ABSTRACT

WEBSITE OF SUB-DISTRICT XYZ BANDUNG REGENCY SECURITY ANALYSIS USING STANDARD PENETRATION TESTING WITH INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) *METHODOLOGY*

A website is a collection of pages that are used to display various types of information. Oftentimes websites get security attacks from irresponsible parties. Based on the data obtained from Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) *is the types of attacks that are often carried out are trojan-activity, information gathering, and web application attacks. This can be experienced on the website xyz.xyz.go.id belonging to the local government X. This can also be experienced on the xyz.xyz.go.id website belonging to the regional government X. Because the government website is vulnerable to these threats, it is necessary to scan the website for vulnerability to provide security recommendations. The test was carried out using the Information System Security Assessment Framework (ISSAF) methodology using the BlackBox method and using the ZAP, Nikto, Zenmap, and Netcraft tools. The vulnerability obtained is the basis for making recommendations. The test results with Zenmap and Netcraft resulted in information gathering. Security vulnerability testing with ZAP found six low levels, three medium levels, and three informational levels. The test results with Nikto resulted in five security vulnerabilities. After scanning for vulnerability on the X local government website, several vulnerabilities have been obtained that have different levels of risk. After analyzing the security gaps, verification of several vulnerabilities is carried out by verifying the gaps found, namely anti-clickjacking X-Frame-Options and Application Error Disclosure.*

Keywords: Vulnerability, Website, Black Box Testing, Vulnerability Assessment, ZAP, Nikto.