Dynamic Application Security Testing-DAST Fundamentals

DAST often is called a web application vulnerability scanner. It looks for security vulnerabilities by simulating attacks on an application while the application is running in production. DAST leverages several real world application testing processes, including brute force login attacks to synthetic transactions.

Web applications enable many mission-critical business processes today, from public-facing e-commerce stores to internal financial systems. While these web applications can influence business growth, they also often hide potential weaknesses that, if left unidentified and not remediated, could quickly lead to a damaging data breach.

DAST is good at discovering external issues and risk vulnerabilities within the platform. This includes several security risks from OWASP's top ten. One of DAST's advantages is its ability to identify runtime problems without scanning the source code. DAST is excellent at finding server configuration and single and multi-factor authentication problems, as well as flaws that are only visible when a known user logs in. These tools are excellent for discovery a variety of security risks, including:

- Cross-site scripting
- SQL injection
- Command injection
- Insecure server configuration
- SSRF

DAST Challenges and Successes

DAST is a valuable testing tool that can uncover security vulnerabilities other tools can't. DAST is very limited to simulation for application of expected behaviors based on the design of the test. DAST can, however, attempt a variety of user level exploits, including password spraying and token reuse.

***DAST doesn't look at source code, it is not language or platform dependent.*

Businesses are investing into dynamic application security testing scanning tools as part of a security-forward approach to web application development. DAST tools provide context into how your web applications behave while they are in production. DAST solutions scan the production applications continuously. The output of this activity gives businesses the needed information to determine which systems need to get remediated.

How Does DAST Differ from Other Security Testing processes?

Developers within DEVOPS, SECOPS, and NETOPS teams have several testing tools available today. Many of these teams have moved ahead and deployed automation vulnerability scanning in real time for production and QA testing instead of engaging with one-off scanning engagements. Specifically NETOPS runs specific scanning tools to validate the integrity of the network layer, firewalls, and other adaptive controls supporting the DEVOPS and SECOPS teams. These tools in conjunction with DEVOPS are part of the overall scrum when new projects are created.

These tools vary in nature:

- Static application security testing -SAST

Focuses on scanning the source code. It operates in the CI/CD cycle, by scanning the source code and the binary code in order to identify coding flaws that go against industry best practices.

- Dynamic application security testing -DAST

DAST is an excellent method for preventing security regressions after remediations have been completed. DAST is an automated and continuous testing tool.

- Interactive application security testing -IAST

IAST analysis based on a combination of manual testing, scanning, and analysis of internal application flows. The benefit of IAST is its ability to link DAST-like findings to source code like SAST.

DAST vulnerabilities and the need for True en testing

While the DAST tool is suitable for reporting real threats in some use cases. Experienced code analysts can identify whether the risk applies to their portion of the platform. False positives can degrade the reliability and usefulness of the DAST tool. Having a human pen engagement in parallel to the DAST prior to enablement is a critical step in gaining value output from the scanning tool and verifying its efficacy.

Like many tools, hackers will scan the network looking for access to the privileged DAST tools. Hackers will even attempt to alter the DAST tool in order to change the course of the client's source. In a recent attack against Solarwinds, they used a DAST tool to scan inside of the company and inject vulnerable code within Solarwinds platform. "The attackers tamper with the development process of the software to inject a malicious component, such as a remote access tool, that will let them establish a foothold into the targeted organisation or individual."

An actual pen test itself would be performed against the DAST tool and other application security components. Pen testers can alter between a white box, gray box, and blackout testing methods during the DAST cycle. The output of the pen testing engagement can only benefit the DAST sequence. By knowing ahead of time that the DAST is vulnerable, this could save the organization problems later if a hacker attempts to take over the scanning tool. In addition, pen testers can verify the accuracy and correctness of setup of the tool.

***Without a pen test engagement against the DAST, IAST, and SAST tools, organizations will not trust the output of these tools.*

Pen testing as part of the DAST, SAST, and IAST work stream.

DAST, SAST, and IAST are important because developers don't have to rely solely on their own knowledge when building applications, especially in understanding ongoing security vulnerabilities. By conducting DAST during the product life cycle, developers will catch vulnerabilities in an application before it's deployed to the public. Using pen testing in the development cycle will also help overcome shortcomings with DAST testing. Vulnerabilities are left unchecked, this could lead to a data breach, resulting in major financial loss and damage to your brand reputation. Human error is always prevalent in an organization. People will make mistakes, especially in code development and leveraging automated tools like DAST. Pen testing will be a necessity in the application development process to ensure the testing tools are secure prior to enablement.

What makes CYBRI one of the Premier penetration testing companies?

Our outstanding penetration testing company services have attracted several clients that range from small startups to huge multinational companies. We are dedicated to improving cybersecurity across the board, so our services to your organization continue even after the pen test report has been delivered.

No matter the size of your organization, we will assess all of your cybersecurity needs from scratch to provide security measures tailored to your business needs. Our experts are always available to all of our clients in an advisory capacity should you wish to contact us.

Discuss your project with Us!

Click here to go to our site, fill out the form and the engagement team will contact you shortly!

https://cybri.com/red-team/