Security

1. Trivy

- **What it is:** An **open-source vulnerability scanner** for containers, filesystems, and Git repositories.
- **What it checks for:**
  - Vulnerabilities in **OS packages** (like Ubuntu, Debian, Alpine)
  - Issues in **application dependencies** (Node.js, Python, Java, etc.)
  - Misconfigurations in **Docker/Kubernetes**
- It's **easy to use** → just run one command and get results.
- **Installation**: **docker run --rm aquasec/trivy image alpine:latest**
- **Example Command:**
- **trivy image my-docker-app:latest**

  → This scans your Docker image for security issues.

---

2. OWASP Dependency Check

- **What it is:** A tool from **OWASP** (a popular web security community) that checks if your project's **libraries and dependencies** have **known vulnerabilities**.
- **What it checks for:**
  - Insecure versions of libraries (e.g., old Log4j version)
  - Maps them to CVEs (Common Vulnerabilities & Exposures)
- **Why it's useful:** Most hacks happen not because your code is bad, but because you use a **vulnerable library**.
- **How it works:**
  - Runs on your project (Java, .NET, Python, Node.js, etc.)
  - Gives a report of vulnerable dependencies.
- Download:- https://jeremylong.github.io/DependencyCheck/?utm_source
- **Example Command:**
- **dependency-check --project "MyApp" --scan ./my-app**

---

3. Prowler

- **What it is:** A **cloud security tool** for AWS, Azure, and GCP.
- **What it checks for:**
  - Misconfigurations (like an S3 bucket open to the public)
  - Compliance with standards (CIS, GDPR, HIPAA, etc.)

- **Why it matters:** Cloud accounts are common entry points for attackers. Misconfigured services = risk.
- **Installation:** **Requirements:** **Python 3 + AWS CLI configured**.
- **pip install prowler**
- **Example Command:**
- **prowler aws**

  → Runs security checks on your AWS account.

---

4. Dockle

- **What it is:** A **linting tool** for Docker images.
- **What it checks for:**
  - Best practices in Dockerfiles (don't run as root, avoid hardcoding secrets, etc.)
  - Security configurations
- **Why it helps:** Prevents you from shipping insecure Docker images.
- **Installation:** **choco install dockle**
- **Example Command:**

  dockle my-docker-app:latest