



Integrating OpenSSF Scorecard and Other Health Metadata

Community Meeting – 2025-08-06

Florian Schmidt

Technical University of Munich

Fraunhofer AISEC, Rohde & Schwarz

About me

- Master's studies in Computer Science at Technical University of Munich
- Working on thesis in software supply chain security affiliated with Fraunhofer AISEC and Rohde & Schwarz
- Overarching goal:
 - Provide developers with a better basis for decision-making in dependency selection
 - Equip organizations with a better baseline/quality gate for security posture of projects

Call for Guest Presentations

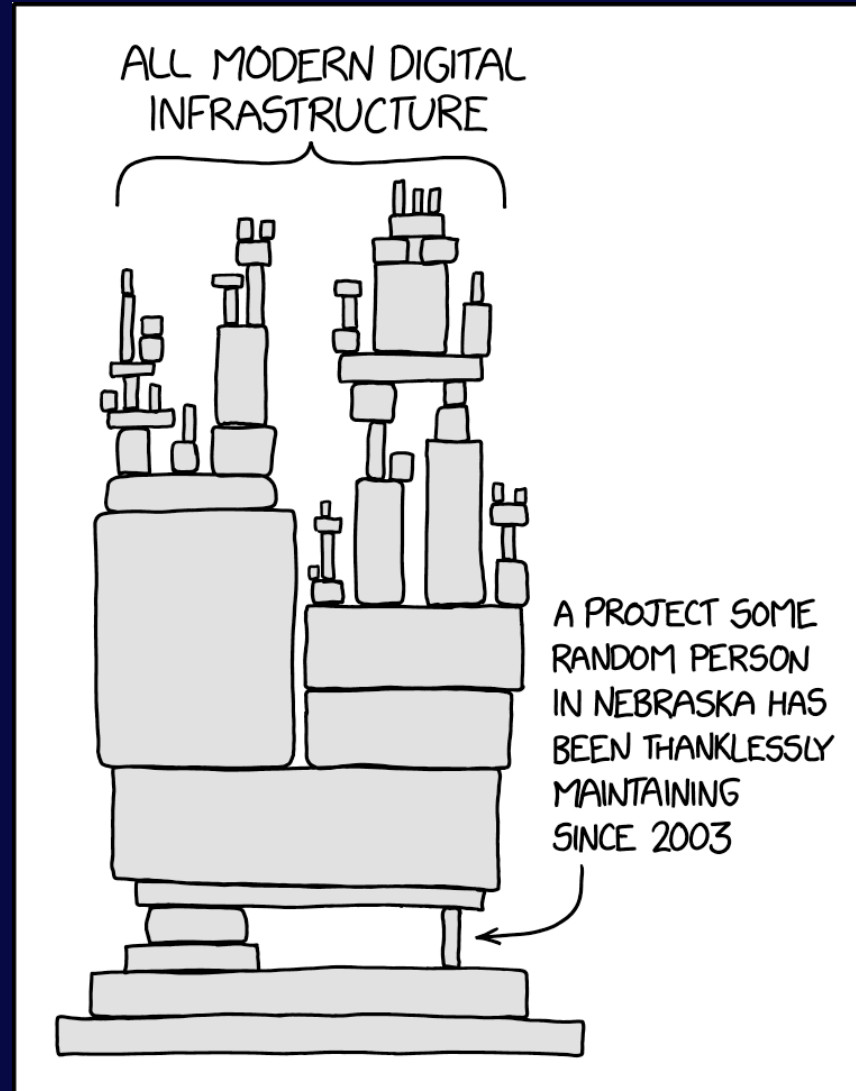
- ➔ ● Want to brag about the cool DT setup you've built?
 - Want to vent about what needs improvement?
- ➔ ● Want to get input on DT-related designs?
 - Want to propose changes?

We'd love to host you here!



Slide shamelessly stolen from
Community Meeting July 2025

Motivation



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

Goals

- Enrich available component **metadata** with **activity** and **maintenance** insights
 - Add support for **OpenSSF Scorecard** scores in DT ([#3048](#))
 - Retrieve key project health metrics
(contributors, commit activity, bus factor, issue count/age, ...)
- Introduce **health** data in CEL policy environment
 - Enables rich combinations of health and vulnerability data
 - Supports context-aware dependency assessments
(think: critical vulnerability and project is not actively maintained)

New Project Health Data

- stars, forks, contributors, commitFrequencyWeekly, openIssues, openPRs, lastCommitDate, busFactor, hasReadme, hasCodeOfConduct, hasSecurityPolicy, dependents, files, isRepoArchived, avgIssueAgeDays
- scoreCardScore, scoreCardReferenceVersion, scoreCardTimestamp
- scoreCardChecks.
 - ...packaging, ...tokenPermissions, ...codeReview, ...pinnedDependencies, ...binaryArtifacts, ...dangerousWorkflow, ...maintained, ...ciiBestPractices, ...securityPolicy, ...fuzzing, ...license, ...signedReleases, ...branchProtection, ...sast, ...vulnerabilities, ...ciTests, ...contributors, ...dependencyUpdateTool, ...webhooks

Example Policies

Unmaintained/Stale & Vulnerable

```
(health.scoreCardChecks.maintained <= 5.0 || component.compare_age(">=",  
"P180D")) && vulns.exists(vuln, vuln.severity in ["CRITICAL", "HIGH"])
```

Low Activity & Old Issues

```
health.avgIssueAgeDays > 365.0 && health.commitFrequencyWeekly <= 0.5
```

Abandoned but Widely Used

```
(now - health.lastCommitDate) > duration('8760h') && health.dependents > 100
```

Demo Time

🌟 Live Demo 🌟



OWASP WebGoat

2025.3

LATEST VERSION

8

12

3

0

0

View Details >

-  Overview
-  Components 202
-  Services 0
-  Dependency Graph 1
-  Audit Vulnerabilities 32 32
-  Exploit Predictions 32
-  Policy Violations 197 143 51 3

+ Add Component

− Remove Component

⬆ Upload BOM



⬇ Download BOM

⬇ Download Components

☐ Outdated only

☐ Direct only

Search



| <input type="checkbox"/> | Component | Version | Published | Group | Internal | License | Risk Score | Scorecard | Vulnerabilities |
|--------------------------|------------------|---|-------------|----------------------------|----------|---------|------------|-----------|-----------------|
| <input type="checkbox"/> | log4j-to-slf4j | 2.24.3 | 10 Dec 2024 | org.apache.logging.log4j | | | 0 | 9.1 | 0 |
| <input type="checkbox"/> | log4j-api | 2.24.3 | 10 Dec 2024 | org.apache.logging.log4j | | | 0 | 9.1 | 0 |
| <input type="checkbox"/> | guava | 33.4.8-jre | 14 Apr 2025 | com.google.guava | | | 0 | 8.7 | 0 |
| <input type="checkbox"/> | failureaccess | 1.0.3 | 19 Mar 2025 | com.google.guava | | | 0 | 8.7 | 0 |
| <input type="checkbox"/> | listenablefuture | 9999.0-empty-to-avoid-conflict-with-guava | 11 Sep 2018 | com.google.guava | | | 0 | 8.7 | 0 |
| <input type="checkbox"/> | gson | 2.11.0 | 19 May 2024 | com.google.code.gson | | | 5 | 8.0 | 0 |
| <input type="checkbox"/> | jackson-databind | 2.18.3 | 1 Mar 2025 | com.fasterxml.jackson.core | | | 0 | 7.9 | 0 |
| <input type="checkbox"/> | commons-codec | 1.17.2 | 28 Dec 2024 | commons-codec | | | 0 | 7.9 | 0 |
| <input type="checkbox"/> | mockito-core | 5.14.2 | 15 Oct 2024 | org.mockito | | | 0 | 7.5 | 0 |



OWASP WebGoat

▼ 2025.3

LATEST VERSION

8

12

3

0


0


View Details >


-  Overview
-  Components 202
-  Services 0
-  Dependency Graph 1
-  Audit Vulnerabilities 32 32
-  Exploit Predictions 32
-  Policy Violations 197 143 51 3

+ Add Component

− Remove Component

 Upload BOM



 Download BOM ▼























 Download Components ▼

☐ × Outdated only

☐ × Direct only

Search



| <input type="checkbox"/> | Component |  | Version |  | Published |  | Group | Internal | License | Risk Score |  | Scorecard | Vulnerabilities |
|--------------------------|----------------------|---|---------|---|-------------|---|-------------------|----------|---------|------------|---|-----------|-----------------|
| <input type="checkbox"/> | jquery |  | 3.7.1 |  | 29 Aug 2023 | | org.webjars | | | 0 | | 2.6 | <div>0</div> |
| <input type="checkbox"/> | javax.activation-api |  | 1.2.0 |  | 7 Sep 2017 | | javax.activation | | | 0 | | 2.7 | <div>0</div> |
| <input type="checkbox"/> | aspectjweaver |  | 1.9.23 |  | 13 Mar 2025 | | org.aspectj | | | 0 | | 2.9 | <div>0</div> |
| <input type="checkbox"/> | jaxb-api |  | 2.3.1 |  | 12 Sep 2018 | | javax.xml.bind | | | 0 | | 3.0 | <div>0</div> |
| <input type="checkbox"/> | dirgra |  | 0.5 |  | 21 Mar 2024 | | org.jruby | | | 0 | | 3.0 | <div>0</div> |
| <input type="checkbox"/> | options |  | 1.6 |  | 6 Mar 2021 | | com.headius | | | 0 | | 3.0 | <div>0</div> |
| <input type="checkbox"/> | backport9 |  | 1.13 |  | 23 May 2023 | | com.headius | | | 0 | | 3.0 | <div>0</div> |
| <input type="checkbox"/> | angus-activation |  | 2.0.2 |  | 15 Feb 2024 | | org.eclipse.angus | | | 0 | | 3.2 | <div>0</div> |
| <input type="checkbox"/> | javaniotcproxy |  | 1.6 |  | 16 Apr 2020 | | com.github.terma | | | 0 | | 3.2 | <div>0</div> |

org.webjars ▶ jquery ▶ 3.7.1

EXTERNAL

0

0

0

0

0

View Details

Overview

Vulnerabilities 0

Health 2.6

Component Health Metrics

Package URL

pkg:maven/org.webjars/jquery@3.7.1

Stars

22

Forks

26

Contributors

3

Weekly Commits

0.27

Open Issues

4

Open PRs

1

Last Commit

29 Aug 2023 at 21:45:11

Bus Factor

1

Known Dependents

455

August 6, 2025

Dependency-Track | OpenSSF Scorecard Integration | Florian Schmidt

11



Files

4

Scorecard Score

2.6

Average Issue Age (days)

2806

Archived

No

Repository Features

- Readme: ✓
- Code of Conduct: ✗
- Security Policy: ✗

Scorecard Checks

• Token-Permissions: -1/10

Determines if the project's workflows follow the principle of least privilege.

Reason: No tokens found

[Read more](#)

• SAST: 0/10

Determines if the project uses static code analysis.

Reason: no SAST tool detected


[Read more](#)


• Dangerous-Workflow: -1/10


Determines if the project's GitHub Action workflows avoid dangerous patterns.

Reason: no workflows found

[Read more](#)


 Policies 9

 License Groups 4

 Vulnerability Policies 0

+ Create Policy

Search



| | |
|------|--|
| FAIL | (P1) Malicious Package |
| FAIL | (P2) Unmaintained / Stale & Vulnerable |
| WARN | (P3) Bad Scorecard Score |
| WARN | (P4) Low Activity & Old Issues |
| WARN | (P5) Abandoned but Widely Used |
| FAIL | (P6) Archived |
| INFO | (P7) Widely Used & Low Bus Factor |
| INFO | (P8) Unpopular & Young or Niche |
| INFO | (P9) Single Maintainer Risk |

Showing 1 to 9 of 9 rows

 Policies 9

 License Groups 4

 Vulnerability Policies 0

+ Create Policy

Search



- FAIL (P1) Malicious Package
- FAIL (P2) Unmaintained / Stale & Vulnerable

Name *

(P2) Unmaintained / Stale & Vulnerable

✓

Operator *

Any

✓

Violation State *

Fail

✓

Conditions


Expression


✓

```
1 (health.scoreCardChecks.maintained <= 5.0 || component.compare_age(">=", "P180D")) &&
  vulns.exists(vuln, vuln.severity in ["CRITICAL", "HIGH"])
```

Security

⌵





Limit To

Delete Policy

- WARN (P3) Bad Scorecard Score
- WARN (P4) Low Activity & Old Issues
- WARN (P5) Abandoned but Widely Used

Filters

Clear all



Projects

☐ Show inactive projects

Analysis Status

☐ Show suppressed violations

Violation State

☐ Fail

☐ Warn

☐ Info

Risk Type

☐ License

☐ Security

☐ Operational


Analysis State


☐ Not Set

☐ Rejected

☐ Approved

Occurred On


 From

 To

Text Search

Search in:

☒ Policy Name

| State | Risk Type | Policy Name | Component | Project Name | Occurred On | Analysis | Suppressed | License |
|-------|-----------|--|---|----------------------|-------------|----------|------------|---------|
| FAIL | Security | (P2) Unmaintained / Stale & Vulnerable | xstream 1.4.5  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |

Showing 1 to 1 of 1 rows

Filters

Clear all

Projects

☐ Show inactive projects

Analysis Status

☐ Show suppressed violations

Violation State

☐ Fail

☐ Warn

☐ Info

Risk Type

☐ License

☐ Security

☐ Operational

Analysis State

☐ Not Set

☐ Rejected

☐ Approved

Occurred On

Text Search

Search in:


☒ Policy Name


Filters

Clear all

- Projects
- ☐ Show inactive projects
- Analysis Status
- ☐ Show suppressed violations
- Violation State
- ☐ Fail
- ☐ Warn
- ☐ Info
- Risk Type
- ☐ License
- ☐ Security
- ☐ Operational
- Analysis State
- ☐ Not Set
- ☐ Rejected
- ☐ Approved

Occurred On

 From

 To

Text Search

Search

Search in:

☒ Policy Name

State

⬆

⬆

Risk Type

⬆

⬆

Policy Name

⬆

⬆

Component

⬆

⬆

Project Name

⬆

⬆

Occurred On

⬇

⬇

Analysis

⬆

⬆

Suppressed











⬆

⬆

License

⬆

⬆

| | | | | | | | | | |
|------|----------|--------------------------------|------------------------------|---|----------------------|------------|---|--|--|
| WARN | Security | (P5) Abandoned but Widely Used | cglib-nodep 3.3.0 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | jquery 3.7.1 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | webjars-locator-core 0.59 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | jcip-annotations 1.0-1 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | options 1.6 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | jzlib 1.1.5 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | backport9 1.13 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | crac 1.5.0 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | istack-commons-runtime 4.1.2 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| WARN | Security | (P5) Abandoned but Widely Used | jakarta.inject-api 2.0.1 |  | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |

Showing 1 to 10 of 13 rows

10 rows per page

<

1

2

>

August 6, 2025

Dependency-Track | OpenSSF Scorecard Integration | Florian Schmidt

17

Filters

Clear all

Projects

☐ Show inactive projects

Analysis Status

☐ Show suppressed violations

Violation State

☐ Fail

☐ Warn

☐ Info

Risk Type

☐ License

☐ Security

☐ Operational

Analysis State

☐ Not Set

☐ Rejected

☐ Approved

Occurred On

From

To

Text Search

Search

Search in:

☒ Policy Name

| State | Risk Type | Policy Name | Component | Project Name | Occurred On | Analysis | Suppressed | License |
|-------|-----------|-----------------------------|------------------------------|----------------------|-------------|----------|------------|---------|
| INFO | Security | (P9) Single Maintainer Risk | mockito-core 5.14.2 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | objenesis 3.3 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | mockito-junit-jupiter 5.14.2 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | wiremock-standalone 3.13.0 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | rest-assured 5.5.1 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | commons-codec 1.17.2 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | json-path 5.5.1 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | rest-assured-common 5.5.1 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | xml-path 5.5.1 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |
| INFO | Security | (P9) Single Maintainer Risk | playwright 1.51.0 | OWASP WebGoat 2025.3 | 2 Aug 2025 | - | | |

Technical Details (1/2)

for more information:
see [ADR #007](#) in flodt/hyades

- **Proposed Changes**

- Expansion of repository-meta-analyzer service with integration for health metadata
 - OpenSSF Scorecard + known dependents from deps.dev API
 - Source code repository from deps.dev API...
 - ...then contributor statistics + repository metrics from GitHub API
- Persist in HEALTH_META_COMPONENT, mapped by PURL coordinates, provide API endpoints
- Retrieve and map new data to component in CEL engine
 - Populate health variable
 - Skip evaluation if required fields are not available (no automatic failure)

Technical Details (2/2)

for more information:
see [ADR #007](#) in flodt/hyades

- Potential **Limitations**

- Currently limited to components listed with **deps.dev** project and on **GitHub**
 - **Authenticated GitHub API** access required (needs to be registered in DT repository settings)
 - High processing/retrieval **time**, especially with certain GitHub API endpoints
- Lacking **data quality** in some cases
- Not all metrics are available for all components (duh)
- Same Kafka dependence as the rest of repository-meta-analyzer

Source Code



flodt/hyades-apiserver



flodt/hyades



flodt/hyades-frontend

Summary & Contact

- Enrich **metadata** with **OpenSSF Scorecard** and other **health** and **activity** metadata
- Retrieve data from external **sources**: deps.dev/GitHub API
- Provide this new data to **CEL policy engine**
- Enable rich **combinations** of health and vulnerability data for better dependency assessment



linkedin.com/in/flodt