Hi everyone,

**Dependency Scanning**

Dependency scanning is a very important practice in software development that helps identify vulnerabilities in the libraries and frameworks used in an application. Since most modern applications rely on open-source components, they can inadvertently include known security issues if these dependencies aren’t monitored and updated regularly.

For example, GitLab has a dependency scanning feature integrated that automatically checks for vulnerabilities. By scanning dependencies during the build process, issues can be caught early, therefore the chances of bad or insecure code into put into production are minimal. The way it works is that it cross-references libraries against databases like the National Vulnerability Database (NVD) and flags any known vulnerabilities.

OWASP Dependency-Check takes a similar approach but offers an open-source option for scanning. It is very flexible as it works with several programming languages and ecosystems for sorts, like Java, .NET, and Phyton. It scans files like Maven POM’s, Gradle build files, and npm manifests, so it looks through the project’s configuration and manifest files to find dependencies and compare it to the NVD. Another good thing about OWASP is that very cost-efficient and customizable. All this without sacrificing critical functionality.

Dependency scanning should be part of the development workflow, particularly at the beginning of the project. Catching vulnerabilities early serves not only to strengthen the app but also helps with regulation compliance.

There are many tools available for dependency scanning, some of them are GitLab’s built-in scanner, OWASP Dependency-Check, Snyk, and Dependabot. Each one of them has unique features, but they all serve the same purpose: helping developers maintain secure and reliable applications by staying on top of potential risks in their dependencies.

<https://docs.gitlab.com/ee/user/application_security/dependency_scanning/>

<https://owasp.org/www-project-dependency-check/>