dep-scan v5

OWASP®

APPTHREAT

About me

Prabhu Subramanian

Founder & AppSec consultant

✉️ prabhu@appthreat.dev

_prbh

CDXGEN

BLINT

DEPSCAN

Agenda

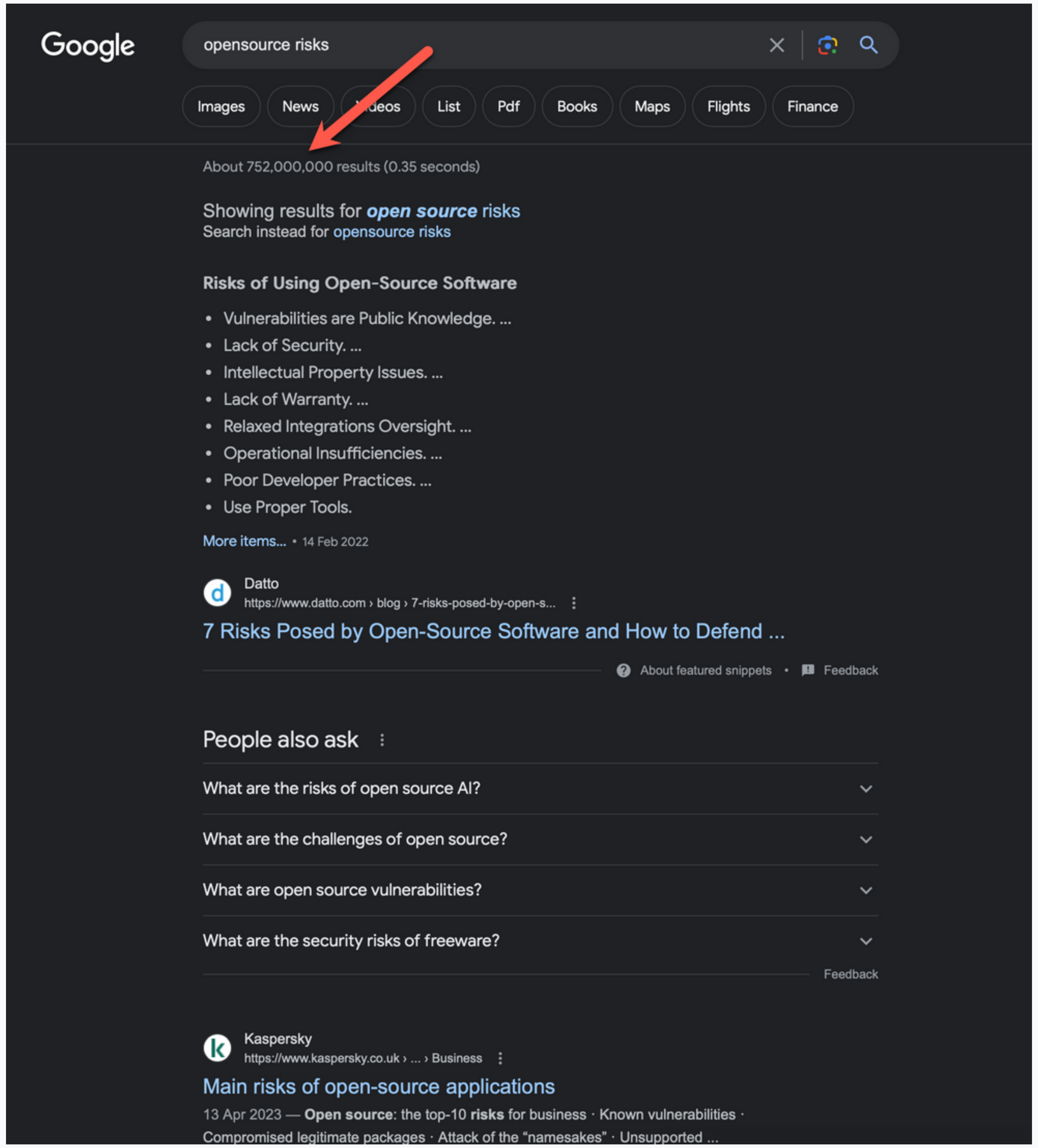
Is Open source **Risky?**

Supply Chain Security from Open source?

Engineering dep-scan

Is Open source Risky?

Open source OMG



Google

opensource risks

Images · News · Videos · List · Pdf · Books · Maps · Flights · Finance

About 752,000,000 results (0.35 seconds)

Showing results for ***open source*** risks
Search instead for opensource risks

Risks of Using Open-Source Software

- Vulnerabilities are Public Knowledge. ...
- Lack of Security. ...
- Intellectual Property Issues. ...
- Lack of Warranty. ...
- Relaxed Integrations Oversight. ...
- Operational Insufficiencies. ...
- Poor Developer Practices. ...
- Use Proper Tools.

More items... • 14 Feb 2022

Datto
https://www.datto.com › blog › 7-risks-posed-by-open-s...

7 Risks Posed by Open-Source Software and How to Defend ...

About featured snippets • Feedback

People also ask

What are the risks of open source AI?

What are the challenges of open source?

What are open source vulnerabilities?

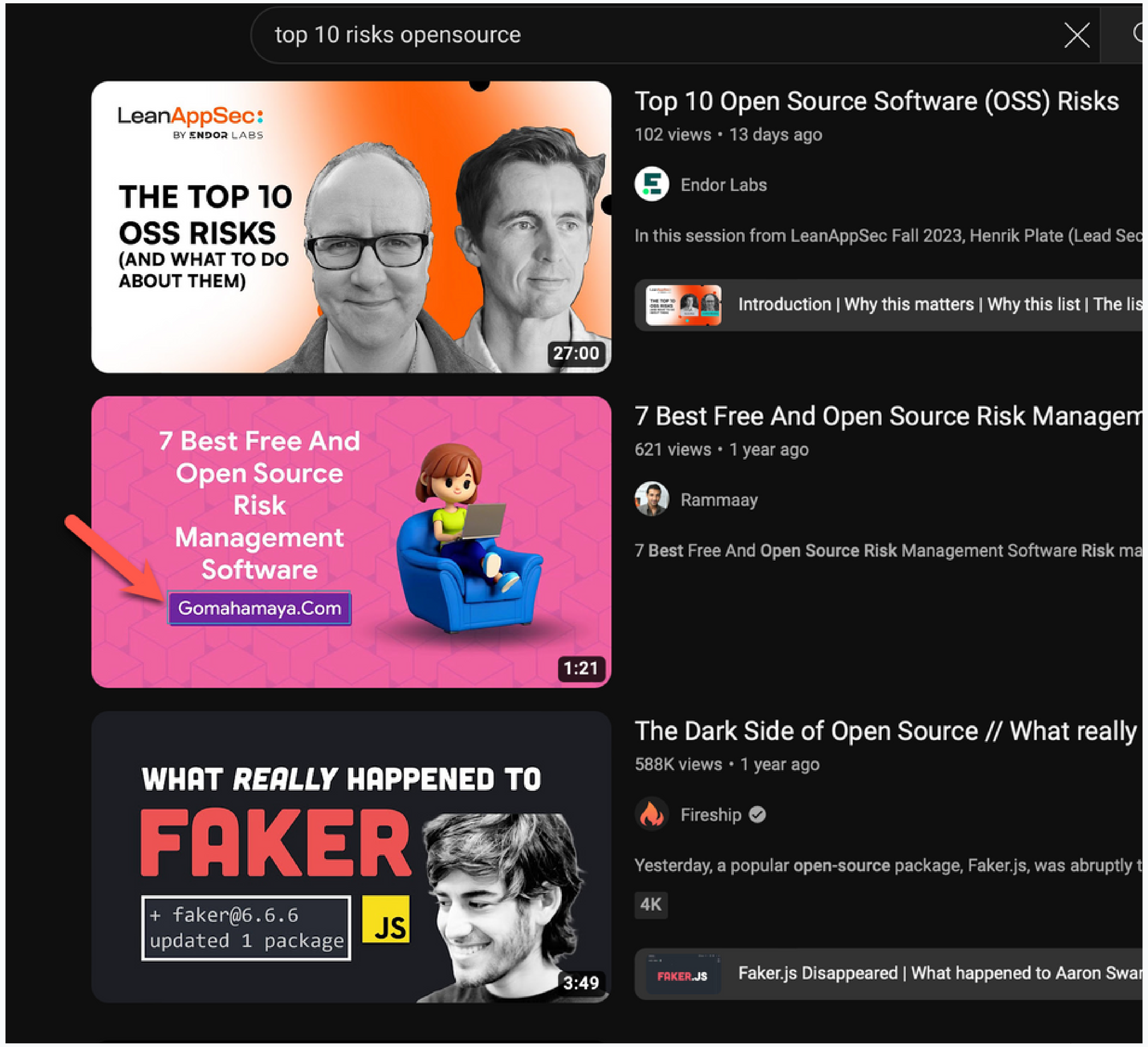
What are the security risks of freeware?

Feedback

Kaspersky
https://www.kaspersky.co.uk › ... › Business

Main risks of open-source applications

13 Apr 2023 — **Open source**: the top-10 **risks** for business · Known vulnerabilities · Compromised legitimate packages · Attack of the "namesakes" · Unsupported ...



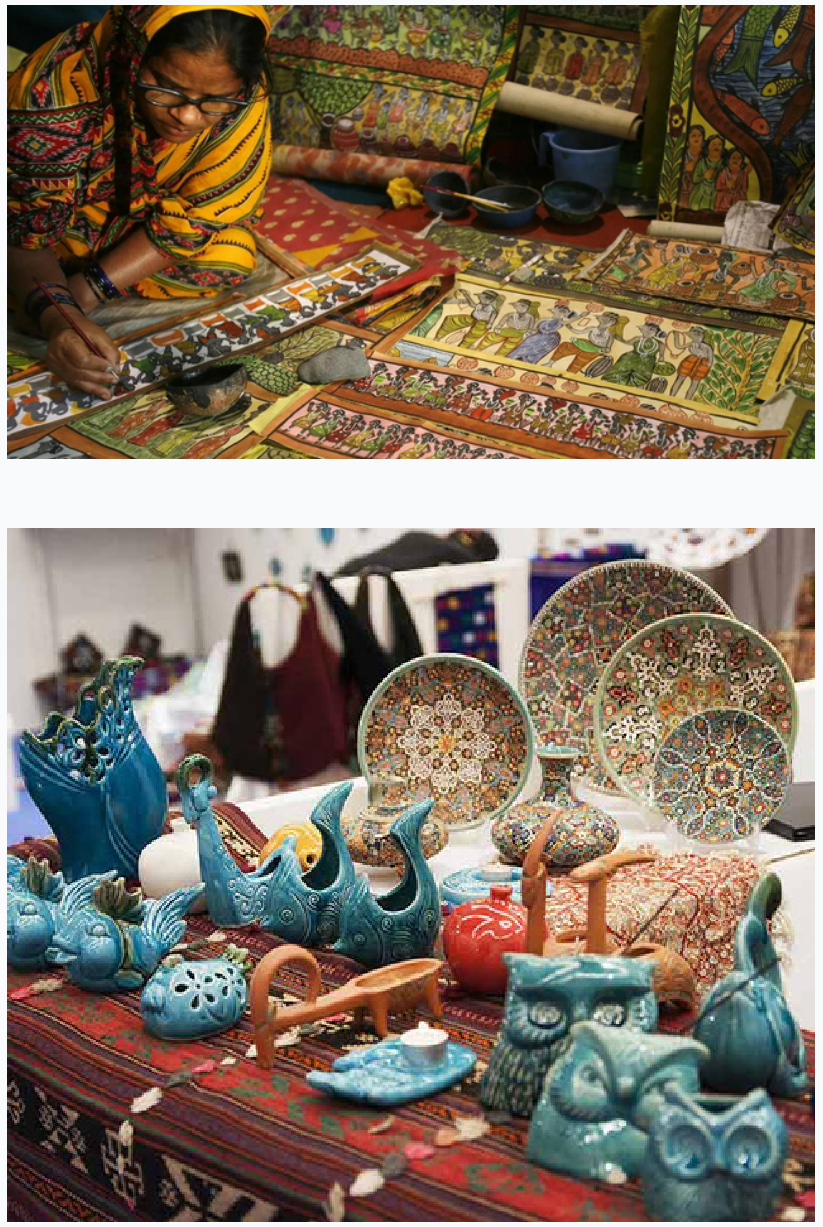
top 10 risks opensource

Top 10 Open Source Software (OSS) Risks
102 views • 13 days ago
Endor Labs
In this session from LeanAppSec Fall 2023, Henrik Plate (Lead Sec
Introduction | Why this matters | Why this list | The lis

7 Best Free And Open Source Risk Managem
621 views • 1 year ago
Rammaay
7 Best Free And **Open Source Risk** Management Software **Risk** ma

The Dark Side of Open Source // What really
588K views • 1 year ago
Fireship
Yesterday, a popular **open-source** package, Faker.js, was abruptly t
4K
Faker.js Disappeared | What happened to Aaron Swar

Open source Publishers



Creators and Artisans

APPTHREAT

Backed by Commercial activities

OWASP®

Backed by Foundation

Why security from Open source?

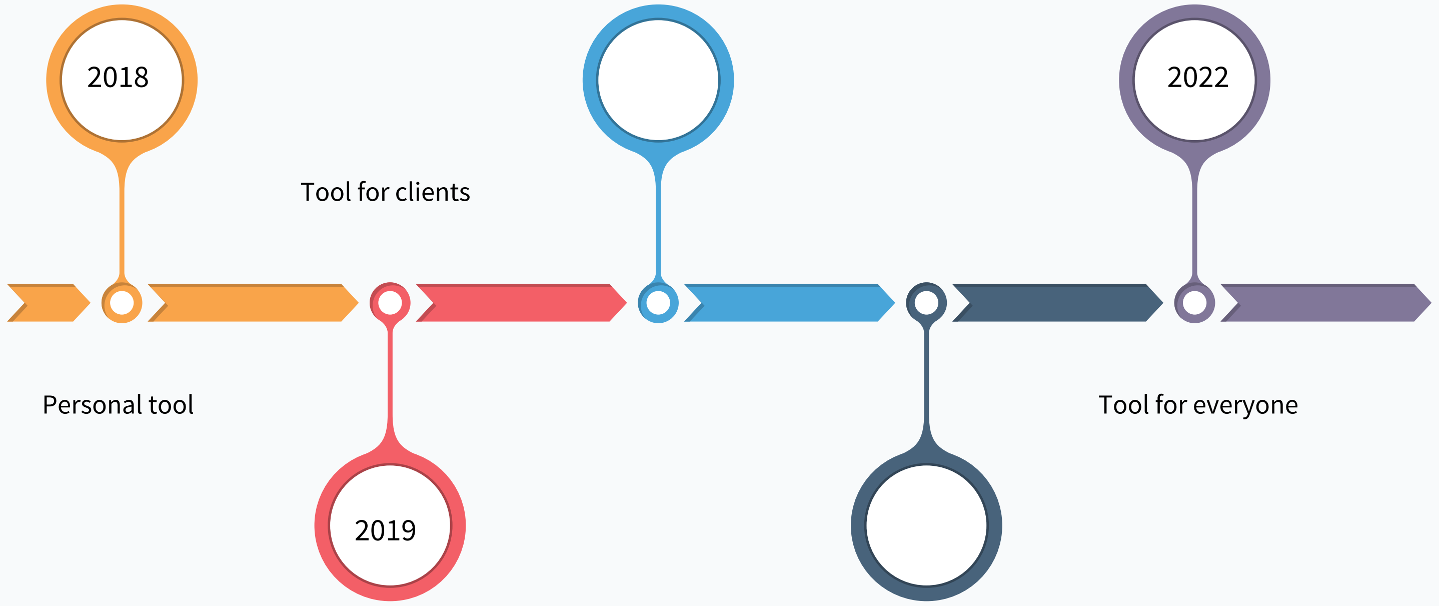
Let’s talk dep-scan

What’s dep-scan?

Purpose built to forget

Next generation analysis

Free, open source with privacy



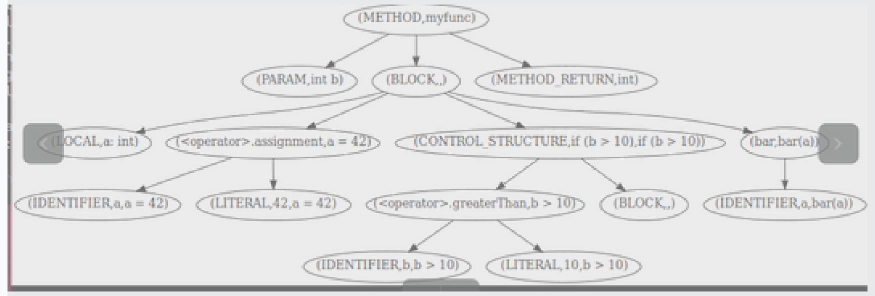
DEMO

Purpose built to forget

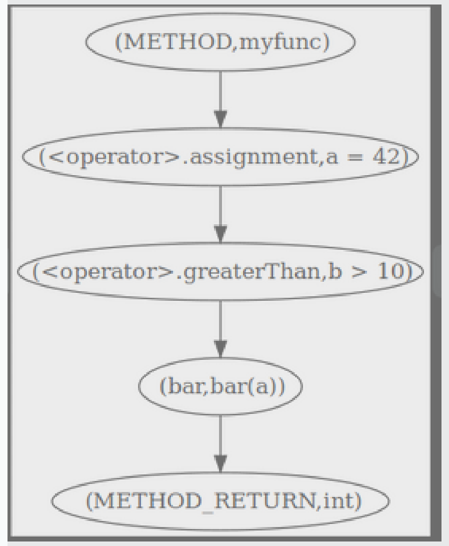
Next generation analysis

Free, open source with privacy

Next Generation Analysis

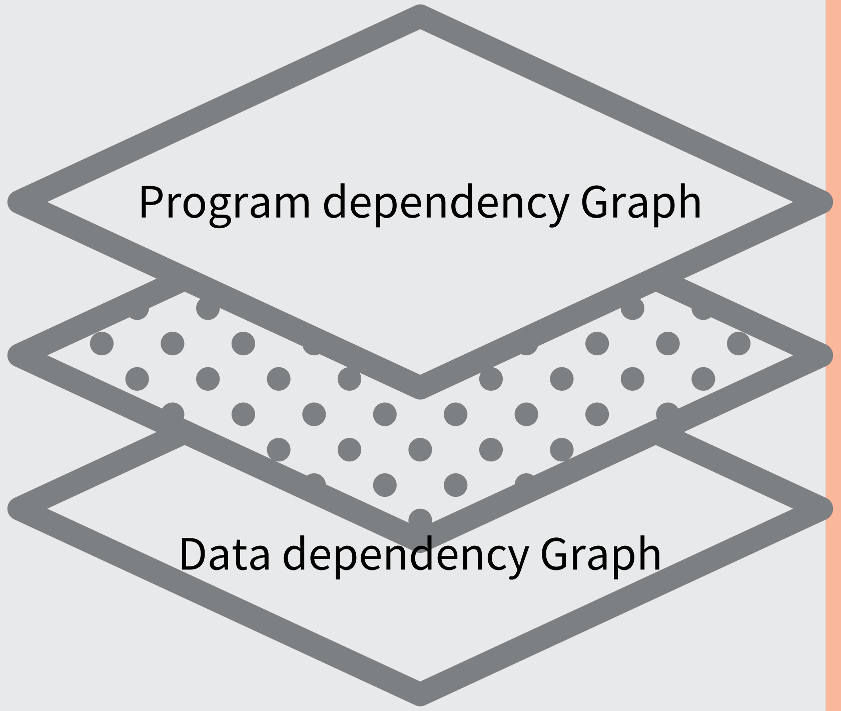


Abstract Syntax Tree


(METHOD,myfunc)
(<operator>.assignment,a = 42)
(<operator>.greaterThan,b > 10)
(bar,bar(a))
(METHOD_RETURN,int)

Control Flow Graph

This is some Java application



This is a Spring application with SQL library

Type Inference

Package Inference

Auto tagging

Semantic tagging

Service dependency Graph

What does this application do?

Why, when, and how are the libraries used?

How can it be improved?

Precision Reachability analysis

Constant time performance

Works **with or without** vulnerabilities

All types supported:

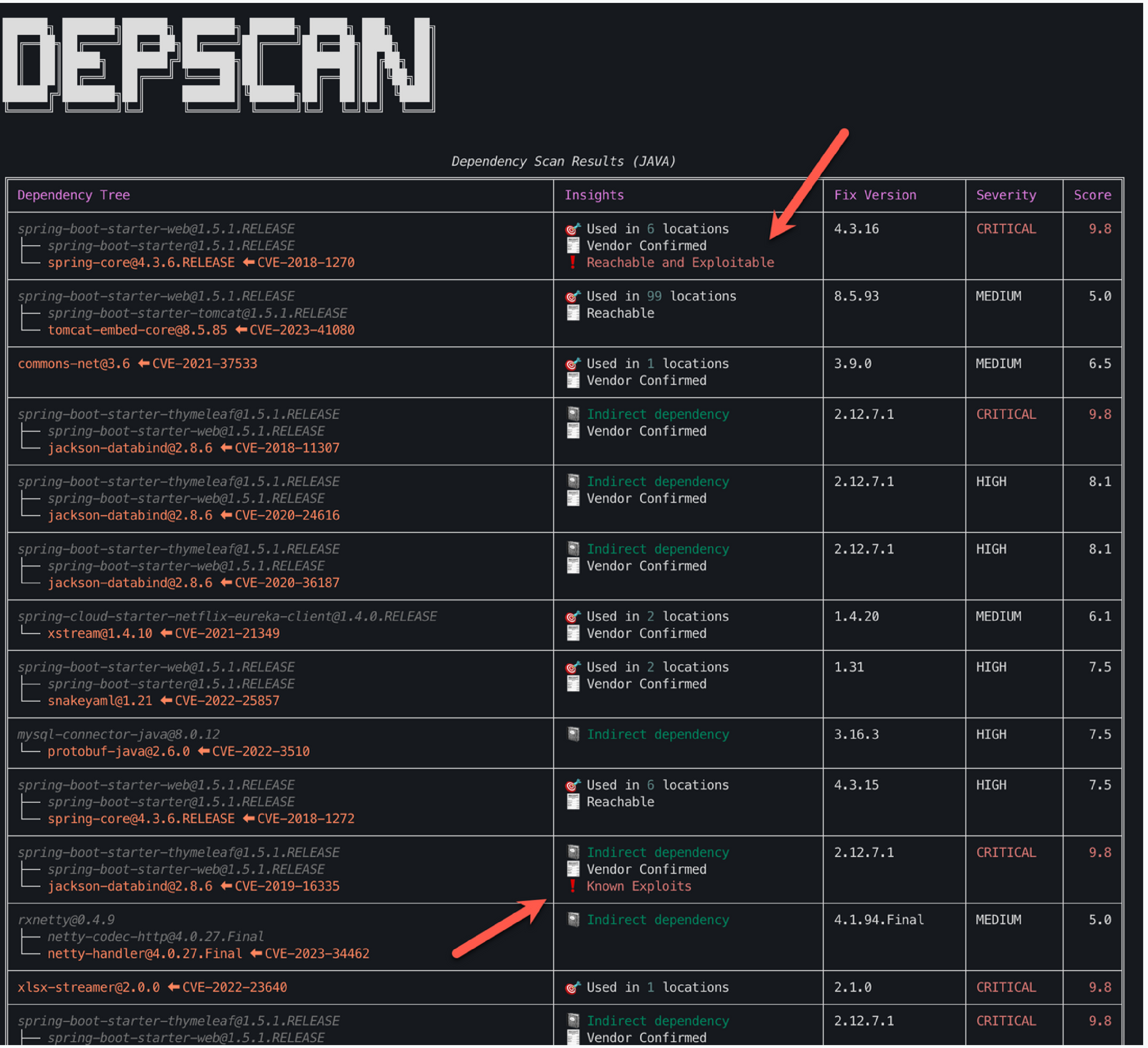
- Forward-Reachability (most applications)
- Reverse-Reachability (libraries without entrypoints)
- Inter moduler Reachability (Across packages)

Coming soon

github.com/owasp-dep-scan/dep-scan

```
pip install owasp-depscan
```

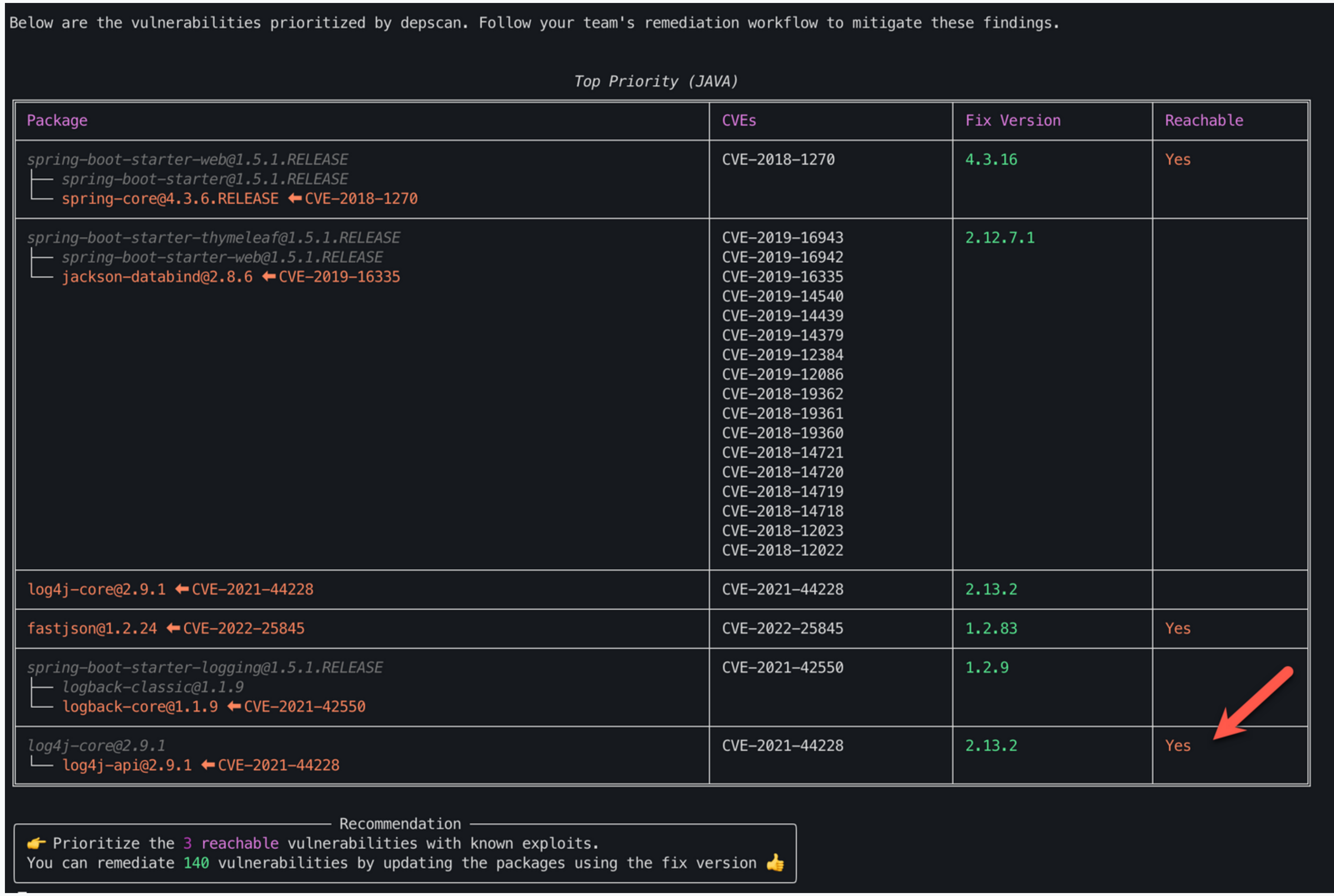
Media



DEPSCAN

Dependency Scan Results (JAVA)

Dependency Tree	Insights	Fix Version	Severity	Score
spring-boot-starter-web@1.5.1.RELEASE ├── *spring-boot-starter@1.5.1.RELEASE* └── spring-core@4.3.6.RELEASE ⬅CVE-2018-1270	🎯 Used in 6 locations 📄 Vendor Confirmed ❗ Reachable and Exploitable	4.3.16	CRITICAL	9.8
spring-boot-starter-web@1.5.1.RELEASE ├── *spring-boot-starter-tomcat@1.5.1.RELEASE* └── tomcat-embed-core@8.5.85 ⬅CVE-2023-41080	🎯 Used in 99 locations 📄 Reachable	8.5.93	MEDIUM	5.0
commons-net@3.6 ⬅CVE-2021-37533	🎯 Used in 1 locations 📄 Vendor Confirmed	3.9.0	MEDIUM	6.5
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE* └── jackson-databind@2.8.6 ⬅CVE-2018-11307	📓 Indirect dependency 📄 Vendor Confirmed	2.12.7.1	CRITICAL	9.8
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE* └── jackson-databind@2.8.6 ⬅CVE-2020-24616	📓 Indirect dependency 📄 Vendor Confirmed	2.12.7.1	HIGH	8.1
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE* └── jackson-databind@2.8.6 ⬅CVE-2020-36187	📓 Indirect dependency 📄 Vendor Confirmed	2.12.7.1	HIGH	8.1
spring-cloud-starter-netflix-eureka-client@1.4.0.RELEASE └── xstream@1.4.10 ⬅CVE-2021-21349	🎯 Used in 2 locations 📄 Vendor Confirmed	1.4.20	MEDIUM	6.1
spring-boot-starter-web@1.5.1.RELEASE ├── *spring-boot-starter@1.5.1.RELEASE* └── snakeyaml@1.21 ⬅CVE-2022-25857	🎯 Used in 2 locations 📄 Vendor Confirmed	1.31	HIGH	7.5
mysql-connector-java@8.0.12 └── protobuf-java@2.6.0 ⬅CVE-2022-3510	📓 Indirect dependency	3.16.3	HIGH	7.5
spring-boot-starter-web@1.5.1.RELEASE ├── *spring-boot-starter@1.5.1.RELEASE* └── spring-core@4.3.6.RELEASE ⬅CVE-2018-1272	🎯 Used in 6 locations 📄 Reachable	4.3.15	HIGH	7.5
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE* └── jackson-databind@2.8.6 ⬅CVE-2019-16335	📓 Indirect dependency 📄 Vendor Confirmed ❗ Known Exploits	2.12.7.1	CRITICAL	9.8
rxnetty@0.4.9 ├── *netty-codec-http@4.0.27.Final* └── netty-handler@4.0.27.Final ⬅CVE-2023-34462	📓 Indirect dependency	4.1.94.Final	MEDIUM	5.0
xlsx-streamer@2.0.0 ⬅CVE-2022-23640	🎯 Used in 1 locations	2.1.0	CRITICAL	9.8
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE*	📓 Indirect dependency 📄 Vendor Confirmed	2.12.7.1	CRITICAL	9.8



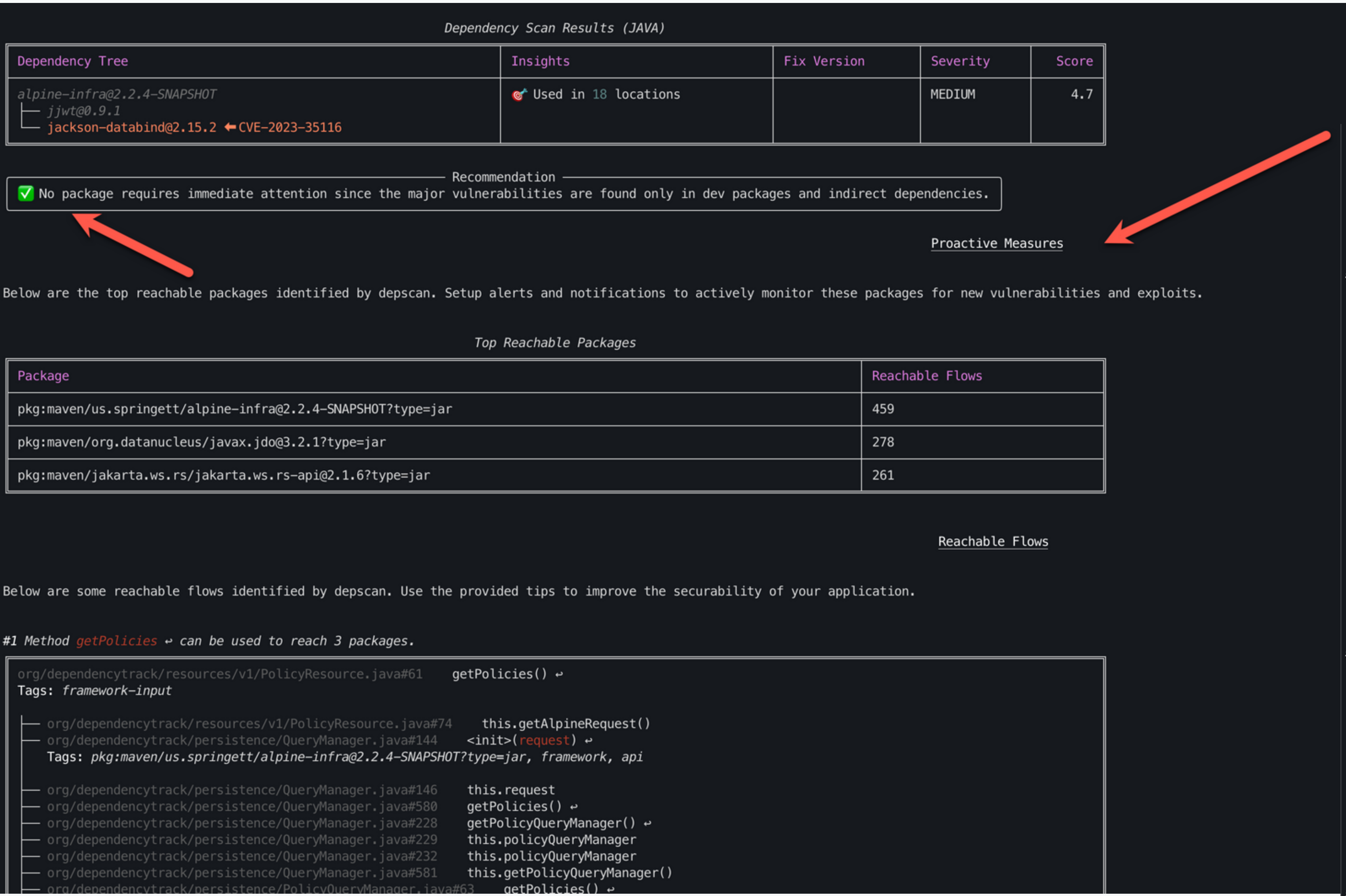
Below are the vulnerabilities prioritized by depscan. Follow your team's remediation workflow to mitigate these findings.

Top Priority (JAVA)

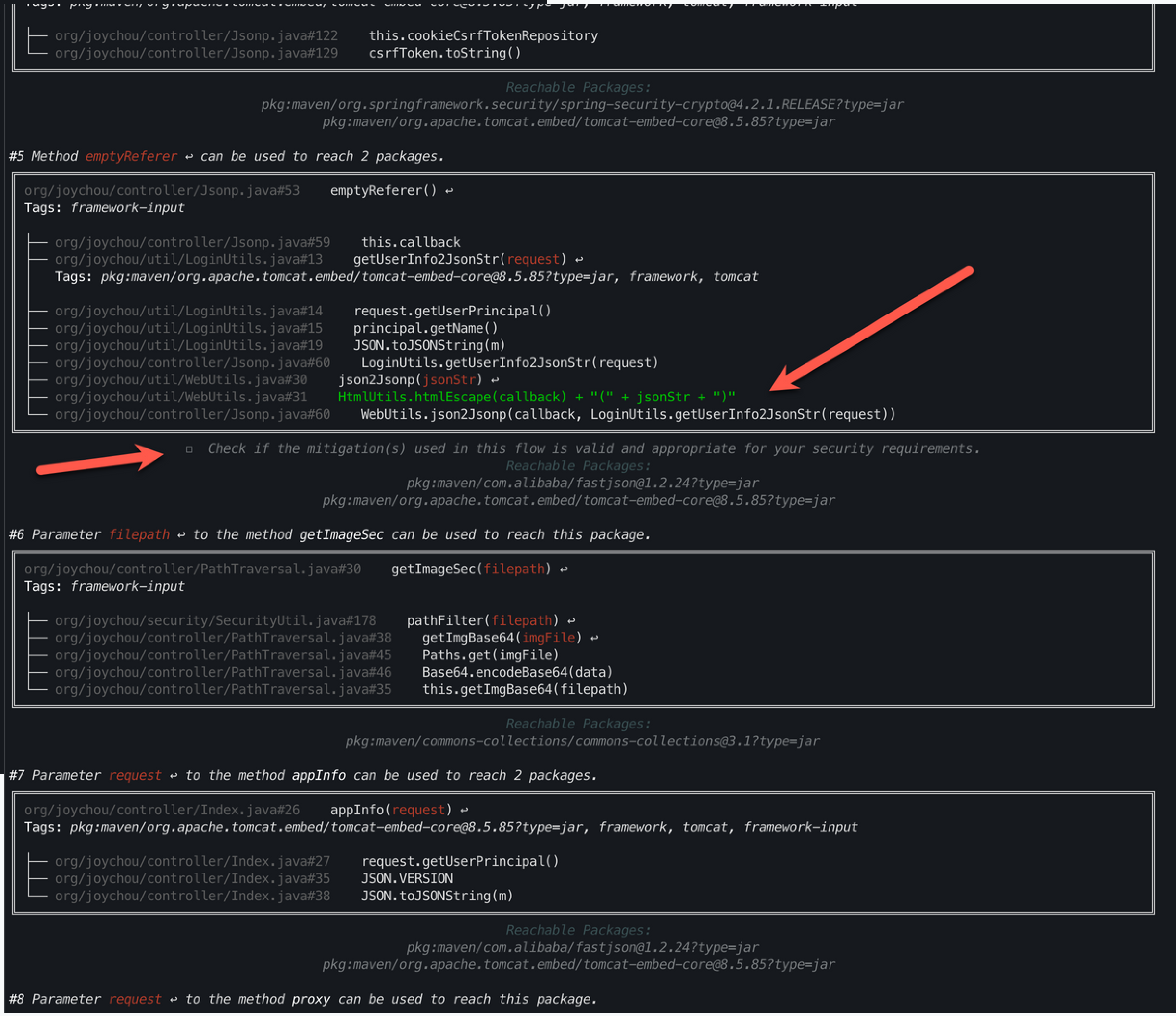
Package	CVEs	Fix Version	Reachable
spring-boot-starter-web@1.5.1.RELEASE ├── *spring-boot-starter@1.5.1.RELEASE* └── spring-core@4.3.6.RELEASE ⬅CVE-2018-1270	CVE-2018-1270	4.3.16	Yes
spring-boot-starter-thymeleaf@1.5.1.RELEASE ├── *spring-boot-starter-web@1.5.1.RELEASE* └── jackson-databind@2.8.6 ⬅CVE-2019-16335	CVE-2019-16943 CVE-2019-16942 CVE-2019-16335 CVE-2019-14540 CVE-2019-14439 CVE-2019-14379 CVE-2019-12384 CVE-2019-12086 CVE-2018-19362 CVE-2018-19361 CVE-2018-19360 CVE-2018-14721 CVE-2018-14720 CVE-2018-14719 CVE-2018-14718 CVE-2018-12023 CVE-2018-12022	2.12.7.1	
log4j-core@2.9.1 ⬅CVE-2021-44228	CVE-2021-44228	2.13.2	
fastjson@1.2.24 ⬅CVE-2022-25845	CVE-2022-25845	1.2.83	Yes
spring-boot-starter-logging@1.5.1.RELEASE ├── *logback-classic@1.1.9* └── logback-core@1.1.9 ⬅CVE-2021-42550	CVE-2021-42550	1.2.9	
log4j-core@2.9.1 └── log4j-api@2.9.1 ⬅CVE-2021-44228	CVE-2021-44228	2.13.2	Yes

Recommendation

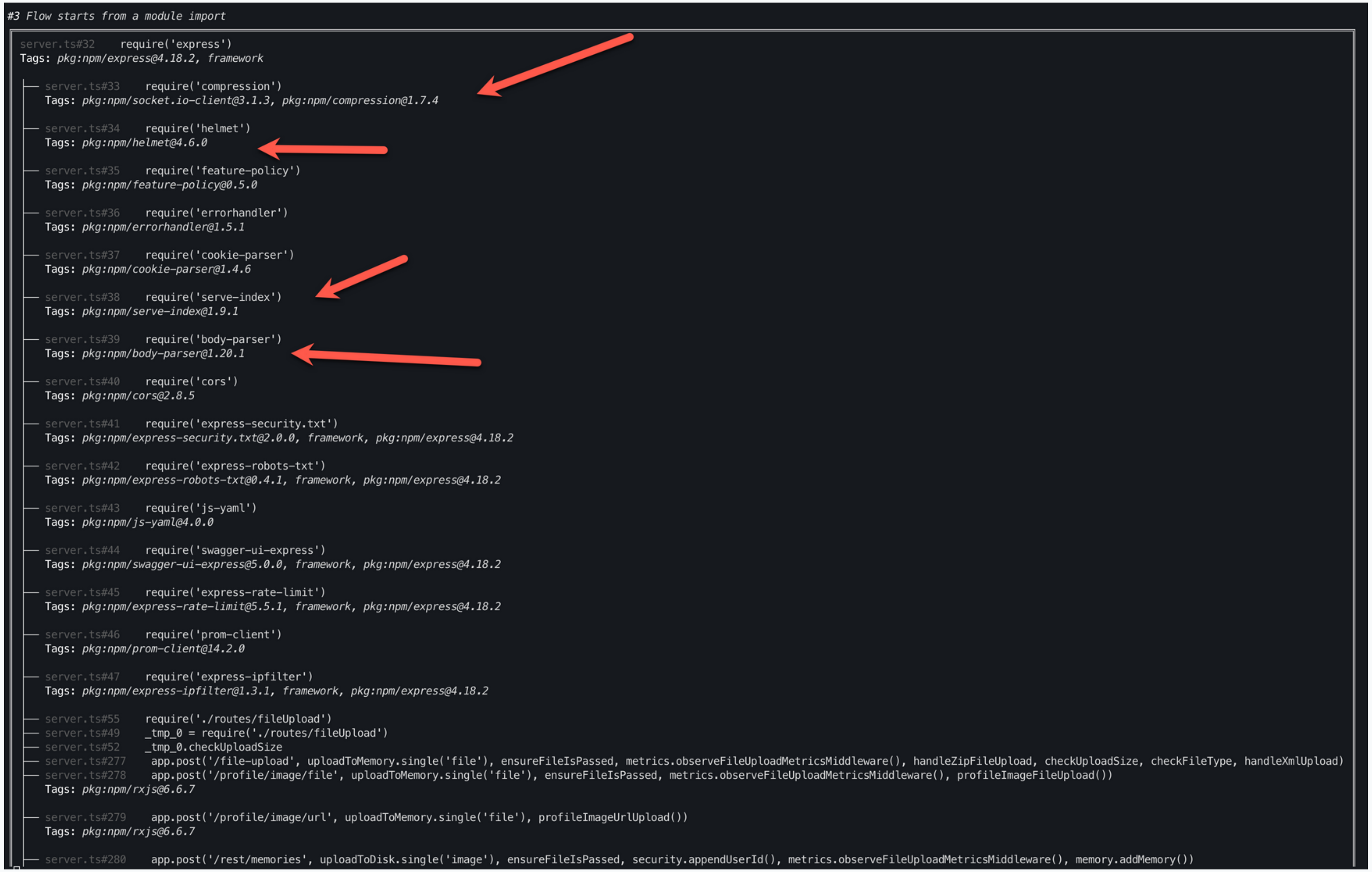
👉 Prioritize the 3 reachable vulnerabilities with known exploits.
You can remediate 140 vulnerabilities by updating the packages using the fix version 👍



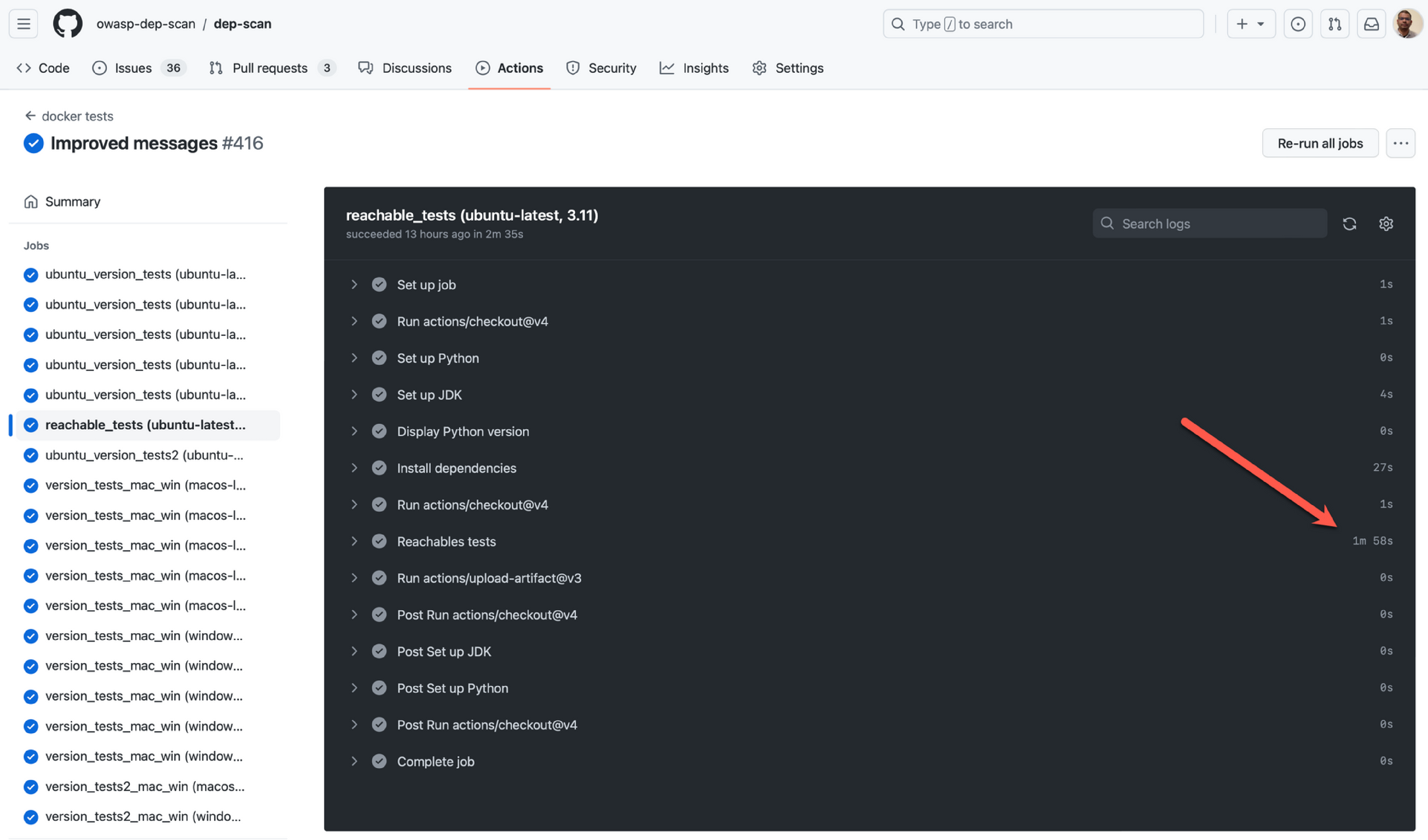
```
                          Dependency Scan Results (JAVA)
┌──────────────────────────────────────┬────────────────────┬───────────┬──────────┬───────┐
│ Dependency Tree                      │ Insights           │ Fix Version │ Severity │ Score │
├──────────────────────────────────────┼────────────────────┼───────────┼──────────┼───────┤
│ alpine-infra@2.2.4-SNAPSHOT          │ 🎯 Used in 18 locations │      │ MEDIUM   │   4.7 │
│ ├── jjwt@0.9.1                       │                    │           │          │       │
│ └── jackson-databind@2.15.2 ⬅CVE-2023-35116 │             │           │          │       │
└──────────────────────────────────────┴────────────────────┴───────────┴──────────┴───────┘

┌────────────────────────────────── Recommendation ──────────────────────────────────┐
│ ✅ No package requires immediate attention since the major vulnerabilities are found only in dev packages and indirect dependencies. │
└─────────────────────────────────────────────────────────────────────────────────────┘

                                                        Proactive Measures

Below are the top reachable packages identified by depscan. Setup alerts and notifications to actively monitor these packages for new vulnerabilities and exploits.

                              Top Reachable Packages
┌──────────────────────────────────────────────────────────┬─────────────────┐
│ Package                                                  │ Reachable Flows │
├──────────────────────────────────────────────────────────┼─────────────────┤
│ pkg:maven/us.springett/alpine-infra@2.2.4-SNAPSHOT?type=jar │ 459          │
│ pkg:maven/org.datanucleus/javax.jdo@3.2.1?type=jar        │ 278             │
│ pkg:maven/jakarta.ws.rs/jakarta.ws.rs-api@2.1.6?type=jar  │ 261             │
└──────────────────────────────────────────────────────────┴─────────────────┘

                                                         Reachable Flows

Below are some reachable flows identified by depscan. Use the provided tips to improve the securability of your application.

#1 Method getPolicies ↩ can be used to reach 3 packages.
┌──────────────────────────────────────────────────────────────────────────────────┐
│ org/dependencytrack/resources/v1/PolicyResource.java#61    getPolicies() ↩
│ Tags: framework-input
│
│ ├── org/dependencytrack/resources/v1/PolicyResource.java#74    this.getAlpineRequest()
│ ├── org/dependencytrack/persistence/QueryManager.java#144    <init>(request) ↩
│ │   Tags: pkg:maven/us.springett/alpine-infra@2.2.4-SNAPSHOT?type=jar, framework, api
│ │
│ ├── org/dependencytrack/persistence/QueryManager.java#146    this.request
│ ├── org/dependencytrack/persistence/QueryManager.java#580    getPolicies() ↩
│ ├── org/dependencytrack/persistence/QueryManager.java#228    getPolicyQueryManager() ↩
│ ├── org/dependencytrack/persistence/QueryManager.java#229    this.policyQueryManager
│ ├── org/dependencytrack/persistence/QueryManager.java#232    this.policyQueryManager
│ ├── org/dependencytrack/persistence/QueryManager.java#581    this.getPolicyQueryManager()
│ ├── org/dependencytrack/persistence/PolicyQueryManager.java#63    getPolicies() ↩
```



```
│ Tags: pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar, framework, tomcat, framework-input
│
│ ├── org/joychou/controller/Jsonp.java#122    this.cookieCsrfTokenRepository
│ └── org/joychou/controller/Jsonp.java#129    csrfToken.toString()
└──────────────────────────────────────────────────────────────────────────────────┘
                                Reachable Packages:
        pkg:maven/org.springframework.security/spring-security-crypto@4.2.1.RELEASE?type=jar
           pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar

#5 Method emptyReferer ↩ can be used to reach 2 packages.
┌──────────────────────────────────────────────────────────────────────────────────┐
│ org/joychou/controller/Jsonp.java#53    emptyReferer() ↩
│ Tags: framework-input
│
│ ├── org/joychou/controller/Jsonp.java#59    this.callback
│ ├── org/joychou/util/LoginUtils.java#13    getUserInfo2JsonStr(request) ↩
│ │   Tags: pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar, framework, tomcat
│ │
│ ├── org/joychou/util/LoginUtils.java#14    request.getUserPrincipal()
│ ├── org/joychou/util/LoginUtils.java#15    principal.getName()
│ ├── org/joychou/util/LoginUtils.java#19    JSON.toJSONString(m)
│ ├── org/joychou/controller/Jsonp.java#60    LoginUtils.getUserInfo2JsonStr(request)
│ ├── org/joychou/util/WebUtils.java#30    json2Jsonp(jsonStr) ↩
│ ├── org/joychou/util/WebUtils.java#31    HtmlUtils.htmlEscape(callback) + "(" + jsonStr + ")"
│ └── org/joychou/controller/Jsonp.java#60    WebUtils.json2Jsonp(callback, LoginUtils.getUserInfo2JsonStr(request))
└──────────────────────────────────────────────────────────────────────────────────┘
          ▫ Check if the mitigation(s) used in this flow is valid and appropriate for your security requirements.
                                Reachable Packages:
                    pkg:maven/com.alibaba/fastjson@1.2.24?type=jar
           pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar

#6 Parameter filepath ↩ to the method getImageSec can be used to reach this package.
┌──────────────────────────────────────────────────────────────────────────────────┐
│ org/joychou/controller/PathTraversal.java#30    getImageSec(filepath) ↩
│ Tags: framework-input
│
│ ├── org/joychou/security/SecurityUtil.java#178    pathFilter(filepath) ↩
│ ├── org/joychou/controller/PathTraversal.java#38    getImgBase64(imgFile) ↩
│ ├── org/joychou/controller/PathTraversal.java#45    Paths.get(imgFile)
│ ├── org/joychou/controller/PathTraversal.java#46    Base64.encodeBase64(data)
│ └── org/joychou/controller/PathTraversal.java#35    this.getImgBase64(filepath)
└──────────────────────────────────────────────────────────────────────────────────┘
                                Reachable Packages:
            pkg:maven/commons-collections/commons-collections@3.1?type=jar

#7 Parameter request ↩ to the method appInfo can be used to reach 2 packages.
┌──────────────────────────────────────────────────────────────────────────────────┐
│ org/joychou/controller/Index.java#26    appInfo(request) ↩
│ Tags: pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar, framework, tomcat, framework-input
│
│ ├── org/joychou/controller/Index.java#27    request.getUserPrincipal()
│ ├── org/joychou/controller/Index.java#35    JSON.VERSION
│ └── org/joychou/controller/Index.java#38    JSON.toJSONString(m)
└──────────────────────────────────────────────────────────────────────────────────┘
                                Reachable Packages:
                    pkg:maven/com.alibaba/fastjson@1.2.24?type=jar
           pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.5.85?type=jar

#8 Parameter request ↩ to the method proxy can be used to reach this package.
```



```
#3 Flow starts from a module import

  server.ts#32    require('express')
  Tags: pkg:npm/express@4.18.2, framework

  ├── server.ts#33    require('compression')
      Tags: pkg:npm/socket.io-client@3.1.3, pkg:npm/compression@1.7.4

  ├── server.ts#34    require('helmet')
      Tags: pkg:npm/helmet@4.6.0

  ├── server.ts#35    require('feature-policy')
      Tags: pkg:npm/feature-policy@0.5.0

  ├── server.ts#36    require('errorhandler')
      Tags: pkg:npm/errorhandler@1.5.1

  ├── server.ts#37    require('cookie-parser')
      Tags: pkg:npm/cookie-parser@1.4.6

  ├── server.ts#38    require('serve-index')
      Tags: pkg:npm/serve-index@1.9.1

  ├── server.ts#39    require('body-parser')
      Tags: pkg:npm/body-parser@1.20.1

  ├── server.ts#40    require('cors')
      Tags: pkg:npm/cors@2.8.5

  ├── server.ts#41    require('express-security.txt')
      Tags: pkg:npm/express-security.txt@2.0.0, framework, pkg:npm/express@4.18.2

  ├── server.ts#42    require('express-robots-txt')
      Tags: pkg:npm/express-robots-txt@0.4.1, framework, pkg:npm/express@4.18.2

  ├── server.ts#43    require('js-yaml')
      Tags: pkg:npm/js-yaml@4.0.0

  ├── server.ts#44    require('swagger-ui-express')
      Tags: pkg:npm/swagger-ui-express@5.0.0, framework, pkg:npm/express@4.18.2

  ├── server.ts#45    require('express-rate-limit')
      Tags: pkg:npm/express-rate-limit@5.5.1, framework, pkg:npm/express@4.18.2

  ├── server.ts#46    require('prom-client')
      Tags: pkg:npm/prom-client@14.2.0

  ├── server.ts#47    require('express-ipfilter')
      Tags: pkg:npm/express-ipfilter@1.3.1, framework, pkg:npm/express@4.18.2

  ├── server.ts#55    require('./routes/fileUpload')
  ├── server.ts#49    _tmp_0 = require('./routes/fileUpload')
  ├── server.ts#52    _tmp_0.checkUploadSize
  ├── server.ts#277    app.post('/file-upload', uploadToMemory.single('file'), ensureFileIsPassed, metrics.observeFileUploadMetricsMiddleware(), handleZipFileUpload, checkUploadSize, checkFileType, handleXmlUpload)
  ├── server.ts#278    app.post('/profile/image/file', uploadToMemory.single('file'), ensureFileIsPassed, metrics.observeFileUploadMetricsMiddleware(), profileImageFileUpload())
      Tags: pkg:npm/rxjs@6.6.7

  ├── server.ts#279    app.post('/profile/image/url', uploadToMemory.single('file'), profileImageUrlUpload())
      Tags: pkg:npm/rxjs@6.6.7

  ├── server.ts#280    app.post('/rest/memories', uploadToDisk.single('image'), ensureFileIsPassed, security.appendUserId(), metrics.observeFileUploadMetricsMiddleware(), memory.addMemory())
```



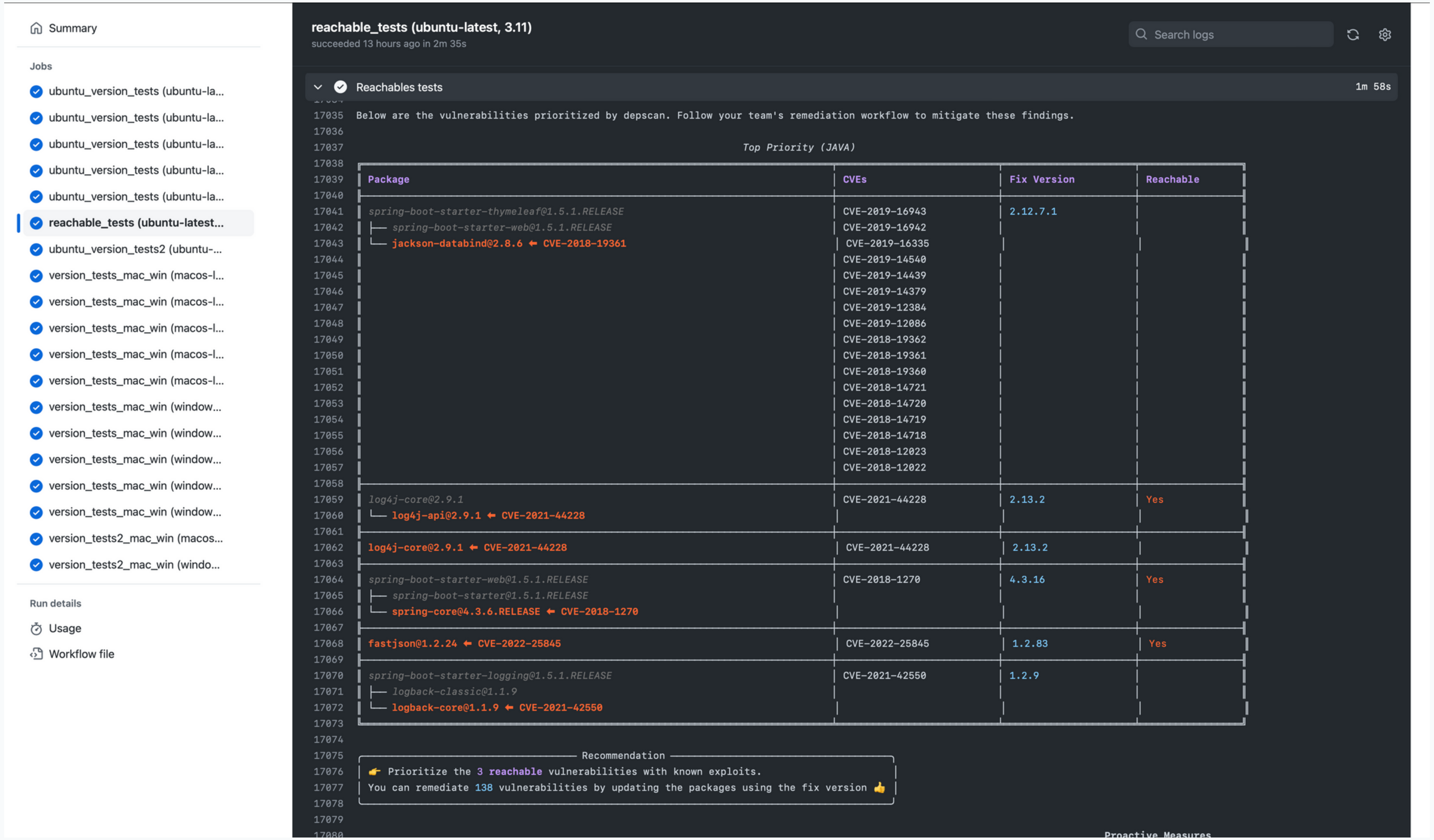
Improved messages #416

Jobs

- ubuntu_version_tests (ubuntu-la...
- ubuntu_version_tests (ubuntu-la...
- ubuntu_version_tests (ubuntu-la...
- ubuntu_version_tests (ubuntu-la...
- ubuntu_version_tests (ubuntu-la...
- reachable_tests (ubuntu-latest...
- ubuntu_version_tests2 (ubuntu-...
- version_tests_mac_win (macos-l...
- version_tests_mac_win (macos-l...
- version_tests_mac_win (macos-l...
- version_tests_mac_win (macos-l...
- version_tests_mac_win (macos-l...
- version_tests_mac_win (window...
- version_tests_mac_win (window...
- version_tests_mac_win (window...
- version_tests_mac_win (window...
- version_tests_mac_win (window...
- version_tests2_mac_win (macos...
- version_tests2_mac_win (windo...

reachable_tests (ubuntu-latest, 3.11)
succeeded 13 hours ago in 2m 35s

```
Set up job                          1s
Run actions/checkout@v4             1s
Set up Python                       0s
Set up JDK                          4s
Display Python version              0s
Install dependencies               27s
Run actions/checkout@v4             1s
Reachables tests               1m 58s
Run actions/upload-artifact@v3      0s
Post Run actions/checkout@v4        0s
Post Set up JDK                     0s
Post Set up Python                  0s
Post Run actions/checkout@v4        0s
Complete job                        0s
```



Summary
Jobs
ubuntu_version_tests (ubuntu-la...
ubuntu_version_tests (ubuntu-la...
ubuntu_version_tests (ubuntu-la...
ubuntu_version_tests (ubuntu-la...
ubuntu_version_tests (ubuntu-la...
reachable_tests (ubuntu-latest...
ubuntu_version_tests2 (ubuntu-...
version_tests_mac_win (macos-l...
version_tests_mac_win (macos-l...
version_tests_mac_win (macos-l...
version_tests_mac_win (macos-l...
version_tests_mac_win (macos-l...
version_tests_mac_win (window...
version_tests_mac_win (window...
version_tests_mac_win (window...
version_tests_mac_win (window...
version_tests_mac_win (window...
version_tests2_mac_win (macos...
version_tests2_mac_win (windo...
Run details
Usage
Workflow file
Search logs

reachable_tests (ubuntu-latest, 3.11)
succeeded 13 hours ago in 2m 35s

Reachables tests 1m 58s

```
Below are the vulnerabilities prioritized by depscan. Follow your team's remediation workflow to mitigate these findings.

                                                 Top Priority (JAVA)

┌──────────────────────────────────────────────────┬────────────────┬──────────────┬───────────┐
│ Package                                          │ CVEs           │ Fix Version  │ Reachable │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ spring-boot-starter-thymeleaf@1.5.1.RELEASE      │ CVE-2019-16943 │ 2.12.7.1     │           │
│ ├── spring-boot-starter-web@1.5.1.RELEASE        │ CVE-2019-16942 │              │           │
│ └── jackson-databind@2.8.6 ⬅ CVE-2018-19361      │ CVE-2019-16335 │              │           │
│                                                  │ CVE-2019-14540 │              │           │
│                                                  │ CVE-2019-14439 │              │           │
│                                                  │ CVE-2019-14379 │              │           │
│                                                  │ CVE-2019-12384 │              │           │
│                                                  │ CVE-2019-12086 │              │           │
│                                                  │ CVE-2018-19362 │              │           │
│                                                  │ CVE-2018-19361 │              │           │
│                                                  │ CVE-2018-19360 │              │           │
│                                                  │ CVE-2018-14721 │              │           │
│                                                  │ CVE-2018-14720 │              │           │
│                                                  │ CVE-2018-14719 │              │           │
│                                                  │ CVE-2018-14718 │              │           │
│                                                  │ CVE-2018-12023 │              │           │
│                                                  │ CVE-2018-12022 │              │           │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ log4j-core@2.9.1                                 │ CVE-2021-44228 │ 2.13.2       │ Yes       │
│ └── log4j-api@2.9.1 ⬅ CVE-2021-44228             │                │              │           │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ log4j-core@2.9.1 ⬅ CVE-2021-44228                │ CVE-2021-44228 │ 2.13.2       │           │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ spring-boot-starter-web@1.5.1.RELEASE            │ CVE-2018-1270  │ 4.3.16       │ Yes       │
│ ├── spring-boot-starter@1.5.1.RELEASE            │                │              │           │
│ └── spring-core@4.3.6.RELEASE ⬅ CVE-2018-1270    │                │              │           │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ fastjson@1.2.24 ⬅ CVE-2022-25845                 │ CVE-2022-25845 │ 1.2.83       │ Yes       │
├──────────────────────────────────────────────────┼────────────────┼──────────────┼───────────┤
│ spring-boot-starter-logging@1.5.1.RELEASE        │ CVE-2021-42550 │ 1.2.9        │           │
│ ├── logback-classic@1.1.9                        │                │              │           │
│ └── logback-core@1.1.9 ⬅ CVE-2021-42550          │                │              │           │
└──────────────────────────────────────────────────┴────────────────┴──────────────┴───────────┘

╭──────────────────────── Recommendation ─────────────────────────╮
│ 👉 Prioritize the 3 reachable vulnerabilities with known exploits. │
│ You can remediate 138 vulnerabilities by updating the packages using the fix version 👍 │
╰──────────────────────────────────────────────────────────────────╯

                                                                              Proactive Measures
```