

GOTO Copenhagen 2023

#GOTOcph

Keep your dependencies in check

GOTO Copenhagen - Oct 2, 2023



<https://maritvandijk.com/>



@MaritvanDijk77



@MaritvanDijk77

Friends: How did you write this
code so beautifully ?
Me(Proudly):



@MaritvanDijk77



@MaritvanDijk77



@MaritvanDijk77

Dec. 2021

@MaritvanDijk77

**INFOSEC GETTING
READY FOR THE HOLIDAYS**



LOG4J

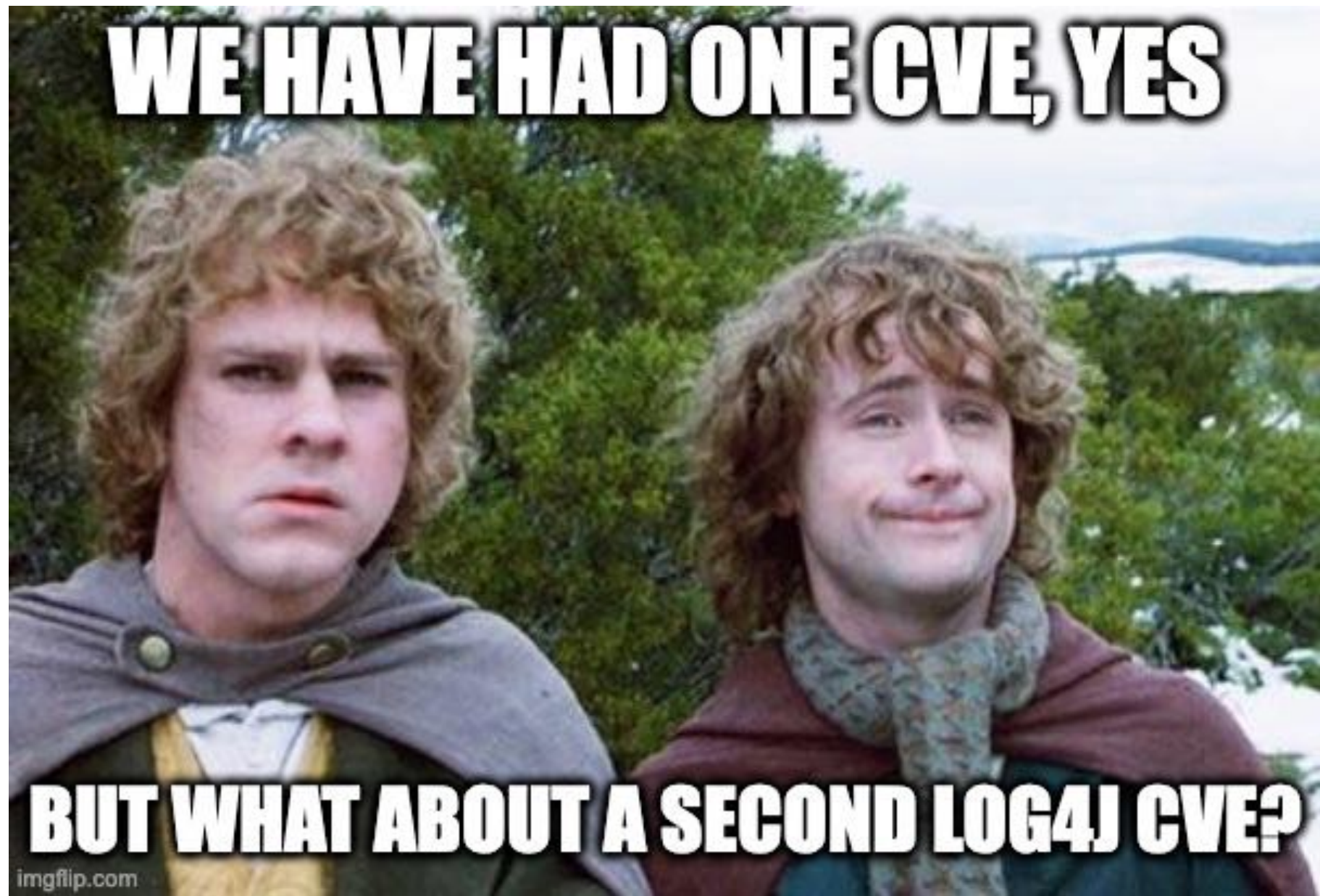


imgflip.com

@MaritvanDijk77



@MaritvanDijk77



@MaritvanDijk77

March 2022

@MaritvanDijk77

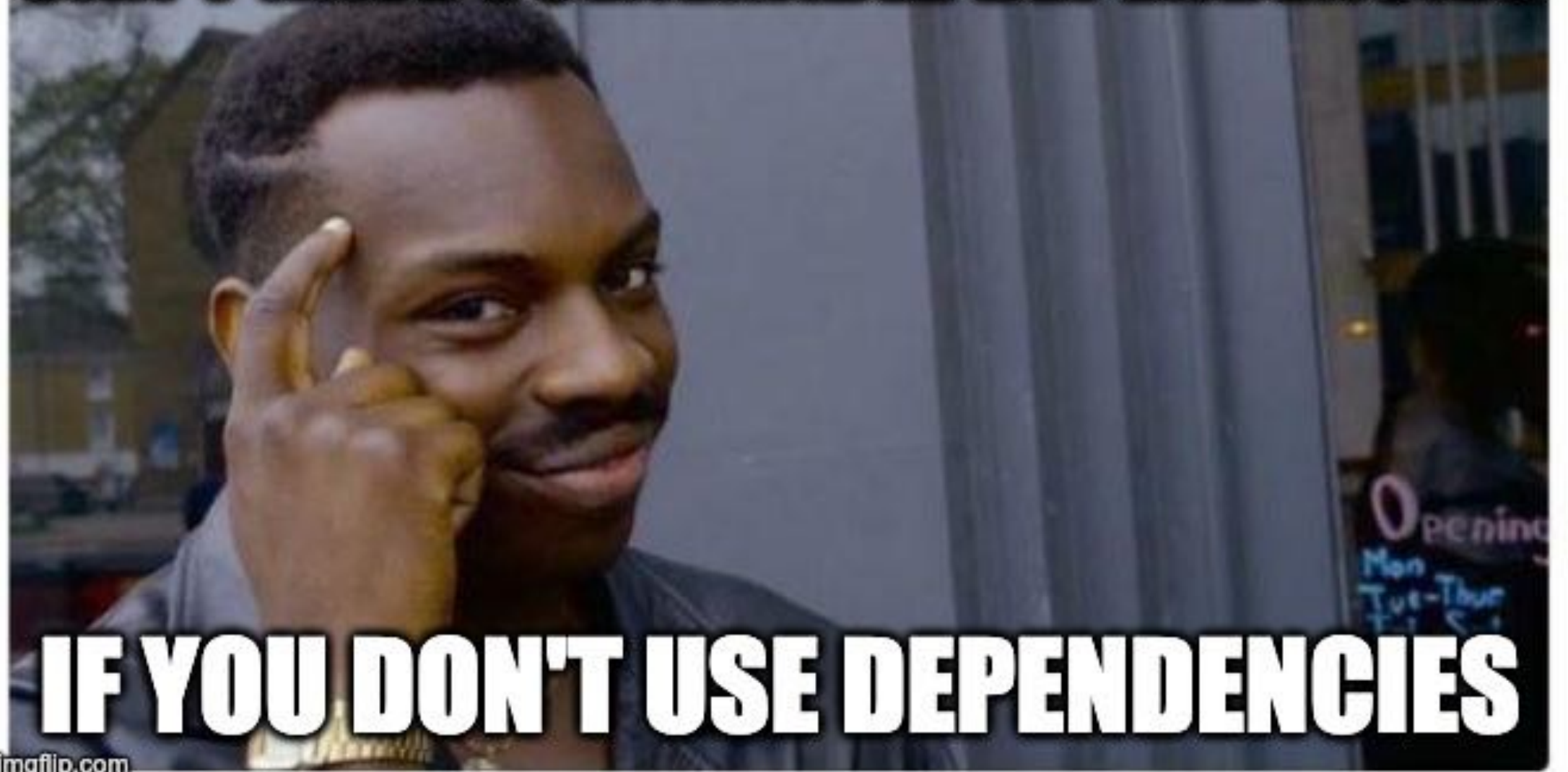


@MaritvanDijk77



@MaritvanDijk77

CAN'T HAVE VULNERABLE DEPENDENCIES



IF YOU DON'T USE DEPENDENCIES

imgflip.com

@MaritvanDijk77

USING



@MaritvanDijk77

Do we
need
this
dependency?



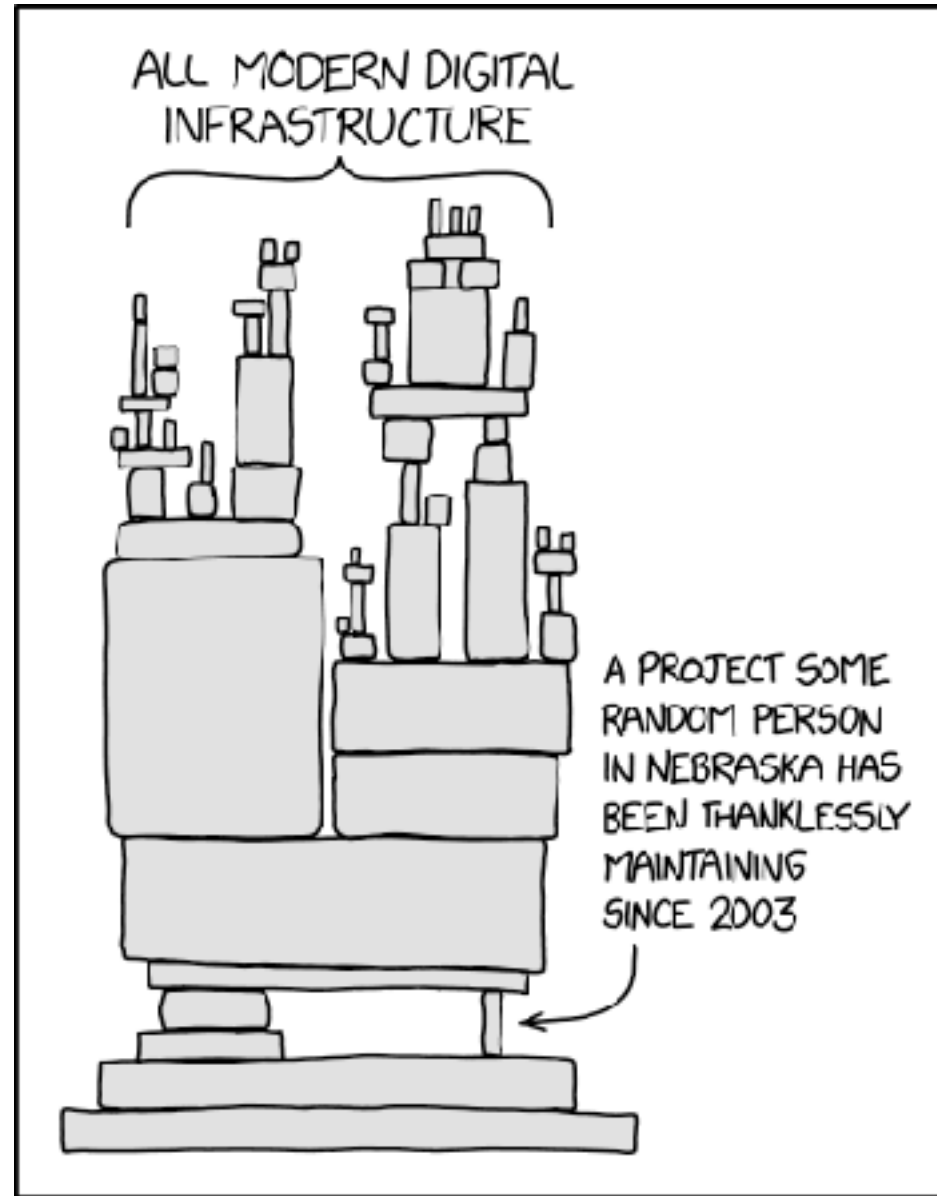
@MaritvanDijk77

Selecting dependencies

Selecting dependencies



@MaritvanDijk77



<https://xkcd.com/2347/>

@MaritvanDijk77

Selecting dependencies



@MaritvanDijk77

Selecting dependencies



@MaritvanDijk77



Selecting dependencies

@MaritvanDijk77



Selecting dependencies

@MaritvanDijk77

Log4j download dashboard

log4j Latest Statistics

249,556,989

Total Downloads Since Dec 10, 2021

29 % vulnerable

23 %

Vulnerable Downloads Last 7 Days

3,490,799 total downloads

<https://www.sonatype.com/resources/log4j-vulnerability-resource-center>

@MaritvanDijk77

Find information



@MaritvanDijk77

Dependency information

 sonatype | Maven Central Repository Search [Quick Stats](#)

 [GitHub](#)

Search



[Advanced Options](#) | [API Guide](#) 

Official search by the maintainers of Maven Central Repository



<https://search.maven.org/>

@MaritvanDijk77

Dependency information

sonatype | maven central repository

[API Doc](#)[Help](#)[Browse](#)[Sign In](#)

Welcome!

On February 23, 2023, we started redirecting users from [search.maven.org](#) to [central.sonatype.com](#). Launched in September of 2022, [central.sonatype.com](#) provides the main functionality of [search.maven.org](#) with enhanced search results, including security vulnerability and software quality information.

If you discover functionality that's missing or have suggestions for things to add, we'd love to hear from you, [so create an Improvement Issue in the MVNCENTRAL project](#).

[Click here to go back to search.maven.org](#), and we won't redirect you back here.

For more details on this change, please see [this FAQ on central.sonatype.org](#).

[Close](#)

Most Popular Packages in Last 90 Days

Most Popular Namespaces in Last 90 Days

Popular Categories

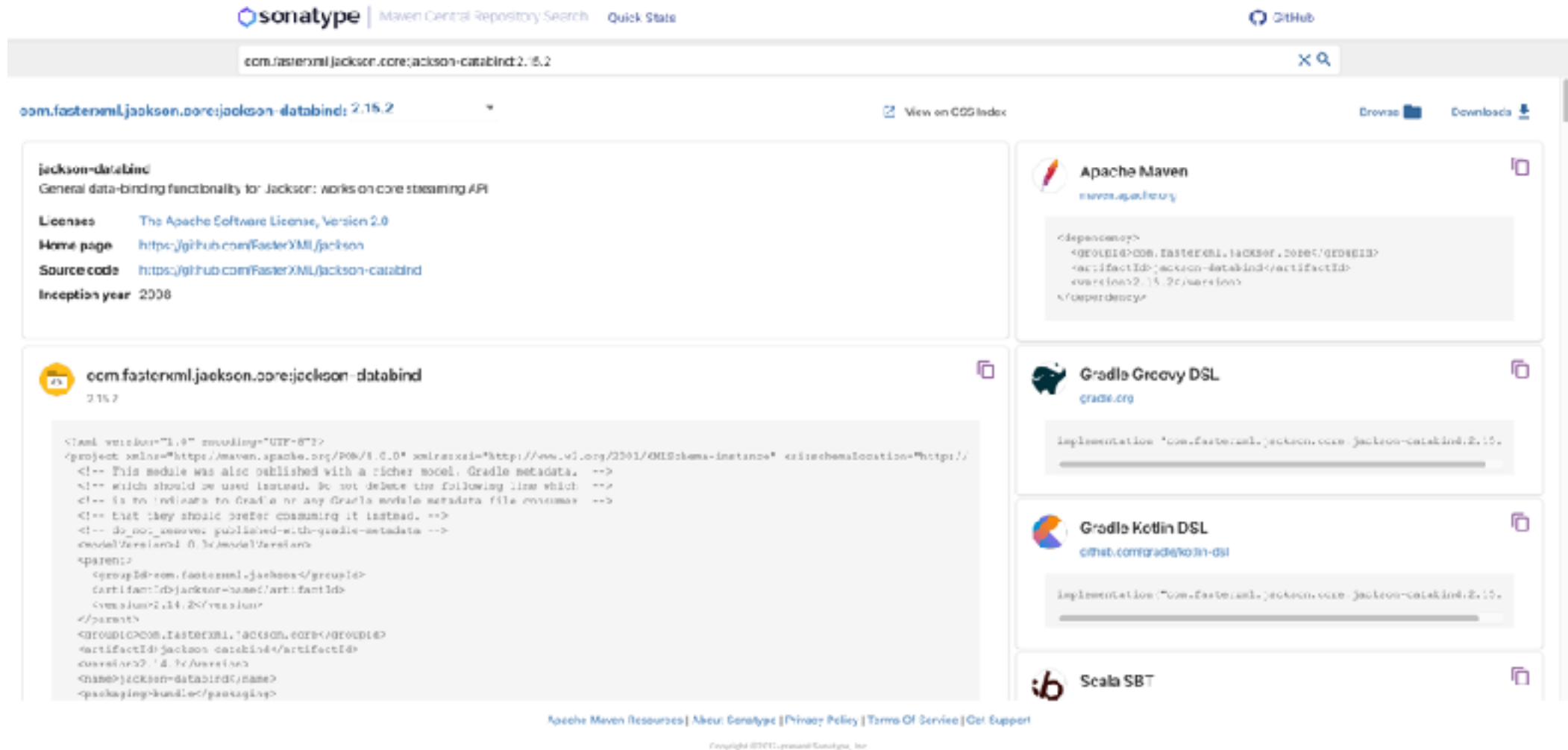
<https://central.sonatype.com/>

@MaritvanDijk77

Dependency information



Dependency information



sonatype | Maven Central Repository Search | Quick Stats

com.fasterxml.jackson.core:jackson-databind:2.15.2

View on OSS Index

Browse Downloads

jackson-databind
General data-binding functionality for Jackson: works on core streaming API

Licenses The Apache Software License, Version 2.0

Home page <https://github.com/FasterXML/jackson>

Source code <https://github.com/FasterXML/jackson-databind>

Inception year 2008

com.fasterxml.jackson.core:jackson-databind
2.15.2

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
  <!-- This module was also published with a richer model, Gradle metadata, -->
  <!-- which should be used instead. Do not delete the following line which -->
  <!-- is to indicate to Gradle or any Gradle module metadata file consumer -->
  <!-- that they should prefer consuming it instead. -->
  <!-- do not remove published-with-gradle-metadata -->
  <modelVersion>0.0.0</modelVersion>
  <parent>
    <groupId>com.fasterxml.jackson</groupId>
    <artifactId>jackson-core</artifactId>
    <version>2.14.2</version>
  </parent>
  <groupId>com.fasterxml.jackson</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.14.2</version>
  <name>jackson-databind</name>
  <packaging>bundle</packaging>
```

Apache Maven
<https://maven.apache.org/>

```
<dependency>
  <groupId>com.fasterxml.jackson</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.15.2</version>
</dependency>
```

Gradle Groovy DSL
gradle.org

```
implementation "com.fasterxml.jackson.core:jackson-databind:2.15.2"
```

Gradle Kotlin DSL
github.com/gradle/kotlin-dsl

```
implementation("com.fasterxml.jackson.core:jackson-databind:2.15.2")
```

Scala SBT

Apache Maven Resources | About Sonatype | Privacy Policy | Terms Of Service | Get Support

Copyright ©2021, present Sonatype, Inc

<https://search.maven.org/artifact/com.fasterxml.jackson.core/jackson-databind/2.15.2/jar>

@MaritvanDijk77

Dependency information

The screenshot shows the Sonatype Maven Central Repository page for the artifact **jackson-databind** version **2.15.2**. The page header includes the Sonatype logo, "maven central repository", a search bar, and links for "API Docs", "Help", "Browse", and "Sign In". Below the header, the artifact name "jackson-databind" is displayed with a version selector set to "2.15.2". A badge indicates it is "Used in 42538 components". A yellow box shows the Maven coordinates: `pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.15.2`. Navigation tabs include "Overview" (selected), "Versions", "Dependents", and "Dependencies". The "Overview" section describes it as "General data-binding functionality for Jackson: works on core streaming API". The "Snippets" section shows a code block for an Apache Maven dependency, with a "Copy to clipboard" button. The "Maven POM File" section also has a "Copy to clipboard" button. On the right, the "Sonatype Safety Rating" is 5 out of 10, with a description and a link to "How did we get this score?". Below that, the "OSS Index" shows "No vulnerabilities" with a "View" link. The "Metadata" section lists "4 months ago", "Licenses: The Apache Software License, Version 2.0", and a size of "12.3 kB".

sonatype | maven central repository [API Docs](#) [Help](#) [Browse](#) [Sign In](#)

jackson-databind

2.15.2

Used in 42538 components

`pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.15.2`

[Overview](#) [Versions](#) [Dependents](#) [Dependencies](#)

Overview

General data-binding functionality for Jackson: works on core streaming API

Snippets

Apache Maven Copy to clipboard

```
<dependency>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.15.2</version>
</dependency>
```

Maven POM File

Copy to clipboard

```
<dependency>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.15.2</version>
</dependency>
```

Sonatype Safety Rating

An aggregate rating designed to represent a project's readiness against vulnerabilities.

5 out of 10

[How did we get this score?](#)

[OSS Index](#) No vulnerabilities [View](#)

Metadata

4 months ago

Licenses
The Apache Software License, Version 2.0

12.3 kB

<https://central.sonatype.com/artifact/com.fasterxml.jackson.core/jackson-databind>

@MaritvanDijk77

Dependency information

 **sonatype** | **OSS INDEX** Search Ecosystems Integrations Documentation Who is Sonatype? Report a Vulnerability

[➔ Sign In](#)

[← Back to Component Details](#)



jackson-databind

com.fasterxml.jackson.core

Version 2.15.2

[Report advisory or correction](#)

Vulnerabilities

This version of jackson-databind has no known vulnerabilities! 🎉

@MaritvanDijk77

Dependency information

 **sonatype** | **OSS INDEX** Search Ecosystems Integrations Documentation Who is Sonatype? Report a Vulnerability

[➔ Sign In](#)

[← Back to Component Details](#)



jackson-databind

com.fasterxml.jackson.core

Version 2.12.7

[Report advisory or correction](#)

Vulnerabilities

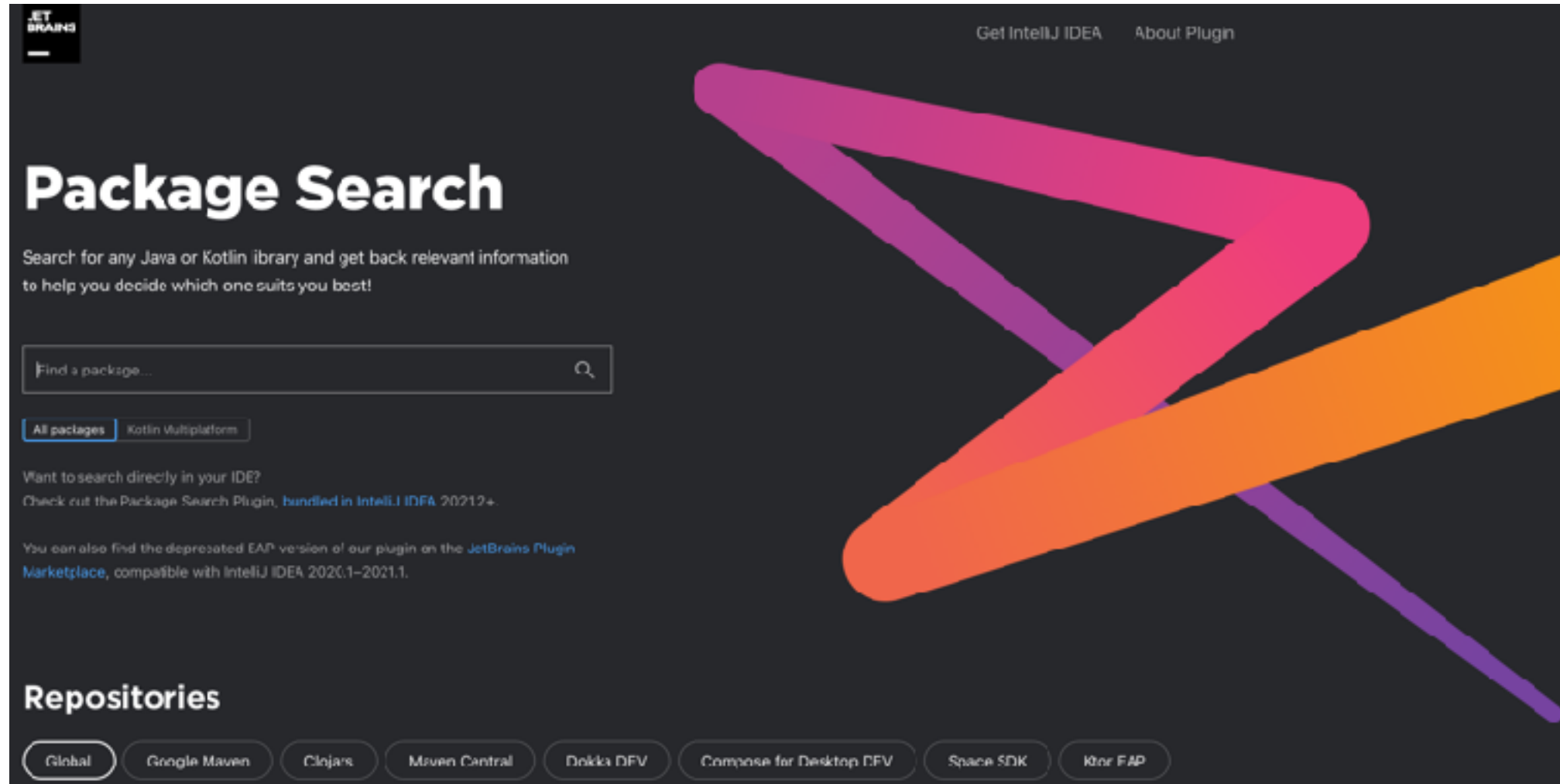
2



HIGH

@MaritvanDijk77

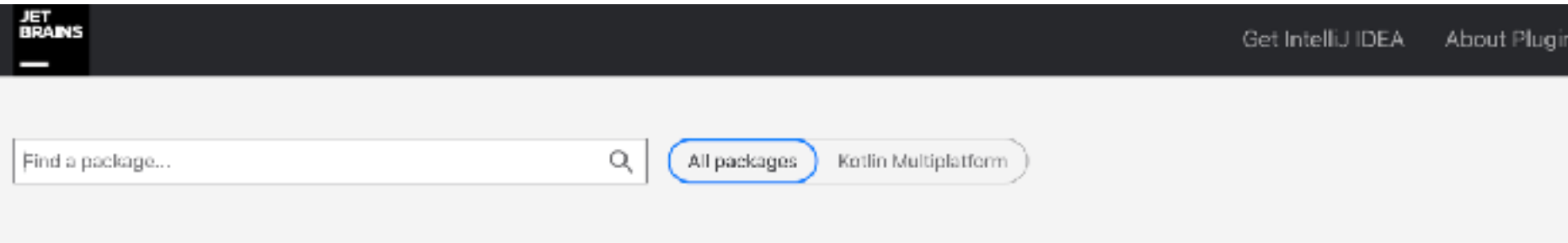
Dependency information



<https://package-search.jetbrains.com/>

@MaritvanDijk77

Dependency information



jackson-databind

com.fasterxml.jackson.core:
jackson-databind

Latest version: 2.15.1

Latest stable: 2.15.1

Updated on: May 17, 2023

StackOverflow: [core](#), [jackson-databind](#)

License: [Apache License 2.0](#)

Platforms: [jvm](#)

Authors: [Tatu Saloranta](#),
[Christopher Currie](#), [Paul Brown](#)

[Package homepage on GitHub](#)

[Source code](#)

[Information](#) [Readme](#) [Versions](#)

About package

General data-binding functionality for Jackson: works on core streaming API

The package is on GitHub, it has 3 313 stars, 168 watchers and has been forked 1 304 times.

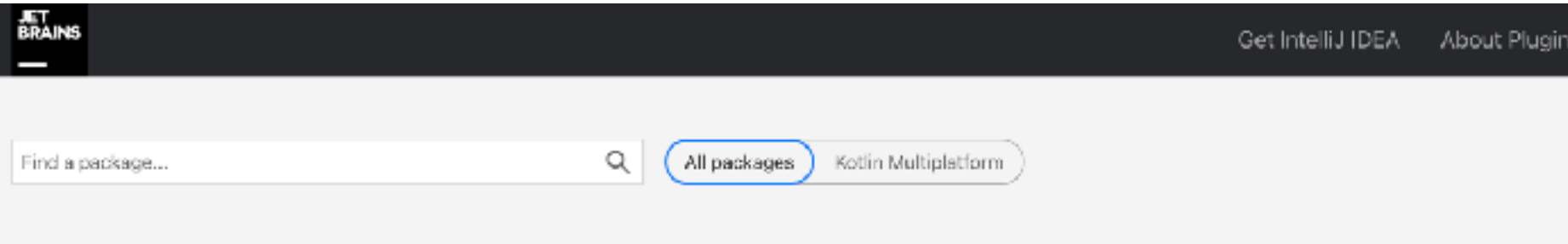
Add the package to your project

[Gradle \(Groovy\)](#) [Gradle \(Kotlin\)](#) [Maven](#) [SBT](#)

```
<dependency>
  <scope>compile</scope>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>2.15.1</version>
</dependency>
```

@MaritvanDijk77

Dependency information



jackson-databind

[com.fasterxml.jackson.core:](#)
[jackson-databind](#)

Latest version: 2.15.1

Latest stable: 2.15.1

Updated on: May 17, 2023

StackOverflow: [core](#), [jackson-databind](#)

License: [Apache License 2.0](#)

Platforms: [jvm](#)

Authors: [Tatu Saloranta](#),
[Christopher Currie](#), [Paul Brown](#)

[Package homepage on GitHub](#)

[Source code](#)

[Information](#) [Readme](#) [Versions](#)

☐ Stable

Version ▲	Repositories	Last Updated ▼	Stable
2.15.1	Maven Central	May 17, 2023	✓
2.14.2	Maven Central	Jan 28, 2023	✓
2.13.5	Maven Central	Jan 23, 2023	✓
2.14.0	Maven Central	Nov 05, 2022	✓
2.14.0-rc3	Maven Central	Oct 28, 2022	—
2.13.4.2	Maven Central	Oct 13, 2022	✓

@MaritvanDijk77

Dependency information



Navigation bar: [FasterXML / jackson-databind](#) | Search: Type / to search | [Code](#) | [Issues](#) 477 | [Pull requests](#) 25 | [Discussions](#) | [Actions](#) | [Projects](#) | [Wiki](#) | [Security](#) | [Insights](#)

Repository: **jackson-databind** (Public) | [Sponsor](#) | [Watch](#) 167 | [Fork](#) 1.3k | [Star](#) 3.4k

Stats: [2.16](#) | [27 branches](#) | [187 tags](#) | [Go to file](#) | [Add file](#) | [Code](#)

Recent commits:

cowtowncoder	A further tweak to handle a corner case of #3647	1 comment b2ab29c 5 hours ago 7,209 commits
.github	Bump actions/checkout from 4.0.0 to 4.1.0 (#4126)	5 days ago
.mvn/wrapper	Merge branch '2.15' into 2.16	3 months ago
attic	Clean up attic...	5 months ago
docs	Add javadoc redirects	9 months ago
release-notes	Update release notes wrt #3647 fix	8 hours ago
src	A further tweak to handle a corner case of #3647	5 hours ago
.gitattributes	Merge branch '2.7' into 2.8	7 years ago
.gitignore	minor ignoral cleanup	6 years ago
LICENSE	Add full LICENSE at main level (backport from master)	3 years ago

About: General data-binding package for Jackson (2.x): works on streaming API (core) implementation(s)

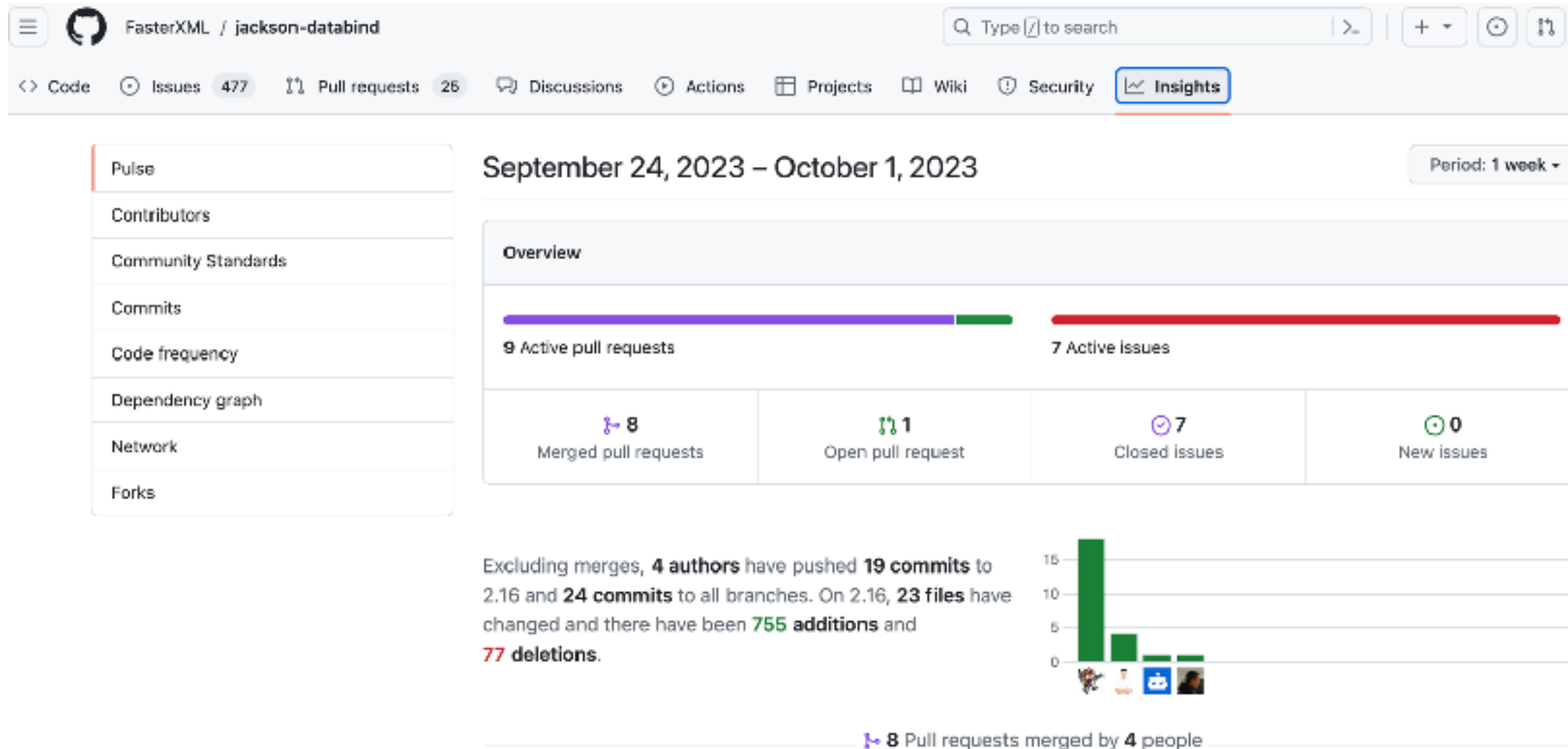
Tags: [json](#) | [jackson](#) | [hacktoberfest](#) | [jackson-databind](#)

Links: [Readme](#) | [Apache-2.0 license](#) | [Security policy](#) | [Activity](#) | [3.4k stars](#) | [167 watching](#) | [1.3k forks](#) | [Report repository](#)

<https://github.com/>

@MaritvanDijk77

Dependency information



<https://github.com/>

@MaritvanDijk77

Dependency information



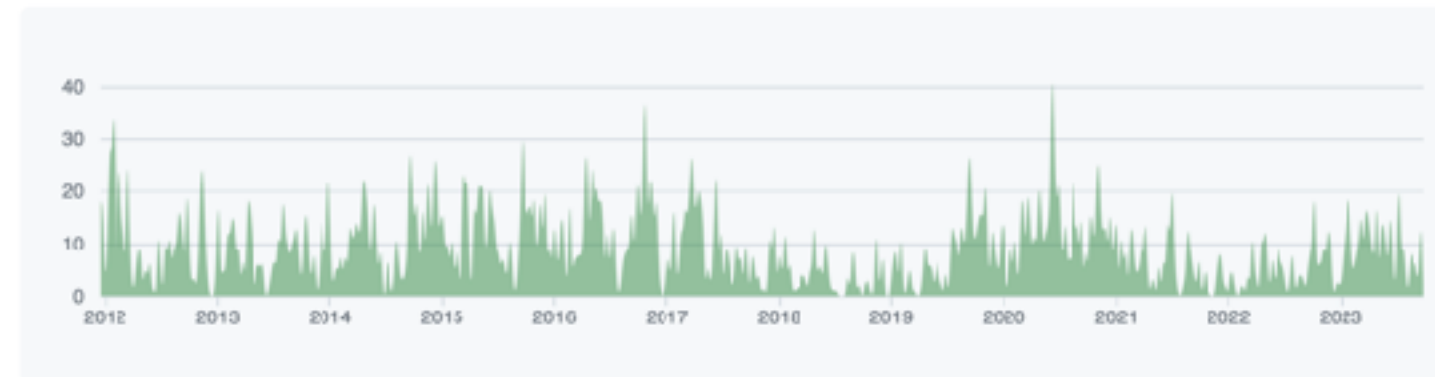
< Code Issues 477 Pull requests 25 Discussions Actions Projects Wiki Security Insights

- Pulse
- Contributors
- Community Standards
- Commits
- Code frequency
- Dependency graph
- Network
- Forcs

Dec 13, 2011 – Oct 1, 2023

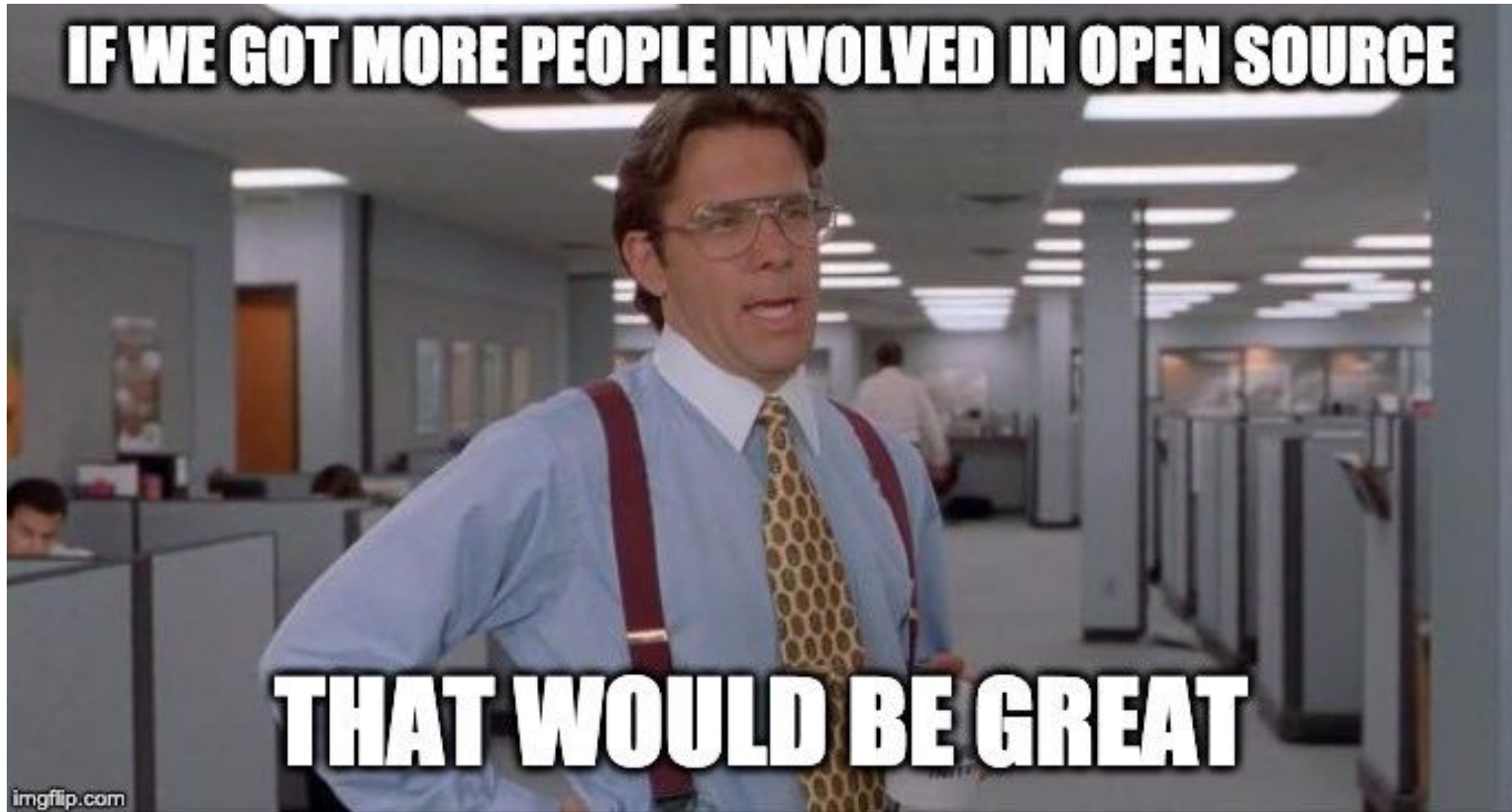
Contributions: Commits

Contributions to 2.16, excluding merge commits and bot accounts



<https://github.com/>

@MaritvanDijk77



Maintain dependencies



@MaritvanDijk77

Maven

- Overview of dependencies: `mvn dependency:tree`

```
marit.van.dijk@NVC00260 FitnessTracker % ./mvnw dependency:tree
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- maven-dependency-plugin:2.8:tree (default-cli) @ FitnessTracker ---
[INFO] com.maritvandijk:FitnessTracker:war:1.0-SNAPSHOT
[INFO] +- junit:junit:jar:3.8.1:compile
[INFO] +- org.springframework:spring-webmvc:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-aop:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-beans:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-context:jar:4.3.5.RELEASE:compile
[INFO] |   +- org.springframework:spring-core:jar:4.3.5.RELEASE:compile
[INFO] |   |   \- commons-logging:commons-logging:jar:1.2:compile
[INFO] |   +- org.springframework:spring-expression:jar:4.3.5.RELEASE:compile
[INFO] |   \- org.springframework:spring-web:jar:4.3.5.RELEASE:compile
```

Maven

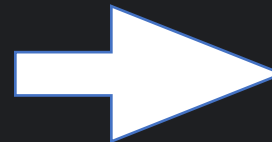
- Check for updates: ``mvn versions:display-dependency-updates``

```
marit.van.dijk@NVC00260 FitnessTracker % mvn versions:display-dependency-updates
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- versions-maven-plugin:2.13.0:display-dependency-updates (default-cli) @ FitnessTracker ---
[INFO] The following dependencies in Dependencies have newer versions:
[INFO]   com.fasterxml.jackson.core:jackson-annotations ..... 2.9.7 -> 2.15.2
[INFO]   com.fasterxml.jackson.core:jackson-core ..... 2.9.7 -> 2.15.2
[INFO]   com.fasterxml.jackson.core:jackson-databind ..... 2.9.7 -> 2.15.2
[INFO]   com.thoughtworks.xstream:xstream ..... 1.4.18 -> 1.4.20
[INFO]   javax.servlet:servlet-api ..... 2.5 -> 3.0-alpha-1
[INFO]   junit:junit ..... 3.8.1 -> 4.13.2
[INFO]   org.hibernate:hibernate-validator ..... 4.2.0.Final -> 8.0.0.Final
[INFO]   org.springframework:spring-oxm ..... 4.3.5.RELEASE -> 6.0.9
[INFO]   org.springframework:spring-webmvc ..... 4.3.5.RELEASE -> 6.0.9
[INFO]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```

Maven

- Check for updates: ``mvn versions:display-dependency-updates``

```
marit.van.dijk@NVC00260 FitnessTracker % ./mvnw versions:display-dependency-updates
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.maritvandijk:FitnessTracker >-----
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] -----[ war ]-----
[INFO]
[INFO] --- versions-maven-plugin:2.13.0:display-dependency-updates (default-cli) @ FitnessTracker ---
[INFO] The following dependencies in Dependencies have newer versions:
[INFO] com.fasterxml.jackson.core:jackson-annotations ..... 2.9.7 -> 2.15.0
[INFO] com.fasterxml.jackson.core:jackson-core ..... 2.9.7 -> 2.15.0
[INFO] com.fasterxml.jackson.core:jackson-databind ..... 2.9.7 -> 2.15.0
[INFO] com.thoughtworks.xstream:xstream ..... 1.4.10 -> 1.4.20
[INFO] javax.servlet:servlet-api ..... 2.5 -> 3.0-alpha-1
[INFO] junit:junit ..... 3.8.1 -> 4.13.2
[INFO] org.hibernate:hibernate-validator ..... 4.2.0.Final -> 5.0.0.Final
[INFO] org.springframework:spring-oxm ..... 4.3.5.RELEASE -> 4.3.10.RELEASE
[INFO] org.springframework:spring-webmvc ..... 4.3.5.RELEASE -> 4.3.10.RELEASE
[INFO]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```



2.15.0-rc2

2.15.0-rc1

2.14.2

2.13.5

2.14.1

@MaritvanDijk77

Maven

- Analyze dependencies: ``mvn dependency:analyze``

```
[INFO] --- maven-dependency-plugin:2.8:analyze (default-cli) @ FitnessTracker ---
[WARNING] Used undeclared dependencies found:
[WARNING]   org.springframework:spring-beans:jar:4.3.5.RELEASE:compile
[WARNING]   org.springframework:spring-web:jar:4.3.5.RELEASE:compile
[WARNING]   javax.validation:validation-api:jar:1.0.0.GA:compile
[WARNING]   org.springframework:spring-context:jar:4.3.5.RELEASE:compile
[WARNING] Unused declared dependencies found:
[WARNING]   junit:junit:jar:3.8.1:compile
[WARNING]   org.springframework:spring-webmvc:jar:4.3.5.RELEASE:compile
[WARNING]   javax.servlet:servlet-api:jar:2.5:provided
[WARNING]   javax.servlet:jstl:jar:1.2:provided
[WARNING]   com.fasterxml.jackson.core:jackson-core:jar:2.9.7:compile
[WARNING]   com.fasterxml.jackson.core:jackson-annotations:jar:2.9.7:compile
[WARNING]   com.fasterxml.jackson.core:jackson-databind:jar:2.9.7:compile
[WARNING]   com.thoughtworks.xstream:xstream:jar:1.4.10:compile
[WARNING]   org.springframework:spring-oxm:jar:4.3.5.RELEASE:compile
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
```

Gradle

- Overview of dependencies: `./gradlew dependencies`

```
aotCompileClasspath - Compile classpath for source set 'aot'.
+--- org.springframework.boot:spring-boot-starter-cache -> 3.1.0
|    +--- org.springframework.boot:spring-boot-starter:3.1.0
|    |    +--- org.springframework.boot:spring-boot:3.1.0
|    |    |    +--- org.springframework:spring-core:6.0.9
|    |    |    |    \--- org.springframework:spring-jcl:6.0.9
|    |    |    \--- org.springframework:spring-context:6.0.9
|    |    |         +--- org.springframework:spring-aop:6.0.9
|    |    |         |    +--- org.springframework:spring-beans:6.0.9
|    |    |         |    |    \--- org.springframework:spring-core:6.0.9 (*)
|    |    |         |    \--- org.springframework:spring-core:6.0.9 (*)
|    |    |         +--- org.springframework:spring-beans:6.0.9 (*)
|    |    |         +--- org.springframework:spring-core:6.0.9 (*)
|    |    |         \--- org.springframework:spring-expression:6.0.9
|    |    |              \--- org.springframework:spring-core:6.0.9 (*)
|    +--- org.springframework.boot:spring-boot-autoconfigure:3.1.0
|    |    \--- org.springframework.boot:spring-boot:3.1.0 (*)
|    +--- org.springframework.boot:spring-boot-starter-logging:3.1.0
|    |    +--- ch.qos.logback:logback-classic:1.4.7
```

Gradle

- Check for updates:
- Add plugin, e.g. gradle-versions-plugin

```
plugins {  
    id 'java'  
    id 'com.github.ben-manes.versions' version '0.48.0'  
}
```

- Run `./gradlew dependencyUpdates`

```
The following dependencies have later milestone versions:  
- com.github.ben-manes.caffeine:caffeine [3.1.6 -> 3.1.8]  
  https://github.com/ben-manes/caffeine  
- com.h2database:h2 [2.1.214 -> 2.2.224]  
  https://h2database.com
```

Gradle



- Analyze dependencies
- Add plugin (e.g. nebula)

nebula-plugins / gradle-lint-plugin Public

<> Code Issues 97 Pull requests 6 Actions Projects Wiki Security Insights

Unused Dependency Rule

Jon Schneider edited this page on Sep 22, 2016 · 4 revisions

The unused dependency rule is an example of a complex dependency hygiene rule.

To apply the rule, add:

```
gradleLint.rules += 'unused-dependency'
```

The rule inspects compiled binaries emanating from your project's [source sets](#) looking for class references, and matches those references to the dependencies that you have declared in your [dependencies](#) block.

Specifically, the rule makes the following adjustments to dependencies:

1. Removes unused dependencies
 - Family-style jars like `com.amazonaws:aws-java-sdk` are removed, as they contain no code
2. Promotes transitive dependencies that are used directly by your code to explicit first order dependencies
 - This has the side effect of breaking up family style jars like `com.amazonaws:aws-java-sdk` into the parts that you are actually using, and adding those as first order dependencies
3. Relocates dependencies to the 'correct' configuration

<https://github.com/nebula-plugins/gradle-lint-plugin/wiki/Unused-Dependency-Rule>

@MaritvanDijk77

Gradle

- Analyze dependencies
- Add plugin (e.g. nebula)
- Run `./gradlew fixGradleLint`

```
buildscript { repositories { mavenCentral() } }  
plugins {  
    id 'nebula.lint' version '18.1.0'  
}  
gradleLint.rules = ['all-dependency']
```

> Task :fixGradleLint

This project contains lint violations. A complete listing of my attempt to fix them follows. Please review and commit the changes.

needs fixing unused-dependency one or more classes in org.springframework.data:spring-data-commons:3.1.1 are required by your code directly

needs fixing unused-dependency this dependency should be removed since its artifact is empty

build.gradle:42

testImplementation 'org.springframework.boot:spring-boot-starter-test'

fixed unused-dependency this dependency is unused and can be removed



IntelliJ IDEA: View Dependencies

A screenshot of the IntelliJ IDEA IDE interface. The main editor window displays a Maven `pom.xml` file for a project named "spring-petclinic". The file is open at the "dependencies" section, which contains several Spring Boot starter dependencies. The IDE's interface includes a top toolbar with icons for running, debugging, and other actions. The bottom status bar shows the current file path: "project > dependencies > dependency".

```
spring-petclinic < versions <
pom.xml [spring-petclinic] <
28 <dependencies>
29 <!-- Spring and Spring Boot dependencies -->
40 <dependency>
41 <groupId>org.springframework.boot</groupId>
42 <artifactId>spring-boot-starter-actuator</artifactId>
43 </dependency>
44 <dependency>
45 <groupId>org.springframework.boot</groupId>
46 <artifactId>spring-boot-starter-cache</artifactId>
47 </dependency>
48 <dependency>
49 <groupId>org.springframework.boot</groupId>
50 <artifactId>spring-boot-starter-data-jpa</artifactId>
51 </dependency>
52 <dependency>
53 <groupId>org.springframework.boot</groupId>
54 <artifactId>spring-boot-starter-web</artifactId>
55 </dependency>
56 <dependency>
57 <groupId>org.springframework.boot</groupId>
58 <artifactId>spring-boot-starter-validation</artifactId>
59 </dependency>
60 <dependency>
61 <groupId>org.springframework.boot</groupId>
62 <artifactId>spring-boot-starter-thymeleaf</artifactId>
63 </dependency>
64 <dependency>
65
```

@MaritvanDijk77



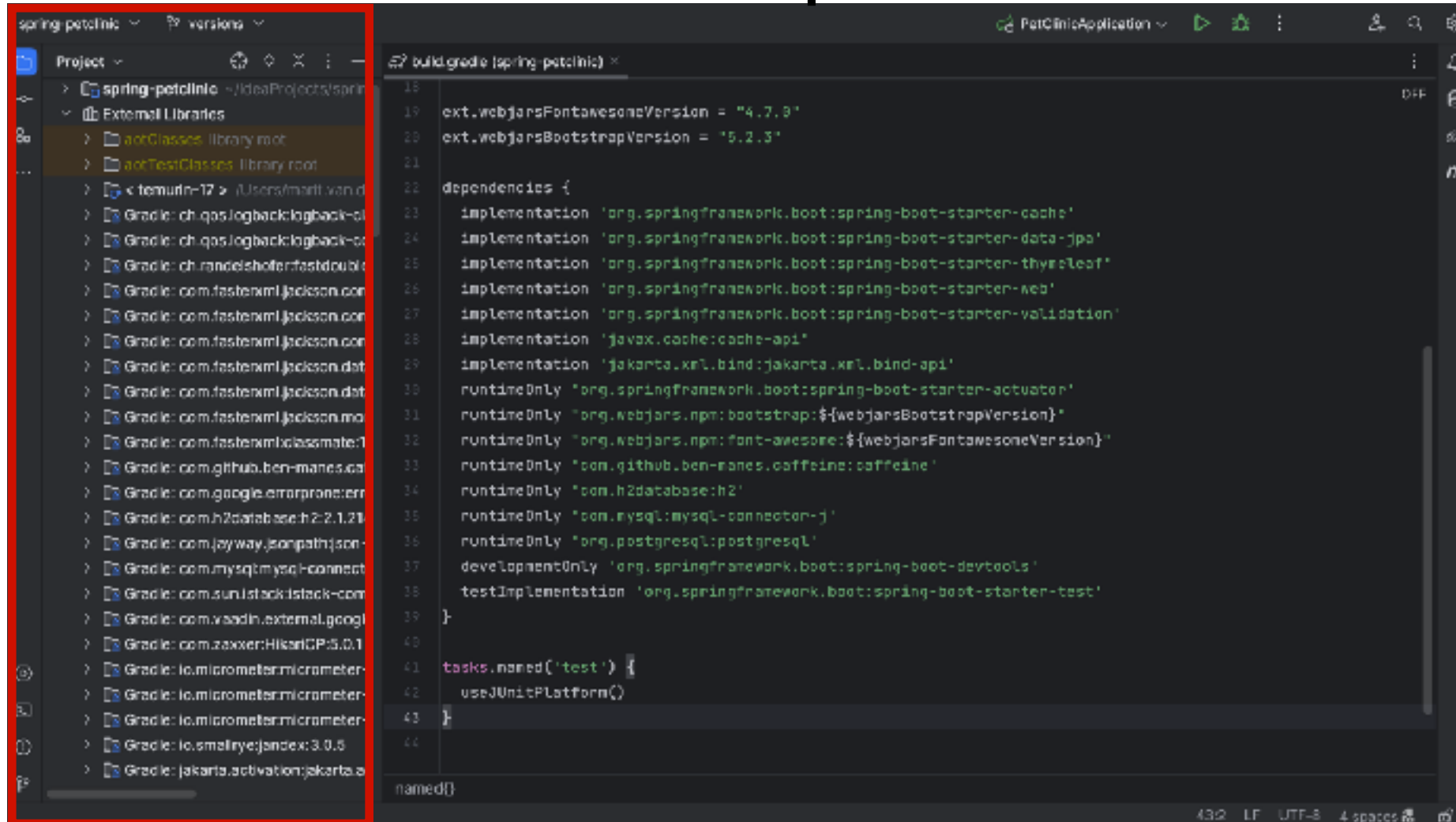
IntelliJ IDEA: View Dependencies



```
spring-petclinic  versions
build.gradle (spring-petclinic)
18
19 ext.webjarsFontawesomeVersion = "4.7.0"
20 ext.webjarsBootstrapVersion = "5.2.3"
21
22 dependencies {
23     implementation 'org.springframework.boot:spring-boot-starter-cache'
24     implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
25     implementation 'org.springframework.boot:spring-boot-starter-thymeleaf'
26     implementation 'org.springframework.boot:spring-boot-starter-web'
27     implementation 'org.springframework.boot:spring-boot-starter-validation'
28     implementation 'javax.cache:cache-api'
29     implementation 'jakarta.xml.bind:jakarta.xml.bind-api'
30     runtimeOnly 'org.springframework.boot:spring-boot-starter-actuator'
31     runtimeOnly 'org.webjars.npm:bootstrap:${webjarsBootstrapVersion}'
32     runtimeOnly 'org.webjars.npm:font-awesome:${webjarsFontawesomeVersion}'
33     runtimeOnly 'com.github.ben-manes.caffeine:caffeine'
34     runtimeOnly 'com.h2database:h2'
35     runtimeOnly 'com.mysql:mysql-connector-j'
36     runtimeOnly 'org.postgresql:postgresql'
37     developmentOnly 'org.springframework.boot:spring-boot-devtools'
38     testImplementation 'org.springframework.boot:spring-boot-starter-test'
39 }
40
41 tasks.named("test") {
42     useJUnitPlatform()
43 }
44
45 plugins()
```

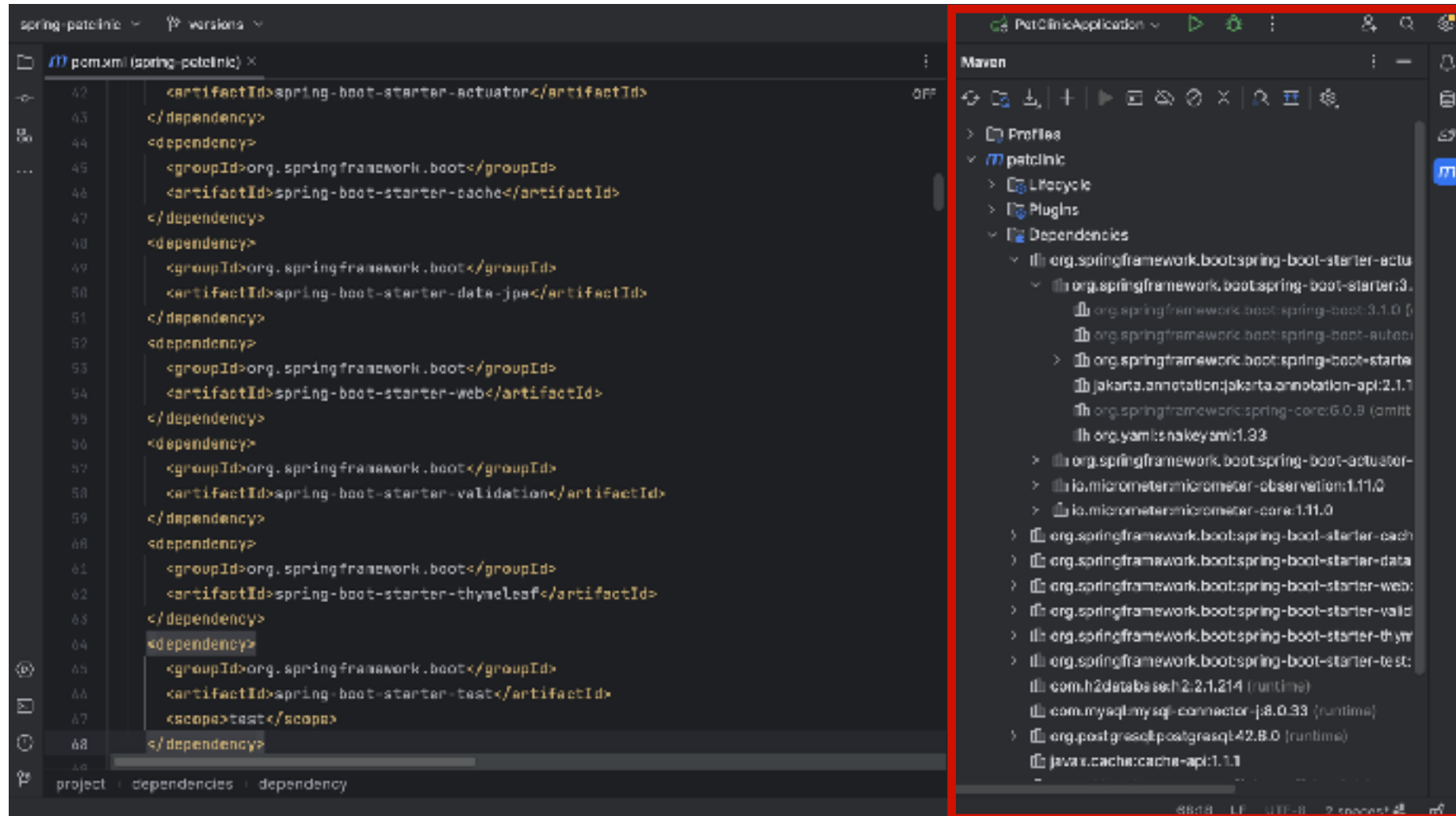
@MaritvanDijk77

IntelliJ IDEA: View Dependencies



@MaritvanDijk77

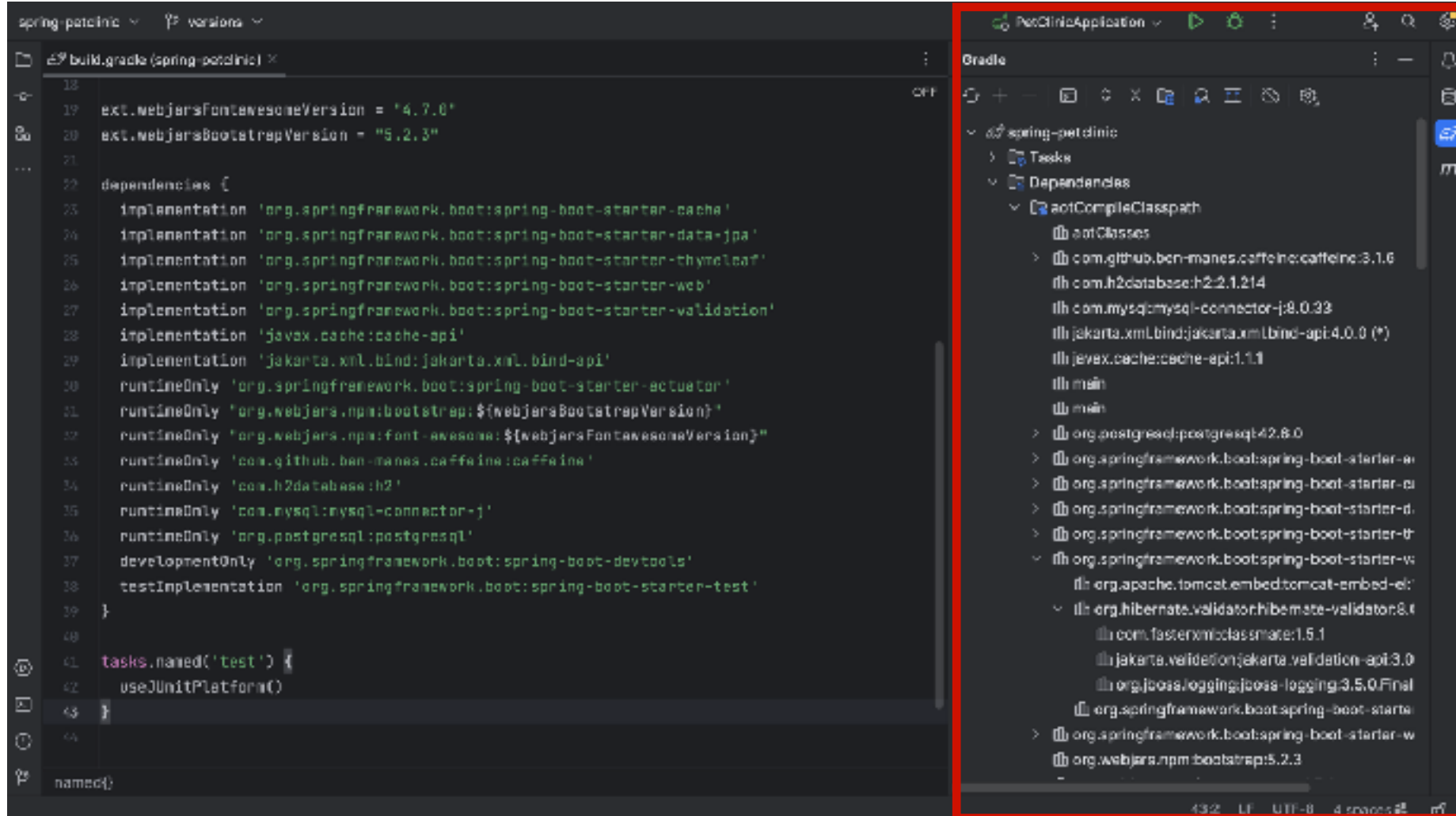
IntelliJ IDEA: View Dependencies



<https://www.jetbrains.com/help/idea/maven-projects-tool-window.html>

@MaritvanDijk77

IntelliJ IDEA: View Dependencies



The screenshot displays the IntelliJ IDEA interface with the Gradle tool window open on the right. The left pane shows the `build.gradle` file for the `spring-petclinic` project. The right pane shows the Gradle tool window with the `Dependencies` tab selected, displaying the `aotCompileClasspath` for the `PerClinicApplication` task.

build.gradle (spring-petclinic)

```
18
19 ext.webjarsFontawesomeVersion = "4.7.0"
20 ext.webjarsBootstrapVersion = "5.2.3"
21
22 dependencies {
23     implementation 'org.springframework.boot:spring-boot-starter-cache'
24     implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
25     implementation 'org.springframework.boot:spring-boot-starter-thymeleaf'
26     implementation 'org.springframework.boot:spring-boot-starter-web'
27     implementation 'org.springframework.boot:spring-boot-starter-validation'
28     implementation 'javax.cache:cache-api'
29     implementation 'jakarta.xml.bind:jakarta.xml.bind-api'
30     runtimeOnly 'org.springframework.boot:spring-boot-starter-actuator'
31     runtimeOnly 'org.webjars.npm:bootstrap:${webjarsBootstrapVersion}'
32     runtimeOnly 'org.webjars.npm:font-awesome:${webjarsFontawesomeVersion}'
33     runtimeOnly 'com.github.ben-manes.caffeine:caffeine'
34     runtimeOnly 'com.h2database:h2'
35     runtimeOnly 'com.mysql:mysql-connector-j'
36     runtimeOnly 'org.postgresql:postgresql'
37     developmentOnly 'org.springframework.boot:spring-boot-devtools'
38     testImplementation 'org.springframework.boot:spring-boot-starter-test'
39 }
40
41 tasks.named('test') {
42     useJUnitPlatform()
43 }
44
45 named()
```

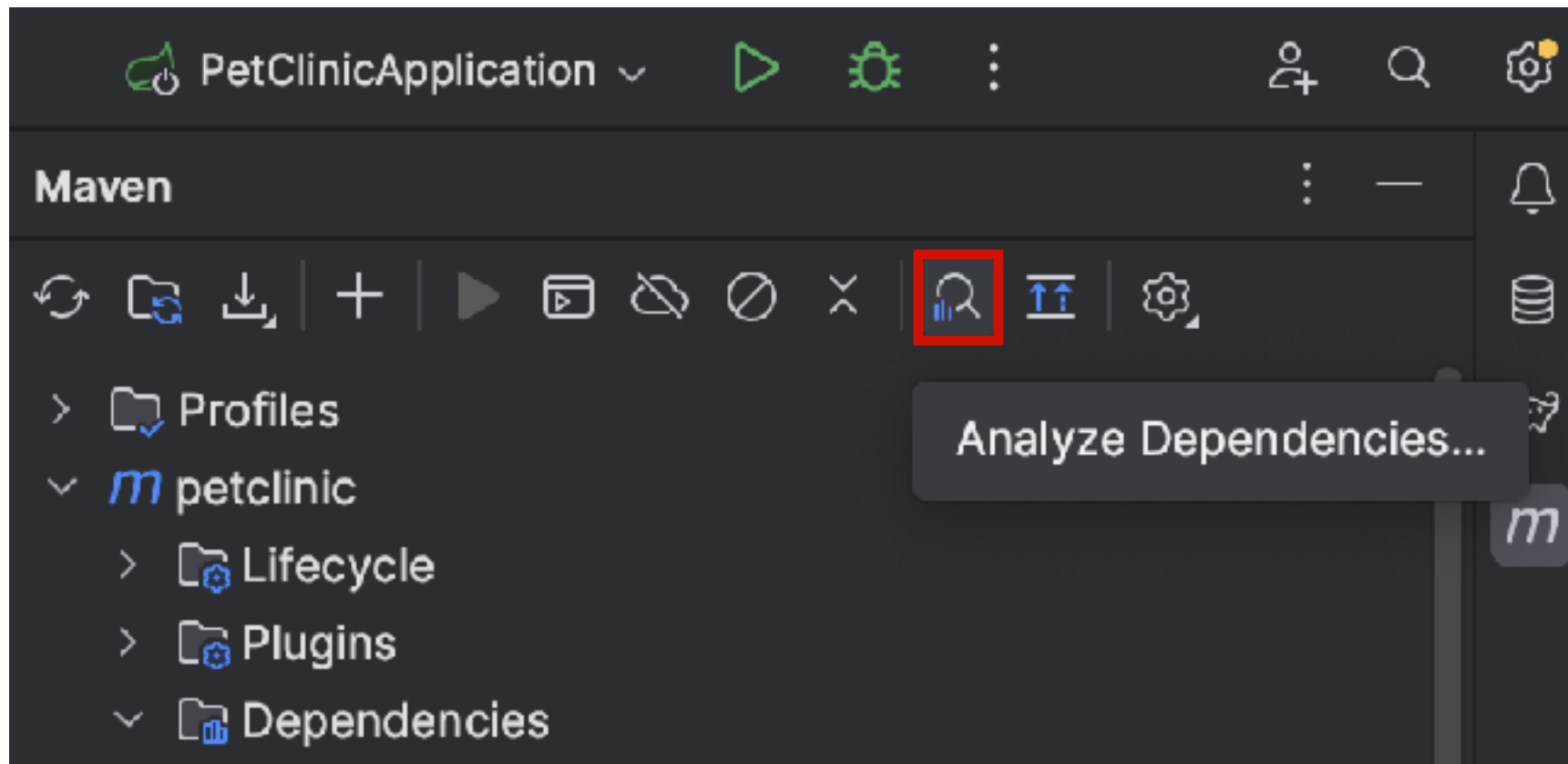
Gradle

PerClinicApplication

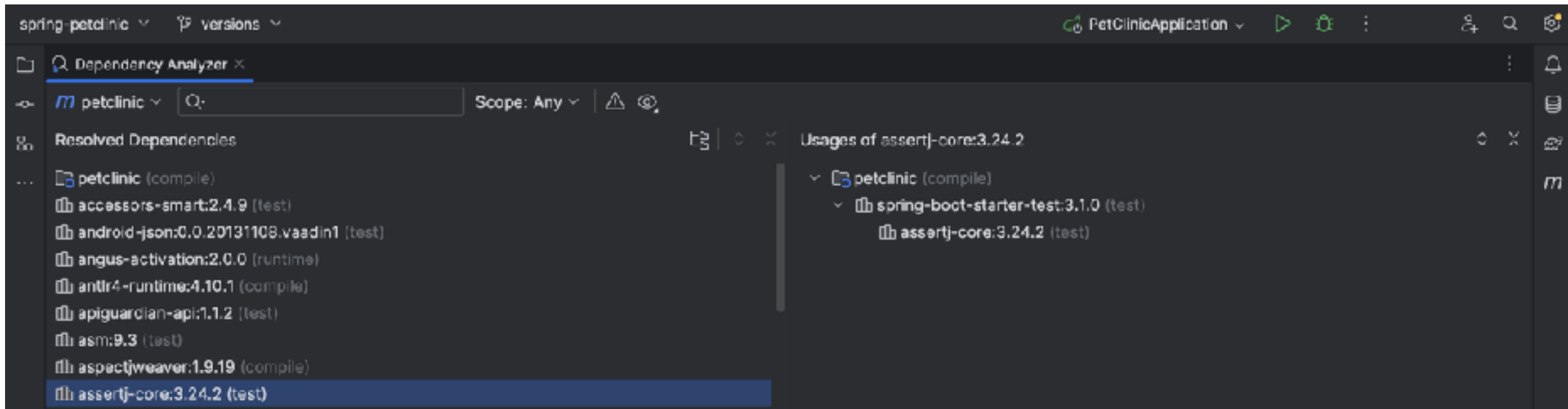
- Tasks
- Dependencies
 - aotCompileClasspath
 - aotClasses
 - com.github.ben-manes.caffeine:caffeine:3.1.6
 - com.h2database:h2:2.1.214
 - com.mysql:mysql-connector-j:8.0.33
 - jakarta.xml.bind:jakarta.xml.bind-api:4.0.0 (*)
 - javax.cache:cache-api:1.1.1
 - main
 - main
 - org.postgresql:postgresql:42.6.0
 - org.springframework.boot:spring-boot-starter-actuator
 - org.springframework.boot:spring-boot-starter-cache
 - org.springframework.boot:spring-boot-starter-data-jpa
 - org.springframework.boot:spring-boot-starter-devtools
 - org.springframework.boot:spring-boot-starter-thymeleaf
 - org.springframework.boot:spring-boot-starter-validation
 - org.apache.tomcat.embed:tomcat-embed-el
 - org.hibernate.validator:hibernate-validator:8.4
 - com.fasterxml:classmate:1.5.1
 - jakarta.validation:jakarta.validation-api:3.0
 - org.jboss.logging:jboss-logging:3.5.0.Final
 - org.springframework.boot:spring-boot-starter-web
 - org.webjars.npm:bootstrap:5.2.3

IntelliJ IDEA: Dependency Analyzer

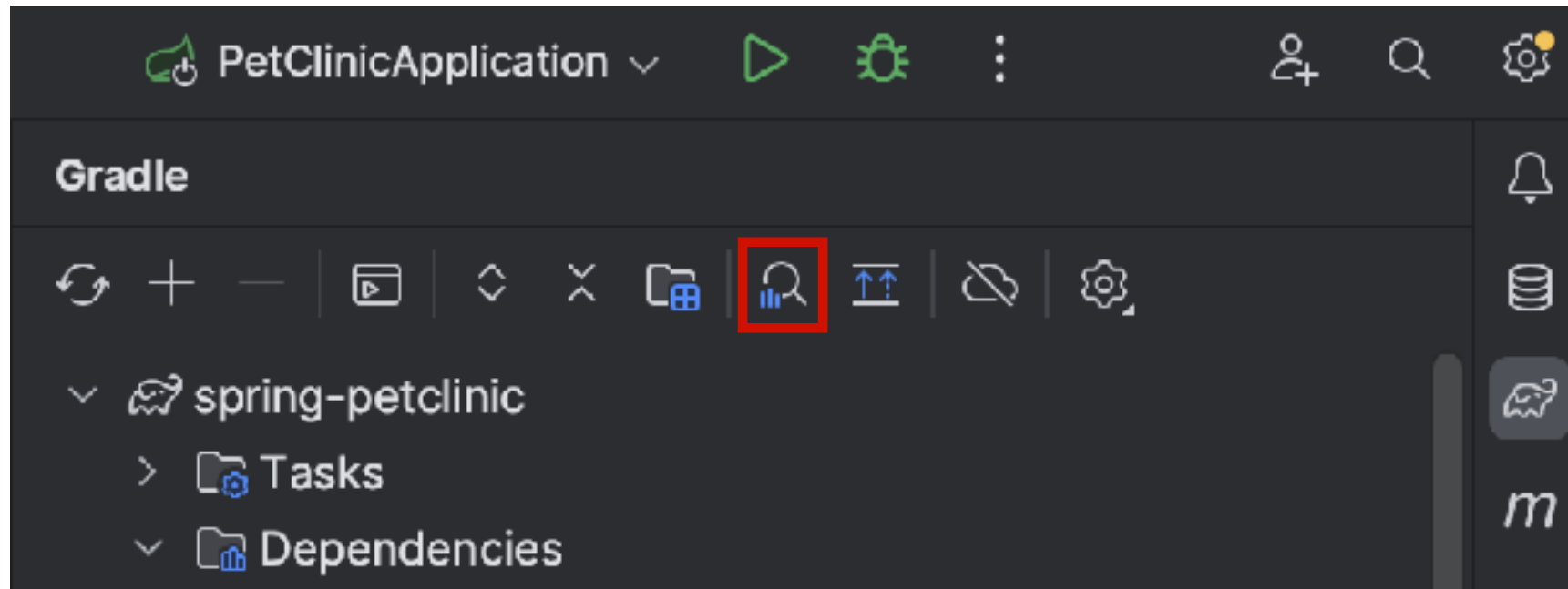
Maven™



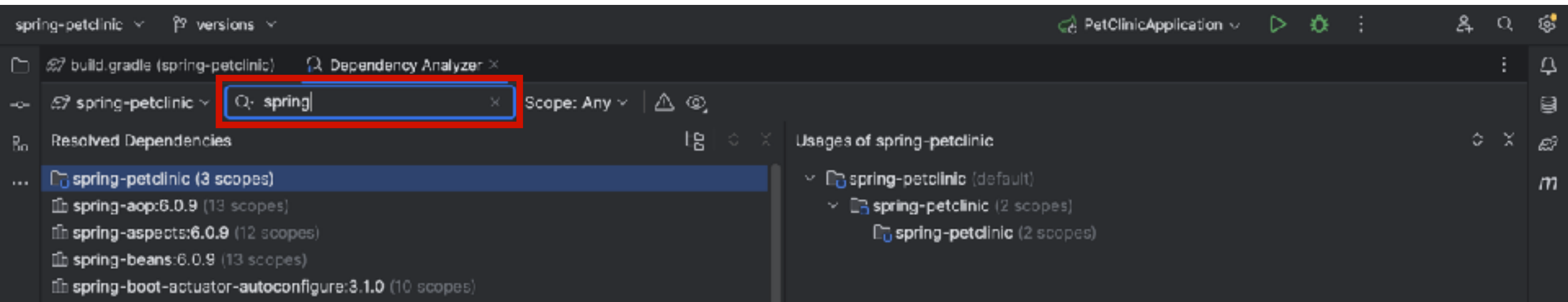
IntelliJ IDEA: Dependency Analyzer



IntelliJ IDEA: Dependency Analyzer

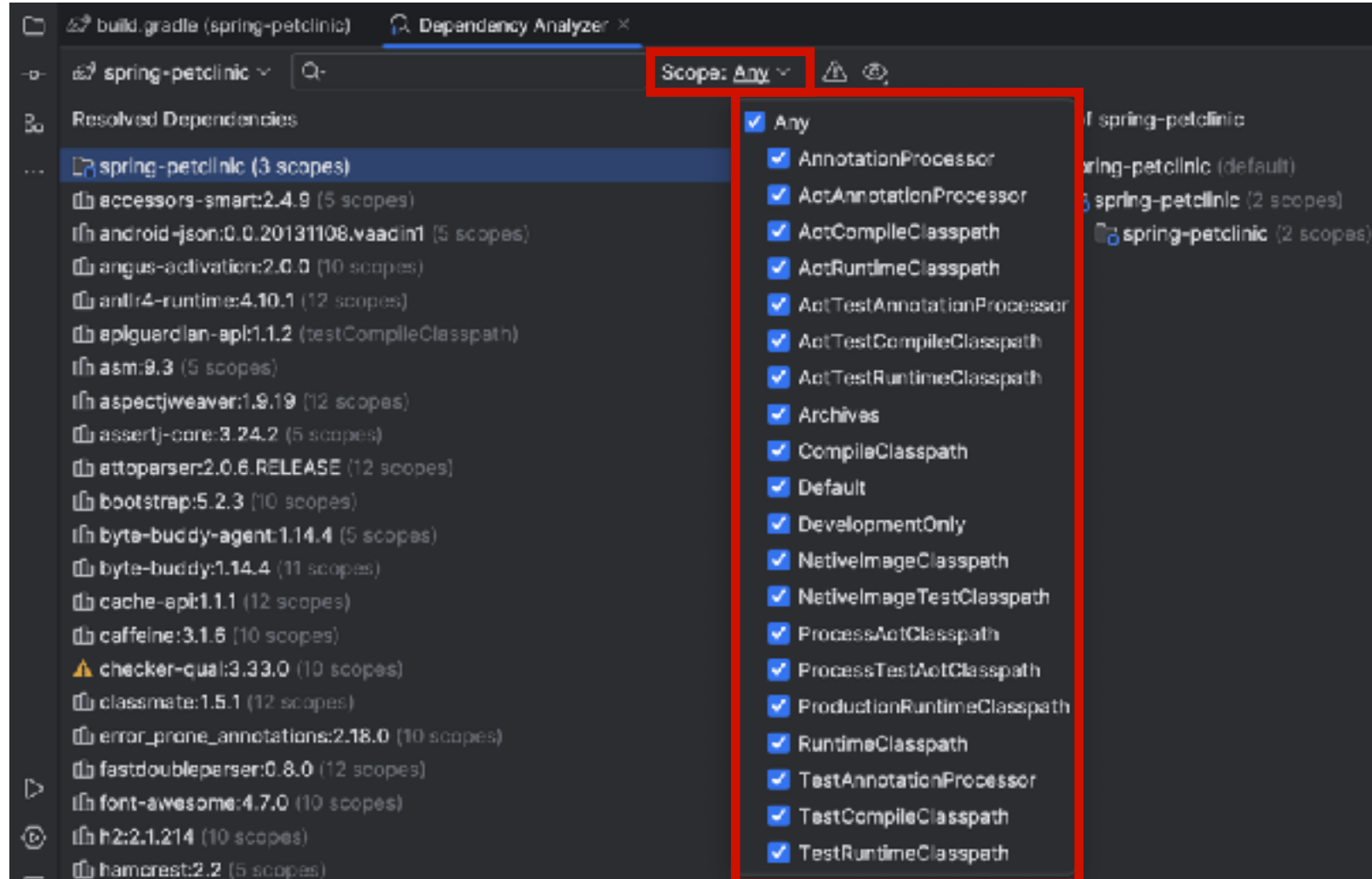


IntelliJ IDEA: Dependency Analyzer





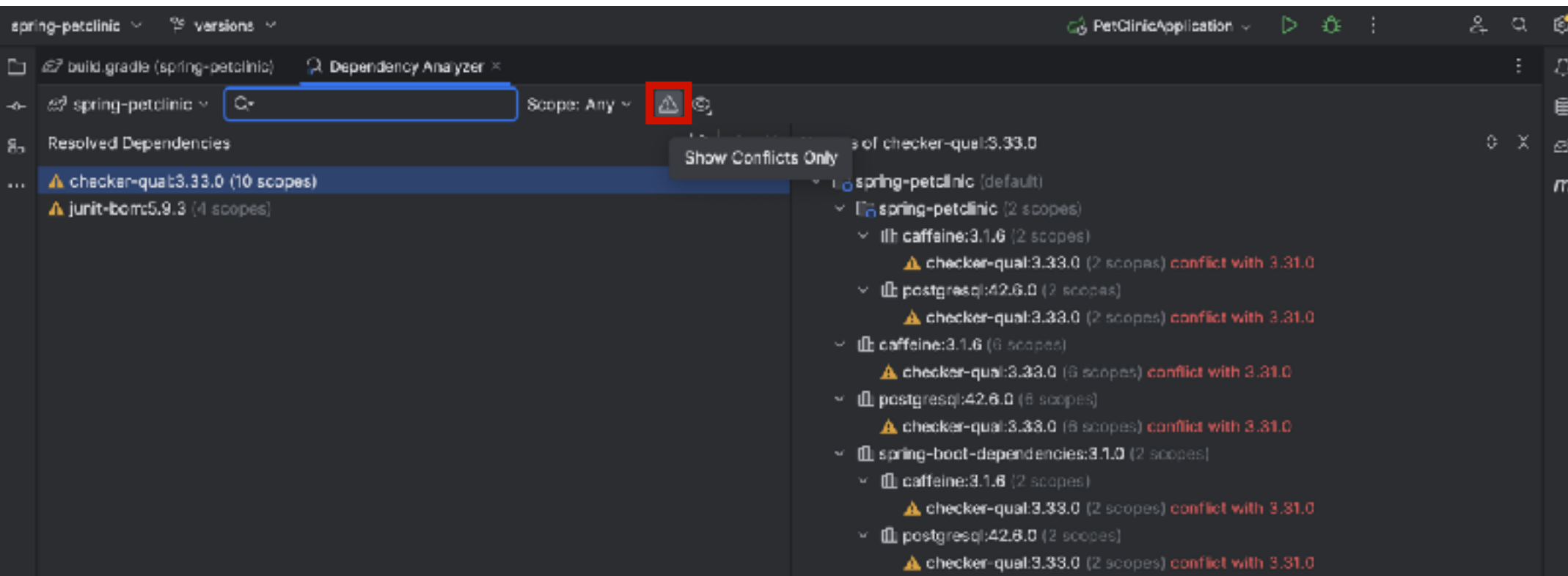
IntelliJ IDEA: Dependency Analyzer



https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer





IntelliJ IDEA

- Package Search: Add dependency

```
120
121     <dependency>
122         <groupId>org.junit.</groupId>
123         <artifactId>org.junit.jupiter</artifactId>
124     </dependency>
125
126 </dependencies>
127
128 <build>
```

org.junit.platform
org.junit.vintage
org.junit

Press ↵ to insert, → to replace Next Tip



IntelliJ IDEA

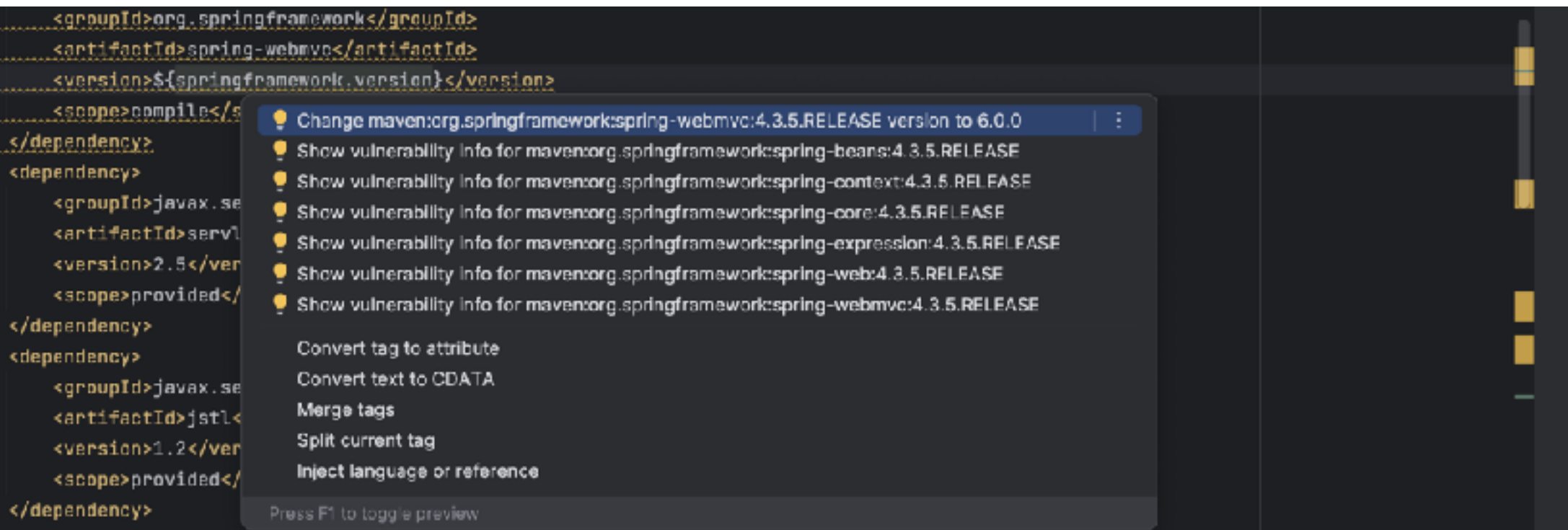
- Package Search: Add dependency

```
120
121     <dependency>
122         <groupId>org.junit.jupiter</groupId>
123         <artifactId>junit-jupiter</artifactId>
124         <scope>test</scope>
125     </dependency>
```



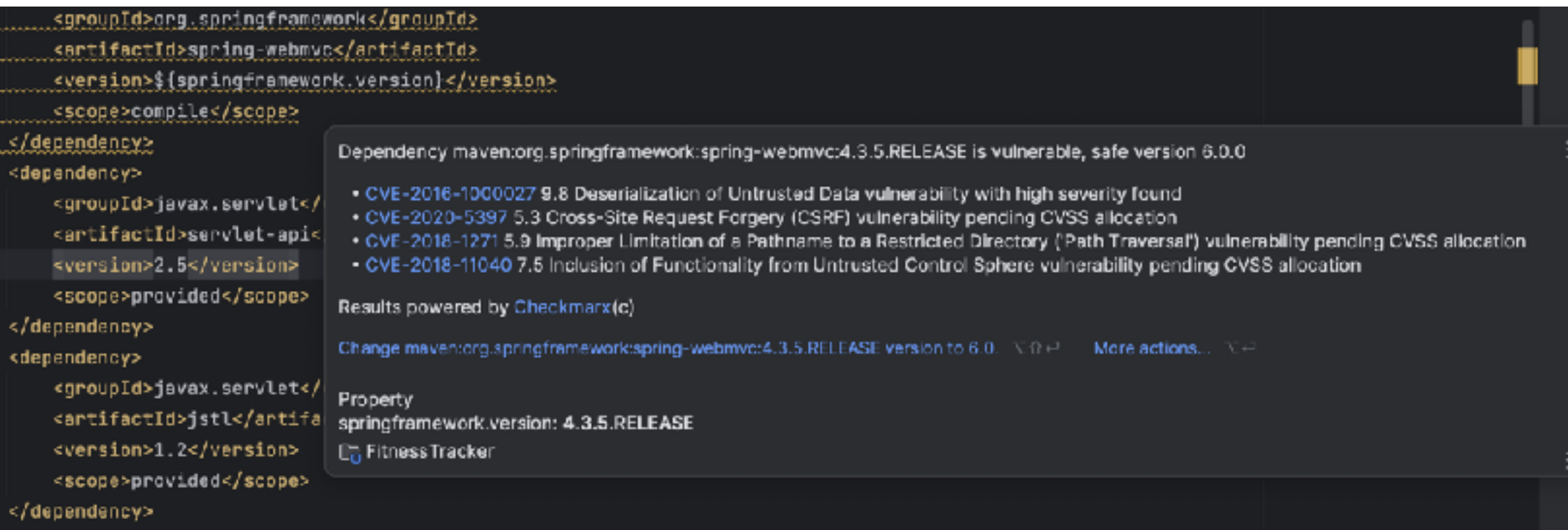
IntelliJ IDEA: Update dependencies

- Context Actions (`⌘ ↵` or `Alt+Enter`)



IntelliJ IDEA: Update dependencies

- Hover



IntelliJ IDEA



- Dependencies tool window

The screenshot shows the IntelliJ IDEA interface with the 'Dependencies' tool window open. The window is divided into three main sections: a left sidebar, a central table of dependencies, and a right-hand details panel.

Left Sidebar: Shows the project structure with 'All Modules' expanded, highlighting the 'FitnessTracker' module.

Central Table: Displays a list of dependencies added in all modules. The table has columns for the dependency name, its coordinates (group ID, artifact ID, version), and an 'Upgrade' button. The table is filtered to show only stable dependencies.

Added in all modules		10	Upgrade all (9)
Jackson-annotations	com.fasterxml.jackson.core:jackson-annotations	2.9.7 → 2.15.1	Upgra...
Jackson-core	com.fasterxml.jackson.core:jackson-core	2.9.7 → 2.14.2	Upgra...
com.fasterxml.jackson.core:jackson-databind		2.9.7 → 2.15.1	Upgra...
XStream Core	com.thoughtworks.xstream:xstream	1.4.10 → 1.4.20	Upgra...
javax.servlet:javax.servlet-api		1.2	
JavaServlet(TM) Specification	javax.servlet:servlet-api	2.5 → 3.0-alpha-1	Upgra...
JUnit	junit:junit	3.8.1 → 4.13.2	Upgra...
Hibernate Validator Engine - Relocation Artifact		4.2.0.Final → 8.0.0	Upgra...
Spring Object/XML Marshalling	org.springframework:spring-oxm	4.3.5.RELEASE → 4.3.5	Upgra...
Spring Web MVC	org.springframework:spring-webmvc	4.3.5.RELEASE → 4.3.5	Upgra...

Right Panel (Jackson-annotations details):

- Upgrade** button
- com.fasterxml.jackson.core:jackson-annotations
- Core annotations used for value types, used by Jackson data binding package.
- GitHub ☆ 0
- License: Apache License 2.0
- Project site
- Used in: FitnessTracker
- Authors: Tatu Saloranta, Christopher Currie, Paul Brown

IntelliJ IDEA



- Dependencies tool window (search)

The screenshot shows the IntelliJ IDEA interface with the 'Dependencies' tool window open. The 'Manage' tab is selected, and the search bar contains 'junit'. The search results list various JUnit dependencies, including JUnit, JUnit-dep, JUnit-pioneer, JUnit-logging, JUnit-theories, JUnit-rules, JUnit-jupiter, JUnit-extensions, JUnit-zookeeper, JUnit-validation, JUnit-utils, and JUnit-categories. The 'JUnit:junit' entry is highlighted, and its details are shown on the right. The details include the version '4.13.2', a link to 'Upgrade all (1)', and a description of JUnit as a unit testing framework for Java. The 'Used in' section shows 'FitnessTracker'.

Search Results	25	Upgrade all (1)
JUnit:junit:junit	[default] v	3.8.1 → 4.13.2 v Upgrade...
JUnit:junit:junit-dep	[default] v	4.11 v Add
org.junit-pioneer:junit-pioneer	[default] v	2.0.0 v Add
com.jcovalent.junit:jcovalent-junit-logging	[default] v	0.1.1 v Add
org.junit.contrib:junit-theories	[default] v	5.0-alpha-3 v Add
JUnit Rules com.btmatthews:junit:junit-rules	[default] v	1.0.1 v Add
JUnit Jupiter (Aggregator) org.junit:jupiter:junit	[default] v	5.9.2 v Add
JUnit Extensions org.dmonix:junit:junit-extensions	[default] v	1.1 v Add
ZooKeeper JUnit org.dmonix:junit:zookeeper-junit	[default] v	1.2 v Add
JUnit Validation com.lotaris:junit:junit-validation	[default] v	0.3.1 v Add
org.fingerprintsoft.junit:junit-utils	[default] v	1.4.0 v Add
JUnit Categories net.ggttools:junit:junit-categories	[default] v	1.0 v Add

JUnit
junit:junit
Upgrade

JUnit is a unit testing framework for Java, created by Erich Gamma and Kent Beck.
GitHub ☆ 8,4k
License: Eclipse Public License 1.0
Project site
Documentation
Readme

Used in:
• FitnessTracker

IntelliJ IDEA



Dependency Checker Vulnerable Dependencies

✓ All libs from FitnessTracker

- ✗ maven:com.thoughtworks.xstream:xstream:
- ✗ maven:com.fasterxml.jackson.core:jackson-
- ✓ maven:org.springframework:spring-context:
- ✗ maven:org.springframework:spring-beans:4
- ✓ maven:org.hibernate:hibernate-validator:4.2
- ✗ maven:org.springframework:spring-webmvc:
- ✓ maven:org.springframework:spring-express

Dependency maven:com.fasterxml.jackson.core:jackson-databind:2.9.7 is vulnerable Results powered by Checkmarx

Upgrade to 2.12.7.1 Copy safe version to clipboard

✗ CVE-2019-16942, Score: 9.8

A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.7.9.7, 2.8x before 2.8.11.5 and 2.9.x before 2.9.10.1. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of

19:21 LF UTF-8 4 spaces

<https://www.jetbrains.com/help/idea/package-analysis.html>

@MaritvanDijk77

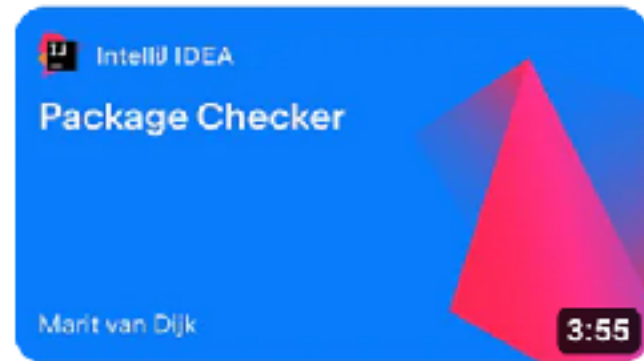
IntelliJ IDEA



IntelliJ IDEA: Viewing Dependencies



IntelliJ IDEA: Managing Dependencies



IntelliJ IDEA Ultimate: Package Checker



IntelliJ IDEA: Analyzing Dependencies

<https://www.youtube.com/@intellijidea>

@MaritvanDijk77

Pros & Cons

- + Check dependencies while working on the project
- Check out each individual project
- Apply & verify updates

Software Composition Analysis (SCA)

- Scan all repos (and containers)
- Overview



SCA: Pros & Cons

- + No need to check out repos individually
- I have to check the dashboard
- Apply & verify updates



@MaritvanDijk77

Bots

 Dependabot

 Renovate

 Snyk Open Source



@MaritvanDijk77

Dependabot



- GitHub native
- Features:
 - Alerts
 - Security updates
 - Version updates

Dependabot enable



Settings

- Pages
- Saved replies

Security

Code security and analysis

Integrations

- Applications
- Scheduled reminders

Archives

- Security log
- Sponsorship log

Developer settings

Dependency graph

Understand your dependencies.

- ☒ Automatically enable for new private repositories

Disable all

Enable all

Dependabot

Keep your dependencies secure and up-to-date. [Learn more about Dependabot.](#)

Dependabot alerts

Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications.](#)

- ☒ Automatically enable for new repositories

Disable all

Enable all

Dependabot security updates

Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

- ☒ Automatically enable for new repositories ✓

Disable all

Enable all

@MaritvanDijk77

Dependabot alerts



mlvandijk / FitnessTracker Public

Pin Watch 1 Fork 0 Star 0

Code Issues 1 Pull requests 53 Actions Security 90 Insights Settings

Pulse Contributors Community Community Standards Traffic Commits Code frequency **Dependency graph** Metadata

Dependency graph

Dependencies Dependents Dependabot

⚠️ We found potential security vulnerabilities in your dependencies.

Dependencies defined in these manifest files have known security vulnerabilities and should be updated:

pom.xml 90 vulnerabilities found

[View Dependabot alerts](#)

Only the owner of this repository can see this message.

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77

Dependabot alerts



< Code Issues 1 Pull requests 52 Actions Security 91 Insights Settings

Pulse
Contributors
Community
Community Standards
Traffic
Commits
Code frequency
Dependency graph
Network
Forks

Dependency graph

Dependencies Dependents Dependabot

Export SBOM

Search all dependencies

com.fasterxml.jackson.core:jackson-databind 2.9.7

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

14 critical

com.thoughtworks.xstream:xstream 1.4.10

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · NOASSERTION

1 critical

org.springframework:spring-webmvc 4.3.5.RELEASE

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

1 critical

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77

Dependabot alerts



Contributors

Community

Community Standards

Traffic

Commits

Code frequency

Dependency graph

Network

Forks

DependenciesDependentsDependabot

Export SBOM

Search all dependencies

com.fasterxml.jackson.core:jackson-databind 2.9.7

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

com.thoughtworks.xstream:xstream 1.4.10

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · NOASSERTION

org.springframework:spring-webmvc 4.3.5.RELEASE

Detected automatically on Feb 14, 2023 (Maven) · pom.xml · Apache-2.0

org.hibernate:hibernate-validator 4.2.0

Detected automatically on Feb 14, 2023 (Maven) · pom.xml

14 critical

View Dependabot alerts

14 critical · 55 total

Update to v2.12.7.1

#70

pom.xml update suggested:

com.fasterxml.jackson...

Always verify the validity and compatibility of suggestions with your codebase.

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>

@MaritvanDijk77



Dependabot security updates

Dependabot alerts / #85

Deserialization of untrusted data in FasterXML jackson-databind #85

Dismiss alert ▾

 Open Opened 7 months ago on com.fasterxml.jackson.core:jackson-databind (Maven) · pom.xml

 **Bump jackson-databind from 2.9.7 to 2.12.7.1** 

Merging this pull request would fix [55 Dependabot alerts](#) on com.fasterxml.jackson.core:jackson-databind in [pom.xml](#).

Package	Affected versions	Patched version
 com.fasterxml.jackson.core:jackson-databind (Maven)	<= 2.9.9.1	2.9.9.2 

SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used (because of net.sf.ehcache.transaction.manager.DefaultTransactionManagerLookup), leading to remote code execution.

 dependabot bot opened this 7 months ago

Severity

Critical 9.8 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weaknesses

CWE-915

CWE-1321

<https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/about-dependabot-security-updates>

@MaritvanDijk77

Dependabot security updates



> Code Issues 1 Pull requests 52 Actions Security 91 Insights Settings

Bump jackson-databind from 2.9.7 to 2.12.7.1 #70

Edit <> Code

Open dependabot wants to merge 1 commit into `main` from `dependabot/maven/com.fasterxml.jackson.core:jackson-databind-2.12.7.1`

Merging this pull request will resolve 55 Dependabot alerts on `com.fasterxml.jackson.core:jackson-databind` including a critical severity alert.

Conversation 1 Commits 1 Checks 0 Files changed 1 +1 -1

dependabot bot commented on behalf of github on Nov 16, 2022 • edited

Bumps `jackson-databind` from 2.9.7 to 2.12.7.1.

► Commits

Reviewers
No reviews
Still in progress? Convert to draft

<https://docs.github.com/en/code-security/dependabot/dependabot-security-updates/about-dependabot-security-updates>

@MaritvanDijk77



Dependabot version updates

- Add dependabot.yml
- Specify:
 - Package manager & location of manifest file
 - Schedule interval (daily, weekly, or monthly)
- Optional:
 - Max. number of PR's (default 5)
 - Rebase strategy
 - Etc

Dependabot: Supported platforms



- GitHub native
- Can run on GitLab too



Renovate

- Available via GitHub App
- Features:
 - Security updates
 - Version updates
 - Project dashboard

Renovate enable



GitHub App

Renovate



Configure

Manage your installation settings.

Developer

 [renovatebot](#)

 [Website](#)

Renovate is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

 [Report abuse](#)

<https://github.com/apps/renovate>

@MaritvanDijk77

Renovate enable - 3



Install Renovate

Install on your personal account Marit van Dijk

☐ All repositories

This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).

☒ Only select repositories

Select at least one repository.
Also includes public repositories (read-only).

 Select repositories ▾

Selected 1 repository.

 mlvandijk/FitnessTracker

×

@MaritvanDijk77

Renovate onboarding PR



Configure Renovate #59

[Open](#) renovate wants to merge 1 commit into `main` from `renovate/configure`

Conversation 0 Commits 1 Checks 0 Files changed 1

renovate bot commented 3 minutes ago

MENDRenovate

Welcome to [Renovate](#)! This is an onboarding PR to help you understand and configure settings before regular Pull Requests begin.

To activate Renovate, merge this Pull Request. To disable Renovate, simply close this Pull Request unmerged.

Detected Package Files

- `pom.xml` (maven)

Configuration Summary

Based on the default config's presets, Renovate will:

- Start dependency updates only once this onboarding PR is merged
- Enable Renovate Dependency Dashboard creation.
- If Renovate detects semantic commits, it will use semantic commit type `fix` for dependencies and `chore` for all others.
- Ignore `node_modules`, `bower_components`, `vendor` and various test/tests directories.
- Autodetect whether to pin dependencies or maintain ranges.
- Rate limit PR creation to a maximum of two per hour.
- Limit to maximum 10 open PRs at any time.
- Group known monorepo packages together.
- Use curated list of recommended non-monorepo package groupings.
- A collection of workarounds for known problems with packages.

```
1 + {  
2 +   "$schema": "https://docs.renovatebot.com/renovate-schema.json",  
3 +   "extends": [  
4 +     "config:base"  
5 +   ]  
6 + }
```

@MaritvanDijk77



Renovate configuration

- All repos or selected repos
- Config file is created for you
- Scheduling
- Max. number of PR's / concurrent branches
- Rule based auto merge
- More options & more fine-grained



Renovate PR

Update jackson.version to v2.13.4 #64

 Open renovate wants to merge 1 commit into `main` from `renovate/jackson.version` 

 Conversation 0  Commits 1  Checks 1  Files changed 1



renovate bot commented 12 days ago

Contributor



This PR contains the following updates:

Package	Change	Age	Adoption	Passing	Confidence
<code>com.fasterxml.jackson.core:jackson-databind</code> (source)	2.9.7 -> 2.13.4	 16d	 15%	 96%	 neutral
<code>com.fasterxml.jackson.core:jackson-annotations</code> (source)	2.9.7 -> 2.13.4	 16d	 11%	 99%	 high
<code>com.fasterxml.jackson.core:jackson-core</code>	2.9.7 -> 2.13.4	 16d	 15%	 97%	 neutral

<https://docs.renovatebot.com/merge-confidence/>

@MaritvanDijk77



Renovate Dashboard: Project

Dependency Dashboard #68

[Open](#) [9 tasks](#) renovate bot opened this issue 21 hours ago · 0 comments

 renovate bot commented 21 hours ago Contributor ...

This issue lists Renovate updates and detected dependencies. Read the [Dependency Dashboard](#) docs to learn more.

Open

These updates have all been created already. Click a checkbox below to force a retry/rebase of any.

- ☐ Update dependency com.thoughtworks.xstream:xstream to v1.4.19
- ☐ Update dependency junit:junit to v3.8.2
- ☐ Update spring core to v4.3.30.RELEASE (org.springframework:spring-oxm , org.springframework:spring-webmvc)
- ☐ Update jackson.version to v2.13.4 (com.fasterxml.jackson.core:jackson-databind , com.fasterxml.jackson.core:jackson-annotations , com.fasterxml.jackson.core:jackson-core)
- ☐ Update dependency junit:junit to v4
- ☐ Update dependency org.hibernate:hibernate-validator to v8
- ☐ Update spring core to v5 (major) (org.springframework:spring-oxm , org.springframework:spring-webmvc)
- ☐ Click on this checkbox to rebase all open PRs at once

Detected dependencies

► maven

☐ Check this box to trigger a request for Renovate to run again on this repository

@MaritvanDijk77

Renovate Dashboard: Jobs



Renovate Dashboard			Documentation	Sign out
cucumber/cucumber-jvm logs				
Search				
cucumber-json-converter	Job ID	Result	Date	
cucumber-json-schema	991877684	done	16 minutes ago	
cucumber-junit-xml-formatter	991973171	done	4 hours ago	
cucumber-jvm	991985485	done	7 hours ago	
cucumber-jvm-groovy	991776931	done	11 hours ago	
cucumber-jvm-scala	991631974	done	16 hours ago	
cucumber-lua	991516227	done	28 hours ago	
cucumber-message-upload-service	991448085	done	a day ago	
cucumber-parent	991278531	done	a day ago	
cucumber-rails	991281844	done	a day ago	
cucumber-ruby	991096798	done	a day ago	
cucumber-ruby-core	991977987	done	2 days ago	
cucumber-ruby-meta	991886491	done	2 days ago	
cucumber-ruby-wire	991554817	done	2 days ago	
cucumber-icli-wire	991326488	done	2 days ago	
cucumber.ml	991118578	done	2 days ago	
demo-formatter	991883169	done	3 days ago	
docs	991653641	done	3 days ago	
	991388884	done	3 days ago	

@MaritvanDijk77



Renovate: Supported platforms

- GitHub (.com and Enterprise Server)
- GitLab (.com and CE/EE)
- Bitbucket Cloud
- Bitbucket Server
- Azure DevOps
- AWS CodeCommit
- Gitea



Snyk Open Source

- Available via Snyk
- Features:
 - Security updates
 - Version updates
 - Test for new vulnerabilities (on PRs)
 - Test for vulnerabilities in source code
 - Dashboards

<https://snyk.io/>

@MaritvanDijk77

Snyk enable



Developer loved, Security trusted.

Find and automatically fix vulnerabilities in your code, open source dependencies, containers, and IaC — powered by Snyk's industry-leading security intelligence and DeepCode AI.

Start free

Book a live demo →

→ snyk test

Testing /users/gooddog/projects/woof...

Tested 3 dependencies for known issues, found 2 issues, 2 vulnerable paths.

⚠ Remote Code Execution (RCE) [Critical Severity] in log4j-core@2.14.1
Introduced by io.gooddog:woof@0.6.1

This issue was fixed in versions: 2.8.1, 2.12.2, 2.15.0

Package manager: maven
Target file: pom.xml
Project name: io.gooddog:woof

SNYK-JAVA-ORGAPACHELOGGINGLOG4J-231728 (See <https://snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-231728>)

We highly recommend fixing this vulnerability. If it cannot be fixed by upgrading, see mitigation information here:



Snyk enable

Where is the code you want to scan?
Scan your projects for security issues

1 Choose integration method
Connect Snyk to your code and run scans directly in your workflow

☒
GitHub

☐
Bitbucket Cloud

☐
CLI

Next step

Not what you're looking for?
[View all integrations](#) OR [Learn more about integrations](#)

2 Set access permissions

3 Configure automation settings & authenticate

@MaritvanDijk77



Snyk enable

Where is the code you want to scan?
Scan your projects for security issues

✓ Choose integration method

2 Set access permissions

☒ **Private and public repositories**
Grant Snyk access to all repository types under your Github account whether private or public.

☐ **Public repositories only**
Grant Snyk access to repositories marked public under your Github account.

Once authenticated, Snyk:

- ✓ Scans the directory trees of selected repos and automatically represents them as projects
- ✓ Generates security reports that enable you to explore issues in your repositories and assist you with fixing them
- ✓ Continuously checks imported projects for vulnerabilities. When new vulnerabilities are found, you'll be notified

[Next step](#) [Previous](#)

3 Configure automation settings & authenticate

@MaritvanDijk77

Snyk enable



✓ Choose integration method

✓ Set access permissions

3 Configure automation settings & authenticate

Enabled features:

- ☒ Pull Request Checks
Test your pull requests for new issues and vulnerabilities
- ☒ New Fix Pull Requests
Automatically create pull requests for newly discovered open source issues and vulnerabilities
- ☒ Dependency Upgrade Pull Requests
Keep your packages up to date with automatic dependency upgrade pull requests
- ☒ Snyk Code
Analyze your source code for issues and vulnerabilities ⓘ

Authenticate GitHub

Previous

@MaritvanDijk77

Snyk enable



Authorize Snyk



Snyk by **Snyk**

wants to access your mlvandijk account



Organizations and teams

Read-only access



Repositories

Public and private



Personal user data

Email addresses (read-only)



@MaritvanDijk77



Snyk PR

[Snyk] Security upgrade com.fasterxml.jackson.core:jackson-databind from 2.9.7 to 2.9.10.7 #47

Edit <> Code

Open snyk-bot wants to merge 1 commit into [main](#) from [snyk-fix-6545eb40c5d321178cd9bea857119a55](#)

Conversation 0 Commits 1 Checks 0 Files changed 1

+1 -1



snyk-bot commented on 19 Jan 2021

First-time contributor

Snyk has created this PR to fix one or more vulnerable packages in the `maven` dependencies of this project.

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Upgrade	Breaking Change
	691/1000 Why? Recently disclosed, Has a fix available, CVSS 8.1	Deserialization of Untrusted Data SNYK-JAVA-COMFASTERXMLJACKSONCORE-1061931	<code>com.fasterxml.jackson.core:jackson-databind:</code> 2.9.7 => 2.9.10.7	No

Reviewers

No reviews

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

@MaritvanDijk77



Snyk PR

[Snyk] Fix for 5 vulnerabilities #49

Open mlvandijk wants to merge 1 commit into [main](#) from [snyk-fix-854f735a21477e79bcea4d5278b3d1ba](#)

Conversation 0 Commits 1 Checks 0 Files changed 1



mlvandijk commented on 21 Feb 2021

Owner

Snyk has created this PR to fix one or more vulnerable packages in the `maven` dependencies of this project.

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Upgrade	Breaking Change	Exploit Maturity
H	644/1000 Why? Has a fix available, CVSS 8.6	Improper Input Validation SNYK-JAVA-ORGSRINGFRAMEWORK-1009832	<code>org.springframework:spring-webmvc</code> 4.3.5.RELEASE → 4.3.29.RELEASE	No	No Known Exploit
M	509/1000 Why? Has a fix available, CVSS 6.9	Information Exposure SNYK-JAVA-ORGSRINGFRAMEWORK-31689	<code>org.springframework:spring-webmvc</code> 4.3.5.RELEASE → 4.3.29.RELEASE	No	No Known Exploit

@MaritvanDijk77

Snyk PR Check





**All checks have passed**
1 successful check

[Hide all checks](#)

 security/snyk (mlvandijk) — 1 security test has passed

[Details](#)

@MaritvanDijk77

Snyk dashboard



 **snyk**

ORGANIZATION

 mlvandijk

 Dashboard

 Projects

 Integrations

 Members

 Settings

 Help

 Marit van Dijk

mlvandijk > Dashboard

Add projects

Pending tasks

Snyk tracks and flags Pull Requests (PRs) in the top most vulnerable projects

PROJECT	FIXABLE ISSUES	ACTIONS
 mlvandijk/kotlin-bootstrap	19  50  21  3 	Fix vulnerabilities
 mlvandijk/rugbymatch	19  50  16  3 	Fix vulnerabilities

Vulnerable projects

Projects with vulnerabilities detected

PROJECT	TESTED	ISSUES	ACTIONS
 mlvandijk/kotlin-bootstrap/pom.xml	Mar 2, 2021	0  69  21  3 	Fix vulnerabilities
 mlvandijk/rugbymatch/pom.xml	Mar 2, 2021	0  69  16  3 	Fix vulnerabilities
 mlvandijk/springbootproject/pom.xml	Mar 2, 2021	0  67  16  3 	Fix vulnerabilities
 mlvandijk/tul-restnonrest/pom.xml	Mar 2, 2021	0  65  9  4 	Fix vulnerabilities

Issues summary

SECURITY ISSUES

Critical
0

High
1015

Medium
329

Low
74

[Learn about reports](#)

@MaritvanDijk77



Snyk Open Source Configuration

- Frequency (daily, weekly, never)
- Enable/disable: New and/or known vulnerabilities
- Enable/disable PR's for single project



Snyk Open Source: Supported Platforms

- GitHub
- GitHub Enterprise
- GitHub Read-only projects
- Bitbucket Cloud Personal Access Token (Legacy)
- Bitbucket Cloud App
- Bitbucket Data Center/Server
- GitLab
- Azure Repos

<https://docs.snyk.io/integrations/git-repository-scm-integrations>

@MaritvanDijk77

Bots

 Dependabot

 Renovate

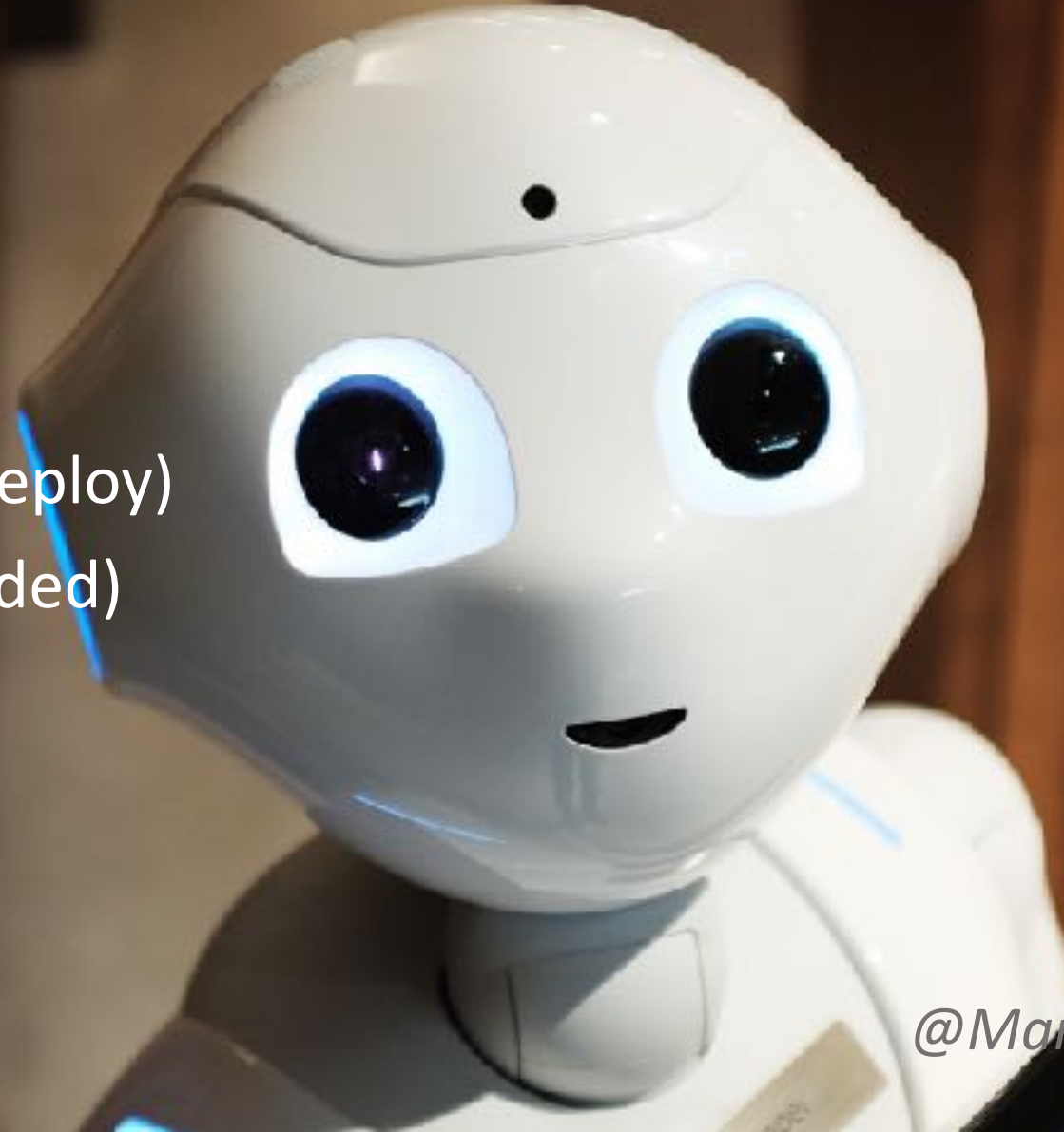
 Snyk Open Source



@MaritvanDijk77

Bots: Pros & Cons

- + Relatively easy to install
- + Automatic PR's
- Can create "noise"
- Manage PRs (merge & deploy)
- No code changes (if needed)



@MaritvanDijk77

Migration tools

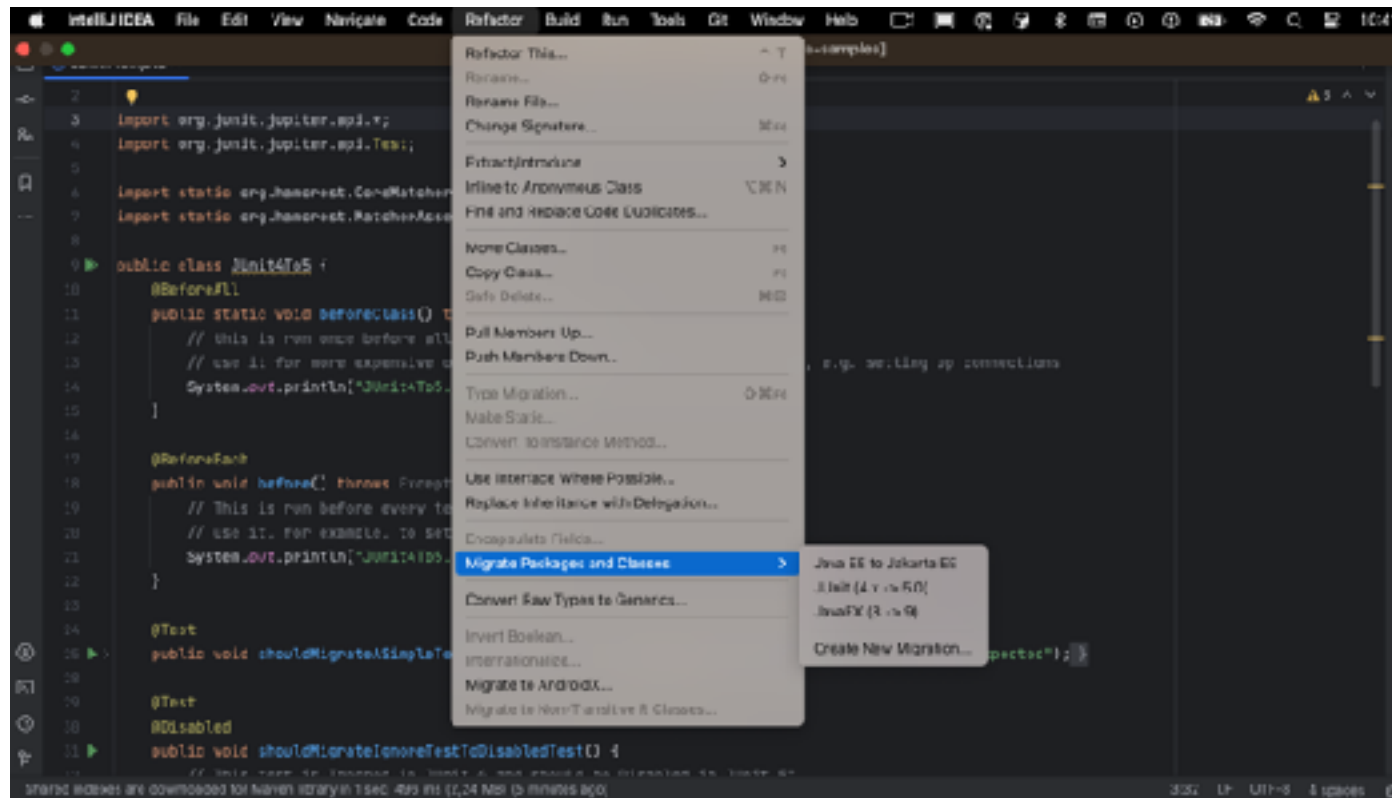


@MaritvanDijk77

IntelliJ IDEA



- Refactor > Migrate Packages and Classes



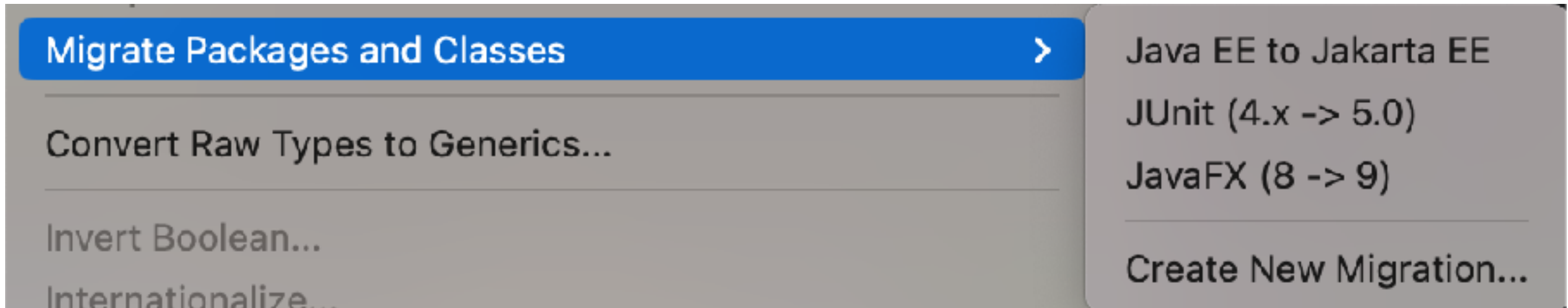
<https://www.jetbrains.com/help/idea/migrate.html>

@MaritvanDijk77

IntelliJ IDEA



- Refactor > Migrate Packages and Classes >
 - Java EE to Jakarta EE
 - JUnit (4.x -> 5.0)
 - JavaFX (8 -> 9)



IntelliJ IDEA



- Create New Migration

New Migration Map

Map name: Copy an existing ▾

Map description:

Type	Old name	New name
Nothing to show		

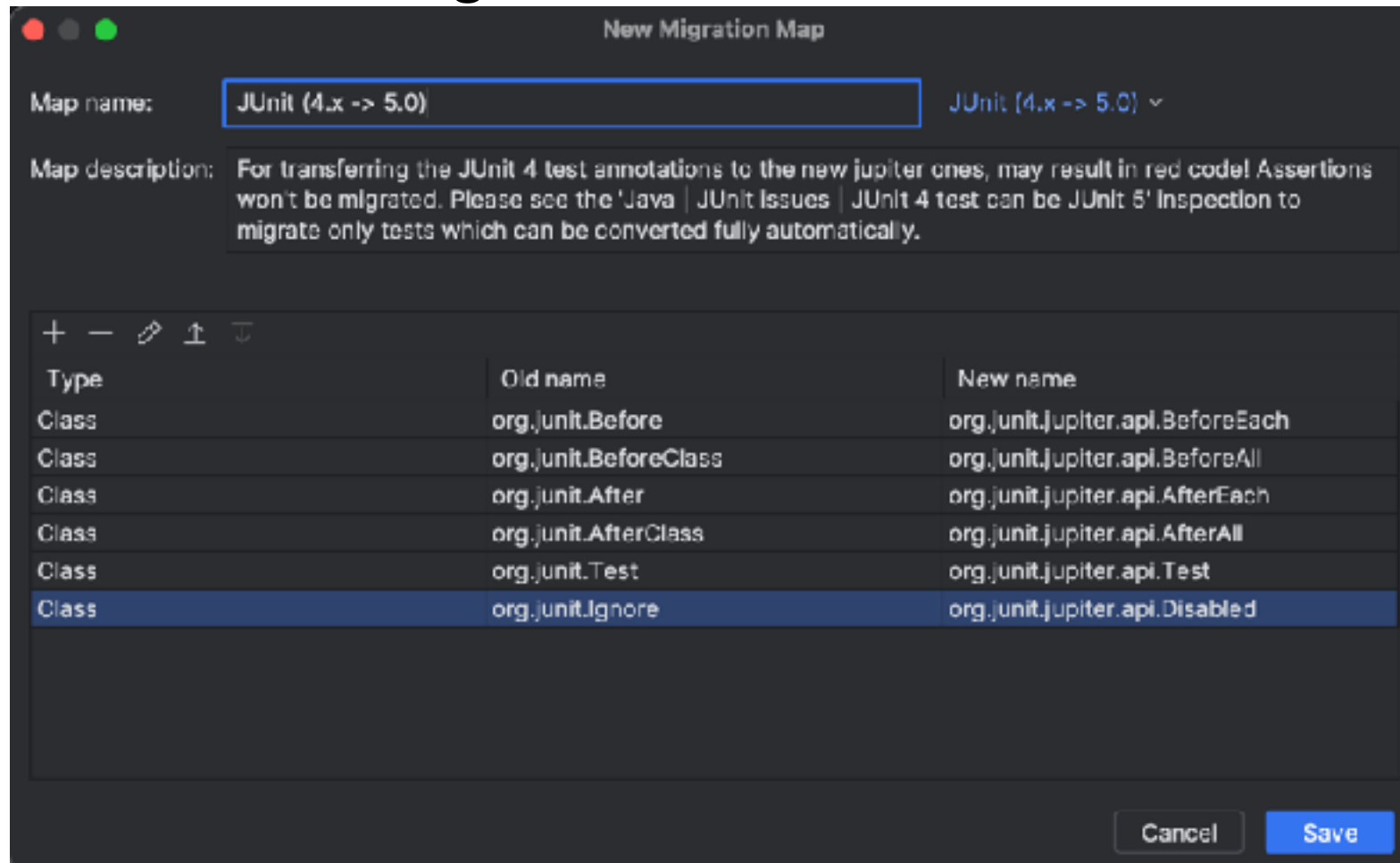
Cancel Save

@MaritvanDijk77

IntelliJ IDEA



- Create New Migration



@MaritvanDijk77

IntelliJ IDEA

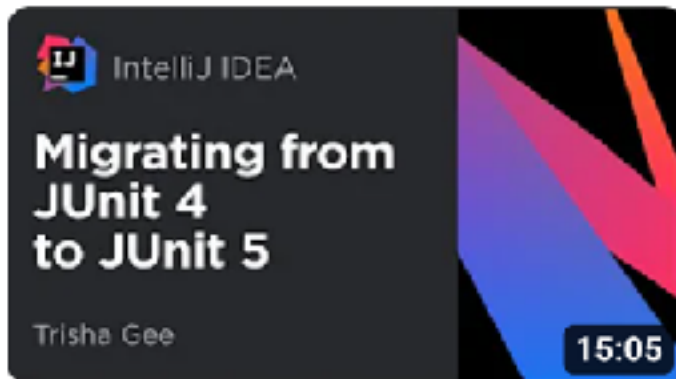


Migrating from javax to jakarta namespace

IntelliJ IDEA by JetBrains • 14K views • 11 months ago

In this video, we'll look at how to migrate an application from using the javax namespace to the jakarta namespace. This change is expected to impact a lot of enterprise Java developers, especially...

CC



IntelliJ IDEA. Migrating from JUnit 4 to JUnit 5

IntelliJ IDEA by JetBrains • 18K views • 2 years ago

JUnit has been around for a long time, and many applications will have a large number of JUnit tests written using JUnit 4. JUnit 5 was released in 2017, and provides a lot of features that...

CC

<https://www.youtube.com/@intellijidea>

@MaritvanDijk77

Error Prone

- **Static analysis tool** for Java to **catch common programming mistakes** at compile-time.
- Maven, Gradle, etc.
- IntelliJ IDEA / Eclipse plugin, Command line
- Bug patterns
- Report or fix
- Custom checks
- Includes **Refaster**: refactor code using before-and-after templates

Error Prone

Error Prone



The thumbnail features a green background with a white circular logo in the top right corner containing a stylized leaf and the text "J-SPRING 2022". Below the logo, the name "SANDER MAK" is written in white. The main image shows a white delivery truck with "PIC NIC" branding on a bridge over a canal, surrounded by lush green trees. A red "PIC NIC" logo is overlaid on the image. Below the image, a white banner contains a cartoon character holding a megaphone, the title "Streamlining Large-scale Java Development using Error Prone", and the handle "@Sander_Mak". At the bottom, a teal banner displays the text "STREAMLINING LARGE-SCALE JAVA DEVELOPMENT USING ERROR PRONE" in white. A small inset in the bottom right shows a man speaking at a podium with a "WELCOME" sign and a "nl jug" logo.

PIC NIC

Streamlining Large-scale Java Development using Error Prone

@Sander_Mak

STREAMLINING LARGE-SCALE JAVA DEVELOPMENT USING ERROR PRONE

SANDER MAK

WELCOME

nl jug

<https://www.youtube.com/watch?v=NPuLeolzIR0>

@MaritvanDijk77

Error Prone Support

[Bug Patterns](#)[Refaster Rules](#)

Error Prone Support

Error Prone Support is a [Picnic](#)-opinionated extension of Google's [Error Prone](#). It aims to improve code quality, focussing on maintainability, consistency and avoidance of common pitfalls.

<https://error-prone.picnic.tech/>

@MaritvanDijk77

OpenRewrite

- **Source code refactoring** for framework/API migrations, vulnerability patches, and static code analysis fixes
- Java, Kotlin & Groovy support
- Run with Maven or Gradle
- Run without a build tool
- Early support for Python, Typescript, ...

OpenRewrite



- Existing recipes
 - Upgrade versions
 - Migrate libraries

Popular recipe guides

Here are the articles in this section:

Common static analysis issue remediation

Automatically fix Checkstyle violations

Migrate to Java 17

Migrate to JUnit 5 from JUnit 4

Migrate to Spring Boot 3 from Spring Boot 2

Migrate to Spring Boot 2 from Spring Boot 1

Migrate to Quarkus 2 from Quarkus 1

Migrate to Micronaut 4 from Micronaut 3

Migrate to Micronaut 3 from Micronaut 2

Migrate to SLF4J from Log4J

Use SLF4J parameterized logging

Refactoring with declarative YAML recipes

Automating Maven dependency management

Migrate Hamcrest to AssertJ

<https://docs.openrewrite.org/running-recipes/popular-recipe-guides>

@MaritvanDijk77

OpenRewrite

- Existing recipes
 - Find by topic

Recipe catalog



Here are the articles in this section:

Kotlin	Python
Analysis	CircleCI
Cloud suitability analyzer	Concourse
Cucumber	GitHub Actions
Hibernate	Java
Jenkins	Kubernetes
XML	Micrometer
Okio	OkHttp
Quarkus	Recommendations
Gradle	Maven
SQL	Static analysis and remediation

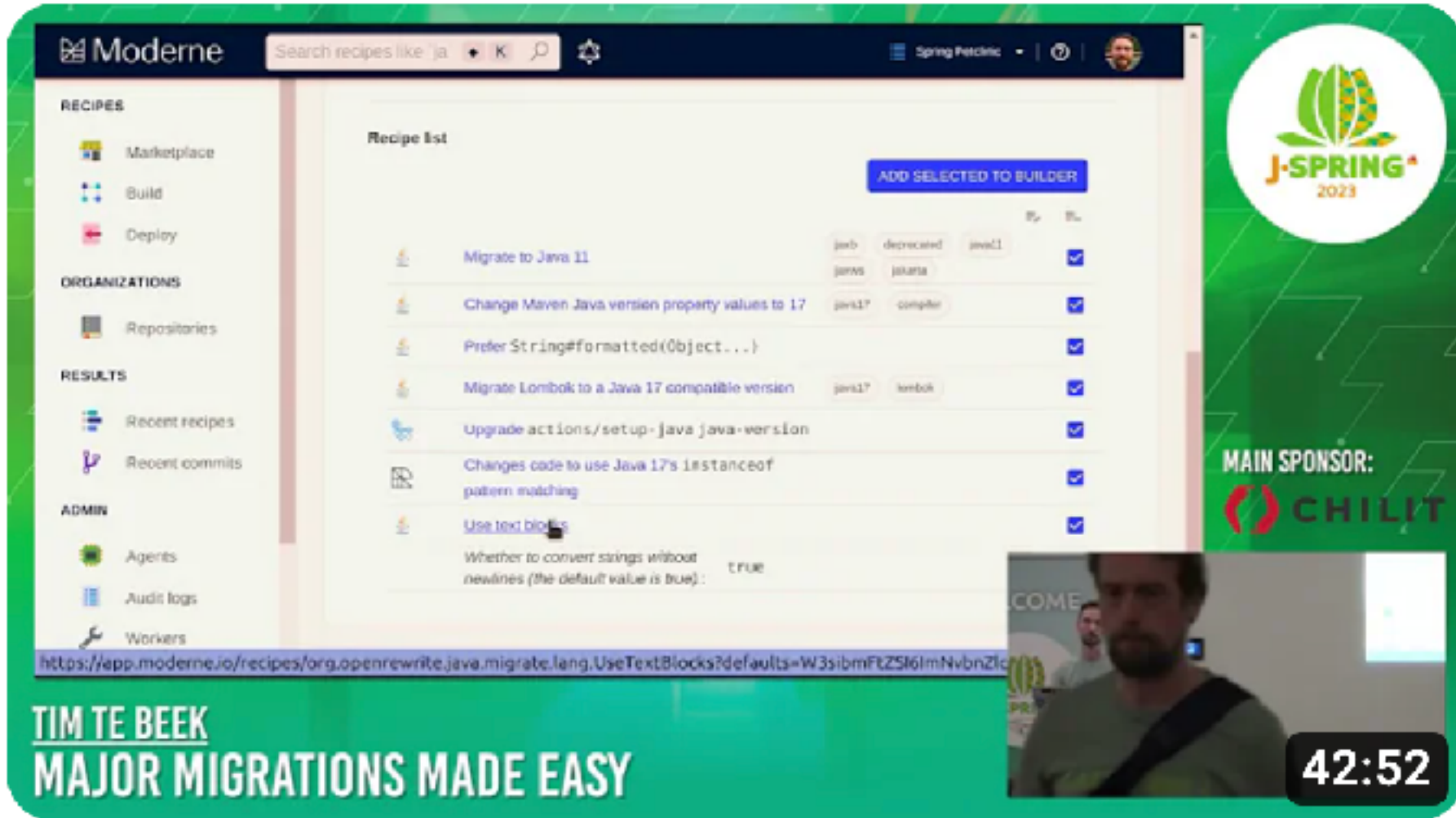
<https://docs.openrewrite.org/reference/recipes>

@MaritvanDijk77

OpenRewrite

- Existing recipes
- Can author your own recipes

OpenRewrite

A screenshot of the Moderne OpenRewrite web interface. The interface has a dark blue header with the "Moderne" logo, a search bar, and user information. A left sidebar contains navigation links for "RECIPES", "ORGANIZATIONS", "RESULTS", and "ADMIN". The main area, titled "Recipe list", shows a table of recipes with columns for recipe name, tags, and a checkbox. The recipes listed are: "Migrate to Java 11", "Change Maven Java version property values to 17", "Prefer String#formatted(Object...)", "Migrate Lombok to a Java 17 compatible version", "Upgrade actions/setup-java java-version", "Changes code to use Java 17's instanceof pattern matching", and "Use text blocks". A blue button "ADD SELECTED TO BUILDER" is at the top right of the recipe list. The interface is overlaid on a green background with a circuit pattern. On the right, there is a circular logo for "J-SPRING 2023" and text indicating "MAIN SPONSOR: CHILIT". At the bottom, there is a video player showing a man speaking, with the text "TIM TE BEEK MAJOR MIGRATIONS MADE EASY" and a timestamp "42:52".

RECIPES

- Marketplace
- Build
- Deploy

ORGANIZATIONS

- Repositories

RESULTS

- Recent recipes
- Recent commits

ADMIN

- Agents
- Audit logs
- Workers

Recipe list

Recipe	Tags	Actions
Migrate to Java 11	java8 deprecated java11	☒
Change Maven Java version property values to 17	java17 compiler	☒
Prefer String#formatted(Object...)		☒
Migrate Lombok to a Java 17 compatible version	java17 lombok	☒
Upgrade actions/setup-java java-version		☒
Changes code to use Java 17's instanceof pattern matching		☒
Use text blocks		☒

MAIN SPONSOR: CHILIT

TIM TE BEEK
MAJOR MIGRATIONS MADE EASY

42:52

<https://www.youtube.com/watch?v=jOffCAleUI8>

@MaritvanDijk77

Conclusion

- (Re)evaluate dependencies carefully
- Automate checks & updates
- Stay safe!

Slides & More

<https://maritvandijk.com/presentations/keep-your-dependencies-in-check/>



Don't forget to
rate this session
in the **GOTO Guide app**