DAST Methodology

Our DAST methodology which includes automated testing with removing false positives is designed to cover both traditional and modern web applications across various architectures. The methodology ensures comprehensive coverage of the OWASP Top 10 risks and beyond. Below is the methodology that is used for an automated security review of web applications:

Application Overview/Pre-Requisites

As a foundational step, we take an overview of the application – core functionalities, business logic, use cases, and integration points. This includes reviewing the user/data setup, inter-tenant scenarios and data required to initiate automated scans. Gaining this context is critical to understanding the intended behaviour of the application, which in turn enables accurate identification of security risks that may arise from misuse, abuse, or misconfigurations.

Vulnerability Assessment with Provided Scanner

On the basis of resource attributes and control categories, an automated vulnerability scan is performed using scanner identified by client. This detects the vulnerabilities residing in the application, thus giving an actionable item list from application security standpoint. A comprehensive automated scan (excluding Denial of Service, Buffer Overflow & Brute-force) is performed on the application functionalities to uncover any vulnerabilities. Scan configuration is modified and scan is monitored to make sure the scanner is attacking application with an active session.

Removing False Positives

False positives in Dynamic Application Security Testing (DAST) scans can be a major obstacle for security teams, leading to wasted time, unnecessary remediation efforts, and missed vulnerabilities. By removing false positives, client can streamline their vulnerability management process, ensuring that their development teams focus only on real threats that need attention. To provide a key deliverable from the scans, false positives are removed with manual effort.

Mitigation Strategies

Based on the identified vulnerabilities, weaknesses, and overall risk posture—along with the system architecture and industry best practices—a mitigation plan is formulated. This includes a set of actionable, prioritized recommendations outlining the security measures required to effectively harden the environment.

Tools

Blueinfy team has expertise with most DAST tools and uses its experience in customizing scan configuration.