

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?

Und was ist mit
der Security?

Umfrage



www.menti.com

Code: 1243 7365

Real Talk

 Auch wenn es weh tut...

„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*



Code-Metrik: WTFs/min

Ernsthafte Symptome für Legacy

Ziel: 5-Minuten-Setup



Kompliziertes lokales Setup und Onboarding

Skalierung der Entwicklungsleistung schwierig



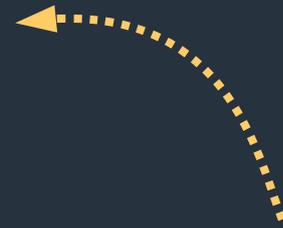
Architektur und Setup
verhindern paralleles Arbeiten

Viele Bugs („Mikado Software“)

Sichtbar durch
Zwiebelschalen-Pattern



Fehlerregression



Chronische Verschlimmbesserungen

Offene Bibliotheksupdates,
erfasste Schulden



Offensichtliche technische Schulden

Lange Time-to-Market

Lead-Time vs. Process-Time



Unverhältnismäßige Featurekosten



Viel Muda/Waste im Prozess

Webinar – 26. Juni 2024 10:00 Uhr

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

A photograph of a dense rainforest with tall, thin trees and thick undergrowth. The scene is shrouded in mist or fog, with sunlight filtering through the canopy, creating a soft, ethereal atmosphere. The foreground is filled with various green plants and ferns.

Das Stockdale Paradoxon

A photograph of a lush, misty rainforest. The scene is filled with tall, slender trees and dense, vibrant green foliage. A thick layer of mist or fog hangs in the air, softening the background and creating a sense of depth and mystery. The lighting is diffused, highlighting the textures of the leaves and the intricate network of vines and branches. The overall atmosphere is serene yet slightly somber due to the mist.

Confront the brutal facts...

A photograph of a lush, misty rainforest. Tall, slender trees rise vertically, their trunks partially obscured by a thick layer of white mist or fog. The foreground is filled with dense, vibrant green foliage, including various ferns and broad-leafed plants. The overall atmosphere is serene and ethereal, with soft light filtering through the canopy.

... yet never lose faith!

Fahrplan

- Bestandsaufnahme
- Entscheiden
- Zwischenzeit gestalten



Regelmäßig wiederholen!

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?

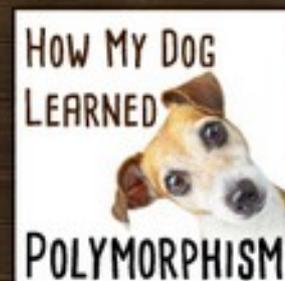
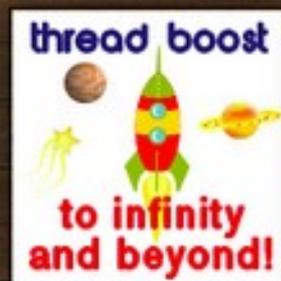
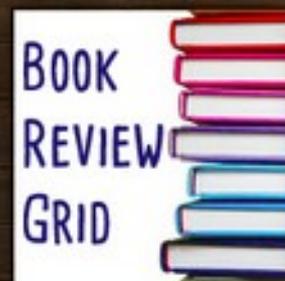
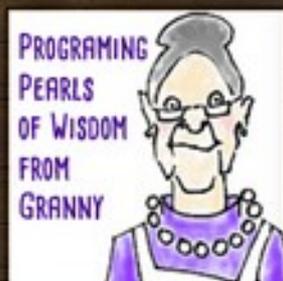
- Existieren Tests und wie hoch ist die Testabdeckung?
- Wie hoch ist die Testqualität?
- Gibt es CI/CD Pipelines? Ist das Ziel mehrerer Livedeployments pro Stunde erreichbar?
- Wie komplex ist das Projektsetup?

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?



Post Reply

Bookmark Topic

Watch Topic

New Topic

programming forums

Java

Mobile

Certification

Databases

Caching

Books

Forum: Struts

Need help regarding Struts 2

Sagar Rohankar

Ranch Hand

Posts: 2908



1 like...



posted 16 years ago



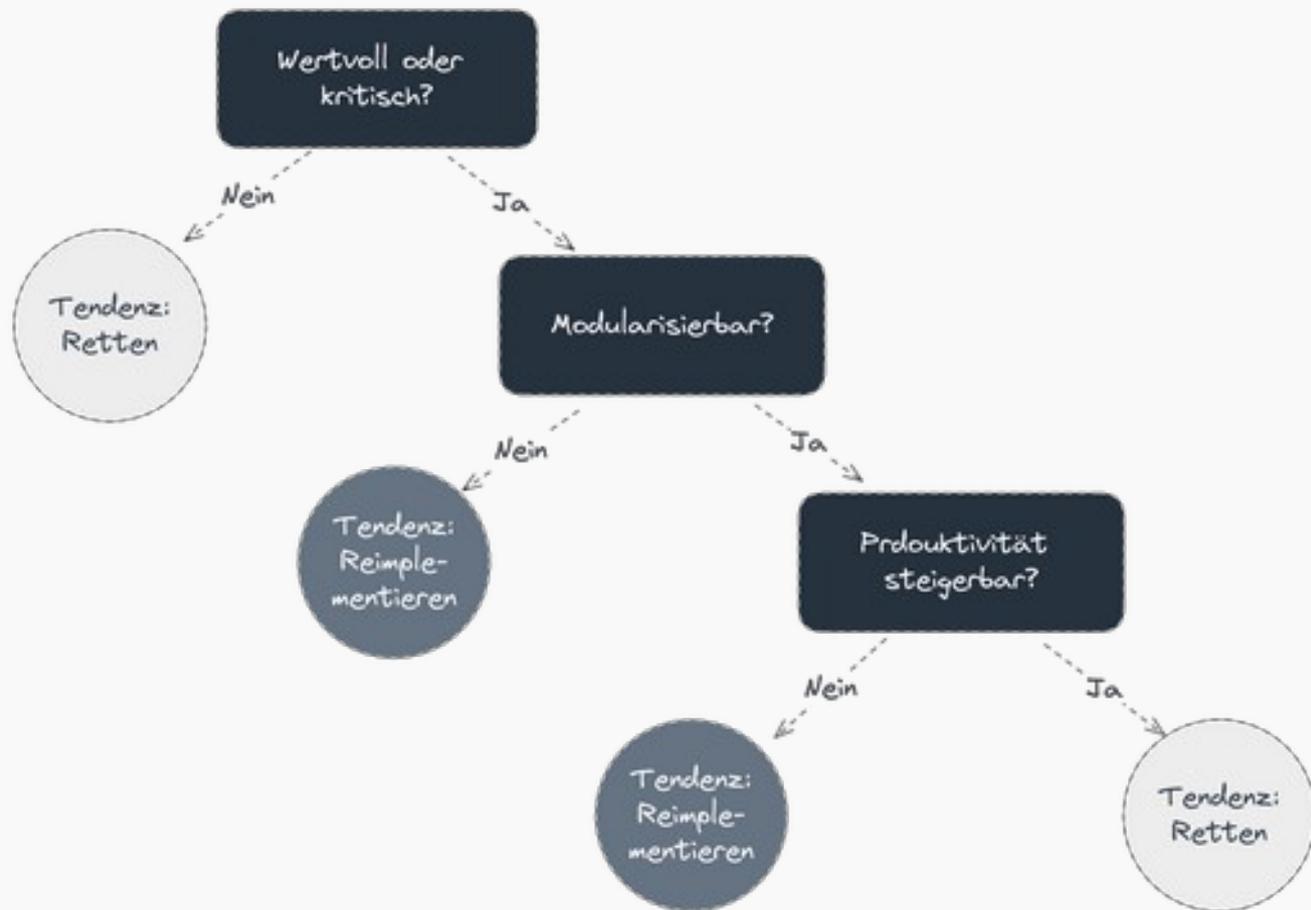
Hi ranchers,.

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 ,

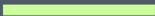
regardz,

Entscheidungsfindung



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

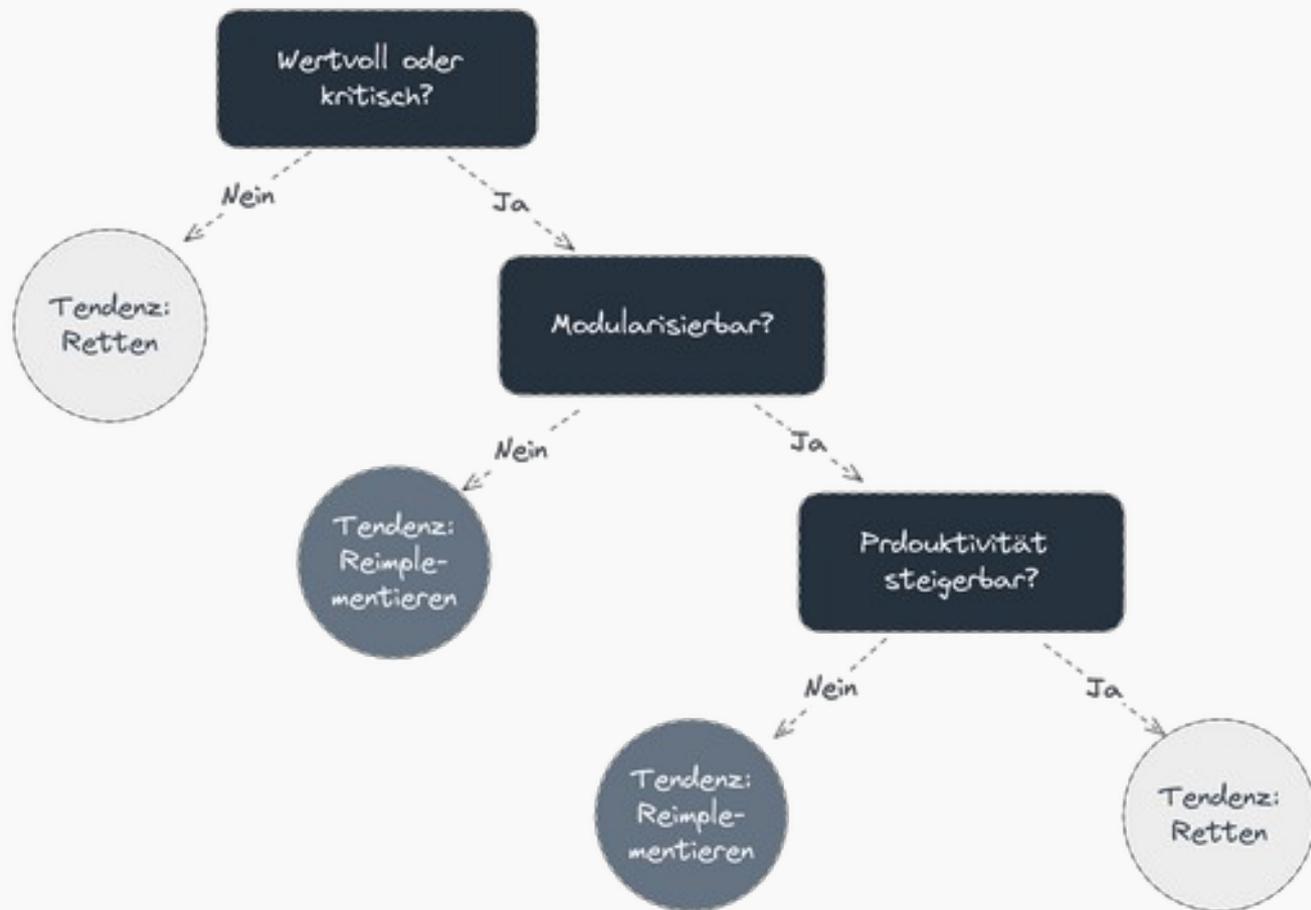
Nein? Tendenz „Retten“!



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



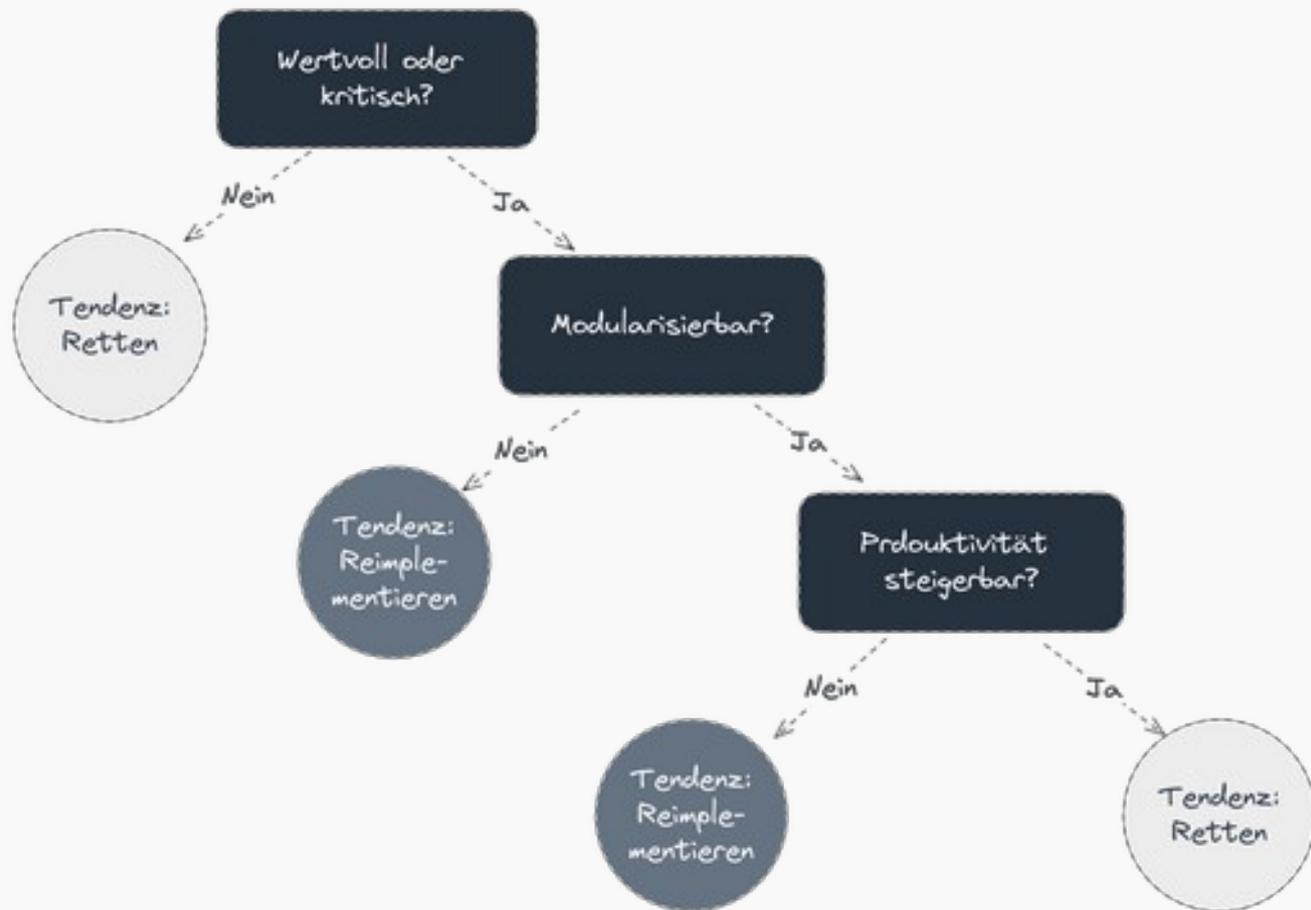
Lebenserhaltende
Maßnahmen



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?



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?

Die Zwischenzeit gestalten

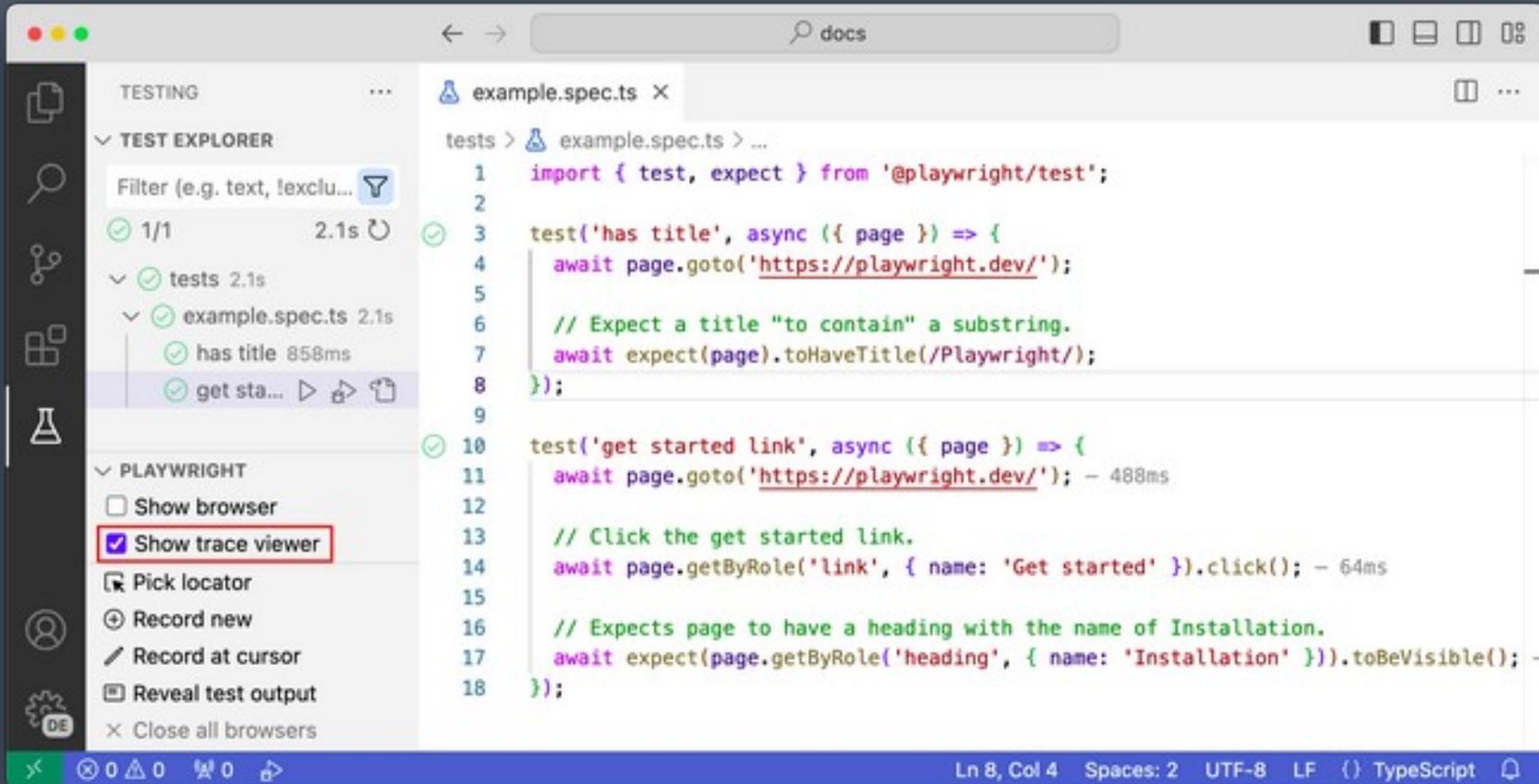
A high-angle, first-person perspective shot of two people paragliding. They are suspended by a network of colorful ropes (red, blue, purple, green) against a backdrop of a lush green forest, a winding road, and a body of water. The sun is bright, creating a lens flare effect on the left side of the image. The two individuals are wearing helmets and harnesses, and appear to be smiling and enjoying the activity. A semi-transparent white banner is overlaid across the middle of the image, containing the text 'Tests als Basis für Refactoring'.

Tests als Basis für Refactoring

A large cable-stayed bridge with white pylons and cables spans across a body of water. In the background, a city skyline is visible under a clear blue sky. The bridge's deck is a light grey color, and the water below is a deep blue. The overall scene is bright and clear.

Reusable E2E Tests

Beispiel: Playwright



The image shows a perspective view down a hallway in an unfinished building. The walls are white, and the ceiling is made of exposed wooden beams. A doorway is visible at the end of the hallway, leading to another room with a window. The floor is concrete. There are some electrical wires and outlets visible on the wall in the foreground.

Interfaces/Blackboxes

An overhead view of three people sitting around a wooden conference table in an office. The table is covered with large architectural blueprints. A man in a light blue shirt is pointing at a blueprint with a yellow highlighter. A man in a light grey shirt is using a calculator. A woman in a blue shirt is looking at the blueprints. On the table, there is a blue hard hat, a dark mug, a smartphone, a laptop, a printer, and several stacks of papers. The office floor has a patterned carpet.

Conways Law

A close-up photograph of a person's hand holding a large, green, unripe mango. The mango is the central focus, held gently in the palm. The background is filled with lush green mango leaves, some in sharp focus and others blurred, creating a sense of depth. A semi-transparent grey horizontal bar is overlaid across the middle of the image, containing the text "Impact/Effort".

Impact/Effort

Impact versus effort



X Axis: Effort Y Axis: Impact score Size: Filter: Fields: [Icons]



Case Study

OWASP Dependency Check einbinden

Situation: Eine unfreiwillige Zeitreise

Ziel: Argumentation gegenüber Management

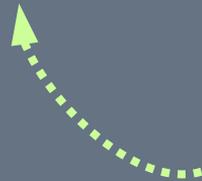
About Buildtools

```
<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  
...
```

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

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_