

security testing in continuous integration

Agenda

whoami?

why?

what?

how?

whoami?



synyx GmbH Karlsruhe

**Software nach Maß
Code Clinic
Open Source**

**Christian Kühn
Senior System Developer**

#java #kubernetes #devops

@DevOpsKA Meetup Organizer



questions ?!

software security issues: what could possibly go wrong?

- leakage of business data**
- leakage of user/customer data**
- service interruption**
- industry malfunction**
- death (🤯)**

examples:

equifax - "Credit Monitoring"

hacked 2017

vulnerability in Apache Struts dependency

143,000,000 SSN

209,000 credit card numbers

182,000 "consumers" with PII

<https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/>

examples:

Mossack Fonseca - "Law Firm and corporate service provider"

**hacked 2015
vulnerability in Drupal**

**11.5 million leaked documents about
money laundering
tax avoidance
corruption**

https://en.wikipedia.org/wiki/Panama_Papers

what stops developers from patching?

negligence

priorities / lack of time

skills / training

insight

"security - not my department" (or is it?)

security issues = technical debt

Solution?

DevSecOps

CAUTION

**ENTERING
BUZZWORD
ZONE**

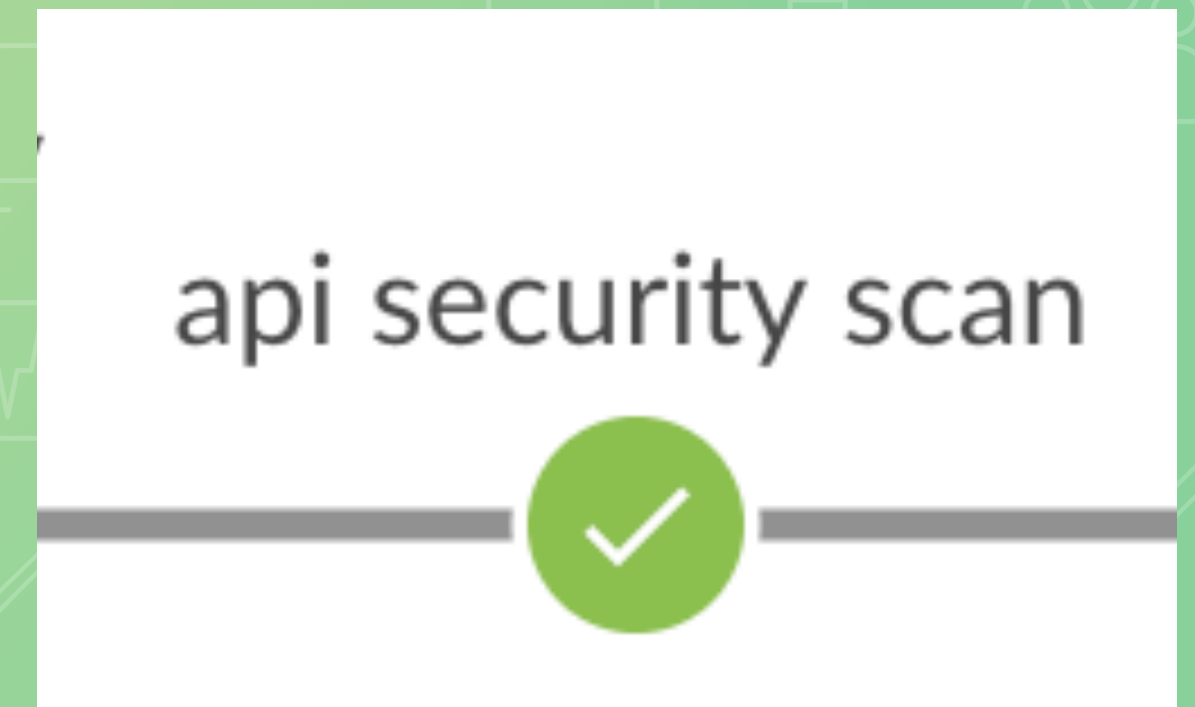
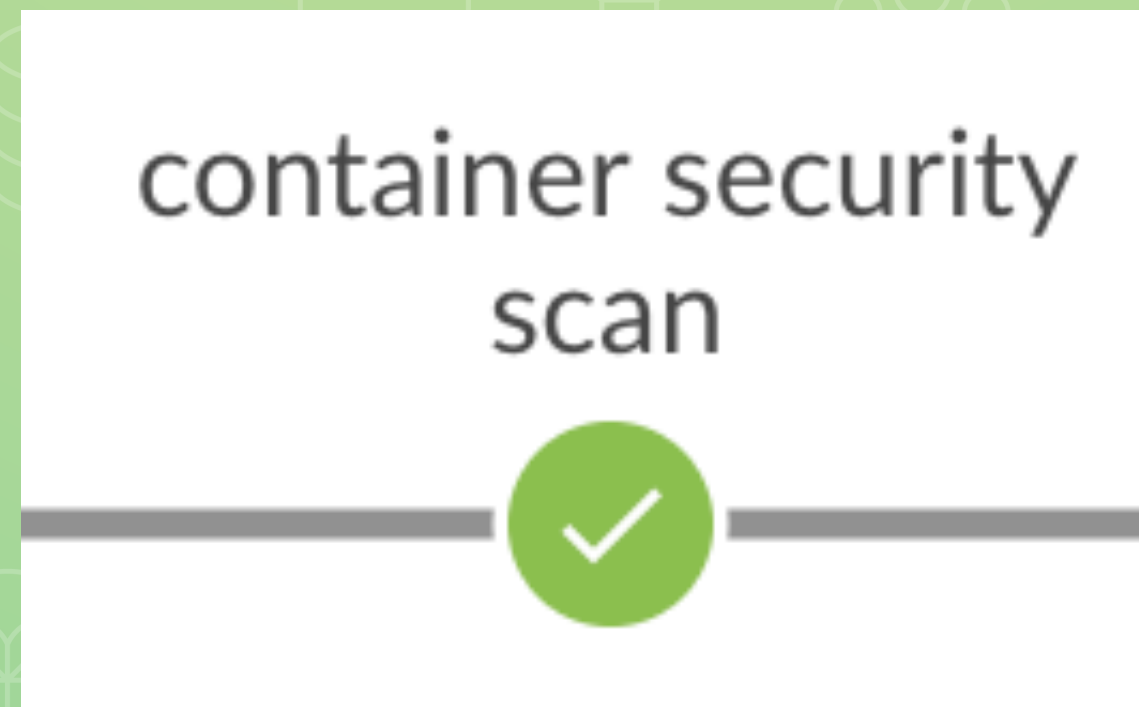
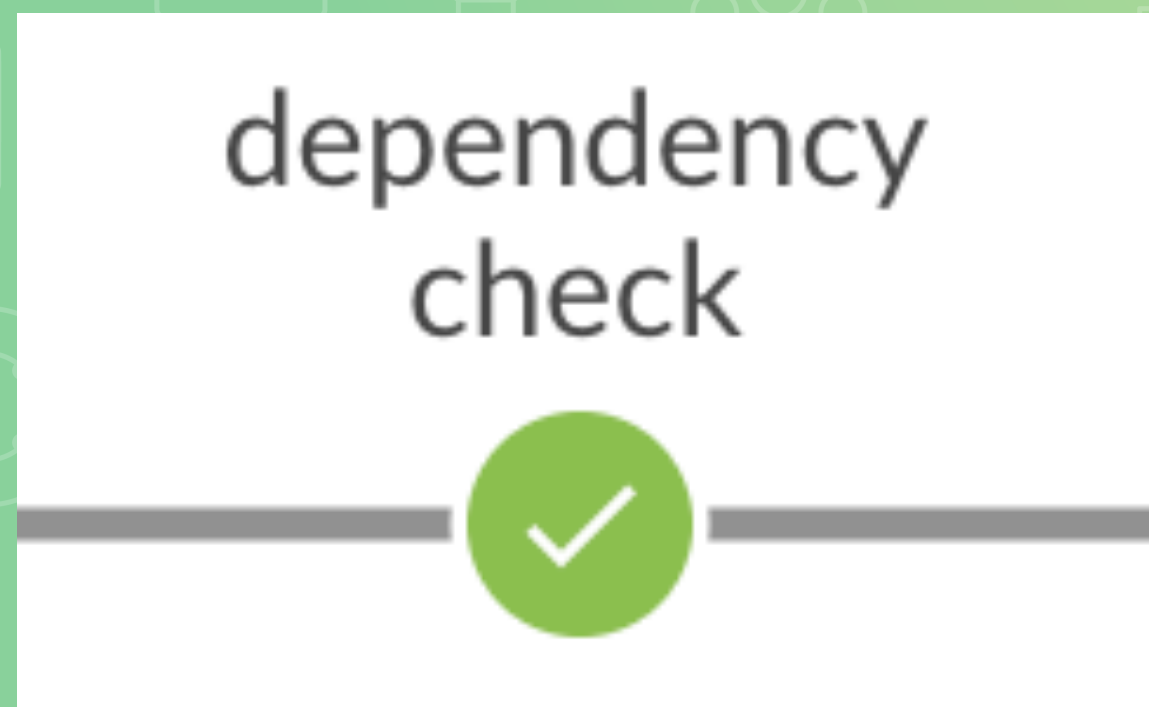
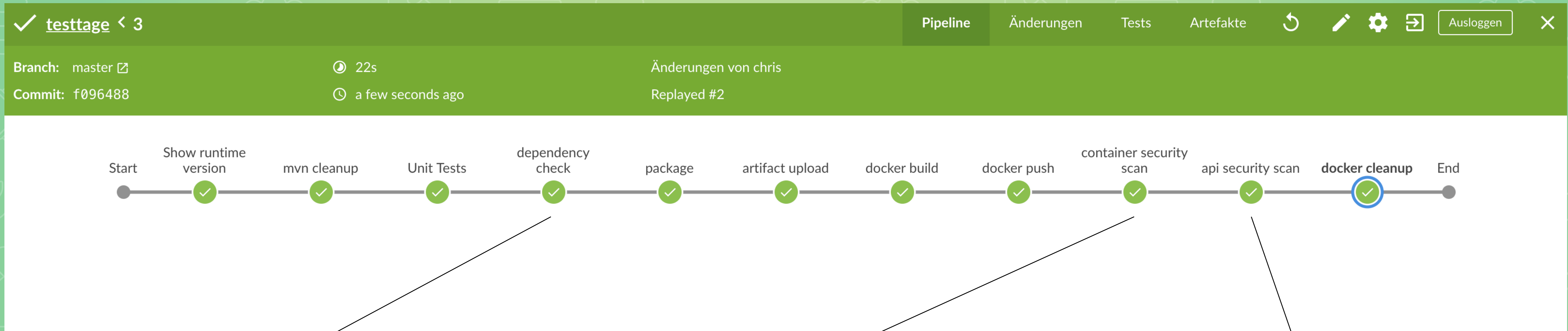
continuous delivery

✓ **testtage 1** > Pipeline Änderungen Tests Artefakte Ausloggen

Branch: master 1m 41s Keine Änderungen
Commit: 35bd92b 7 minutes ago Branch indexing

```
graph LR; Start((Start)) --- S1((✓ Show runtime version)); S1 --- S2((✓ mvn cleanup)); S2 --- S3((✓ Unit Tests)); S3 --- S4((✓ package)); S4 --- S5((✓ artifact upload)); S5 --- S6((✓ docker build)); S6 --- S7((✓ docker push)); S7 --- End((End)); style S7 stroke:#007bff,stroke-width:2px
```

continuous delivery++



continuous delivery++

testtage < 2

Pipeline

Änderungen

Tests

Artefakte



Ausloggen

Branch: master

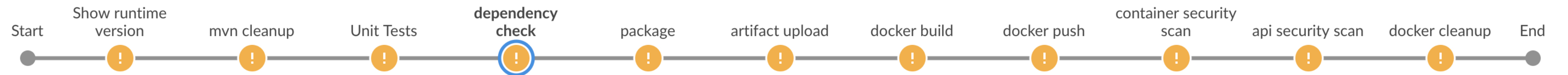
2m 40s

Änderungen von chris

Commit: f096488

an hour ago

Branch indexing



automatically find KNOWN vulnerabilities in

dependencies

docker images

web apis / urls

CVE - Common Vulnerabilities and Exposures

vulnerability

/vʌln(ə)rə'bilɪti/

noun

1. the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

...

CVE - reference for publicly known information-security vulnerabilities and exposures

CVE-2017-5638 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Source: MITRE

Description Last Modified: 09/22/2017

[+View Analysis Description](#)

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 10.0 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (V3 legend)

Impact Score: 6.0

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Changed

CVSS v2.0 Severity and Metrics:

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): Complete

Integrity (I): Complete

Availability (A): Complete

QUICK INFO

CVE Dictionary Entry:

[CVE-2017-5638](#)

NVD Published Date:

03/10/2017

NVD Last Modified:

03/03/2018

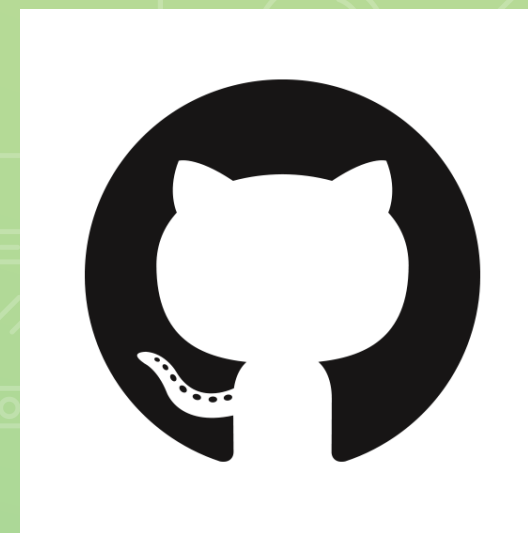
dependencies

**example: little maven/springboot demo-project:
github.com/cy4n/broken**

6 maven dependencies

71 transitive dependencies

find vulnerable dependencies

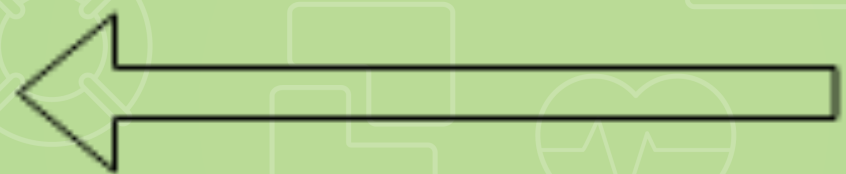


DEPENDENCY-CHECK



local .h2 db

CVE Data



<https://NVD.nist.gov>



`mvn dependency-check:check`



> Issues

▼ OWASP-Dependency-Check

Critical Severity Vulnerabilities	0
High Severity Vulnerabilities	1
Inherited Risk Score	9
Low Severity Vulnerabilities	1
Medium Severity Vulnerabilities	1
Total Dependencies	178
Total Vulnerabilities	5
Vulnerable Component Ratio	1.7%

> Reliability ?	
▼ Security ?	
Overview	🔗
On new code	
Vulnerabilities	0
Rating	A
Remediation Effort	0
Overall	
Vulnerabilities	14
Rating	D
Remediation Effort	3h 40min
> Maintainability ?	
> Coverage	
> Duplications	
> Size	
> Complexity ?	
> Issues	
▼ OWASP-Dependency-Check	
Critical Severity Vulnerabilities	0
High Severity Vulnerabilities	1
Inherited Risk Score	9
Low Severity Vulnerabilities	1
Medium Severity Vulnerabilities	1
Total Dependencies	178
Total Vulnerabilities	5
Vulnerable Component Ratio	1.7%



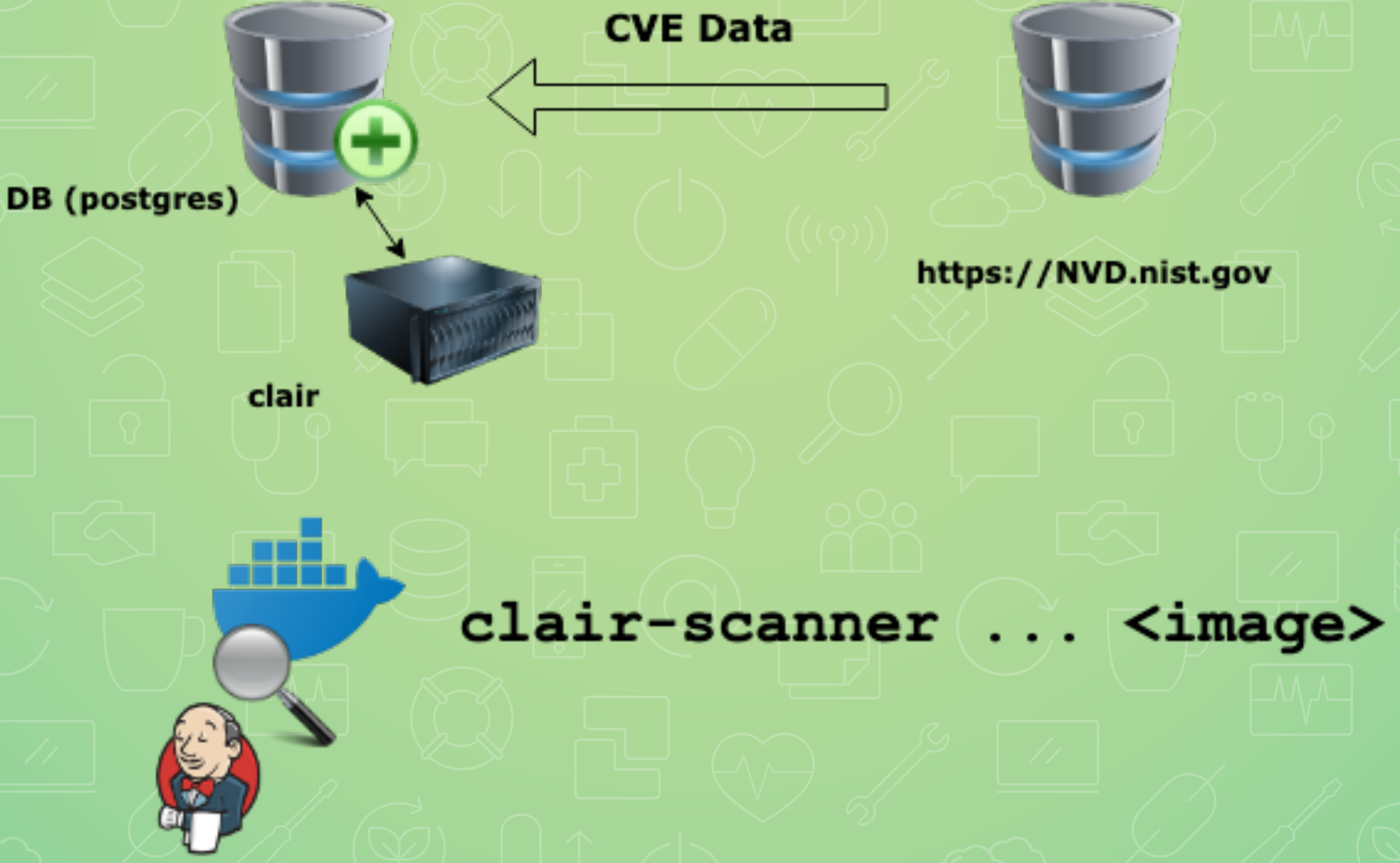
container

docker pull cy4n/broken

```
FROM cy4n/broken:latest
```

clair

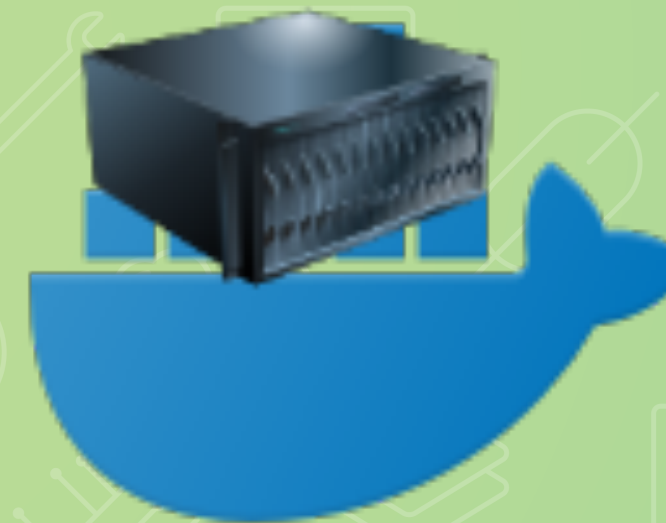
A Container Image Security Analyzer by CoreOS



<https://github.com/arminc/clair-local-scan>



**arminc/clair-db
(nightly)**



arminc/clair-local-scan

```
docker run -d --name db arminc/clair-db:latest
```

```
docker run -p 6060:6060 --link db:postgres -d --name clair arminc/clair-local-scan
```



clair

A Container Image Security Analyzer by CoreOS

QUAY Repositories Tutorial Docs Blog + 5+ J jakedt

example/repository 56c0fa71e47b

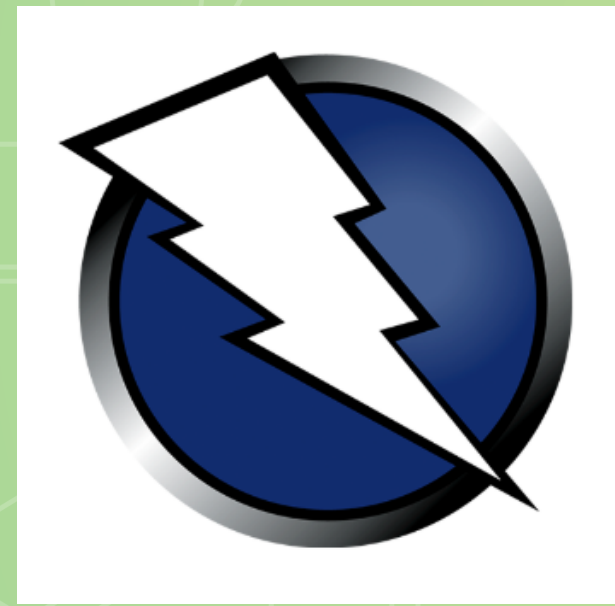
Quay Security Scanner has detected **13** vulnerabilities.
Patches are available for **4** vulnerabilities.

🔴 1 High-level vulnerabilities.
🟡 1 Medium-level vulnerabilities.
🟠 2 Low-level vulnerabilities.
⚠️ 5 Negligible-level vulnerabilities.
🔍 4 Unknown-level vulnerabilities.

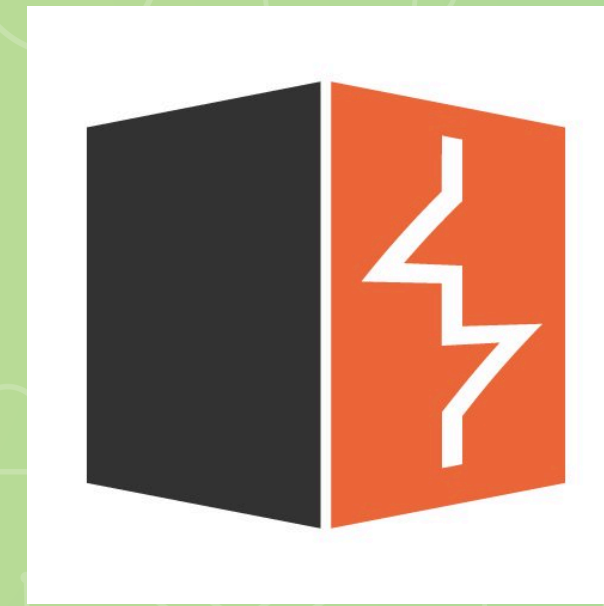
Image Vulnerabilities Filter Vulnerabilities... Only show fixable

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
▶ CVE-2013-7445	🔴 High	linux	3.16.7-ckt20-1+deb8u3	(None)	RUN apt-get up.
▶ CVE-2015-5276	🟡 Medium	gcc-4.9	4.9.2-10	(None)	ADD file:b5391.
▶ CVE-2016-2856	🟠 Low	glibc	2.19-18+deb8u3	(None)	ADD file:b5391.
▶ CVE-2016-0823	🟠 Low	linux	3.16.7-ckt20-1+deb8u3	(None)	RUN apt-get up.
▶ CVE-2005-3660	⚠️ Negligible *	linux	3.16.7-ckt20-1+deb8u3	(None)	RUN apt-get up.
▶ CVE-2015-4003	⚠️ Negligible *	linux	3.16.7-ckt20-1+deb8u3	(None)	RUN apt-get up.
▶ CVE-2008-4108	⚠️ Negligible *	python-defaults	2.7.9-1	(None)	RUN apt-get up.
▶ CVE-2015-8830	⚠️ Negligible	linux	3.16.7-ckt20-1+deb8u3	🟢 3.16.7-ckt20-1+deb8u4	RUN apt-get up.
▶ CVE-2013-4392	⚠️ Negligible *	systemd	215-17+deb8u3	(None)	ADD file:b5391.
▶ CVE-2015-7515	⚠️ Unknown	linux	3.16.7-ckt20-1+deb8u3	(None)	RUN apt-get up.
▶ CVE-2015-8816	⚠️ Unknown	linux	3.16.7-ckt20-1+deb8u3	🟢 3.16.7-ckt20-1+deb8u4	RUN apt-get up.
▶ CVE-2016-2547	⚠️ Unknown	linux	3.16.7-ckt20-1+deb8u3	🟢 3.16.7-ckt20-1+deb8u4	RUN apt-get up.
▶ CVE-2016-2545	⚠️ Unknown	linux	3.16.7-ckt20-1+deb8u3	🟢 3.16.7-ckt20-1+deb8u4	RUN apt-get up.

API / Webserver



ZAP Proxy



burp

API / Webservice

OWASP ZAProxy



url spider
passive (and active) modes
dynamic scanner
ajax supported



zap2docker



myApp

```
docker run -t owasp/zap2docker-stable zap-baseline.py -t http://<URL>  
HTTP
```



how to react?