ABSTRACT

To reduce the number of traffic accidents on the road, it is necessary to have positive behaviour from all drivers, namely compliance with driving regulations and traffic signs. In the current technological era, a website specifically designed to conduct surveillance using electronic means so that violators will get evidence of violations electronically called e-tickets, which is digitizing tickets. One of the websites specifically designed to monitor violations electronically is the XYZ website, which is the research target, namely vulnerability analysis and security testing using the NIST 800-115 standard. The problems raised in this study are related to the security of a website, which focuses on the security of the XYZ website, to know the results of the vulnerability assessment on the XYZ website, obtaining results and analyzing the loopholes on the XYZ website, as well as conducting penetration testing on the XYZ website with a high level of vulnerability. (high level). The benefits of research for website owners can be used to find out existing loopholes as a reference for improving security. Researchers can increase knowledge about vulnerability assessment and penetration testing as a reference for doing so on other websites to improve website security. While the benefits for future research can be used as a starting material. The tests carried out in this study use the black box method using the NIST 800-115 standard by going through 4 main stages, namely planning, discovery, attack, and reporting. Vulnerability analysis was carried out using several tools such as Nmap, OWASP ZAP, Burp Suite and foxyproxy. At the attacking stage, this research uses SQL Injection testing after obtaining vulnerability information at the discovery stage. From this vulnerability analysis, it was found that on the XYZ website, there are 7 vulnerability gaps with different levels. In testing the vulnerability to high-level vulnerabilities (SQL Injection), 198 combinations of code injection were used. From the study's overall results, it can be concluded that based on the vulnerability analysis results, there were 7 vulnerability gaps on the XYZ website with 3 levels, namely high, medium, and low. In the high-level vulnerability testing stage (SQL Injection), 2 information was obtained, namely information about the database contents and information about the XYZ website directory. Suggestions can be given for further research so that the results of this study can be used as a starting material and to use more diverse tools to get more information about the website under investigation.

***Keywords**: Information System, Academic, Telkom, Vulnerability, and NIST 800-115.*