

ABSTRAK

Perkembangan teknologi informasi mendorong perguruan tinggi memanfaatkan *Learning Management System* (LMS) sebagai media pendukung pembelajaran daring. Universitas Muhammadiyah Purwokerto menggunakan *Website ON&CLASS* sebagai pusat aktivitas akademik, sehingga keamanan sistem perlu dievaluasi untuk melindungi data dan menjaga keberlangsungan layanan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada *Website ON&CLASS UMP* menggunakan pendekatan *penetration testing* berbasis *Information System Security Assessment Framework* (ISSAF). Metode pengumpulan data dilakukan melalui observasi, wawancara, dan studi pustaka. Tahapan pengujian mengikuti *framework* ISSAF yang meliputi *planning and preparation, assessment, serta reporting, clean up and destroy artifacts*. Alat bantu yang digunakan antara lain *PING, Whois, Dnsrecon, DNSDumpster, WhatWeb, Wappalyzer, Nmap, OWASP ZAP, SQLmap, Burp Suite Community Edition, Metasploit, dan Shred*. Hasil penelitian menunjukkan bahwa *Website ON&CLASS UMP* berada di belakang layanan *Cloudflare* dan belum menerapkan *DNSSEC*. Hasil pemindaian juga menemukan beberapa kelemahan konfigurasi keamanan, seperti *Content Security Policy* yang belum optimal, *Strict-Transport-Security Header Not Set, Missing Anti-clickjacking Header*, serta beberapa *alert* dengan tingkat risiko *medium, low, dan informational*. Pengujian *Reflected XSS, SQL Injection, brute-force, dan Remote Code Execution* tidak berhasil memperoleh akses ke sistem. Dengan demikian, risiko utama *Website ON&CLASS UMP* berada pada aspek konfigurasi keamanan web. Rekomendasi perbaikan meliputi penerapan *DNSSEC, konfigurasi security header, optimalisasi CSP, pembaruan komponen sistem, serta evaluasi keamanan secara berkala*.

Kata kunci: *Penetration Testing, ISSAF, Keamanan Website, LMS, ON&CLASS UMP*.

ABSTRACT

The development of information technology encourages higher education institutions to use Learning Management Systems (LMS) as supporting media for online learning. Universitas Muhammadiyah Purwokerto uses the ON&CLASS website as the center of academic activities; therefore, system security needs to be evaluated to protect data and maintain service continuity. This study aims to identify and analyze security vulnerabilities in the ON&CLASS UMP website using a penetration testing approach based on the Information System Security Assessment Framework (ISSAF). Data were collected through observation, interviews, and literature study. The testing stages followed the ISSAF framework, consisting of planning and preparation, assessment, and reporting, clean up and destroy artifacts. The tools used in this research included PING, Whois, Dnsrecon, DNSDumpster, WhatWeb, Wappalyzer, Nmap, OWASP ZAP, SQLmap, Burp Suite Community Edition, Metasploit, and Shred. The results show that the ON&CLASS UMP website is protected by Cloudflare services and has not implemented DNSSEC. The scanning process also identified several security configuration weaknesses, such as suboptimal Content Security Policy, Strict-Transport-Security Header Not Set, Missing Anti-clickjacking Header, and several alerts with medium, low, and informational risk levels. Reflected XSS, SQL Injection, brute-force, and Remote Code Execution testing did not successfully gain access to the system. Therefore, the main security risks of the ON&CLASS UMP website are found in web security configuration aspects. Recommended improvements include implementing DNSSEC, configuring security headers, optimizing CSP, updating system components, and conducting periodic security evaluations.

Keywords: Penetration Testing, ISSAF, Website Security, LMS, ON&CLASS UMP.