Continous Integration — https://github.com/OWASP/DevSecOpsGuideline

Build(Mandatory)

Build + Artifact Upload

reactjs

JOB - BUILD
- step1 → npm install
- step2 → npm run build

Lint

Code me jo bhi unwanted chize, ya kuch gadbad, uska pata lagana

Unwanted Chize Lint ka pata lgaya aur usko hata dia..

js | python | .yml

jslint

pylint

yAML linter

.java

java linter

https://github.com/super-linter/super-linter

Scans

Software Composition Analysis

Secret Scanning Tools

SCA Scan (To scan dependencies)

Static scanning (SAST Scan)

Container Scaning

IAC Scan

Dynamic Scanning (DAST Scan)

gittyleaks

Blackduck

SonarQube/ Checkmarx

ZED Attack Proxy

HomeWork

Jo bhi issues ye tool nikalte hai vo alg alg category ke hote hai..

Critical | High | Medium | Low

Ye do to solve karne hi padenge

https://ui.jhandu.shop

JOB - LINT

step1	biome linter
step2	markdown linter
step3	json linter
step4	yml linter
step5	css linter

biome-win32-x64.exe lint .\src\

Download biome exe
Run biome lint

Download mdlint
Run mdlint

Download yamllint
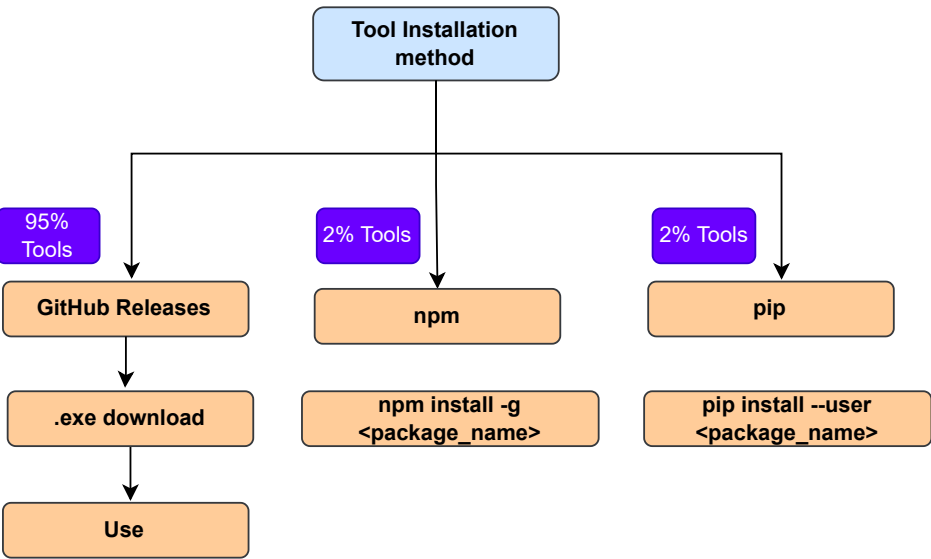Run yamllint

Download csslint exe
Run csslint

Linting is the process of automatically checking source code for errors, bugs, stylistic issues, and suspicious patterns to improve code quality and maintain consistency.

Tool Installation method

95% Tools → **GitHub Releases** → .exe download → Use

2% Tools → **npm** → npm install -g <package_name>

2% Tools → **pip** → pip install --user <package_name>

App Pipeline Revision

Code ka Quality - SonarQube

Bugs | Code Coverage | Vulnerabilities

| BlackDuck |
| Checkmarx |
| Prisma |
| Trivy |
| Veracode |
| semgrep tool |
| synk |
| checkov |

SonarQube

1. Install and Configure - Sonarqube server

2. Install SonarScanner - Ek tool hai jo code ko utha kar sonarqube server pr bhjta hai

3. Scan repo and project code

4. Quality Gates set

Linting Tool

cli tool - path
Pura scanning local pr ho jata hai..

Download tool cli

Run tool cli

SonarQube

Pura end to end scan

- Syntax violations
- Security vulnerabilities
- Programming errors
- Coding standard violations
- Undefined values

Tools

CLI Tool | **Server - Client cli Tool**

SonarQube Server

Processing and Reporting

Secret Scanning → Sonar CLI Client Upload code to server → Build → Publish Artifact

---

Code → Static Scanning → Server → DAST Scanning

→ Cost Analysis