INTISARI

Keamanan sistem informasi berbasis web merupakan aspek krusial dalam menjaga integritas data dan layanan, terutama di lingkungan institusi pendidikan tinggi. Website SIAKU Universitas Wijaya Kusuma Purwokerto (UNWIKU) sebagai sistem informasi akademik dan kemahasiswaan pernah mengalami insiden keamanan pada tahun 2024 berupa serangan spam iklan yang mengganggu layanan. Penelitian ini bertujuan untuk menganalisis keamanan website SIAKU UNWIKU menggunakan framework OWASP Top 10 versi 2021 untuk mengidentifikasi celah keamanan dan memberikan rekomendasi perbaikan. Hasil pengujian berhasil menemukan 10 kerentanan dengan level risiko yang bervariasi, terdiri dari 1 kerentanan kritis (critical), 1 berisiko tinggi (high), dan 8 lainnya berisiko sedang (medium). Beberapa eksploitasi berhasil dilakukan, mengindikasikan adanya potensi ancaman terhadap sistem. Berdasarkan pengukuran menggunakan CVSS (Common Vulnerability Scoring System) diperoleh rata-rata CVSS Score 6,0 yang mengindikasikan bahwa website SIAKU UNWIKU memiliki tingkat keparahan kerentanan medium. Framework OWASP Top 10 versi 2021 terbukti dapat mengidentifikasi serta menganalisis kerentanan keamanan secara sistematis, sekaligus menyusun rekomendasi mitigasinya. Temuan ini menunjukkan bahwa website SIAKU UNWIKU perlu dilakukan perbaikan dan penguatan sistem keamanan secara menyeluruh guna melindungi integritas, kerahasiaan, dan ketersediaan data. Penelitian ini juga diharapkan menjadi acuan dalam peningkatan keamanan sistem informasi akademik secara berkelanjutan.

Kata kunci: OWASP, CVSS, Kerentanan, Keamanan Website, Pengujian Penetrasi

ABSTRACT

Web-based information system security is a crucial aspect in maintaining data and service integrity, particularly within higher education institutions. The SIAKU website of Universitas Wijaya Kusuma Purwokerto (UNWIKU), which functions as an academic and student information system, experienced a security incident in 2024 involving spam advertisement attacks that disrupted services. This study aims to analyze the security of the SIAKU UNWIKU website using the OWASP Top 10 framework version 2021 to identify security vulnerabilities and provide mitigation recommendations. The testing process successfully identified 10 vulnerabilities with varying risk levels, consisting of 1 critical, 1 high, and 8 medium-risk vulnerabilities. Several exploitation attempts were successful, indicating potential threats to the system. Based on measurements using the Common Vulnerability Scoring System (CVSS), an average score of 6.0 was obtained, indicating that the website has a medium severity level. The OWASP Top 10 framework version 2021 proved can systematically identifying and analyzing security vulnerabilities as well as formulating appropriate mitigation recommendations. These findings indicate that the SIAKU UNWIKU website requires improvement and comprehensive security enhancements to protect data integrity, confidentiality, and availability. This research is also expected to serve as a reference for improving the security of academic information systems in a sustainable manner.

Keywords: OWASP, CVSS, Vulnerability, Website Security, Penetration Testing