

WEBSITE INFORMATION SECURITY ANALYSIS USING THE VULNERABILITY ASSESSMENT METHOD

Name : Fitriatul Hikmayani
NIM : 6404201026
Supervisor 1 : Kasmawi, M.Kom.
Supervisor 2 : Nurmi Hidayasari, ST., M.Kom.

ABSTRACT

Information security on websites is an important aspect in protecting the system, facing potential attacks that can cause damage, data theft and disruption of website functionality. As a marketplace for UMKM, the information security of the Soodu.id website is key in protecting the data and business integrity of UMKM. This research aims to conduct information security analysis on websites using the vulnerability assessment (VA) method. This method involves a process of defining, identifying and classifying the vulnerabilities of a system. VA can identify vulnerabilities on websites and provide recommended solutions to reduce the risk of attacks. The results of this research show that the Vulnerability Assessment process for the soodu.id website contained 18 vulnerabilities from the OWASP ZAP results and 1 vulnerability from the Openvas results. Findings based on the parameters used in OWASP ZAP involve vulnerabilities to Injection, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, and Using Components with Known Vulnerabilities. Serious security threats were identified in Sensitive Data Exposure with high levels and several low levels. Based on information security aspects (CIA Triad), the identified vulnerabilities have the potential to jeopardize the confidentiality of information through vulnerabilities like PII Disclosure and Application Error Disclosure. They also threaten data integrity from vulnerabilities such as Cross-Site Scripting (XSS) and impact information availability through potential attacks like CSRF and Clickjacking, which can disrupt services.

Keywords: *Information security, website, Vulnerability Assessment, OWASP ZAP, OpenVAS*