goto;

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

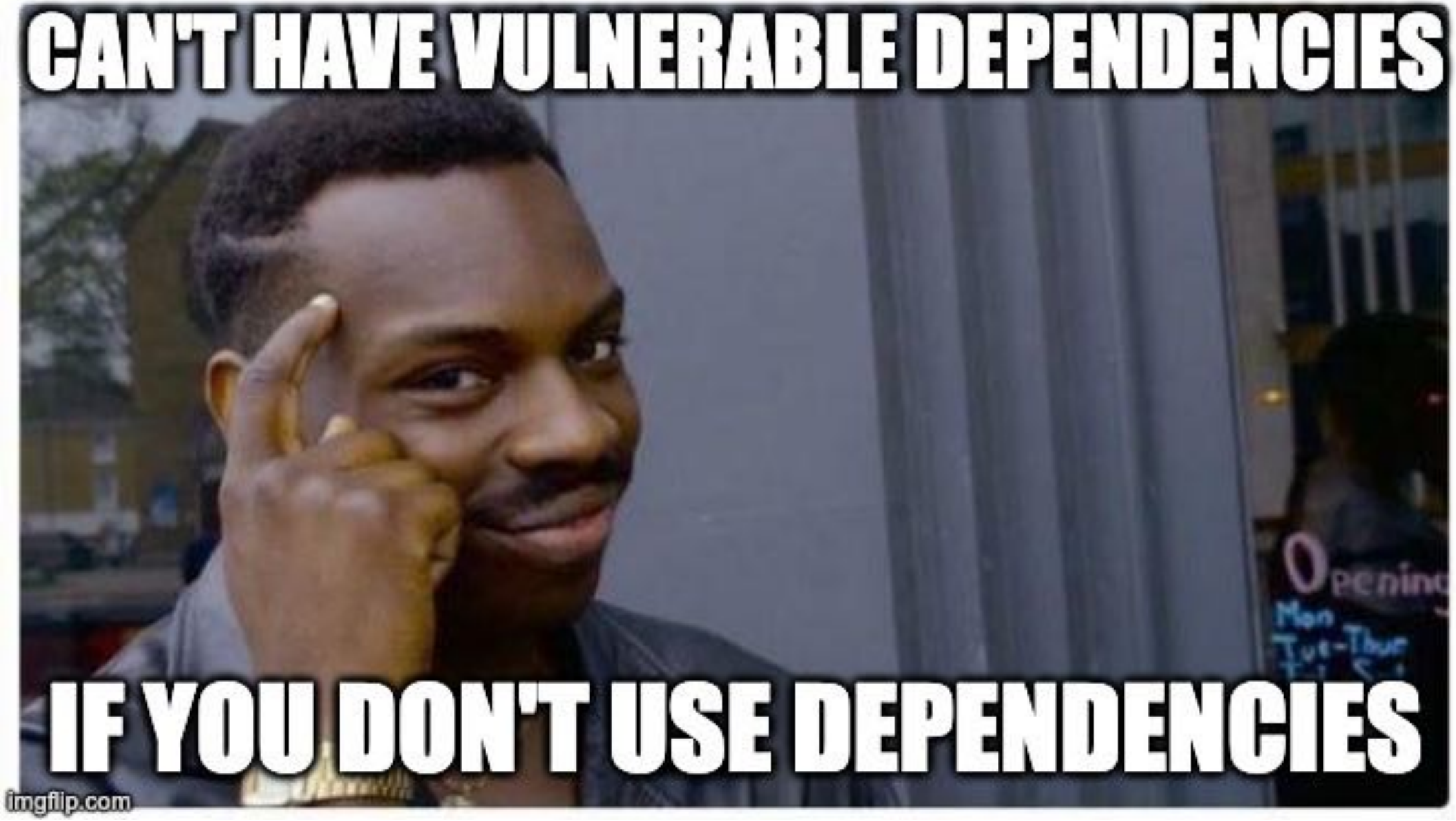
@MaritvanDijk77

@MaritvanDijk77

March 2022

@MaritvanDijk77


@MaritvanDijk77



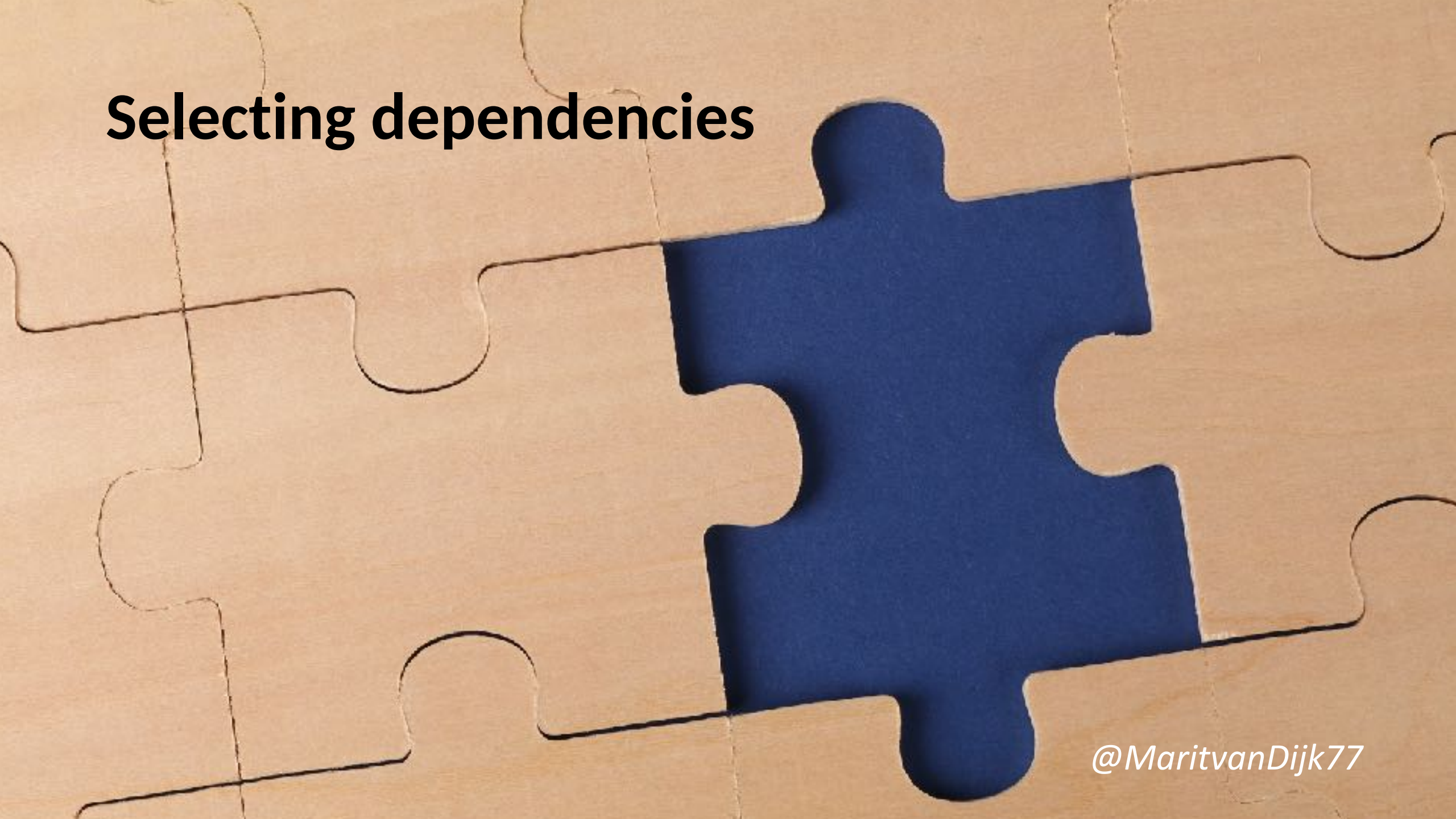
@MaritvanDijk77

@MaritvanDijk77

Do we **need** this dependency?

@MaritvanDijk77

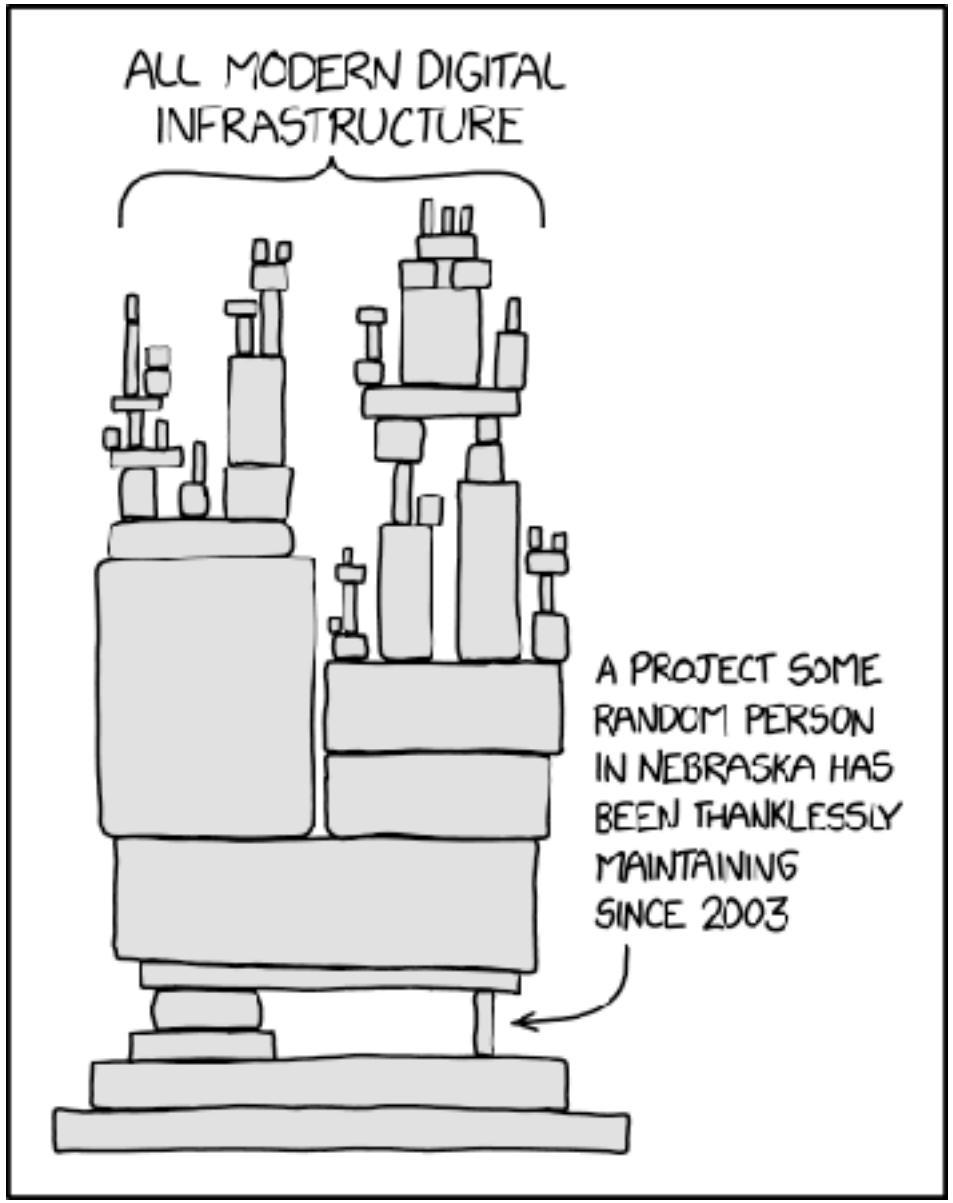
Selecting dependencies



@MaritvanDijk77

Selecting dependencies

@MaritvanDijk77



https://xkcd.com/2347/

@MaritvanDijk77

Selecting dependencies

@MaritvanDijk77

Selecting dependencies

@MaritvanDijk77

Selecting dependencies

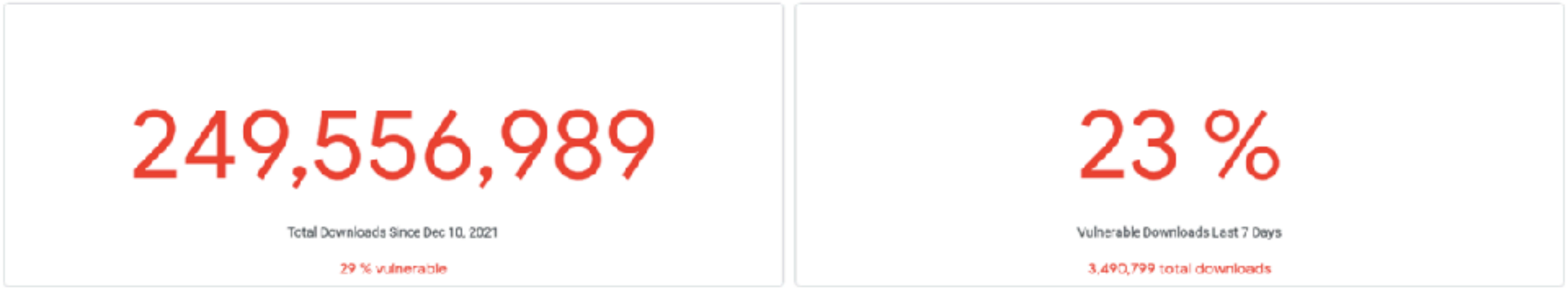
@MaritvanDijk77

Selecting dependencies

@MaritvanDijk77

Log4j download dashboard

log4j Latest Statistics

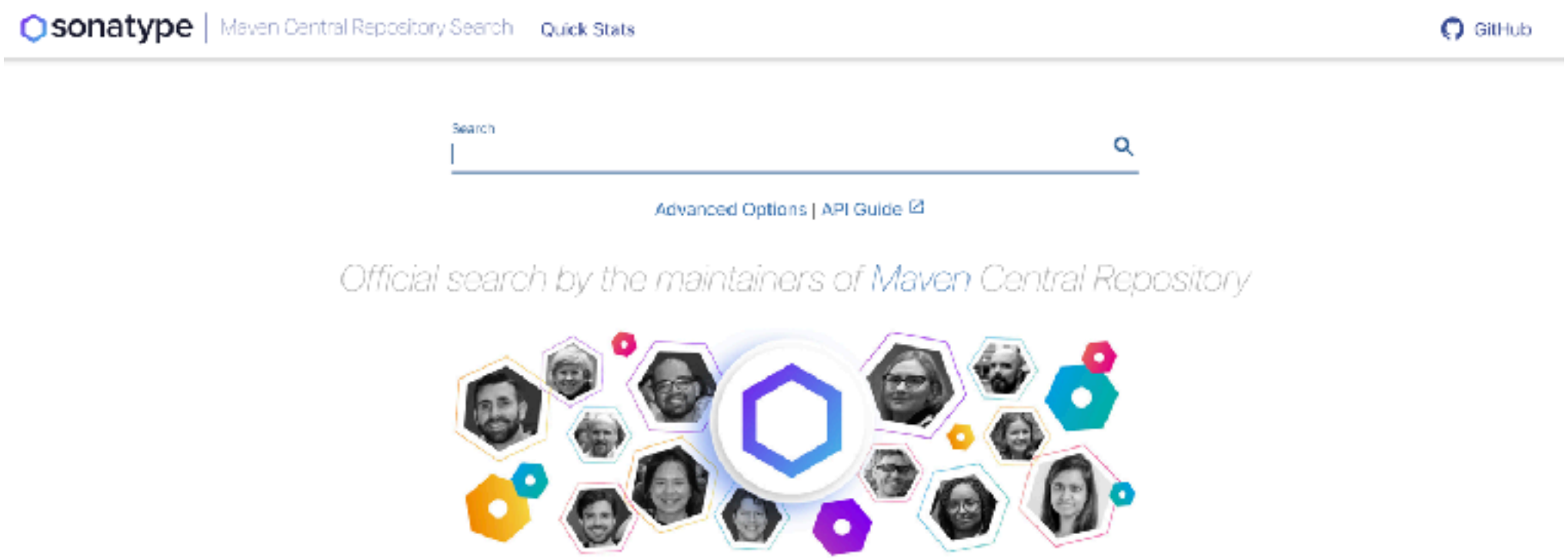


https://www.sonatype.com/resources/log4j-vulnerability-resource-center

@MaritvanDijk77

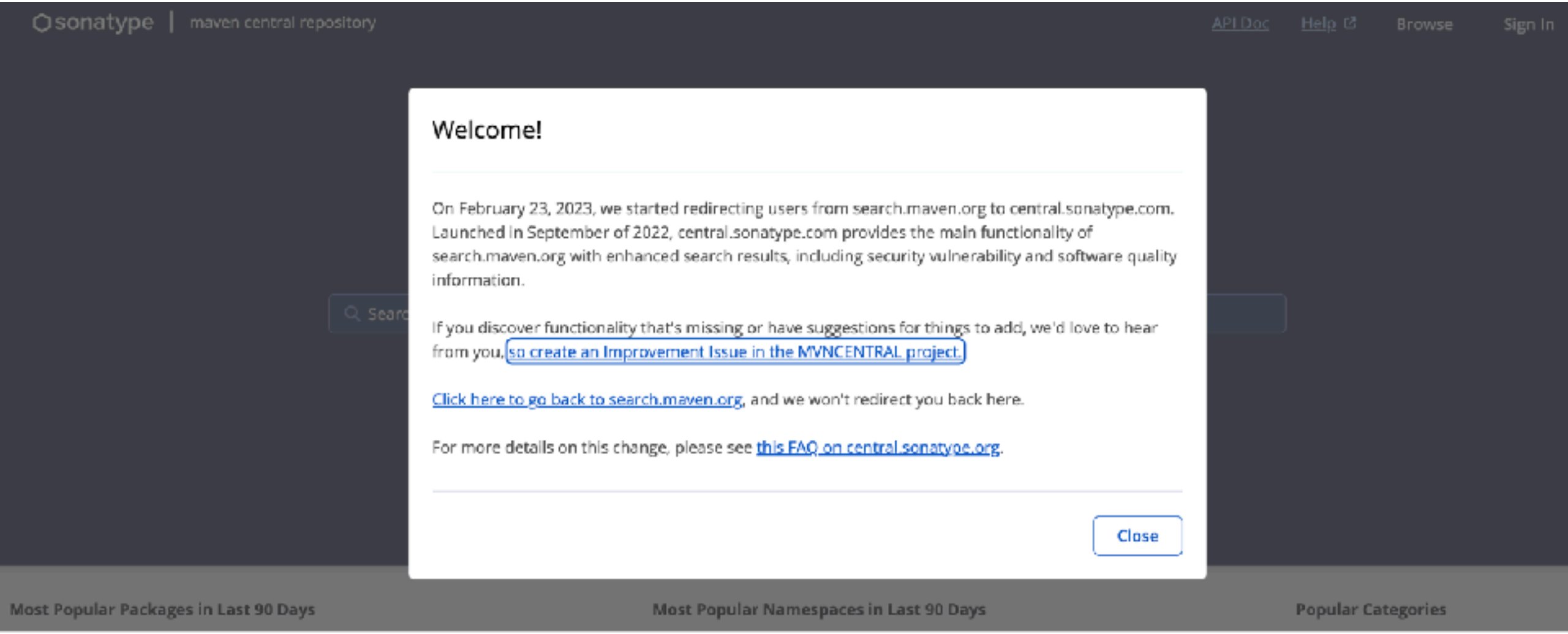

Find information
@MaritvanDijk77

Dependency information



https://search.maven.org/

Dependency information

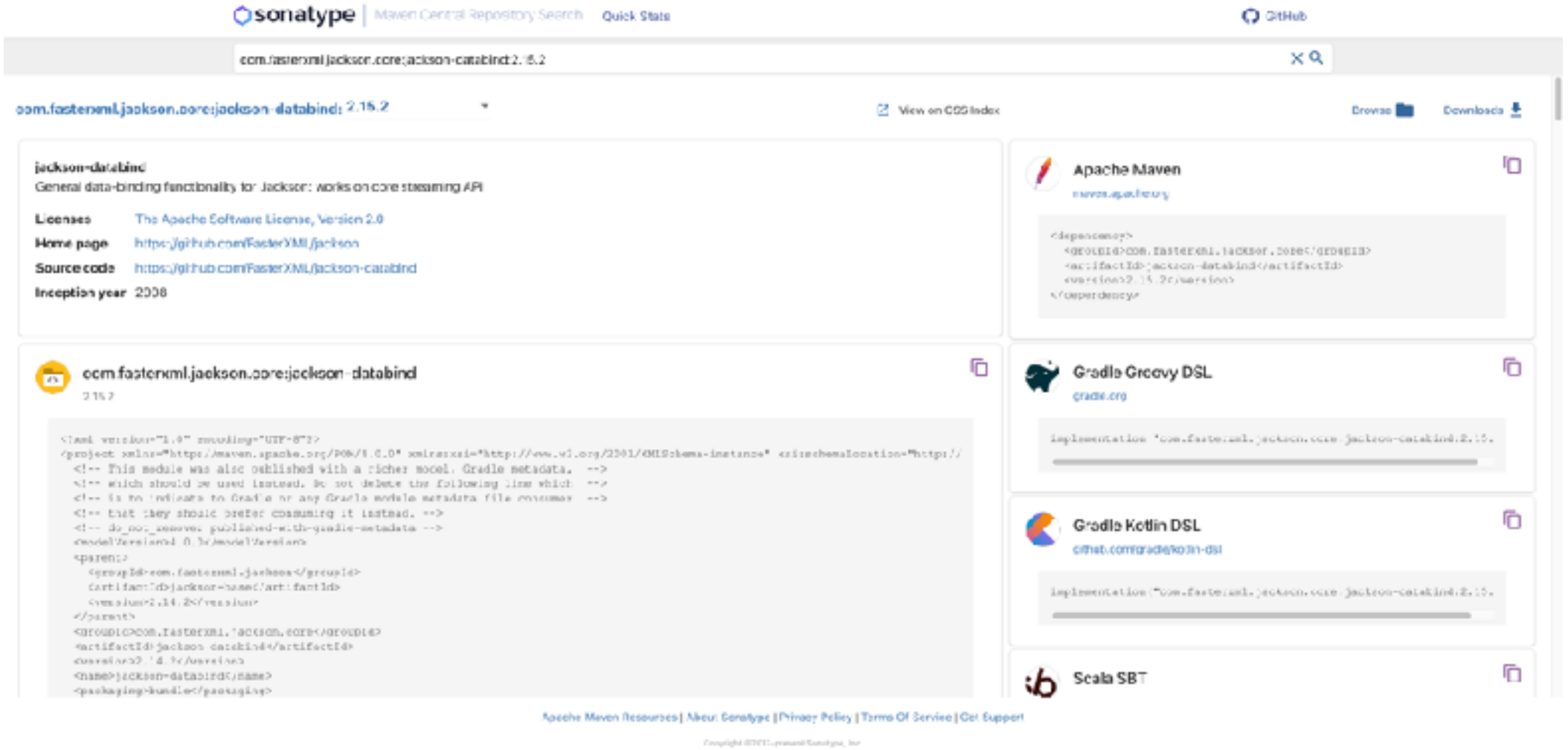


https://central.sonatype.com/

Dependency information

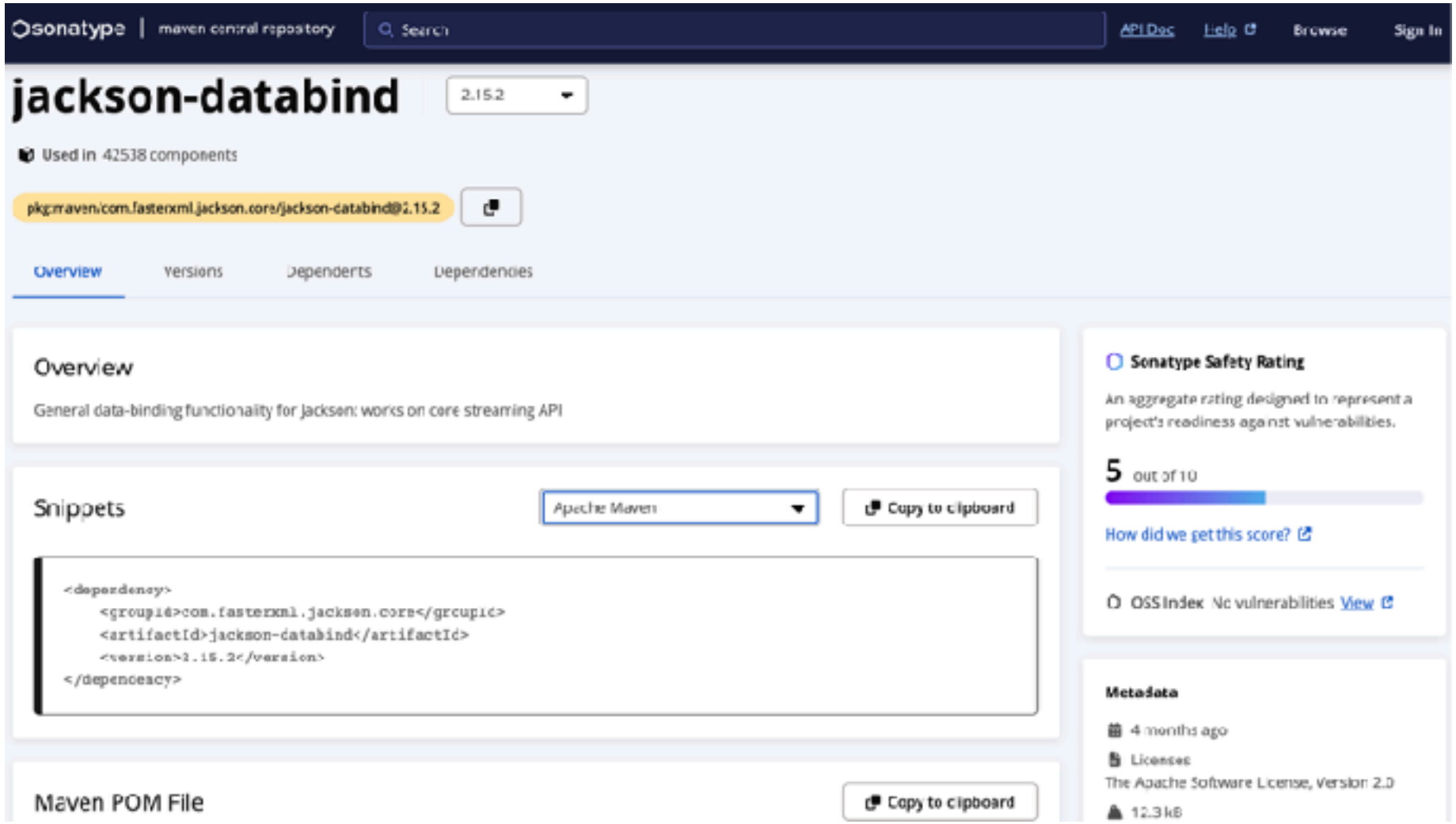
https://central.sonatype.com/

Dependency information



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

Dependency information



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

Maven Central Repository Search

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! 🎉

Maven Central Repository Search

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

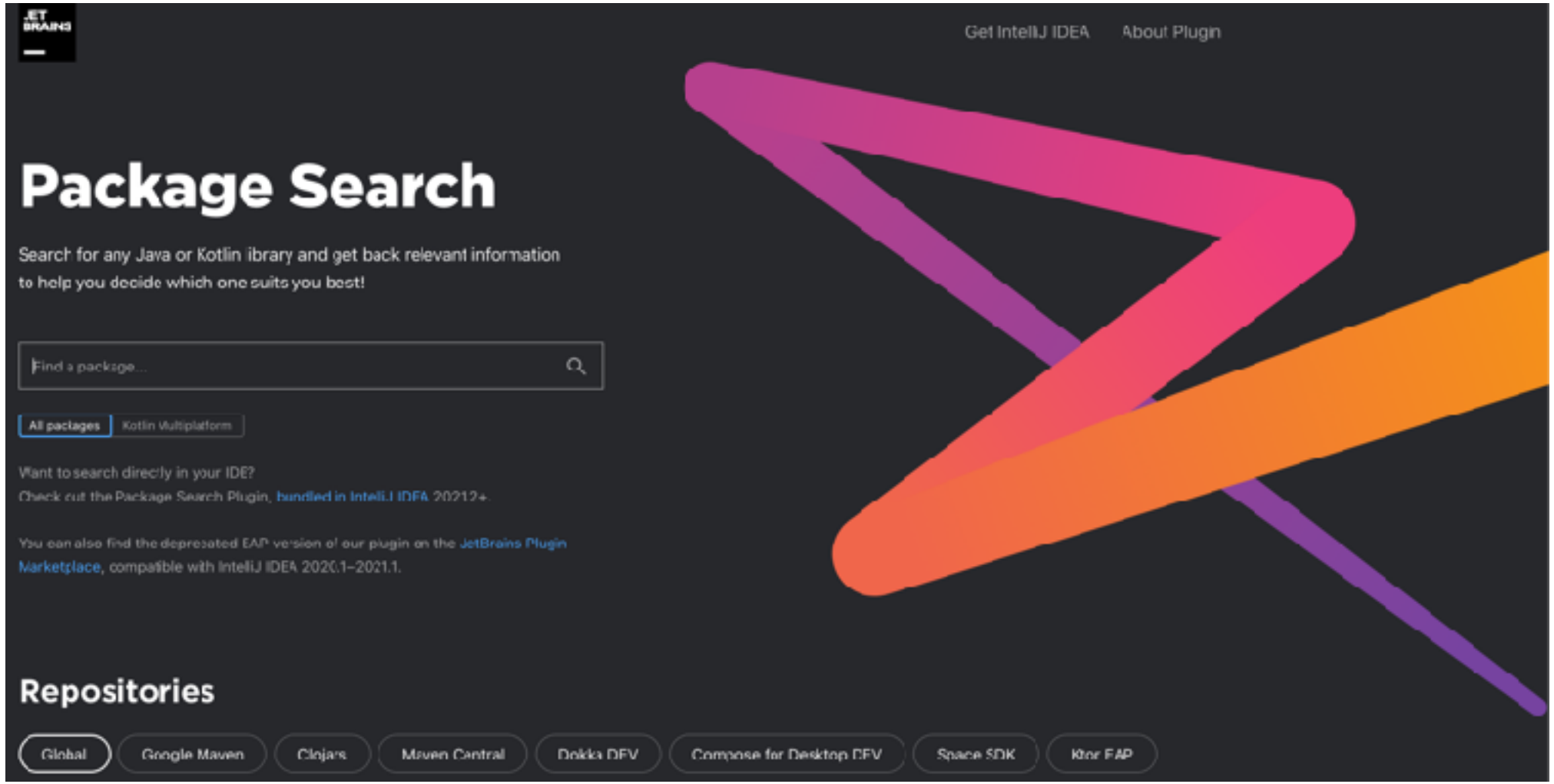
Report advisory or correction

Vulnerabilities

2 HIGH

@MaritvanDijk77

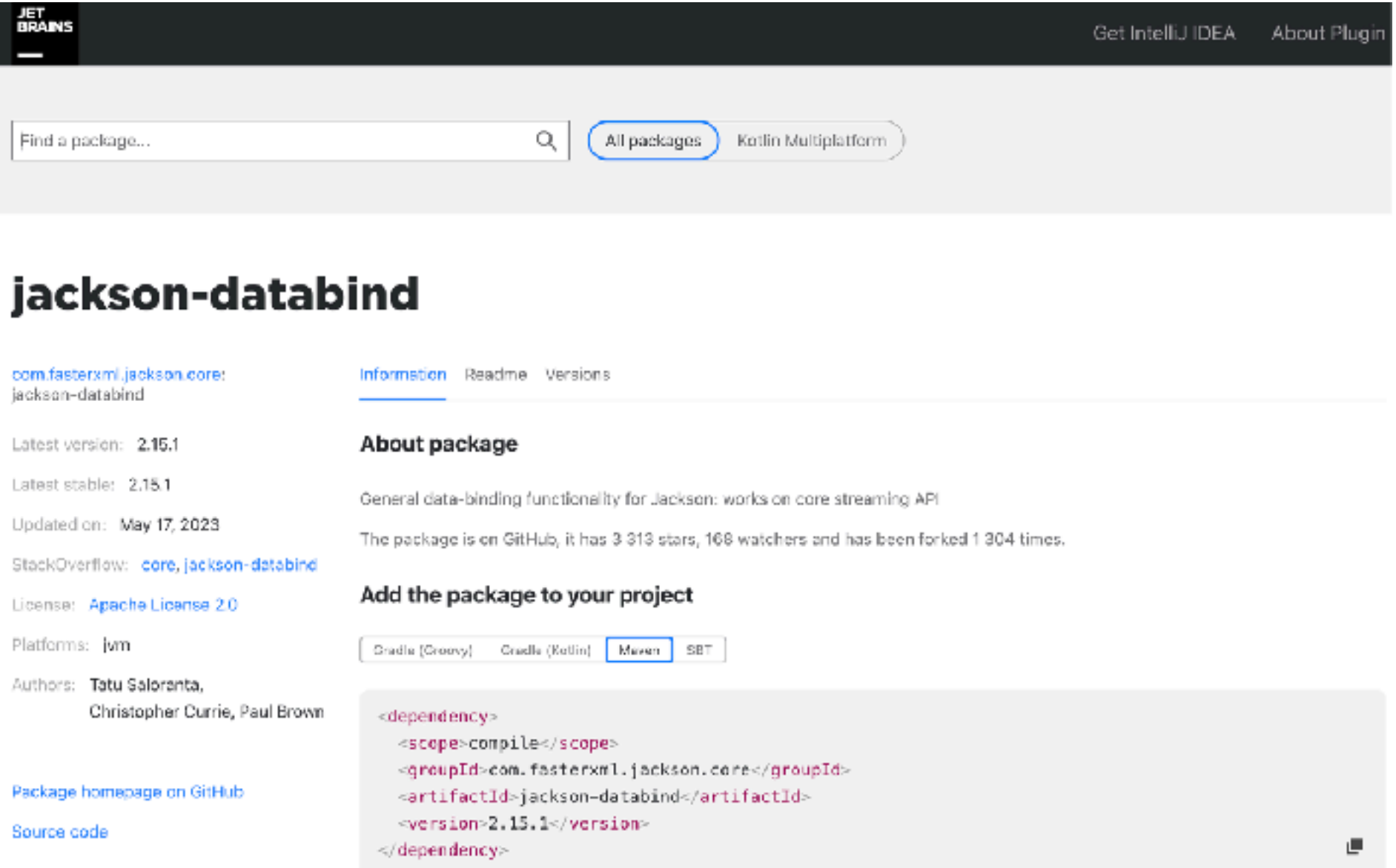
Dependency information



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

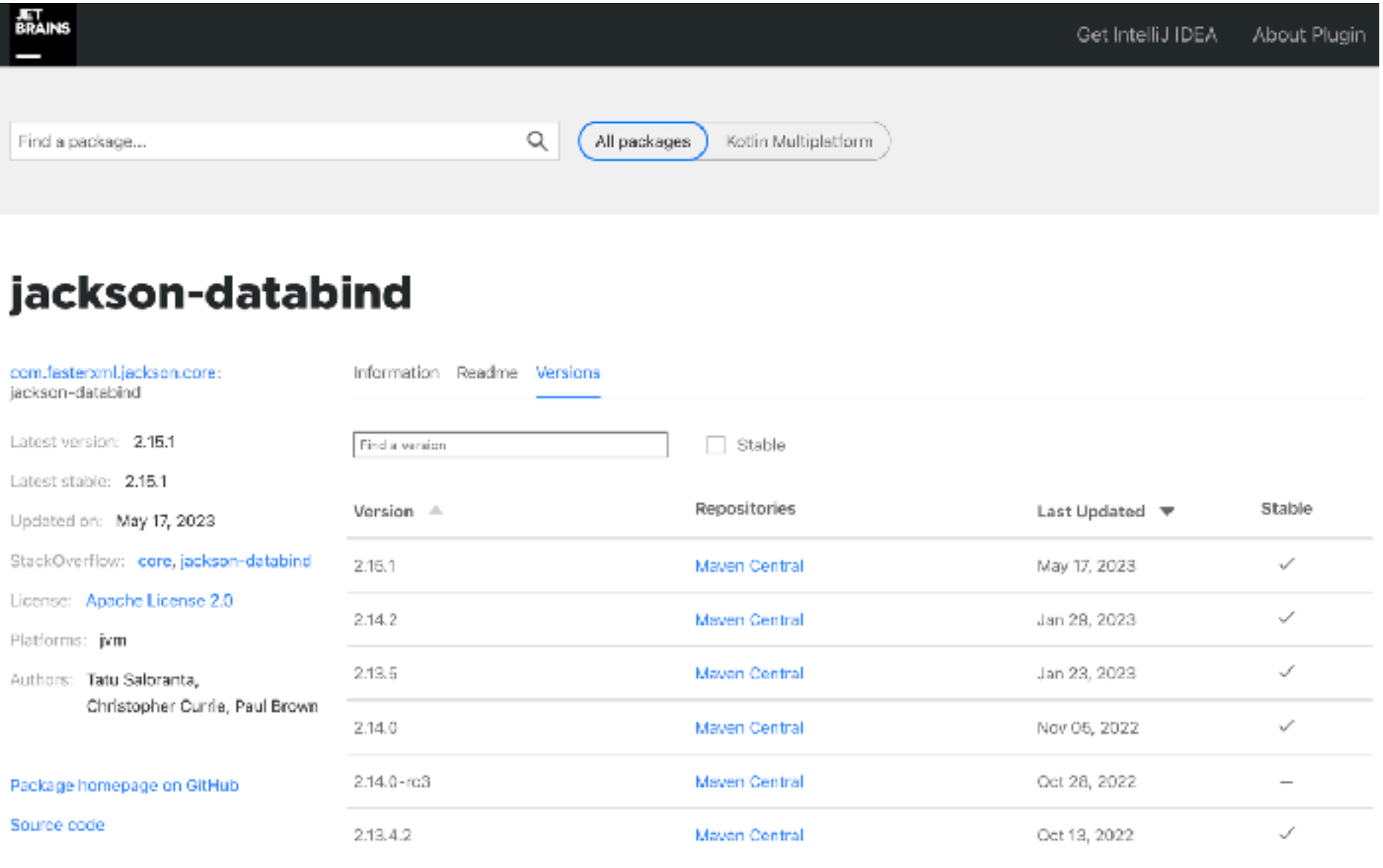
@MaritvanDijk77

Dependency information



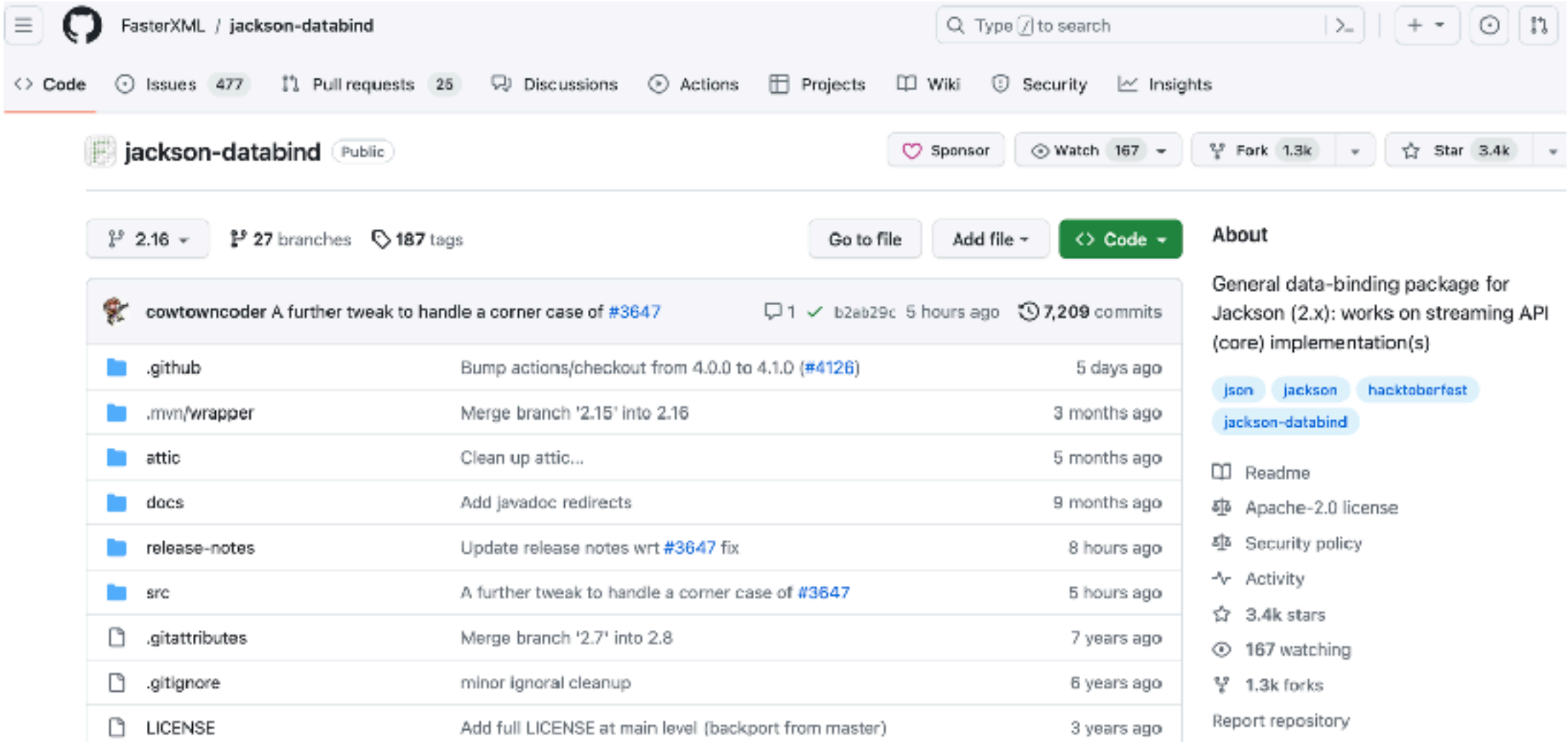
@MaritvanDijk77

Dependency information



@MaritvanDijk77

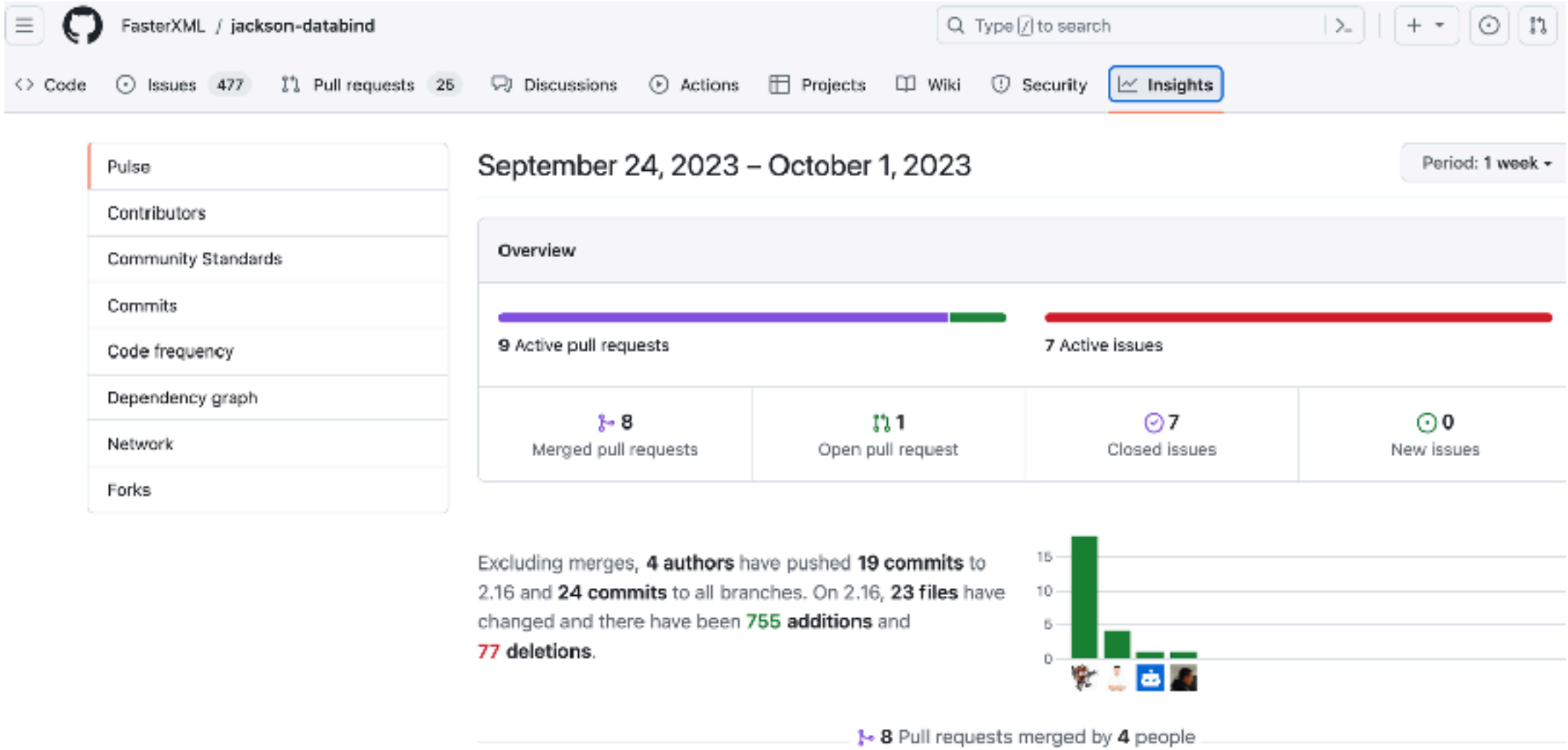
Dependency information



https://github.com/

@MaritvanDijk77

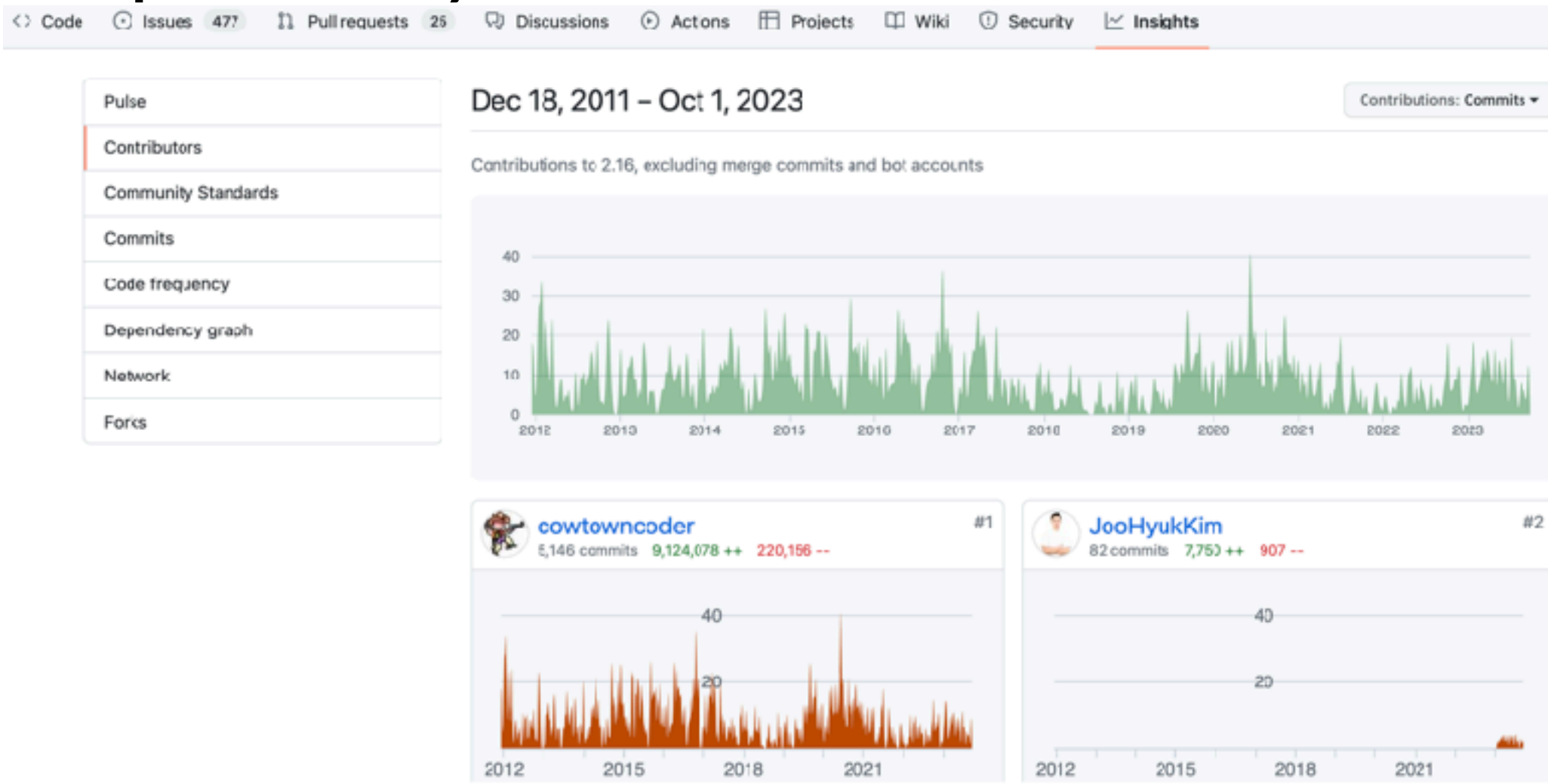
Dependency information



https://github.com/

@MaritvanDijk77

Dependency information



https://github.com/

@MaritvanDijk77

https://maritvandijk.com/presentations/collaborating-on-open-source-software/ @MaritvanDijk77

Maintain dependencies

@MaritvanDijk77

Maven

- Overview of dependencies: `mvn dependency:tree`

```
marit.van.dijk@NVC60260 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
```

@MaritvanDijk77

Maven

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

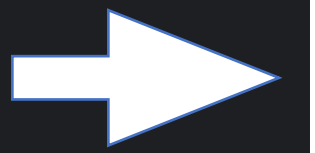
```
marit.van.dijk@NVC00260 FitnessTracker % mvn versions:display-dependency-updates
[INFO] Scanning for projects...
[INFO]
[INFO] ------------------< com.maritvandijk:FitnessTracker >-------------------
[INFO] Building FitnessTracker 1.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
[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] ------------------------------------------------------------------------
```

@MaritvanDijk77

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 -> 8.0.0.Final
[INFO]   org.springframework:spring-oxm ................ 4.3.5.RELEASE -> 6.0.8
[INFO]   org.springframework:spring-webmvc ............. 4.3.5.RELEASE -> 6.0.8
[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'
}
```

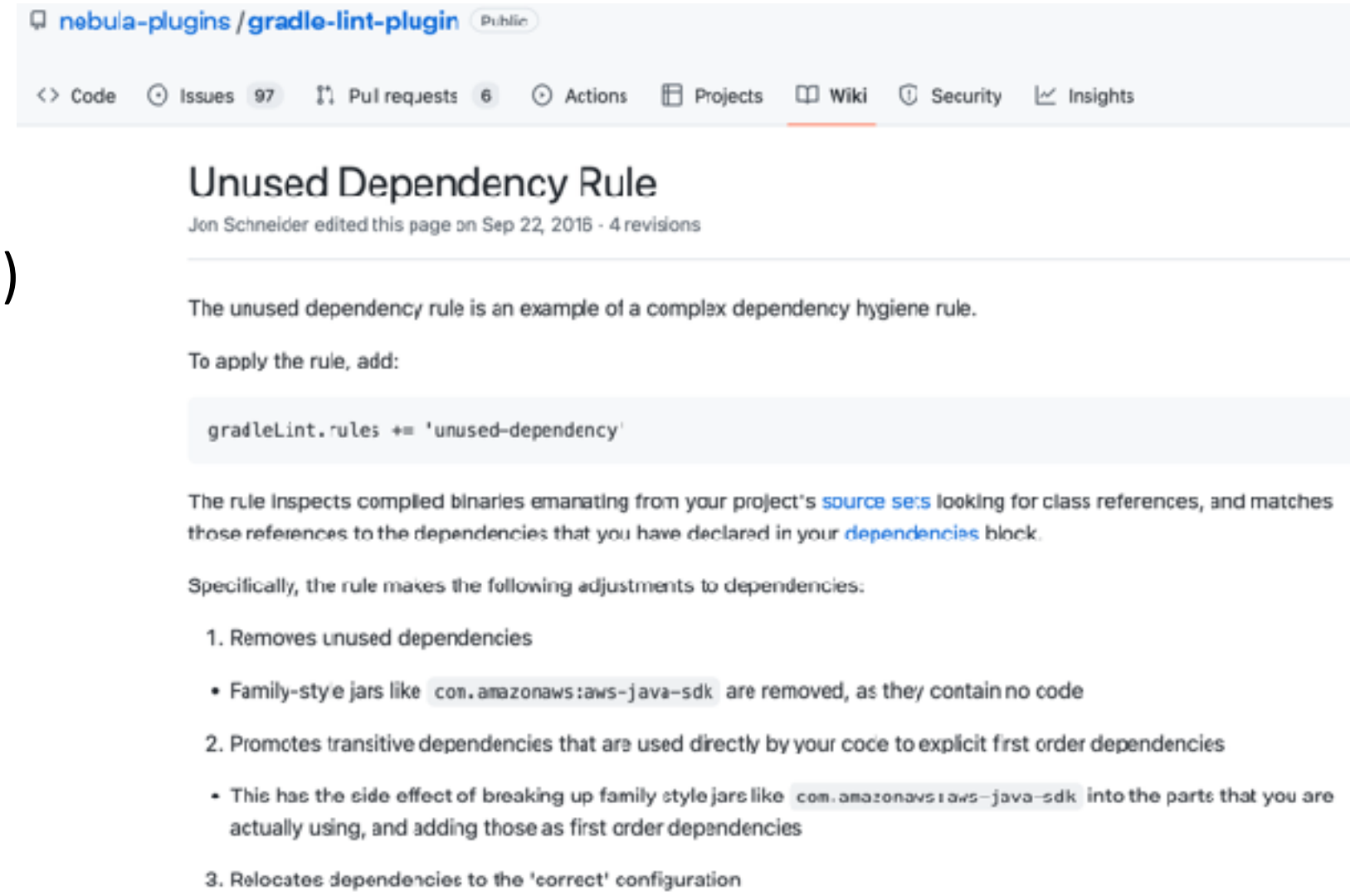
- Run `./gradlew dependencyUpdates`

```
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
```

https://github.com/ben-manes/gradle-versions-plugin

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`

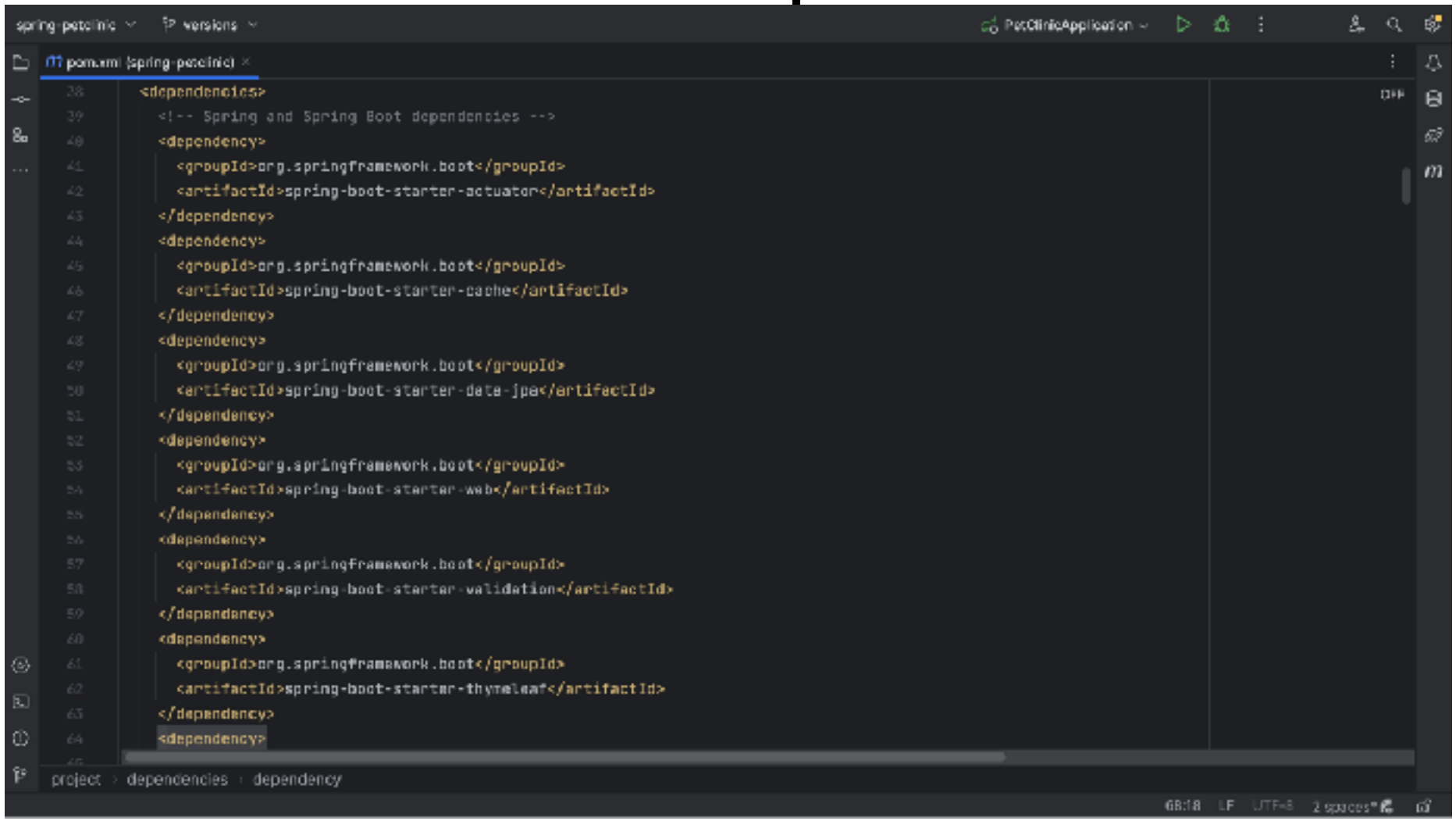
```
buildscript { repositories { mavenCentral() } }
plugins {
    id 'nebula.lint' version '18.1.0'
}
gradleLint.rules = ['all-dependency']
```

```
> 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
```

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

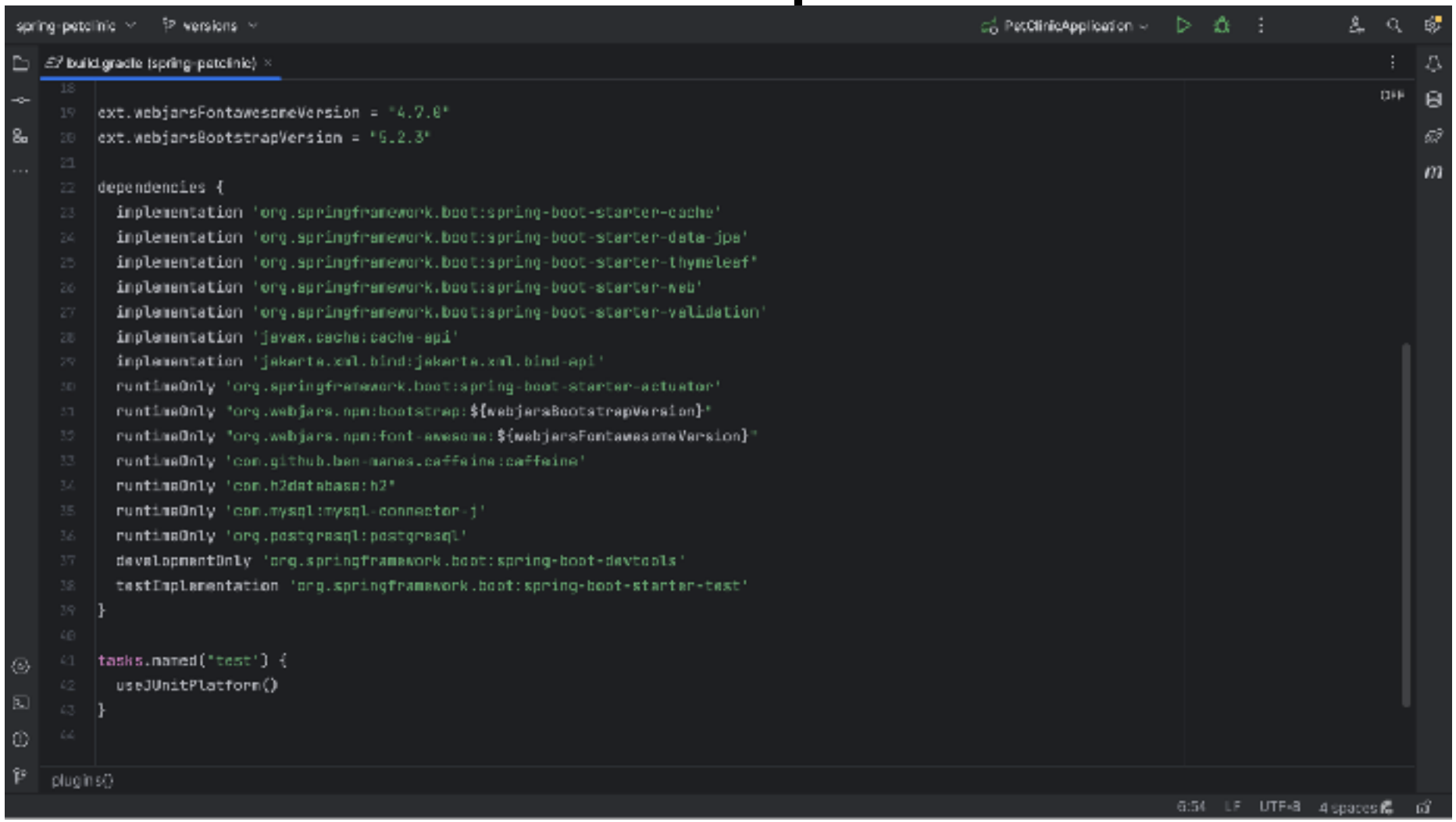
@MaritvanDijk77

IntelliJ IDEA: View Dependencies



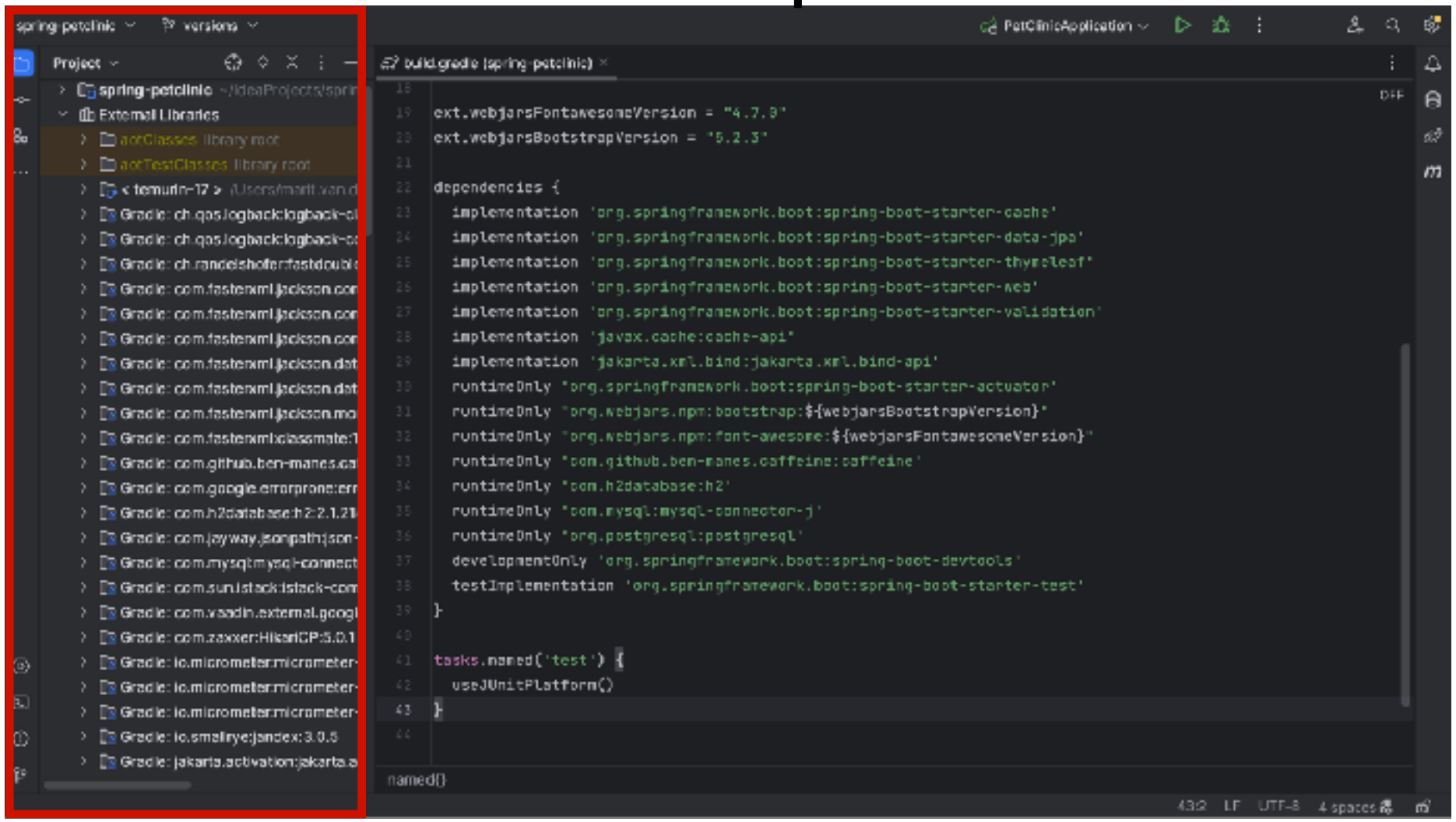
@MaritvanDijk77

IntelliJ IDEA: View Dependencies



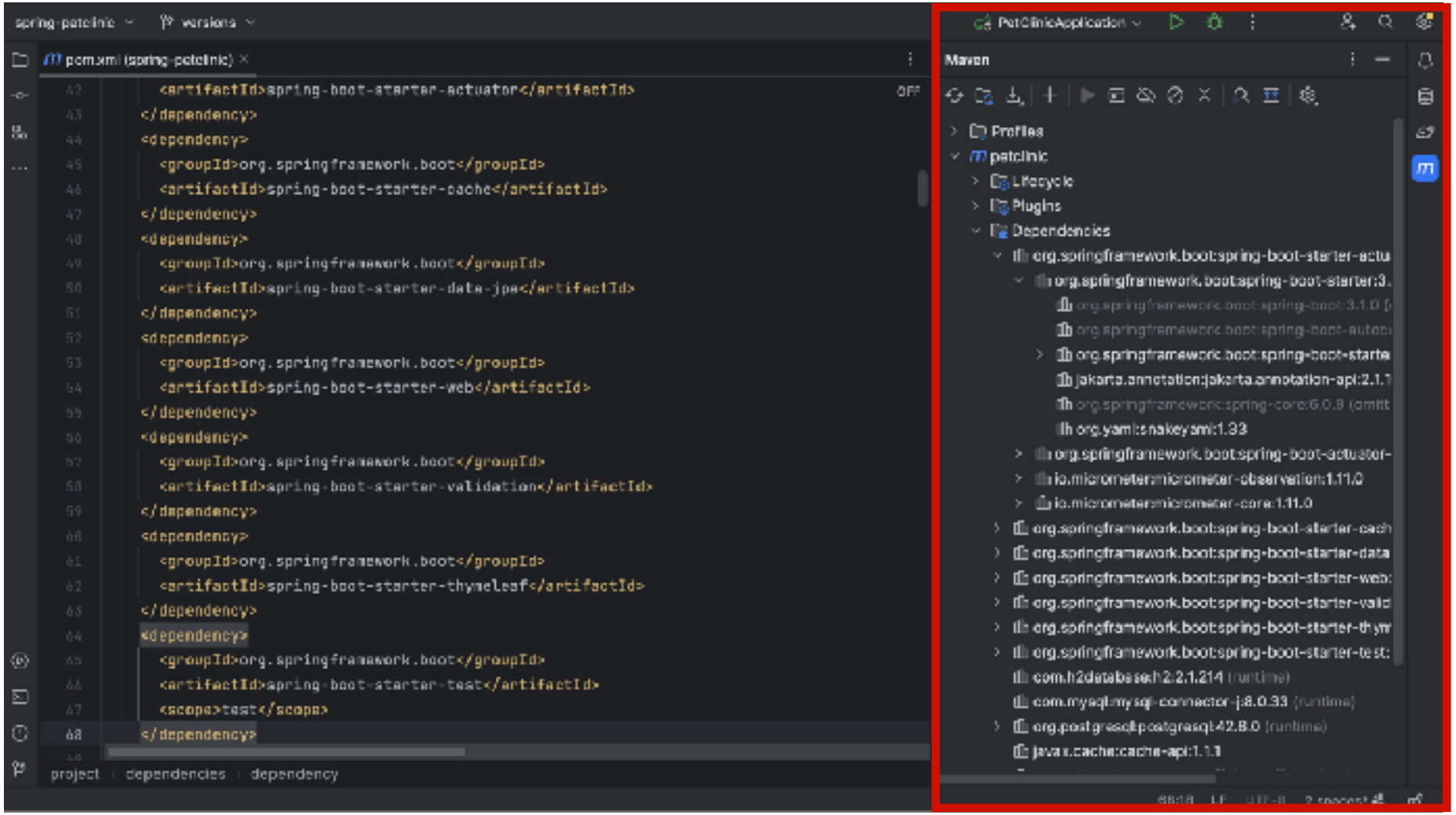
@MaritvanDijk77

IntelliJ IDEA: View Dependencies



@MaritvanDijk77

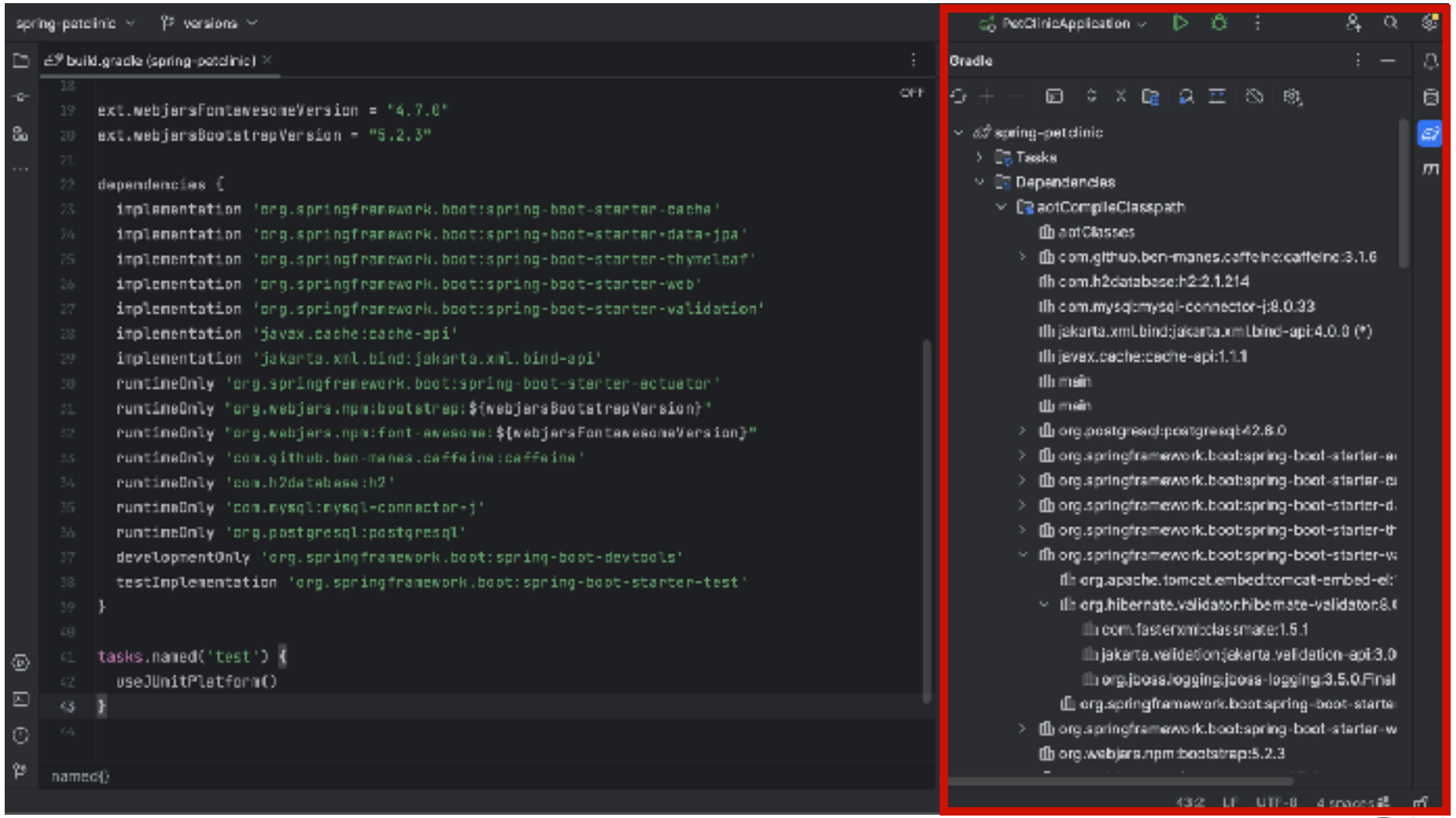
IntelliJ IDEA: View Dependencies



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

@MaritvanDijk77

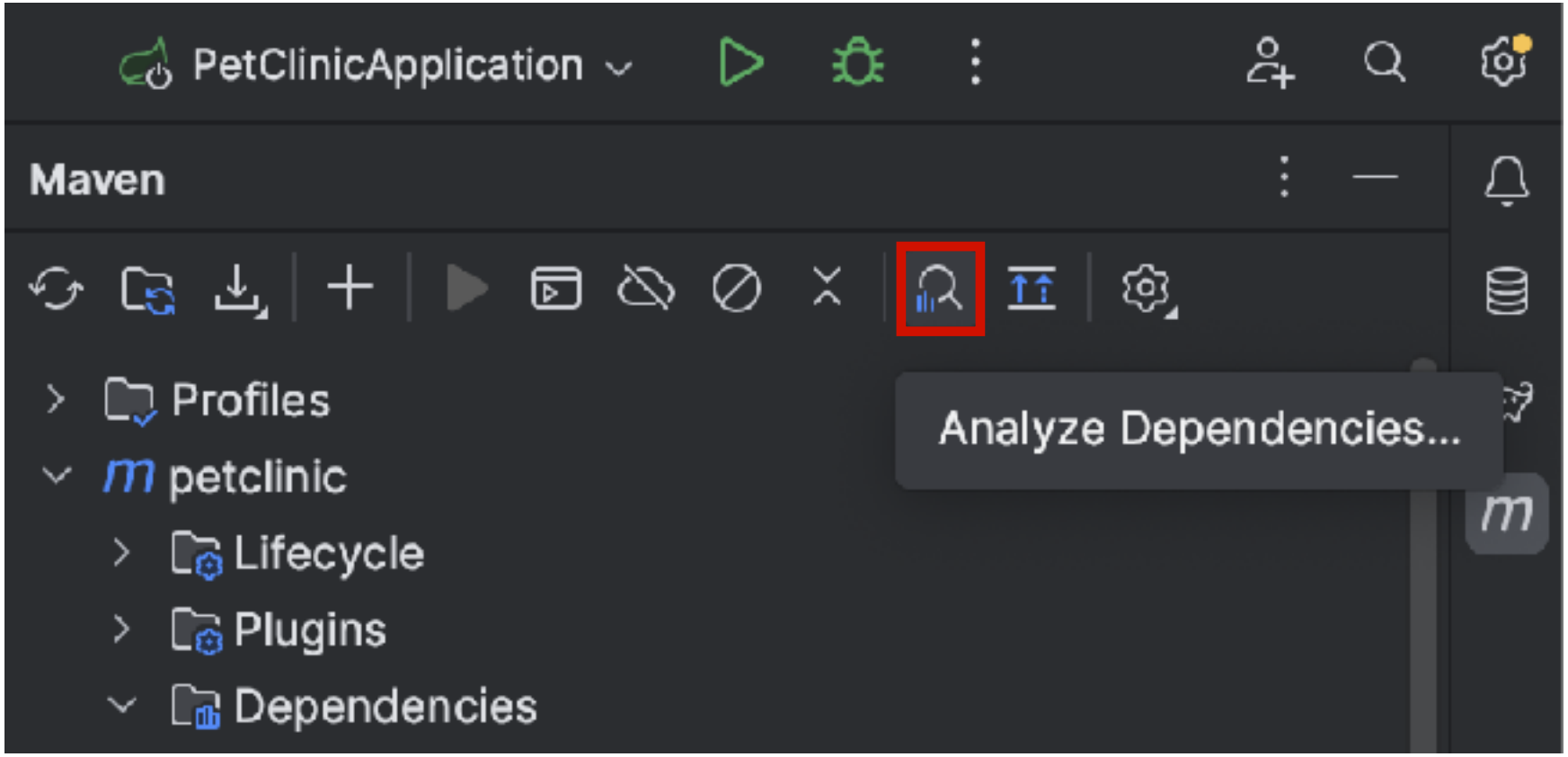
IntelliJ IDEA: View Dependencies



https://www.jetbrains.com/help/idea/jetgradle-tool-window.html

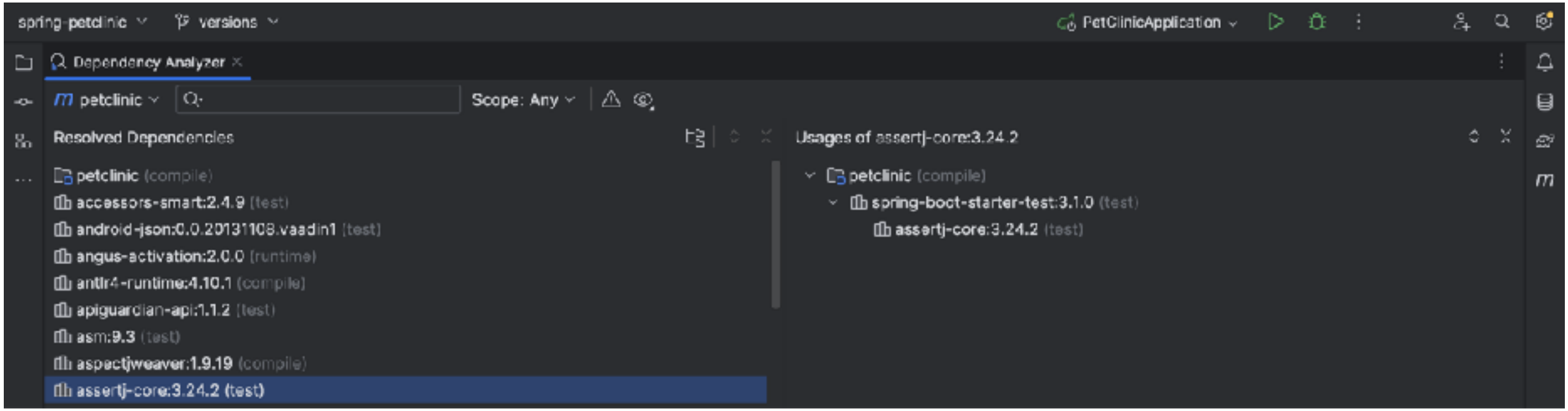
@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer



https://www.jetbrains.com/help/idea/work-with-maven-dependencies.html#dependency_analyzer

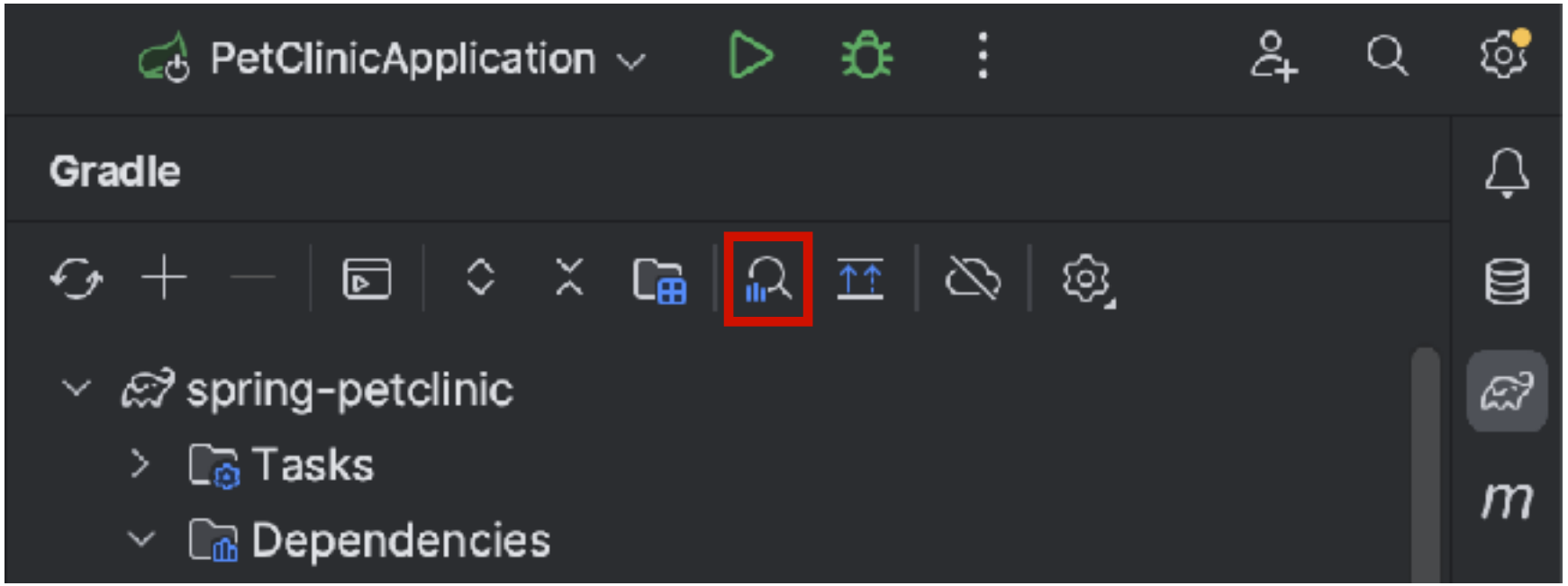
IntelliJ IDEA: Dependency Analyzer



https://www.jetbrains.com/help/idea/work-with-maven-dependencies.html#dependency_analyzer

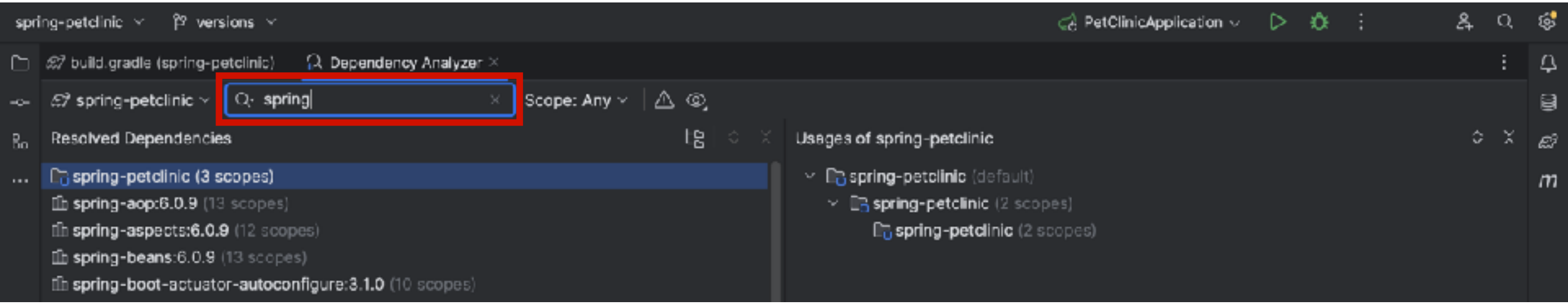
@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer



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

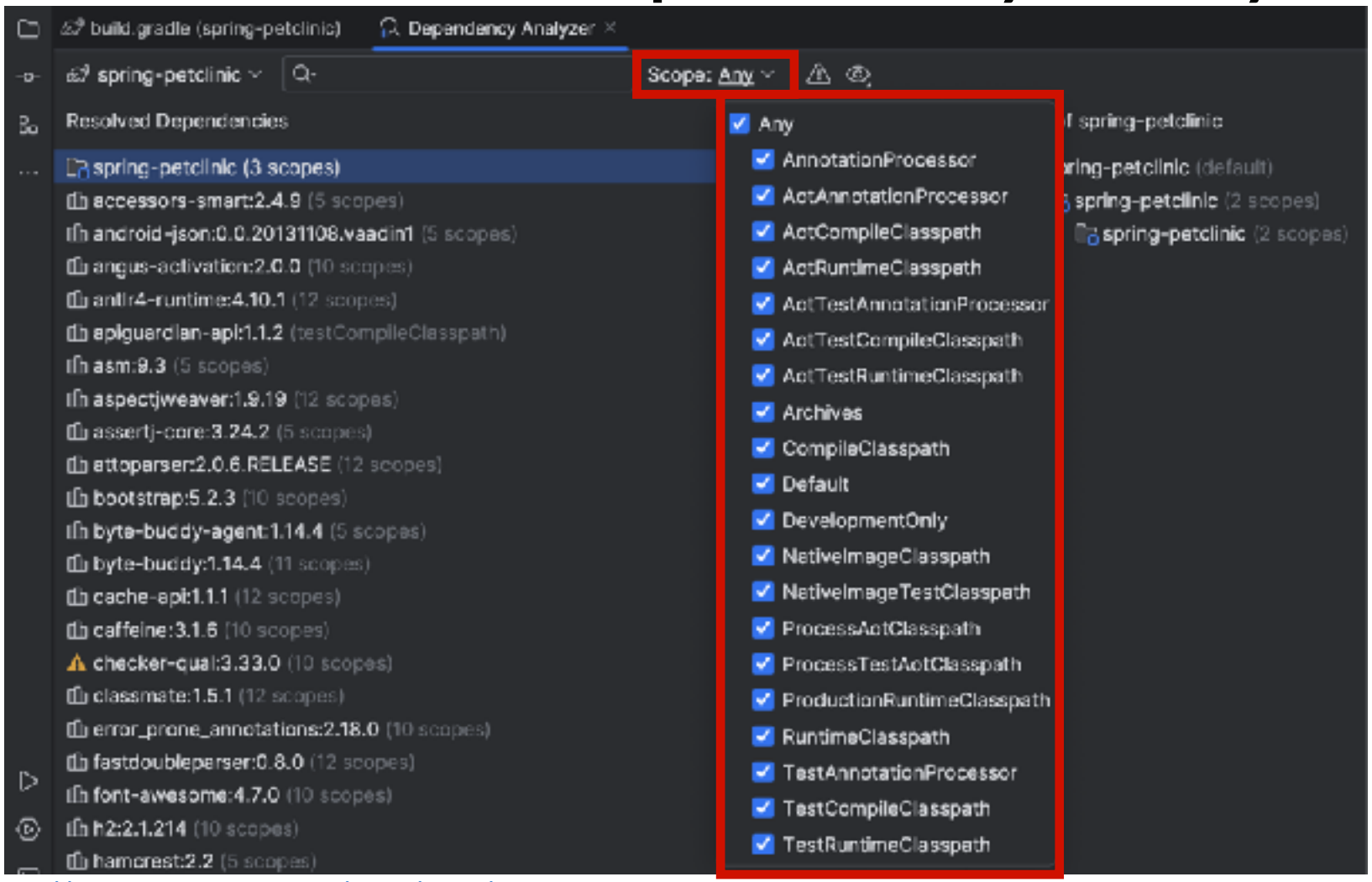
IntelliJ IDEA: Dependency Analyzer



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

@MaritvanDijk77

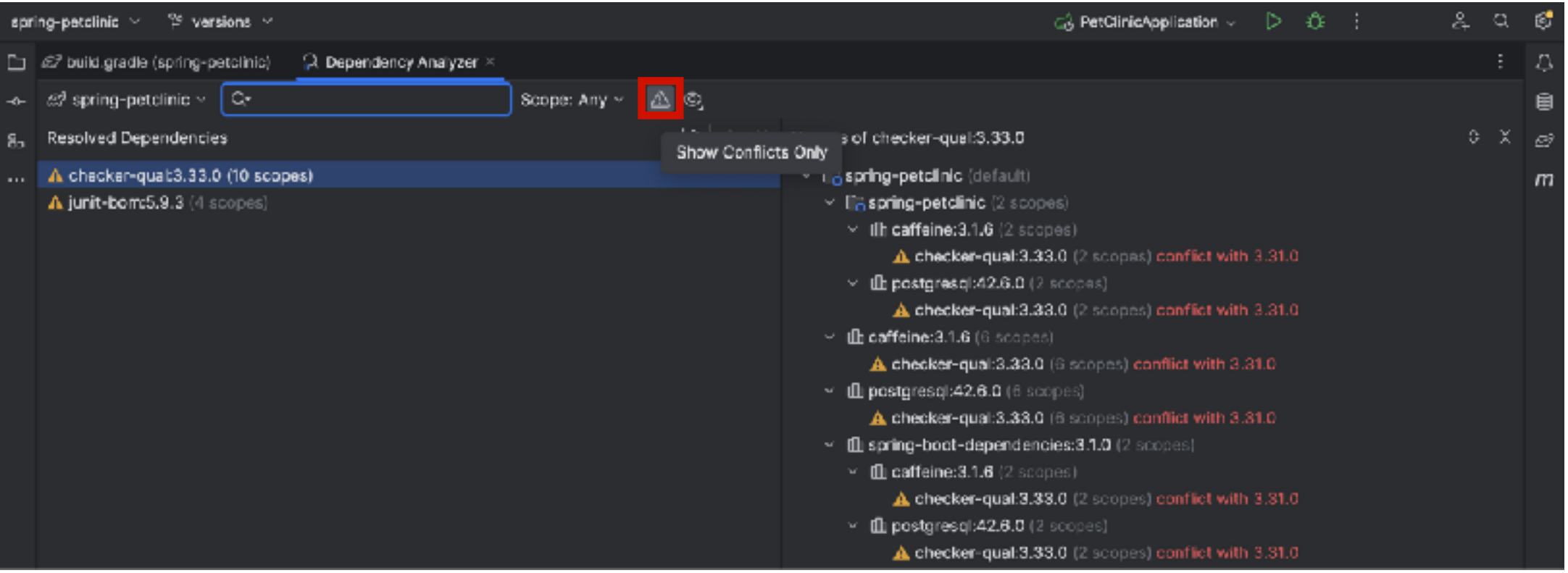
IntelliJ IDEA: Dependency Analyzer



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

@MaritvanDijk77

IntelliJ IDEA: Dependency Analyzer

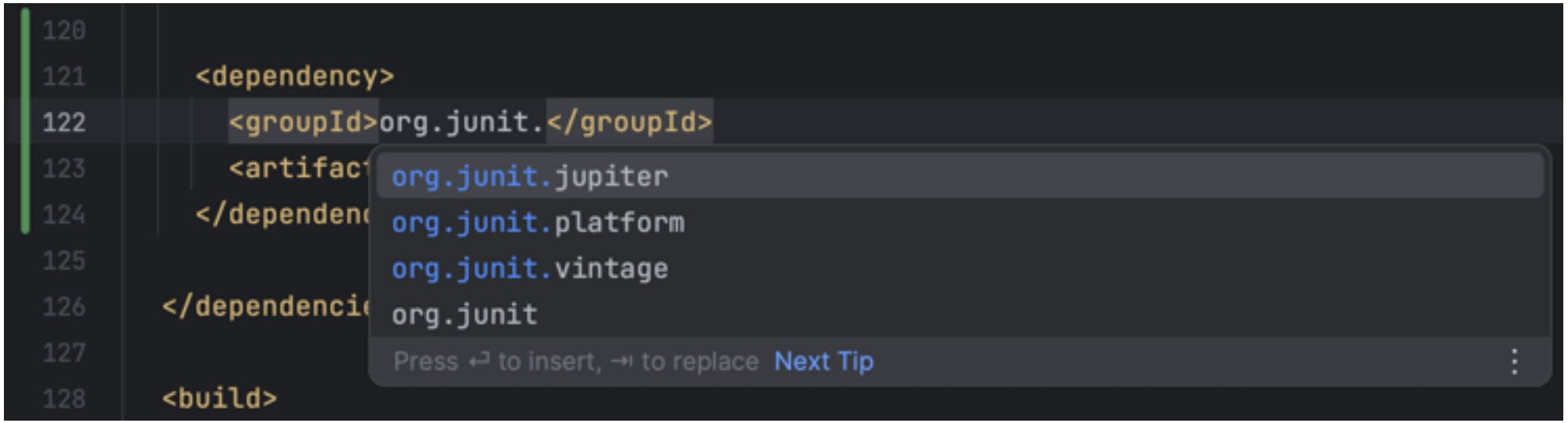


https://www.jetbrains.com/help/idea/work-with-gradle-dependency-diagram.html#dependency_analyzer

@MaritvanDijk77

IntelliJ IDEA

- Package Search: Add dependency



https://www.jetbrains.com/help/idea/package-search.html

IntelliJ IDEA

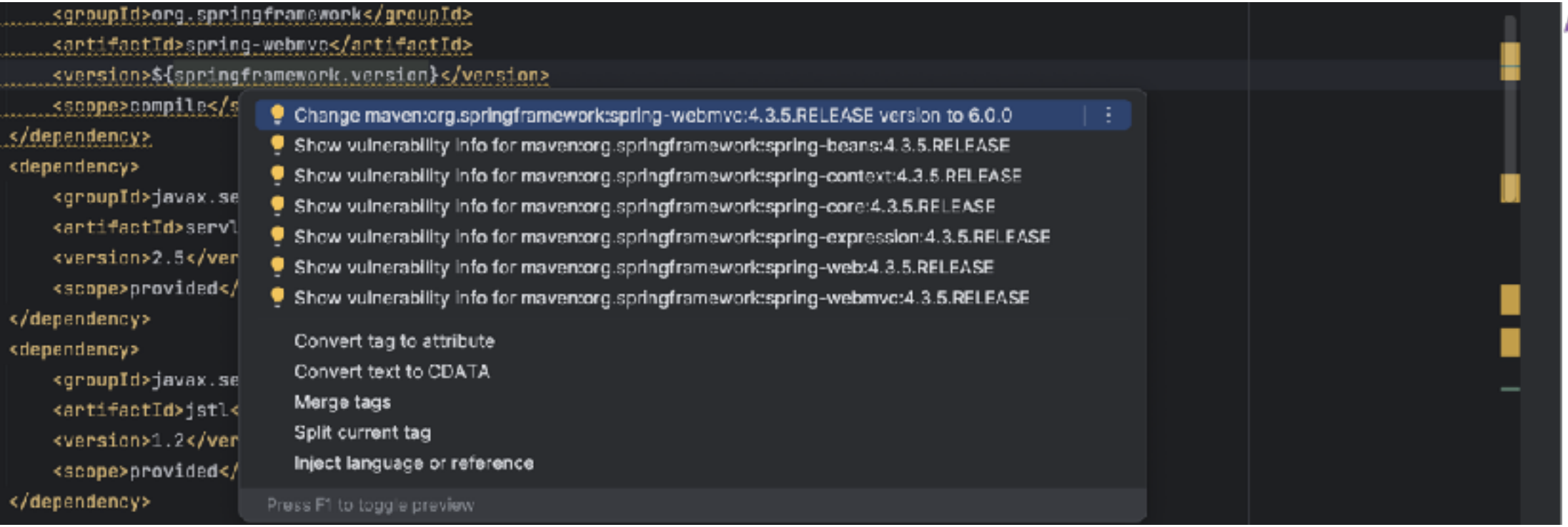
- Package Search: Add dependency

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

https://www.jetbrains.com/help/idea/package-search.html

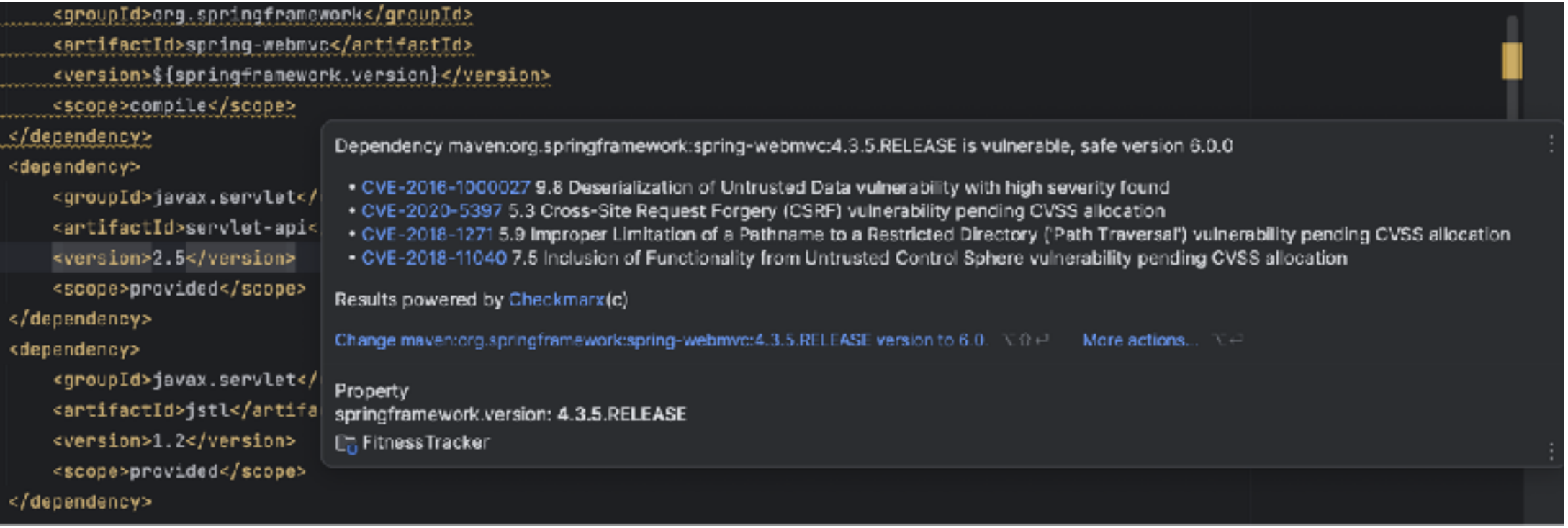
IntelliJ IDEA: Update dependencies

- Context Actions (⌥ ↵ or Alt+Enter)



IntelliJ IDEA: Update dependencies

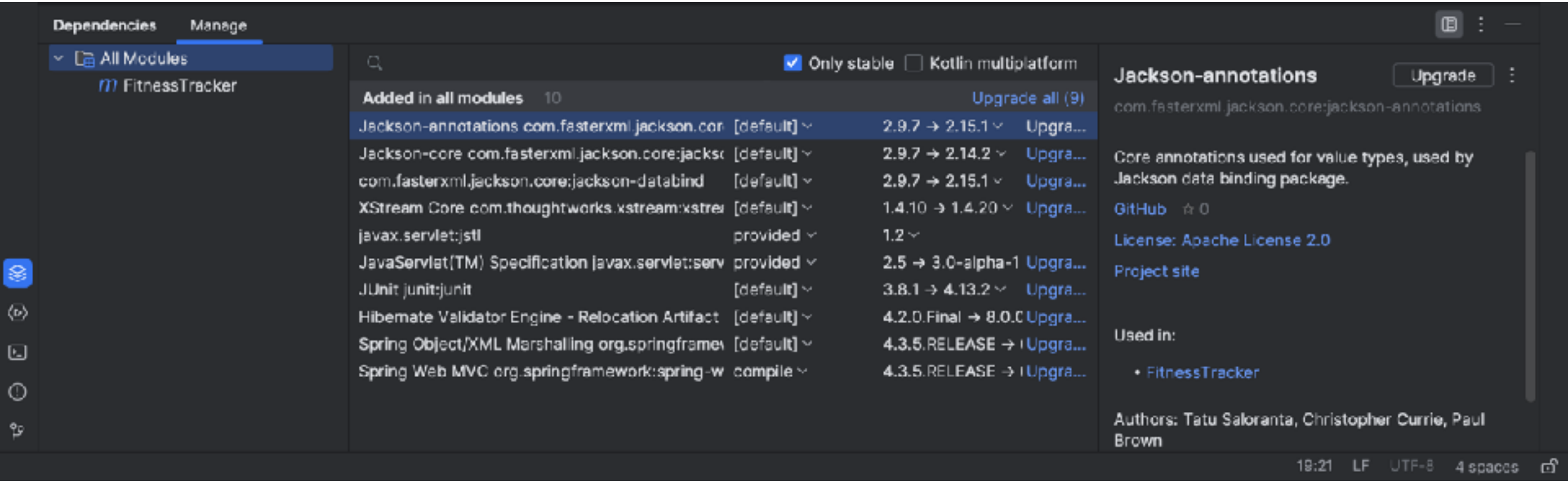
- Hover



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

IntelliJ IDEA

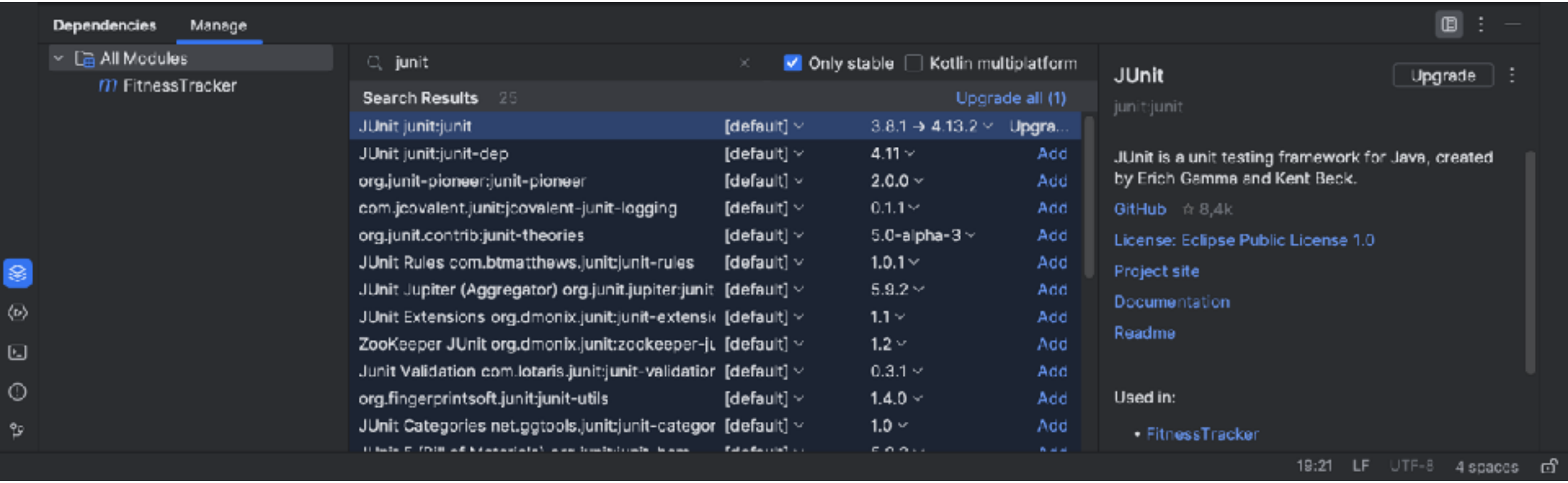
- Dependencies tool window



https://www.jetbrains.com/help/idea/package-search.html

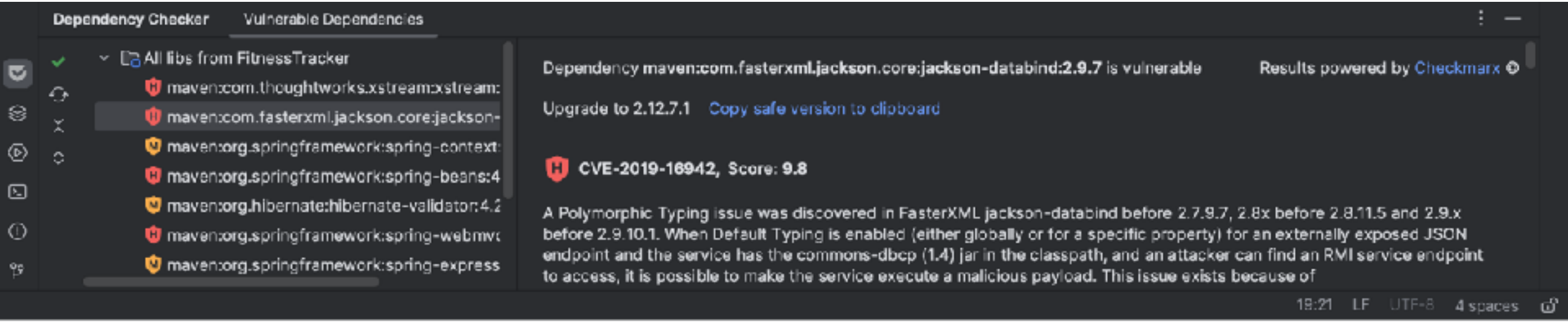
IntelliJ IDEA

- Dependencies tool window (search)



https://www.jetbrains.com/help/idea/package-search.html

IntelliJ IDEA



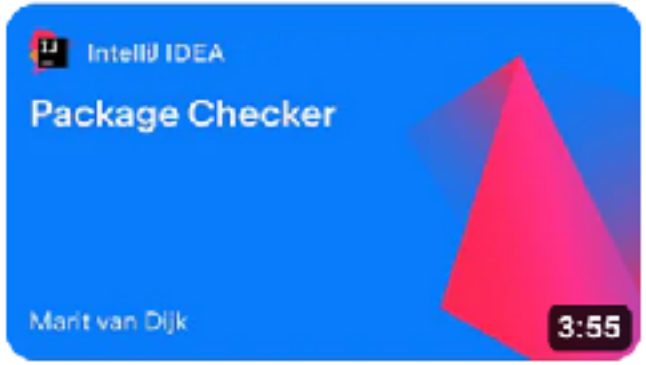
https://www.jetbrains.com/help/idea/package-analysis.html

@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

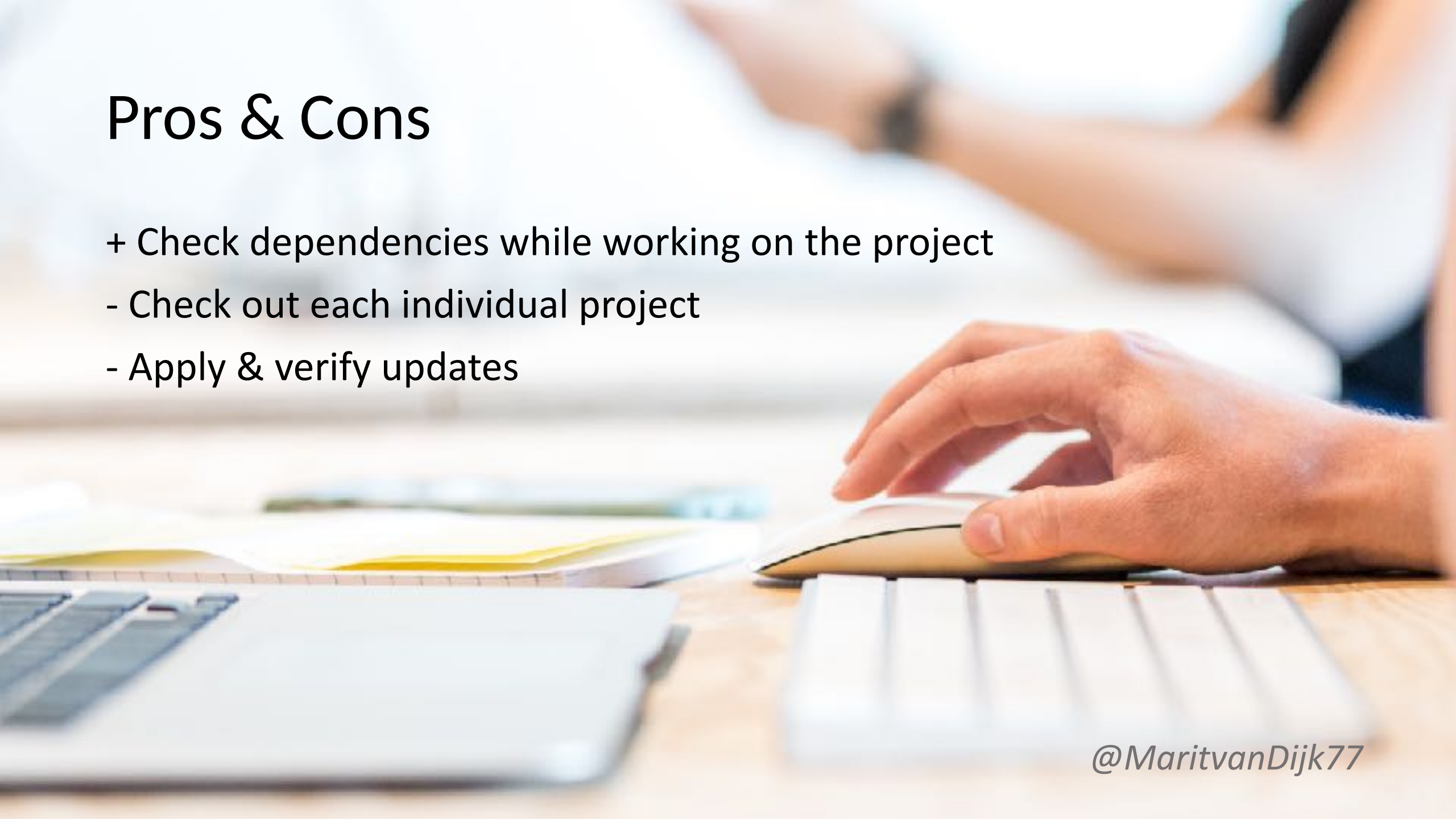
@MaritvanDijk77

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

Bots

- Dependabot
- Renovate
- Snyk Open Source

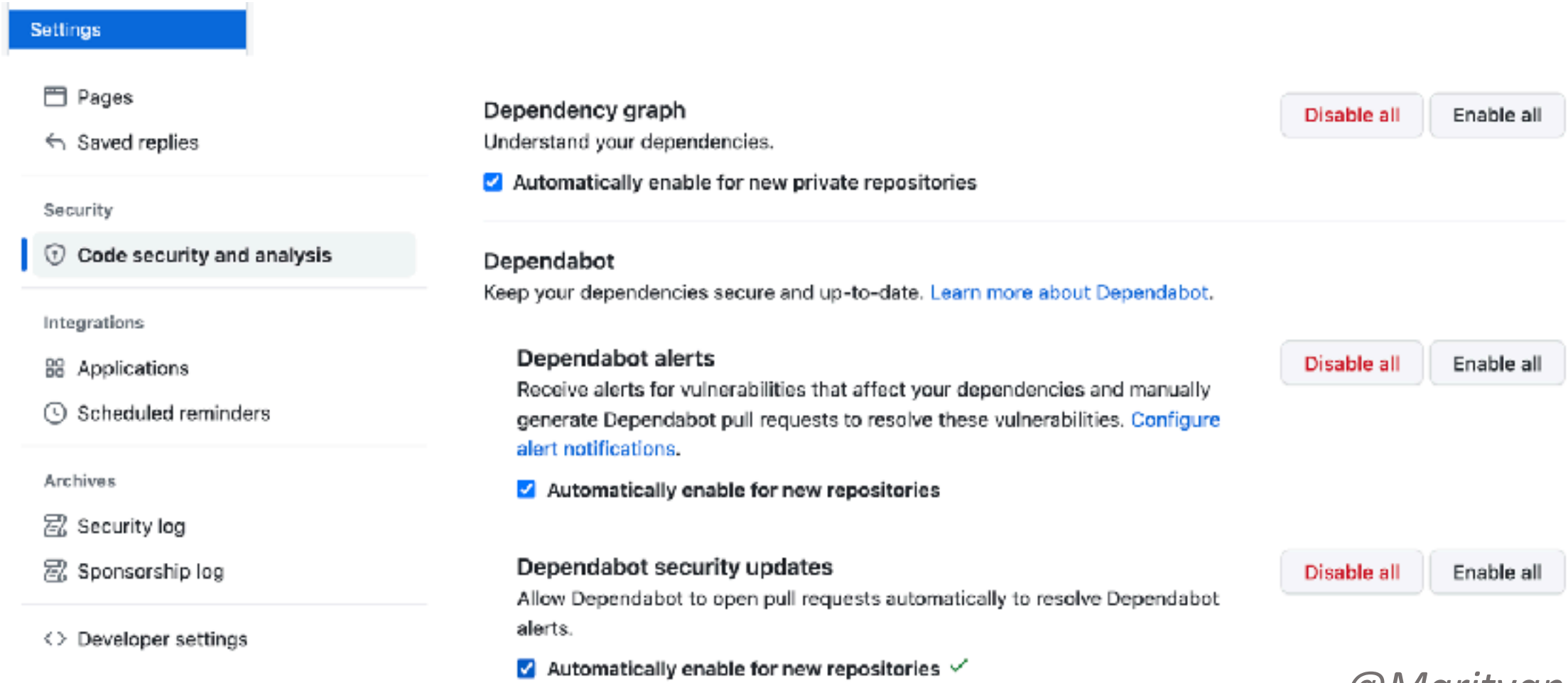
@MaritvanDijk77

Dependabot

- GitHub native

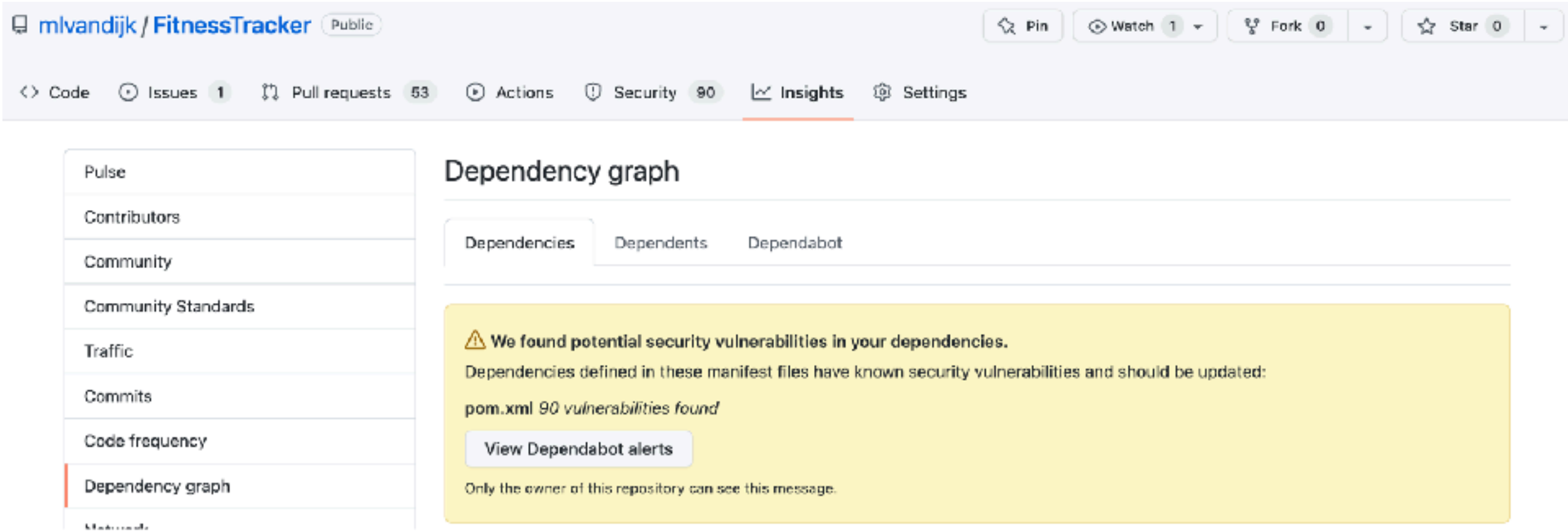
- Features:
  - Alerts
  - Security updates
  - Version updates

Dependabot enable



@MaritvanDijk77

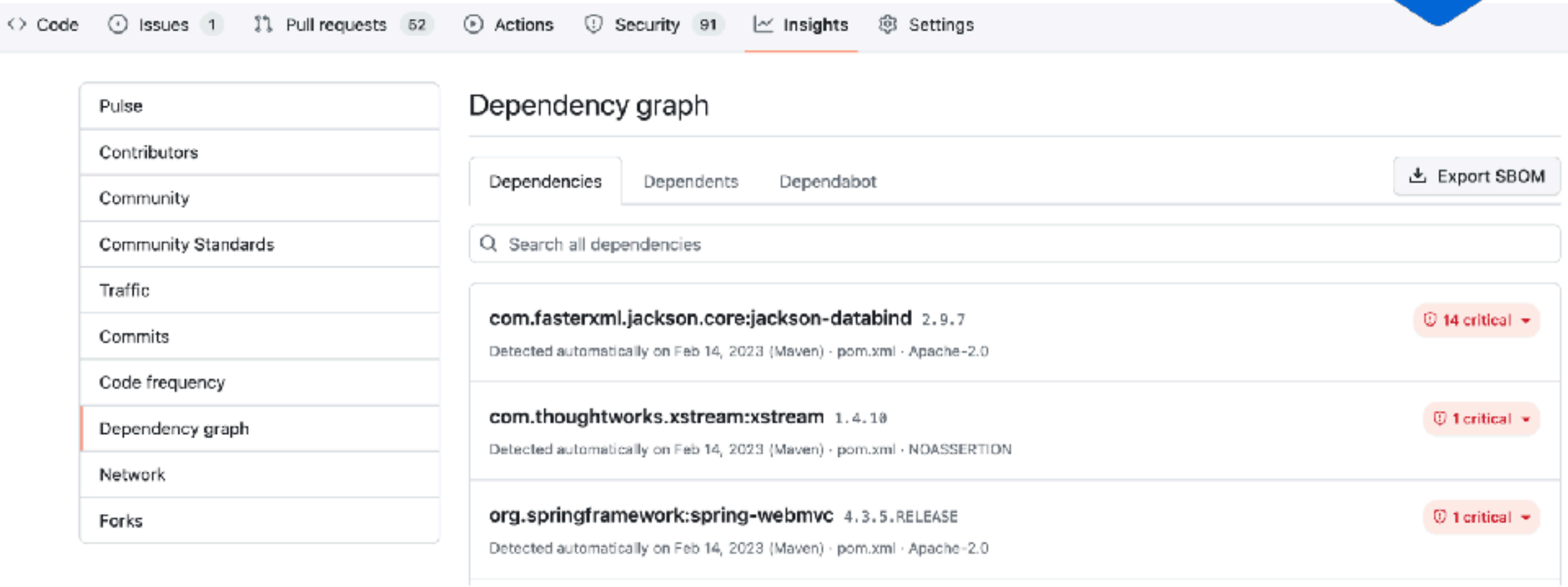
Dependabot alerts



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

@MaritvanDijk77

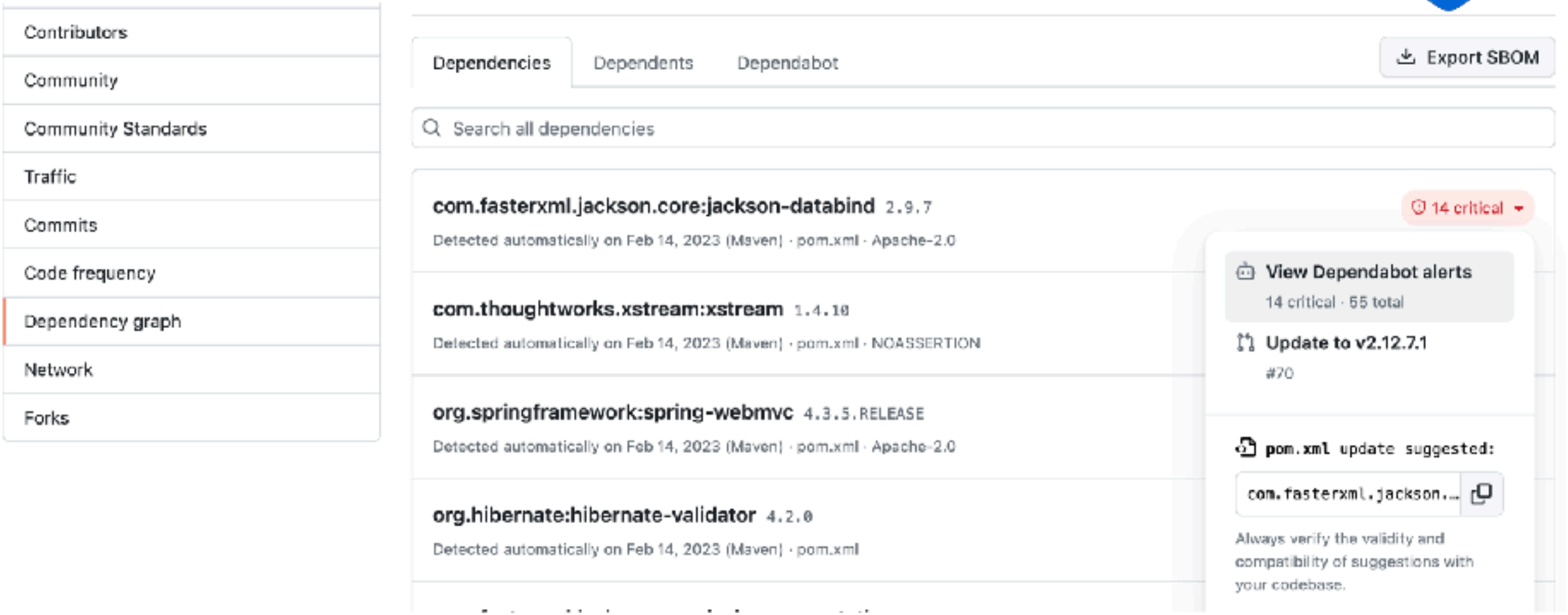
Dependabot alerts



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

@MaritvanDijk77

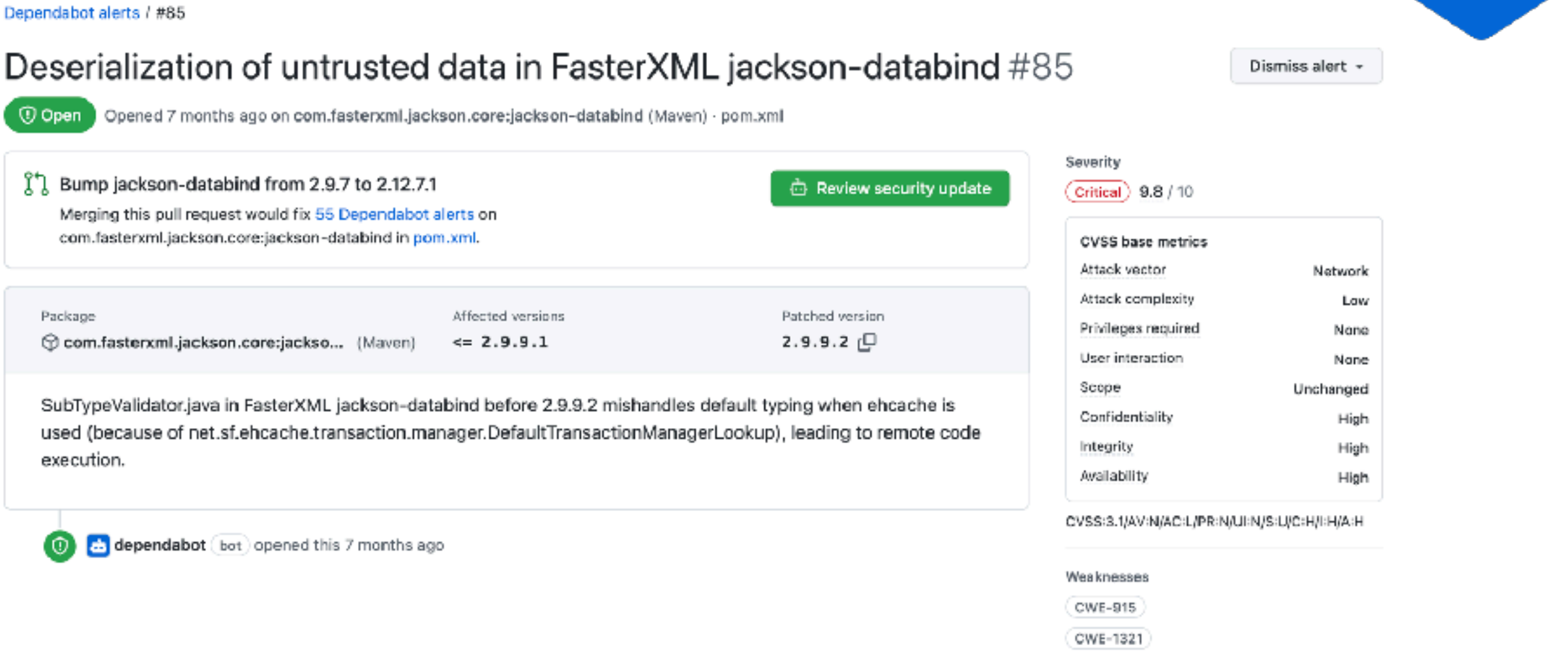
Dependabot alerts



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

@MaritvanDijk77

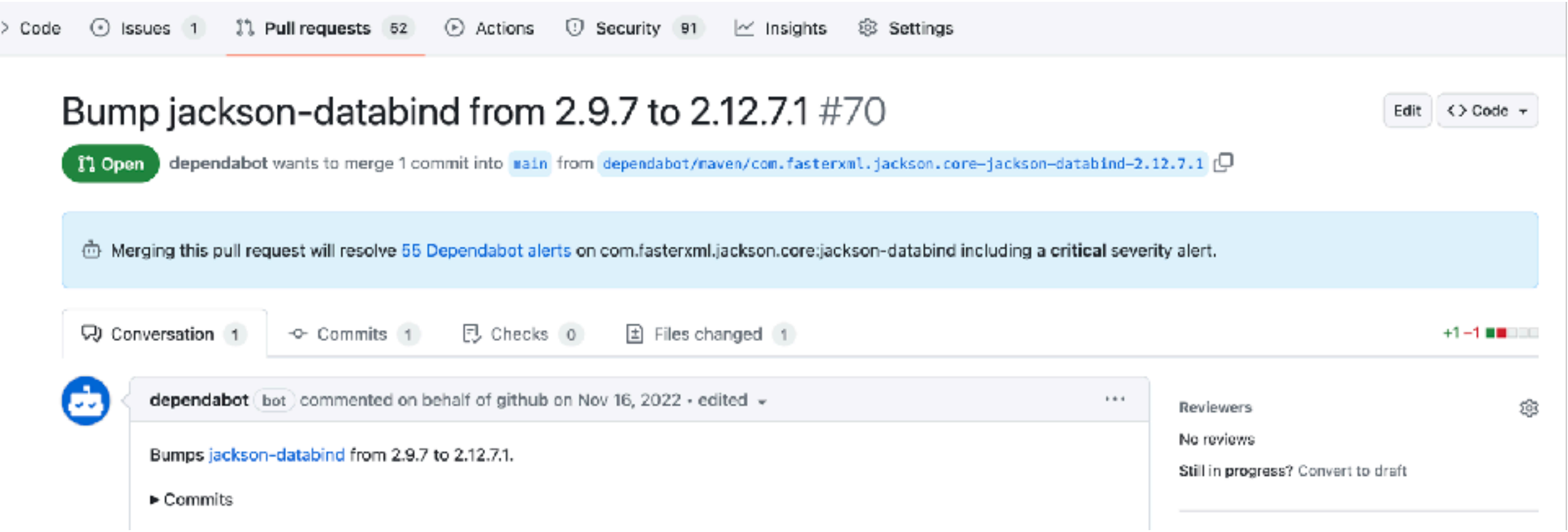
Dependabot security updates



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

@MaritvanDijk77

Dependabot security updates



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

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

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

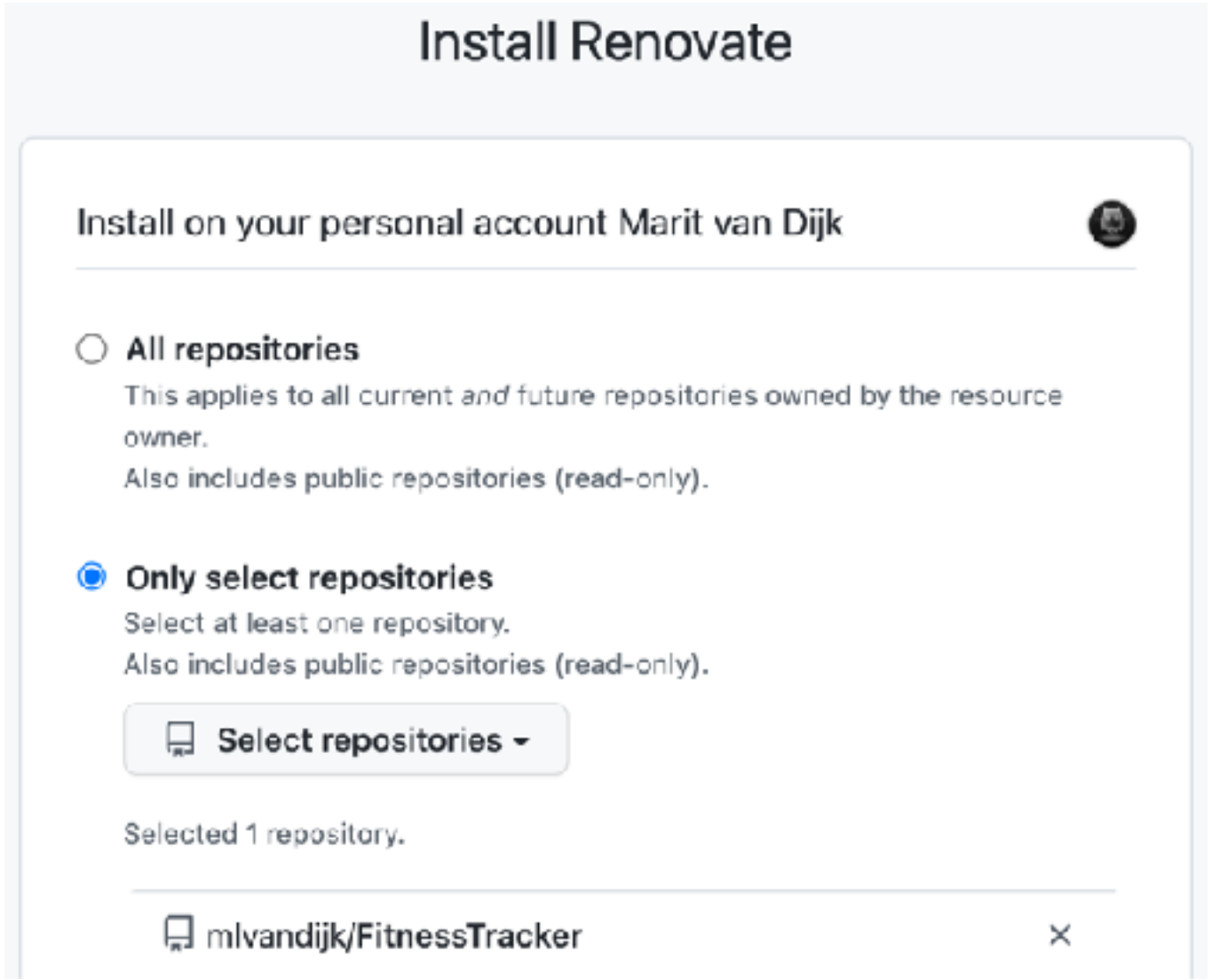
Renovate is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

Report abuse

https://github.com/apps/renovate

@MaritvanDijk77

Renovate enable - 3



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 + }
```

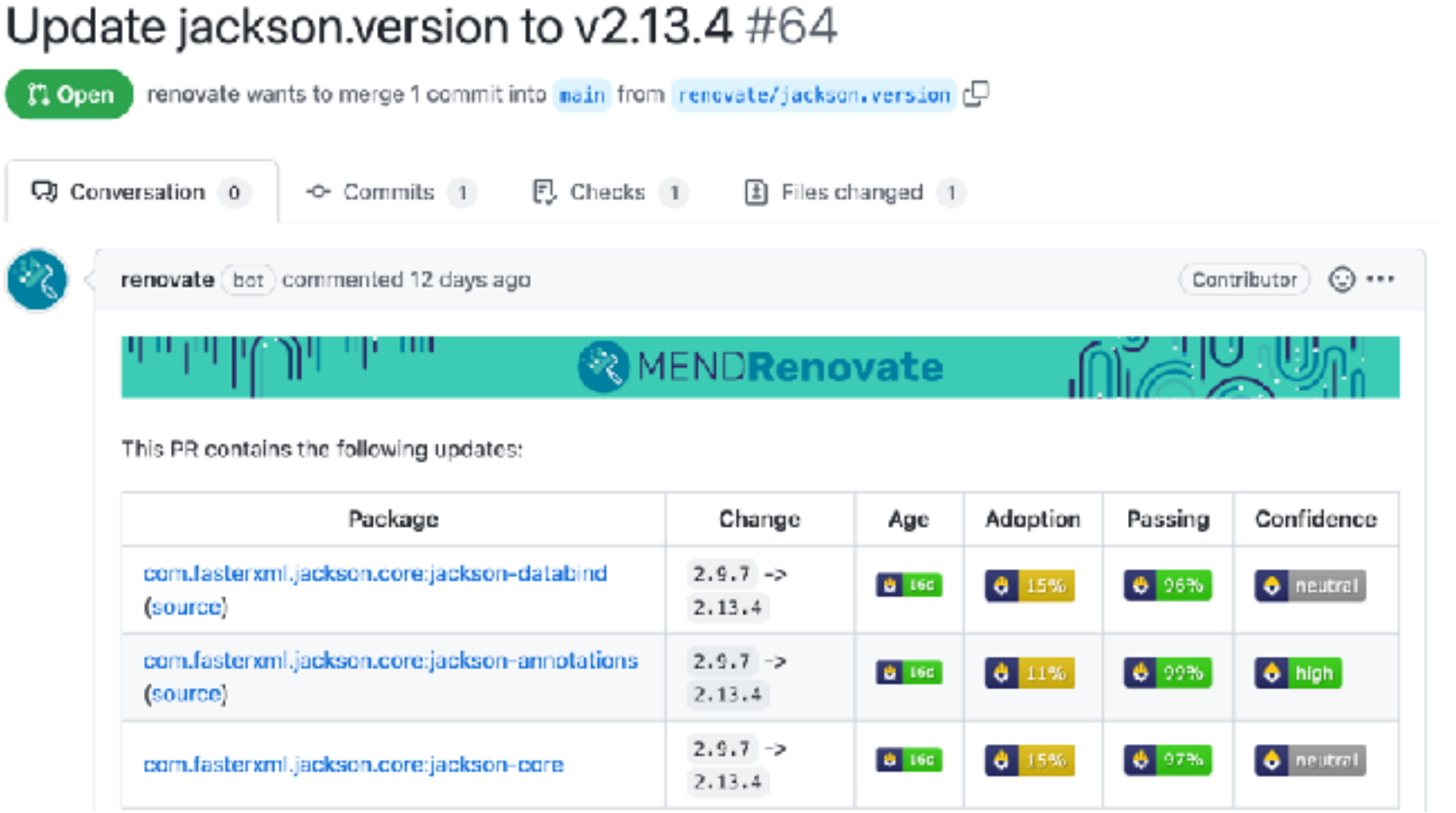
@MaritvanDijk77

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

https://docs.renovatebot.com/configuration-options/

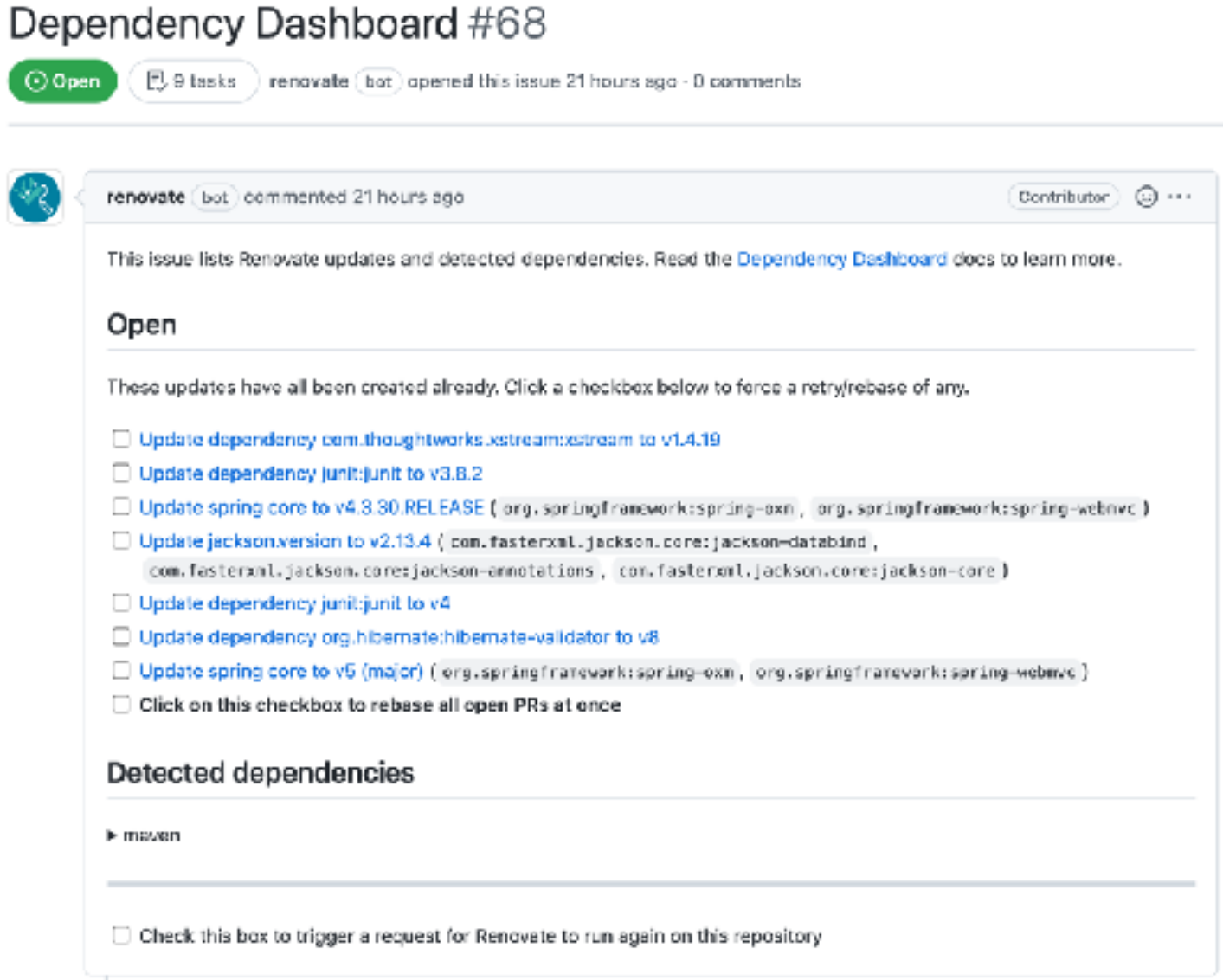
Renovate PR



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

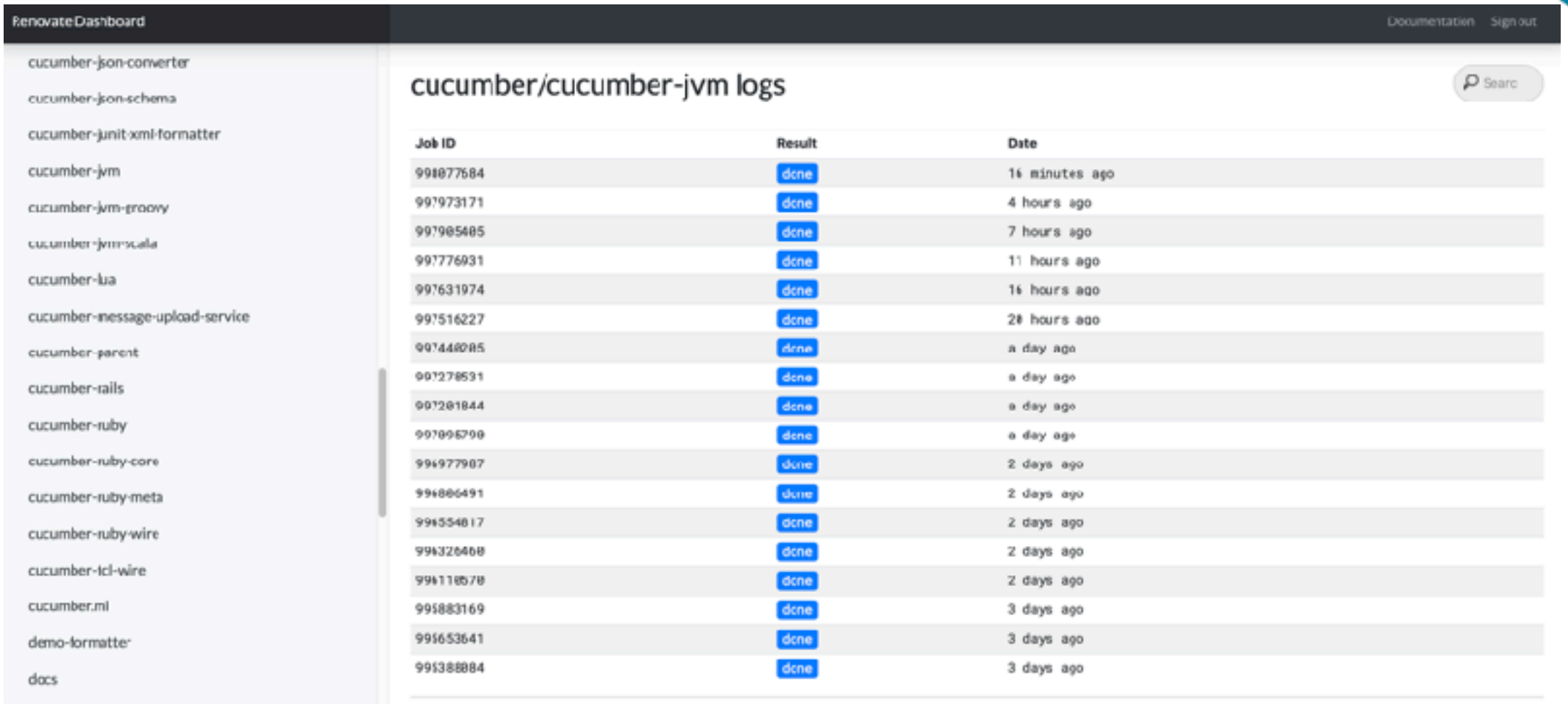
Detected dependencies

▸ maven

- [ ] Check this box to trigger a request for Renovate to run again on this repository

@MaritvanDijk77

Renovate Dashboard: Jobs



@MaritvanDijk77

Renovate: Supported platforms

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

https://docs.renovatebot.com/#supported-platforms

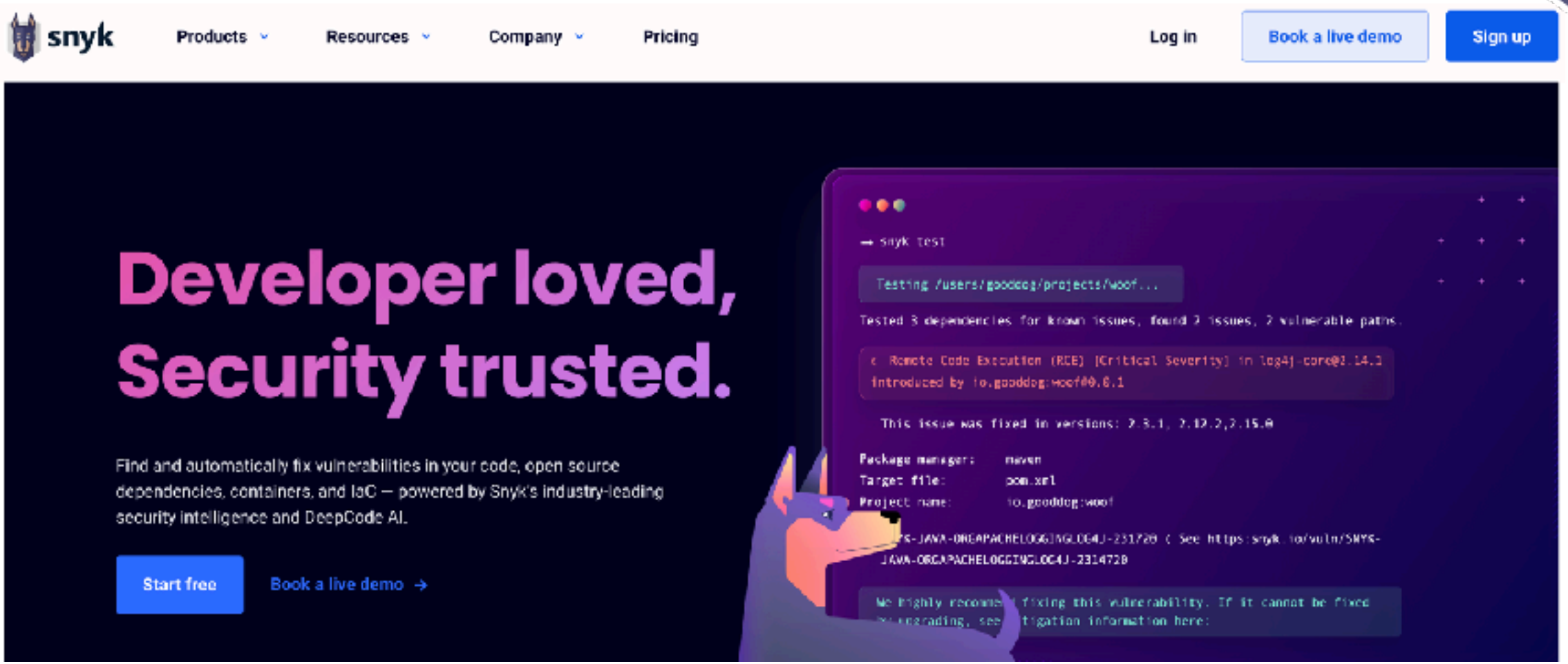
Snyk Open Source

- Available via Snyk

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

https://snyk.io/

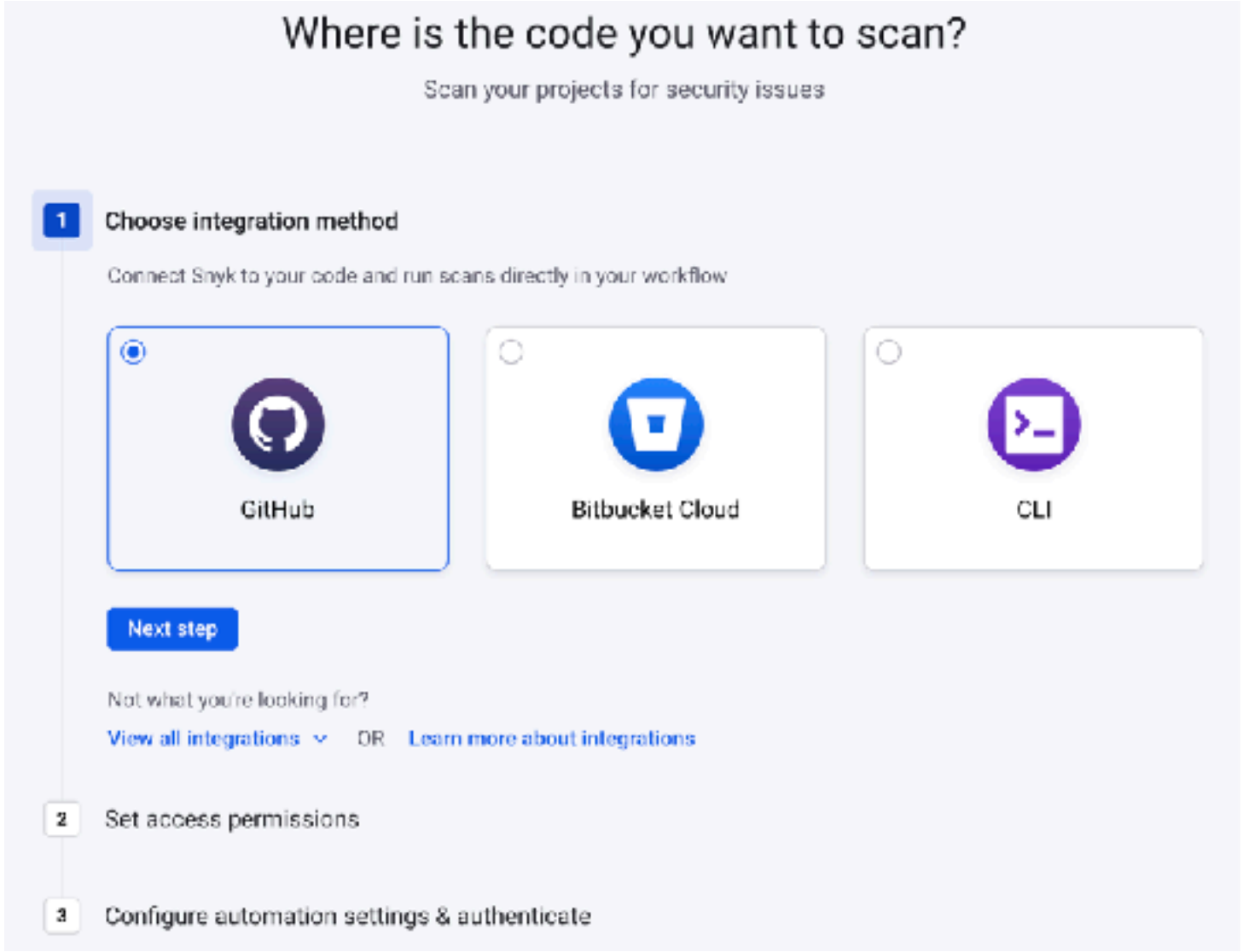
Snyk enable



https://snyk.io/

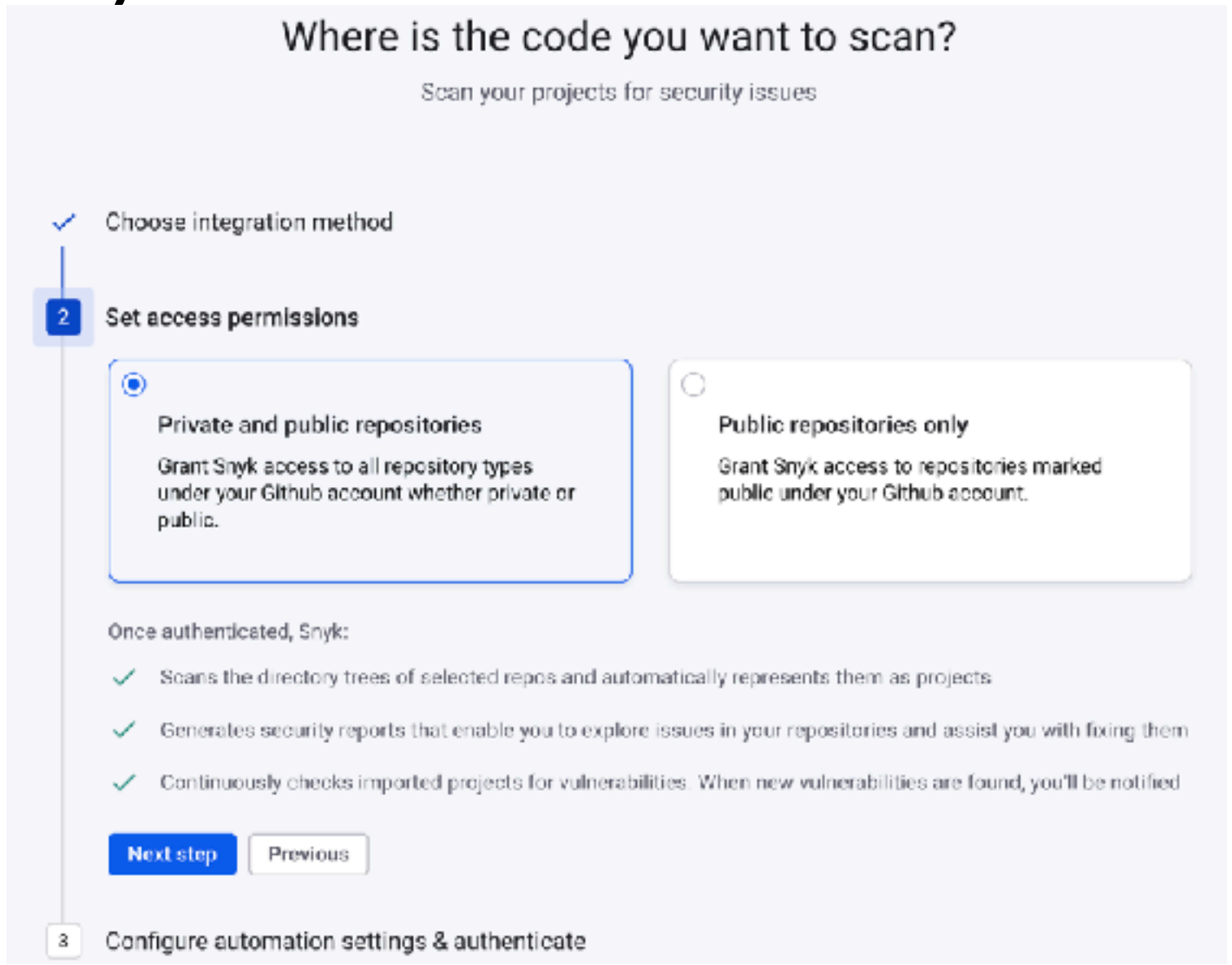
@MaritvanDijk77

Snyk enable



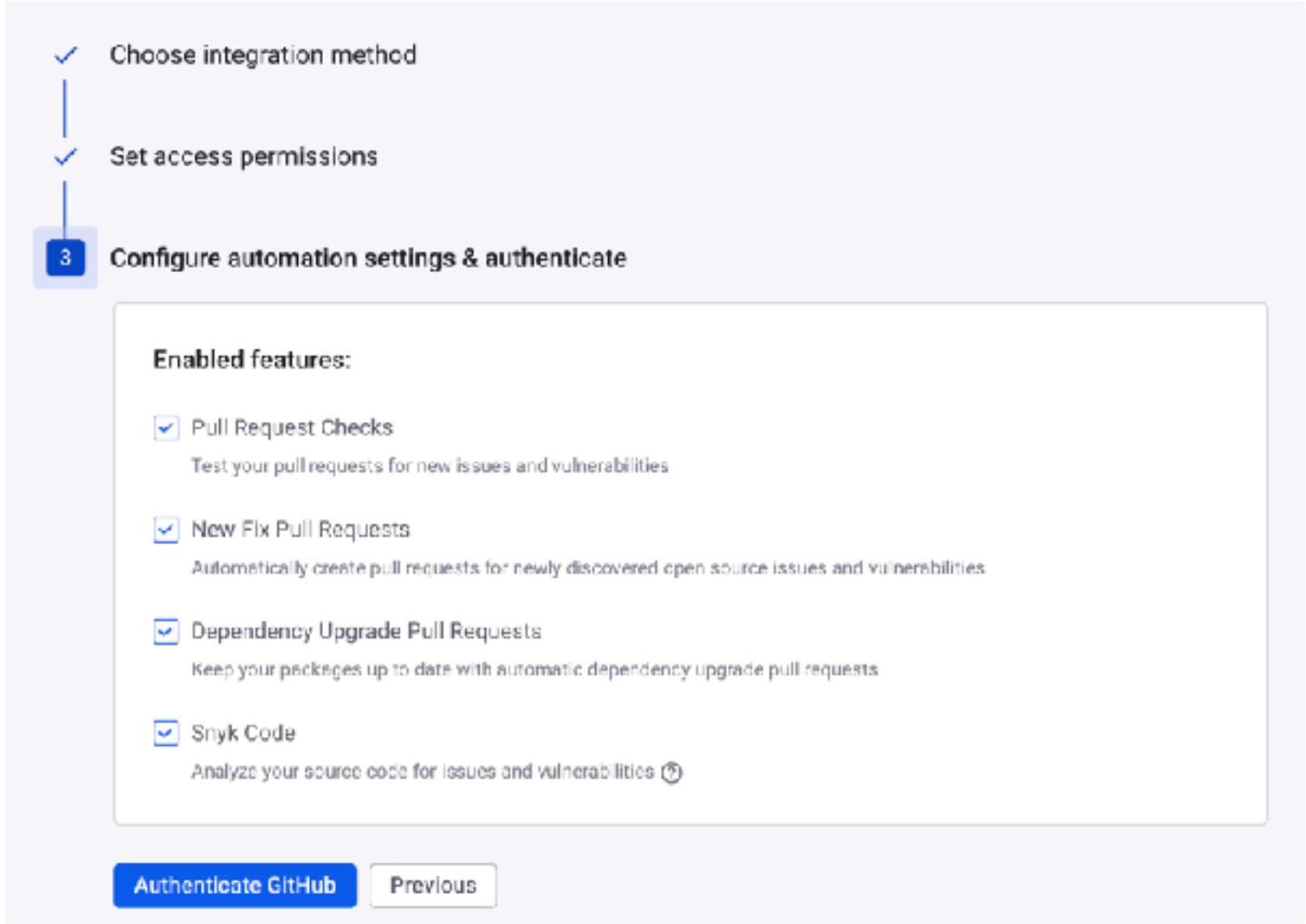
@MaritvanDijk77

Snyk enable



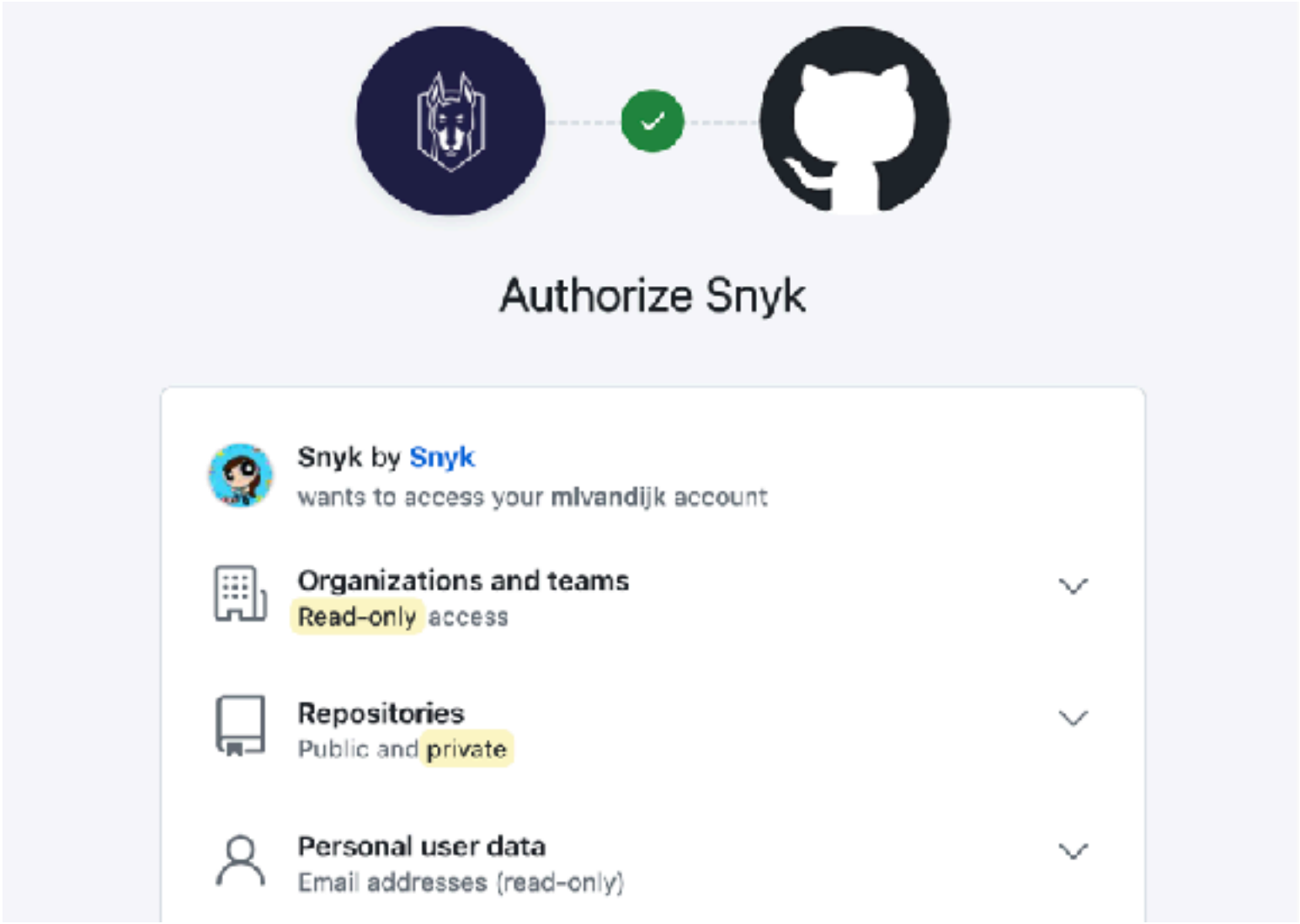
@MaritvanDijk77

Snyk enable



@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)

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-6545eb40e5d321170cd9baa857119a65

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
H	691/1000 Why? Recently disclosed, Has a fix available, CVSS 8.1	Deserialization of Untrusted Data SNYK-JAVA-COMFASTERXMLJACKSONCORE-1061931	`com.fasterxml.jackson.core:jackson-databind:` `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-894f739a21477e79bcca4d5278b3dfba`

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

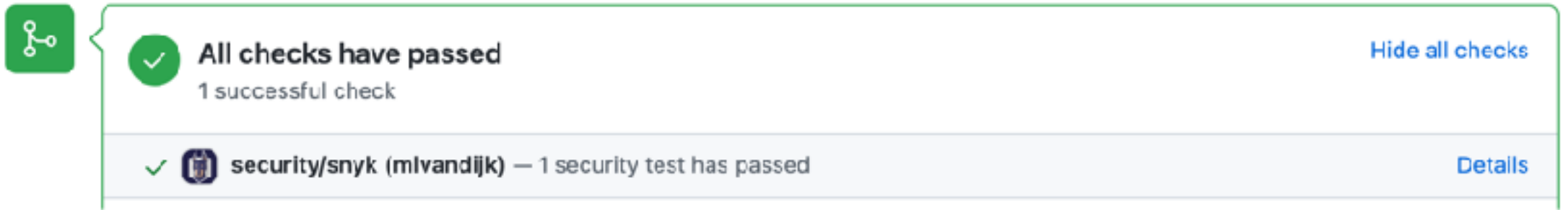
Vulnerabilities that will be fixed

With an upgrade:

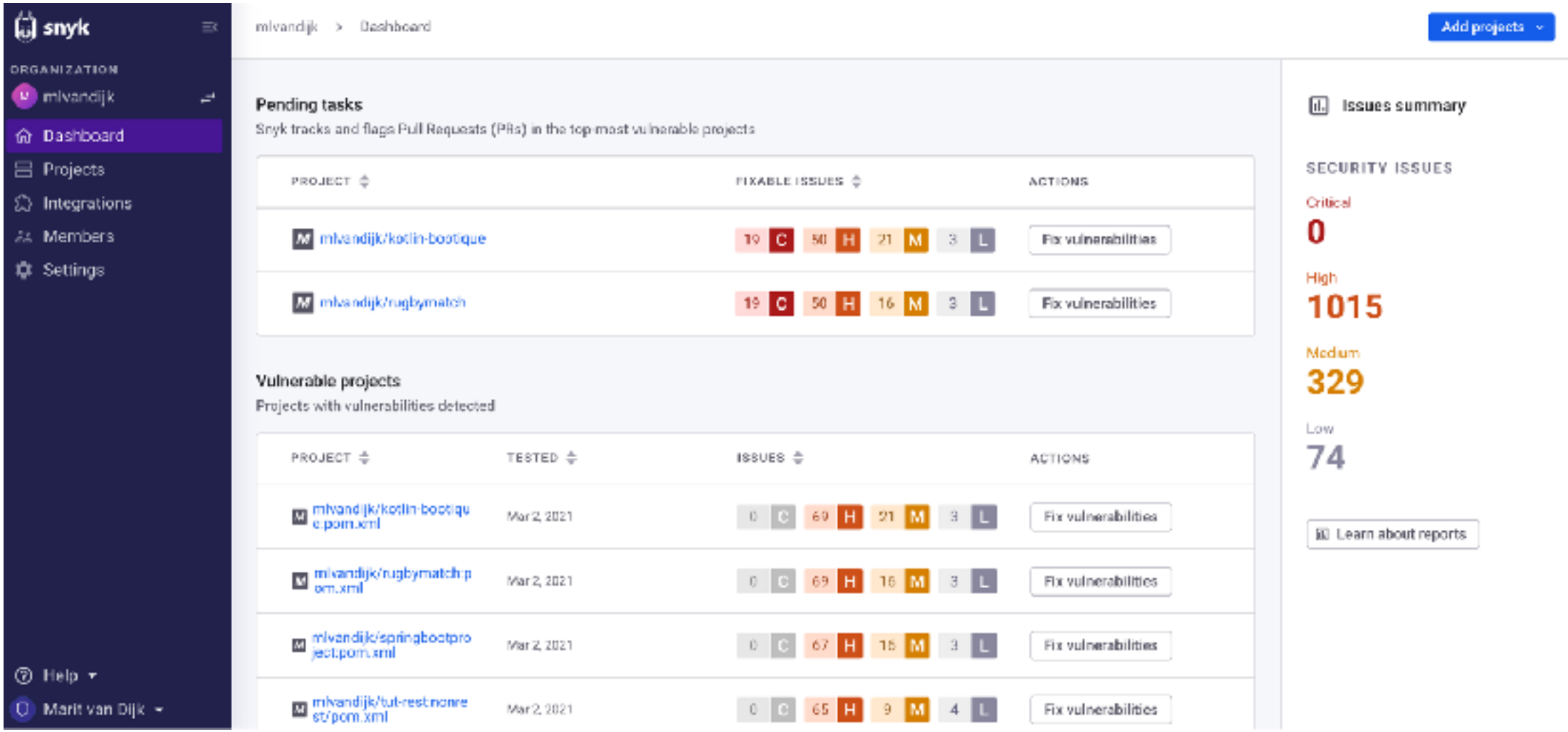
Severity	Priority Score (*)	Issue	Upgrade	Breaking Change	Exploit Maturity
H	644/1000 Why? Has a fix available, CVSS 8.6	Improper Input Validation SNYK-JAVA-ORGSPRINGFRAMEWORK-1009832	`org.springframework:spring-webmvc` `4.3.5.RELEASE` -> `4.3.29.RELEASE`	No	No Known Exploit
M	509/1000 Why? Has a fix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

@MaritvanDijk77

Snyk PR Check



Snyk dashboard



@MaritvanDijk77

Snyk Open Source Configuration

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

https://docs.snyk.io/products/snyk-open-source/open-source-basics

Snyk Open Source: Supported Platforms

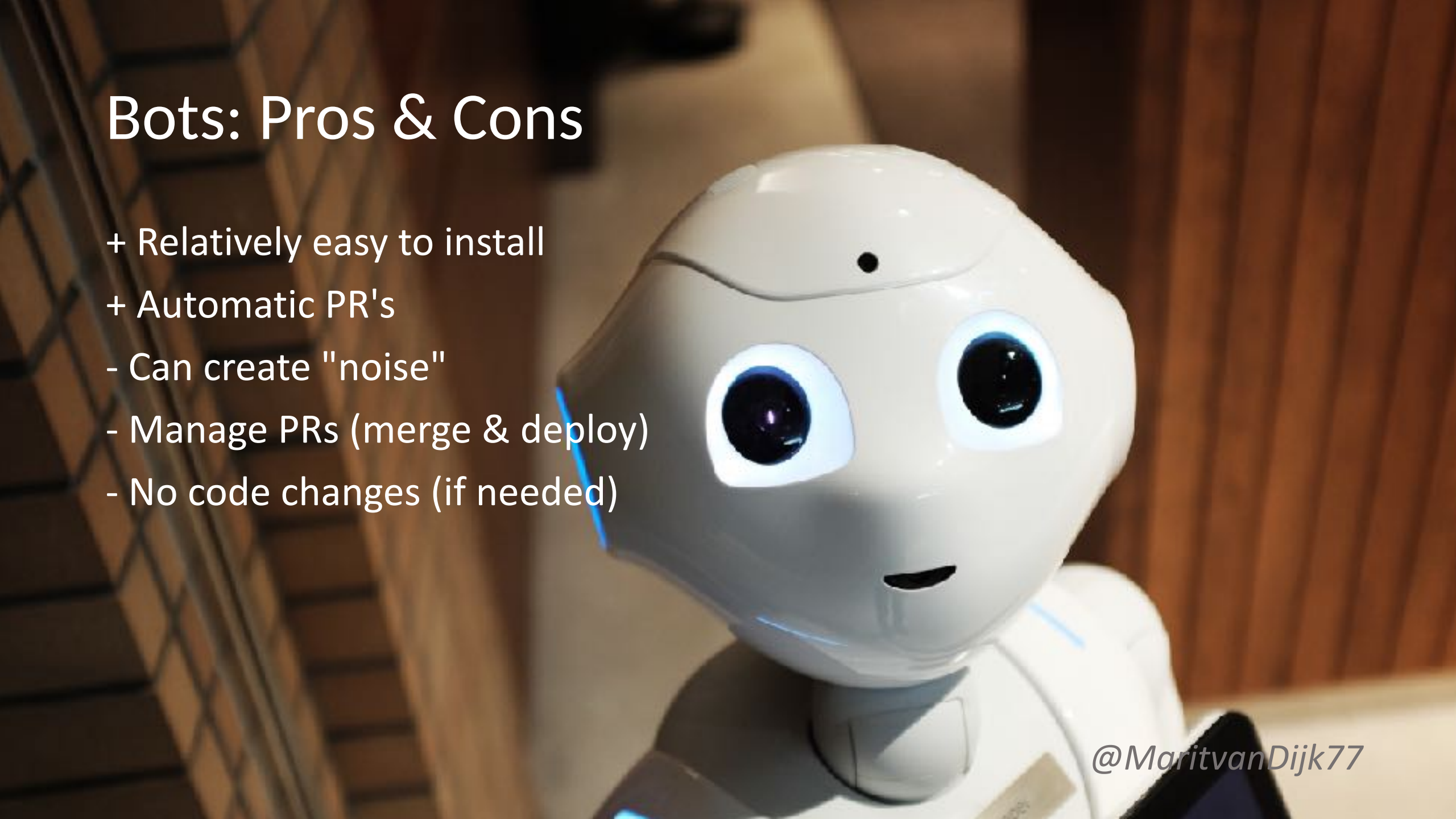
- GitHub
- GitHub Enterprise
- GitHub Read-only projects
- Bitbucket Cloud Personal Access Token (Legacy)
- Bitbucket Cloud App
- Bitbucket Data Center/Server
- GitLab
- Azure Repos

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

Bots

- Dependabot
- Renovate
- Snyk Open Source

Bots: Pros & Cons



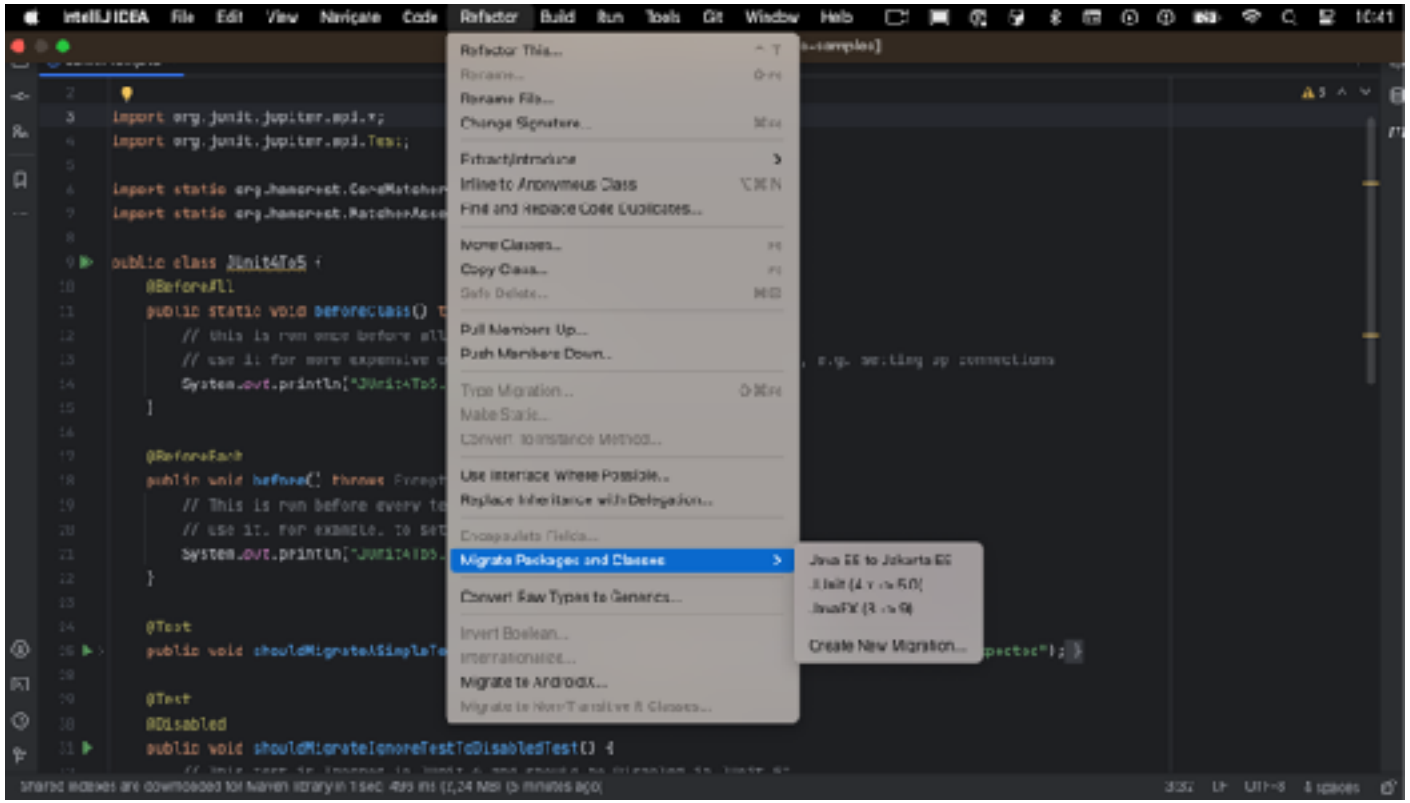
+ Relatively easy to install
+ Automatic PR's
- Can create "noise"
- Manage PRs (merge & deploy)
- No code changes (if needed)

Migration tools

@MaritvanDijk77

IntelliJ IDEA

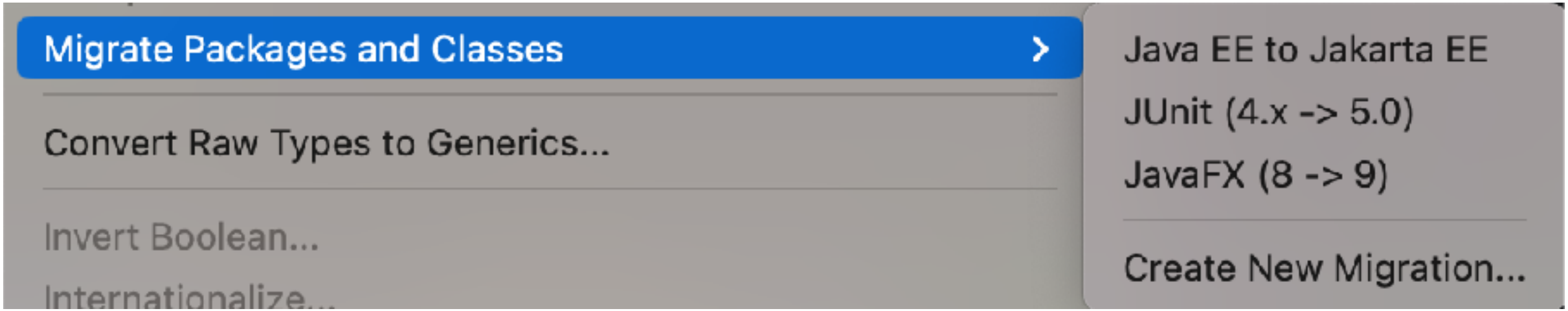
- Refactor > Migrate Packages and Classes



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

IntelliJ IDEA

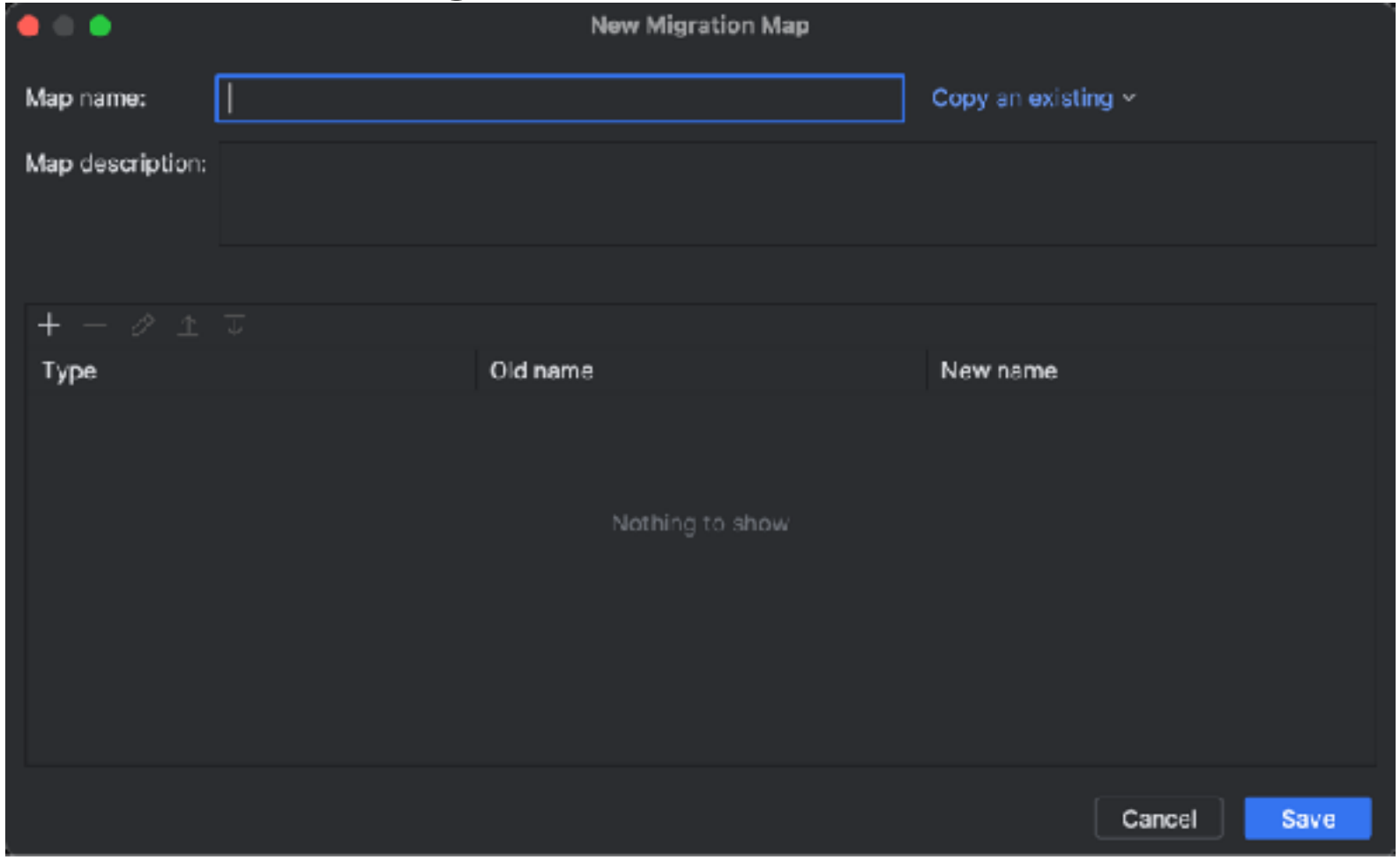
- Refactor > Migrate Packages and Classes >
  - Java EE to Jakarta EE
  - JUnit (4.x -> 5.0)
  - JavaFX (8 -> 9)



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

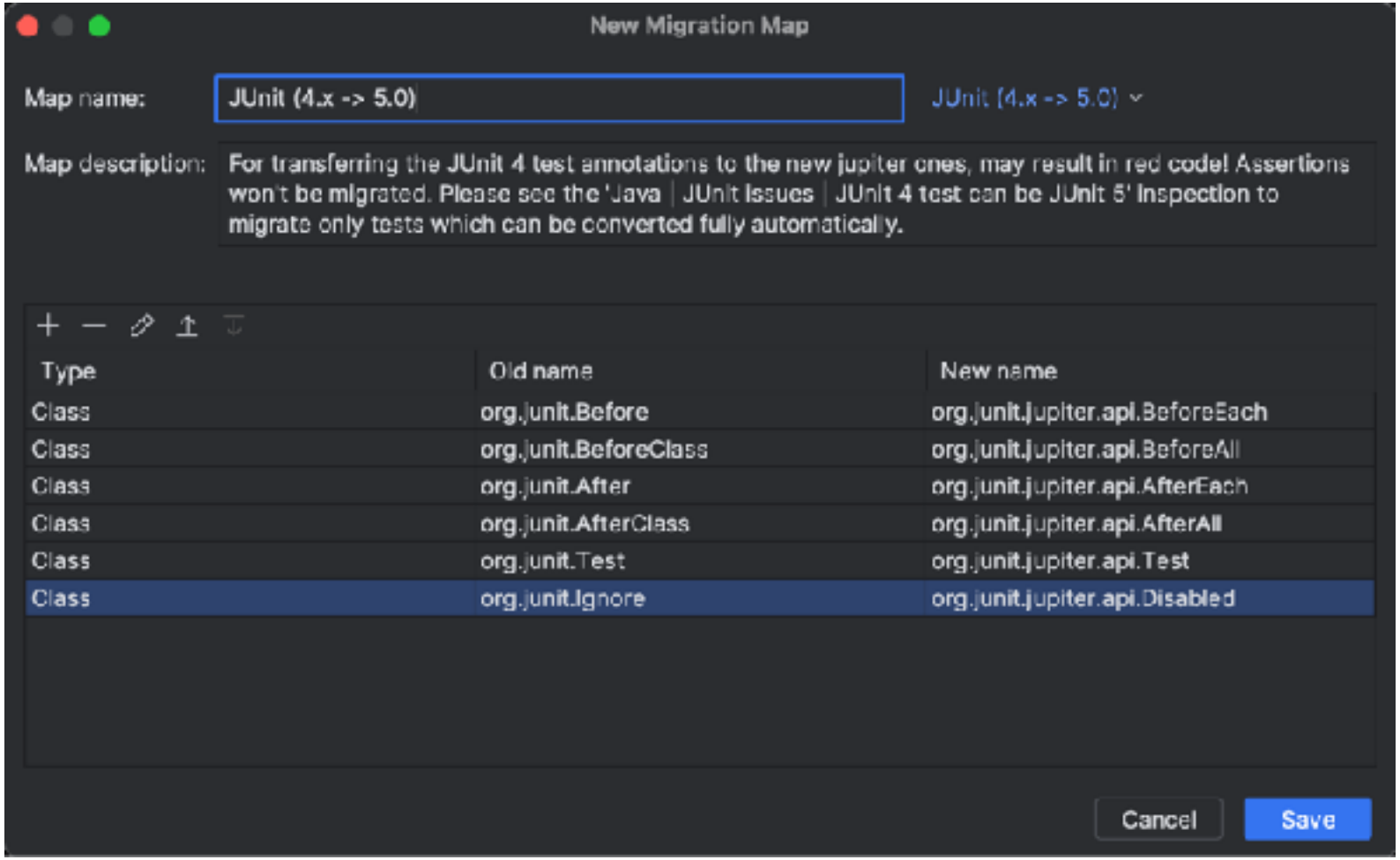
IntelliJ IDEA

- Create New Migration



IntelliJ IDEA

- Create New Migration



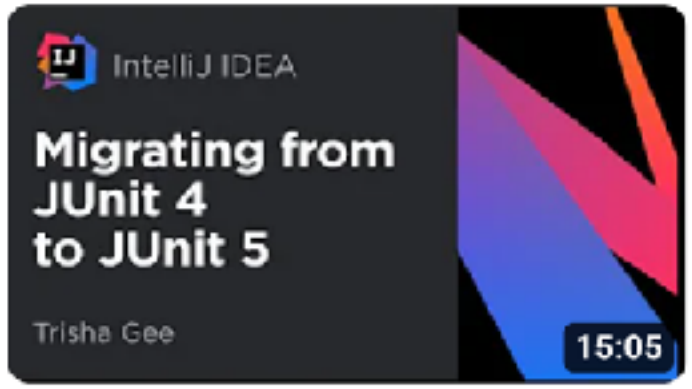
IntelliJ IDEA

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

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

https://errorprone.info/

Error Prone

Error Prone

https://www.youtube.com/watch?v=NPuLeoIzIR0

@MaritvanDijk77

Error Prone Support

Error Prone

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

Rewrite

- **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, ...

https://docs.openrewrite.org/

OpenRewrite

- Existing recipes
  - Upgrade versions
  - Migrate libraries

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

Rewrite

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

@MaritvanDijk77

OpenRewrite

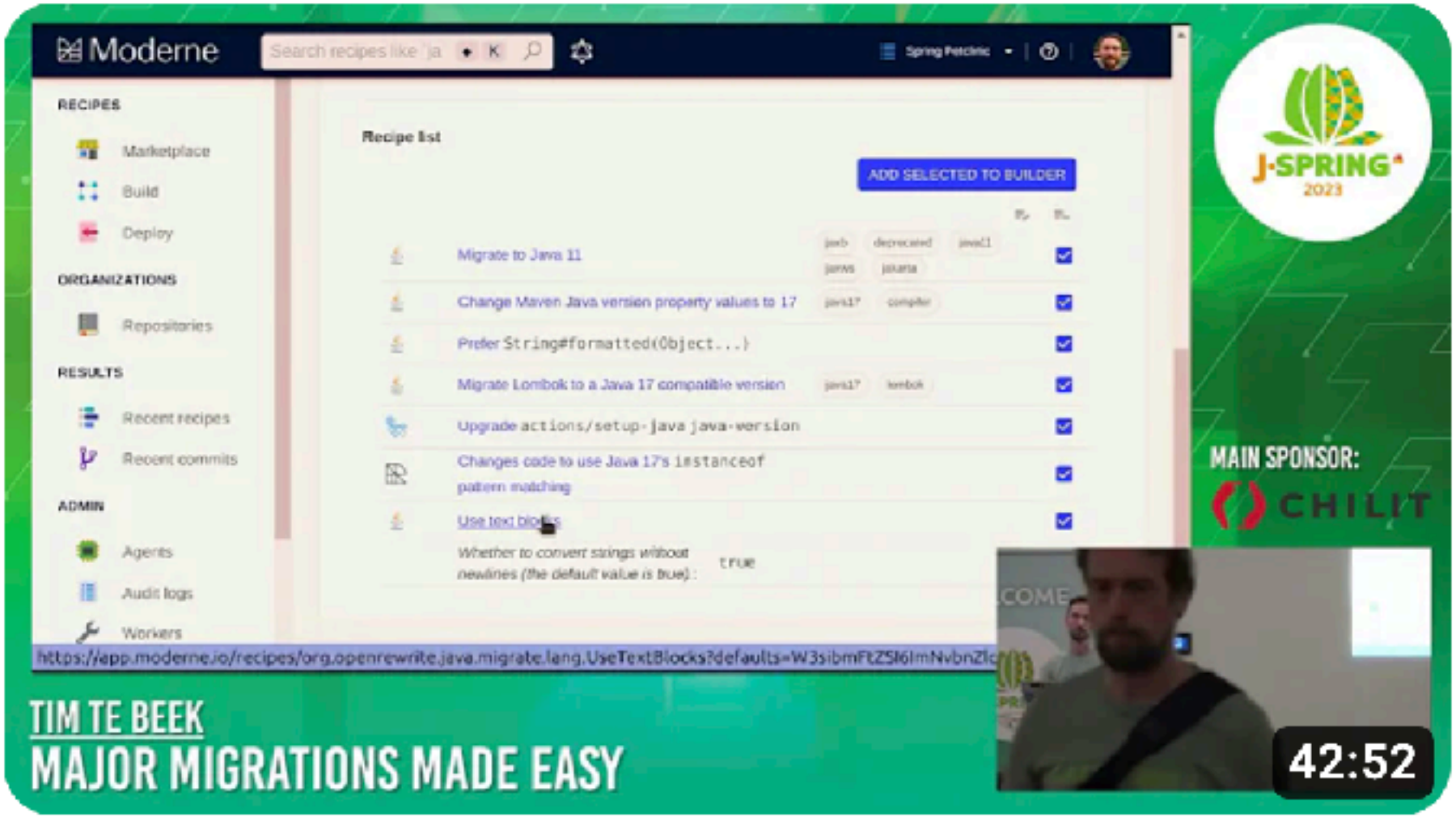
- Existing recipes
- Can author your own recipes

https://docs.openrewrite.org/

@MaritvanDijk77

OpenRewrite

Rewrite



https://www.youtube.com/watch?v=jOFfCAleUI8

@MaritvanDijk77

Conclusion

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

@MaritvanDijk77

Slides & More

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

@MaritvanDijk77

goto;

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