Secure Software Development Life Cycle (SSDLC)

Project Name: LibOrate Organization: AImpower.org Description: A videoconferencing companion app that offers emotional and relational support during video calls.

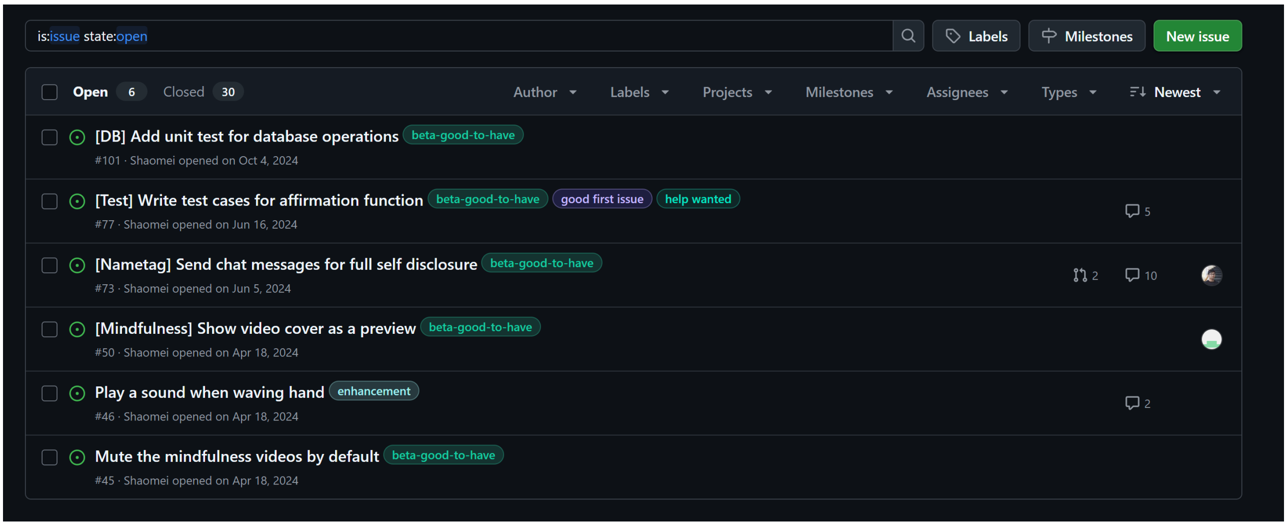
1. Planning & Requirements

- Task Management:

  We use GitHub Issues to capture feature requests, enhancements, and bug reports.

  Each issue includes labels (e.g., enhancement, beta-good-to-have) and acceptance criteria.

- Evidence:

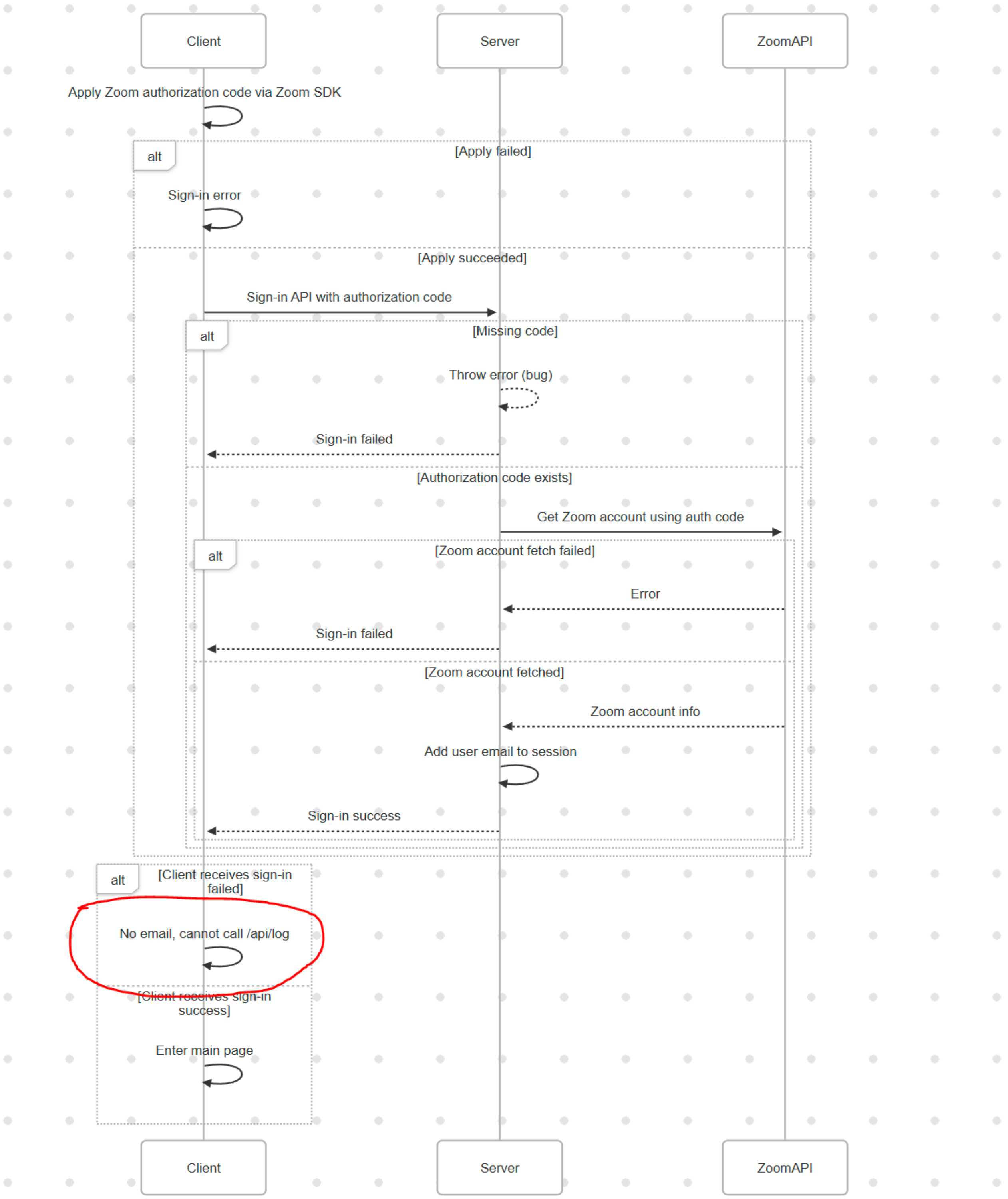


Open 6 Closed 30

- [DB] Add unit test for database operations `beta-good-to-have`
  #101 · Shaomei opened on Oct 4, 2024
- [Test] Write test cases for affirmation function `beta-good-to-have` `good first issue` `help wanted` — 5
  #77 · Shaomei opened on Jun 16, 2024
- [Nametag] Send chat messages for full self disclosure `beta-good-to-have` — 2 — 10
  #73 · Shaomei opened on Jun 5, 2024
- [Mindfulness] Show video cover as a preview `beta-good-to-have`
  #50 · Shaomei opened on Apr 18, 2024
- Play a sound when waving hand `enhancement` — 2
  #46 · Shaomei opened on Apr 18, 2024
- Mute the mindfulness videos by default `beta-good-to-have`
  #45 · Shaomei opened on Apr 18, 2024

2. Design

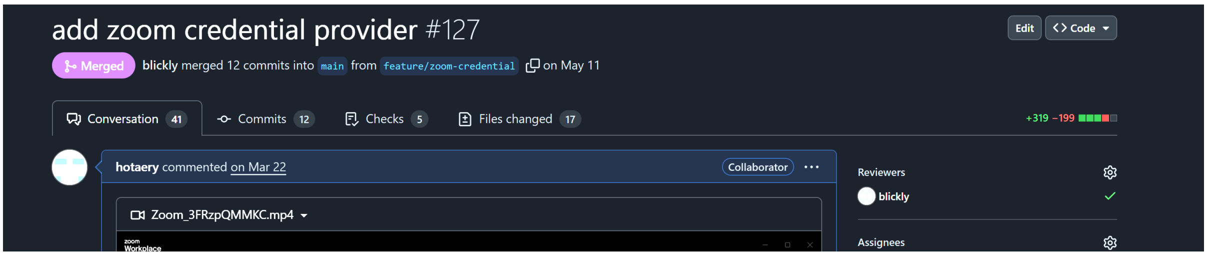
- Designs are reviewed for security flaws.
- Use of secure design principles: least privilege, fail-safe defaults, input validation, etc.
- Architecture diagrams and data flow documentation are required before development starts.
- Evidence:


Client
Server
ZoomAPI
Apply Zoom authorization code via Zoom SDK
alt
[Apply failed]
Sign-in error
[Apply succeeded]
Sign-in API with authorization code
alt
[Missing code]
Throw error (bug)
Sign-in failed
[Authorization code exists]
Get Zoom account using auth code
alt
[Zoom account fetch failed]
Error
Sign-in failed
[Zoom account fetched]
Zoom account info
Add user email to session
Sign-in success
alt
[Client receives sign-in failed]
No email, cannot call /api/log
[Client receives sign-in success]
Enter main page
Client
Server
ZoomAPI

3. Implementation

- Branch Strategy:
  - We follow GitHub Flow. main is protected. All features/fixes are implemented via pull requests (PRs).
- Code Review:
  - Peer review is mandatory before merging.
  - Reviewers use GitHub's "Request Changes" or "Approve" features.

- Evidence:
  - PR Review



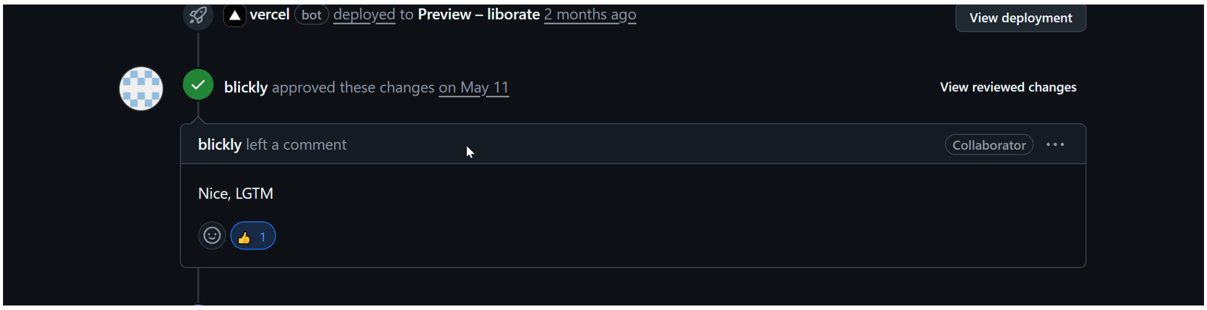
add zoom credential provider #127

Merged blickly merged 12 commits into main from feature/zoom-credential on May 11

hotaery commented on Mar 22

Zoom_3FRzpQMMKC.mp4

  - PR Approved



vercel bot deployed to Preview – liborate 2 months ago

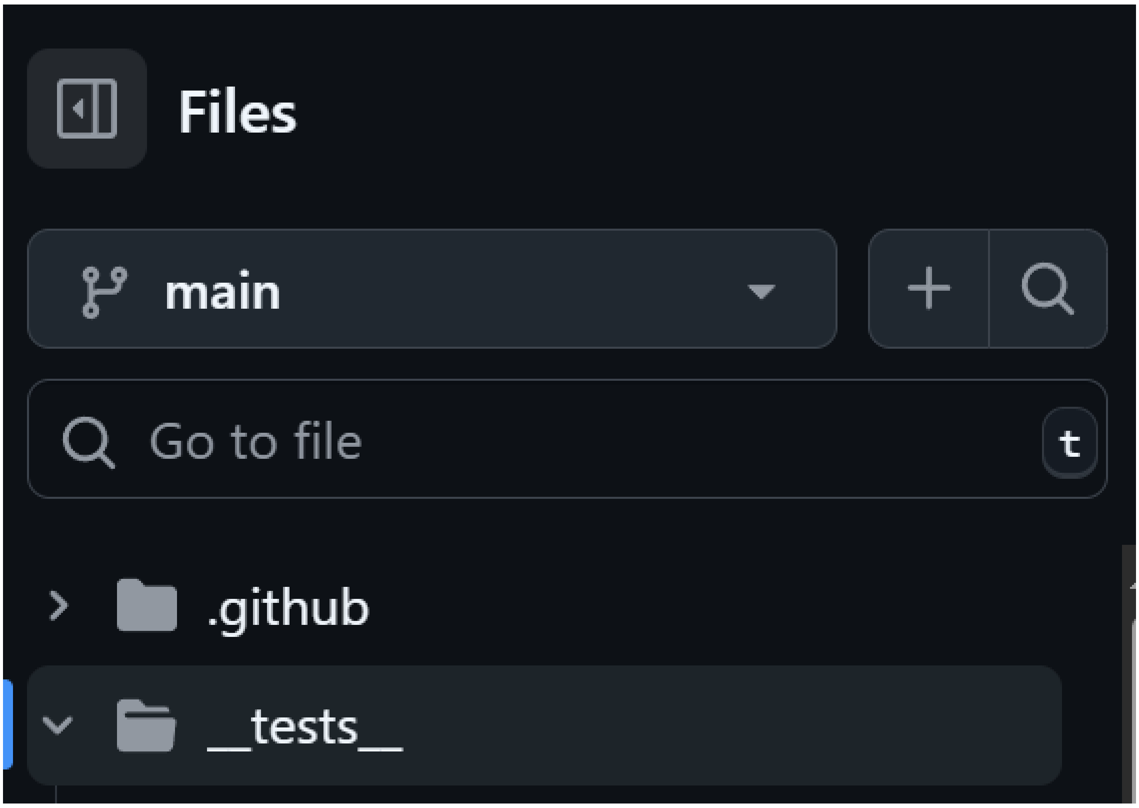
blickly approved these changes on May 11

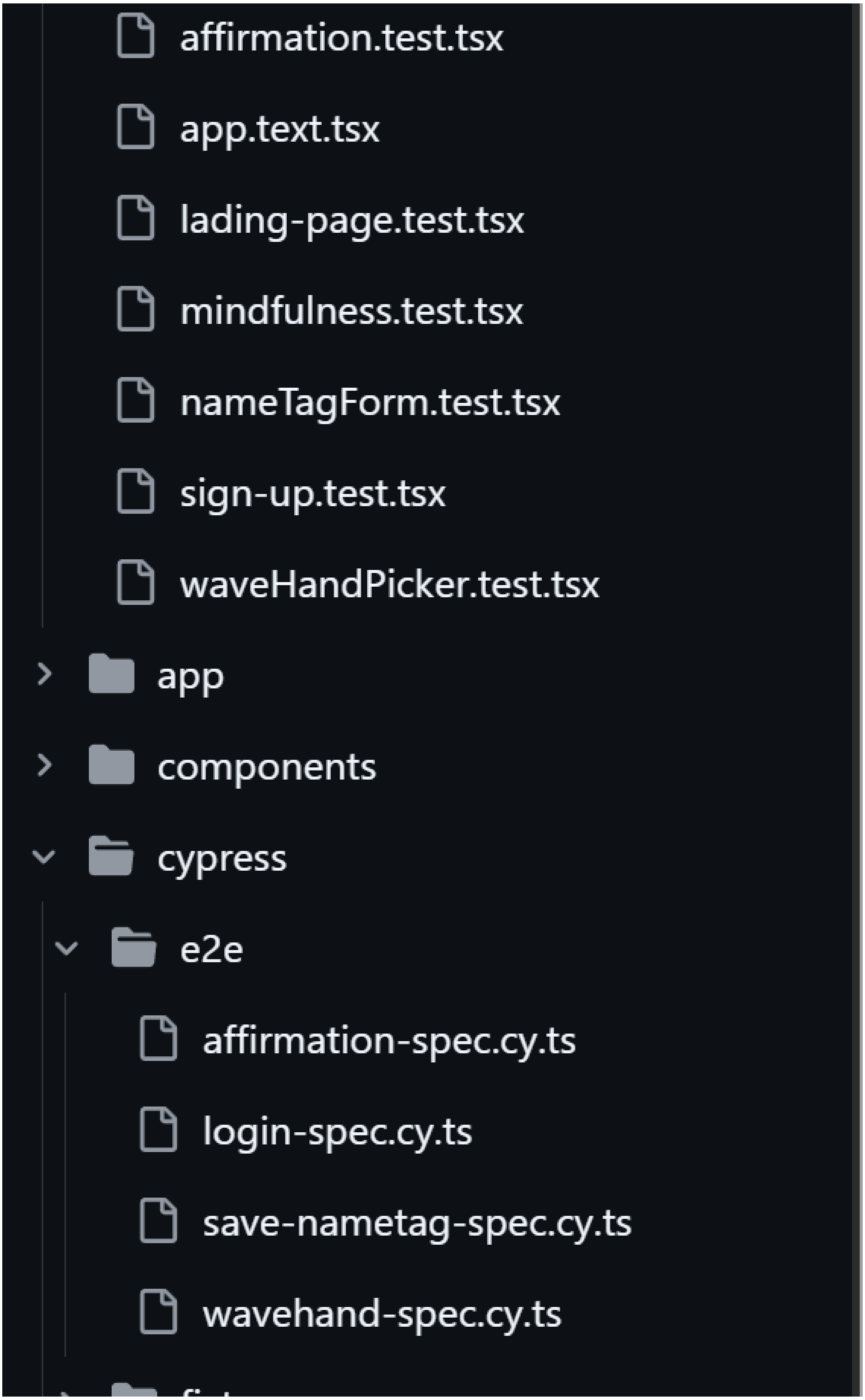
blickly left a comment

Nice, LGTM

4. Testing

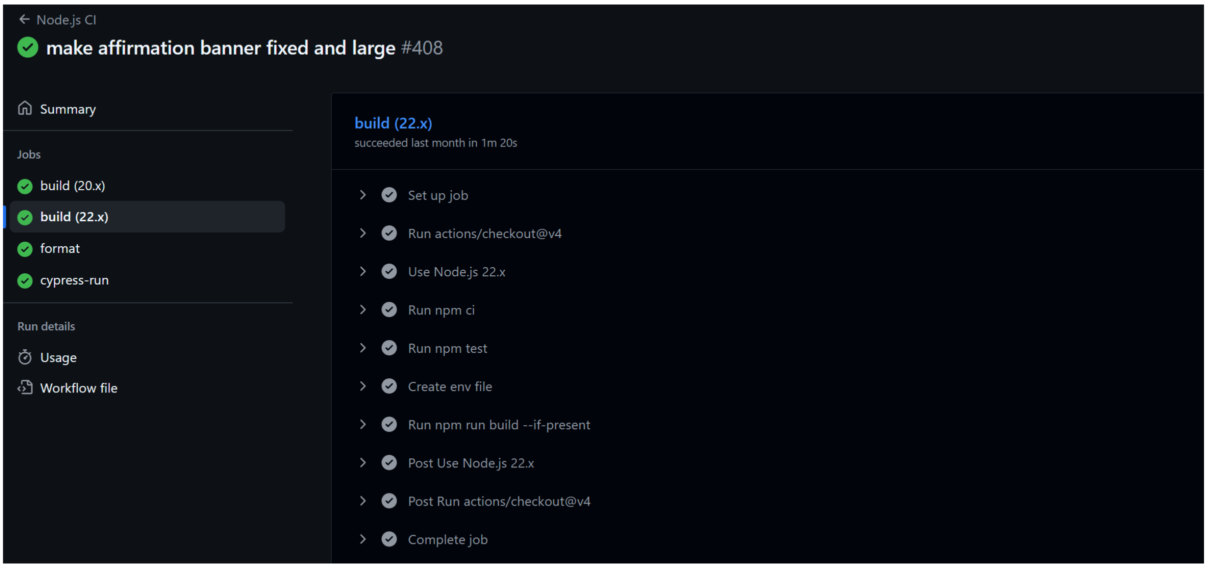
- Automated Tests:
  - We run unit tests and Cypress E2E tests on each PR and push.
  - Test results are validated in GitHub Actions.
- Evidence:
  - UT and cypress E2E tests





```
affirmation.test.tsx
app.text.tsx
lading-page.test.tsx
mindfulness.test.tsx
nameTagForm.test.tsx
sign-up.test.tsx
waveHandPicker.test.tsx
> app
> components
v cypress
  v e2e
    affirmation-spec.cy.ts
    login-spec.cy.ts
    save-nametag-spec.cy.ts
    wavehand-spec.cy.ts
```

- Run UT

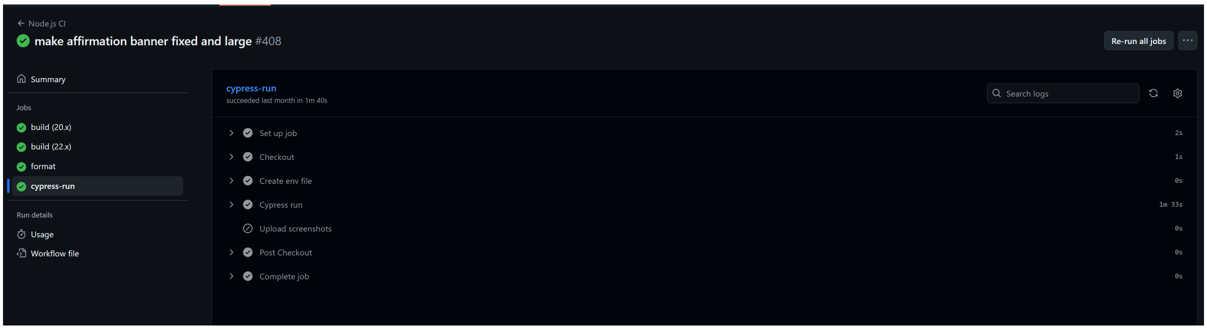


make affirmation banner fixed and large #408

build (22.x)
succeeded last month in 1m 20s

```
Set up job
Run actions/checkout@v4
Use Node.js 22.x
Run npm ci
Run npm test
Create env file
Run npm run build --if-present
Post Use Node.js 22.x
Post Run actions/checkout@v4
Complete job
```

- Run cypress E2E tests



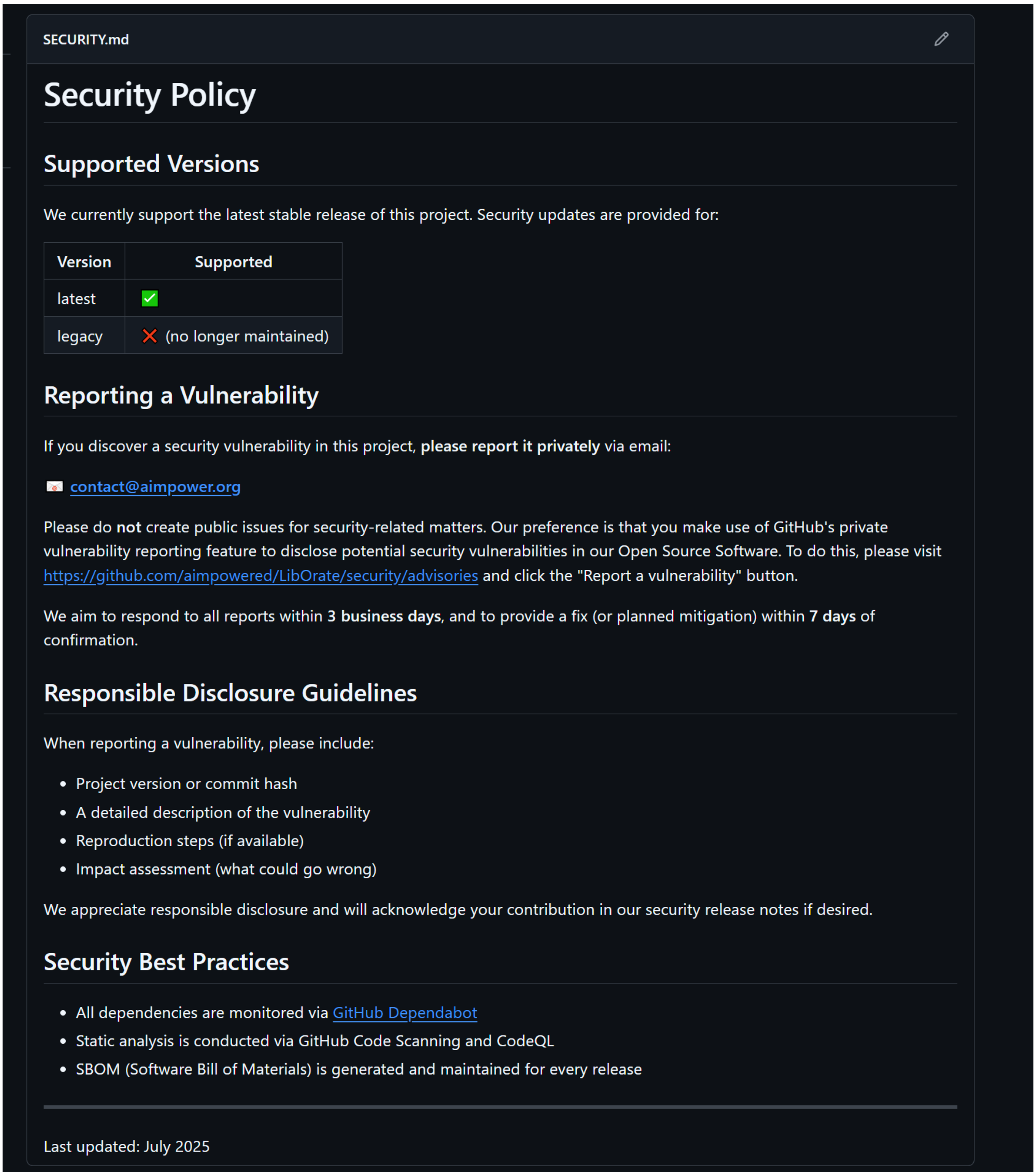
make affirmation banner fixed and large #408

cypress-run
succeeded last month in 1m 40s

```
Set up job                2s
Checkout                  1s
Create env file           0s
Cypress run           1m 33s
Upload screenshots        0s
Post Checkout             0s
Complete job              0s
```

6. Security Practices

- Tools Used:
  - npm audit
  - Snyk
  - GitHub Code Scanning (CodeQL)
  - Dependabot
  - Secret Scanning (GitHub Secrets)
- Security Policy
  - SECURITY.md defines vulnerability reporting process.
- Evidence:
  - Security policy



SECURITY.md

Security Policy

Supported Versions

We currently support the latest stable release of this project. Security updates are provided for:

Version	Supported
latest	✅
legacy	❌ (no longer maintained)

Reporting a Vulnerability

If you discover a security vulnerability in this project, **please report it privately** via email:

📧 contact@aimpower.org

Please do **not** create public issues for security-related matters. Our preference is that you make use of GitHub's private vulnerability reporting feature to disclose potential security vulnerabilities in our Open Source Software. To do this, please visit https://github.com/aimpowered/LibOrate/security/advisories and click the "Report a vulnerability" button.

We aim to respond to all reports within **3 business days**, and to provide a fix (or planned mitigation) within **7 days** of confirmation.

Responsible Disclosure Guidelines

When reporting a vulnerability, please include:

- Project version or commit hash
- A detailed description of the vulnerability
- Reproduction steps (if available)
- Impact assessment (what could go wrong)

We appreciate responsible disclosure and will acknowledge your contribution in our security release notes if desired.

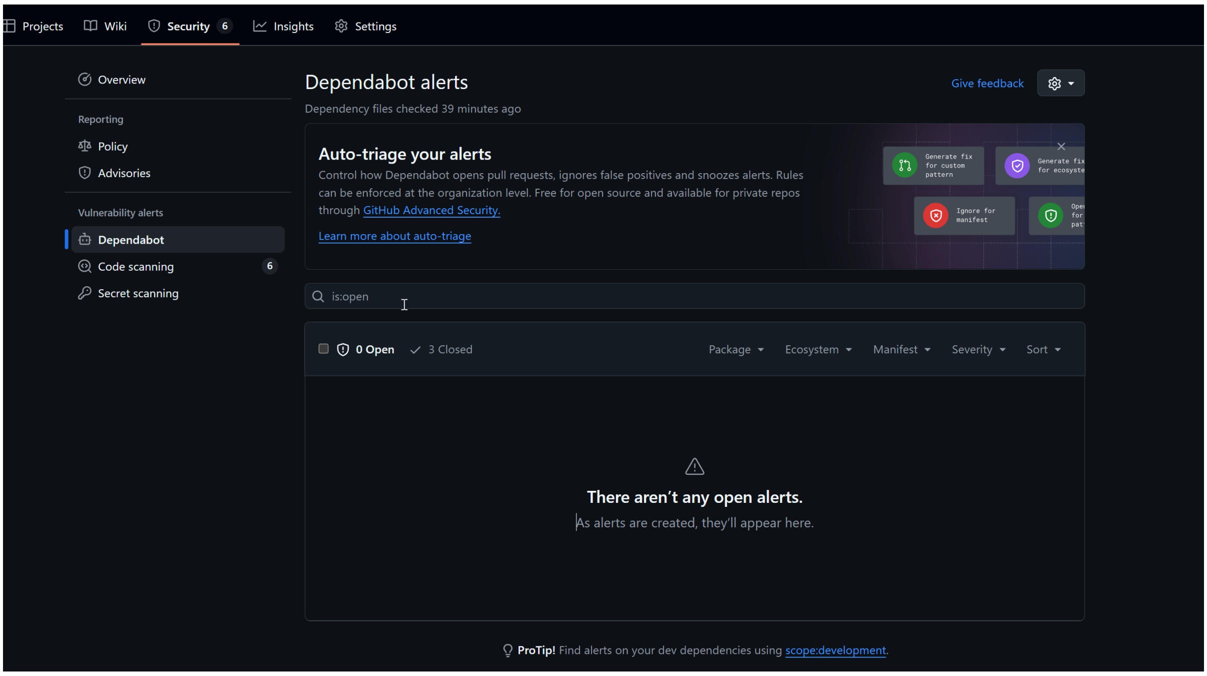
Security Best Practices

- All dependencies are monitored via GitHub Dependabot
- Static analysis is conducted via GitHub Code Scanning and CodeQL
- SBOM (Software Bill of Materials) is generated and maintained for every release

---

Last updated: July 2025

- Github Dependabot Alert



Dependabot alerts

Dependency files checked 39 minutes ago

Auto-triage your alerts

Control how Dependabot opens pull requests, ignores false positives and snoozes alerts. Rules can be enforced at the organization level. Free for open source and available for private repos through GitHub Advanced Security.

Learn more about auto-triage

is:open

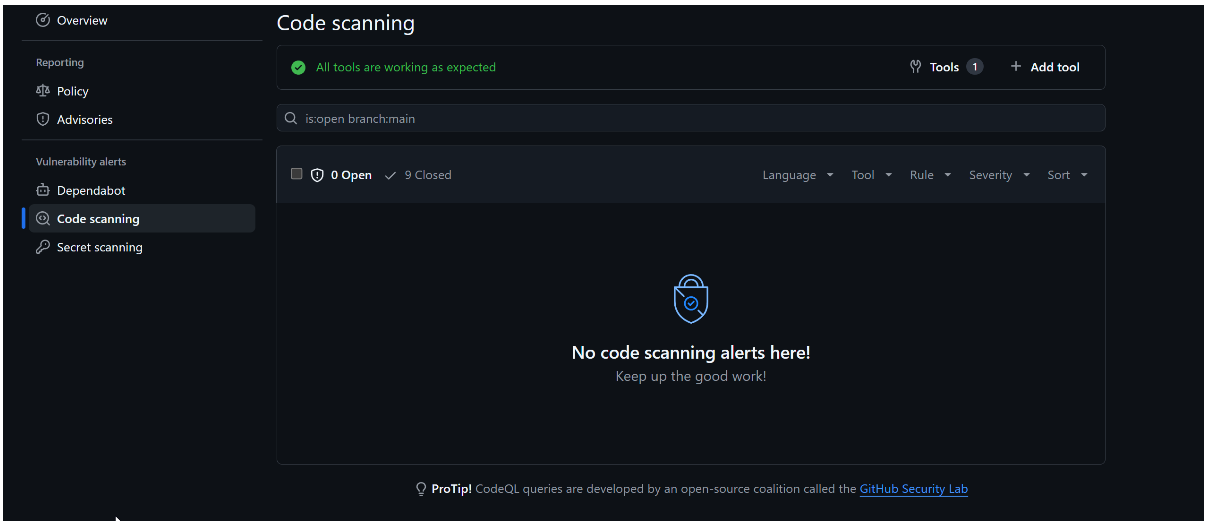
0 Open ✓ 3 Closed

There aren't any open alerts.

As alerts are created, they'll appear here.

ProTip! Find alerts on your dev dependencies using scope:development.

- Code Scanning Alert



Code scanning

All tools are working as expected

is:open branch:main

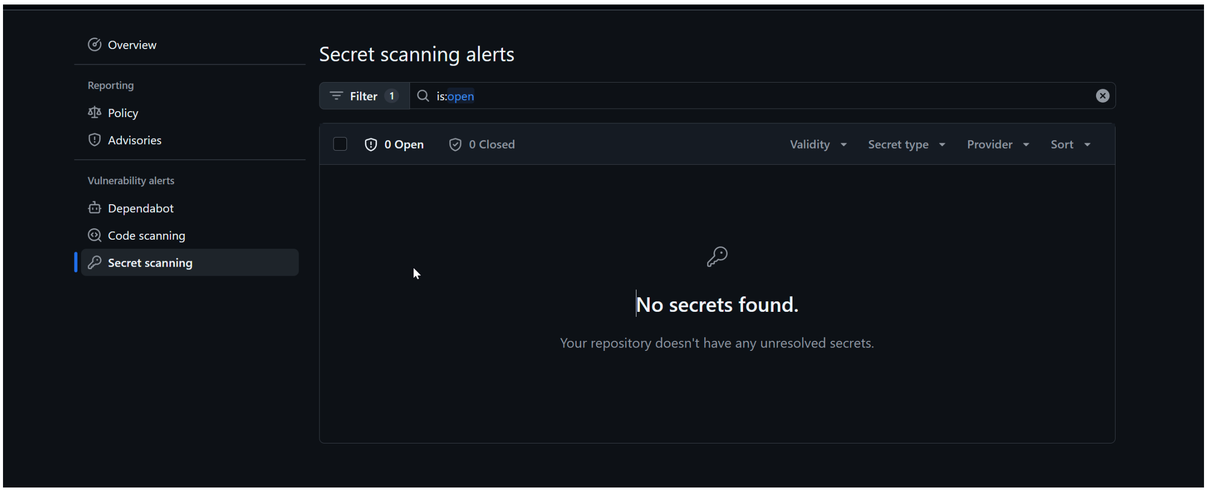
0 Open ✓ 9 Closed

No code scanning alerts here!

Keep up the good work!

ProTip! CodeQL queries are developed by an open-source coalition called the GitHub Security Lab

- Secret Scanning Alert



Secret scanning alerts

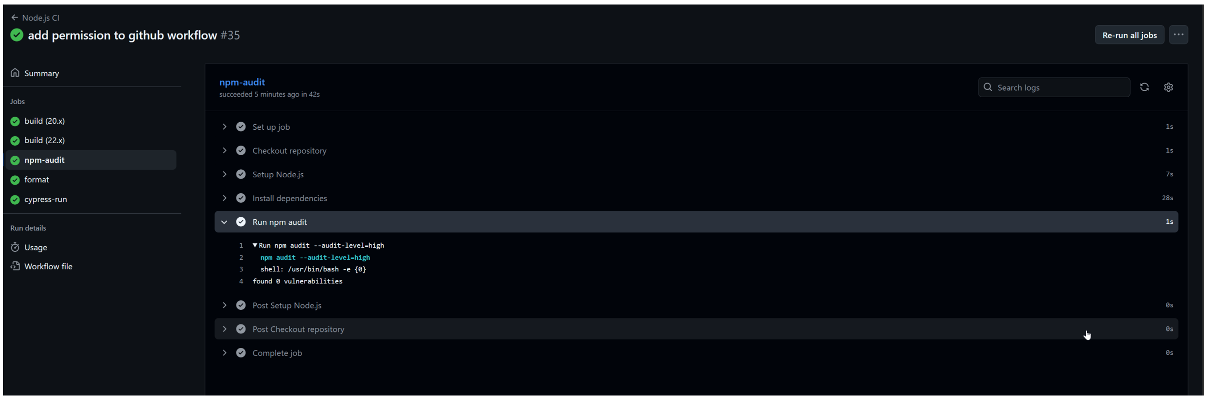
is:open

0 Open 0 Closed

No secrets found.

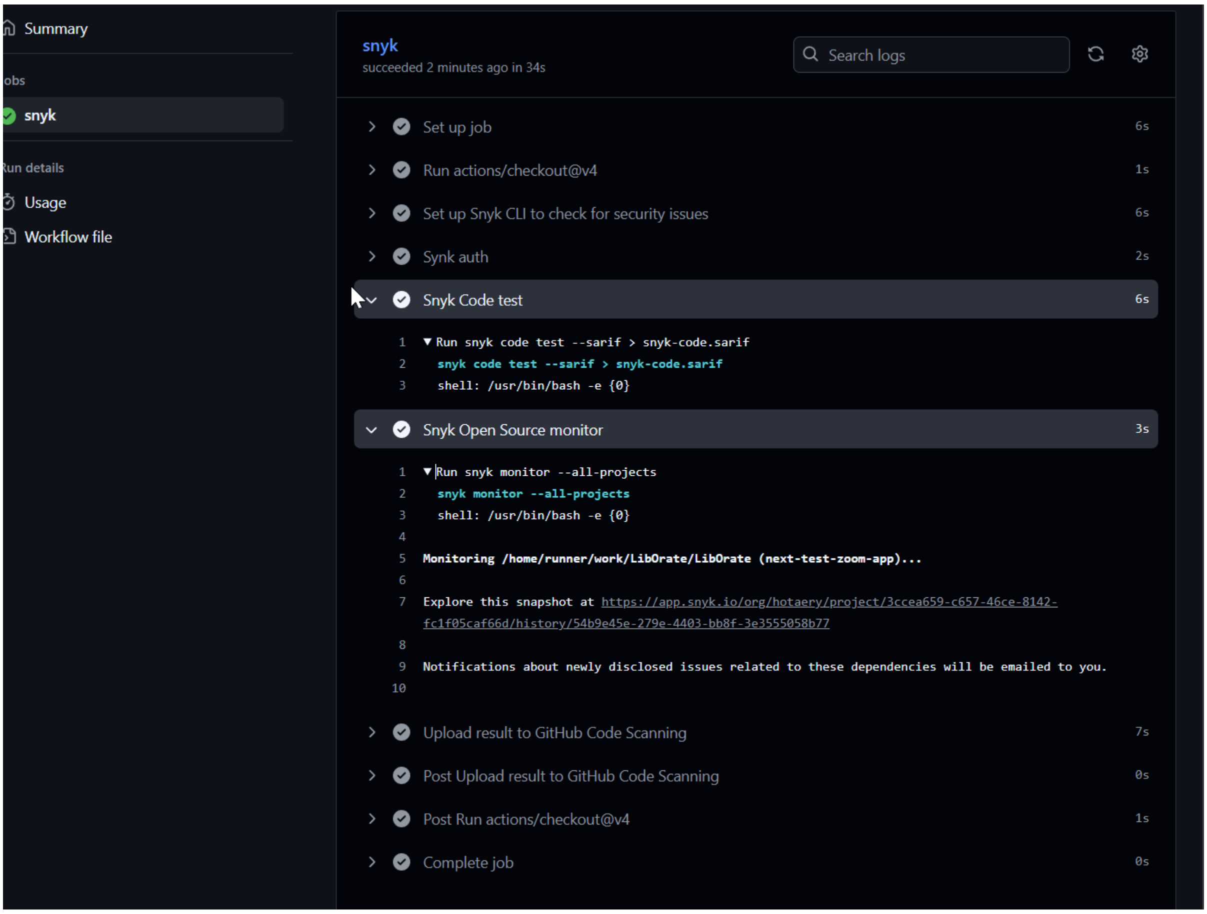
Your repository doesn't have any unresolved secrets.

- npm audit



```
▼Run npm audit --audit-level=high
  npm audit --audit-level=high
  shell: /usr/bin/bash -e {0}
found 0 vulnerabilities
```

- Integrate Snyk

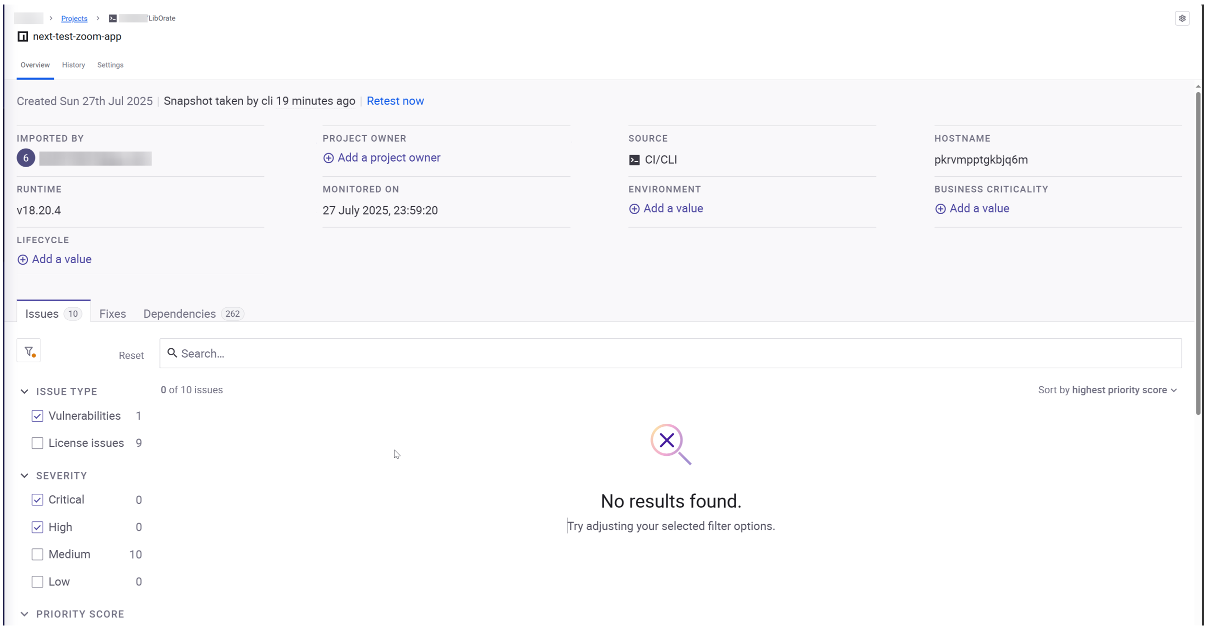

Summary
obs
snyk
un details
Usage
Workflow file
snyk
succeeded 2 minutes ago in 34s
Search logs
Set up job 6s
Run actions/checkout@v4 1s
Set up Snyk CLI to check for security issues 6s
Synk auth 2s
Snyk Code test 6s

```
▼Run snyk code test --sarif > snyk-code.sarif
  snyk code test --sarif > snyk-code.sarif
  shell: /usr/bin/bash -e {0}
```

Snyk Open Source monitor 3s

```
▼Run snyk monitor --all-projects
  snyk monitor --all-projects
  shell: /usr/bin/bash -e {0}

Monitoring /home/runner/work/LibOrate/LibOrate (next-test-zoom-app)...

Explore this snapshot at https://app.snyk.io/org/hotaery/project/3ccea659-c657-46ce-8142-
fc1f05caf66d/history/54b9e45e-279e-4403-bb8f-3e3555058b77

Notifications about newly disclosed issues related to these dependencies will be emailed to you.

```

Upload result to GitHub Code Scanning 7s
Post Upload result to GitHub Code Scanning 0s
Post Run actions/checkout@v4 1s
Complete job 0s



[redacted] › Projects › [redacted]/LibOrate

next-test-zoom-app

Created Sun 27th Jul 2025 | Snapshot taken by cli 19 minutes ago | Retest now

IMPORTED BY: 6 [redacted]

PROJECT OWNER: Add a project owner

SOURCE: CI/CLI

HOSTNAME: pkrvmpptgkbjq6m

RUNTIME: v18.20.4

MONITORED ON: 27 July 2025, 23:59:20

ENVIRONMENT: Add a value

BUSINESS CRITICALITY: Add a value

LIFECYCLE: Add a value

ISSUE TYPE
- ☑ Vulnerabilities 1
- □ License issues 9

SEVERITY
- ☑ Critical 0
- ☑ High 0
- □ Medium 10
- □ Low 0

PRIORITY SCORE

0 of 10 issues

Sort by highest priority score

No results found.

Try adjusting your selected filter options.

Last reviewed: July 2025

Owner: AImpower.org