ABSTRACT

Based on the 2023 BSSN Indonesian Cyber Security LANSKAP report, the sector that often experiences cyber attacks occurs in the government administration sector. The website of the Sidoarjo Regency Cooperative and Micro Business Service is a service that provides information to support the economic welfare of the Sidoarjo community regarding cooperative capital loans and MSME actors. The website has experienced vulnerabilities through SQL Injection attacks to obtain databases that are still active. Therefore, the Service requires strong security measures to protect all information and prevent potential other cyber attacks by conducting tests using the penetration testing method with the OWASP Top 10 - 2017 approach. This test was carried out on three websites and the test results from the three websites had a total of forty-two vulnerabilities with a risk of 4 high vulnerabilities, 17 medium vulnerabilities, and 21 low vulnerabilities. The measurement of vulnerability risk priorities is based on the OWASP Risk Rating Methodology, with the highest risk vulnerabilities being SQL Injection - MySQL, Cross-Site Scripting (XSS), and Weak Password Change or Reset Functionalities. One of the high vulnerabilities is successfully getting the database so that at some point the website can be exploited or manipulated by the attacker. The recommendation suggested to the organization is to immediately fix the vulnerabilities that have been found and replace the components to the latest version.

Keywords— penetration testing, website, OWASP Top 10, OWASP Risk Rating Methodology, information system security