**Security Testing**

Liz Hinz

CSD370-A339: Secure Software Development

Module 5.2 Assignment

Professor Nathan Braun

April 13, 2025

DAST

Dynamic Application Security Testing can scan applications for potential software vulnerabilities after release. After running the code, all updates are sent to the designated security team for review and implemented with strong security practices. DAST is a type of black box testing, so it is conducted outside, meaning there is no internal access to source code and design. DAST scans for vulnerabilities used after the code is compiled and completed. This can only scan specific web applications. One automated tool for DAST is OWASP ZAP.

SAST

Static Application Security Testing is another form of security tool. SAST is a scan of the inner software completed before the program's release. It helps to identify issues early on but only on static code. SAST is supported for any applications. SAST can be integrated into an IDE for testing. SAST is a form of white box testing, meaning there is inside access to source code, design, and implementation. An example of an automated tool is SonarQube.

IAST

Interactive Application Security Testing tests web and mobile applications for any possible issues that occur when the application is running. IAST runs in a staging environment, looks for problematic parts of code, and returns errors to a developer or team. The source code is referenced after the code is built, which is referred to as the grey box testing methodology. An example of an automated tool is Invicti.

RASP

Runtime Application Self Protection is programmed into an application to work during runtime after the product is released. It is more security-focused for web or applications. RASP will automatically deploy additional security attempts if a vulnerability in the code is found. A tool for RASP is Prevoty.