BACK TO BLOG

Top 7 DAST tools for 2024

James Harrison

February 6, 2024

What is Dynamic Application Security Testing?

Dynamic Application Security Testing (DAST) tools are a method of testing the security of your web applications where a running app is actively tested and probed using real traffic and requests. This evaluates the application from the “outside in”, by attacking the application like an attacker would, to find any security vulnerabilities.

As your application changes, grows and evolves, DAST scanning tools can continue to scan them so that your DevOps team can quickly fix any new or emerging issues before they can grow into more serious risks.

What's the difference between DAST and SAST?

While DAST solutions test the app from the outside, SAST (Static Application Security Testing) looks at the application from the "inside out" by searching for vulnerabilities in the source code.

DAST security testing tools test the application in runtime to see if it's vulnerable to common security vulnerabilities. As a form of closed box testing, DAST assumes the tester doesn't know the application's inner functions, such as those that appear only when the program is running.

As DAST requires a complete working application to do this, it's often used at later or the end phase of the development cycle. Testers need to interact with the application such as providing inputs, checking outputs, and simulating other actions typical of user interactions. These make sure the application is not susceptible to attacks such as cross-site scripting or SQL injection.

When should you use DAST or SAST?

Because SAST tests your application's internal source code early on, it helps developers to follow best practice and write secure code. SAST is technology-dependent, so any tool should support your programming language and dev framework to make sure everything is covered. As such, it can make remediation quick and easy.

On the other hand, DAST is technology-independent, because it tests the application when running from an external user perspective and doesn't just check your code. DAST security tools also look at the environment that the web application runs in. For example, it will help pinpoint a vulnerability in the application itself and in the web server configuration. It can even tell you if you're using a weak password. No other tool can do all that at the same time.

If possible, you should integrate both SAST and DAST in your CI/CD pipeline as part of a comprehensive DevSecOps approach. This will help your team integrate security without reducing the speed of deployment. But that's not always possible, practical or affordable, so in this article, we'll focus on the best DAST scanning tools for 2024.

4 best DAST tools for security teams in 2024

Intruder

Intruder is an automated attack surface management tool that includes continuous scanning for known weaknesses in a wide range of products, web apps and their underlying infrastructure. Its dynamic application security testing (DAST) scanner checks for common application layer vulnerabilities as well as known weaknesses in web application software, and provides comprehensive reports to show the security of your apps to customers and auditors.

Key benefits

- Easily add application scanning licenses to your subscription to scan against both authenticated or unauthenticated web applications
- Integrates easily into DevOps and CI/CD pipeline and issue trackers to save your developers time and effort
- Uses multiple commercial and open-source scanning engines including, OpenVAS, Zap, Tenable and Nuclei

Acunetix

Acunetix from Invicti is dedicated web application scanner that blends DAST and interactive application security testing (IAST) to detect over 7,000 vulnerabilities. This includes

scanning in hard-to-scan places like password-protected areas and multi-level forms.

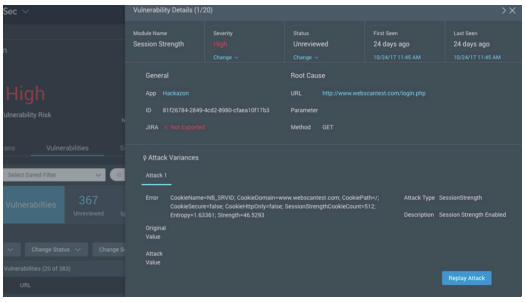
Acunetix dashboard

Key benefits

- High level of automation makes prioritizing high-risk areas and web applications easier
- Send tickets direct to developers by connecting to your CI/CD issue tracker
- Scans all web apps and complex web apps, including SPAs with HTML5 and JavaScript

Rapid7 InsightAppSec

InsightAppSec is a vulnerability management tool that's aimed at enterprises with large IT networks and security teams. Performs black-box security testing of web applications to automate identification, triage vulnerabilities, prioritize actions, and remediate application risk, providing reports to established security teams.



InsightAppSec dashboard

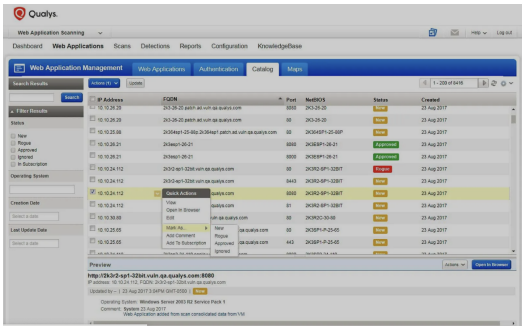
Key benefits

- Good visibility into risk, regardless of API or application complexity
- Universal Translator understands formats, protocols and dev technologies used in modern mobile and browser-based applications

- Pre-production and internal web applications on closed networks can also be scanned with optional on-prem scan engine

Qualys WAS

The Qualys WAS cloud-based application scanner discovers, detects, and catalogs web applications and APIs to uncover runtime vulnerabilities, misconfigurations, PII exposures, and web malware. Designed primarily for larger enterprises with hundreds of apps, it provides visibility and control by finding official, 'unofficial', and forgotten applications.



Qualys WAS dashboard

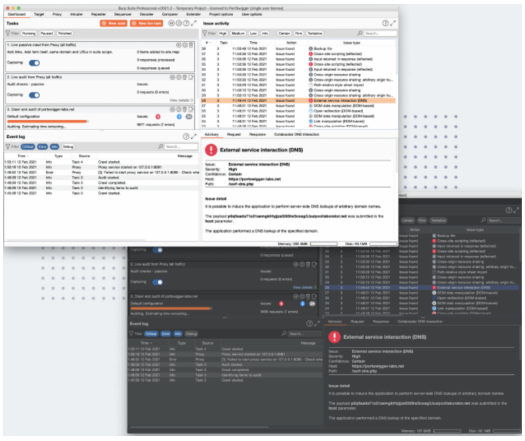
Key benefits

- Organizes data and reports using labels with customizable web application asset tagging
- Reports can be scheduled on command for responsive vulnerability management
- Integrates with Jenkins, AzureDevOps, Bamboo, and Team City

3 best DAST testing tools for penetration testers in 2024

Burp Suite Professional

Burp Suite's Porfessional edition has long been one of the industry's most trusted toolkits because of its comprehensive features and reliability. Its intercepting proxy feature allows users to intercept and modify HTTP requests and responses so you get a thorough analysis of the communication between web browsers and the target application to help you discover potential security vulnerabilities.



Burp Suite Professional dashboards

Key benefits

- Extensive range of features and functionality, including ‘active scanning’ for DAST-based automated vulnerability detection
- Out-of-band application security testing can find many otherwise invisible issues, including blind/asynchronous vulnerabilities
- Extensible with a wide range of add-on modules for targeted testing of a wide range of protocols and technologies

Nuclei

Open-source scanner Nuclei uses a vast library of community-powered templates to scan web applications. Seamlessly integrates into CI/CD pipelines for automated security testing as part of the development process to ensure continuous security and regression of custom vulnerabilities, and is actively maintained by the ProjectDiscovery team to provide an up-to-date scanning framework.

```
fuzzing:
  - part:
    query (default) - url query fuzz

  - fuzz:
    - {{variable to be replaced / fuzz}}

  - type:
    replace (default) - replaces the value of parameter with payload
    prefix - append the payload to existing parameter value
    postfix - prepend the payload to existing parameter value
    infix - place the payload in between the existing parameter value

  - mode:
    multiple (default) - multiple / all values to be replaced at once
    single - one parameter value to be replaced at a time

  - keys:
    list of parameter names to fuzz (exact match)

  - keys-regex:
    list of parameter regex to fuzz

  - values:
    list of value regex to fuzz
```

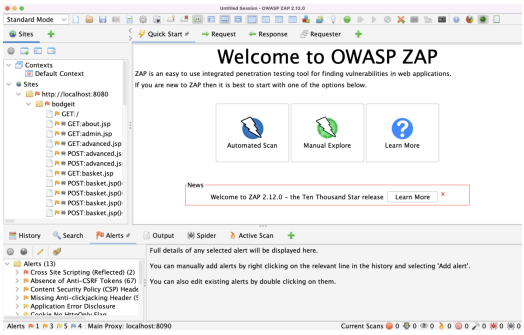
Nuclei fuzzing options

Key benefits

- Based on a simple YAML-based DSL makes it very easy to use and customize
- URL fuzzing finds well-known security vulnerabilities such as open redirects, XSS, SSRF, RCE, SQLi and more
- Shared execution context between templates means that all templates in the same workflow have access to the same information, such as named extractors and session data

ZAP

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP). ZAP is designed specifically for testing web applications and is both flexible and extensible.



ZAP portal

Key benefits

- Can be used as a stand-alone application or as a daemon process
- Provides functionality for a range of skill levels from developers to penetration testers
- Versions available for each major OS and Docker, so you are not tied to a single OS

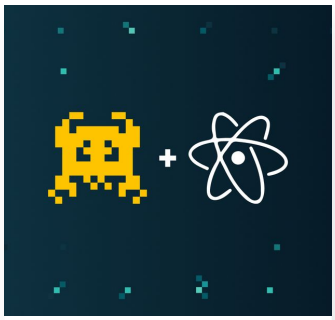
How Intruder can do the hard work for you

With web app attacks on the rise, it's important to prioritize web application security early in the development cycle. DAST tools give you timely insights into the behavior of web applications once they're in production and running, but penetration testing is another tried and tested form of web application security testing that you should consider using in combination with DAST – especially if you're using DAST tools for DevSecOps. Penetration testing provides a real-world demo of how an attacker might break into your web application.

Intruder provides dedicated penetration testing services in addition to its automated web application security scanner, which is a robust and effective DAST security testing tool that proactively scans your systems for emerging threats, notifying you as soon as new vulnerabilities are discovered. Intruder's Rapid Response can also manually check for the latest issues that are being exploited in the wild before automated scanners check for them. ***Why not try us for free for 14 days?***

Written by James Harrison

Recommended articles



Better together: Nuclei and Tenable

How do Tenable and Nuclei compare? We researched both to see how they work together for even better coverage.

James Harrison — February 1, 2024

How to build a vulnerability management program

One of the biggest challenges today is the lack of effective vulnerability management. But it doesn't need to be difficult if you follow our step by step guide.

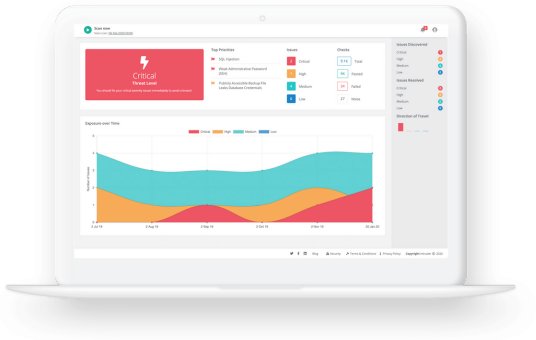
James Harrison — August 10, 2023

Patch now? Is Looney Tunables [CVE-2023-4911] as bad as everyone says?

Grab security updates for your Linux distributions because there's a security hole that can be easily exploited by rogue users, intruders, & malicious software to gain root access.

October 6, 2023

Ready to get started with



your 14-day trial?

TRY FOR FREE

intruder

SOLUTIONS

Developers

Start-ups and scale-ups

Enterprise

COMPARISONS

Intruder vs Acunetix

Intruder vs Qualys

Intruder vs Rapid7

Intruder vs Netsparker (Invicti)

Intruder vs Detectify

Intruder vs Pentest-Tools.com

USE CASES

Automated Penetration Testing

Cloud Vulnerability Scanner

Network Vulnerability Scanner

External Vulnerability Scanner

Internal Vulnerability Scanner

Website Security Scanner

COMPLIANCE

SOC 2

ISO 27001

PCI DSS

RESOURCES

Developer Hub

Help Centre

Blog

Guides

Glossary

Success Stories

Research

Webinars

COMPANY

About Us

Contact

Become a Partner

Careers (We're hiring!)

Protected by intruder

Contact us