STATS lab activity

Analysis of vulnerable repositories with SAST and SCA

Gabriele Tomai 27/11/2025

Repos and tool

Repos:

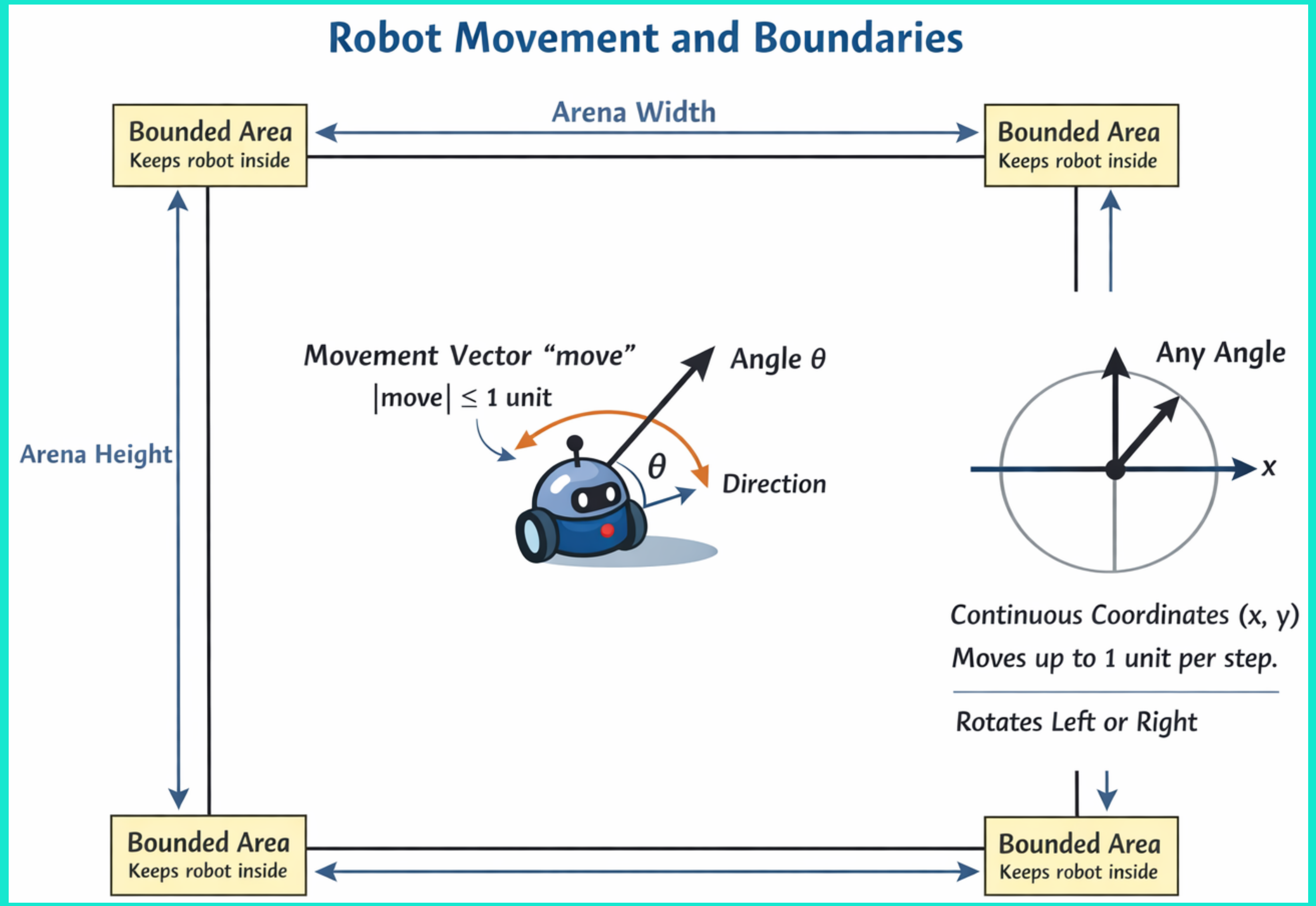
- Co-evolution of Robots - Good
- Monitor for Solar Production - Vulnerable

Tools:

- SonarCloud scanner
- Trivy scanner

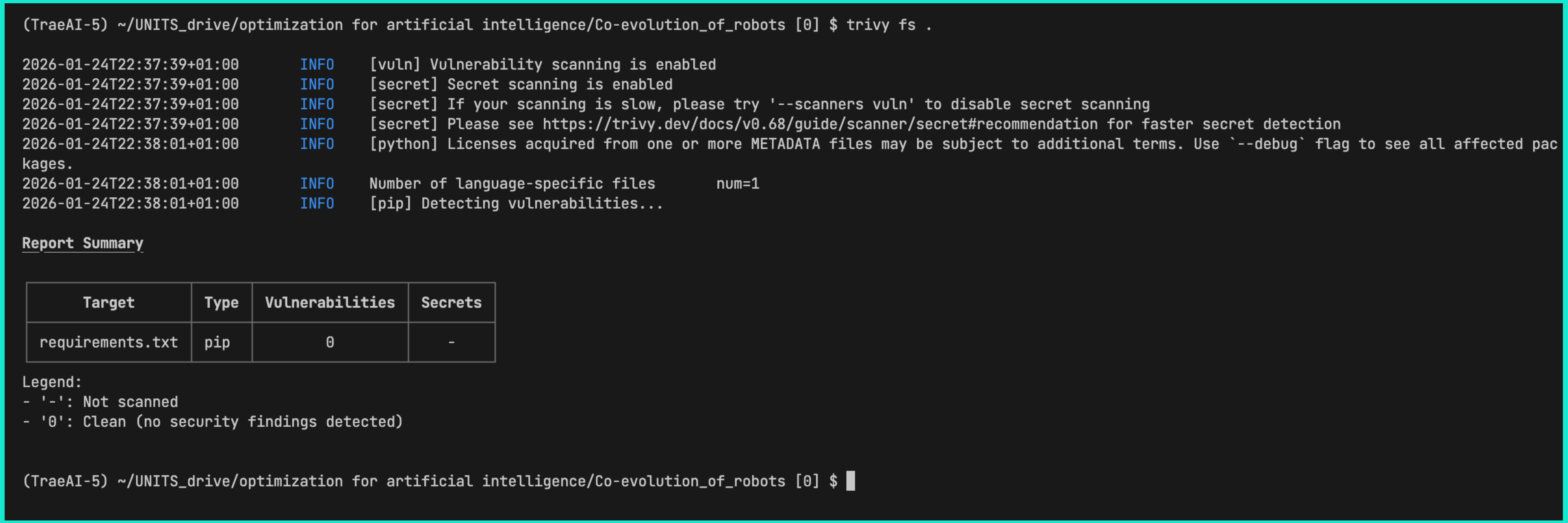
What is Co-evolution of Robots

- Python artificial intelligence project
- Developed with a NEAT neural network
- Requires some external Python packages
- Personaly used and developed by me
- https://github.com/Gabriele-tomai00/Co-evolution_of_robots



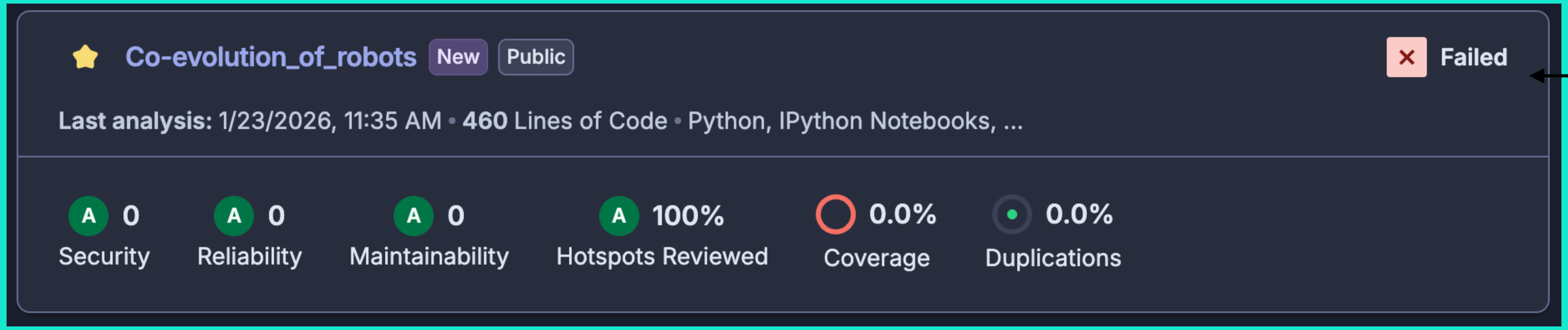
Let’s see if my application has vulnerabilities

With Trivy…



```
(TraeAI-5) ~/UNITS_drive/optimization for artificial intelligence/Co-evolution_of_robots [0] $ trivy fs .

2026-01-24T22:37:39+01:00       INFO    [vuln] Vulnerability scanning is enabled
2026-01-24T22:37:39+01:00       INFO    [secret] Secret scanning is enabled
2026-01-24T22:37:39+01:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2026-01-24T22:37:39+01:00       INFO    [secret] Please see https://trivy.dev/docs/v0.68/guide/scanner/secret#recommendation for faster secret detection
2026-01-24T22:38:01+01:00       INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all affected pac
kages.
2026-01-24T22:38:01+01:00       INFO    Number of language-specific files       num=1
2026-01-24T22:38:01+01:00       INFO    [pip] Detecting vulnerabilities...

Report Summary

┌──────────────────┬──────┬─────────────────┬─────────┐
│      Target      │ Type │ Vulnerabilities │ Secrets │
├──────────────────┼──────┼─────────────────┼─────────┤
│ requirements.txt │ pip  │        0        │    -    │
└──────────────────┴──────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


(TraeAI-5) ~/UNITS_drive/optimization for artificial intelligence/Co-evolution_of_robots [0] $ █
```

With SonarCloud



Co-evolution_of_robots New Public ☒ Failed

Last analysis: 1/23/2026, 11:35 AM • **460** Lines of Code • Python, IPython Notebooks, ...

A 0 Security

A 0 Reliability

A 0 Maintainability

A 100% Hotspots Reviewed

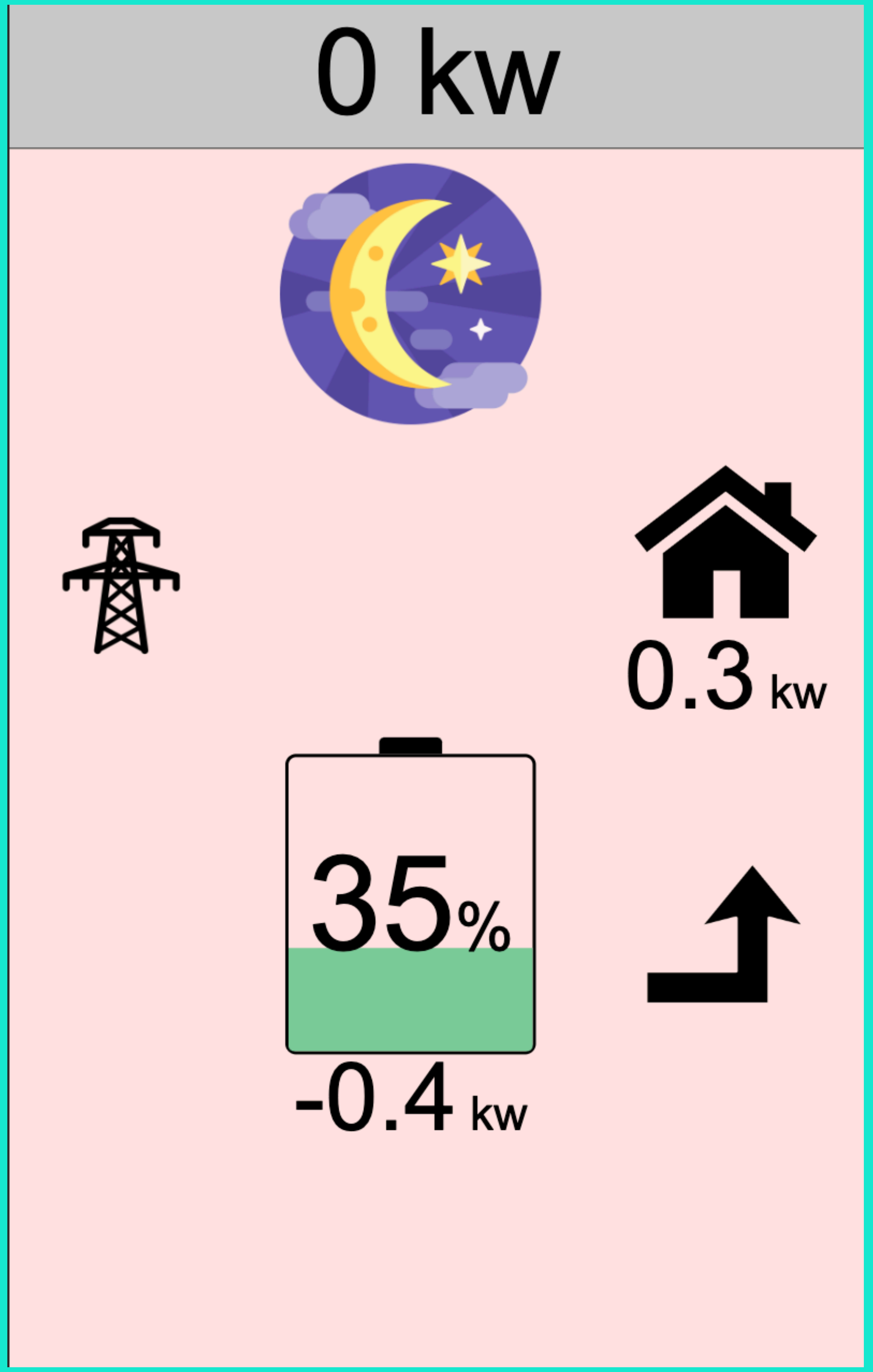
○ 0.0% Coverage

● 0.0% Duplications

The quality gate fails due to the lack of unit tests that have not been implemented.

What is Monitor for Solar Production

- A simple webapp developed with nodejs, html and css
- Accessible from a web browser
- It uses a MQTT connection
- It's something personal (does not use public API or standard protocol)
- No authentication required
- Personaly used and developed by me
- https://github.com/Gabriele-tomai00/Monitor4SolarProduction

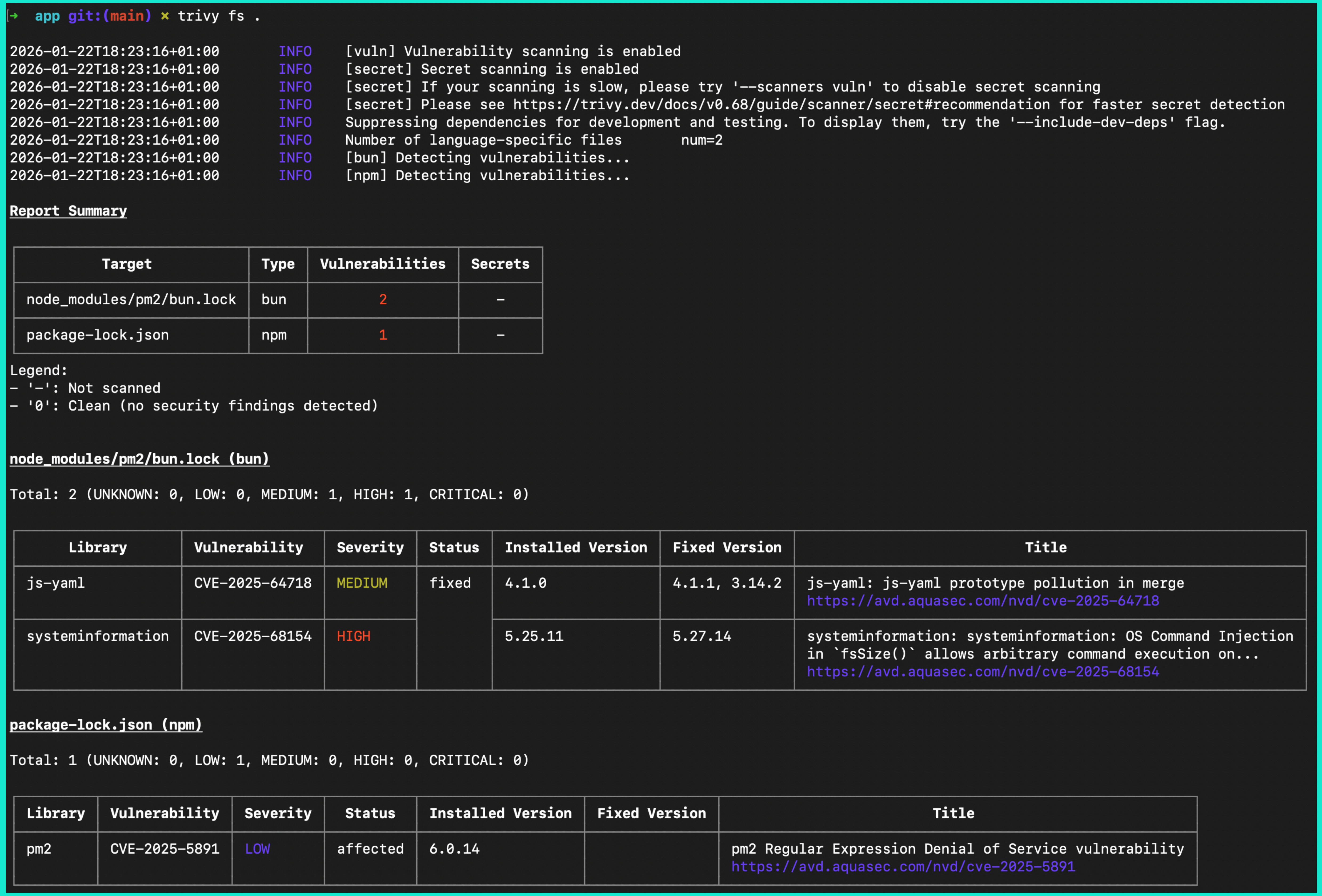


Why Monitor for Solar Production

- It is a web application with various dependencies (it uses npm packages)Accessible from a web browser
- It is connected to Home Assistant (my home automation supervisor) via MQTT or API
- It is a project developed before I studied cybersecurity, without my attention to security!
- I want to see if there are any vulnerabilities and if it is possible to improve its security
- https://github.com/Gabriele-tomai00/Monitor4SolarProduction

Let’s see if my application has vulnerabilities

With Trivy



```
→ app git:(main) ✗ trivy fs .

2026-01-22T18:23:16+01:00       INFO    [vuln] Vulnerability scanning is enabled
2026-01-22T18:23:16+01:00       INFO    [secret] Secret scanning is enabled
2026-01-22T18:23:16+01:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2026-01-22T18:23:16+01:00       INFO    [secret] Please see https://trivy.dev/docs/v0.68/guide/scanner/secret#recommendation for faster secret detection
2026-01-22T18:23:16+01:00       INFO    Suppressing dependencies for development and testing. To display them, try the '--include-dev-deps' flag.
2026-01-22T18:23:16+01:00       INFO    Number of language-specific files       num=2
2026-01-22T18:23:16+01:00       INFO    [bun] Detecting vulnerabilities...
2026-01-22T18:23:16+01:00       INFO    [npm] Detecting vulnerabilities...

Report Summary

┌───────────────────────────┬──────┬─────────────────┬─────────┐
│          Target           │ Type │ Vulnerabilities │ Secrets │
├───────────────────────────┼──────┼─────────────────┼─────────┤
│ node_modules/pm2/bun.lock │ bun  │        2        │    -    │
├───────────────────────────┼──────┼─────────────────┼─────────┤
│ package-lock.json         │ npm  │        1        │    -    │
└───────────────────────────┴──────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


node_modules/pm2/bun.lock (bun)

Total: 2 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 1, CRITICAL: 0)

┌───────────────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬────────────────────────────────────────────────────────────┐
│      Library      │ Vulnerability  │ Severity │ Status │ Installed Version │ Fixed Version │                            Title                           │
├───────────────────┼────────────────┼──────────┼────────┼───────────────────┼───────────────┼────────────────────────────────────────────────────────────┤
│ js-yaml           │ CVE-2025-64718 │ MEDIUM   │ fixed  │ 4.1.0             │ 4.1.1, 3.14.2 │ js-yaml: js-yaml prototype pollution in merge              │
│                   │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2025-64718                 │
├───────────────────┼────────────────┼──────────┤        ├───────────────────┼───────────────┼────────────────────────────────────────────────────────────┤
│ systeminformation │ CVE-2025-68154 │ HIGH     │        │ 5.25.11           │ 5.27.14       │ systeminformation: systeminformation: OS Command Injection │
│                   │                │          │        │                   │               │ in `fsSize()` allows arbitrary command execution on...     │
│                   │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2025-68154                 │
└───────────────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴────────────────────────────────────────────────────────────┘

package-lock.json (npm)

Total: 1 (UNKNOWN: 0, LOW: 1, MEDIUM: 0, HIGH: 0, CRITICAL: 0)

┌─────────┬───────────────┬──────────┬──────────┬───────────────────┬───────────────┬────────────────────────────────────────────────────────┐
│ Library │ Vulnerability │ Severity │  Status  │ Installed Version │ Fixed Version │                         Title                          │
├─────────┼───────────────┼──────────┼──────────┼───────────────────┼───────────────┼────────────────────────────────────────────────────────┤
│ pm2     │ CVE-2025-5891 │ LOW      │ affected │ 6.0.14            │               │ pm2 Regular Expression Denial of Service vulnerability │
│         │               │          │          │                   │               │ https://avd.aquasec.com/nvd/cve-2025-5891              │
└─────────┴───────────────┴──────────┴──────────┴───────────────────┴───────────────┴────────────────────────────────────────────────────────┘
```

CVE	Solutions?
CVE-2025-68154	Update Systeminformation to 5.27.14
CVE-2025-64718	Update PM2 to 4.1.1

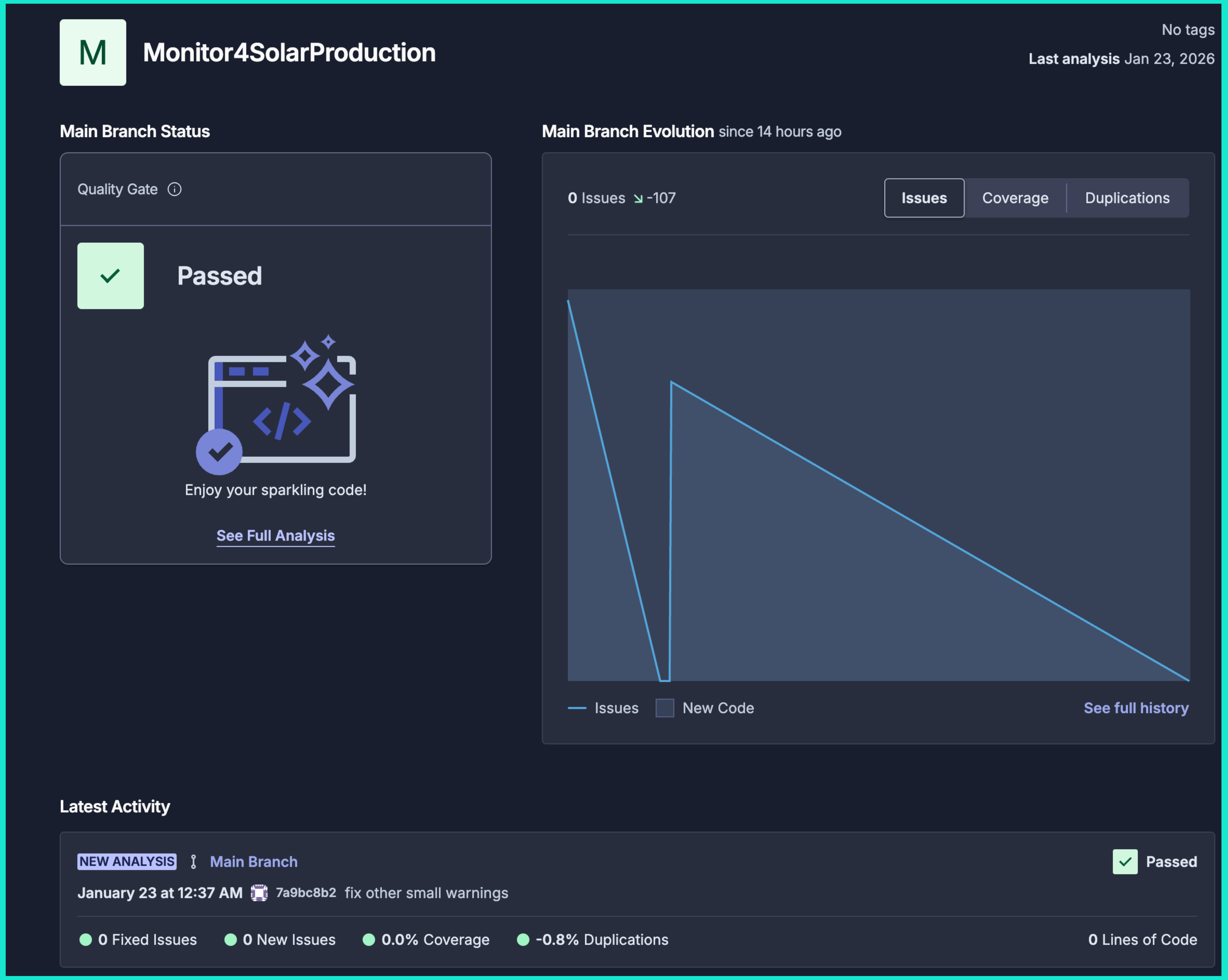
False positive → Trivy flags this due to outdated vulnerability definitions or overly conservative matching.

Let’s see if my application has vulnerabilities

With SonarCloud

I corrected some small warnings…

But not security errors found!



M Monitor4SolarProduction

No tags

Last analysis Jan 23, 2026

Main Branch Status

Quality Gate ⓘ

✓ Passed

Enjoy your sparkling code!

See Full Analysis

Main Branch Evolution since 14 hours ago

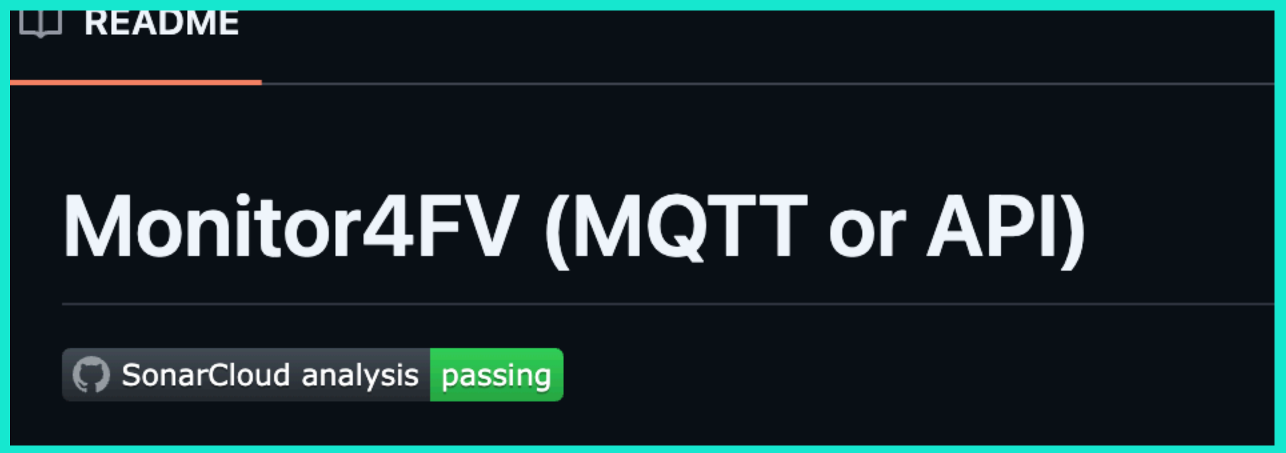
0 Issues ↘ -107

Latest Activity

NEW ANALYSIS Main Branch ☑ Passed

January 23 at 12:37 AM 7a9bc8b2 fix other small warnings

● **0** Fixed Issues ● **0** New Issues ● **0.0%** Coverage ● **-0.8%** Duplications **0** Lines of Code



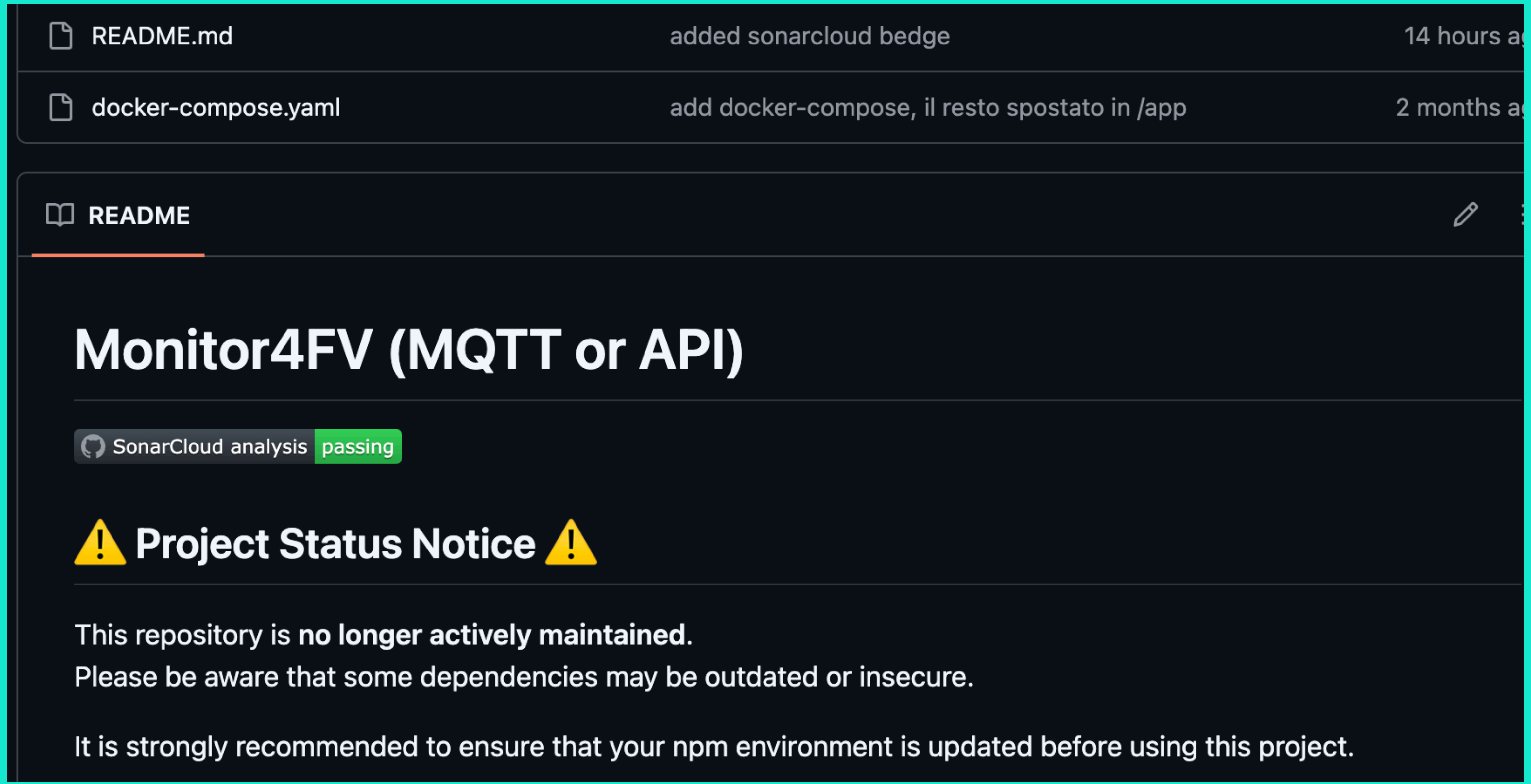
README

Monitor4FV (MQTT or API)

SonarCloud analysis passing

What I do

- I updated all npm packages.
- I updated the package-lock.json file (so even those who download the repo won't have any problems).
- I added an warning message in README.md.
- I added the SonarCloud workflow on GitHub (Github actions)
- I added the SonarCloud analysys bedge in README.md



README.md	added sonarcloud bedge	14 hours a
docker-compose.yaml	add docker-compose, il resto spostato in /app	2 months a

Monitor4FV (MQTT or API)

SonarCloud analysis passing

⚠️ Project Status Notice ⚠️

This repository is **no longer actively maintained**.
Please be aware that some dependencies may be outdated or insecure.

It is strongly recommended to ensure that your npm environment is updated before using this project.