‹ Dashboard

AUTOMATED CODE REVIEW

DevSecOps Basics

What is Automated Code Review?

The Automated Code Review (ACR) phase scans the code for known mistakes, security issues and vulnerabilities. This is way efficient and easily scalable than Manual Code Review done for the same purpose. It is not to be confused with Peer Code review practice that is done to improve the code quality and find business/logical/flow mistakes.

The following components are there in this phase:

- ACR tools i.e. PMD, DevSkim, FindSecBugs

People involved: Developers

External sources

- What is Automated Code Review? https://en.wikipedia.org/wiki/Automated_code_review
- Benefits of Automated Code Review (ACR) over Manual Code Review (MCR) https://www.codegrip.tech/productivity/manual-vs-automated-code-review/

Why is it important in DevSecOps?

The Automated Code Review makes sure to weed out the security-related issues, mistakes of the developers on the code phase itself. The developers can remove these issues before even the project is built and test deployed. And, ACR will scale with the increase in release frequency.

What will you learn in this section?

The user will learn to perform the following tasks

- Finding security issues in code using PMD
- Locating security issues in code using DevSkim
- Using FindSecBugs to find security bugs in the code

Tools Covered

- PMD
- DevSkim
- FindSecBugs

Labs

- PMD: Finding Common Vulnerabilities
  - A Kali machine is provided to the user with PMD installed on it. The source code for two sample web applications is provided in the home directory of the root user.
    Objective: Analyze the given source code with PMD to find security issues!
- DevSkim: Code Security Review
  - A Kali machine is provided to the user with Devskim installed on it. The source code for three sample web applications is provided in the home directory of the root user.
    Objective: Use Devskim to find issues in the code!
- FindSecBugs: Securing Java Applications
  - A Kali machine is provided to the user with FindSecBugs installed on it. The source code of a sample web application is provided in the home directory of the root user.
    Objective: Use FindSecBugs to find issues in the code.