Maven Lockfile

4th KTH Workshop on the Software Supply Chain 2025

Presentation by Elias Lundell

AGENDA

- Why
- What (is)
- How (to use)

WHY LOCKFILES?

- Deterministic builds
- Integrity
- Version ranges
- Diff dependencies
- Visualize full dependency tree

WHAT IS MAVEN LOCKFILE?

No native lockfiles in Maven.

State of the art plugin to generate, validate and rebuild (freeze) from lockfiles.

Github Action to generate and validate lockfiles in CI/CD.

Since maven 3.9.x:

+ Verify integrity with trusted checksums

- Difficult to rebuild from trusted checksums

MINIMAL EXAMPLE
SINGLE DEPENDENCY

```xml
<project>
  <modelVersion>4.0.0</modelVersion>

  <groupId>com.mycompany.app</groupId>
  <artifactId>custom-app</artifactId>
  <packaging>jar</packaging>
  <version>1</version>
  <properties>
    <maven.compiler.target>11</maven.compiler.target>
    <maven.compiler.source>11</maven.compiler.source>
    <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
  </properties>
  <dependencies>
    <dependency>
      <groupId>org.junit.jupiter</groupId>
      <artifactId>junit-jupiter-api</artifactId>
      <version>5.9.2</version>
      <scope>test</scope>
    </dependency>
  </dependencies>
</project>
```


```json
{
  "artifactId": "custom-app",
  "groupId": "com.mycompany.app",
  "version": "1",
  "lockFileVersion": 1,
  "dependencies": [
    {
      "groupId": "org.junit.jupiter",
      "artifactId": "junit-jupiter-api",
      "version": "5.9.2",
      "checksumAlgorithm": "SHA-256",
      "checksum": "f767a170f97127b0ad3582bf3358eabbbbe981d9f96411853e629d9276926fd5",
      "scope": "test",
      "resolved": "https://repo.maven.apache.org/maven2/org/junit/jupiter/junit-jupiter-api/5.
      "selectedVersion": "5.9.2",
      "included": true,
      "id": "org.junit.jupiter:junit-jupiter-api:5.9.2",
      "children": [
        {
          "groupId": "org.apiguardian",
          "artifactId": "apiguardian-api",
          "version": "1.1.2",
          "checksumAlgorithm": "SHA-256",
          "checksum": "b509448ac506d607319f182537f0b35d71007582ec741832a1f111e5b5b70b38",
          "scope": "test",
          "resolved": "https://repo.maven.apache.org/maven2/org/apiguardian/apiguardian-api/1.
          "selectedVersion": "1.1.2",
          "included": true,
          "id": "org.apiguardian:apiguardian-api:1.1.2",
          "parent": "org.junit.jupiter:junit-jupiter-api:5.9.2",
          "children": []
        },
        {
          "groupId": "org.junit.platform",
          "artifactId": "junit-platform-commons",
          "version": "1.9.2",
          "checksumAlgorithm": "SHA-256",
          "checksum": "624a3d745ef1d28e955a6a67af8edba0fdfc5c9bad680a73f67a70bb950a683d",
          "scope": "test",
          "resolved": "https://repo.maven.apache.org/maven2/org/junit/platform/junit-platform-
          "selectedVersion": "1.9.2",
          "included": true,
          "id": "org.junit.platform:junit-platform-commons:1.9.2",
          "parent": "org.junit.jupiter:junit-jupiter-api:5.9.2",
          "children": [
            {
              "groupId": "org.apiguardian",
              "artifactId": "apiguardian-api",
              "version": "1.1.2",
              "checksumAlgorithm": "SHA-256",
              "checksum": "b509448ac506d607319f182537f0b35d71007582ec741832a1f111e5b5b70b38",
              "scope": "test",
```

MINIMAL EXAMPLE
SINGLE DEPENDENCY

```xml
<project>
  <modelVersion>4.0.0</modelVersion>

  <groupId>com.mycompany.app</groupId>
  <artifactId>custom-app</artifactId>
  <packaging>jar</packaging>
  <version>1</version>
  <properties>
    <maven.compiler.target>11</maven.compiler.target>
    <maven.compiler.source>11</maven.compiler.source>
    <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
  </properties>
  <dependencies>
    <dependency>
      <groupId>org.junit.jupiter</groupId>
      <artifactId>junit-jupiter-api</artifactId>
      <version>5.9.2</version>
      <scope>test</scope>
    </dependency>
  </dependencies>
</project>
```


```
                "resolved": "https://repo.maven.apache.org/maven2/org/apiguardian/apiguardi
                "selectedVersion": "1.1.2",
                "included": false,
                "id": "org.apiguardian:apiguardian-api:1.1.2",
                "parent": "org.junit.platform:junit-platform-commons:1.9.2",
                "children": []
              }
            ]
          },
          {
            "groupId": "org.opentest4j",
            "artifactId": "opentest4j",
            "version": "1.2.0",
            "checksumAlgorithm": "SHA-256",
            "checksum": "58812de60898d976fb81ef3b62da05c6604c18fd4a249f5044282479fc286af2",
            "scope": "test",
            "resolved": "https://repo.maven.apache.org/maven2/org/opentest4j/opentest4j/1.2
            "selectedVersion": "1.2.0",
            "included": true,
            "id": "org.opentest4j:opentest4j:1.2.0",
            "parent": "org.junit.jupiter:junit-jupiter-api:5.9.2",
            "children": []
          }
        ]
      }
    ],
    "mavenPlugins": [],
    "metaData": {
      "environment": {
        "osName": "Mac OS X",
        "mavenVersion": "3.8.2",
        "javaVersion": "21.0.5"
      },
      "config": {
        "includeMavenPlugins": false,
        "allowValidationFailure": false,
        "includeEnvironment": true,
        "reduced": false,
        "mavenLockfileVersion": "5.4.3-SNAPSHOT",
        "checksumMode": "local",
        "checksumAlgorithm": "SHA-256"
      }
    }
  }

```

HOW TO USE?

:generate

Creates lockfile. Can either calculate checksums from local repository (default) or download them from maven-central (or other repository).

:validate

Validates all dependencies against lockfile. Ensures correct versions and untampered local repository.

:freeze

Create pom with all dependencies, direct and transtivie, to rebuild from lockfile.

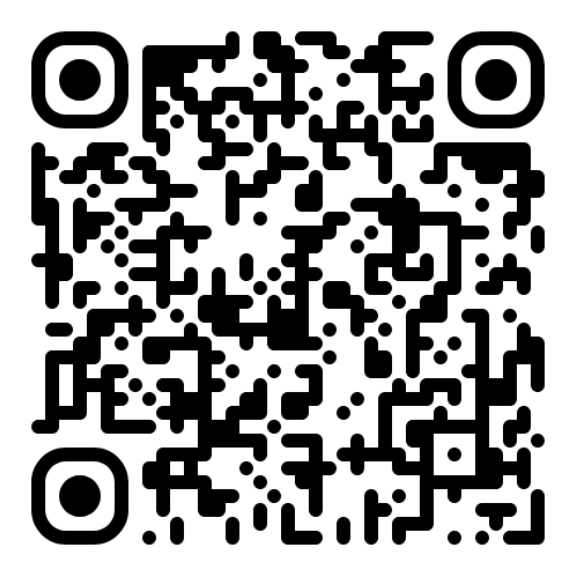
DEMO

GITHUB ACTION

- Automatically update lockfile
- Validate lockfile in PRs and main branch

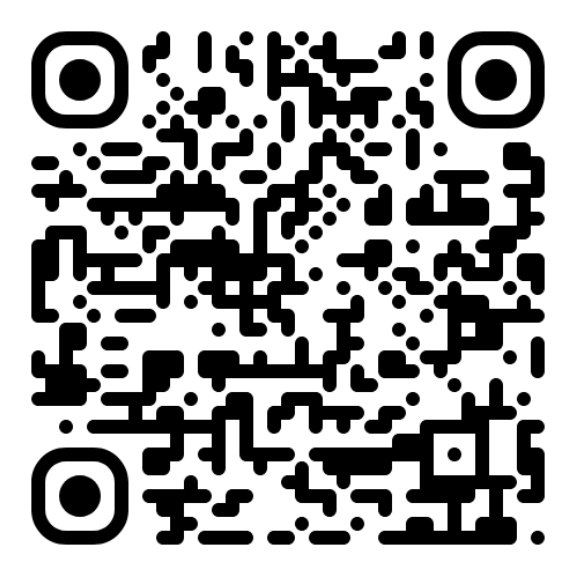
```yaml
name: Lockfile
on:
  pull_request:
  push:
    branches:
      - main

jobs:
  check-lockfile:
    permissions:
      contents: write
    runs-on: ubuntu-latest
    steps:
      - name: run maven-lockfile
        uses: chains-project/maven-lockfile@3e6d390f9f6ac757c7af9f120b51ebd5e4279b88 # v5.5.0
        with:
          github-token: ${{ secrets.GITHUB_TOKEN }}
          include-maven-plugins: true
```

THANKS FOR LISTENING!



Github Repository

https://github.com/chains-project/maven-lockfile



Github Action

https://github.com/marketplace/actions/maven-lockfile