Abstract

In the era of rapid technological development, health services, especially hospitals, are asked to provide more efficient services by utilizing information technology. There is a need for technology implementation to facilitate services, namely with a patient registration system that has a positive impact but is also vulnerable to security threats. This study will focus on conducting vulnerability assessments by identifying risks, implementing security controls, finding security problems, responding to results, and reporting using OWASP. The research method is carried out from the footprinting stage, vulnerability scanning, to penetration testing to find results that can be analyzed. The results of the study showed that SIMPONI had 26 medium risks and 2643 low risks, with a total of 2669 vulnerabilities found. Penetration testing showed vulnerabilities that were successfully exploited, such as wildcard directives, style-src unsafe-inline, and sensitive information leaks. The use of a Content Security Policy (CSP), cookie security, input validation implementation, and activation of HSTS are recommendations for improvement based on the analysis of the results found. This study concludes that the SIMPONI system still has many security holes that must be fixed immediately to improve security. The use of more sophisticated pen-testing tools and better methods to increase the accuracy and effectiveness of vulnerability detection should be suggested for future research.

Keyword : vulnerability assessment, OWASP, patient registration system, security system, early detection, penetration