INTISARI

Perkembangan teknologi informasi telah mendorong berbagai institusi, termasuk lembaga pendidikan, untuk memanfaatkan sistem informasi berbasis web sebagai sarana utama dalam penyampaian informasi dan layanan. Studi ini melaksanakan analisis kerentanan keamanan terhadap situs web resmi SMA Negeri 3 Purwokerto dengan menggunakan framework OWASP (Open Web Application Security Project) sebagai acuan utama. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis kelemahan keamanan yang terdapat pada website sekolah serta menyusun rekomendasi mitigasi berdasarkan temuan yang diperoleh. Pengujian keamanan dilakukan dengan menggunakan tools OWASP ZAP (Zed Attack Proxy), yang mampu memindai dan mengidentifikasi kerentanan secara otomatis. Hasil pemindaian menunjukkan terdapat 12 kerentanan keamanan, yang terdiri dari 1 kerentanan tinggi, 3 sedang, 4 rendah, dan 4 informasional. Setiap kerentanan dianalisis berdasarkan tingkat kerentanan, dampak, dan kemungkinan eksploitasi, lalu dievaluasi untuk menentukan perlakuan kerentanan menggunakan pendekatan Tolerate, Treat, dan Transfer. Seluruh kerentanan dikaitkan dengan klausul OWASP ASVS 5.0.0, serta diberikan rekomendasi teknis untuk mitigasi. Temuan ini diharapkan dapat menjadi acuan bagi SMA Negeri 3 Purwokerto maupun institusi pendidikan lainnya dalam memahami serta mengelola kerentanan keamanan website secara sistematis dan berkelanjutan.

Kata kunci: OWASP, keamanan website, kerentanan, mitigasi, ASVS 5.0.0

ABSTRACT

The advancement of information technology has encouraged various institutions, including educational organizations, to utilize web-based information systems as a primary medium for delivering services and information. This study conducts a vulnerability analysis of the official website of SMA Negeri 3 Purwokerto using the OWASP (Open Web Application Security Project) framework as the primary reference. The objective of this research is to identify and analyze potential security weaknesses and provide mitigation recommendations based on the findings. The security testing was performed using OWASP ZAP (Zed Attack Proxy), a tool capable of automatically scanning and detecting vulnerabilities. The results revealed 12 security risks consisting of 1 high-level risk, 3 medium-level risks, 4 low-level risks, and 4 informational risks. Each risk was analyzed based on its vulnerability, impact, and likelihood of exploitation, then evaluated using the approaches of Tolerate, Treat, or Transfer. All findings were mapped to the relevant clauses of OWASP ASVS 5.0.0, followed by appropriate technical mitigation recommendations. The results of this study are expected to serve as a reference for SMA Negeri 3 Purwokerto and other educational institutions in understanding and managing website security risks in a structured and continuous manner.

Keywords: OWASP, website security, vulnerability, mitigation, ASVS 5.0.0