



Universität Augsburg
Fakultät für Angewandte
Informatik

Seminar Softwareentwicklung mit Dev(Sec)Ops:

Compliance: License-Checker

Jonas Kell

Augsburg, 26+27.07.2021

Situation

- Kleines Unternehmen in der Webentwicklung

Situation

- Kleines Unternehmen in der Webentwicklung
- Frontend **Javascript mit NPM** (Hauptfokus in diesem Referat)
- Backend **PHP mit Laravel und Composer**
- **GitLab** wird bereits als Versionskontrollsystem eingesetzt

Situation

- Kleines Unternehmen in der Webentwicklung
- Frontend **Javascript mit NPM** (Hauptfokus in diesem Referat)
- Backend **PHP mit Laravel und Composer**
- **GitLab** wird bereits als Versionskontrollsystem eingesetzt
- Keine Rechtsabteilung (wie Hilft uns CI/CD, wenn wir keinen Plan von Recht haben)

Situation

- Kleines Unternehmen in der Webentwicklung
- Frontend **Javascript mit NPM** (Hauptfokus in diesem Referat)
- Backend **PHP mit Laravel und Composer**
- **GitLab** wird bereits als Versionskontrollsystem eingesetzt
- Keine Rechtsabteilung (wie Hilft uns CI/CD, wenn wir keinen Plan von Recht haben)
- Raum soll davon überzeugt werden, das License-Monitoring an sich wichtig ist
- Raum soll informiert werden, was für License-Monitoring Angebote es gibt
- Raum soll zwischen mehreren präsentierten Tools für das Monitoring entscheiden

Agenda

- 1 Warum Lizenzen? - Compliance
- 2 Warum muss man aufpassen?
- 3 Was für (OpenSource) Lizenzen gibt es? / Wie interagieren Lizenzen?
- 4 Vorstellung & Vergleich CI/CD – Tools
- 5 Demonstration: Gitlab License-Compliance
- 6 Demonstration: OpenSource Wrapper: NPM-License-Compliance

Disclaimer

Warum Lizenzen? - Compliance

Achtung:

Ich bin kein Anwalt und das ist keine Rechtsberatung!

Die nachfolgenden Folien dienen lediglich als Übersicht und Information zu einem rechtlichen Thema.

Caution:

I'm no lawyer and this is not intended to constitute legal advice!

This presentation is for informational purposes only.



Compliance

Warum Lizenzen? - Compliance

- „Compliance beschreibt im rechtlichen Bereich die Einhaltung aller gesetzlichen Bestimmungen sowie interner Richtlinien durch Unternehmen und ihre Mitarbeiter.“ [2]
- „Rechtstreue“ bzw. „Regelkonformität“
 - Privates Recht (v.a. Handelsrecht) [2]
 - Öffentliches Recht (v.a. Strafrecht) [3]
- [4]

Compliance

Warum Lizenzen? - Compliance

- „Compliance beschreibt im rechtlichen Bereich die Einhaltung aller gesetzlichen Bestimmungen sowie interner Richtlinien durch Unternehmen und ihre Mitarbeiter.“ [2]
- „Rechtstreue“ bzw. „Regelkonformität“
 - Privates Recht (v.a. Handelsrecht) [2]
 - Öffentliches Recht (v.a. Strafrecht) [3]
- Aufbau interner Regeln zur Unterstützung der Mitarbeiter bei der Einhaltung der Vorgaben [4]



[3]

Lizenzen

Warum Lizenzen? - Compliance

- „Software-Lizenzen regeln die Konditionen, unter denen Software eingesetzt, erweitert, und verbreitet werden darf. Insbesondere für kommerzielle Software stellen sich hier grundsätzliche Fragen.“ [5]

[5]

[6]

[5]

Lizenzen

Warum Lizenzen? - Compliance

- „Software-Lizenzen regeln die Konditionen, unter denen Software eingesetzt, erweitert, und verbreitet werden darf. Insbesondere für kommerzielle Software stellen sich hier grundsätzliche Fragen.“ [5]
- Closed-Source [5]
 - Quellcode ist nicht frei Zugänglich
 - Nicht zwangsweise kostenpflichtig, aber meist kommerzielle Lizenz
 - Weiterverbreitung meist in Ordnung, Modifikation meistens kritisch

Man weiß meist, auf was man sich einlässt.

[6]

[5]

Lizenzen

Warum Lizenzen? - Compliance

- „Software-Lizenzen regeln die Konditionen, unter denen Software eingesetzt, erweitert, und verbreitet werden darf. Insbesondere für kommerzielle Software stellen sich hier grundsätzliche Fragen.“ [5]
- Closed-Source [5]
 - Quellcode ist nicht frei Zugänglich
 - Nicht zwangsweise kostenpflichtig, aber meist kommerzielle Lizenz
 - Weiterverbreitung meist in Ordnung, Modifikation meistens kritisch
- Open-Source [6]
 - Quellcode ist für jeden frei zugänglich
 - Monetarisierungsmodelle:
 - Komplett frei (Spendenbasis)
 - Verknüpft mit Bezahlversion (SaaS, Enterprise/Premium-Editionen, Support)
 - Man unterscheidet:
 - Produktnutzung
 - Nutzung/Modifikation des Source-Codes

Man weiß meist, auf was man sich einlässt.

Achtung! Versteckte Risiken. [5]



[2]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Beispiel: MIT-Lizenz

Warum Lizenzen? - Compliance

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[7]

Risikos: Verbot der Monetarisierung

Warum muss man aufpassen?

- Lizenzen können die kommerzielle Nutzung Verboten/Einschränken

[6]

[8]

Risikos: Verbot der Monetarisierung

Warum muss man aufpassen?

- Lizenzen können die kommerzielle Nutzung Verbieten/Einschränken
- Vorteil: Echte Open-Source Lizenzen erlauben Verbreitung und Monetarisierung
 - “The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.”

[6]

[8]

Risikos: Verbot der Monetarisierung

Warum muss man aufpassen?

- Lizenzen können die kommerzielle Nutzung Verboten/Einschränken
- Vorteil: Echte Open-Source Lizenzen erlauben Verbreitung und Monetarisierung
 - “The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.” [6]
- Problem: Nicht alles was Quelloffen ist, ist auch Open-Source
 - Vorsicht vor Code, der offen zur Verfügung steht, aber nicht als Open-Source zur Verfügung steht [8]

Risikos: Verbot der Monetarisierung

Warum muss man aufpassen?

- Lizenzen können die kommerzielle Nutzung Verboten/Einschränken
- Vorteil: Echte Open-Source Lizenzen erlauben Verbreitung und Monetarisierung
 - “The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.” [6]
- Problem: Nicht alles was Quelloffen ist, ist auch Open-Source
 - Vorsicht vor Code, der offen zur Verfügung steht, aber nicht als Open-Source zur Verfügung steht
- Problem: Unterschiedliche Lizenzierung
 - Dual-Licensing [8]
 - Restriktive Lizenz für nicht-zahlende Nutzer
 - Offene Lizenz für zahlende Nutzer

Risikos: Zusätzliche Anforderungen

Warum muss man aufpassen?

- Die Open-Source Lizenz, kann Schritte fordern, damit von den Rechten Gebrauch gemacht werden kann [6]
 - Gut für eine Firma, weil es ihr Garantien einräumt
 - „Schlecht“, wenn die Forderung in der Lizenz von der Firma ebenfalls erfüllt werden muss

[6]

[6]

[6]

Risikos: Zusätzliche Anforderungen

Warum muss man aufpassen?

- Die Open-Source Lizenz, kann Schritte fordern, damit von den Rechten Gebrauch gemacht werden kann [6]
 - Gut für eine Firma, weil es ihr Garantien einräumt
 - „Schlecht“, wenn die Forderung in der Lizenz von der Firma ebenfalls erfüllt werden muss
- **Beispiel:** Gleiches Recht für alle [6]
- **Beispiel:** Gleiches Recht für alle Anwendungsfälle [6]
- **Beispiel:** Offene Darlegung der Lizenzen der benutzten Quellen! [6]

Risikos: Zusätzliche Anforderungen

Warum muss man aufpassen?

- Die Open-Source Lizenz, kann Schritte fordern, damit von den Rechten Gebrauch gemacht werden kann [6]
 - Gut für eine Firma, weil es ihr Garantien einräumt
 - „Schlecht“, wenn die Forderung in der Lizenz von der Firma ebenfalls erfüllt werden muss
- **Beispiel:** Gleiches Recht für alle [6]
- **Beispiel:** Gleiches Recht für alle Anwendungsfälle [6]
- **Beispiel:** Offene Darlegung der Lizenzen der benutzten Quellen! [6]

!!!KRITISCH!!!



Risikos: Zusätzliche Anforderungen

Warum muss man aufpassen?

- Die Open-Source Lizenz, kann Schritte fordern, damit von den Rechten Gebrauch gemacht werden kann [6]
 - Gut für eine Firma, weil es ihr Garantien einräumt
 - „Schlecht“, wenn die Forderung in der Lizenz von der Firma ebenfalls erfüllt werden muss
- **Beispiel:** Gleiches Recht für alle
- **Beispiel:** Gleiches Recht für alle Anwendungsfälle
- **Beispiel:** Offene Darlegung der Lizenzen der benutzten Quellen! [6]

!!!KRITISCH!!!



[4]

Risikos: Einschränkung der Lizenzierung – Permissive vs. Copyleft

Warum muss man aufpassen?

- Permissive:
 - Generelle Offenheit in der Lizenzierung
 - Von „Permissive“ Lizenz Abgeleitetes **kann** kommerziell Lizenziert werden, **sogar** Closed-Source

[10]

[11]

[9]

Risikos: Einschränkung der Lizenzierung – Permissive vs. Copyleft

Warum muss man aufpassen?

- Permissive:
 - Generelle Offenheit in der Lizenzierung
 - Von „Permissive“ Lizenz Abgeleitetes **kann** kommerziell Lizenziert werden, **sogar** Closed-Source
- Copyleft:
 - Eine Lizenz mit „Copyleft“ Teil verbietet es, eine restriktivere Lizenz für ein abgeleitetes Werk zu verwenden
 - Wichtiger Faktor für die Open-Source
 - Einzelne Pakete/Bibliotheken können die ganze Lizenzierung kippen

[10]

[11]

[9]

Risikos: Einschränkung der Lizenzierung – Permissive vs. Copyleft

Warum muss man aufpassen?

- Permissive:
 - Generelle Offenheit in der Lizenzierung
 - Von „Permissive“ Lizenz Abgeleitetes **kann** kommerziell Lizenziert werden, **sogar** Closed-Source
- Copyleft:
 - Eine Lizenz mit „Copyleft“ Teil verbietet es, eine restriktivere Lizenz für ein abgeleitetes Werk zu verwenden
 - Wichtiger Faktor für die Open-Source
 - Einzelne Pakete/Bibliotheken können die ganze Lizenzierung kippen **!!KRITISCH!!**

[10]

[11]

[9]

Risikos: Einschränkung der Lizenzierung – Permissive vs. Copyleft

Warum muss man aufpassen?

- Permissive:
 - Generelle Offenheit in der Lizenzierung
 - Von „Permissive“ Lizenz Abgeleitetes **kann** kommerziell Lizenziert werden, **sogar** Closed-Source
- Copyleft:
 - Eine Lizenz mit „Copyleft“ Teil verbietet es, eine restriktivere Lizenz für ein abgeleitetes Werk zu verwenden
 - Wichtiger Faktor für die Open-Source
 - Einzelne Pakete/Bibliotheken können die ganze Lizenzierung kippen **!!KRITISCH!!**
- Schwaches Copyleft:
 - Erlaubt Nutzung von Bibliotheken/Paketen, wenn diese **nicht modifiziert werden**
 - Meist beschränkt auf Code der „**Verteilt wird**“
 - Der Nutzer **muss** die Bibliothek gegen andere Versionen austauschen können:
 - Offener Quellcode/Objektcode (meist unerwünscht)
 - Dynamisch verlinkte Bibliotheken (dynamically linked libraries)

[10]

[11]

[9]

Erklärung: Dynamic vs. Static Linking bei Node.js

Warum muss man aufpassen?

- Beispiel: Node.js / npm: Javascript im Web-Bereich

[11]

[9]



[6]

Erklärung: Dynamic vs. Static Linking bei Node.js

Warum muss man aufpassen?

- Beispiel: Node.js / npm: Javascript im Web-Bereich
- Was zählt als Distribution (Verteilung):
 - Verschicken / Nutzen in der Firma: **NEIN**
 - Bereitstellen einer API / Anwendung über das Netzwerk: **NEIN**
 - Bereitstellen auf einem Server: **JA**

(Dev-Dependencies!)

(außer „Network Protective Licenses“)

(alles „normale“ Frontend Javascript)

[11]

[9]



[6]

Erklärung: Dynamic vs. Static Linking bei Node.js

Warum muss man aufpassen?

- Beispiel: Node.js / npm: Javascript im Web-Bereich
- Was zählt als Distribution (Verteilung):
 - Verschicken / Nutzen in der Firma: **NEIN**
 - Bereitstellen einer API / Anwendung über das Netzwerk: **NEIN**
 - Bereitstellen auf einem Server: **JA**
- Was zählt als Linking (Verwendung/Einbindung)
 - Bundle-Programme: **Statischer Link**
 - Require-Script-Tag oder require: **Dynamischer Link**
 - Achtung beim transitiven Verlinken!

(Dev-Dependencies!)

(außer „Network Protective Licenses“)

(alles „normale“ Frontend Javascript)

(z.B. Webpack)

(extra Laden von meist anderen Servern)

(Bibliothek verwendet selbst Bibliotheken)

[11]

[9]



[6]

Lizenzen und deren Typ

Was für (OpenSource) Lizenzen gibt es? / Wie interagieren Lizenzen?

- MIT: Massachusetts-Institute-of-Technology-License
 - Permissive
- BSD: Berkley-Software-Distribution-License
 - Permissive
- Apache 2.0
 - Permissive
- LGPL: Lesser-Gnu-Public-License
 - Protective (Weak copyleft)
- MPL: Mozilla-Public-License
 - Protective (Weak copyleft)
- GPL: Gnu-Public-License
 - Protective (Strong copyleft)

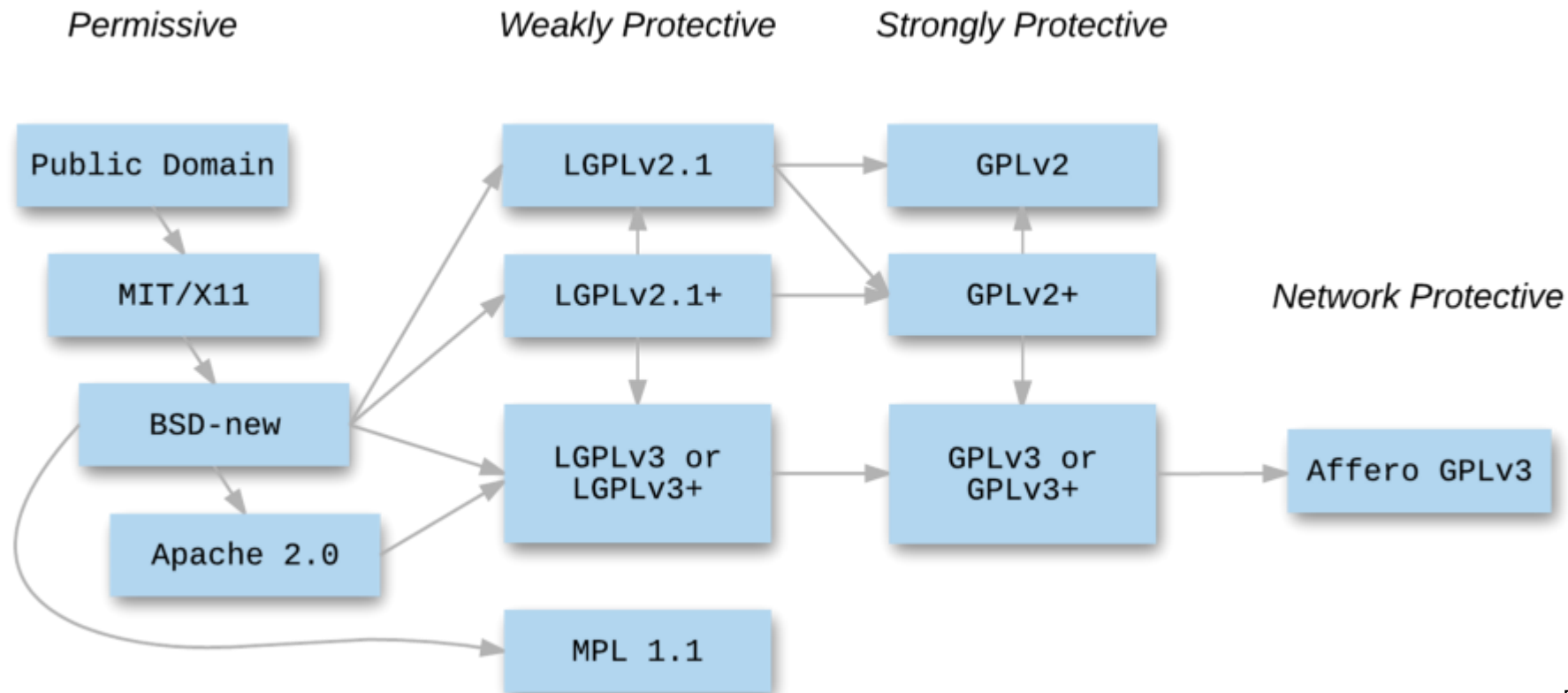
[10]



[7]

Lizenzen und deren Interaktion

Was für (OpenSource) Lizenzen gibt es? / Wie interagieren Lizenzen?



[5]

Überleitung: Was hat das mit DevOps und CI/CD zu tun?

Vorstellung & Vergleich CI/CD – Tools

Warum braucht man DevOps / CI/CD Verfahren bei der Arbeit mit OpenSource Paketen?

Überleitung: Was hat das mit DevOps und CI/CD zu tun?

Vorstellung & Vergleich CI/CD – Tools

Warum braucht man DevOps / CI/CD Verfahren bei der Arbeit mit OpenSource Paketen?

- **Situation:**

- Junior Entwickler sind schlecht über die Lizenzsituation informiert
- Senior Entwickler beachten Lizenzen gar nicht mehr, weil sie Pakete schon automatisiert verwenden
- Pakete haben indirekte Abhängigkeiten, die nicht sofort sichtbar sind

Überleitung: Was hat das mit DevOps und CI/CD zu tun?

Vorstellung & Vergleich CI/CD – Tools

Warum braucht man DevOps / CI/CD Verfahren bei der Arbeit mit OpenSource Paketen?

- **Situation:**

- Junior Entwickler sind schlecht über die Lizenzsituation informiert
- Senior Entwickler beachten Lizenzen gar nicht mehr, weil sie Pakete schon automatisiert verwenden
- Pakete haben indirekte Abhängigkeiten, die nicht sofort sichtbar sind

- **Wozu führt das:**

- Manuelles Checken bei jeder Installation kostet Zeit
- Durch mehrere Entwickler entstehen Abhängigkeiten, die jeder für sich nicht erkennt
- Das Problem der Lizenzen wird generell ignoriert
- Trotz allem können Lizenzen übersehen werden

Überleitung: Was hat das mit DevOps und CI/CD zu tun?

Vorstellung & Vergleich CI/CD – Tools

Warum braucht man DevOps / CI/CD Verfahren bei der Arbeit mit OpenSource Paketen?

■ **Situation:**

- Junior Entwickler sind schlecht über die Lizenzsituation informiert
- Senior Entwickler beachten Lizenzen gar nicht mehr, weil sie Pakete schon automatisiert verwenden
- Pakete haben indirekte Abhängigkeiten, die nicht sofort sichtbar sind

■ **Wozu führt das:**

- Manuelles Checken bei jeder Installation kostet Zeit
- Durch mehrere Entwickler entstehen Abhängigkeiten, die jeder für sich nicht erkennt
- Das Problem der Lizenzen wird generell ignoriert
- Trotz allem können Lizenzen übersehen werden

■ **Lösung:**

- Automatisiertes auslesen, sammeln und anzeigen der Lizenzen
- evtl. sogar automatisierte Warnungen

Tool-Vorstellung: **Snyk** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Snyk ist eine „Open Source Security Platform“

[12]



[8]

Tool-Vorstellung: **Snyk** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Snyk ist eine „Open Source Security Platform“
- Breit gefächertes Portfolio an Funktionen
 - Zentrale Features beziehen sich auf viele Formen des Vulnerability-Scanning
 - License Compliance als „Nebenfeature“ angeboten

[12]



[8]

Tool-Vorstellung: **Snyk** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Snyk ist eine „Open Source Security Platform“
- Breit gefächertes Portfolio an Funktionen
 - Zentrale Features beziehen sich auf viele Formen des Vulnerability-Scanning
 - License Compliance als „Nebenfeature“ angeboten
- Angebotene Funktionen:
 - Per-Lizenz Regeln, was erlaubt ist und wie darüber hinaus zu verfahren ist
 - Bereitstellen von Lizenztexten
 - Zentrale Abhängigkeitsübersicht in Baum-Form
 - Tracking der Verstöße nach Schwere-Graden
 - Push-Nachrichten-Integration

[12]



[8]

Tool-Vorstellung: **Snyk** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

```
This issue was fixed in versions: 2.0.1, 3.0.1
x Insecure use of Tmp files [Medium Severity][https://snyk.io/vuln/npm:sync-exec:20160124] in sync
.6.2
  introduced by gulp-scss-lint@0.7.0 > sync-exec@0.6.2
  No upgrade or patch available

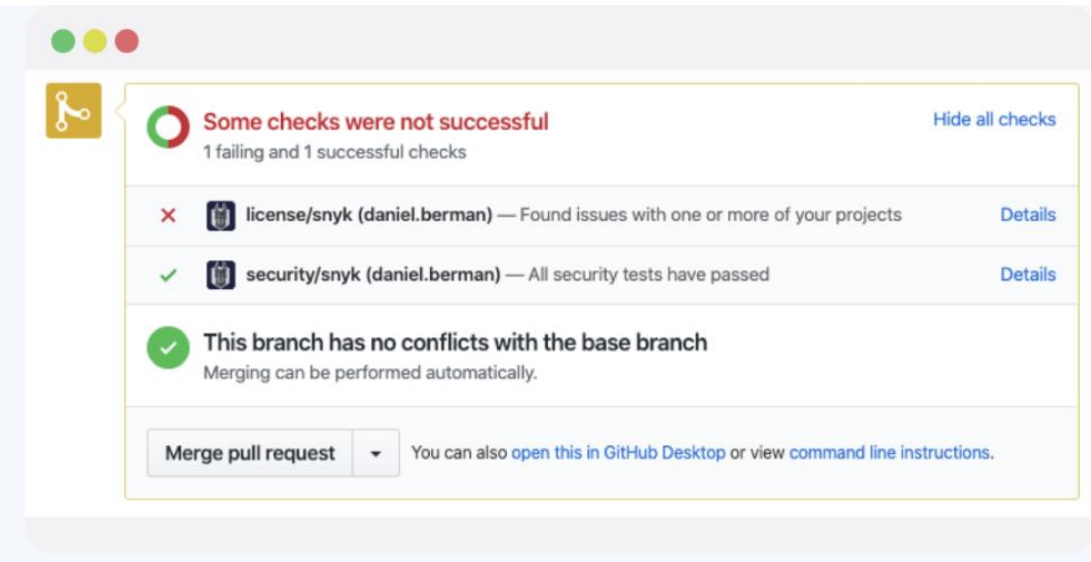
License issues:

x GPL-3.0 license (new) [High Severity][https://snyk.io/vuln/snyk:lic:npm:scrollreveal:GPL-3.0] in
reveal@4.0.6
  Legal instructions:
  o for GPL-3.0: Please consult with the legal team at legal@snyk.io

x GPL-2.0 license (new) [High Severity][https://snyk.io/vuln/snyk:lic:npm:goof:GPL-2.0] in goof@1.0
  Legal instructions:
  o for GPL-2.0: Violates company policies. Please contact the legal team for further instructions.

Organization:    daniel.berman
Package manager: npm
Target file:     package-lock.json
Project name:    goof
Open source:     no
Project path:    /Users/daniel/Projects/goof
Licenses:        enabled

Run `snyk wizard` to address these issues.
```



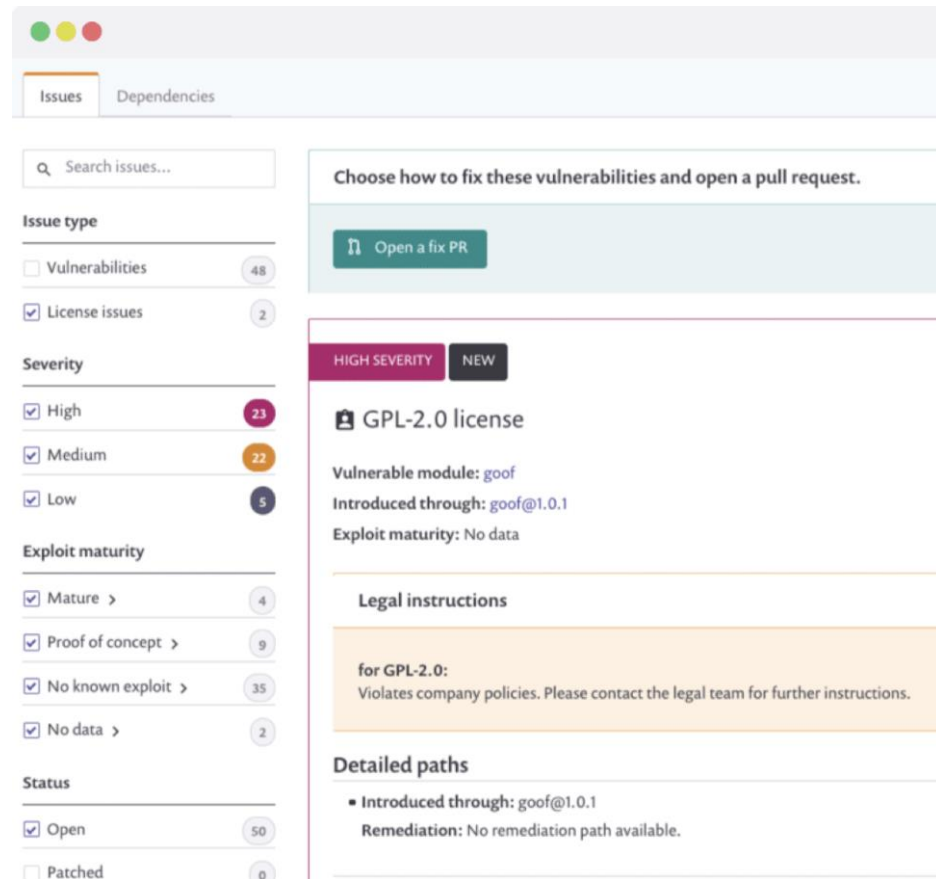
[13]



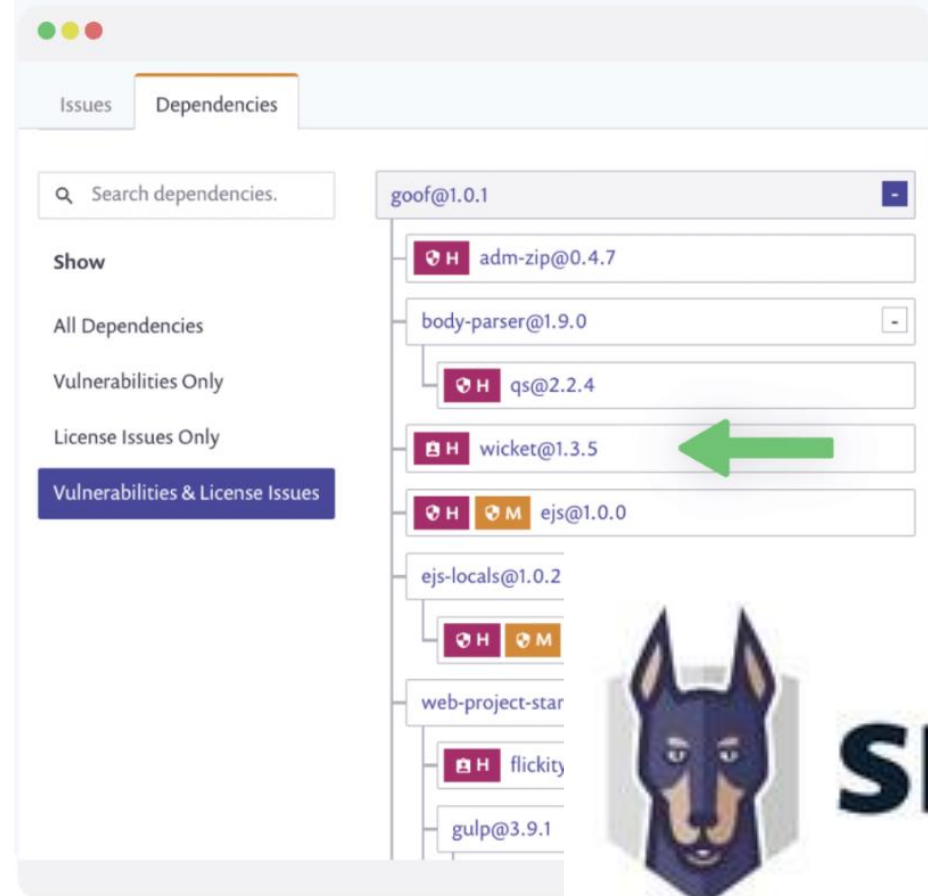
[8]

Tool-Vorstellung: **Snyk** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools



[13]



[13]

[8]

Tool-Vorstellung: **Fossa** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Fossa hat nach eigenen Angaben das größte Inventar an Lizenzen, die getrackt und eingeordnet werden können

[13]



[9]

Tool-Vorstellung: **Fossa** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Fossa hat nach eigenen Angaben das größte Inventar an Lizenzen, die getrackt und eingeordnet werden können [13]
- Zwei Hauptfunktionen werden angeboten:
 - License Compliance
 - Security-Management (Sicherheitslücken erkennen)



[9]

Tool-Vorstellung: **Fossa** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

- Fossa hat nach eigenen Angaben das größte Inventar an Lizenzen, die getrackt und eingeordnet werden können [13]
- Zwei Hauptfunktionen werden angeboten:
 - License Compliance
 - Security-Management (Sicherheitslücken erkennen)
- Dabei wird besonders die Abdeckung des gesamten Entwicklungsprozesses angepriesen
 - Von Planung über Entwicklung zu Verifizierung ist der ganze Prozess abgedeckt
 - „Shift-Left“ der Erkennung von Problemen im Prozessablauf



[9]

Tool-Vorstellung: **Fossa** Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

Devops Test Uni Augsburg > [Select team](#)

[Add Projects](#) [Rescan All](#)

Search by title... [Add to...](#) [Delete](#) 1 - 1 of 1 projects

<input type="checkbox"/>	TITLE	STATUS	STATS	LAST UPDATED
<input type="checkbox"/>	license-check-gitlab	2 Issues Found	95 deps • 12 licenses	7 minutes ago

Open source management powered by FOSSA, Inc. © 2021

[12]



[9]

Tool-Vorstellung: Fossa Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

12 Licenses Found

DIRECTLY IN CODE

⊕ ADD

MIT License

GNU Lesser General Public License v3.0 only

Apache License 2.0

BSD 3-Clause "New" or "Revised" License

STARTING IN DIRECT DEPENDENCIES

PHP License v3.01

STARTING FROM 2-LEVEL DEEP DEPENDENCIES

GNU Lesser General Public License v2.1 only

Mozilla Public License 2.0

Public Domain

BSD 2-Clause "Simplified" License

GNU General Public License v3.0 only

STARTING FROM 3-LEVEL DEEP DEPENDENCIES

GNU General Public License v3.0 or later

7 Obligations Found

▼ Include License for projects

"You must **include** the **license** notice in all copies or substantial uses of the work."

MIT

89 Projects...

"Including the full text of **license** in modified software."

LGPL-2.1-ONLY & LGPL-3.0-ONLY & MPL-2.0 & APACHE-2.0 & BSD-2-CLAUSE & PHP-3.0

12 Projects...

"Including the full text of **license** in source or object code copies."

BSD-3-CLAUSE

14 Projects...

► Include Copyright for projects

► Disclose Source for projects

► Include Original for projects

► Include Notice for projects

► State Changes for projects

► Include Install Instructions for projects

FOSSA

[12]

[9]

Tool-Vorstellung: Fossa Open Source License Compliance Management

Vorstellung & Vergleich CI/CD – Tools

Active 2Exported 0Resolved 0

Order issues by...

Search issues by package name

9 minutes ago
Flagged: GPL-3.0-only in monolog/monolog
Used by license-check-gitlab

9 minutes ago
Flagged: GPL-3.0-only in phenx/php-svg-lib
Used by license-check-gitlab

Flagged: GPL-3.0-only in monolog/monolog

These packages contain code files that may require you to disclose your source code under a compatible license, unless they're distributed and run as completely separate processes & packages.

ResolveSetup Issue Tracker

Affected Dependency

Edit Package

monolog/monolog

comp

VERSION USED: 2.2.0

Homepage

Sends your logs to files, sockets, inboxes, databases and various web services

Deep Scan Match: GPL-3.0-only

```
374 )@9a_^JPN,
375 d:4[
376 !y.z.A0*2G<V!mqfP[.E]
377 ~R[,J/rr_I|a<N1.2.xB@[$Zy#tUe.Y.E.tl)kYK9
378 kq:8.Q^/EefXb.D8GAa='Qe}Bj;^N^A-GK *Xja.I+4uv^"
379 7(<I.7;
380 gxxxxx...E.)Y@n~+0,E`_{U%43'c4*.*5>wMZyM--s+Z00`sg9f
381 k9|YiivvifE+8+"nR?tzMDC^c0i~v.h&3`+
382 >AG_R:d.e.YL3XMx
383 pC66v!i(/
384 l$er>x:2Thw.}^Fw.r.!b
385 M,._iq79`<J.Zl*%#wLi-Z$F=L$an
386 lR}.....<thN>.dh.p"y3`{.*
```

File: monolog-monolog-2-^

FOSSA

[12]

[9]

21 | 26+27.07.2021 | Seminar Softwareentwicklung mit Dev(Sec)Ops: Kell – Compliance: License-Checker

UNIA

Tool-Vorstellung: **GitLab** License Compliance

Vorstellung & Vergleich CI/CD – Tools

- GitLab **Ultimate** hat die „License Compliance“ als Standardfeature, das automatisch aktiv ist
- Informationen werden in den CI-CD Pipelines generiert und automatisch verarbeitet

[14]



GitLab

[10]

Tool-Vorstellung: **GitLab** License Compliance

Vorstellung & Vergleich CI/CD – Tools

- GitLab **Ultimate** hat die „License Compliance“ als Standardfeature, das automatisch aktiv ist
- Informationen werden in den CI-CD Pipelines generiert und automatisch verarbeitet
- Anzeige der Informationen in (minimalistischem Dashboard)

[14]

License Compliance ⓘ

Displays licenses detected in the project, based on the [latest successful scan](#) • 1 minute ago

Detected in Project **5** Policies **0**

Name	Component
MIT License	asm89/stack-cors (v2.0.3), barryvdh/laravel-dumpdf (v0.9.0), and 63 more
GNU Lesser General Public License v3.0 only	phenx/php-font-lib (0.5.2) and phenx/php-svg-lib (v0.3.3)
GNU Lesser General Public License v2.1 only	dompdf/dompdf (v1.0.2)
BSD 3-Clause "New" or "Revised" License	league/commonmark (1.6.5), nikic/php-parser (v4.10.5), and 2 more
Apache License 2.0	phpoption/phpoption (1.7.5)

[1]



GitLab

[10]

Tool-Vorstellung: **GitLab** License Compliance

Vorstellung & Vergleich CI/CD – Tools

- GitLab **Ultimate** hat die „License Compliance“ als Standardfeature, das automatisch aktiv ist
- Informationen werden in den CI-CD Pipelines generiert und automatisch verarbeitet
- Anzeige der Informationen in (minimalistischem Dashboard)
- Jede einzelne Lizenz kann erlaubt oder verboten werden

[14]

License Compliance ⓘ

Displays licenses detected in the project, based on the [latest successful scan](#) • 1 minute ago

Detected in Project **5** Policies **0**

Name	Component
MIT License	asm89/stack-cors (v2.0.3), barryvdh/laravel-dumpdf (v0.9.0), and 63 more
GNU Lesser General Public License v3.0 only	phenx/php-font-lib (0.5.2) and phenx/php-svg-lib (v0.3.3)
GNU Lesser General Public License v2.1 only	dompdf/dompdf (v1.0.2)
BSD 3-Clause "New" or "Revised" License	league/commonmark (1.6.5), nikic/php-parser (v4.10.5), and 2 more
Apache License 2.0	phpoption/phpoption (1.7.5)

[1]



GitLab

[10]

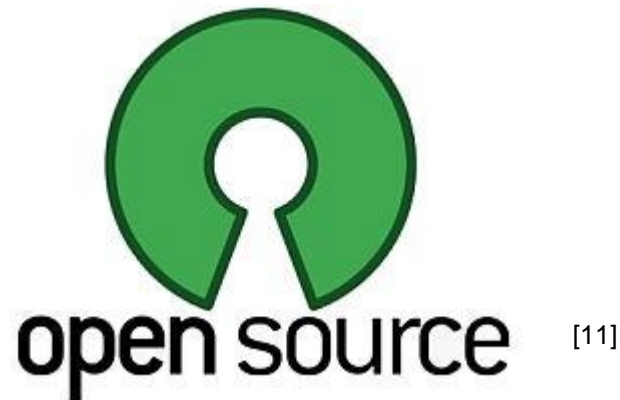
Tool-Vorstellung: **OpenSource** Eigene (GitLab) Schnittstelle für OS-Tools

Vorstellung & Vergleich CI/CD – Tools

- Für praktisch alle Package-Manager gibt es Quelloffene Lizenz-Sammel-Pakete
 - Kann mit wenig Aufwand in GitLab-Pipelines automatisch generiert werden

[15]

[16]



+



GitLab

[10]

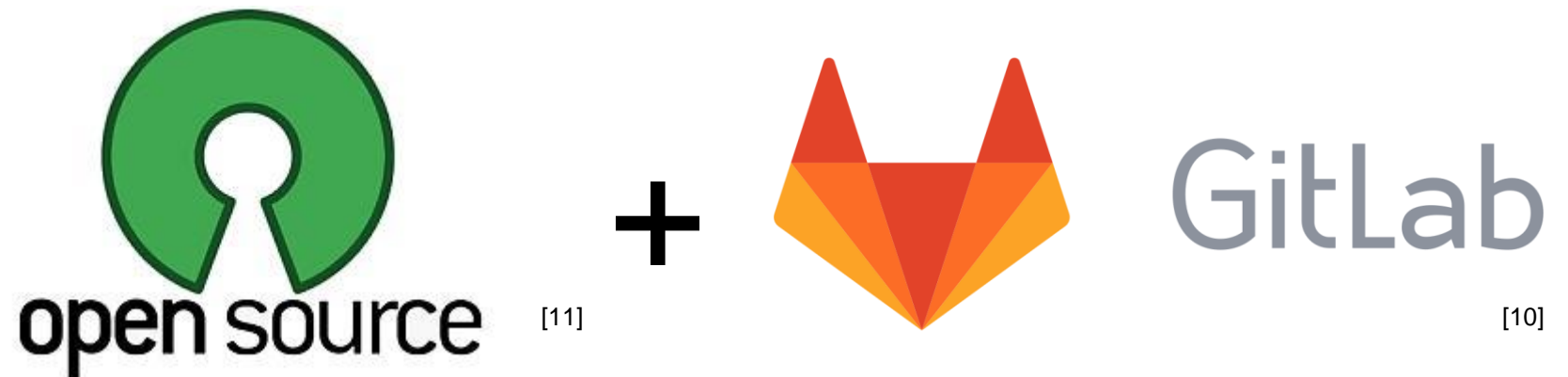
Tool-Vorstellung: **OpenSource** Eigene (GitLab) Schnittstelle für OS-Tools

Vorstellung & Vergleich CI/CD – Tools

- Für praktisch alle Package-Manager gibt es Quelloffene Lizenz-Sammel-Pakete
 - Kann mit wenig Aufwand in GitLab-Pipelines automatisch generiert werden
- Viele unterstützen auch das setzen einfacher „Only Accept“ oder „Do not Accept“ Filter
 - Kann mit mäßig Aufwand in GitLab-Pipelines automatisch erzeugt werden

[15]

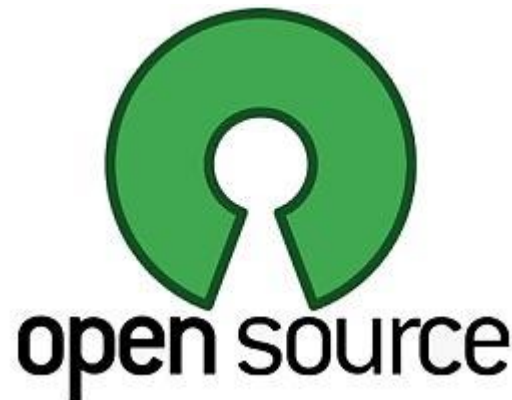
[16]



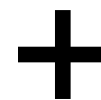
Tool-Vorstellung: **OpenSource** Eigene (GitLab) Schnittstelle für OS-Tools

Vorstellung & Vergleich CI/CD – Tools

- Für praktisch alle Package-Manager gibt es Quelloffene Lizenz-Sammel-Pakete [15]
 - Kann mit wenig Aufwand in GitLab-Pipelines automatisch generiert werden
- Viele unterstützen auch das setzen einfacher „Only Accept“ oder „Do not Accept“ Filter
 - Kann mit mäßig Aufwand in GitLab-Pipelines automatisch erzeugt werden
- Ausgaben meist im JSON-Format
 - Kann mit (relativ) hohem Aufwand in das JUnit Format übergeführt werden, das GitLab als Test-Output parsen und darstellen kann [16]



[11]



GitLab

[10]

Tabelle: Vergleich und Abwägung der Tools

Vorstellung & Vergleich CI/CD – Tools

Tool	SNYK [12]	FOSSA [13]	GitLab [14]	OpenSource [15]
Preis Version:	\$195 /5 Entwickler/Monat (Team)	\$230 /5 Entwickler/Monat (Bereits Fähige Free Version)	\$99 /Entwickler/Monat (Ultimate)	Gratis (Developer Kosten)
Installations Aufwand	Mittel (gibt Snyk einen Application Access Token)	Mittel (quick-Import per Token, oder lokales Tool (Aufwand))	Sehr Niedrig (Out of the box bei bestehendem GitLab)	Hoch (Muss eigens geschrieben werden)
Konfigurations Aufwand	Einfache Regeln in Team Komplexe in teurerer Version	Vorkurierte Lizenz-Regel Vorlagen	Hoch (Einmalig, muss Eigene Regelfestlegung pro Lizenz)	Hoch (Einmalig, Muss Eigene Regelfestlegung pro Lizenz)
Unterstützte Sprachen	8 (Alle benötigten)	17 ++ (Alle benötigten)	6 + 9 experimentell (Alle benötigten)	Praktisch Alle, aber jeweils extra Aufwand
Statische Checks	Ja + IDE-Integration	Ja, lokales CLI Tool	Nein aber Übersicht	Ja
Checks bei Merges	Ja + detaillierte Verbesserungsvorschläge	Ja + detaillierte Verbesserungsvorschläge	Ja + Übersicht über Violation	Ja + etwas Übersicht über Violation
Deployment	SaaS, (SelfHost in High Tier)	Tool lokal -> SaaS (nur Infos), Oder On-Prem -> SaaS	SaaS oder SelfHost	Zwangsweise In der gleichen Konfiguration wie GitLab
Dep. Manager Integration	Integriert direkt mit GitLab	Integration für Code Import und Webhooks Export	Ist der Dependency Manager	Ja, Bleibt hinter der normalen GitLab Version zurück
Regel komplex.	Hoch	Hoch	Niedrig	Mittel (frei, aber aufwändig)
Dashboard	Sehr Detailliert	Sehr Detailliert	Ja, aber wenig Details	Nein

Installation

Demonstration: Gitlab License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des GitLab internen Tools gegeben werden

- Voraussetzungen:
 - Source-Code ist in GitLab Ultimate eingcheckedt
 - GitLab-Docker-Runner sind für das Projekt konfiguriert

Installation

Demonstration: Gitlab License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des GitLab internen Tools gegeben werden

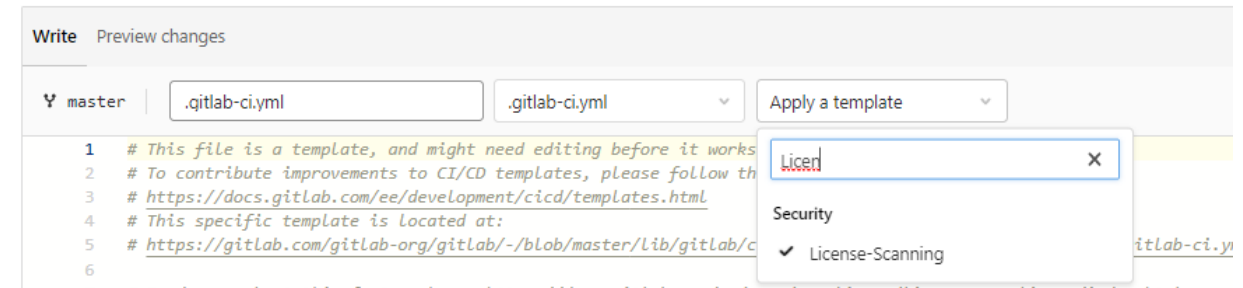
- Voraussetzungen:
 - Source-Code ist in GitLab Ultimate eingchecked
 - GitLab-Docker-Runner sind für das Projekt konfiguriert
- Schritte (Lizenzcheck ist einziges Pipeline Feature):
 - Aktiviere die „Auto License Compliance“, die von „Auto Devops“ bereitgestellt wird
 - Starte eine Pipeline auf dem Master-Branch

Installation

Demonstration: Gitlab License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des GitLab internen Tools gegeben werden

- Voraussetzungen:
 - Source-Code ist in GitLab Ultimate eingecheckt
 - GitLab-Docker-Runner sind für das Projekt konfiguriert
- Schritte (Lizenzcheck ist einziges Pipeline Feature):
 - Aktiviere die „Auto License Compliance“, die von „Auto Devops“ bereitgestellt wird
 - Starte eine Pipeline auf dem Master-Branch
- Schritte (Code in der eigenen **.gitlab-ci.yml**):
 - Lade die License-Scanning Vorlage (oben)



[1]

Installation

Demonstration: Gitlab License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des GitLab internen Tools gegeben werden

- Voraussetzungen:

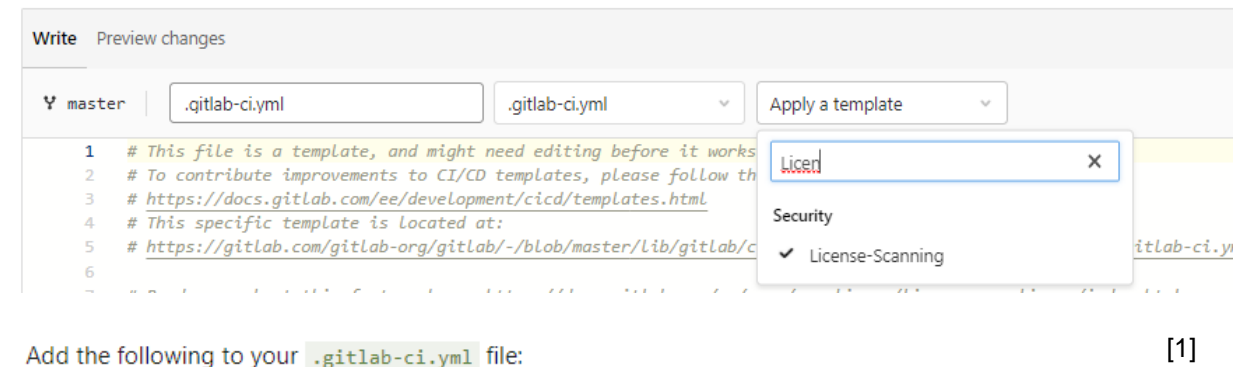
- Source-Code ist in GitLab Ultimate eingcheckedt
- GitLab-Docker-Runner sind für das Projekt konfiguriert

- Schritte (Lizenzcheck ist einziges Pipeline Feature):

- Aktiviere die „Auto License Compliance“, die von „Auto Devops“ bereitgestellt wird
- Starte eine Pipeline auf dem Master-Branch

- Schritte (Code in der eigenen **.gitlab-ci.yml**):

- Lade die License-Scanning Vorlage (oben)
- Alternativ: Einbinden der Vorlage in der bestehenden Konfiguration (unten)
- Starte eine Pipeline auf dem Master-Branch



[1]

```
include:  
  - template: License-Scanning.gitlab-ci.yml
```

[1]

Installation: Übersicht über Unterstützte Paket-Manager

Supported languages and package managers

The following languages and package managers are supported.

Java 8 and Gradle 1.x projects are not supported. The minimum supported version of Maven is 3.2.5.

Language	Package managers	Notes
JavaScript	Bower , npm (7 and earlier)	
Go	Godep , go mod	
Java	Gradle , Maven	
.NET	NuGet	The .NET Framework is supported via the mono project . There are, however, some limitations. The scanner doesn't support Windows-specific dependencies and doesn't report dependencies of your project's listed dependencies. Also, the scanner always marks detected licenses for all dependencies as unknown .
Python	pip	Python is supported through requirements.txt and Pipfile.lock .
Ruby	gem	

[1]

Experimental support

The following languages and package managers are supported experimentally .

Language	Package managers
JavaScript	Yarn
Go	go get , gvt , glide , dep , trash , govendor
Erlang	Rebar
Objective-C, Swift	Carthage , CocoaPods v0.39 and below
Elixir	Mix
C++/C	Conan
Scala	sbt
Rust	Cargo
PHP	Composer

[1]

GitLab: Lizenz-Menü

Demonstration: Gitlab License-Compliance

Project information

Repository

Issues1

Merge requests3

Requirements

CI/CD

Security & Compliance

Deployments

Monitor

Infrastructure

Packages & Registries

Analytics

Wiki

Snippets

Settings

Security Dashboard

Vulnerability Report

On-demand Scans

Dependency List

License Compliance

Threat Monitoring

Audit Events

Configuration

Detected in Project5Policies5

Add a license

License Approvals

License Approvals are inactive

Search

✓Mozilla Public License 2.0

Allowed

✓Apache License 2.0

Allowed

✓BSD 3-Clause "New" or "Revised" License

Allowed

✓MIT License

Allowed

✗GPLv3

Denied

License Compliance?

Displays licenses detected in the project, based on the latest successful scan • 1 minute ago

Detected in Project5Policies0

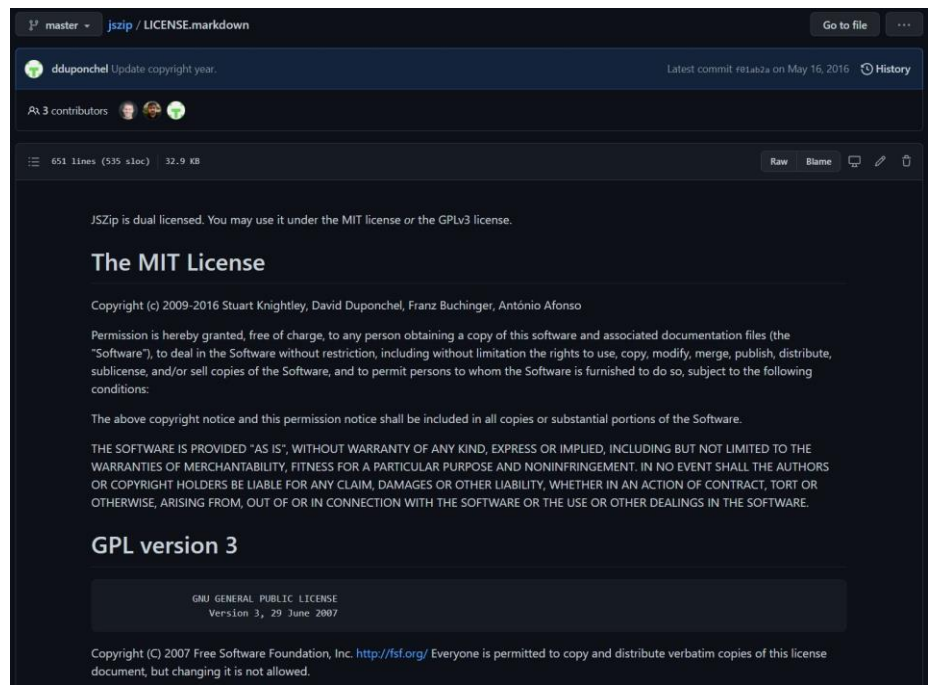
Name	Component
MIT License	asm89/stack-cors (v2.0.3), barryvdh/laravel-dompdf (v0.9.0), and 63 more
GNU Lesser General Public License v3.0 only	phenx/php-font-lib (0.5.2) and phenx/php-svg-lib (v0.3.3)
GNU Lesser General Public License v2.1 only	dompdf/dompdf (v1.0.2)
BSD 3-Clause "New" or "Revised" License	league/commonmark (1.6.5), nikic/php-parser (v4.10.5), and 2 more
Apache License 2.0	phpoption/phpoption (1.7.5)

[1]

[1]

Pipeline: Nicht-Erlaubtes Paket (JSZip)

Demonstration: Gitlab License-Compliance



[15]

Resolve "Test Forbidden License"

Overview 0 Commits 1 Pipelines 1 Changes 2

Closes #1

Edited just now by Jonas Kell

Request to merge 1-test-forbidden-lice... into master Open in Web IDE Check out branch Download

Pipeline #340814553 passed for d74c7884 on 1-test-forbidden-lice... 2 days ago Download

Approval is optional View eligible approvers

License Compliance detected 3 new licenses and policy violations View full report Manage licenses Collapse

Denied
Out-of-compliance with this project's policies and should be removed

GPLv3 Used by jszip

Uncategorized
No policy matches this license

ISC License Used by , and inherits

zlib License Used by pako

Merge You can merge after removing denied licenses

Closes #1

[1]

Pipeline: Erlaubtes Paket (fsm)

Demonstration: Gitlab License-Compliance

trunk fsm / LICENSEGo to file...

escapace/fsm is licensed under the Mozilla Public License 2.0

Permissions of this weak copyright license are conditioned on making available source code of licensed files and modifications of those files under the same license (or in certain cases, one of the GNU licenses). Copyright and license notices must be preserved. Contributors provide an express grant of patent rights. However, a larger work using the licensed work may be distributed under different terms and without source code for files added in the larger work.

This is not legal advice. Learn more about repository licenses.

Permissions

Commercial use

Modification

Distribution

Patent use

Private use

Limitations

Liability

Trademark use

Warranty

Conditions

Disclose source

License and copyright notice

Same license (file)

markmartirosian feat: first commit

Latest commit b6478a8 on May 31, 2020History

At 1 contributor

373 lines (293 sloc) | 16.3 KB

RawBlame

1 Mozilla Public License Version 2.0

2 -----

3

4 1. Definitions

5 -----

6

7 1.1. "Contributor"

8 means each individual or legal entity that creates, contributes to

9 the creation of, or owns Covered Software.

10

11 1.2. "Contributor Version"

12 means the combination of the Contributions of others (if any) used

13 by a Contributor and that particular Contributor's Contribution.

14

15 1.3. "Contribution"

16 means Covered Software of a particular Contributor.

17

[16]

License Compliance detected no new licenses

View full reportManage licenses

Merge

☒ Delete source branch

☐ Squash commits

2 commits and 1 merge commit will be added to master. Modify merge commit

[1]

Open

Created 4 minutes ago by Jonas Kell

Maintainer

Edit

Mark as draft

add new but allowed license

Overview0

Commits1

Pipelines1

Changes2

Request to merge 3-add-new-but-allowed... into master

Open in Web IDE

Check out branch

Pipeline #340830260 passed for b2a8462e on 3-add-new-but-allowed... 1 minute ago

Approval is optional

View eligible approvers

License Compliance detected 2 new licenses

View full report

Manage licenses

Collapse

Uncategorized

No policy matches this license

BSD Zero Clause License Used by , and tslib

Allowed

Acceptable for use in this project

Mozilla Public License 2.0 Used by , @escapace/fsm, and @escapace/typelevel

Merge

☒ Delete source branch

1 commit and 1 merge commit will be added to master. Modify merge commit

[1]

Installation

Demonstration: OpenSource Wrapper: NPM-License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des NPM Paketes „license-checker“ in einer GitLab Pipeline gegeben werden.

- Voraussetzungen:
 - Source-Code ist in GitLab Ultimate eingecheckt
 - GitLab-Docker-Runner sind für das Projekt konfiguriert
 - NPM ist für das Projekt installiert (packages.json)

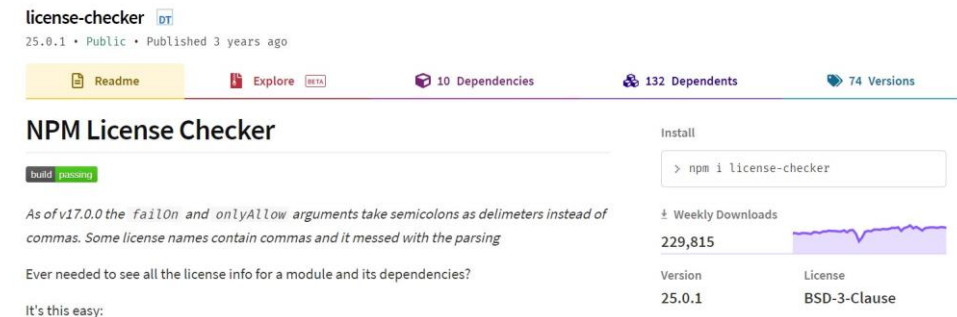
<https://www.npmjs.com/package/license-checker>

Installation

Demonstration: OpenSource Wrapper: NPM-License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des NPM Paketes „license-checker“ in einer GitLab Pipeline gegeben werden.

- Voraussetzungen:
 - Source-Code ist in GitLab Ultimate eingcheckedt
 - GitLab-Docker-Runner sind für das Projekt konfiguriert
 - NPM ist für das Projekt installiert (packages.json)



- NPM-Paket: <https://www.npmjs.com/package/license-checker>

Installation

Demonstration: OpenSource Wrapper: NPM-License-Compliance

Es soll nun ein Überblick über die Installation/Inbetriebnahme des NPM Paketes „license-checker“ in einer GitLab Pipeline gegeben werden.

- Voraussetzungen:

- Source-Code ist in GitLab Ultimate eingcheckedt
- GitLab-Docker-Runner sind für das Projekt konfiguriert
- NPM ist für das Projekt installiert (packages.json)

- Schritte:

- Füge den hierfür erstellten GitLab Job „licenses-custom “ in die **.gitlab-ci.yml** ein
- Füge das hierfür erstellte Script **npm-licenses.sh** auf der obersten Ebene des Projektes ein
- Betrachte die, durch den Commit gestartete, Pipeline in einem Merge-Request

- NPM-Paket: <https://www.npmjs.com/package/license-checker>

The screenshot shows the NPM package page for 'license-checker'. At the top, it displays the package name 'license-checker' with a 'DT' logo, version '25.0.1', and status 'Public • Published 3 years ago'. Below this are links for 'Readme', 'Explore', '10 Dependencies', '132 Dependents', and '74 Versions'. The main section is titled 'NPM License Checker' and features a 'build passing' badge. A note mentions a change in behavior for 'failOn' and 'onlyAllow' arguments in version 17.0.0. A table on the right shows 'Weekly Downloads' as 229,815 and 'License' as 'BSD-3-Clause'. The version '25.0.1' is also listed. A small '[14]' is visible at the bottom right of the screenshot area.

Installation: Datei-Übersicht

Demonstration: OpenSource Wrapper: NPM-License-Compliance

5-faulty-package-...


license-check-gitlab / .gitlab-ci.yml


Find file

Blame



History




Permalink

 Merge branch 'master' of gitlab.com:testultimate1/license-check-gitlab into...
Jonas Kell authored 17 minutes ago

✓ 4fd7645d 

✓ This GitLab CI configuration is valid. [Learn more](#)

 .gitlab-ci.yml  303 Bytes

EditWeb IDEPipeline EditorLockReplaceDelete

```
1 image: node:16
2
3 # custom npm license checking
4 licenses-custom:
5   script:
6     - /bin/bash ./npm-licenses.sh "(MIT OR GPL-3.0)" "Other License"
7
8   artifacts:
9     when: always
10    paths:
11      - license_summary.txt
12      - license_detailed.json
13    expire_in: 3 days
14    reports:
15      junit: licenses.xml
```

[1, für das Seminar geschrieben]



Correct exit code

Jonas Kell authored 5 minutes ago



4398163e



npm-licenses.sh 961 Bytes

Edit

Web IDE

Lock

Replace

Delete



```
1  npm install
2  npm install -g license-checker
3  npm install -g yui-lint
4
5  license-checker --summary --out "license_summary.txt"
6  license-checker --json --out "license_detailed.json"
7
8  # Generate Output.xml
9
10 echo '<?xml version="1.0" encoding="UTF-8"?><testsuites><testsuite id="NPM-CUSTOM-LICENSE-CHECKER">' > licenses.xml
11
12 fails=0
13 for VARIABLE in "$@"
14 do
15     echo '<testcase name="NPM check license ' $VARIABLE '">' >> licenses.xml
16
17     # execute test and capture error stream in variable
18     ERROR=$(license-checker --failOn "$VARIABLE" 2>&1 >/dev/null)
19
20     if [ $? != 0 ];
21     then
22         let "fails++"
23         echo '<failure type="FAILURE">' >> licenses.xml
24         echo $ERROR >> licenses.xml
25         echo '</failure>' >> licenses.xml
26     else
27         echo '<passed type="PASSED"></passed>' >> licenses.xml
28     fi
29     echo '</testcase>' >> licenses.xml
30 done
31
32 echo '</testsuite></testsuites>' >> licenses.xml
33
34 # 0 if all succeeded, larger 0 otherwise
35 exit $fails
```


[1, für das Seminar geschrieben]

Ausgabe: Artefakte

Demonstration: OpenSource Wrapper: NPM-License-Compliance

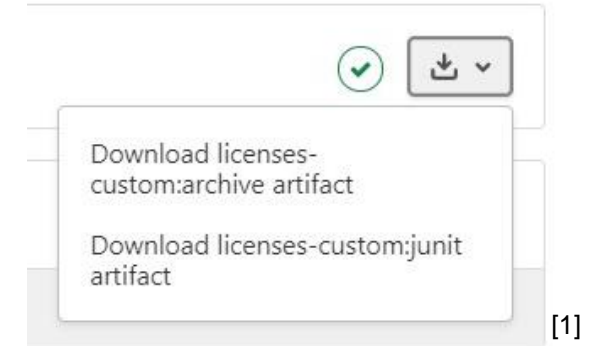
✓ passed Job #1444691922 in pipeline #341275998 for f1830090 from 6-allowed-package-on-npm-custom-checker by  Jonas Kell 8 minutes ago

Artifacts

 Download artifacts archive

Name	Size
 license_detailed.json 	284 KB
 license_summary.txt 	339 Bytes

[1]



[1]

Ausgabe: Artefakte

Demonstration: OpenSource Wrapper: NPM-License-Compliance

✓ passed Job #1444691922 in pipeline #341275998 for f1830090 from 6-allowed-package-on-npm-custom-checker by Jonas Kell 8 minutes ago

Artifacts

Download artifacts archive

Name	Size
license_detailed.json	284 KB
license_summary.txt	339 Bytes

[1]

Download licenses-
custom:archive artifact

Download licenses-custom:junit
artifact

[1]

```
license_detailed.json
1 {
2   "@babel/code-frame@7.14.5": {
3     "licenses": "MIT",
4     "repository": "https://github.com/babel/babel",
5     "publisher": "The Babel Team",
6     "url": "https://babel.dev/team",
7     "path": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/code-frame",
8     "licenseFile": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/code-frame/LICENSE"
9   },
10  "@babel/compat-data@7.14.7": {
11    "licenses": "MIT",
12    "repository": "https://github.com/babel/babel",
13    "publisher": "The Babel Team",
14    "url": "https://babel.dev/team",
15    "path": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/compat-data",
16    "licenseFile": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/compat-data/LICENSE"
17  },
18  "@babel/core@7.14.8": {
19    "licenses": "MIT",
20    "repository": "https://github.com/babel/babel",
21    "publisher": "The Babel Team",
22    "url": "https://babel.dev/team",
23    "path": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/core",
24    "licenseFile": "/builds/testultimatel/license-check-gitlab/node_modules/@babel/core/LICENSE"
25  },
26 }
```


```
license_summary.txt
1 MIT: 667
2 ISC: 52
3 BSD-2-Clause: 21
4 BSD-3-Clause: 11
5 Apache-2.0: 7
6 Unlicense: 2
7 (MIT OR Apache-2.0): 1
8 CC-BY-4.0: 1
9 CC0-1.0: 1
10 (BSD-3-Clause OR GPL-2.0): 1
11 (MIT AND Zlib): 1
12 MIT*: 1
13 (MIT AND BSD-3-Clause): 1
14 0BSD: 1
15 (MIT OR CC0-1.0): 1
16
```


Pipeline: Nicht-Erlaubtes Paket



Demonstration: OpenSource Wrapper: NPM-License-Compliance


faulty package on npm custom checker

Overview 0 Commits 18 Pipelines 3 Changes 5


 Request to merge 5-faulty-package-on-n... into master


[Open in Web IDE](#) [Check out branch](#) [Download](#)

 Pipeline #341275574 failed for 4398163e on 5-faulty-package-on-n... 12 minutes ago  [Download](#)


 Approval is optional


[View eligible approvers](#)

 Test summary contained 1 failed out of 2 total tests [View full report](#) [Collapse](#)

 licenses-custom found 1 failed out of 2 total tests

New

 NPM check license (MIT OR GPL-3.0)

 Merge The pipeline for this merge request did not complete. Push a new commit to fix the failure, or check the [troubleshooting documentation](#) to see other possible actions.

[1]

Pipeline: Nicht-Erlaubtes Paket

Demonstration: OpenSource Wrapper: NPM-License-Compliance

Pipeline Needs Jobs 1 Failed Jobs 1 Tests 2

< licenses-custom

2 tests



1 failures

0 errors

50% success rate

0.00ms

Tests

Suite	Name	Filename	Status	Duration	Details
	NPM check license (MIT OR GPL-3.0)			0.00ms	View details
	NPM check license Other License			0.00ms	View details



[1]



Pipeline: Erlaubtes Paket





Demonstration: OpenSource Wrapper: NPM-License-Compliance


allowed package on npm custom checker

Overview 0 Commits 21 Pipelines 4 Changes 4


 **Request to merge** 6-allowed-package-on-...  into master


[Open in Web IDE](#) [Check out branch](#)  


 Pipeline #341275998 passed for f1830090 on 6-allowed-package-on-... 14 minutes ago   

 Approval is optional

[View eligible approvers](#)

 Test summary contained no changed test results out of 2 total tests [View full report](#) [Collapse](#)

 licenses-custom found no changed test results out of 2 total tests

 [Merge](#) ☒ Delete source branch ☐ Squash commits [?](#)

[21 commits](#) and [1 merge commit](#) will be added to master. [Modify merge commit](#)

[1]

Vielen Dank für Ihre Aufmerksamkeit

Jonas Kell
Universität Augsburg
jonas.kell@uni-augsburg.de
www.uni-augsburg.de

Quellen:

Textquellen & Referenzen

- (1) <https://gitlab.com/> (Dokumentation)
- (2) <https://www.validatis.de/kyc-prozess/news-fachwissen/compliance/> (Compliance)
- (3) <https://wirtschaftslexikon.gabler.de/definition/privatrecht-51965/wikipedia#Handelsrecht> (Rechtsformen)
- (4) https://www.haufe.de/compliance/management-praxis/compliance/bedeutung-von-compliance-fuer-unternehmen_230130_474234.html (Interne Regeln)
- (5) <https://www.intechcore.com/software-lizenzen-ein-ueberblick/> (Closed <-> Open Source)
- (6) <https://opensource.org/osd> (Definition Open-Source)
- (7) <https://opensource.org/licenses/mit-license.php> (MIT-Lizenz)
- (8) <https://thenewstack.io/options-for-monetizing-your-open-source-project/> (Dual-Licensing)
- (9) <https://medium.com/@vovabilonenko/licenses-of-npm-dependencies-bacaa00c8c65> (NPM and web licenses)
- (10) <https://medium.com/shakuro/software-licenses-explained-77f4f18eb1> (Welche Lizenzen und deren Interaktion)
- (11) <https://www.youtube.com/watch?v=0k-9DsStie0> (Weak Copyleft)
- (12) <https:// snyk.io/product/open-source-license-compliance/> (Snyk-Tool)
- (13) <https://fossa.com/product/open-source-license-compliance> (Fossa-Tool)
- (14) https://docs.gitlab.com/ee/user/compliance/license_compliance/ (Gitlab-Tool)
- (15) <https://www.npmjs.com/package/license-checker> (NPM OpenSource Tool)
- (16) <https://www.ibm.com/docs/de/adfz/developer-for-zos/14.1.0?topic=formats-junit-xml-format> (Dokumentation JUnit Format)

Quellen:

Bildquellen

- (1) <https://gitlab.com/> (Screenshots von Menüs, Eigens erstellte Projekte/Skripte)
- (2) https://images.clipartlogo.com/files/images/44/444589/warning-sign-clip-art_f.jpg
- (3) <https://www.ecovis.com/duesseldorf-koeln/wp-content/uploads/2020/09/compliance-1280x550.jpeg>
- (4) <https://www.spotify.com/de/>
- (5) https://miro.medium.com/max/1000/0*pCNV6XkrXyMCiLH9.png
- (6) [https://de.wikipedia.org/wiki/Npm_\(Software\)#/media/Datei:Npm-logo.svg](https://de.wikipedia.org/wiki/Npm_(Software)#/media/Datei:Npm-logo.svg)
- (7) <https://nabenhauer-consulting.com/wp-content/uploads/2012/09/lizenzen.png>
- (8) https://mma.prnewswire.com/media/1079457/Snyk_Logo.jpg?w=200
- (9) https://pbs.twimg.com/profile_images/1410659542279475201/KNZROjHy_400x400.jpg
- (10) https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/GitLab_logo.svg/1200px-GitLab_logo.svg.png
- (11) <https://www.suse.com/c/wp-content/uploads/2018/10/Open-Source-Software-.jpg>
- (12) <https://app.fossa.com/> (Screenshots von Test-Scan)
- (13) <https://snyk.io/product/open-source-license-compliance/> (Screenshots von Demo-Page)
- (14) <https://www.npmjs.com/package/license-checker> (NPM-Paket)
- (15) <https://github.com/Stuk/jszip/blob/master/LICENSE.markdown> (Lizenz Jszip)