SOFTWARE COMPONENT ANALYSIS

DevSecOps Basics

What is Software Composition Analysis?

Software Composition Analysis is performed to identify the dependency packages/libraries for the project and check those against known vulnerabilities.

The following components are there in this phase:

- SCA tools i.e. Flawfinder, Graudit, Bandit, Spotbugs, SonarQube

People involved: Developers

External sources

- What is Software Composition Analysis? https://resources.whitesourcesoftware.com/blog-whitesource/sca-software-composition-analysis

Why is it important in DevSecOps?

It is very common for the projects to use 3rd party open-source libraries to extend their capabilities. However, as a downside, if the library has any security issue or vulnerability, it can also affect the project. By running the checks every time the DevSecOps pipeline runs, the risk of using vulnerable/outdated components.

What will you learn in this section?

The user will learn to perform the following tasks

- Perform the Software Composition Analysis on projects

Tools Covered

- Retire.js
- OSSAudit
- OWASP Dependency-Check

Labs

- Retire.js: Finding Vulnerable Libraries
  - A Kali machine is provided to the user with Retire.js installed on it. The source code for three sample web applications is provided in the home directory of the root user.

    Objective: Scan the web applications with Retire.js and find vulnerable/insecure libraries!
- OSSAudit: Auditing Python Packages
  - A Kali machine is provided to the user with OSSAudit installed on it. The source code for three Python web applications is provided in the home directory of the root user.

    Objective: Use OSSAudit utility to find issues in web applications!
- OWASP Dependency-Check
  - A Kali machine is provided to the user with Dependency-Check installed on it. The source code for three sample web applications is provided in the home directory of the root user.

    Objective: Use OWASP Dependency-Check to detect vulnerable code dependencies!

Safety: Python Dependency Check

Start