AUTOMATED VULNERABILITY RESEARCH

E.G. BROENINK MSC

INDEX

AUTOMATED VULNERABILITY RESEARCH (AVR)

01. AUTOMATED VULNERABILITY RESEARCH

02. LOG4J

03. KEY APPLICATIONS

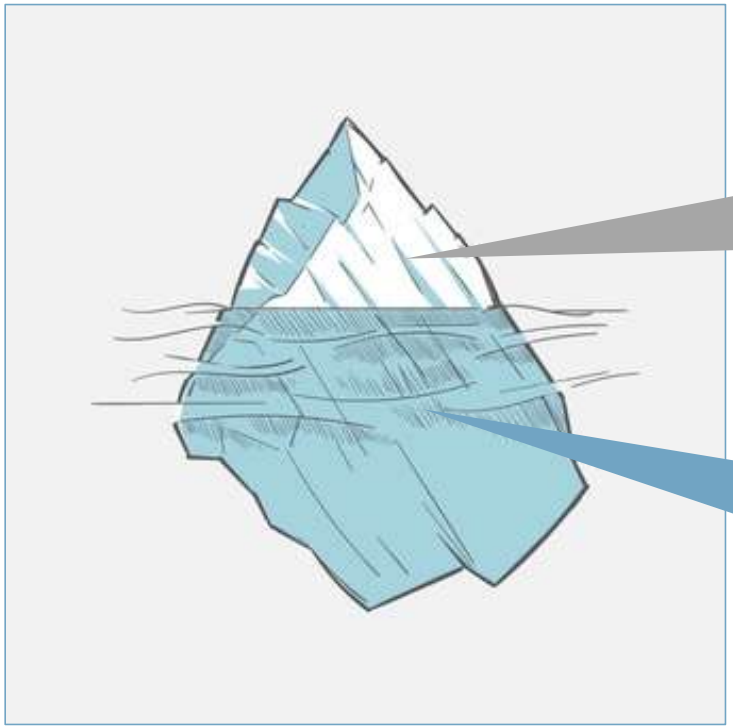
04. COLLABORATION

05. TECHNOLOGY FOCUS: FUZZING

06. CURRENT RESEARCH

TNO innovation for life

AUTOMATED VULNERABILITY RESEARCH (AVR)



current cyber security practice:

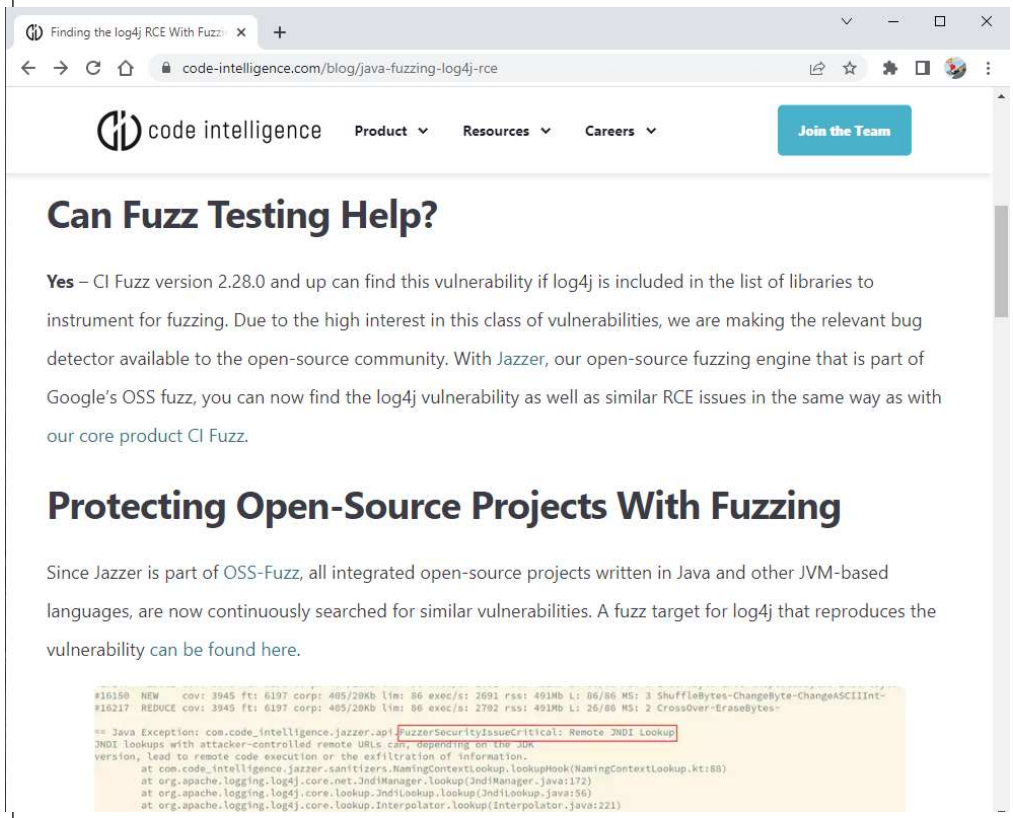
protect own IT against
software vulnerabilities that have been
published and patched

AVR:

discovering and patching
unknown/unpublished vulnerabilities

using smart automation to make it scalable

LOG4J



Bron: nu.nl

14 december 2021 05:30
Laatste update: 14 december 2021 10:59

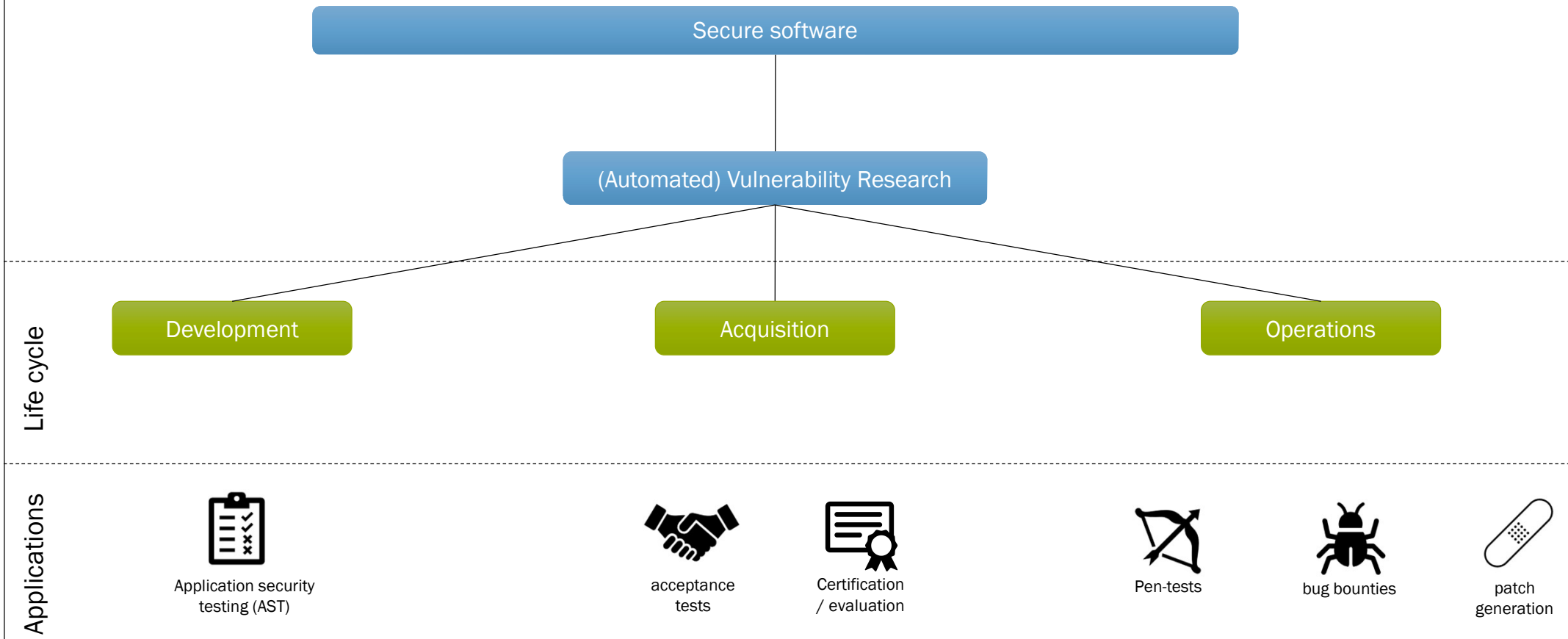
121 NUjij-reacties

Een veelgebruikt stukje software in webservers bevat een ernstige kwetsbaarheid, waardoor veel organisaties kans lopen om gehackt te worden. Er is een oplossing beschikbaar, maar het probleem is dat organisaties lang niet altijd weten dát ze gevaar lopen.

Het gaat om software met de naam Apache Log4j. Dit programma wordt massaal door bedrijven en organisaties gebruikt om bij te houden wat er op hun webservers gebeurt. In dit logboek kan van alles staan, bijvoorbeeld wanneer gebruikers ergens inloggen of waar in de systemen foutmeldingen worden gegeven, zodat beheerders ze kunnen oplossen.

TNO innovation for life

SECURE SOFTWARE AND AVR



TNO innovation for life

KEY AVR APPLICATIONS

APPLICATION SECURITY TESTING

- Industry focus on uniform, agile development (DevOps)
- “shift-left security”: move security to early lifecycle stages
- AVR to complement current application testing practices

SECURING APPLICATION PROGRAMMING INTERFACES (API)

- Crucial in modern cloud/microservices architectures
- External attack surface
- Securing APIs is an important first line of defence

COLLABORATIONS

Academic

TU Delft

VUSec

UNIVERSITY OF TWENTE.

Application

Ministerie van Defensie

dcypher

essent

TNO innovation for life

POLITIE

ABN·AMRO

SIG Software Improvement Group

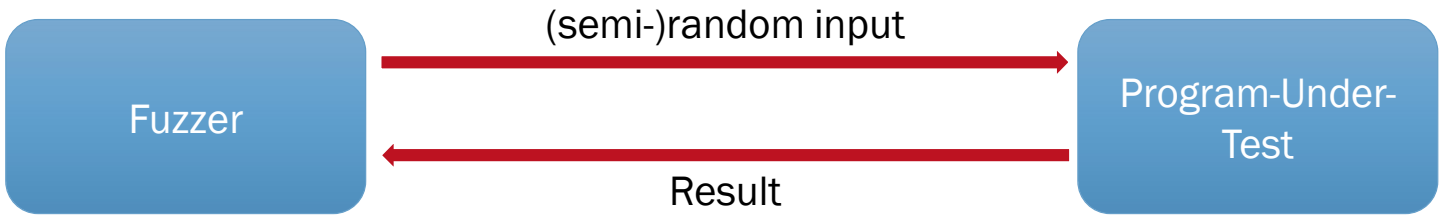
NBV

TECHNOLOGY FOCUS: FUZZING

- Addition to unit and integration testing
- SAST tooling already widely used, and can be combined with fuzzing
- Fuzzing technology is maturing, but not widely applied yet

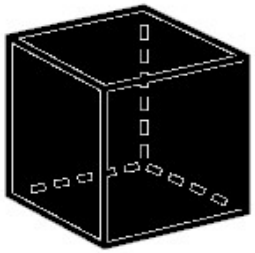
FUZZING

- Fuzzer sends (semi-) random data to program-under-test.
- Fuzzer tests how the program responds.

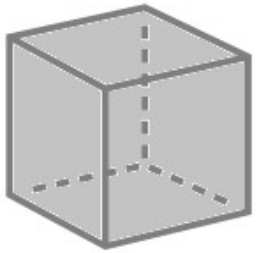


BLACKBOX – GREYBOX – WHITEBOX

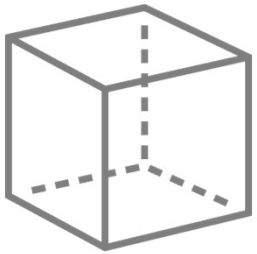
- Different approaches



Black box
- No source code
- Only binary file



Grey box:
- No source code
- Instrumented binary

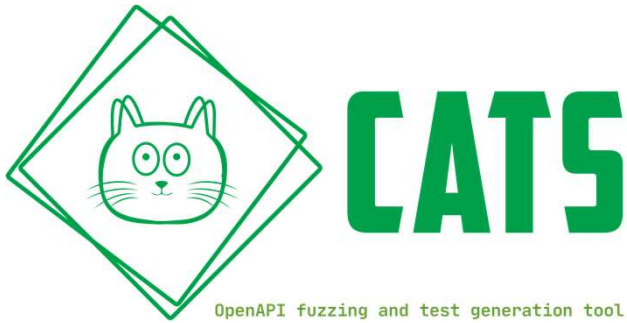


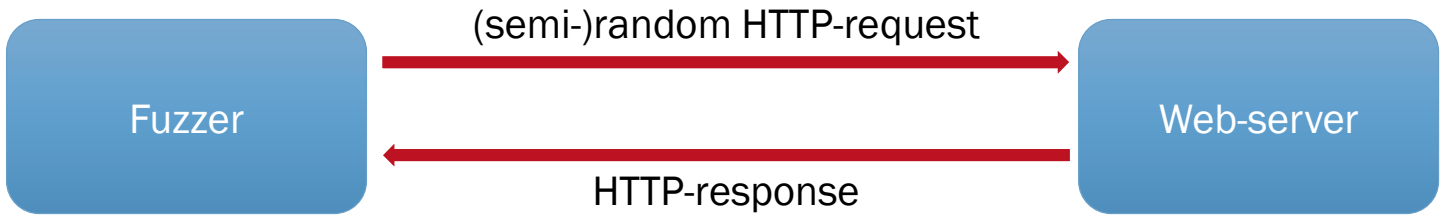
White box:
- Source code

WEB-API FUZZING – STATE OF THE ART

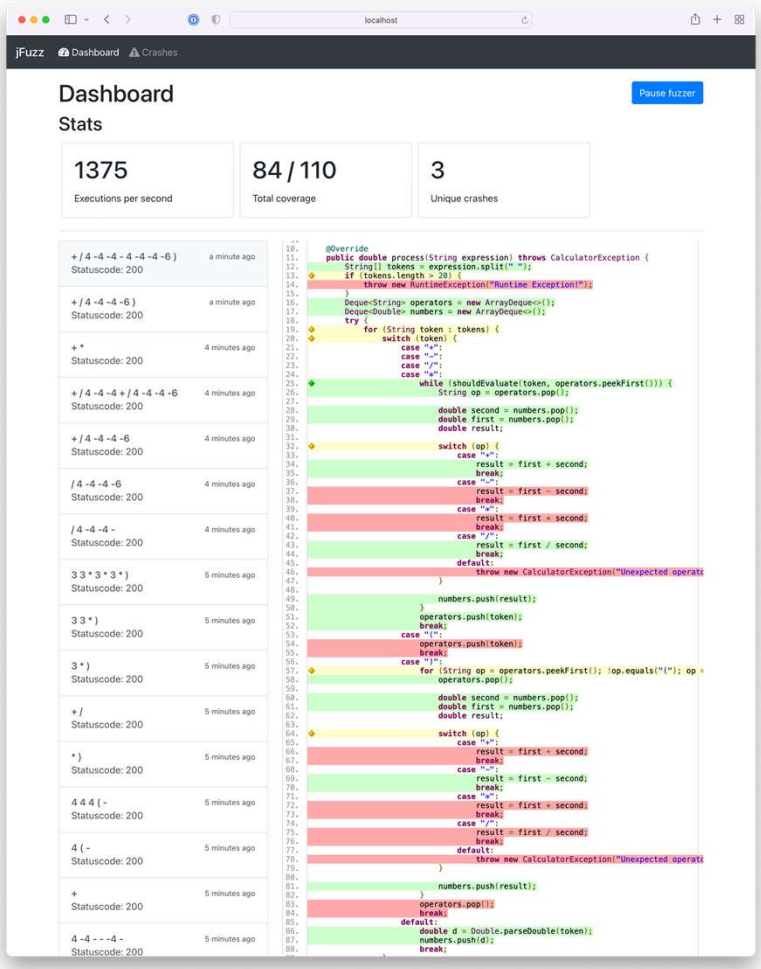
- Open source tools available
  - CATS
  - RESTler

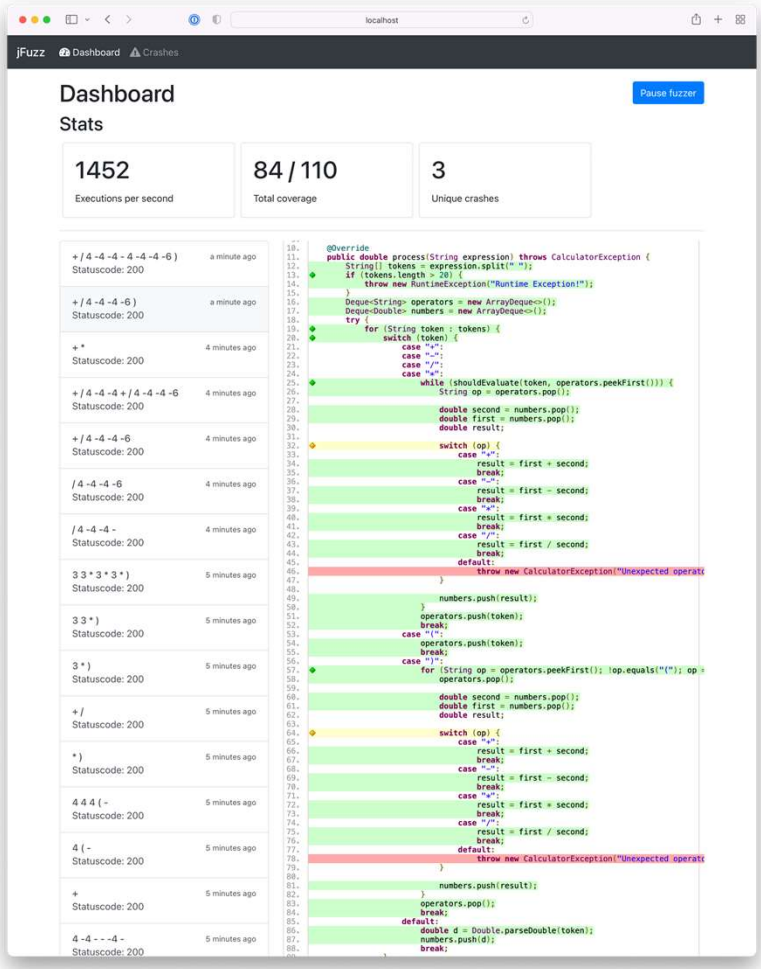
- Blackbox approach (based on OpenAPI spec)





WEB-API FUZZING – CURRENT RESEARCH





TNO innovation for life

FUZZING IN CI/CD CHAIN

- Early in the development proces, bugs are easy to fix
- CI/CD tooling already have extensive test environment
- Fuzzing takes place at pre-defined moments:
  - Each commit
  - Every day
  - Every weekend

RESEARCH PROJECT

- New research project on applying fuzzing technology. (TKI)
- Aim: make fuzzing technology applicable in:
  - CI/CD chains
  - Grey-box web API's
- Aim: 5 industry partners
- Timeline: Start Q3/Q4 2022

ABN·AMRO

THANK YOU FOR YOUR TIME

Paske, B.J. (Bert Jan) te

Senior Consultant Cybersecurity

Rooljakkers, T.A. (Thomas)

Scientist Integrator

Broenink, E.G. (Gerben)

Security specialist

TNO innovation for life