INTISARI

STT Wiworotomo Purwokerto menyediakan sistem pembelajaran dalam jaringan atau elearning berbasis website. Situs website yang tidak memiliki keamanan yang memadai akan menjadi sasaran bagi para peretas cyber. Adapun tujuan yang ingin dicapai pada penelitian ini adalah untuk melakukan analisis kerentanan dengan metode Penetration Testing Execution Standard (PTES) dengan tahapan yang digunakan Intelegence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation dan Reporting. Hasil penelitian menggunakan alat pemindaian OWASP ZAP menunjukan adanya 12 kerentanan pada website Elearning STT Wiworotomo Purwokerto, dengan tingkat risiko 2 high risk, 3 medium risk dan 7 low risk. Pada akhir penelitian, dapat disimpulkan bahwa website Elearning STT Wiworotomo Purwokerto terindikasi memiliki celah pada Absence of Anti-CSRF Tokens karena website belum diterapkan token Anti CSRF sehingga permintaan pemalsuan lintas situs dapat dilakukan dan tidak terverifikasi namun website memiliki tingkat keamanan yang tinggi karena hanya ada satu pengujian yang berhasil. Hal ini terjadi karena website telah menerapkan penggunaan Moodle Session yang dapat dilindungi lebih lanjut dengan menggunakan Web Application Firewalls (WAF) dan aktivasi fitur Content Security Policy (CSP) sebagai langkah keamanan. Meskipun website telah memiliki keamanan yang kuat, pengembang harus melakukan cek keamanan secara teratur untuk memastikan website aman dari serangan ataupun kerentanan yang mungkin akan terjadi.

Kata kunci: Website, keamanan, PTES

ABSTRACT

STT Wiworotomo Purwokerto provides an online learning system or e-learning based on a website. Websites that do not have adequate security will become targets for cyber attackers. The objective of this research is to analyze vulnerabilities using the Penetration Testing Execution Standard (PTES) method, following the stages of Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, and Reporting. The research results, obtained using the OWASP ZAP scanning tool, identified 12 vulnerabilities on the STT Wiworotomo Purwokerto e-learning website, categorized into 2 high-risk, 3 medium-risk, and 7 low-risk vulnerabilities. At the end of the research, it was concluded that the website is vulnerable to the Absence of Anti-CSRF Tokens, as it has not implemented Anti-CSRF tokens, allowing cross-site request forgery (CSRF) attacks to occur without verification. However, the website maintains a high level of security, as only one test was successful in breaching it. This is due to the implementation of Moodle sessions, which can be further secured by using Web Application Firewalls (WAF) and activating the Content Security Policy (CSP) feature as additional security measures. Although the website already has strong security, developers should conduct regular security checks to ensure it remains protected from potential attacks and vulnerabilities.

Keywords: Website, security, PTES