mischok
better. software_

Retten oder Reimplementieren?

ITS-NOW – 6. Juni 2024

It depends...

Julius Mischok

Was?

Konzeption und Umsetzung von Digitalstrategien in Web und Apps

Wie?

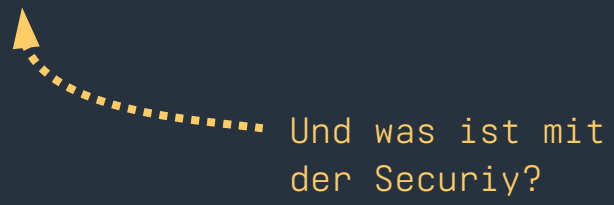
Durch hohe Qualität und moderne Teamarbeit

Warum?

Um die Welt ein bisschen besser zu machen!

Agenda

- Auf welcher Grundlage treffen wir die Entscheidung?
- Retten oder Reimplementieren?
- Wie überleben wir bis dahin?



mischok
better. software_

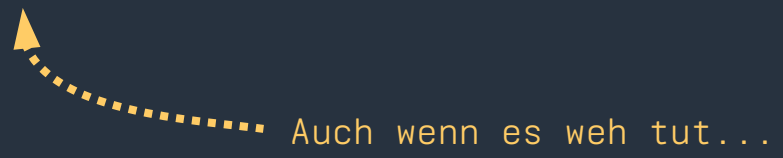
Umfrage

www.menti.com

Code: 1243 7365

mischok
better. software_

Real Talk



„Fiktives“ Beispiel

- Aufgabe: Refresh per JS nachziehen
- Lokales Setup: VM starten, da nur dort AD verfügbar ist
- Build mit ant, lokale Version inkompatibel
- Umgebungsvariablen nachziehen
- Build erfolgreich!
- Keine Veränderung im System

„Fiktives“ Beispiel

- Shutdown Tomcat, cleanup webapp Verzeichnis, neuer Build
- Änderung immer noch nicht da
- Browsercache leeren
- Änderung immer noch nicht da
- Duplizierten JavaScript Code finden
- ant Build starten
- *to be continued*

Quelle: https://www.pexels.com/photo/yelling-formal-man-watching-news-on-laptop-3760778/

mischok
better. software_

Code-Metrik: WTFs/min

mischok
better. software_

Ernsthafte Symptome für Legacy

mischok
better. software_

Ziel: 5-Minuten-Setup

Kompliziertes lokales Setup und Onboarding

mischok
better. software_

Skalierung der Entwicklungsleistung schwierig

Architektur und Setup
verhindern paralleles Arbeiten

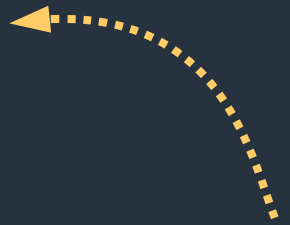
mischok
better. software_

Viele Bugs („Mikado Software“)

Sichtbar durch
Zwiebelschalen-Pattern

mischok
better. software_

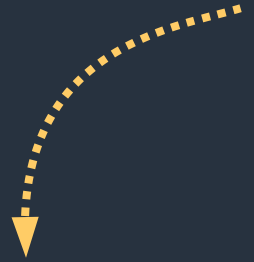
Fehlerregression



Chronische Verschlimmbesserungen

mischok
better. software_

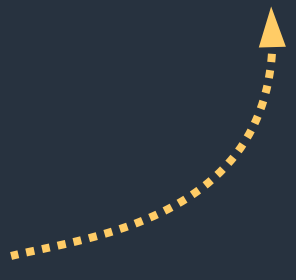
Offene Bibliotheksupdates,
erfasste Schulden



Offensichtliche technische Schulden

mischok
better. software_

Lange Time-to-Market



Lead-Time vs. Process-Time

mischok
better. software_

Unverhältnismäßige Featurekosten

Viel Muda/Waste im Prozess

mischok
better. software_

Webinar – 26. Juni 2024 10:00 Uhr

„Legacy Red Flags: Wann Wegwerfen die beste Option ist…“

Das Stockdale Paradoxon

Quelle: https://www.pexels.com/photo/rainforest-surrounded-by-fog-975771/

Quelle: https://www.pexels.com/photo/rainforest-surrounded-by-fog-975771/

Quelle: https://www.pexels.com/photo/rainforest-surrounded-by-fog-975771/

Fahrplan

- Bestandsaufnahme
- Entscheiden
- Zwischenzeit gestalten

Regelmäßig wiederholen!

mischok
better. software_

Fragen zur Bestandsaufnahme

Welchen Wert hat die Software?

- Für welchen Preis würde sie jemand kaufen?
- Wie viele Lizenzen sind verkauft?
- Welche Vertriebsperspektiven gibt es?

Wie kritisch ist die Software?

- Welche Geschäftsprozesse basieren darauf?
- Welche anderen Systeme sind davon abhängig?
- Welche Downtimes sind verkraftbar?
- Läuft die Software durchgehend oder nur zeitweise?

Wie ist die Software dokumentiert?

- Ist wirklich bekannt, wie das System funktioniert?
- Wie hoch ist der „Bus-Faktor“ des Projekts?

Wie ist der technische Zustand der Software?

- Werden veraltete Bibliotheken verwendet?
- Werden abgekündigte Bibliotheken verwendet?
- Wie ist die Codequalität (statische Codeanalyse)?
- Wie viel globalen Status und wie viele Seiteneffekte gibt es?
- Gibt es erfasste technische Schulden?

Wie ist die Systemarchitektur?

- Welche Komponenten werden verwendet?
- Werden diese Komponenten immer noch unterstützt?
- Besteht die Möglichkeit zur Modularisierung?

Wie ist der Automatisierungsstand der Software?

- Existieren Tests und wie hoch ist die Testabdeckung?
- Wie hoch ist die Testqualität?
- Gibt es CI/CD Pipelines? Ist das Ziel mehrerer Livedeployments pro Stunde erreichbar?
- Wie komplex ist das Projektsetup?

Wie steht es um die Sicherheit?

- Welches Ergebnis liefert ein OWASP Scan?
- Gibt es auslaufenden Support für verwendete Systembestandteile und Bibliotheken?

Haben wir die Technologie im Griff?

- Besteht im Team Erfahrung mit den verwendeten Technologien?
- Sind die Bibliotheken dokumentiert?
- Gibt es eine lebendige Community?

Forum: Struts

Need help regarding Struts 2

Sagar Rohankar
Ranch Hand
Posts: 2908

1

I like...

posted 16 years ago

+1 Quote Report

Hi ranchers,.

I am new to struts,

How to create and run a simple app of Struts 2 in tomcat , plus how to import Struts 2 project in Easy Eclipse ?

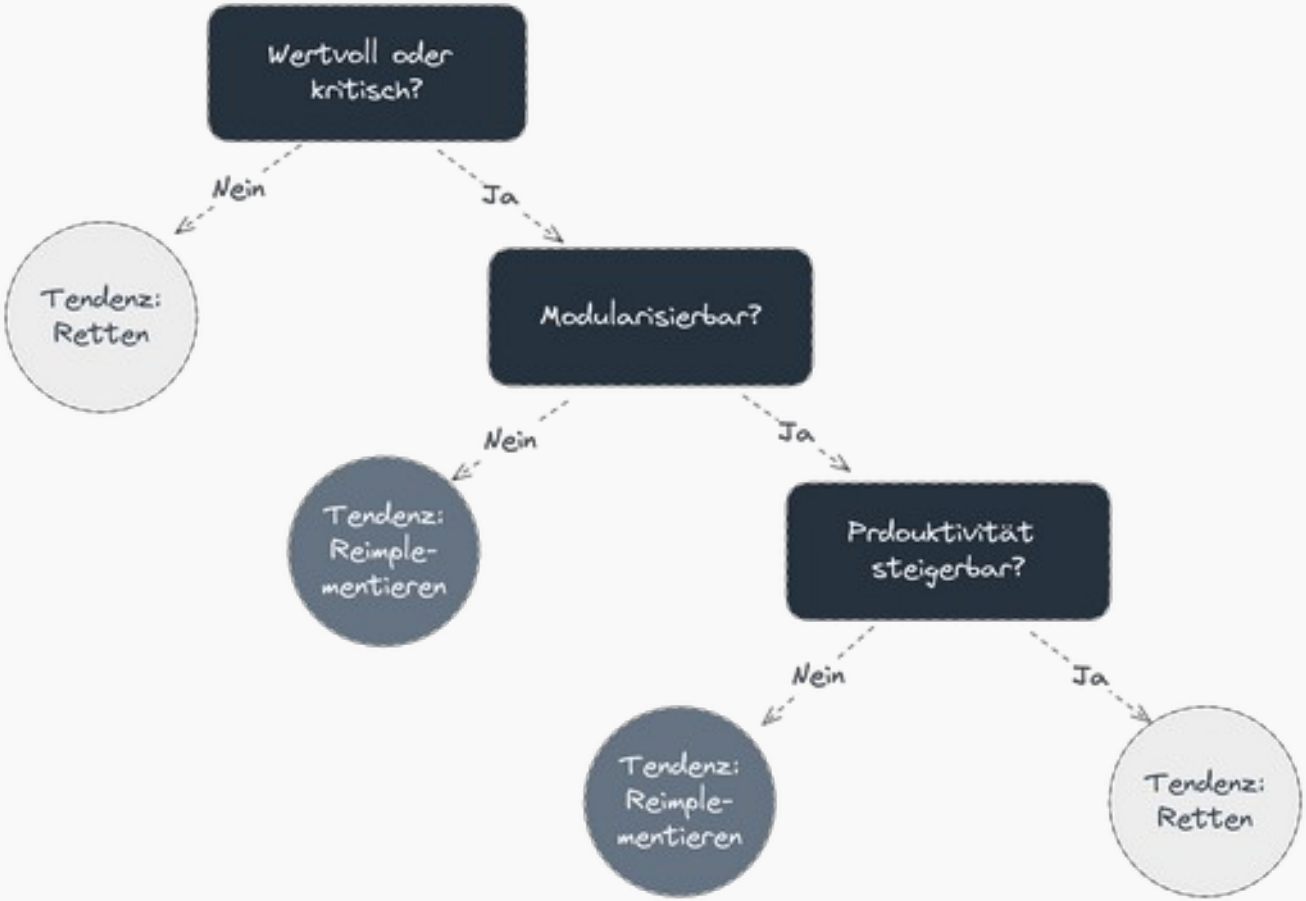
Thanks in advance ,

regardz,

mischok
better. software_

Entscheidungsfindung

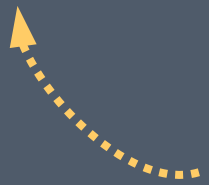
mischok
better. software_



mischok
better. software_

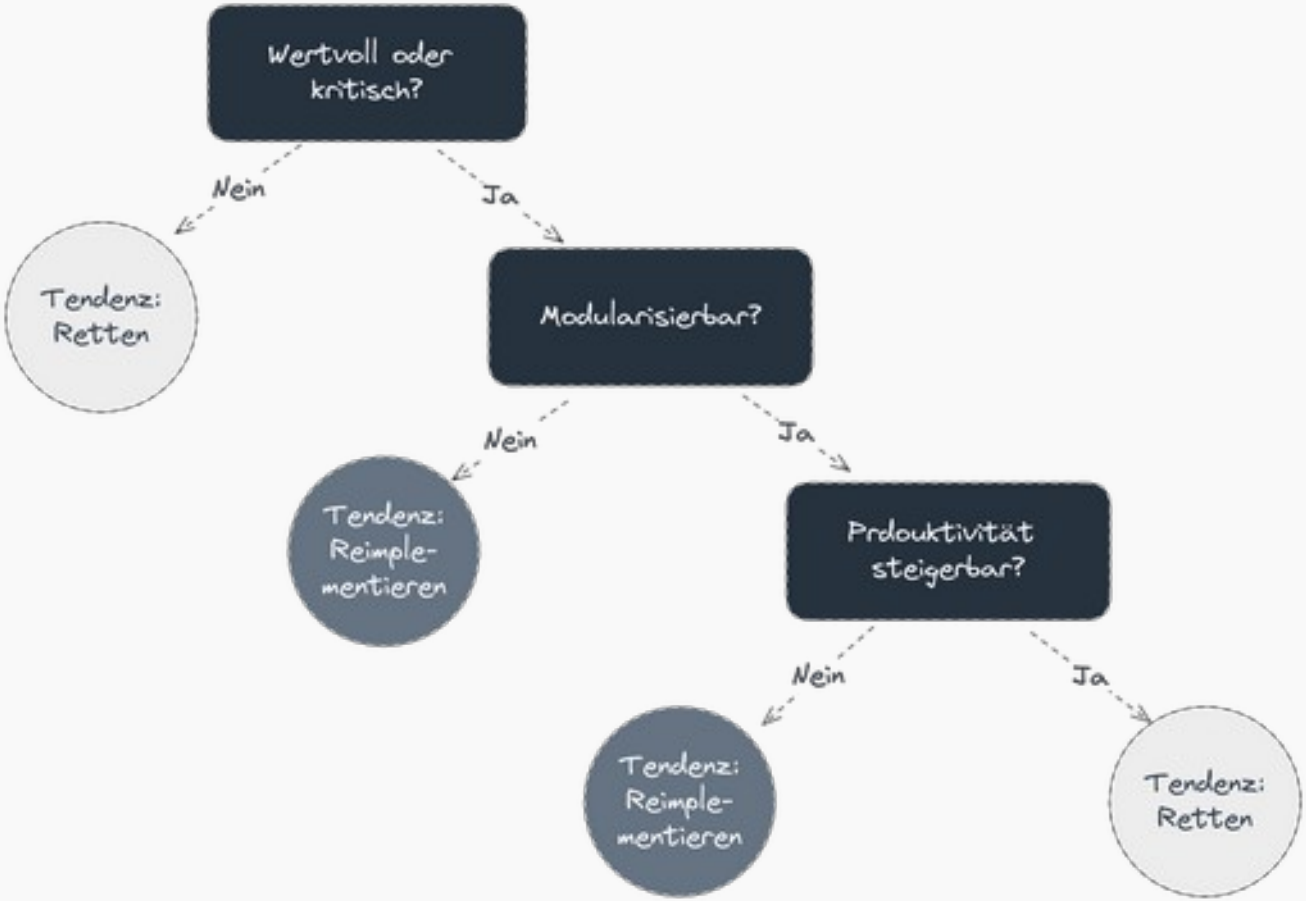
Ist die Software so wertvoll oder kritisch,
dass sie weiterlaufen muss?

Nein? Tendenz „Retten“!



- Wie lange muss sie noch laufen?
- Wie kann der Betrieb sichergestellt werden?
- Ist ein plötzlicher Ausfall zu verkraften?
- Welche sicherheitskritischen Patches müssen umgesetzt werden?

mischok
better. software_



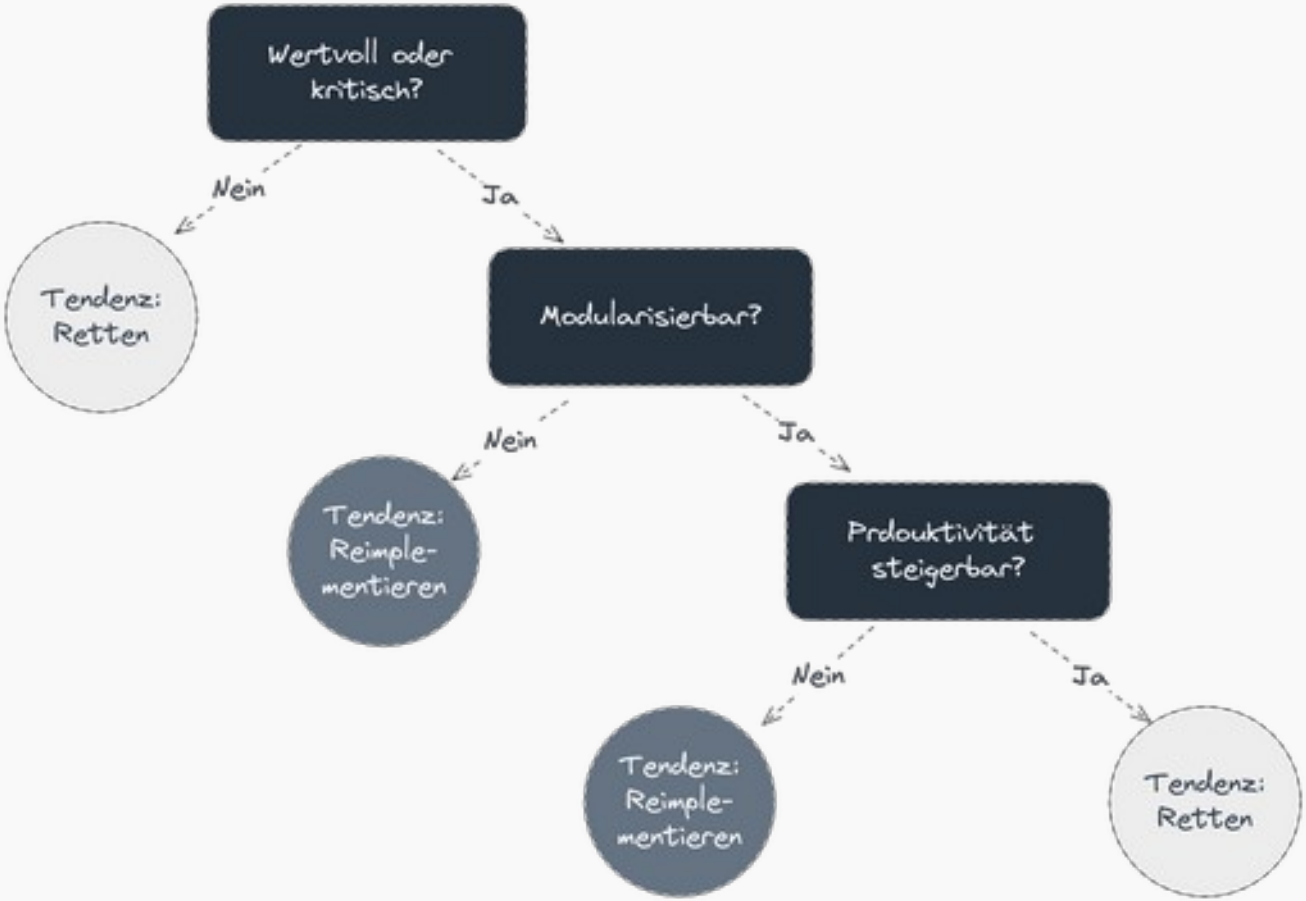
mischok
better. software_

Kann die Software
inkrementell/modular angepasst werden?

Nein? Tendenz „Reimplementieren“!

- Können Betrieb und Reimplementierung parallel laufen?
- Sind die Anforderungen für die Reimplementierung klar?
- Was kann wiederverwendet werden?
- Wie ist der Zeitrahmen für die Reimplementierung (Security, abgekündigte Komponenten)?
- Wie kann der Switchover aussehen? Wie eine Datenmigration?

mischok
better. software_



mischok
better. software_

Lässt sich die Produktivität
durch Prozessanpassung deutlich steigern?

Nein? Tendenz „Reimplementieren“!

- Können Betrieb und Reimplementierung parallel laufen?
- Sind die Anforderungen für die Reimplementierung klar?
- Was kann wiederverwendet werden?
- Wie ist der Zeitrahmen für die Reimplementierung (Security, abgekündigte Komponenten)?
- Wie kann der Switch-Over aussehen? Wie eine Datenmigration?

Ja? Tendenz „Retten“!

- Wie lässt sich ein gesunder Mix aus Konsolidierung und Weiterentwicklung finden?
- Wie lange darf sich der Rettungsprozess hinziehen, was ist das Ziel?
- Besteht die technische Kompetenz für die Rettung?
- Übersteigen die Kosten für die Rettung den zu erzielenden Mehrwert?

mischok
better. software_

Die Zwischenzeit gestalten

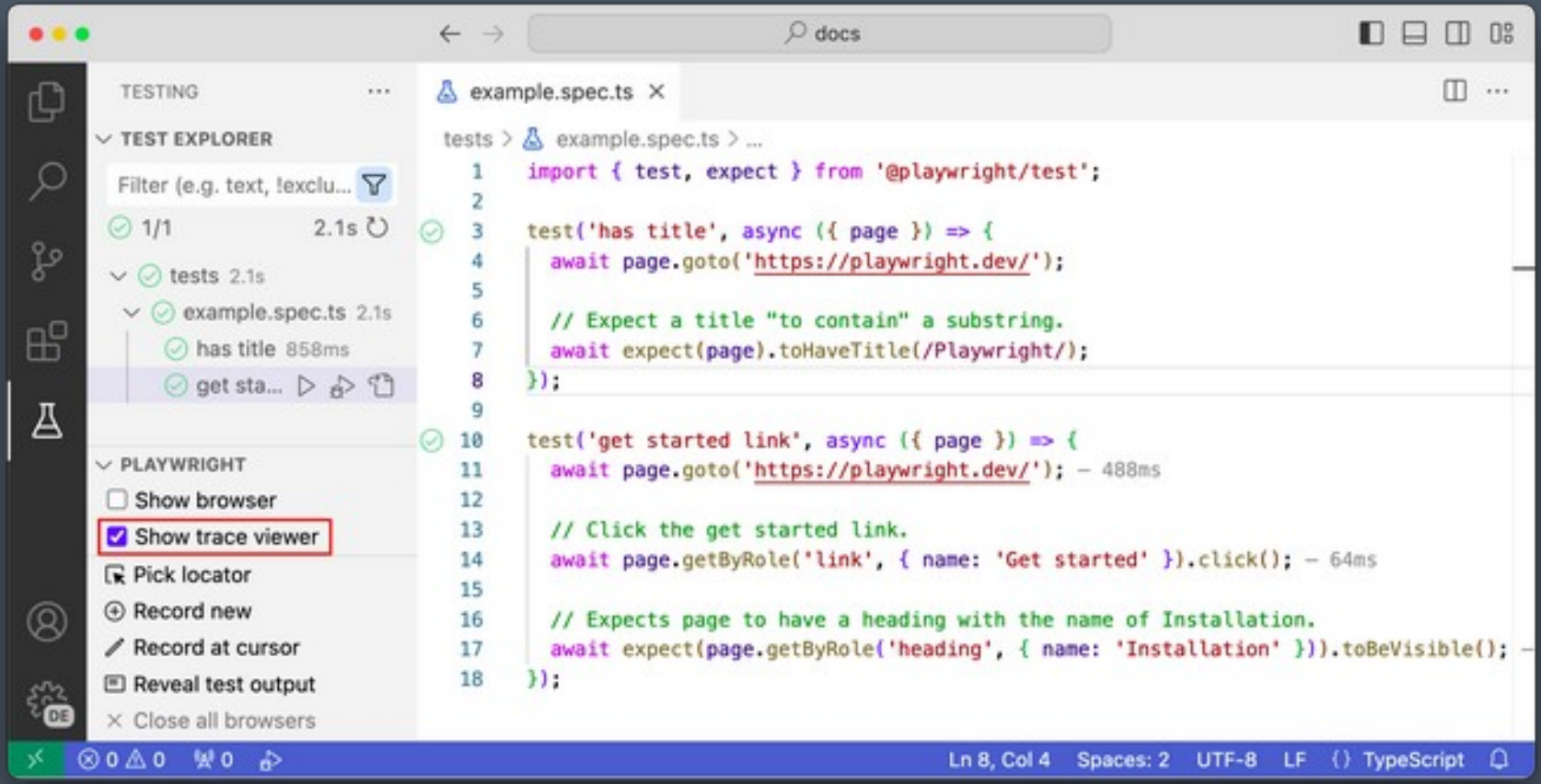
Tests als Basis für Refactoring

Quelle: https://www.pexels.com/photo/two-people-paragliding-together-12575878/

Reusable E2E Tests

Quelle: https://www.pexels.com/photo/two-people-paragliding-together-12575878/

Beispiel: Playwright



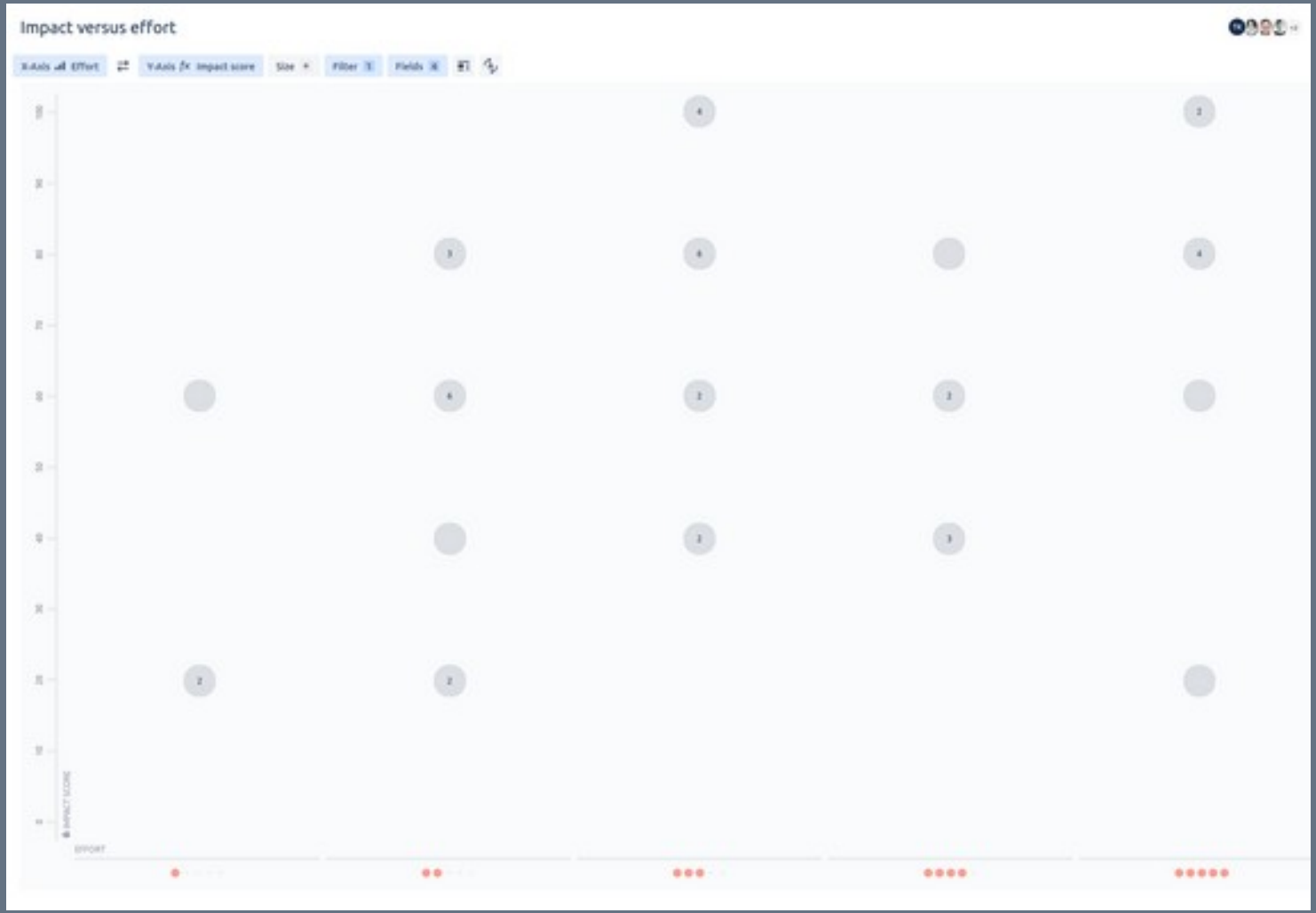
Quelle: https://playwright.dev/docs/getting-started-vscode

Interfaces/Blackboxes

Quelle: https://www.pexels.com/photo/interior-of-unfinished-building-with-white-paint-7937303/

Quelle: https://www.pexels.com/photo/three-people-sitting-beside-table-416405/

Quelle: https://www.pexels.com/photo/close-up-photo-of-person-holding-unripe-mango-2895712/


Impact versus effort
X-Axis Effort
Y-Axis Impact score
Size
Filter
Fields
IMPACT SCORE
EFFORT

mischok
better. software_

Case Study

OWASP Dependency Check einbinden

mischok
better. software_

Situation: Eine unfreiwillige Zeitreise

mischok
better. software_

Ziel: Argumentation gegenüber Management

mischok
better. software_

About Buildtools

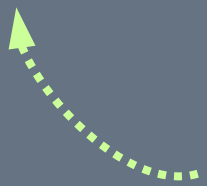
mischok
better. software_

```
<dependencies>
    ...
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-data-jpa</artifactId>
    </dependency>
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-security</artifactId>
    </dependency>
    ...
</dependencies>
```

```
./mvnw dependency:tree
...
[INFO] +- org.springframework.boot:spring-boot-starter-data-jpa:jar:3.3.0:compile
[INFO] |  +- org.springframework.boot:spring-boot-starter-aop:jar:3.3.0:compile
[INFO] |  |  \- org.aspectj:aspectjweaver:jar:1.9.22:compile
[INFO] |  +- org.springframework.boot:spring-boot-starter-jdbc:jar:3.3.0:compile
[INFO] |  |  +- com.zaxxer:HikariCP:jar:5.1.0:compile
[INFO] |  |  \- org.springframework:spring-jdbc:jar:6.1.8:compile
[INFO] |  +- org.hibernate.orm:hibernate-core:jar:6.5.2.Final:compile
[INFO] |  |  +- jakarta.persistence:jakarta.persistence-api:jar:3.1.0:compile
[INFO] |  |  +- jakarta.transaction:jakarta.transaction-api:jar:2.0.1:compile
[INFO] |  |  +- org.jboss.logging:jboss-logging:jar:3.5.3.Final:compile
[INFO] |  |  +- org.hibernate.common:hibernate-commons-annotations:jar:6.0.6.Final:runtime
[INFO] |  |  +- io.smallrye:jandex:jar:3.1.2:runtime
[INFO] |  |  +- com.fasterxml:classmate:jar:1.7.0:compile
[INFO] |  |  +- net.bytebuddy:byte-buddy:jar:1.14.16:runtime
[INFO] |  |  +- org.glassfish.jaxb:jaxb-runtime:jar:4.0.5:runtime
[INFO] |  |  |  \- org.glassfish.jaxb:jaxb-core:jar:4.0.5:runtime
[INFO] |  |  |     +- org.glassfish.jaxb:txw2:jar:4.0.5:runtime
[INFO] |  |  |     \- com.sun.istack:istack-commons-runtime:jar:4.1.2:runtime
[INFO] |  |  +- jakarta.inject:jakarta.inject-api:jar:2.0.1:runtime
[INFO] |  |  \- org.antlr:antlr4-runtime:jar:4.13.0:compile
[INFO] |  +- org.springframework.data:spring-data-jpa:jar:3.3.0:compile
[INFO] |  |  +- org.springframework.data:spring-data-commons:jar:3.3.0:compile
[INFO] |  |  +- org.springframework:spring-orm:jar:6.1.8:compile
[INFO] |  |  +- org.springframework:spring-context:jar:6.1.8:compile
[INFO] |  |  \- org.springframework:spring-tx:jar:6.1.8:compile
[INFO] |  \- org.springframework:spring-aspects:jar:6.1.8:compile
...
```

mischok
better. software_

About OWASP Dependency Check



Open Worldwide Application
Security Project

Published Vulnerabilities

CVE-2021-29425 (OSSINDEX) suppress

commons-io - Path Traversal [CVE-2021-29425]

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv3:

- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:

- OSSINDEX - [CVE-2021-29425] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- OSSIndex - https://github.com/apache/commons-io/pull/52
- OSSIndex - https://issues.apache.org/jira/browse/IO-556
- OSSIndex - https://issues.apache.org/jira/browse/IO-559

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:commons-io:commons-io:1.3.2:*:*:*:*:*:*:*

Vorgehen

- Umstellung auf Maven
- Durchführung Dependency Check
- Anheben möglichst vieler Dependencies

Ergebnis

- Dringender Handlungsbedarf!
- Isoliertes Update einzelner Bibliotheken möglich
- Gesamtprojekt muss reimplementiert werden

Wrapup

Wrapup

- Legacy is real – Confront the brutal facts!
- Bestandsaufnahme aus unterschiedlichen Blickwinkeln
- Weiterbetrieb gestalten
- Iterieren

mischok
better. software_

Wo steht dein Projekt?

Weiterführende Informationen

Inventory Canvas

https://www.mischok.digital/legacy-software/inventory-tool

Webinar

„Legacy Red Flags: Wann Wegwerfen die beste Option ist…“

26. Juni 2024 10:00 Uhr

Vielen Dank!

Kontakt:

julius.mischok@mischok.de

https://www.linkedin.com/in/julius-mischok/

mischok
better. software_