

INTISARI

Keamanan adalah hal yang penting dan harus diperhatikan dalam mengelola atau membuat sebuah web. Di tengah kemajuan teknologi saat ini, hampir semua lembaga pendidikan di Indonesia menggunakan website sebagai sarana informasi yang memudahkan orang untuk menemukan informasi yang berkaitan dengan lembaga tersebut. Oleh karena itu, diperlukan langkah-langkah untuk menjaga keamanan website tersebut, metode pengujian yang dirancang dari sudut pandang penyerang untuk memastikan bahwa kondisi pengujian serealistis mungkin, salah satunya adalah melakukan penetration testing. Penetration testing ini bertujuan untuk mendeteksi kerentanan dan menguji keamanan pada aplikasi website SMK Muhammadiyah 1 Ajibarang menggunakan framework OWASP (Open Web Application Security Project). Pentingnya mengidentifikasi tingkat risiko dan mencegah serangan cybercrime yang dapat merugikan. Dalam transisi komunikasi dari tradisional ke aplikasi berbasis website, potensi serangan dunia maya meningkat, sehingga deteksi kerentanan keamanan menjadi sangat penting. Metode penelitian yang digunakan sebagai parameter keamanan website adalah OWASP Top-10 2021. Data dikumpulkan melalui observasi, wawancara, studi pustaka dan dilanjutkan proses scanning dan exploitation website menggunakan tools OWASP ZAP, Nslookup, Whois Subfinder, Nmap, WhatWeb dan BurpSuite. Hasil penelitian ini dapat diketahui bahwa website smkmuh1ajb.sch.id memiliki 12 kerentanan dengan 3 kerentanan dengan tingkat risiko medium, 6 kerentanan dengan tingkat risiko low, dan 3 kerentanan dengan tingkat risiko informational. Keamanan sistem pada website telah memenuhi prinsip keamanan CIA TRIAD, Walaupun beberapa keberhasilan eksploitasi celah keamanan yang ada dan didapatkan informasi penting namun informasi tersebut tidak terlalu sensitif.

Kata Kunci: Kerentanan, OWASP, Website, Penetration testing.

ABSTRACT

Security is crucial and must be considered when managing or creating a website. In today's technological advancement, almost all educational institutions in Indonesia use websites as an information medium that makes it easier for people to find information related to the institution. Therefore, steps are needed to ensure the security of these websites, including testing methods designed from an attacker's perspective to ensure that testing conditions are as realistic as possible. One such method is penetration testing. The aim of this penetration testing is to detect vulnerabilities and test the security of the SMK Muhammadiyah 1 Ajibarang website application using the OWASP (Open Web Application Security Project) framework. Identifying risk levels and preventing cybercrime attacks that can cause harm is crucial. As communication transitions from traditional to web-based applications, the potential for cyber-attacks increases, making vulnerability detection vital. The research method used to evaluate website security is the OWASP Top-10 2021. Data were collected through observation, interviews, literature review, and continued with the scanning and exploitation process of the website using tools such as OWASP ZAP, Nslookup, Whois, Subfinder, Nmap, WhatWeb, and BurpSuite. The research results indicate that the website smkmuh1ajb.sch.id has 12 vulnerabilities, with 3 medium-risk vulnerabilities, 6 low-risk vulnerabilities, and 3 informational risk vulnerabilities. The system security of the website has met the principles of the CIA Triad, although some security flaws were successfully exploited, yielding important information that was not overly sensitive.

Keywords: Vulnerability, OWASP, Website, Penetration testing.