security testing
in continuous integration

Christian Kühn - @CYxChris

Agenda

whoami?

why?

what?

how?

whoami?

Christian Kühn
Senior System Developer

#java #kubernetes #devops

synyx GmbH Karlsruhe

Software nach Maß
Code Clinic
Open Source

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 coprorate 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

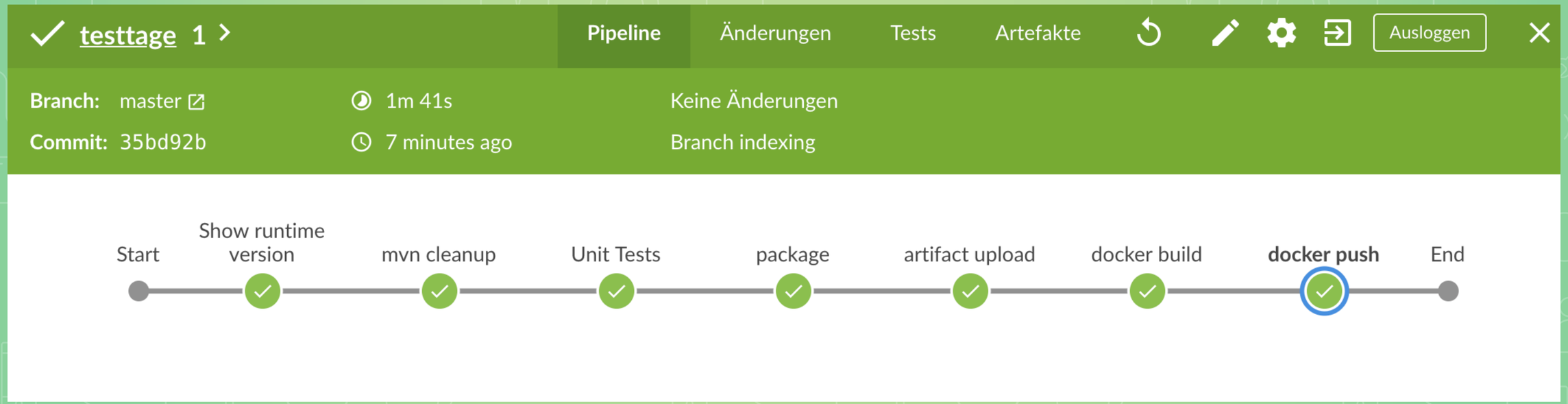
Solution?

DevSecOps

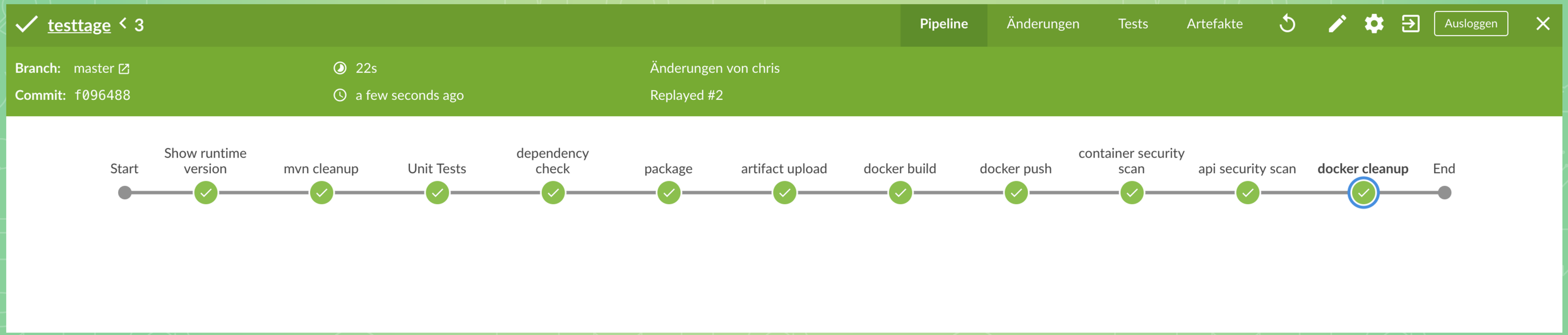
DevOps

DevOps is a set of practices that automates the processes between software development and IT teams, in order that they can build, test, and release software faster and more reliably.

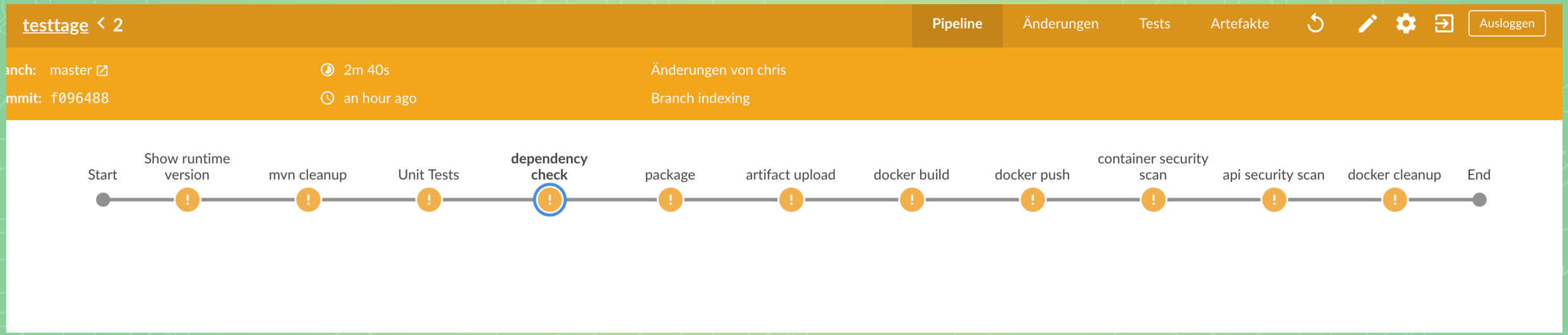
continuous delivery



continuous delivery extended



continuous delivery extended



automate the sh!t out of it

automatically find KNOWN vulnerabilities in

dependencies

docker images

web apis / urls

CVE - Common Vulnerabilities and Exposures

vulnerability

/vʌln(ə)rəˈbɪlɪti/

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

OWASP dependency-check

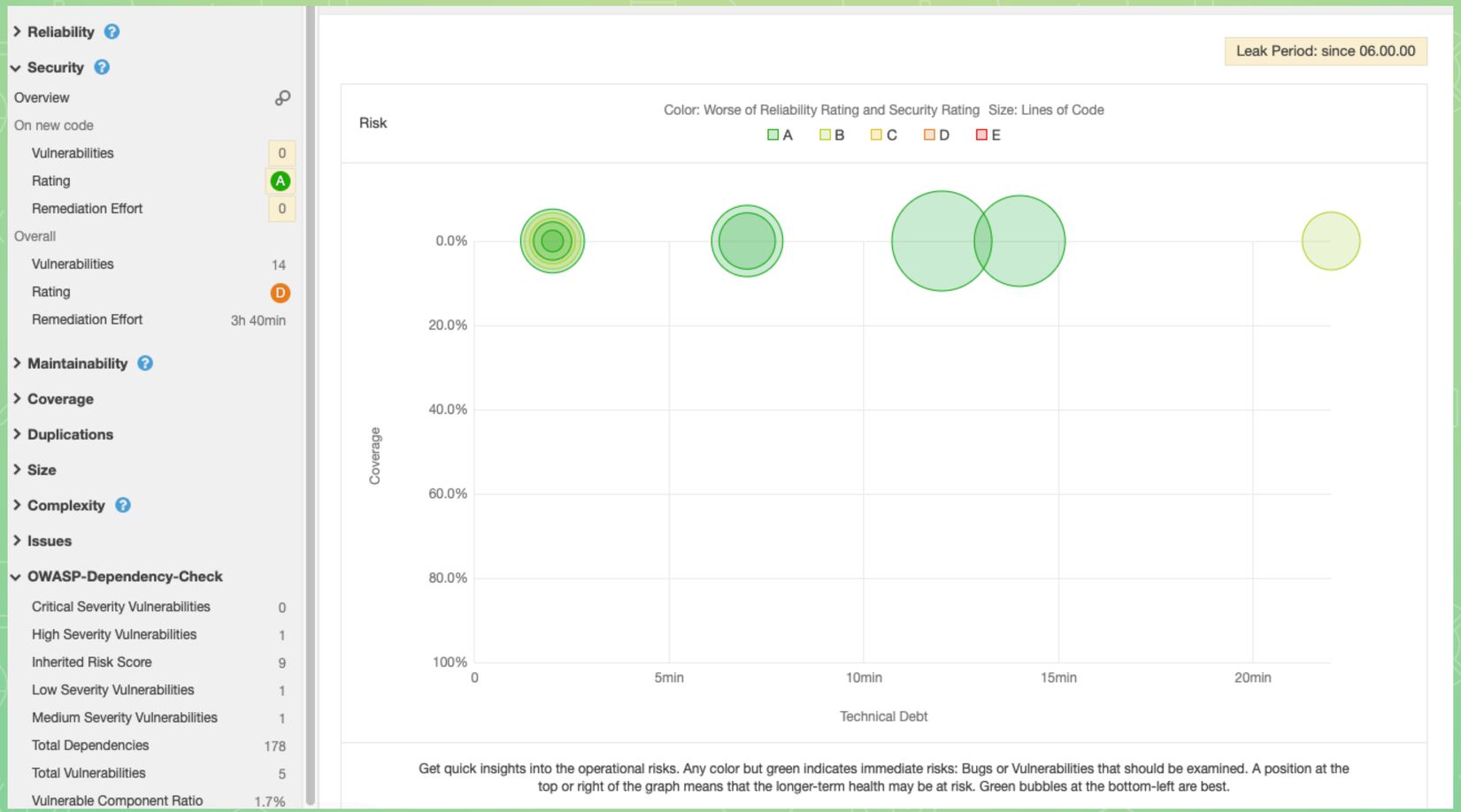
pulls CVE data from NIST database

check local project and write report

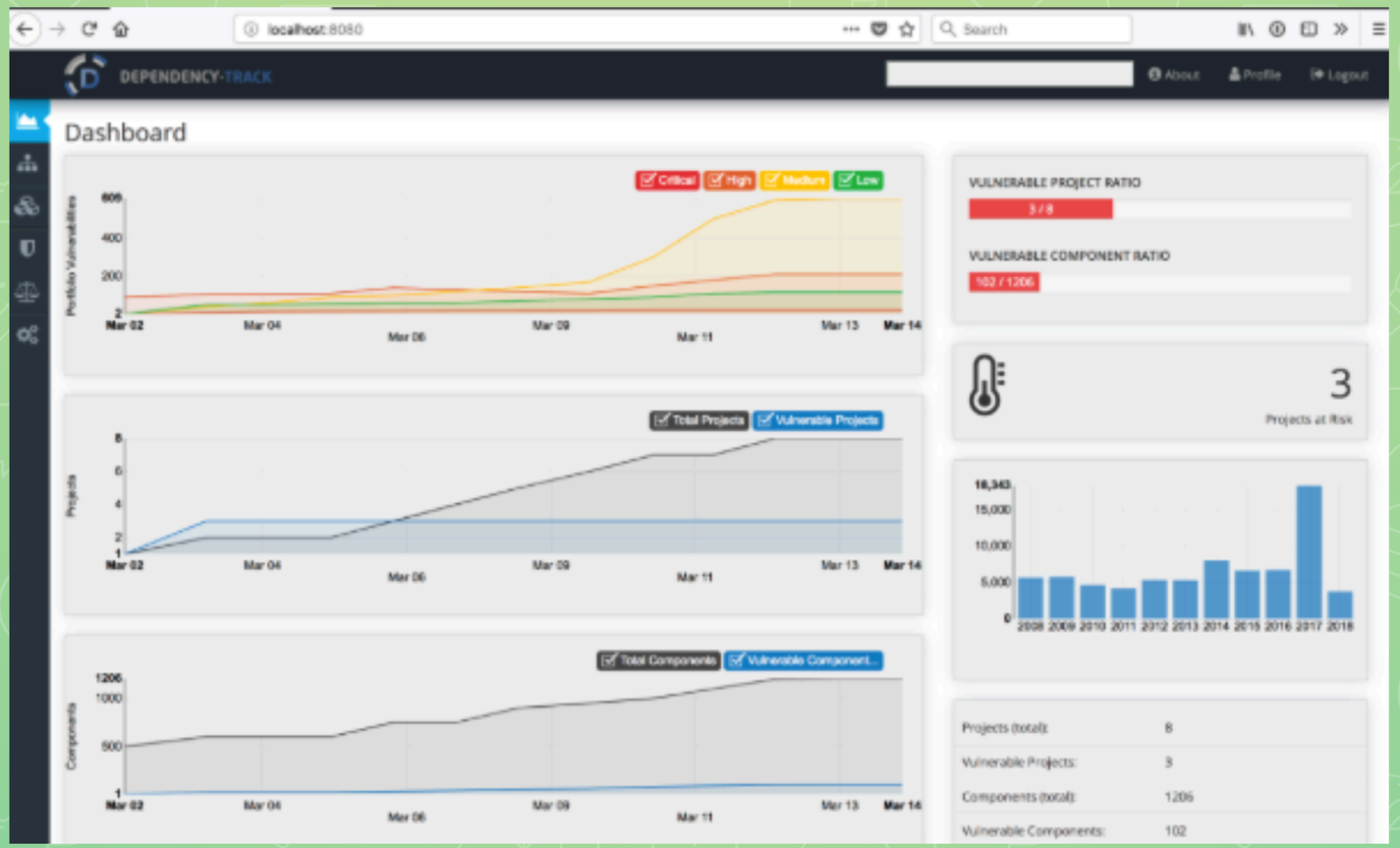
supports multiple Languages

can be run as docker-container, maven/gradle package...

OWASP dependency-check



OWASP dependency-check



container

docker pull cy4n/broken

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

find vulnerable packages in container images

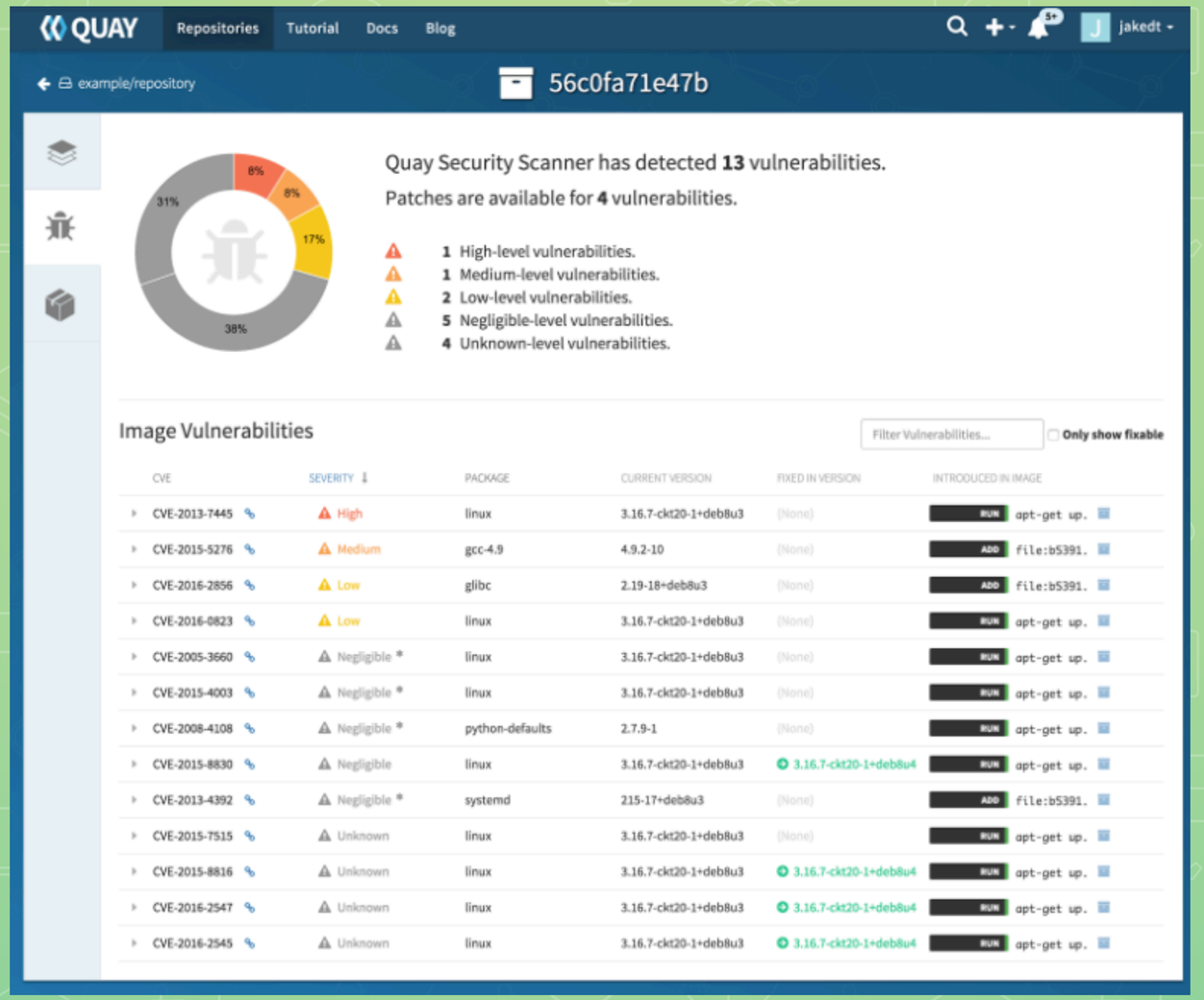
CoreOS Clair

database

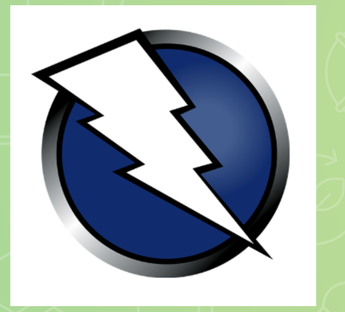
clair-server

clair-scanner (client)

CoreOS Clair



API / Webserver



ZAProxy

burp

API / Webserver

OWASP ZAProxy

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

how to react?

workshop

try the tools

unbreak the deliberately broken application

discuss :-)