ABSTRAK

Murtadlo, Moh. Hammim. 2026. Analisis dan Evaluasi Keamanan *Website* Menggunakan Metode *Penetration Testing* Berdasarkan Standar *OWASP TOP 10.*

Pembimbing: (1) Ari Eko Wardoyo, S.T., M.Kom; (2) Triawan Adi Cahyanto, M.Kom.

Sistem Informasi Akademik (SIAKAD) Universitas Muhammadiyah Jember merupakan aplikasi berbasis web yang digunakan untuk mendukung berbagai layanan akademik. Mengingat pentingnya data yang dikelola, diperlukan evaluasi keamanan untuk mengidentifikasi potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Penelitian ini bertujuan menganalisis keamanan SIAKAD Universitas Muhammadiyah Jember menggunakan metode *grey box penetration testing* berdasarkan OWASP Top 10 2021. Pengujian dilakukan melalui tahapan *information gathering*, *vulnerability analysis*, *exploitation*, *risk assessment*, *reporting*, dan pemberian rekomendasi perbaikan menggunakan *OWASP Risk Rating Methodology*. Hasil penelitian menunjukkan bahwa pada skenario pengujian yang dilakukan tidak ditemukan kerentanan pada kategori *Cryptographic Failures, Injection, Insecure Design, dan Server-Side Request Forgery*. Namun, ditemukan beberapa kelemahan keamanan pada kategori *Broken Access Control, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, serta Security Logging and Monitoring Failures*. Berdasarkan penilaian risiko, kerentanan pada kategori *Identification and Authentication Failures* dan *Software and Data Integrity Failures* memperoleh tingkat risiko *High*, *Vulnerable and Outdated Components* memperoleh tingkat risiko *Medium*, sedangkan *Broken Access Control, Security Misconfiguration, dan Security Logging and Monitoring Failures* memperoleh tingkat risiko *Low*. Hasil penelitian ini diharapkan menjadi bahan evaluasi untuk meningkatkan keamanan SIAKAD.

Kata Kunci: SIAKAD, *Penetration Testing*, *OWASP Top 10* 2021, Keamanan *Website*, *OWASP Risk Rating Methodology*.

ABSTRACT

Murtadlo, Moh. Hammim. 2026. *Website Security Analysis and Evaluation Using Penetration Testing Method Based on OWASP TOP 10 Standards*.

Advisors: (1) Ari Eko Wardoyo, S.T., M.Kom; (2) Triawan Adi Cahyanto, M.Kom.

The Academic Information System (SIAKAD) of Universitas Muhammadiyah Jember is a web-based application used to support various academic services. Considering the importance of the data managed by the system, a security evaluation is necessary to identify potential vulnerabilities that could be exploited by unauthorized parties. This study aims to analyze the security of SIAKAD Universitas Muhammadiyah Jember using the *grey box penetration testing* method based on the OWASP Top 10 2021 framework. The testing process consisted of *information gathering, vulnerability analysis, exploitation, risk assessment, reporting*, and providing security improvement recommendations using the OWASP Risk Rating Methodology. The results indicate that no vulnerabilities were identified under the testing scenarios for the *Cryptographic Failures, Injection, Insecure Design, and Server-Side Request Forgery* categories. However, *several security weaknesses were identified* in the *Broken Access Control, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, and Security Logging and Monitoring Failures* categories**.** Based on the risk assessment, the vulnerabilities in the *Identification and Authentication Failures* and *Software and Data Integrity Failures* categories were classified as *High* risk, the *Vulnerable and Outdated Components* category was classified as *Medium* risk, while the *Broken Access Control, Security Misconfiguration, and Security Logging and Monitoring Failures* categories were classified as *Low* risk. The findings of this study are expected to serve as a reference for improving the security of the SIAKAD application.

Keywords: SIAKAD, *Penetration Testing*, *OWASP Top 10* 2021, *Website Security*, *OWASP Risk Rating Methodology*.