UNIVERSITAS
GADJAH MADA
Analisis Keamanan Source Code Menggunakan SonarQube Self-Hosted pada Pemerintah Daerah Berbasis ISO 27001
Tazkia Amelya Fisya'Bani, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Analisis Keamanan *Source Code* Menggunakan SonarQube *Self-Hosted* pada Pemerintah Daerah Berbasis ISO 27001

Transformasi digital dalam pemerintah daerah meningkatkan penggunaan aplikasi berbasis web untuk meningkatkan layanan publik. Aspek keamanan *source code* penting untuk menjaga kualitas perangkat lunak, melindungi data, serta mendukung kepatuhan terhadap standar ISO 27001 dan UU PDP. Proses *code review* manual memerlukan waktu yang lama dan berisiko menyebabkan kerentanan keamanan tidak terdeteksi. Penelitian ini menerapkan *automatic deployment* berbasis SonarQube *Self-Hosted* untuk analisis kualitas dan keamanan *source code*. Sistem penelitian menggunakan *server* Linux dengan teknologi kontainer menggunakan Podman dan PostgreSQL sebagai *database* utamanya. Penelitian ini juga memanfaatkan SonarScanner dan metode *Static Application Security Testing* (SAST) untuk menganalisis aplikasi seperti WordPress, SLiMS8 Akasia, CKAN, dan GeoServer. Tujuan penelitian ini adalah untuk menganalisis kemampuan SonarQube *Self-Hosted* dalam mendeteksi kerentanan keamanan dan efisien proses *code review* otomatis. Hasil dari penelitian ini menunjukkan bahwa SonarQube *Self-Hosted* efektif dalam mendeteksi *issue security*, *reliability*, *maintainability*, dan *duplication* secara otomatis dan *real time*. GeoServer menghasilkan jumlah masalah tertinggi dengan 115 masalah keamanan, 3,4 ribu *issue reliability*, dan 32 ribu *issue maintainability*. CKAN menghasilkan tingkat duplikasi paling tinggi sebesar 9,5%. GeoServer menunjukkan tingkat efisiensi pemindaian paling tinggi di angka 85,17%, sedangkan WordPress menunjukkan waktu *delay* pemindaian tertinggi sebesar 256 detik. Implementasi *automatic deployment* berhasil meningkatkan efisiensi proses analisis kode dan mendukung penerapan DevSecOps dan memenuhi kepatuhan terhadap standar ISO 27001.

Kata kunci: *Automatic Deployment*, *Code Review*, DevSecOps, ISO 27001, Keamanan Aplikasi, SAST, SonarQube, SonarScanner.

UNIVERSITAS
GADJAH MADA
Analisis Keamanan Source Code Menggunakan SonarQube Self-Hosted pada Pemerintah Daerah Berbasis ISO 27001
Tazkia Amelya Fisya'Bani, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

Source Code Security Analysis Using Self-Hosted SonarQube in ISO 27001-Based Local Government

Digital transformation in local government increases the use of web-based applications to improve public services. Source code security is crucial for maintaining software quality, protecting data, and supporting compliance with ISO 27001 standards and the PDP Law. Manual code review processes are time-consuming and risk leaving security vulnerabilities undetected. This study implemented a SonarQube Self-Hosted automated deployment for source code quality and security analysis. The research system uses a Linux server with container technology using Podman and PostgreSQL as its main database. This study also utilized SonarScanner and the Static Application Security Testing (SAST) method to analyze applications such as WordPress, SLiMS8 Akasia, CKAN, and GeoServer. The purpose of this study was to analyze SonarQube Self-Hosted's ability to detect security vulnerabilities and the efficiency of the automated code review process. The results of this study indicate that SonarQube Self-Hosted is effective in detecting security, reliability, maintainability, and duplication issues automatically and in real time. GeoServer generated the highest number of issues with 115 security issues, 3.4,000 reliability issues, and 32,000 maintainability issues. CKAN generated the highest duplication rate at 9.5%. GeoServer demonstrated the highest scanning efficiency at 85.17%, while WordPress showed the highest scan delay at 256 seconds. The implementation of automatic deployment successfully improved the efficiency of the code analysis process and supported DevSecOps implementation and compliance with ISO 27001 standards.

Keywords: Automatic Deployment, Code Review, DevSecOps, ISO 27001, Application Security, SAST, SonarQube, SonarScanner.