ABSTRACT

This research examines security vulnerabilities in WordPress, a very popular Content Management System (CMS) that is often the target of cyberattacks. The main objectives of this research are to identify vulnerabilities in WordPress.org version 6.4.3, design security controls based on the OWASP Top Ten standards, and prioritize effective security measures based on the severity of the vulnerabilities. Through experimental and simulation approaches, five major vulnerabilities were identified. First, the Broken Access Control category revealed exploits in PHP 8.1.0-dev and Apache 2.4.49 with a vulnerability level of "High" and a threat of "Alteration", which can be addressed using a Web Application Firewall (WAF) and directory access restrictions. Second, the SQL Injection vulnerability in the Injection category is identified as "Critical" with the threat of "Disclosure", which is addressed through the implementation of parameterized queries. Third, in the Insecure Design category, a Path Traversal exploit was found with a vulnerability level of "Medium" which can be resolved using security plugins such as Wordfence. Fourth, vulnerabilities in the Social Warfare Plugin in the Vulnerable and Outdated Components category were addressed through regular updates and the use of WAF. Security priorities are focused on "Critical" vulnerabilities to reduce the risk of exploitation. This research emphasizes the importance of implementing security controls in accordance with the OWASP Top Ten standards to reduce risk in WordPress.org version 6.4.3, especially against vulnerabilities with high risk levels.

Keywords— ***WordPress, security, vulnerability, exploit, OWASP***