DAST (Dynamic Application Security Testing)

It is a type of security testing that focuses on identifying vulnerabilities and weaknesses in an application while it is running, i.e., in a dynamic state. DAST is often used to assess the security of web applications, APIs, and other software systems that interact with users or external entities.

Goal: simulate real-world attack scenarios by sending various inputs and payloads to the application, observing its responses, and analyzing the results for potential security issues.

It is a form of black box testing (as everything is behind the scene)

Eg. Burp Suite (commercial/licenced), OWASP ZAP (open source)

DAST (Dynamic Application Security Testing)

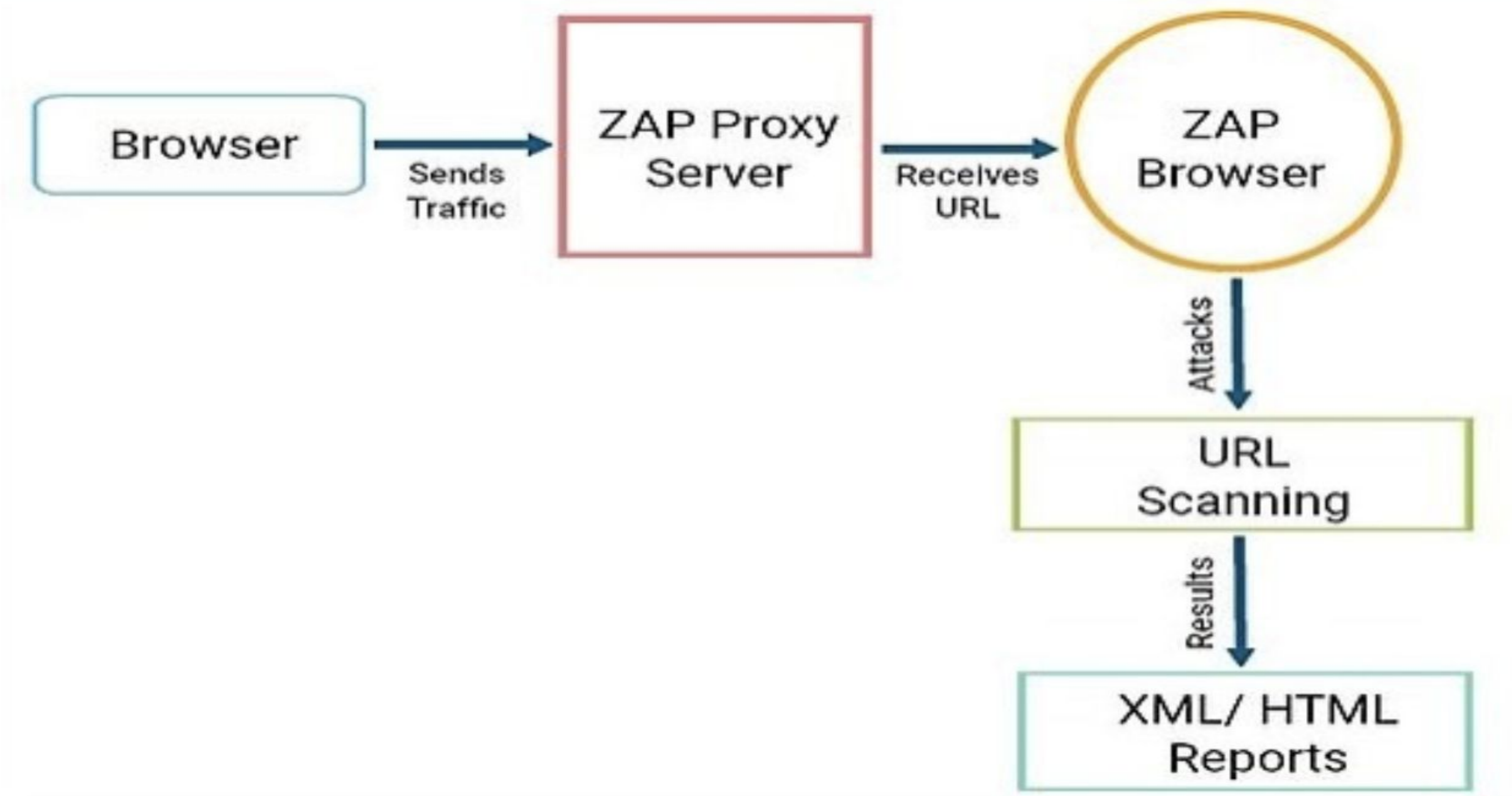
Crawling: The DAST tool explores the application by automatically navigating through different parts of it, submitting forms, and following links to reach as many pages and functionalities as possible.

Attack Simulation: The tool injects various attack payloads (e.g., SQL injection, cross-site scripting) into the application's input fields to check if it responds in a way that indicates a vulnerability.

Analysis: The tool collects and analyzes the responses from the application to detect potential security flaws, such as injection vulnerabilities, authentication issues, insecure configurations, etc.

Reporting: After the scan is complete, DAST generates a comprehensive report that highlights the identified vulnerabilities, their severity, and possible remediation steps.

DAST (Dynamic Application Security Testing)



Browser
Sends Traffic
ZAP Proxy Server
Receives URL
ZAP Browser
Attacks
URL Scanning
Results
XML/ HTML Reports