ABSTRACT

The advancement of digital technology has encouraged various institutions, including educational institutions, to utilize web-based applications to improve operational efficiency. However, cybersecurity threats have become a significant challenge, especially for applications that handle sensitive data, such as the Student Enrollment and Education Data System (S.E.E.D.S) at Telkom University. With approximately 12.7 million data breaches reported in Indonesia in 2022 and the high number of cyberattacks targeting web-based applications, the need for security testing has become increasingly critical. This study aims to analyze the security of the S.E.E.D.S application using the OWASP Top 10 methodology, which is an international standard for identifying critical threats in web applications. The research methodology includes vulnerability identification, the creation of security testing scenarios, and the execution of tests based on the OWASP Top 10. The study focuses on simulating attacks that represent real-world threats to the application. After thorough testing of the S.E.E.D.S application based on OWASP documentation, the application was found to be vulnerable, with issues identified in 7 out of the 10 OWASP categories. Therefore, the S.E.E.D.S application can be considered vulnerable, as even minor vulnerabilities can significantly impact application security and potentially damage the credibility and reputation of the institution.

Keywords: *web application, security, OWASP*