Making a Lockfile for Maven

Adam Kaplan, Red Hat

OpenSSF Community Day
NORTH AMERICA 2026

whoami

Adam Kaplan (he/him)

- Software Engineer at Red Hat
- Open source maintainer

SHIPWRIGHT

CD.FOUNDATION

What is a lockfile?

The Design Space of Lockfiles

Université de Montréal

KTH VETENSKAP OCH KONST

Source

Provenance

Is it complete?

Integrity

Checksums

Signatures

Automatic

On by default

Integrated with tools

Python vs. JavaScript

Python

- Poetry - `pyproject.toml` -> `poetry.lock`
- Pipenv - `Pipfile` -> `Pipfile.lock`
- Uv - `pyproject.toml` -> `requirements.txt`

New standard - `pylock.toml` (PEP-0751)!

JavaScript

- Npm - `package.json` -> `package-lock.json`
- Yarn - `package.json` -> `yarn.lock`
- Pnpm - `package.json` -> `pnpm-lock.yaml`

No cross-tool standard

Maven Lockfile Plugin

OpenSSF Community Day
NORTH AMERICA 2026

Ingredients List

Code Dependencies

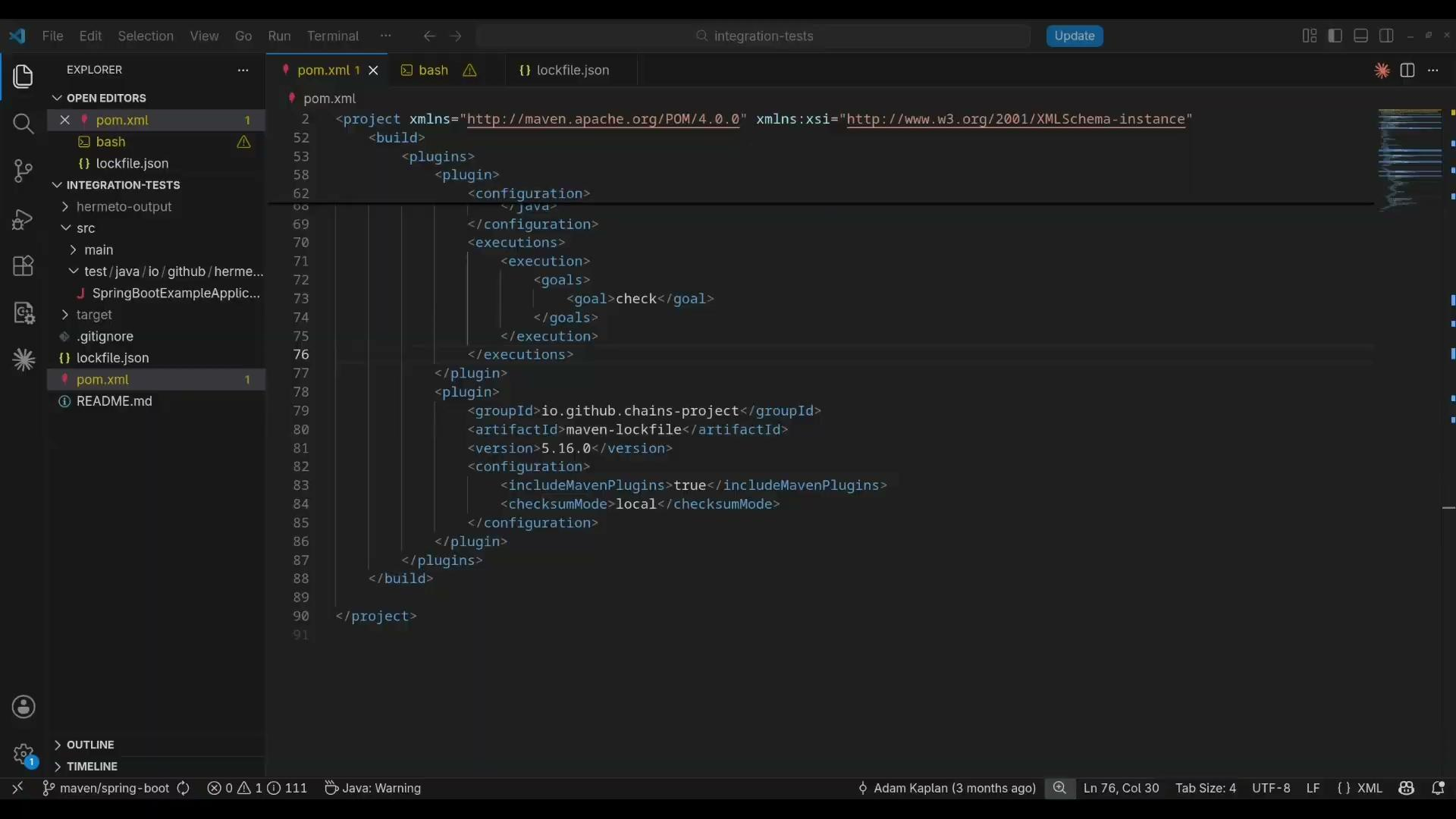
Compile
Runtime
Provided
Test

Plugins

Artifacts
Documentation
Automated testing
...anything!

Metadata

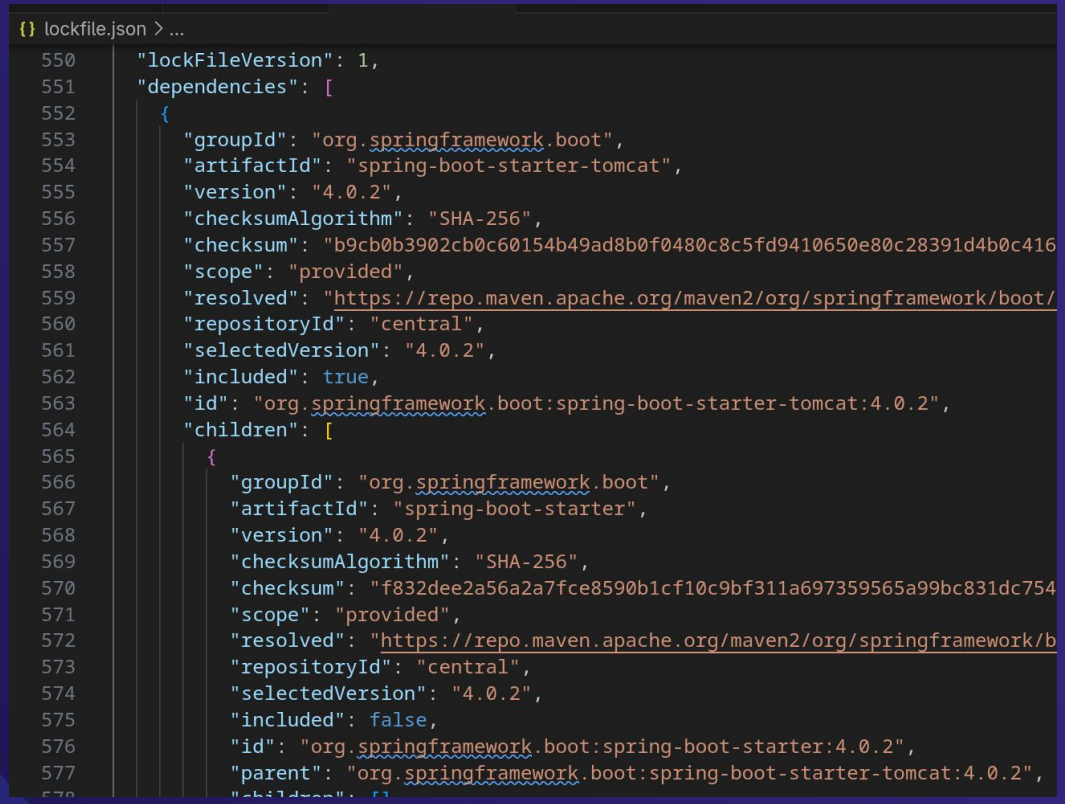
Parent POMs
BOM POMs


File Edit Selection View Go Run Terminal
integration-tests
Update
EXPLORER
OPEN EDITORS
pom.xml 1
bash
lockfile.json
INTEGRATION-TESTS
hermeto-output
src
main
test / java / io / github / herme...
SpringBootExampleApplic...
target
.gitignore
lockfile.json
pom.xml 1
README.md
OUTLINE
TIMELINE
pom.xml
2 <project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
52 <build>
53 <plugins>
58 <plugin>
62 <configuration>
69 </configuration>
70 <executions>
71 <execution>
72 <goals>
73 <goal>check</goal>
74 </goals>
75 </execution>
76 </executions>
77 </plugin>
78 <plugin>
79 <groupId>io.github.chains-project</groupId>
80 <artifactId>maven-lockfile</artifactId>
81 <version>5.16.0</version>
82 <configuration>
83 <includeMavenPlugins>true</includeMavenPlugins>
84 <checksumMode>local</checksumMode>
85 </configuration>
86 </plugin>
87 </plugins>
88 </build>
89
90 </project>
91
maven/spring-boot
0 1 111
Java: Warning
Adam Kaplan (3 months ago)
Ln 76, Col 30
Tab Size: 4
UTF-8
LF
XML

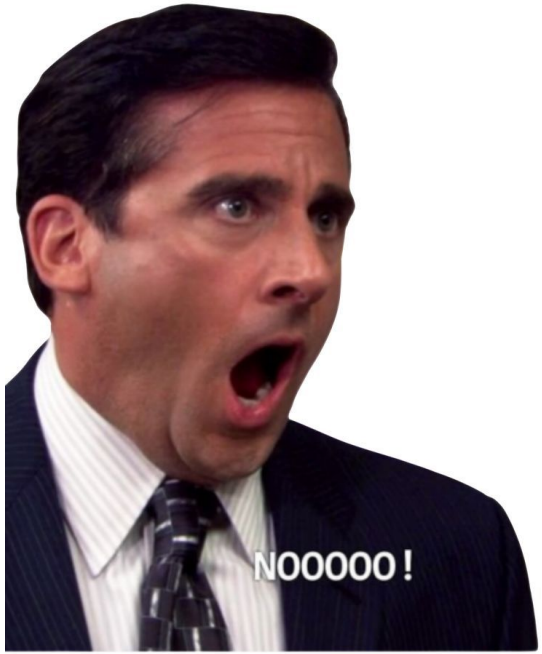
Challenges

Aesthetics

- Full tree - necessary?
- Repeated information
- Spring Boot “hello world” -> 34,000 lines of JSON!
- Integrate with Maven [trusted checksums](#)?



Plugin dependencies



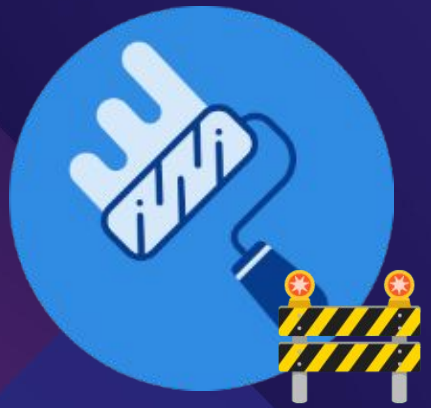
Maven Surefire Plugin

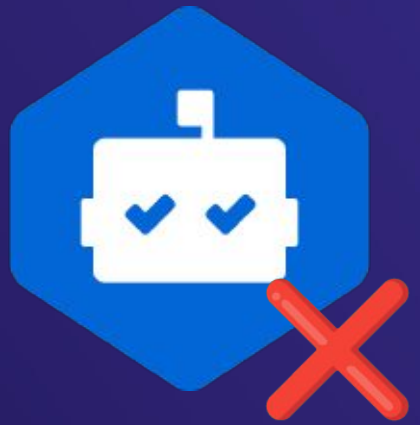
- Dynamic dependency resolution
- Avoids “classpath hell”

Protobuf Maven Plugins

- Requires external binary
- Custom XML configuration

Dependency Automation





References

- Gamage, Y., Tiwari, D., Monperrus, M. et al. The design space of lockfiles across package managers. *Empir Software Eng* **31**, 63 (2026). https://doi.org/10.1007/s10664-025-10789-w
- Maven lockfile plugin: https://github.com/chains-project/maven-lockfile
- CHAINS project: https://chains.proj.kth.se/
- Maven Trusted Checksums: maven.apache.org

Thank you!

OpenSSF Community Day
NORTH AMERICA 2026


HONK
OpenSSF Community Day
NORTH AMERICA 2026