Application Security for Developers and DevOps Professionals

Module 2 Glossary: Security Testing and Mitigation Strategies

Welcome! This alphabetized glossary contains many of the terms in this course. This comprehensive glossary also includes additional industry-recognized terms not used in course videos. These terms are essential for you to recognize when working in the industry, participating in user groups, and participating in other certificate programs.

Estimated reading time: 5 minutes

Term	Definition
Ad hoc testing	Random, informal testing without a plan for the discovery of a vulnerability.
BDD-Security	A security testing framework that uses behavior-driven development.
Burp Suite	A vulnerability scanner that is popular for scanning web applications. You can set up automated scans of a website or perform manual scanning by crawling the overall structure of a website or web application.
Code review	In code review, you use automated static analysis security testing and perform manual code inspection.
DAST	Dynamic application security testing (or DAST) evaluates the application from the outside in through the front end.
Dynamic analysis	Dynamic analysis is the process of testing and evaluating an application as it is executing.
Exploratory testing	Takes place outside of formal testing.
GitHub SCA	It is for viewing dependency packages and vulnerabilities while using GitHub.com.
GPL	General Public License.
Guantlt	A security framework that hooks into security tools for simplified integration.
Integration tests	For testing the integration of several coded classes within an application. You can perform integration tests across application tiers and a wide testing scope.
IAST	Interactive Application Self-testing (or IAST) scans for vulnerabilities during testing.
JSON	JavaScript Object Notation.
Mittn	Popular tool suite to include in continuous integration.
Nessus	It is a vulnerability scanner that scans operating systems, network devices, and critical infrastructure for vulnerabilities, threats, and compliance violations.
OWASP	Open Web Application Security Project.
OWASP Dependency-Check	It is an SCA for checking for vulnerabilities within project dependencies.
OWASP Dependency-Track	It is an SCA for identifying any risks within the software supply chain.
OWASP Software Component Verification Standard	It is a community-supported effort to build a sustainable framework for reducing risk within a software supply chain.
RASP	Runtime Application Self-Protection (or RASP) looks for assaults in the production environment.
Runtime protection	Runtime protection is a modern security mechanism that shields applications against threats while the applications are running.
SALSA	Supply-chain Levels for Software Artifacts (or SALSA) provides a security framework for improving integrity and preventing tampering by implementing standards and controls.
SAST	Static application security testing (or SAST) examines source code to identify security flaws that render your organization's applications vulnerable to attack.
SCA	Software component analysis (or SCA) is the process of determining which open-source components and dependencies are used in your application.
SCM	Source control management.
Security testing	Security testing provides a secure code baseline for development. It should be performed on all new codes to reduce the risk of impacts.
Snyk	A developer security platform for securing code, dependencies, containers, and infrastructure as code.
Static analysis	Static analysis examines all code or runtime binaries to help detect common vulnerabilities without executing code or running programs.
SWID Tags	Software Identification Tags (or SWID Tags) are standard to track software installed on managed devices.
Unit testing	For testing classes and methods to evaluate application programming interface (or API) contracts. You can perform unit testing on individual classes with limited scope.
Vulnerability analysis	It is a method of identifying possible application flaws that could jeopardize your application.
XML	Extensible Markup Language.
ZAP	Zed Attack Proxy (or Zap) is a vulnerability scanner. It is an OWASP tool and open-source software that uses spiders to crawl web applications.

Author(s)

- Gagandeep Singh

Changelog

Date	Version	Changed by	Change Description
04-08-2023	0.1	Gagandeep Singh	Initial version created