## *ABSTRACT*

*On the server machine where a website is hosted, generally, there is sensitive or confidential data that the general public cannot read. It is necessary to protect the data so that other computers cannot see it. The solution is to apply a Vulnerability Assessment with the Vulnerability Scan method to assess whether the security is guaranteed. This research was conducted in the range of June–July 2022 to test the vulnerability of the IT Telkom Purwokerto repository web server. The research factor is based on the scan results of the system used, what type of personal information is stored in the system, how simple the attack is, and how much damage can occur if the vulnerability is exploited effectively. In detecting vulnerabilities in this study, a quantitative research methodology was used using the Kali Linux Operating System, Zenmap, and Nessus Scanner software, which started from a literature study, footprinting, vulnerability scanning, analysis, recommendations, and reporting (documentation). The results obtained from the Port Scanning test revealed several open and closed ports on the IT Telkom Purwokerto repository server, including port 80 HTTP/WEB, port 445 HTTPS, and port 9595 PDS. Testing on Zenmap found that the checked target host supported the POST, OPTIONS, GET, and HEAD protocols. Target found as HTTP filtered proxy. No cross-site scripting was detected. On the target host, SQL injection was found. Testing using Nessus tools obtained four categories of target IP vulnerabilities for IT Telkom Purwokerto Repository in the form of 15 vulnerabilities for info, 3 for medium, 1 for high, and 1 for critical.*



***Keywords:*** *Website, Kali Linux, Website Security, Vulnerability Assessment*