SonarQube

Descripción

SonarQube es una herramienta de análisis estático de código para detectar bugs, vulnerabilidades, y code smells en más de 25 lenguajes.

Uso local

```
# Análisis local con CLI
sonar-scanner -Dsonar.projectKey=myproject -Dsonar.sources=. -Dsonar.host.url=http://localhost:9000
```

Reportes

- Interfaz web con dashboards.
- Muestra cobertura de código, vulnerabilidades, duplicaciones, etc.

Integración en CI/CD

- Plugins para GitHub Actions.
- DevSecOps: integración con calidad de código.

```
  - name: SonarQube Scan
    uses: SonarSource/sonarqube-scan-action@<action version> # Ex: v4.1.0, See the latest version at https://github.com/marketplace/actions/official-sonarqube-scan
    env:
      SONAR_TOKEN: ${{ secrets.SONAR_TOKEN }}
      SONAR_HOST_URL: ${{ vars.SONAR_HOST_URL }}
```

Integraciones

- GitHub.
- Jira: integraciones para crear tickets automáticamente.
- Slack, Microsoft Teams: plugins para notificaciones.
- VSCode: extensión oficial.

UI

- Sí, una de las mejores UI del sector.

Licencia

- Versión **Community (gratis, OSS)**.
- Versiones Enterprise y Developer con más reglas/lenguajes.
- Puede instalarse en VMs (Docker o instalación manual).

Facilidad de uso

- Moderado. Requiere configuración inicial y escáner. UI muy intuitiva.

Cumplimiento con estándares:

- **OWASP:** Incluye reglas específicas alineadas con OWASP Top 10 (inyecciones, XSS, autenticación insegura, etc.).
- **NIST:** Compatible con NIST CSF y NIST 800-53 al apoyar revisiones de código (controles SA-11, RA-5).
- **ISO/IEC 27001:** Cumple con controles como A.14.2.5 (principios de desarrollo seguro) y A.14.2.8 (pruebas técnicas).
- **PCI DSS:** Cumple con requisitos de análisis de código seguro como el 6.3.2.

Revisión #8
Creado 16 julio 2025 17:40:34
Actualizado 16 julio 2025 22:37:50