Security & Testing

Last updated by | Daniels, Steve | Oct 23, 2025 at 6:53 PM GMT+5:30

Contents

SAST (Static Application Security Testing)

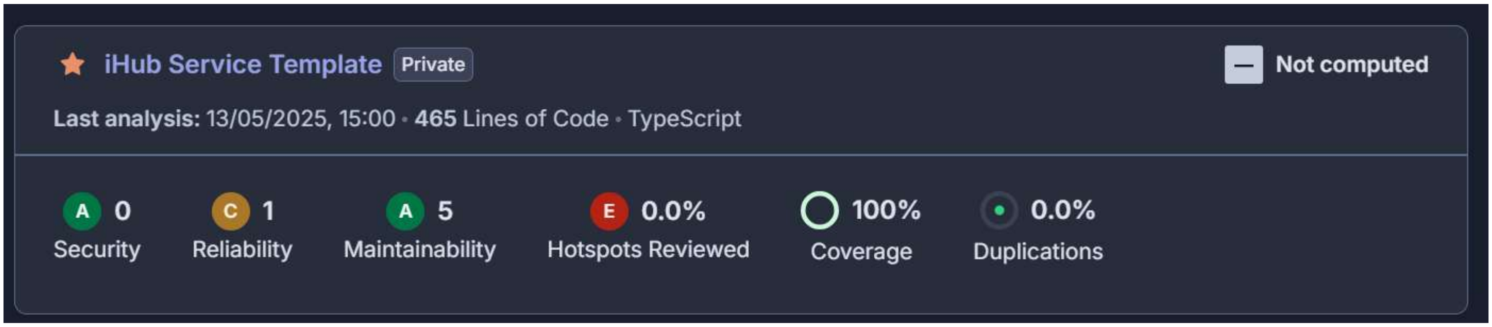
Sonarcloud

Work items:

- 55027 **Sonar Cloud pipeline scanning (iHub)** | Done
- 70759 **Sonar Cloud pipeline scanning (Python)** | Done
- 70761 **Sonar Cloud pipeline scanning (React)** | Done
- 70760 **Sonar Cloud pipeline scanning (Azure Functions)** | Done
- 85128 **Sonar Cloud pipeline scanning (Q FE / API)** | Done

We use SonarCloud to scan source code during development and this is checked during Pull Requests at iHub

- Projects - iquw1856 organization - SonarQube Cloud


iHub Service Template Private

Not computed

Last analysis: 13/05/2025, 15:00 • 465 Lines of Code • TypeScript

A 0 Security

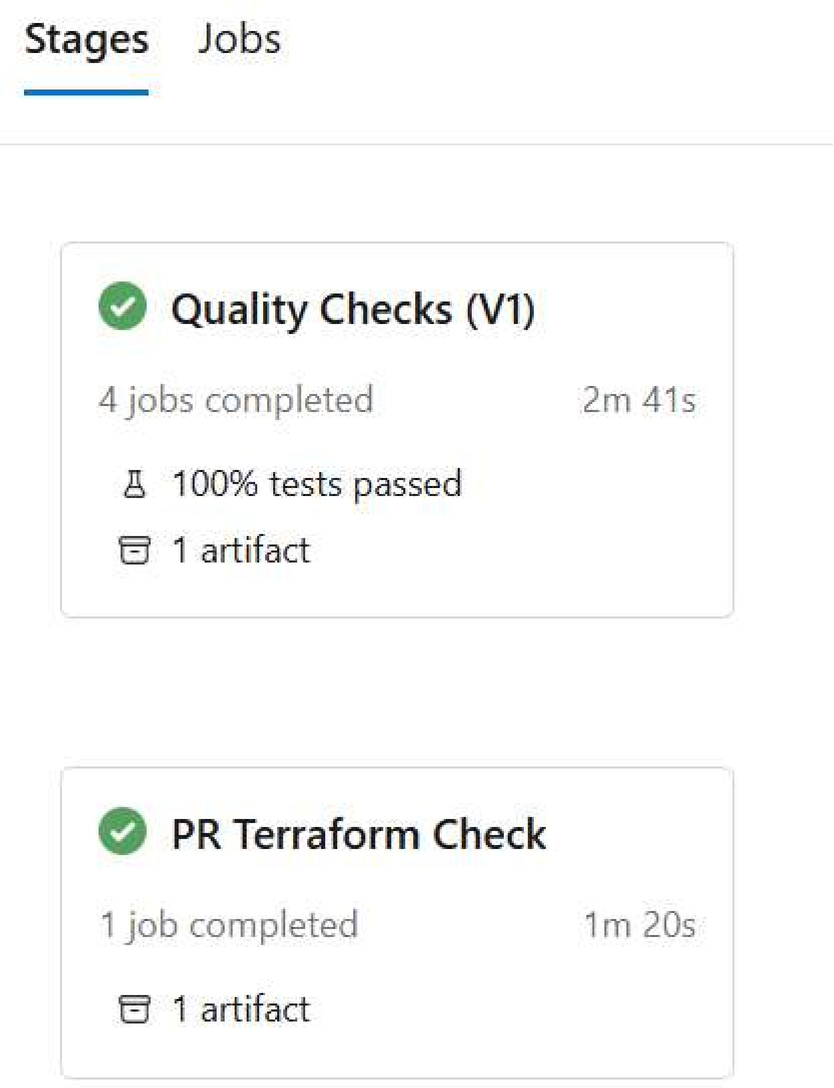
C 1 Reliability

A 5 Maintainability

E 0.0% Hotspots Reviewed

100% Coverage

0.0% Duplications



✓ Quality Checks (V1)

4 jobs completed 2m 41s

100% tests passed

1 artifact

✓ PR Terraform Check

1 job completed 1m 20s

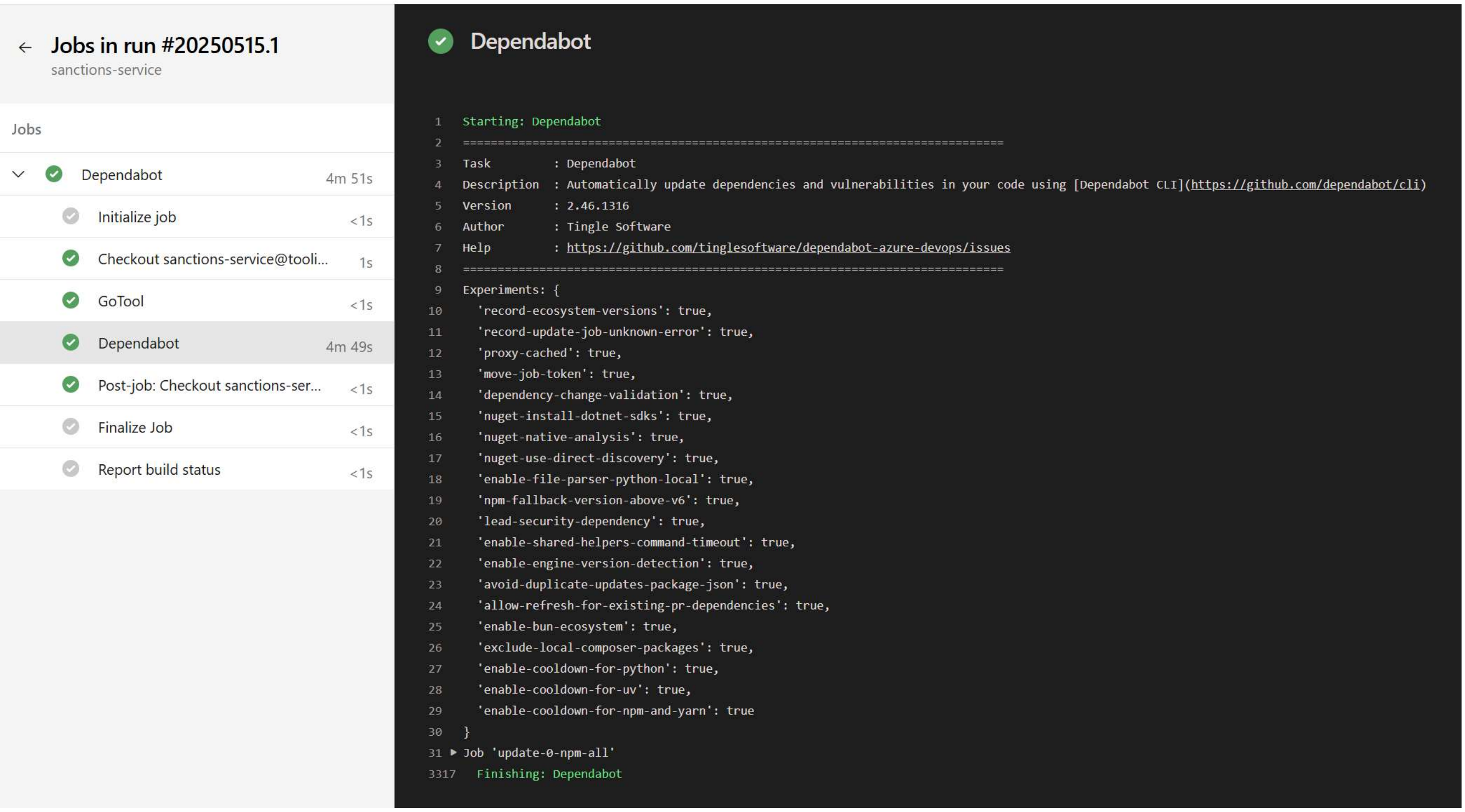
1 artifact

Dependabot

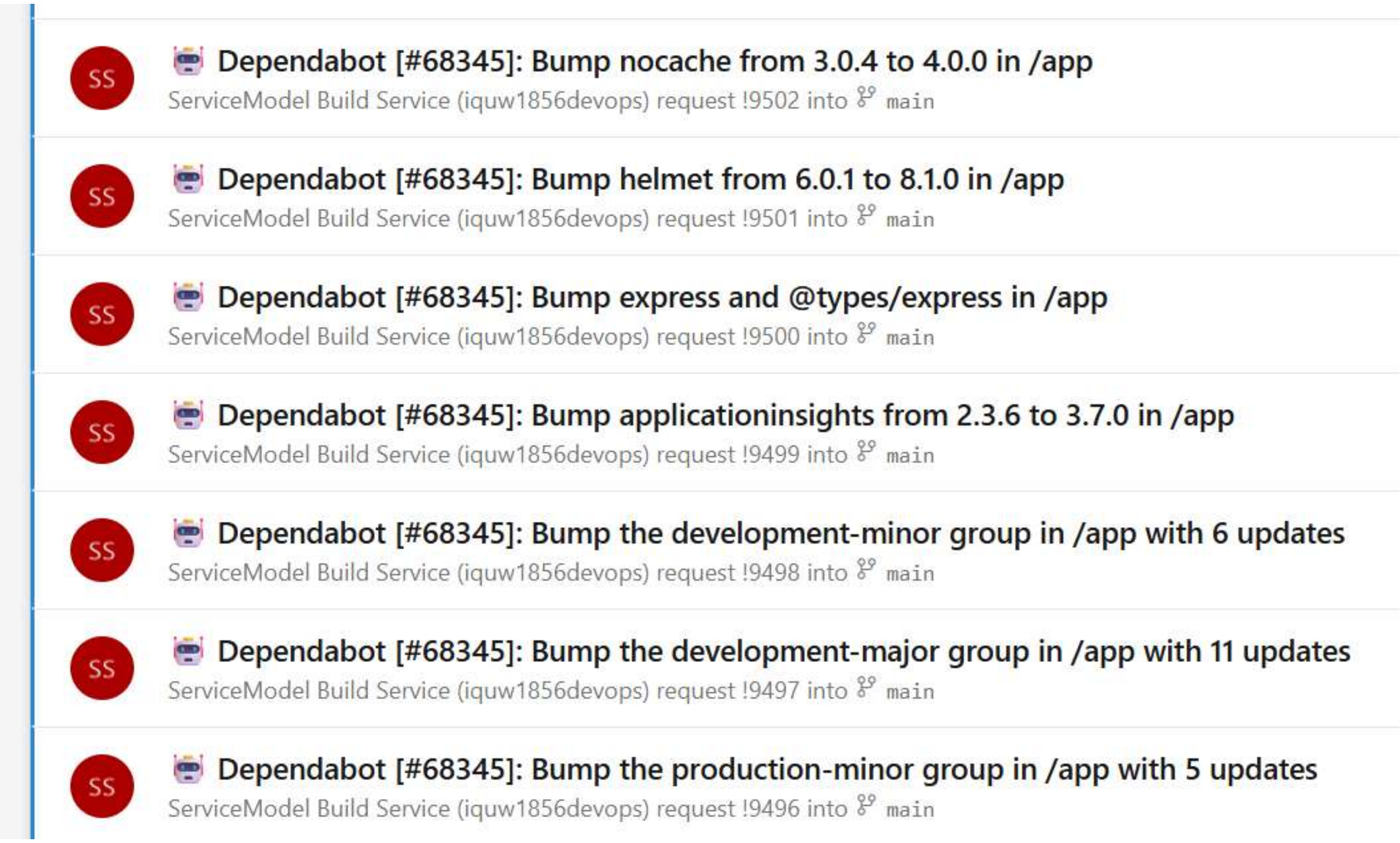
Work items:

- 48313 **Vulnerabilities scanning (iHub)** | Done
- 70762 **Vulnerabilities Scanning (Python)** | Done
- 70763 **Vulnerabilities Scanning (React)** | Done
- 67525 **Vulnerabilities Scanning (Azure Functions)** | Done
- 81543 **Vulnerability Scanning (Dataiku)** | New

We use Dependabot to scan source code for vulnerabilities



```
Starting: Dependabot
==============================================================================
Task         : Dependabot
Description  : Automatically update dependencies and vulnerabilities in your code using [Dependabot CLI](https://github.com/dependabot/cli)
Version      : 2.46.1316
Author       : Tingle Software
Help         : https://github.com/tinglesoftware/dependabot-azure-devops/issues
==============================================================================
Experiments: {
  'record-ecosystem-versions': true,
  'record-update-job-unknown-error': true,
  'proxy-cached': true,
  'move-job-token': true,
  'dependency-change-validation': true,
  'nuget-install-dotnet-sdks': true,
  'nuget-native-analysis': true,
  'nuget-use-direct-discovery': true,
  'enable-file-parser-python-local': true,
  'npm-fallback-version-above-v6': true,
  'lead-security-dependency': true,
  'enable-shared-helpers-command-timeout': true,
  'enable-engine-version-detection': true,
  'avoid-duplicate-updates-package-json': true,
  'allow-refresh-for-existing-pr-dependencies': true,
  'enable-bun-ecosystem': true,
  'exclude-local-composer-packages': true,
  'enable-cooldown-for-python': true,
  'enable-cooldown-for-uv': true,
  'enable-cooldown-for-npm-and-yarn': true
}
▶ Job 'update-0-npm-all'
  Finishing: Dependabot
```



SS Dependabot [#68345]: Bump nocache from 3.0.4 to 4.0.0 in /app
ServiceModel Build Service (iquw1856devops) request !9502 into main

SS Dependabot [#68345]: Bump helmet from 6.0.1 to 8.1.0 in /app
ServiceModel Build Service (iquw1856devops) request !9501 into main

SS Dependabot [#68345]: Bump express and @types/express in /app
ServiceModel Build Service (iquw1856devops) request !9500 into main

SS Dependabot [#68345]: Bump applicationinsights from 2.3.6 to 3.7.0 in /app
ServiceModel Build Service (iquw1856devops) request !9499 into main

SS Dependabot [#68345]: Bump the development-minor group in /app with 6 updates
ServiceModel Build Service (iquw1856devops) request !9498 into main

SS Dependabot [#68345]: Bump the development-major group in /app with 11 updates
ServiceModel Build Service (iquw1856devops) request !9497 into main

SS Dependabot [#68345]: Bump the production-minor group in /app with 5 updates
ServiceModel Build Service (iquw1856devops) request !9496 into main

Snyk

- 83536 **Add Snyk Security scanning (Azure Functions)** | New
- 83534 **Add Snyk Security scanning (Dataiku)** | New

- 83530 **Add Snyk Security scanning (iHub)** | In Technical Analysis
- 83532 **Add Snyk Security scanning (Python)** | New
- 83538 **Add Snyk Security scanning (Q FE / API)** | New

DAST (Dynamic Application Security Testing)

Automated Testing

UI

Automated UI tests (i.e. Unit testing, snapshot testing, etc) are not currently implemented but are planned as upcoming feature:

Work Items:

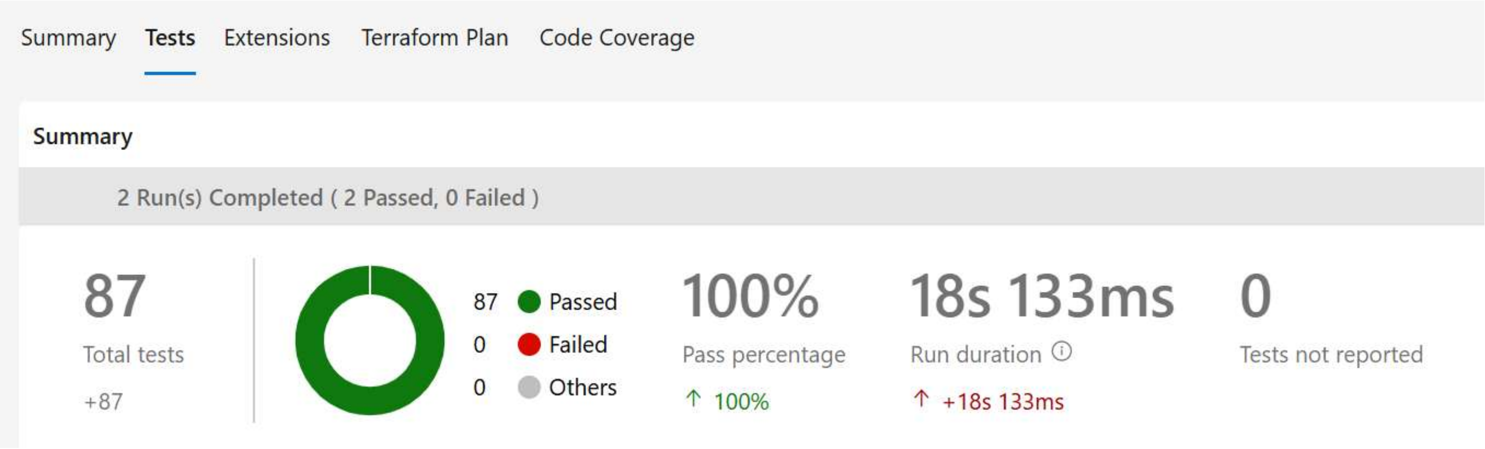
- 70767 **Automated tests for React Apps (unit/integration test)** | Done
- 70765 **Add code coverage reports and ensure 100% test coverage to all PRs (React)** | Done
- 85129 **Automated tests for Q FE / API Apps (unit/integration test)** | To Do
- 85131 **Add 100% test coverage for new code to all PRs (Q FE)** | New

API / Functions

Work Items:

- 65980 **Add 100% test coverage for new code to all PRs (iHub)** | Done
- 69394 **Add 100% test coverage for new code to all PRs (Python)** | Done
- 70764 **Add 100% test coverage for new code to all PRs (Azure Functions)** | Done
- 81544 **Add 100% test coverage for new code to all PRs (Dataiku)** | New
- 85130 **Add 100% test coverage for new code to all PRs (Q API)** | New

We ensure unit and integration tests for our APIs:



Summary

2 Run(s) Completed (2 Passed, 0 Failed)

87
Total tests
+87

87 ● Passed
0 ● Failed
0 ● Others

100%
Pass percentage
↑ 100%

18s 133ms
Run duration ⓘ
↑ +18s 133ms

0
Tests not reported

Automated Pentesting

We are exploring automated pen testing with Snyk

Manual End User Testing

Our test plans are stored here:

Test plans - Test Plans

Manual UAT is carried out:

- Prior to any production release
- Post any production release

Testing Process

- Requirements received in the form of ADO Product Backlog Items, once allocated to a sprint
- Tests scripted based on the acceptance criteria within the Product Backlog Items
- Tests executed on the front end of the application – taking applicable screenshots using the facility in ADO, for evidence of steps and outcomes
- If test is successful, ADO test is marked as Pass
- If test is unsuccessful, ADO test is marked as Fail, and a linked bug is raised from the test
- If a test is unable to be executed, it is marked as Blocked
- If a test becomes out of scope, it is marked as Not Applicable