ABSTRACT

Web applications have increasingly become prime targets for cyberattacks as businesses and organizations grow more dependent on online services in the digital era. Vulnerabilities such as SQL injection, cross-site scripting (XSS), and authentication weaknesses can be exploited by attackers to gain unauthorized access and compromise data integrity. The web application owned by School X experienced a cyberattack that affected its services, prompting the need for a penetration test on the website. This test aims to identify and understand the vulnerabilities present in School X's web application using a black-box testing approach. The assessment was conducted based on the security principles outlined by the Open Web Application Security Project (OWASP) 2021, serving as the foundation for both testing and mitigation. The testing process was carried out in a manner that did not disrupt the overall operation of the website, ensuring that users could continue accessing services without interruption. Furthermore, the confidentiality of school data and other sensitive information was maintained throughout the process. Based on the findings, several vulnerabilities were identified, including the use of outdated JavaScript libraries, absence of security headers such as Content-Security-Policy and X-Frame-Options, susceptibility to brute force attacks due to the lack of login rate limiting mechanisms, and exposure of sensitive information such as administrator email addresses displayed openly. These issues can be addressed through mitigation steps aligned with OWASP recommendations.

***Keywords**: penetration testing, web application, mitigation, OWASP.*