ABSTRACT

The CMS WordPress service is very popular worldwide, making security management on this platform extremely important. This research aims to design application security controls for CMS WordPress, based on the experimentation of vulnerabilities in both plugins and non-plugin functions. The stages of exploitation are used to develop the security control design. The exploited vulnerabilities include the MStore-API plugin, Modern Event Calendar Lite, WPS-Hide-Login, Elementor, and Catch Themes Demo Import. Additionally, the testing also includes the exploitation of XXE vulnerabilities and Brute Force attacks. The analysis results in a WordPress application security control design formulated based on threat and vulnerability analysis. This threat analysis includes threats to data and the OWASP Top 10 standards, where the seven identified vulnerabilities fall into four OWASP Top 10 categories. Of these seven vulnerabilities, five are classified under the disclosure category and two under the alteration category. Each vulnerability is assigned a CVE ID and evaluated using the CVSS system. For example, CVE-2023-2732 in the MStore-API Plugin has the highest score of 9.8 (Critical), while CVE-2021-29447 (XXE) has the lowest score of 6.5 (Medium). The security control design based on the OWASP Top 10 categories helps prioritize the implementation of security mechanisms. For example, in the Identification and Authentication Failures (A07:2021) category, the MStore-API Plugin is classified as critical with a disclosure threat, making security measures like installing the Wordfence plugin a priority. Meanwhile, mitigations for Brute Force attacks with a medium severity level, such as changing the login URL and enabling 2FA, should be implemented after addressing critical vulnerabilities.

Keywords - **Wordpress, *security control design, exploitation, vulnerabilities, plugins***