OWASP ZAP

powerful, open-source web application security testing tool developed by the Open Web Application Security Project (OWASP). It is designed to help developers and security professionals find and fix security vulnerabilities in web applications.

How it works ?

Setup : Download and Install
Target : Specify the URL of application
Spidering : ZAP automatically crawls through identify potential vulnerabilities.
Fuzzer: The fuzzer automatically tests discovered pages with different payloads to uncover security flaws.
Intercepting Proxy: Allows manual manipulation of HTTP/HTTPS requests and responses for deeper testing.
Results Analysis: ZAP generates reports and alerts on detected vulnerabilities, classifying them based on severity.
Automation Integration: ZAP can be integrated into CI/CD pipelines for continuous automated security testing during development.
Customization: Users can extend ZAP's capabilities using plugins to create custom tests and features.
Community-Driven: OWASP ZAP is actively maintained and improved through community contributions and feedback.