Paul Romer

CSD370

Module 5.2 Assignment

Security Testing

For each of the following provide a brief description (in your own words) of the term, a name and description of an automated tool to perform that task (if one exists), and when in the development process each one is implemented:

**DAST (Dynamic Application Security Testing)**

Tool Name: ZAP (Zed attack proxy)

Link to tool: https://www.zaproxy.org/getting-started/

Description: ZAP is a free, open-source penetration testing tool. It scans web application and then uses an active scanner to attack the discovered pages and functionality. This application is used during the testing phase of the SDLC.

I also read that Github actions has what I believe is a built in DAST system.

Source: https://github.com/resources/articles/security/what-is-dast

**SAST (Static Application Security Testing)**

Tool Name: SonarQube

Link to tool: https://www.sonarsource.com/open-source-editions/sonarqube-community-edition/

Description: An automated code quality and security tool that integrates into the IDE and CI/CD pipelines. It scans the codebase and identifies potential issues, highlighting them for the developer to fix. This application is used during the development phase of the SDLC.

**IAST (Interactive Application Security Testing)**

Tool Name: Contrast Assess

Link to tool: https://www.contrastsecurity.com/contrast-assess

Description: Contrast Assess is an IAST application that actively monitors your application, and user interactions with it to identify security vulnerabilities. On the website, it gives the analogy that it’s the security camera for your application. This application is used while the application is deployed (the implementation and maintenance phases.

**RASP (Runtime Application Self-Protection)**

Tool Name: Imperva RASP

Link to tool: https://www.imperva.com/products/runtime-application-self-protection-rasp/

Description: Imperva claims that RASP is the future of application security. RASP is an active security monitor at runtime that looks for known and unknown security vulnerabilities. It is used throughout the SDLC.