Bright

IASTless IAST - The SAST to DAST Bridge

Bright Security White Paper

www.brightsec.com

Version 1.0 03/03/24

In the ever-evolving landscape of application security testing, the pursuit of a more efficient and streamlined approach is a constant endeavor. With the challenges posed by traditional Interactive Application Security Testing (IAST) methodologies, a new paradigm is emerging - one that eliminates the complexities associated with IAST deployment while enhancing the synergy between Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Welcome to the world of "IASTless IAST - The SAST to DAST Bridge."

What is SAST:

SAST (Static Application Security Testing) is a static analysis methodology that examines the source code, bytecode, or binary code of an application for security vulnerabilities without executing the program. Its strengths include early detection of issues in the development lifecycle, but drawbacks include false positives, limited coverage of runtime behaviors, and challenges in handling complex and dynamic code.

What is DAST:

DAST (Dynamic Application Security Testing) is a security testing method that evaluates an application in its running state by simulating real-world attacks. Its benefits encompass a realistic evaluation of security vulnerabilities within a live environment. However, potential drawbacks include restricted visibility into the source code and the possibility of later detection within the SDLC, given its dependency on a running target.

What is IAST:

IAST (Interactive Application Security Testing) is a security testing methodology that analyzes applications in real-time during runtime, providing dynamic insights into vulnerabilities and potential security threats. Its benefits include real-time detection of vulnerabilities, reduced false positives, and the ability to assess an application's security posture during actual usage.

IAST is designed to scrutinize the application's workflow during real-time usage, aiming to provide insights into which paths within the program and its code the relevant payloads or attacks traverse until they encounter the vulnerable section of the code.

The IAST Conundrum:

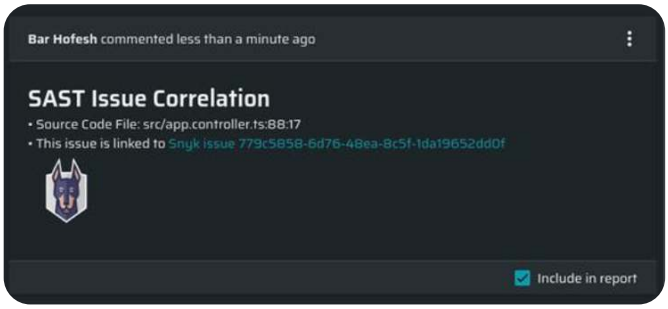
Traditional IAST solutions have long been plagued by intricate deployment processes, runtime tracing requirements, and the need for extensive support for complex frameworks. Additionally, generating traffic for IAST often demands full Quality Assurance (QA) automation or comprehensive end-to-end (e2e) automated testing coverage. These challenges have led security practitioners to seek a more efficient and effective approach that aligns with the dynamic nature of modern application development.

Bridging the Gap with Bright's Dev-Centric DAST:

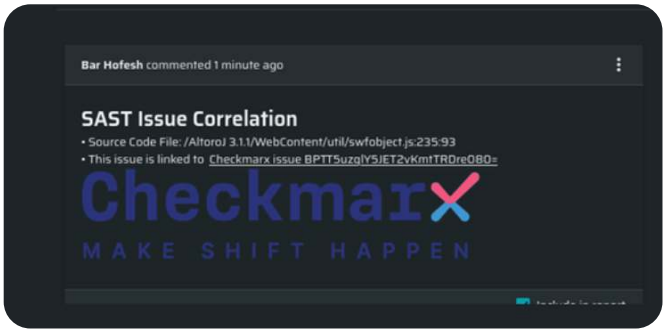
By leveraging DAST's capability to scan applications in runtime without the need for exhaustive setup, organizations can sidestep the hurdles associated with IAST. Bright's DAST provides a comprehensive assessment of an application's security posture without requiring the meticulous instrumentation and runtime tracing that IAST demands.

(Bright's DAST + SAST) > IAST:

In the IASTless IAST approach, we're threading a practical integration between Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), steering clear from the conventional reliance on Interactive Application Security Testing (IAST) for runtime analysis. Here, organizations can harness their existing SAST solutions in tandem with Bright's DAST. This collaboration gets a technical boost from Bright's SAST Validation logic.



This isn't just about cross-checking and correlation; it's about handing developers a nuanced technical insight that's often missing in IAST-centric setups. The SAST to DAST bridge pulls back the curtain, offering a ground-level view—from External Request to Internal Source Code. This technical tweak allows developers to pinpoint the specific request that flags a vulnerability and directly tie it to a file within the source code. It taps into the detailed insights provided by SAST, bringing a hands-on understanding of security issues.



Simply put, this technical maneuver equips developers with a more precise perspective on the security landscape. It lets them dive into the nitty-gritty details of vulnerabilities at a code level and enables them to make decisions based on in-depth technical understanding. The SAST and DAST synergy not only beefs up the technical efficiency of security assessments, but also fosters a collaborative atmosphere between development and security teams, embodying the technical essence of the IASTless IAST methodology.

Advantages of IASTless IAST:

Simplified Deployment:

Say goodbye to the intricacies of IAST deployment. IASTless IAST streamlines the security testing process, making it more accessible and manageable for development teams.

Reduced Overhead:

Eliminate the need for continuous runtime tracing and complex instrumentation. The integration between SAST and DAST minimizes the overhead associated with traditional IAST solutions.

Cost-Effective:

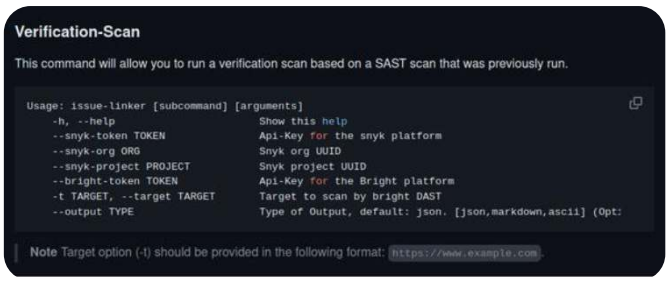
Leveraging existing SAST investments alongside Bright's DAST results in a cost-effective approach to application security. No need for additional tools or extensive training.

Enhanced Accuracy:

Correlating SAST and DAST findings provides a more comprehensive view of potential vulnerabilities, enhancing the accuracy of security assessments.

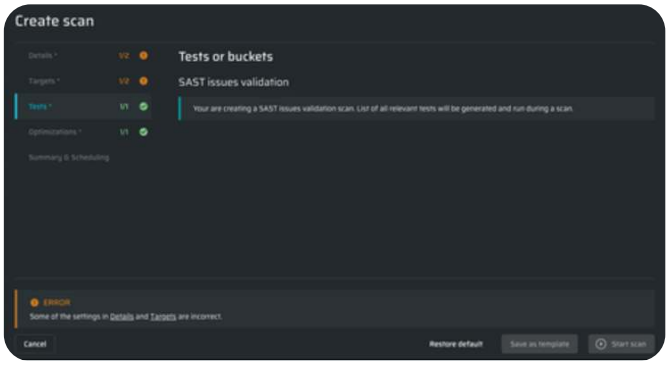
Implementing IASTless IAST:

To seamlessly incorporate the IASTless IAST approach into your application security workflow, leverage the power of Bright's IssueLinker—a sophisticated CLI tool designed for correlating and validating SAST results with Bright's DAST via a straightforward configuration. The integration of this tool introduces a level of professionalism and efficiency, ensuring a seamless sync between SAST and DAST findings.



Explore the capabilities of Bright's IssueLinker to effortlessly link and correlate security vulnerabilities identified by your SAST solutions with Bright's dynamic assessments. This command-line interface tool provides a user-friendly experience, allowing security teams to validate and prioritize findings efficiently.

Furthermore, Bright facilitates in-app integration with various SAST solutions through its "SAST Validation" organization configuration. This feature, documented in detail in the Bright documentation, streamlines the process of cross-referencing static and dynamic security findings, offering a professional and comprehensive security validation solution.



By incorporating Bright's IssueLinker and exploring in-app integrations, organizations can establish a robust IASTless IAST framework that not only simplifies the security testing process,

but also elevates the overall professionalism of the application security workflow. This comprehensive implementation ensures that the correlation and validation of SAST and DAST findings is seamless, providing a detailed and accurate assessment of your application's security posture.

Conclusion

The IASTless IAST approach represents a paradigm shift in application security, offering a more pragmatic and efficient alternative to traditional IAST methodologies and driving additional value from both your SAST and DAST solutions. By leveraging the strengths of both SAST and Bright's DAST, organizations can achieve a comprehensive and accurate understanding of their application security posture, while significantly reducing time wasted evaluating false positives. In addition, this approach simplifies deployment and minimizes operational overhead.

It's time to bridge the gap between static and dynamic testing and embrace a more streamlined and effective approach to securing modern applications!