ABSTRACT

Information security is a critical aspect that must be maintained, especially in systems that store sensitive data. Information security is one of the top priorities for companies. If website owners neglect security, hackers can exploit vulnerabilities for their own gain and compromise information. Some examples of hacker activities include viruses, credit card theft, bank account theft, and email/web server password theft.This research evaluates the security of the website Xyz.id, an online donation platform under the management of Yayasan Dana Sosial (PT. XYZ), which handles important data such as user information, financial reports, and donation transaction histories. The evaluation follows the ISSAF (Information Systems Security Assessment Framework) methodology, consisting of 9 systematic penetration testing phases.Through the Information Gathering and Network Mapping stages, the study identified that the website's infrastructure is managed by DigitalOcean, LLC with the IP address 1xx.2xx.5x.2xx. Vulnerability testing using tools such as Nessus and OWASP ZAP revealed several critical threats, including DNS Server Spoofed Request Amplification DdoS and Cache Poisoning, as well as potential cloud metadata leakage due to server misconfiguration.However, further penetration testing using various tools such as sqlmap, Hydra, and Metasploit demonstrated that the site's security system is well-designed to withstand common attacks. Security mechanisms such as login attempt restrictions, input sanitization, and secure cookie management have proven effective.To further enhance security, it is recommended to perform software updates, server configuration improvements, and implement a Web Application Firewall (WAF) and Intrusion Detection System (IDS). The results of this research provide concrete recommendations to PT. XYZ to strengthen the security of the Xyz.id platform in protecting users' sensitive data and donation transactions.

Keywords: website, Penetration Testing, ISSAF Framework