Bright

A BRIGHT SECURITY WHITE PAPER`

The Unique Value of Bright's Dev-Centric DAST Solution

www.brightsec.com

Version 1.0 11/09/23

Executive Summary

Dynamic Application Security Testing (DAST) is a security testing methodology used to evaluate the security of an application or API. Unlike static analysis, which examines the source code, DAST operates in a compiled state or a running state by actively interacting with the application. The primary goal of DAST is to uncover potential vulnerabilities and security weaknesses that might arise from the application's functionality, configuration, and communication with external systems.

While DAST is an established solution category, it is important to note that most DAST tools rely on outdated technologies resulting in a number of inherent flaws that significantly diminish their benefit and value. Specifically, these tools struggle in crawling and mapping modern applications (e.g., single-page applications and APIs) resulting in missed critical findings. Additionally their scans result in a significantly high number of false positive findings leading to alert fatigue and time wasted on triage and validation. Another key limitation of legacy DAST solutions is that they were specifically built for use by AppSec professionals and can only be used to scan applications and APIs late in the development cycle. This results in security vulnerabilities being detected too late for remediation before the apps and APIs are released to production, greatly increasing the risk for the organization. These legacy DAST solutions fall short in their ability to provide value in organizations utilizing modern development practices.

Bright Security (Bright) was founded in 2018 with the goal of empowering AppSec and Development teams to partner in putting DAST in the hands of developers while enabling the AppSec team to provide the required governance and guidance. We did this due to our strong conviction that the only way to eliminate vulnerabilities and align AppSec with development practices in modern development environments is to empower developers to take an active role in finding and remediating vulnerabilities.

Our solution is purpose built to map and crawl modern web applications and APIs, validating findings to minimize false positives and provide a proof of vulnerability wherever possible. Bright's proprietary test engine offers the broadest test coverage in the industry covering over 10,000 payloads across both technical and Business Logic Vulnerabilities. The solution's enterprise-grade administration and reporting capabilities enable organizations to automate, scale and accelerate the deployment of the solution to thousands of users. Bright integrates across the entire software development lifecycle (SDLC) to provide early detection and remediation of vulnerabilities as early as the IDE and through pre-production.

In summary, Bright has a unique offering which makes it the right choice for organizations dealing with modern application security risks and challenges. The following sections expand on Bright's differentiation and benefits.

Dynamic Application Security Testing (DAST) is a security testing methodology used to evaluate the security of an application or API. Unlike static analysis, which examines the source code, DAST operates in a compiled state or a running state by actively interacting with the application. The primary goal of DAST is to uncover potential vulnerabilities and security weaknesses that might arise from the application's functionality, configuration, and communication with external systems.

While DAST is an established solution category, it is important to note that most DAST tools rely on outdated technologies resulting in a number of inherent flaws that significantly diminish their benefit and value. Specifically, these tools struggle in crawling and mapping modern applications (e.g., single-page applications and APIs) resulting in missed critical findings. Additionally their scans result in a significantly high number of false positive findings leading to alert fatigue and time wasted on triage and validation. Another key limitation of legacy DAST solutions is that they were specifically built for use by AppSec professionals and can only be used to scan applications and APIs late in the development cycle. This results in security vulnerabilities being detected too late for remediation before the apps and APIs are released to production, greatly increasing the risk for the organization. These legacy DAST solutions fall short in their ability to provide value in organizations utilizing modern development practices.

Bright Security (Bright) was founded in 2018 with the goal of empowering AppSec and Development teams to partner in putting DAST in the hands of developers while enabling the AppSec team to provide the required governance and guidance. We did this due to our strong conviction that the only way to eliminate vulnerabilities and align AppSec with development practices in modern development environments is to empower developers to take an active role in finding and remediating vulnerabilities.

Our solution is purpose built to map and crawl modern web applications and APIs, validating findings to minimize false positives and provide a proof of vulnerability wherever possible. Bright's proprietary test engine offers the broadest test coverage in the industry covering over 10,000 payloads across both technical and Business Logic Vulnerabilities. The solution's enterprise-grade administration and reporting capabilities enable organizations to automate, scale and accelerate the deployment of the solution to thousands of users. Bright integrates across the entire software development lifecycle (SDLC) to provide early detection and remediation of vulnerabilities as early as the IDE and through pre-production.

In summary, Bright has a unique offering which makes it the right choice for organizations dealing with modern application security risks and challenges. The following sections expand on Bright's differentiation and benefits.

Application Configuration and Management

Modern and innovative DAST solutions need to focus on scaling scans across hundreds or even thousands of applications and API endpoints. Additionally, they need to optimize for shorter scans that can be run early in the SDLC, without having to re-map or re-crawl the application for each scan.

Logical grouping for scaling the application inventory

Bright includes capabilities for scaling the application inventory by grouping apps and scans into “Projects”. Projects also enable teams to apply governance and permissions. These are key for ensuring only the right stakeholders can modify policies and how findings are reported.

Cached mapping

Bright enables mapping of web applications and APIs and storing that map as cache that can be used for testing without having to re-crawl or revalidate the application.

Incremental scans

Bright’s solution supports testing only parts of the application, with the emphasis on parts that have been added or changed (aka Delta Scanning).

Testing and Identifying Vulnerabilities

Modern and innovative DAST solutions need to have both breadth and depth of vulnerability testing. These solutions must cover both technical and business logic vulnerabilities and have the ability to effectively add and remove vulnerabilities as required to optimize scanning.

Wide/extensive coverage of test types and vectors

Bright’s coverage of vulnerability testing spans several key test types: Server-side, client-side, API, CVEs, business logic and legacy tests. These test types span across roughly 50 different vectors, such as OS Command Injection, HTML Injection, and XML External Entity attack.

Variations via payloads

Bright’s solution tests for variations in aforementioned vulnerabilities by deploying as many as 10,000 different payloads, e.g., manipulating and injecting different data in the header, body, and URL of HTTP requests.

Low false positive rate

Most DAST tools suffer from a high false positive rate, causing alert fatigue and resulting in the inability to prioritize true findings. Bright’s solution offers an industry low false positive rate at around 3% of all findings.

OWASP Top 10 and OWASP API Top 10

Bright effectively tests for virtually all of the OWASP top 10 and OWASP API Top 10 vulnerabilities based on popular benchmarks such as DVWA, BWAP, vAPI and Generic University.

Business logic tests

One of Bright's unique focus areas is the automation of business logic tests. This type of vulnerability test is not provided by any other DAST vendor and typically conducted only in manual penetration testing. Bright's DAST includes several business logic such as Constraint Bypass, ID Enumeration (BOLA), Mass Assignment, and Excessive Data Exposure. Tests are updated frequently.

CVEs

Bright's solution includes the option of scanning for approximately 1,500 high and medium vulnerabilities known as Common Vulnerabilities and Exposures, i.e., vulnerabilities in popular web platforms such as WordPress, Joomla, and Apache Web Server.

AI\LLM

Bright is the only DAST engine that has the capability to scan and check for AI\LLM vulnerabilities (prompt injection, etc...) which are part of the OWASP top 10 for LLMs.

Re-test and re-validate vulnerabilities

Bright enables re-testing or revalidating identified vulnerabilities with a single click, for example by producing a cURL command with the right payload.

Automation and Lifecycle

Modern and innovative DAST solutions need to support and enable frequent scans across multiple types of end-users and use cases, from scans triggered by changes to the application's codebase to local scans on the developer's own machine.

Scheduling

Bright's solution enables flexible scheduling of automated scans; for example during weekends or before software releases.

Automation using scripts

Bright's solution can be fully automated with code, either using the API or with shell scripts using the Command Line Interface (CLI). This automation can go well beyond scripts, for example consuming findings and generating alerts.

Developer triggered scans

Bright provides the unique ability for developers to either automatically or manually scan while they are developing right within the IDE with IDE plugins or as part of Unit Testing with UT solution integrations.

CI/CD scanning and other integrations

Bright's solution supports many use cases through the application scanning lifecycle, from triggering scans following changes to the codebase as part of Continuous Integration/ Continuous Deployment flows in GitHub or Azure Pipelines to automatically generating tickets for remediation in 3rd party products as Jira. In addition, Bright also supports correlating application security vulnerabilities with SAST findings through an integration with Snyk.

Remediation guidance

Bright's solution includes extensive remediation guidance for developers such as input sanitation and whitelisting.

Administration and Governance

As noted in the summary above, modern and innovative DAST solutions must focus on scaling scans across hundreds or even thousands of applications and API services. This kind of scale requires a governance and permissions model which ensures only the right end-users and stakeholders are able to view and modify scan configurations and results.

Scan configuration

Bright is able to control who is able to view and modify scan configuration, for example to ensure that only members of the security team are able to reduce the scope of scanned vulnerabilities but not other stakeholders such as software developers. Bright also enables receiving security events for critical changes.

Scan findings

Bright provides control of who is able to view and modify scan findings, for example to ensure that only members of the security team are able to mark findings as duplicates but not other stakeholders such as software developers. Bright also enables receiving security events for critical changes.

SSO

Bright provides extensive support for SSO platforms inheriting the rights provided within your corporate governance.

Reporting

Modern DAST solutions must provide robust reporting for web applications and API scanning across different domains, teams and organizations.

Inline developer environment reporting

For use cases and integrations outside of Bright's app, such as within the developer's environment (console and IDE). Bright offers inline reporting such that the developer does not need to leave her environment when she deploys tests.

AppSec Reporting

Bright provides a comprehensive set of reports across risk, compliance, ROI and continuous improvement right within our UI.

Extensive Reporting API

Bright has invested significant resources to make sure that all the data that is available in our reports is also available in our APIs so the data can be leveraged by 3rd party reporting apps, VM solutions etc.

OWASP Top 10 and OWASP API Top 10

Bright effectively tests for virtually all of the OWASP top 10 and OWASP API Top 10 vulnerabilities based on popular benchmarks such as DVWA, BWAP, vAPI and Generic University.

Target Mapping

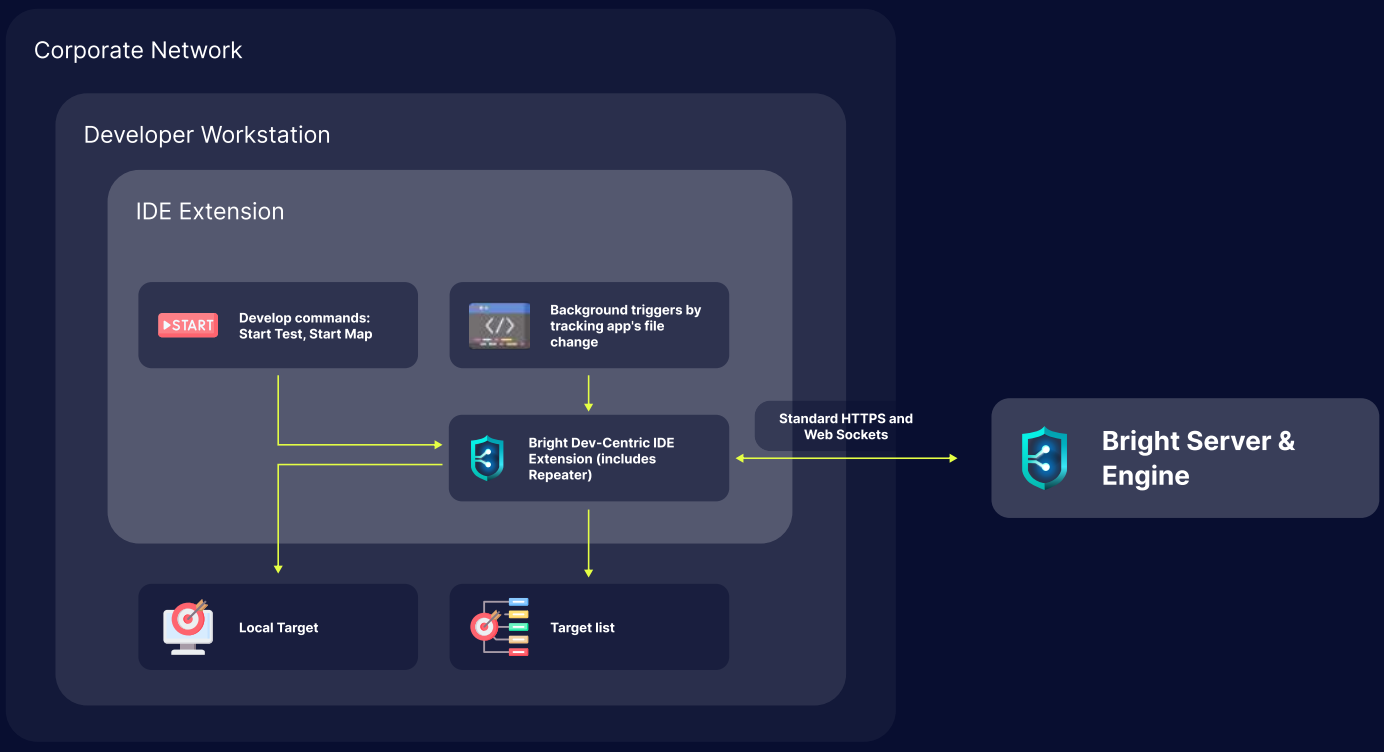
Bright has a unique ability to create an in depth target map based on a contextual understanding of certain parameters and request types. This allows Bright to not only correctly and deeply map application and API targets but to also execute both technical and business logic attacks in an efficient and advanced manner that is optimized for speed and accuracy once this information is available.

Parameter Type Intelligence

Unique ability to analyze each parameter value in requests and find its type, allowing tests to handle and manipulate it correctly.

Persistent Sitemap

Bright saves the discovery face for reusability and uniqueness with each discovery, allowing automation around delta scans and checking only newly added URLs\Entry Points of the system, saving time and providing accuracy and value.



Summary

Organizations utilizing modern development practices cannot afford to continue using legacy DAST solutions that leave them exposed and do not help them align their development and AppSec teams. Organizations should leverage modern DAST solutions that will enable them to put DAST in the hands of developers while AppSec teams focus on governance. This results in significant risk reduction and far better alignment between engineering and Appsec while driving significant positive ROI for the organization. Bright Security has invested significant resources to develop an enterprise-grade Dev-Centric DAST solution that is being used by some of the world's leading Financial institutions and Cyber Security companies.