**Why SonarQube**

**SonarQube can do** : Code smells, bugs, vulnerabilities, quality.

Code smells: something could be wrong or improved but not necessarily a bug, just poor design.

Bugs: something in the code that makes it behave poorly or crash.

Vunlerabilities: like SQL injection

Quality: code is clean

SonarQube is language specific: it understands the syntax and the practices for the language, semantics and the flow.

It also has a dashboard that lists the vunlerability, gives it a criticality, explains why is it bad practice and gives a solution.

Covers the top 10 OWASP:

1. -**Broken Access Control**
2. **Cryptographic Failures** (formerly Sensitive Data Exposure)
3. **Injection**
4. **Insecure Design**
5. **Security Misconfiguration**
6. **Vulnerable and Outdated Components**
7. **Identification and Authentication Failures**
8. **Software and Data Integrity Failures**
9. **Security Logging and Monitoring Failures**
10. **Server-Side Request Forgery (SSRF)**

Since we don’t have actual data of users stored on our pipeline gitleaks might be used as the secondary security tool