Dependency Scanning Documentation - OWASP Dependency-Check

# 🔍 Tool: OWASP Dependency-Check

Purpose: Detect known vulnerabilities (CVEs) in third-party libraries used in our apps (Todo List, Juice Shop).

# 🛠️ Setup

Using Docker:

docker run --rm \  
 -v $(pwd):/src \  
 owasp/dependency-check \  
 --scan /src \  
 --format JSON \  
 --out /src/reports \  
 --project "Todo List App"

Output File:

- dependency-check-report.json  
- Saved in /reports directory

# 📥 Integration with Dashboard

The JSON file is uploaded via the backend /upload endpoint.

Parsed and normalized using a standard schema:

{  
 "tool": "Dependency-Check",  
 "severity": "High",  
 "component": "org.springframework:spring-core",  
 "version": "5.2.3.RELEASE",  
 "cve": "CVE-2020-5421",  
 "description": "Spring Framework exposed to remote code execution"  
}

# ✅ Why It Matters

- Helps identify open-source risks  
- Essential for compliance and audit requirements  
- Complements SAST, DAST, and secret detection tools

# ⚠️ Challenges

- Reports can be noisy (false positives)  
- Sometimes packages need manual mapping (e.g., pom.xml parsing)