Laboratory for DevSecOps

Gabriele Genovese

10 December 2024

1 First exercise

I've forked the repository and created the file `hello.yaml` under `.github/workflows/` with the following content:

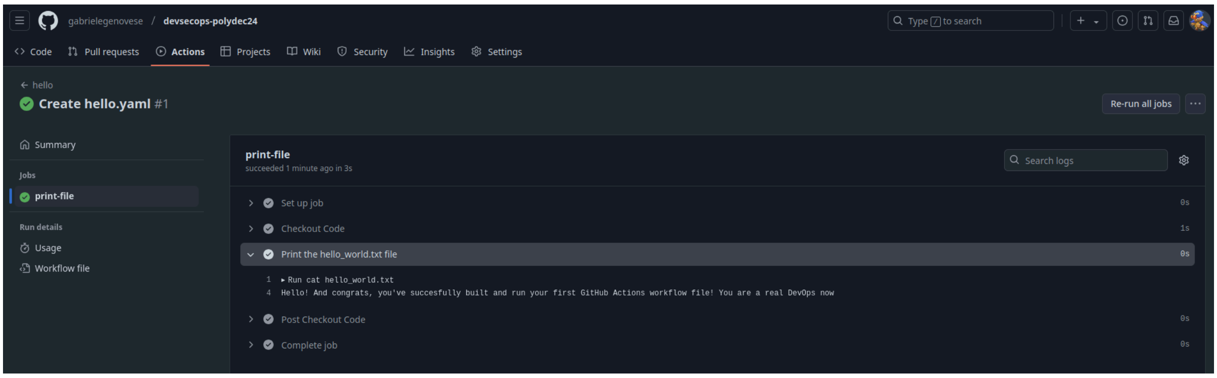
```
name: hello

on:
  push:
    branches:
      - main
  workflow_dispatch:

jobs:
  print-file:
    runs-on: ubuntu-latest

    steps:
      - name: Checkout Code
        uses: actions/checkout@v3
      - name: Print the hello_world.txt file
        run: |
          cat hello_world.txt
```

Pipeline link



Create hello.yaml #1

print-file
succeeded 1 minute ago in 3s

```
Set up job                         0s
Checkout Code                      1s
Print the hello_world.txt file     0s
▸ Run cat hello_world.txt
Hello! And congrats, you've succesfully built and run your first GitHub Actions workflow file! You are a real DevOps now
Post Checkout Code                 0s
Complete job                       0s
```

2 Second exercise

To build and test the application I've created the file `built-and-test.yaml` with the content:

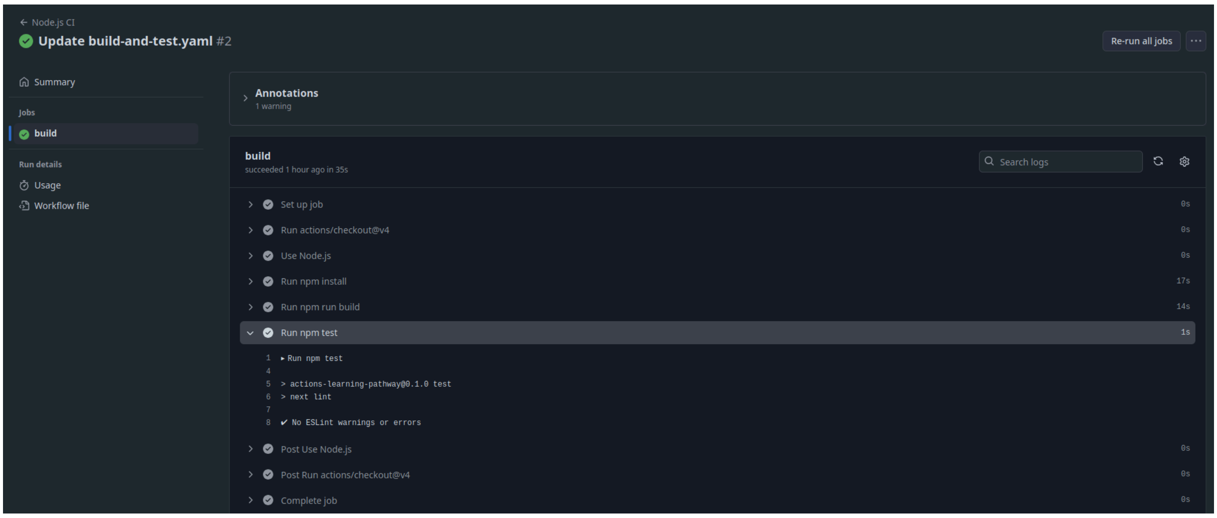
```
name: Node.js CI

on: [push]
```

```
jobs:
  build:

    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v4
      - name: Use Node.js
        uses: actions/setup-node@v4
        with:
          node-version: '20.x'
      - run: npm install
      - run: npm run build
      - run: npm test
```



Update build-and-test.yaml #2

Annotations
1 warning

build
succeeded 1 hour ago in 35s

```
> Set up job                     0s
> Run actions/checkout@v4        0s
> Use Node.js                    0s
> Run npm install               17s
> Run npm run build             14s
v Run npm test                   1s
  ▸ Run npm test

  > actions-learning-pathway@0.1.0 test
  > next lint

  ✔ No ESLint warnings or errors
> Post Use Node.js               0s
> Post Run actions/checkout@v4   0s
> Complete job                   0s
```

Pipeline link

3 Third exercise

I've found out that there are some vulnerabilities just by adding `npm audit` to the previous workflow.

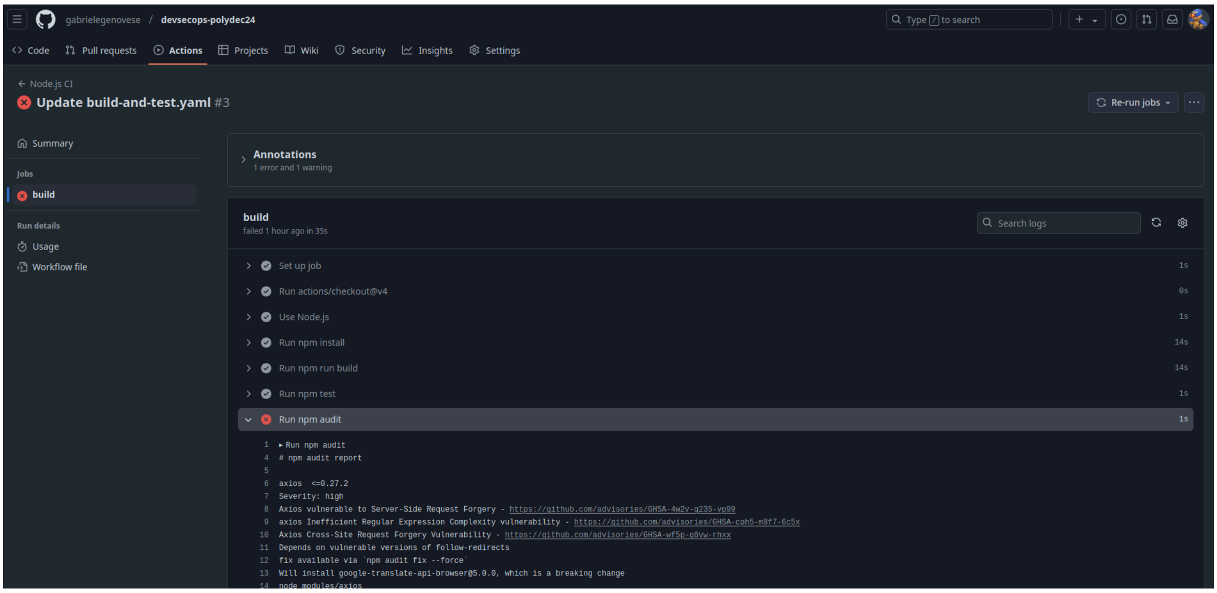
```
name: Node.js CI

on: [push]

jobs:
  build:

    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v4
      - name: Use Node.js
        uses: actions/setup-node@v4
        with:
          node-version: '20.x'
      - run: npm install
      - run: npm audit
      - run: npm run build
      - run: npm test
```



Update build-and-test.yaml #3

Annotations
1 error and 1 warning

build
failed 1 hour ago in 35s

```
Set up job                   1s
Run actions/checkout@v4      0s
Use Node.js                  1s
Run npm install              14s
Run npm run build            14s
Run npm test                 1s
Run npm audit                1s
```

```
▸ Run npm audit
# npm audit report

axios  <=0.27.2
Severity: high
Axios vulnerable to Server-Side Request Forgery - https://github.com/advisories/GHSA-4w2v-q235-vp99
axios Inefficient Regular Expression Complexity vulnerability - https://github.com/advisories/GHSA-cph5-m8f7-6c5x
Axios Cross-Site Request Forgery Vulnerability - https://github.com/advisories/GHSA-wf5p-g6vw-rhxx
Depends on vulnerable versions of follow-redirects
fix available via `npm audit fix --force`
Will install google-translate-api-browser@5.0.0, which is a breaking change
node_modules/axios
```

Pipeline link

The `npm audit` report is the following:

```
axios  <=0.27.2
Severity: high
Axios vulnerable to Server-Side Request Forgery - https://github.com/advisories/GHSA-4w2v-q235-vp99
axios Inefficient Regular Expression Complexity vulnerability - https://github.com/advisories/GHSA-cph5-m8f7-6c5x
Axios Cross-Site Request Forgery Vulnerability - https://github.com/advisories/GHSA-wf5p-g6vw-rhxx
Depends on vulnerable versions of follow-redirects
fix available via `npm audit fix --force`
Will install google-translate-api-browser@5.0.0, which is a breaking change
node_modules/axios
  google-translate-api-browser  <=4.0.6
  Depends on vulnerable versions of axios
  Depends on vulnerable versions of safe-eval
  node_modules/google-translate-api-browser

follow-redirects  <=1.15.5
Severity: high
Exposure of Sensitive Information to an Unauthorized Actor in follow-redirects - https://github.com/advisories/GHSA-pw2r-vq6v-hr8c
Exposure of sensitive information in follow-redirects - https://github.com/advisories/GHSA-74fj-2j2h-c42q
Follow Redirects improperly handles URLs in the url.parse() function - https://github.com/advisories/GHSA-jchw-25xp-jwwc
follow-redirects' Proxy-Authorization header kept across hosts - https://github.com/advisories/GHSA-cxjh-pqwp-8mfp
fix available via `npm audit fix --force`
Will install google-translate-api-browser@5.0.0, which is a breaking change
node_modules/follow-redirects

safe-eval  *
Severity: critical
Sandbox Breakout / Arbitrary Code Execution in safe-eval - https://github.com/advisories/GHSA-9pcf-h8q9-63f6
safe-eval vulnerable to Prototype Pollution - https://github.com/advisories/GHSA-33vh-7x8q-mg35
```

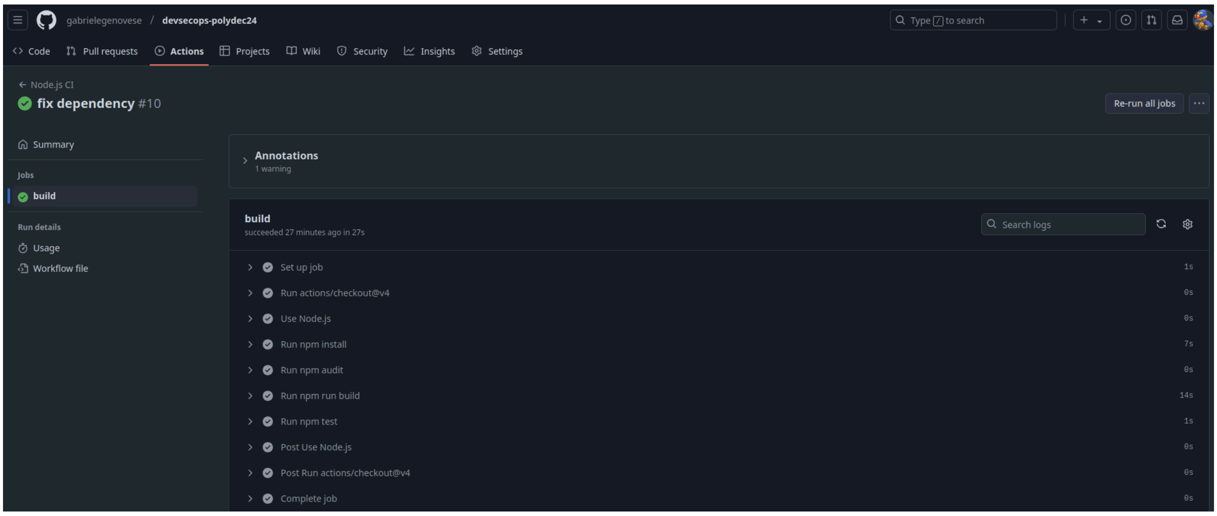
```
safe-eval vulnerable to Prototype Pollution via the safeEval function - https://github.com/
advisories/GHSA-hcg3-56jf-x4vh
safe-eval vulnerable to Sandbox Bypass due to improper input sanitization - https://github.com/
advisories/GHSA-79xf-67r4-q2jj
Sandbox Breakout / Arbitrary Code Execution in safe-eval - https://github.com/advisories/GHSA-
hrpq-r399-whgw
fix available via `npm audit fix --force`
Will install google-translate-api-browser@5.0.0, which is a breaking change
node_modules/safe-eval

4 vulnerabilities (3 high, 1 critical)

To address all issues (including breaking changes), run:
  npm audit fix --force
```

Looking at the report, it's clear that the package `google-translate-api-browser` needs to be updated. After updating `google-translate-api-browser` to version `5.0.0` the action works and it finishes without any error.

Commit fix link



fix dependency #10

Annotations
1 warning

build
succeeded 27 minutes ago in 27s

```
Set up job                      1s
Run actions/checkout@v4         0s
Use Node.js                     0s
Run npm install                 7s
Run npm audit                   0s
Run npm run build              14s
Run npm test                    1s
Post Use Node.js                0s
Post Run actions/checkout@v4    0s
Complete job                    0s
```

Pipeline link

4 Fourth exercise

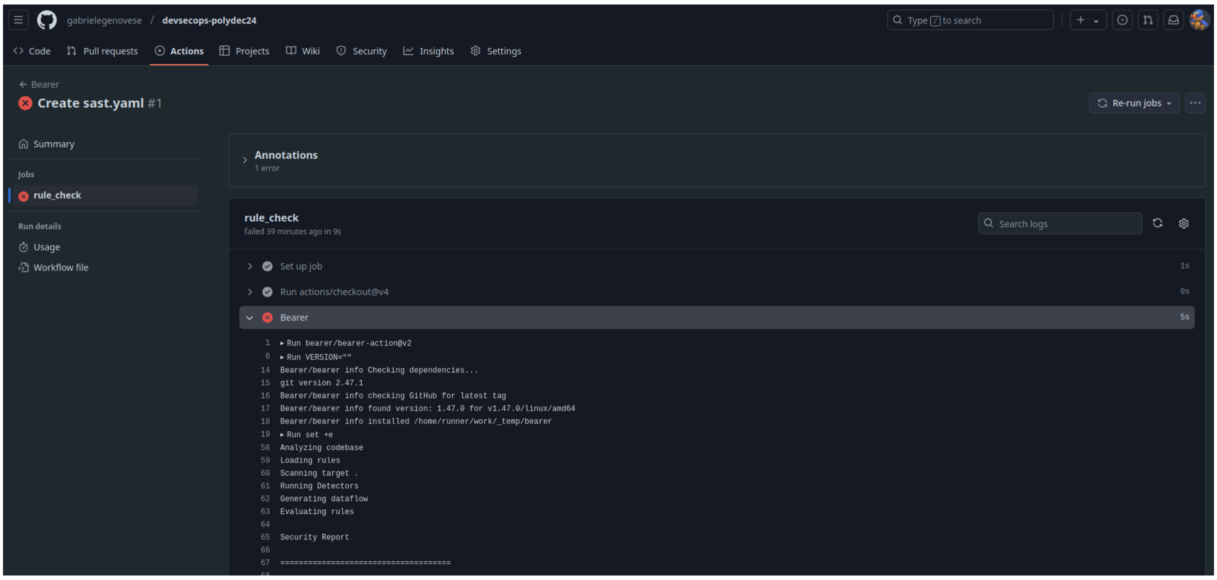
I've decided to use Bearer to check for vulnerabilities with the following workflow (file):

```yaml
name: Bearer

on:
  push:
    branches:
      - main

permissions:
  contents: read

jobs:
  rule_check:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - name: Bearer
        uses: bearer/bearer-action@v2
```



```
▸ Run bearer/bearer-action@v2
▸ Run VERSION=""
Bearer/bearer info Checking dependencies...
git version 2.47.1
Bearer/bearer info checking GitHub for latest tag
Bearer/bearer info found version: 1.47.0 for v1.47.0/linux/amd64
Bearer/bearer info installed /home/runner/work/_temp/bearer
▸ Run set +e
Analyzing codebase
Loading rules
Scanning target .
Running Detectors
Generating dataflow
Evaluating rules

Security Report

=====================================
```

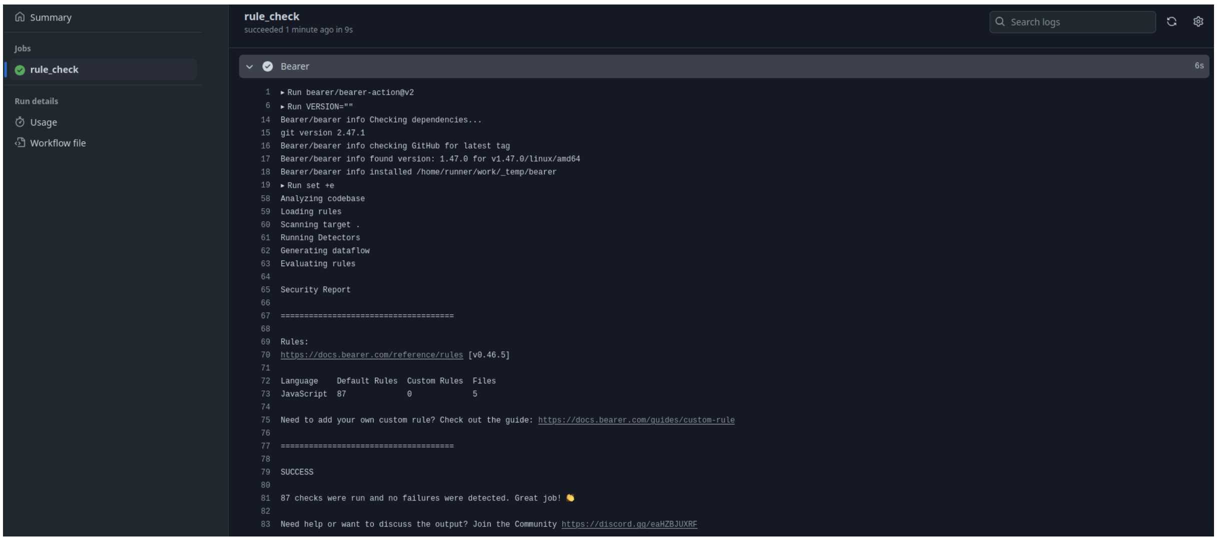
Pipeline link

Here is the content of the report of the error with the following output:

```
Bearer/bearer info Checking dependencies...
git version 2.47.1
Bearer/bearer info checking GitHub for latest tag
Bearer/bearer info found version: 1.47.0 for v1.47.0/linux/amd64
Bearer/bearer info installed /home/runner/work/_temp/bearer
Run set +e
Analyzing codebase
Loading rules
Scanning target .
Running Detectors
Generating dataflow
Evaluating rules
Security Report
=====================================
Rules:
https://docs.bearer.com/reference/rules [v0.46.5]
Language    Default Rules  Custom Rules  Files
JavaScript  87             0             5
CRITICAL: Usage of hard-coded secret [CWE-798]
https://docs.bearer.com/reference/rules/javascript_lang_hardcoded_secret
To ignore this finding, run: bearer ignore add 402ec2c8dd9fa09875d643e45f38ec11_0
File: pages/index.js:6
 6 const PASSWORD = "aSuperSecretPassword"
=====================================
87 checks, 1 findings
CRITICAL: 1 (CWE-798)
HIGH: 0
MEDIUM: 0
LOW: 0
WARNING: 0
Need help or want to discuss the output? Join the Community https://discord.gg/eaHZBJUXRF
```

The error is `CRITICAL: Usage of hard-coded secret [CWE-798]`. The solution is to remove the line with the hard-coded passoword. In fact, the following action will not return an error. Given that the password has been exposed, it needs to be updated to a new one.

Commit link



rule_check
succeeded 1 minute ago in 9s

```
▸ Run bearer/bearer-action@v2
▸ Run VERSION=""
Bearer/bearer info Checking dependencies...
git version 2.47.1
Bearer/bearer info checking GitHub for latest tag
Bearer/bearer info found version: 1.47.0 for v1.47.0/linux/amd64
Bearer/bearer info installed /home/runner/work/_temp/bearer
▸ Run set +e
Analyzing codebase
Loading rules
Scanning target .
Running Detectors
Generating dataflow
Evaluating rules

Security Report

=====================================

Rules:
https://docs.bearer.com/reference/rules [v0.46.5]

Language    Default Rules  Custom Rules  Files
JavaScript  87             0             5

Need to add your own custom rule? Check out the guide: https://docs.bearer.com/guides/custom-rule

=====================================

SUCCESS

87 checks were run and no failures were detected. Great job! 👏

Need help or want to discuss the output? Join the Community https://discord.gg/eaHZBJUXRF
```

Pipeline link