REPORT – SPRINT 3, WEEK 2 (28/05/2025)

# **Implementation of Dependency Scanning – OWASP Juice Shop**

## Tool Used: OWASP Dependency-Check

OWASP Dependency-Check was used to scan the OWASP Juice Shop project for known vulnerabilities in its third-party dependencies. The tool identifies vulnerabilities by analyzing the project's package dependencies and matching them with known CVEs from the National Vulnerability Database (NVD).

## Steps Followed:

• Cloned the OWASP Juice Shop project locally.

• Pulled the official OWASP Dependency-Check Docker image to avoid local dependency conflicts.

• Ran the dependency scan on the project directory using the Docker command.

• Configured the scan to output results in JSON format for potential dashboard integration.

• Saved the output report in a dedicated reports directory for reference and further processing.

## Docker Command Used:

docker run --rm -v "$(pwd):/src" owasp/dependency-check --scan /src --format JSON --out /src/reports --project "Juice Shop"

## Challenges:

• Some CVEs were false positives or not applicable to how the library is used in Juice Shop.

• Noise from devDependencies and transitive dependencies required manual filtering.

• No built-in filtering between production/test dependencies – needs post-processing.

## Recommendations:

• Focus on high/critical CVEs in production dependencies.

• Integrate Dependency-Check into the GitLab CI pipeline for automated scanning.