover, Log, and Patch Application Vulnerabilities with Ease

OWASP ZAP

Dynamic Application Security Testing (DAST) has become an accepted best practice for strong application security. At the same time, many organizations are already managing multiple AppSec tools and don't want to add yet another one.

OpsMx now offers DAST as part of OpsMx Delivery Shield's catalog of application security tools. OpsMx Delivery Shield offers a comprehensive suite of application security capabilities covering all common application security categories (DAST, SAST, SCA, CSPM, etc.), pre-packaged and integrated for easy implementation and unified management. With OpsMx Delivery Shield, one application from one vendor provides a complete application security solution.

OpsMx DAST Powered by OWASP ZAP

OpsMx DAST, powered by OWASP ZAP, is used to find vulnerabilities in web applications by developers,QA teams, and security experts. Its ease of use, comprehensive features, and open source community have it ranked as one of the most downloaded web application penetration testers in the world. Here is a summary of its main capabilities and its primary advantages for software development and security testing.

Core DAST Features

OpsMx DAST, powered by OWASP ZAP, is used to find vulnerabilities in web applications by developers,QA teams, and security experts. Its ease of use, comprehensive features, and open source community have it ranked as one of the most downloaded web application penetration testers in the world. Here is a summary of its main capabilities and its primary advantages for software development and security testing.

Intercepting Proxy

Central to OpsMx DAST is its proxy component, which scans and catches the requests and responses between a browser and the target web application. This lets security testers and developers analyze all messages, change requests on the fly, and watch the response of the server. By acting as a "man-in-the-middle," OpsMx DAST can help the user identify hidden problems that might not be detected by black-box alone.

Spidering and Crawling

OpsMx DAST will automatically crawl (or "spider") a website to scan its entire architecture and source points of entry for testing. This is particularly useful when the web application is massive or dynamic which can be difficult to validate manually. In collecting URLs, parameters, and forms on a regular basis, OpsMx DAST can give a complete snapshot of the application surface and minimize potential missed vulnerability

Passive Scanning

OpsMx DAST scans the traffic going through the proxy without changing anything. This low-level method alerts us to security issues such as no security headers, information leakage and older server technologies.

Active Scanning

OpsMx DAST can also scan the application in depth, attacking it with targeted attacks by auto-sending bogus or malicious requests. These are the security tests for popular ones like SQL Injection, Cross-Site Scripting (XSS), and Command Injection. With OpsMx DAST digging deeper into different parts of an application, it is easy to find the severe vulnerabilities a hacker could attack.

OpsMx DAST Powered by OWASP ZAP

Fuzzer

OpsMx DAST fuzzing engine gives testers the opportunity to try various payloads, strings that should throw up strange behaviour in web apps. Input manipulation is an orderly approach by which Fuzzer function identifies loopholes and invulnerabilities for input verification. This is particularly useful for retesting API endpoints, form fields and query parameters.

Session Management

Contemporary web applications depend on session logs, cookies, tokens, or other fancy authentication. OpsMx DAST provides mechanisms to monitor session and user authentication states, so test cases are representative of reality. : Testers can model roles that are authenticated or non-authenticated, privilege escalation, or logic bugs in workflows.

Reporting and Alerts

OpsMx DAST automatically sorts issues discovered based on severity—from informative to risky. Alerts can be individualized and users can create full-blown reports easily. They are the record of discovery and the reference for corrective action.

Automation and Integration

OpsMx DAST connects seamlessly to common CI/CD pipelines and build environments. It has command-line and API interfaces, which allows for automated scanning in continuous integration frameworks such as Jenkins, GitLab, or GitHub Actions. Automated security inspections also enable developers to catch and fix bugs before they're too late.

Extensibility and Scripting

One of the great things about OpsMx DAST is that it is modular. Admins can add-ons and scripts to extend the capabilities of the application, and those can be written in JavaScript, Python, or Groovy. This extensive community of scripts and extensions cater to individual testing requirements and keeps OpsMx DAST updated on new threats.

OpsMx DAST HUD

The HUD is a new tool that shows data in the browser so learning and testing is much easier. Alerts, potential vulnerabilities, and key testing tools are all available right on top of the web app window — no need to scroll between windows or contexts.

Cross-Platform Availability

The OpsMx DAST is entirely written in Java and it's compatible with Windows, macOS and Linux. – It can be deployed in Docker containers for lightweight, reproducible and scalable testing (great for cloud-based applications).

Why Choose OpsMx DAST?

OpsMx DAST Powered By OWASP ZAP is a must-have tool for every web application security professional or team. Its extensive capabilities — from intercepting proxies to automated scanning, fuzzing, integration with CI/CD, and extensibility — enable teams to discover, log, and patch vulnerabilities with ease. Together with its open-source free source and user community, OpsMx DAST is a practical and instructive resource for all security novices as well as seasoned security experts interested in creating and defending secure web applications. More specifically, OpsMX DAST customers benefit from:

OpsMx DAST Powered by OWASP ZAP

OWASP ZAP

User-Friendly Interface

OpsMx DAST UI is less complex than command-line security tools designed for security specialists. No one, not even security experts, can easily learn to intercept requests, scans, and read rudimentary alerts. Meanwhile, advanced users can use custom scripts and settings to run more advanced penetration tests.

Comprehensive Vulnerability Coverage

OpsMx DAST uses various scanning methods (passive, active, fuzz testing) to identify all types of vulnerabilities. Automation of repetitive activities — OpsMx DAST frees testers for advanced analysis and sophisticated attack scenarios. This comprehensive vulnerability coverage significantly decreases the possibility of not having enough attention to web application security risks.

Integration with Development Pipelines

Modern development models emphasise CI/CD. Integrating OpsMx DAST with these pipelines means that teams can run automated scans in the build pipeline. This can be done to identify problems in a hurry (when they are most convenient and economical to repair), and encourage a security culture throughout the lifecycle of the software development process.

Flexibility for Different Testing Needs

You can deploy OpsMx DAST in a few different ways: as an application, as a command-line tool, or through REST APIs. This adaptability allows organizations to make OpsMx DAST fit their particular workflow. An QAS team, for instance, can use OpsMx DAST visual interface to run a scan quickly and a security analyst can script custom tests to analyse the problem more deeply.

Scalability for Any Organization

From a few developers to a multinational company, OpsMx DAST is scalable to an organization's needs. The user can start with simple manual testing and then proceed with the configurations, integrations and automation. Because it is extensible, OpsMx DAST also evolves as applications architecture evolves.

ABOUT US

OpsMx simplifies and accelerates comprehensive application security from developer to deployment building on AI-driven automation, open source security tools, and a deep understanding of the software delivery process. OpsMx enables tens of thousands of developers at both fast moving innovators and global enterprises to deliver more secure software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY