Was wir wissen, was wir nicht wissen …

Dezernat 4

Bürgerservice, öffentliche Ordnung, Personal und IT

$ whoami
tobiasscherbaum

20+ Jahre Linux & OSS

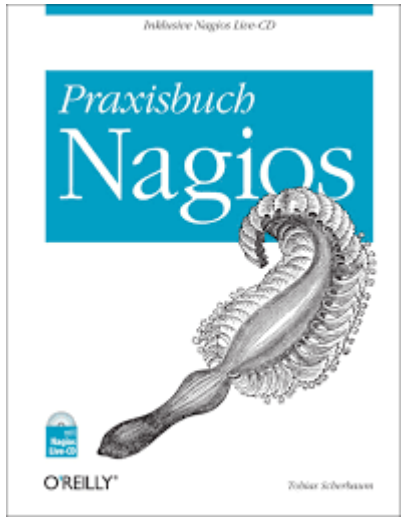
Admin

Monitoring

Sachgebietsleitung für Fachverfahren, Infrastruktur & IT-Sicherheit

Seit 2021: IT-Sicherheit

gentoo linux

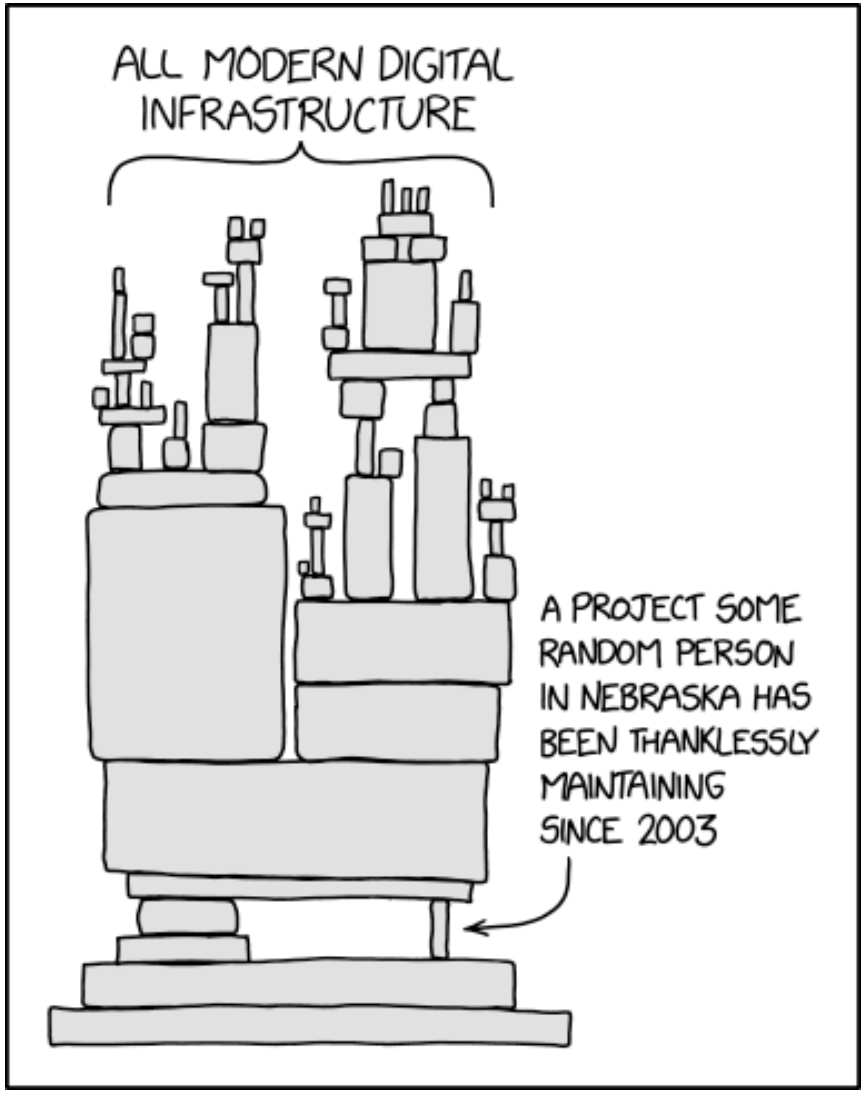


stadt
oberhausen

Was wir wissen, was wir nicht wissen …

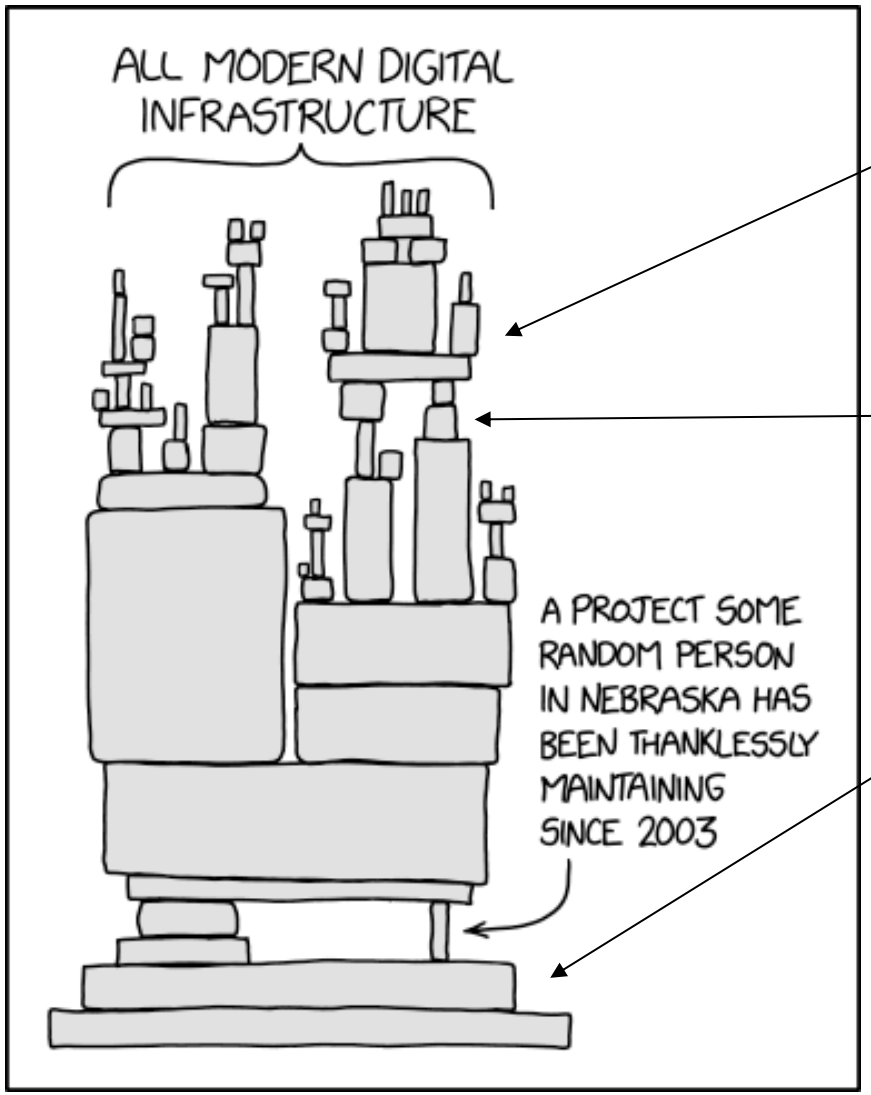
… mit Softwarestücklisten Sichtbarkeit schaffen

Kein Vortrag über Softwarestücklisten ohne …



Quelle: XKCD, https://xkcd.com/2347, Creative Commons Attribution-NonCommercial 2.5

Kein Vortrag über Softwarestücklisten ohne …



?

Alert!

Next.js: Kritische Lücke ermöglicht Kompromittierung von Web-Apps

Angreifer können eine Schwachstelle in Next.js missbrauchen, um die Autorisierung zu umgehen. Updates stehen bereit.

?

Alert!

Sicherheitsupdate: Ghostscript über mehrere Sicherheitslücken attackierbar

Der PostScript- und PDF-Interpreter Ghostscript ist verwundbar. Nutzer sollten die aktuelle Ausgabe installieren.

?

Alert!

Angriffe auf alte jQuery-Bibliotheken beobachtet

Die US-amerikanische IT-Sicherheitsbehörde warnt, dass Angreifer auf eine alte Sicherheitslücke in jQuery losgehen.

Quelle: XKCD, https://xkcd.com/2347, Creative Commons Attribution-NonCommercial 2.5

Quelle: Heise Online, heise.de

Ein funktionierendes Beispiel: Die Müsli-Stückliste

Lebensmittel-Kennzeichnungsverordnung von 1981

EU-Recht: Lebensmittel-Informationsverordnung von 2017

Kennzeichnung muss enthalten:

Verkehrsbezeichnung, Liste der Zutaten, Hersteller, MHD

… und bei Software?

Was ist eine Softwarestückliste?

- BSI TR-03183 Cyber-Resilienz-Anforderungen,
  Teil 2 Softwarestücklisten

- Strukturiert, maschinenlesbar, offene Standards

- SPDX:
  Verwalten von Open Source Lizenzen
  Linux Foundation
  ISO Standard

- CycloneDX:
  Identifizieren von Schwachstellen
  OWASP

Aussagen zu Komponenten oder Softwarestücklisten zu bekommen, ist gar nicht so einfach …

„Was ist das?“

„Haben wir nicht“

Unstrukturierte Listen

„wir entwickeln alles selbst“

Ein Beispiel aus der kommunalen Praxis

Teilkomponente einer Fachanwendung

Java-GUI

57 Bibliotheken

Ein Beispiel aus der kommunalen Praxis

Teilkomponente einer Fachanwendung

Java-GUI

57 Bibliotheken

Bibliothek	URL	Version
javax.mail.jar	https://javaee.github.io/javamail/	1.6.2
jaxb-api.jar	fi.java.net	2.3.0
jaxb-runtime.jar		2.3.1
jaxws-api.jar	https://github.com/javaee/jax-ws-spec	0
jboss-logging-annotations.jar	https://hibernate.org/	1.2.0.Beta1
jboss-logging.jar	https://hibernate.org/	3.4.1.FINAL
jboss-transaction-api_1.2_spec.jar	https://hibernate.org/	1.1.1.FINAL
jcifs.jar	https://www.jcifs.org/	1.3.17
jdom.jar	http://www.jdom.org/	1.0
jsch.jar	http://www.jcraft.com/jsch/	0.1.55
log4j.jar	https://logging.apache.org/log4j/2.x/	1.2.12
lucene-analyzers-common.jar	https://lucene.apache.org/	5.5.5
lucene-core.jar	https://lucene.apache.org/	5.5.5
passay.jar	https://www.passay.org	1.1.0

Ein Beispiel aus der kommunalen Praxis

Teilkomponente einer Fachanwendung

Java-GUI

57 Bibliotheken

Bibliothek	URL	Version
javax.mail.jar	https://javaee.github.io/javamail/	1.6.2
jaxb-api.jar	fi.java.net	2.3.0
jaxb-runtime.jar		2.3.1
jaxws-api.jar	https://github.com/javaee/jax-ws-spec	0
jboss-logging-annotations.jar	https://hibernate.org/	1.2.0.Beta1
jboss-logging.jar	https://hibernate.org/	3.4.1.FINAL
jboss-transaction-api_1.2_spec.jar	https://hibernate.org/	1.1.1.FINAL
jcifs.jar	https://www.jcifs.org/	1.3.17
jdom.jar	http://www.jdom.org/	1.0
jsch.jar	http://www.jcraft.com/jsch/	0.1.55
log4j.jar	https://logging.apache.org/log4j/2.x/	1.2.12
lucene-analyzers-common.jar	https://lucene.apache.org/	5.5.5
lucene-core.jar	https://lucene.apache.org/	5.5.5
passay.jar	https://www.passay.org	1.1.0

9 Komponenten „End of Life“, teilweise > 10 Jahre

Schwachstellen mit CVE in 5 Bibliotheken + 1 weitere ohne CVE

Zurück zu einem funktionierenden Beispiel: Die Müsli-Stückliste

Lebensmittel-Kennzeichnungsverordnung von 1981

EU-Recht: Lebensmittel-Informationsverordnung von 2017

Kennzeichnung muss enthalten:

Verkehrsbezeichnung, Liste der Zutaten, Hersteller, MHD

Auch der Konsum (hoch) verarbeiteter Software benötigt eine Kennzeichnung!

- Koalitionsvertrag 24. Bundesregierung „Ampel 2021-2025“
- Cyber Resilience Act, Lieferketten, Abhängigkeiten
- EU Produkthaftungs-Richtlinie 2024/2853
  Umsetzungsfrist in nationales Recht: 09.12.2026

  Haftung für Hersteller der Software,
  wie auch der Hersteller von Komponenten

  Ausnahme: Open Source, nicht gewerblich vertrieben

Softwarestücklisten selbst erstellen: syft

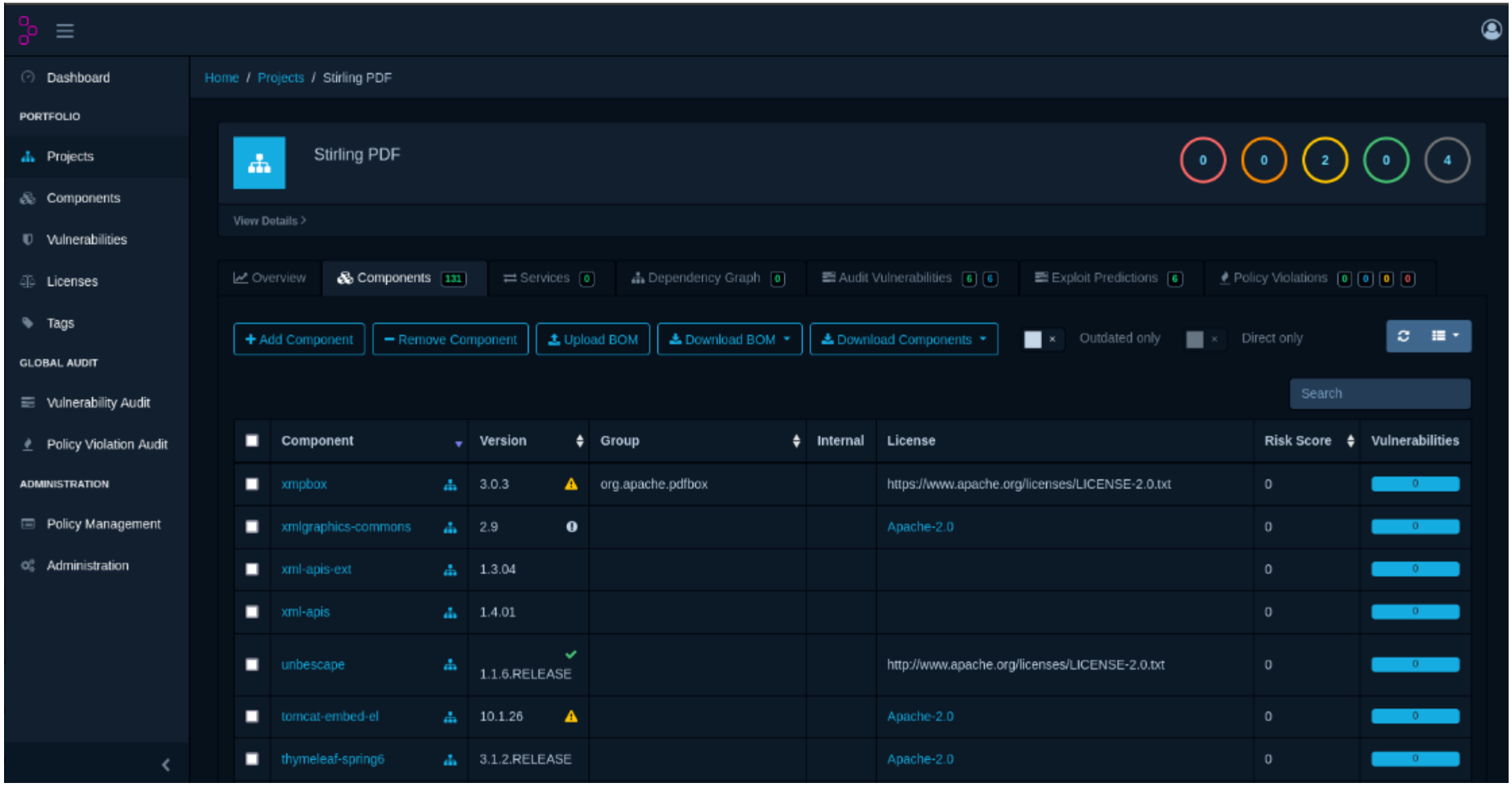
```
tobias@sbom:~/sample$ syft Stirling-PDF.jar
 ✔ Indexed file system                                                                                    Stirling-PDF.jar
 ✔ Cataloged contents                                                                                     7af9f75ac3b8c2dbbfa511579131dedfbd5e763f4920a7649251d51b0740c859
   ├── ✔ Packages                        [131 packages]
   ├── ✔ File digests                    [1 files]
   ├── ✔ File metadata                   [1 locations]
   └── ✔ Executables                     [0 executables]
NAME                                VERSION         TYPE
HdrHistogram                        2.2.2           java-archive
LatencyUtils                        2.0.3           java-archive
Simple-Configuration                1.8.4           java-archive  (+1 duplicate)
Simple-Yaml                         1.8.4           java-archive
Stirling-PDF                        0.28.2          java-archive
asm                                 9.7             java-archive
asm-commons                         9.7             java-archive
asm-tree                            9.7             java-archive
attoparser                          2.0.7.RELEASE   java-archive
batik-all                           1.17            java-archive
bcpkix-jdk18on                      1.78.1          java-archive
bcprov-jdk18on                      1.78.1          java-archive
```

```
tobias@sbom:~/sample$ syft -o cyclonedx-json=StirlingPDF.sbom Stirling-PDF.jar
 ✔ Indexed file system                                                                                    Stirling-PDF.jar
 ✔ Cataloged contents                                                                                     7af9f75ac3b8c2dbbfa511579131dedfbd5e763f4920a7649251d51b0740c859
   ├── ✔ Packages                        [131 packages]
   ├── ✔ File digests                    [1 files]
   ├── ✔ File metadata                   [1 locations]
   └── ✔ Executables                     [0 executables]
```

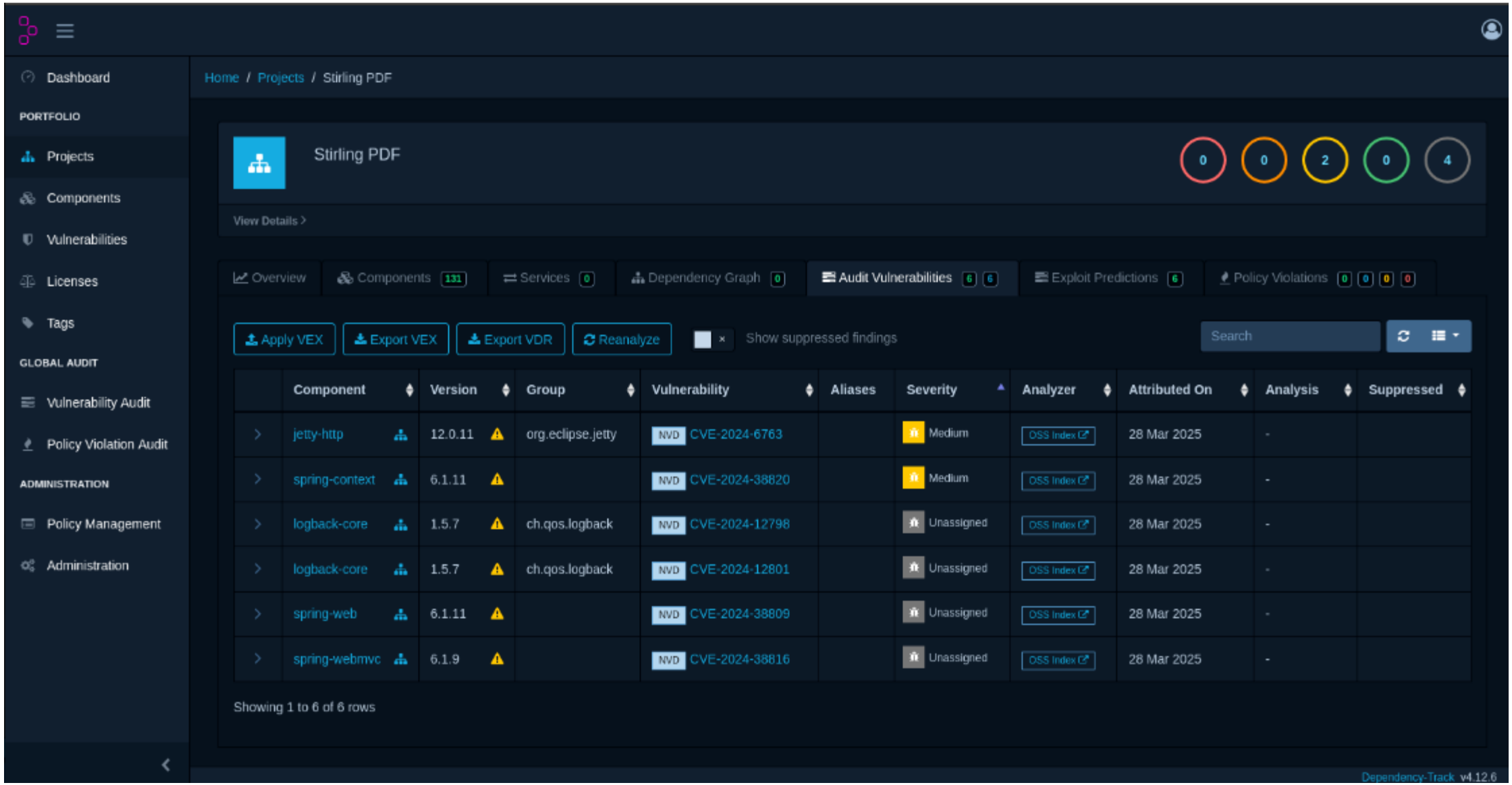
Softwarestückliste auf Schwachstellen analysieren: grype

```
tobias@sbom:~/sample$ grype StirlingPDF.sbom
 ✔ Vulnerability DB                [updated]
 ✔ Scanned for vulnerabilities     [7 vulnerability matches]
   ├── by severity: 0 critical, 2 high, 4 medium, 1 low, 0 negligible
   └── by status:   7 fixed, 0 not-fixed, 0 ignored
NAME             INSTALLED  FIXED-IN  TYPE          VULNERABILITY        SEVERITY
jetty-http       12.0.11    12.0.12   java-archive  GHSA-qh8g-58pp-2wxh  Medium
logback-core     1.5.7      1.5.13    java-archive  GHSA-pr98-23f8-jwxv  Medium
logback-core     1.5.7      1.5.13    java-archive  GHSA-6v67-2wr5-gvf4  Low
spring-context   6.1.11     6.1.14    java-archive  GHSA-4gc7-5j7h-4qph  Medium
spring-web       6.1.11     6.1.12    java-archive  GHSA-2rmj-mq67-h97g  Medium
spring-webmvc    6.1.9      6.1.13    java-archive  GHSA-cx7f-g6mp-7hqm  High
spring-webmvc    6.1.9      6.1.14    java-archive  GHSA-g5vr-rgqm-vf78  High
```

Softwarestückliste auf Schwachstellen analysieren: Dependency Track



Softwarestückliste auf Schwachstellen analysieren: Dependency Track



Es gibt Erfolge!

Ein erster Fachverfahrenshersteller stellt Softwarestücklisten mit dem Produkt bereit.

Die DUVA Anwendergemeinschaft hat Softwarestücklisten in den Entwicklungsprozess aufgenommen.

… und wer Softwarestücklisten findet … ;)

Idee: Sammeln von Softwarestücklisten in einem gemeinsamen OpenCode Repository?

Kontaktdaten

Stadt Oberhausen
Bereich 4-4 / IT
Essenerstr. 59
46047 Oberhausen

tobias.scherbaum@oberhausen.de