SonarQube Notes

Umut

November 7, 2025

1 PDF Reports

PDF based reports are available beginning with the Enterprise edition, so Community and Developer tiers depend on the interactive portal instead.

2 Overview

The Overview page surfaces the core quality metrics at a glance: **Security**, **Reliability**, **Maintainability**, **Coverage**, and **Duplications**. These indicators provide an instant read on project health.

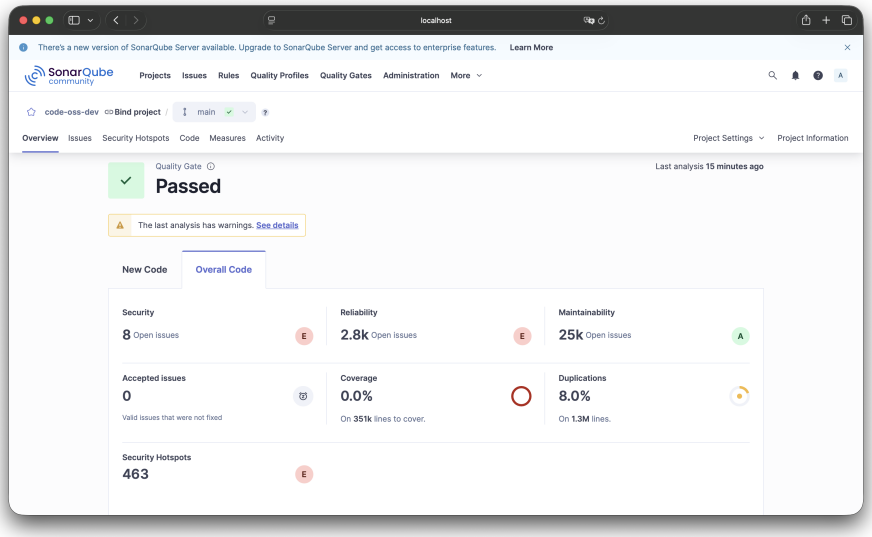

Figure 1: SonarQube Overview

3 Issues

The Issues view lists every open finding in a clean table together with the owning rule, severity, and the effort shown in the header. Extensive filtering is available by severity, status, security category, date, tags, and more, which makes narrowing focus straightforward when triaging.

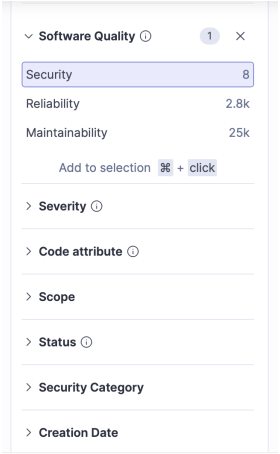

Figure 2: Filtering

Each issue row exposes quick actions to change the status (Accept, False Positive, Confirm, or Fixed) and to assign an owner. Tags are suggested automatically yet can be adjusted whenever extra labeling helps.

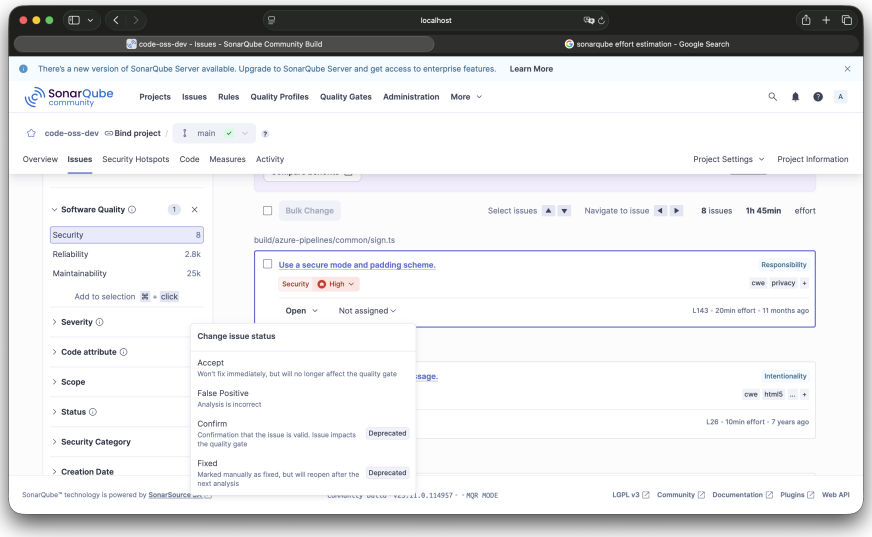

Figure 3: Issues Page

The dedicated Tags view illustrates which labels were applied automatically and lets you add them with custom categories.

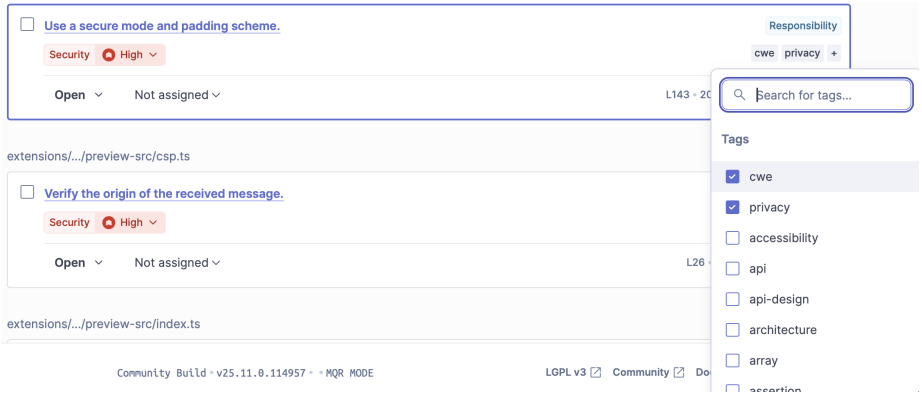

Figure 4: Tags

4 Issue Details

Issue details are intentionally thorough. Each card answers the practical questions: Where is the issue, Why is this an issue, How can I fix it, activities, and where can I find More info.

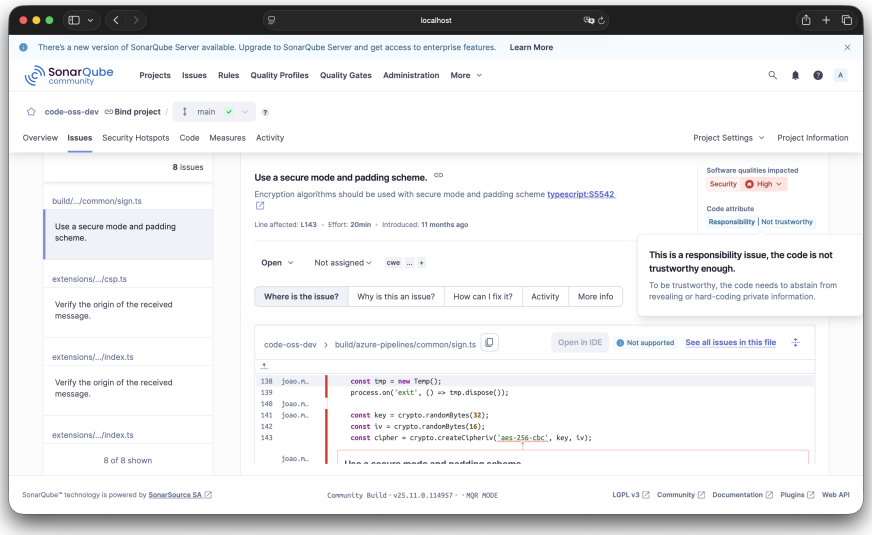

Figure 5: Issues Details

The **Why is this an issue?** panel explains the rule, outlines the impact, and clarifies the scope. Right below, **How can I fix it?** suggests concrete steps tailored to the detected language or framework, which speeds up consistent fixes.

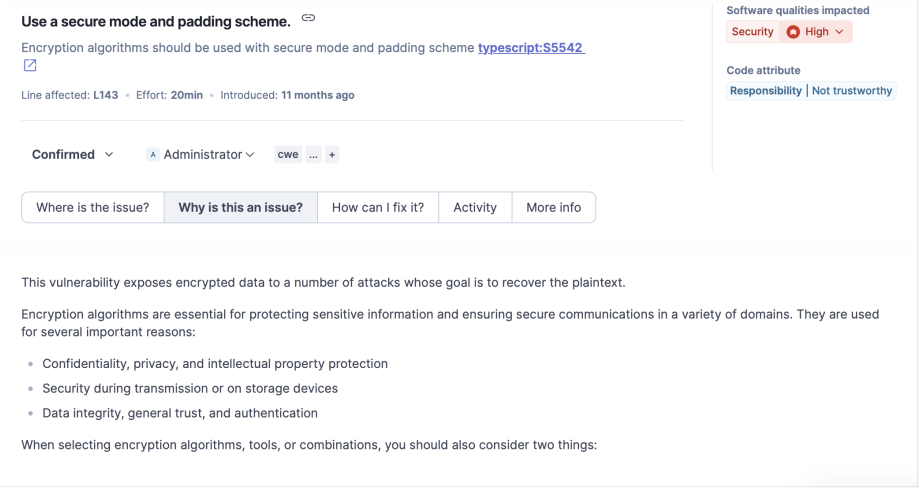

Figure 6: Why is this an issue?

5 Security Hotspot

A Security Hotspot represents code that deserves a second look because it might enable an exploit under the right conditions. It is not yet a confirmed vulnerability, but it is the platform nudging a reviewer to confirm whether the implementation is safe.

Possible alerts are the following:

- Potentially hard coded password
- Command injection
- Code injection
- Denial of Service (DoS)
- Permissions (root)
- Weak Cryptography
- Encryption of Sensitive Data
- Hard coded IP addresses

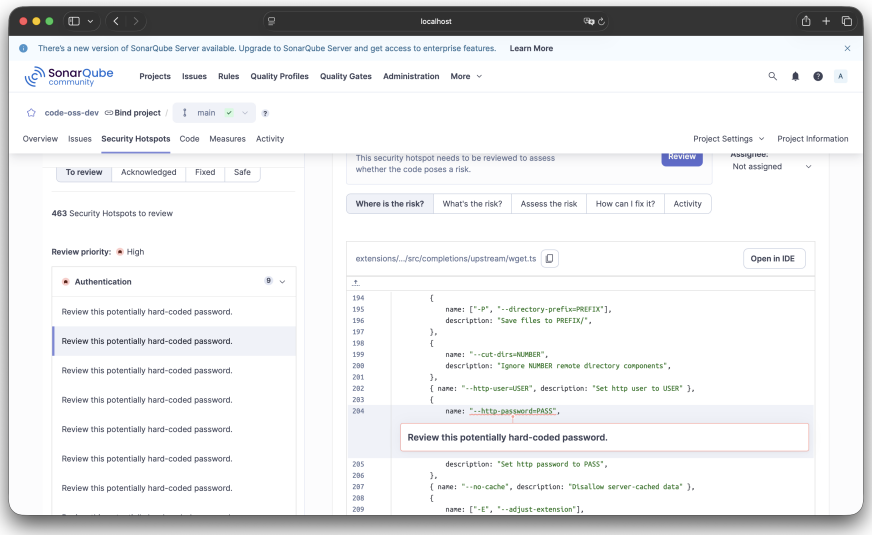

Figure 7: Security Hotspot

The details walk through **Where is the risk?**, **What is the risk?**, **Assess the risk**, and **How can I fix it?**, so reviewers can validate and plan accordingly.

6 Duplications

Duplicates provide a codes that are duplicated.

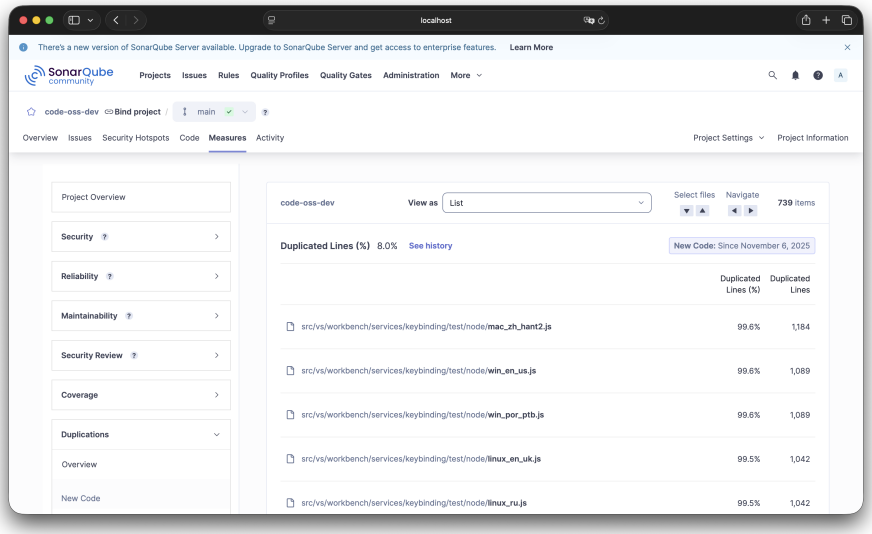

Figure 8: Duplications

7 Coverage

Coverage visualizes how much of the codebase is exercised by automated tests.

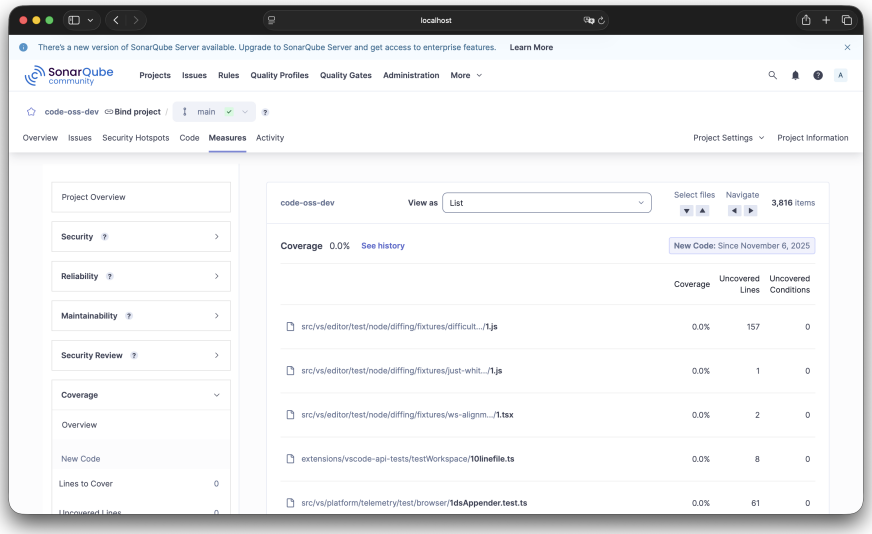

Figure 9: Coverage