ABSTRACT

This study aims to analyze the security level of the Telkom University Faculty of Industrial Engineering practicum website using the Vulnerability Assessment and Penetration Testing (VAPT) approach. This method consists of the stages of information gathering, vulnerability detection, penetration testing, and remediation. The testing was conducted using several security tools, such as NMAP for information gathering. Meanwhile, Nessus, OWASP ZAP, and Nikto were used for vulnerability detection. The testing results revealed four vulnerabilities identified by Nessus, nine by Nikto, and none by OWASP ZAP. The most critical vulnerabilities included an XSRF-TOKEN cookie without HttpOnly, which could lead to data manipulation, and the absence of Strict-Transport-Security, which could enable man-in-the-middle (MITM) attacks and SSL stripping. Mitigation recommendations were then implemented to close these gaps by adding HttpOnly to the XSRF-TOKEN cookie and adding the Strict-Transport Security header, followed by retesting to evaluate the effectiveness of the fixes. After retesting, there were still four vulnerabilities that had not been closed and eight vulnerabilities that had been successfully closed. The vulnerabilities that could not be closed will be recommended to developers for further configuration improvements at the code level. This research produces recommendations for enhancing system security that can serve as a reference for managing the security of academic and institutional websites.

Keywords: Security, Web, VAPT, Vulnerability Assessment, Penetration Testing, Mitigation.