ABSTRACT

The development of information technology has changed the way organizations operate and communicate. One important implementation of information technology is a web-based application information system. At the company PT. XYZ (Abc), information systems have been implemented to provide services to customers. Cyber attacks such as data leaks or access to website services can harm the company and can also disrupt operational activities. In addition, poor cyber security or frequent attacks can damage the company's reputation. This research aims to analyze the security of the Abc website information system at PT. XYZ by penetration testing using the Open Web Application Security Project (OWASP) Top-10 2021 method. This method helps identify potential security vulnerabilities on the website. From the testing and analysis process that has been carried out, the results of the 10 lists of vulnerabilities owned by OWASP Top 10 researchers get 4 lists of vulnerabilities that were successfully found, namely insecure design with a medium scale (Insecure Design (medium)), vulnerable and outdated components with a medium scale (Vulnerable and Outdated Components (Medium)), software and data integrity failures with a high scale (Software and Data Integrity Failures (High), and security logging and monitoring failures with a medium scale Security Logging and Monitoring Failures (Medium)).

Keywords: Information System Security, Penetration testing, OWASP TOP 10, Website.