ABSTRAK

Layanan CMS WordPress sangat populer di seluruh dunia, sehingga penanganan keamanan pada *platform* ini menjadi sangat penting. Penelitian ini bertujuan untuk merancang kontrol keamanan aplikasi pada CMS WordPress, yang didasarkan pada percobaan eksploitasi kerentanan pada *plugin* dan *non-plugin* (fungsi lainnya). Tahapan eksploitasi ini digunakan untuk menyusun desain kontrol keamanan. Kerentanan yang dieksploitasi mencakup *plugin* MStore-API, Modern Event Calendar Lite, WPS-Hide-Login, Elementor, dan Catch Themes Demo Import. Selain itu, pengujian juga mencakup eksploitasi kerentanan XXE dan serangan *Brute Force*.Analisis yang dilakukan menghasilkan desain kontrol keamanan aplikasi WordPress yang dirumuskan berdasarkan analisis ancaman dan kerentanan. Analisis ancaman ini mencakup ancaman terhadap data serta standar OWASP Top 10, di mana tujuh kerentanan yang diidentifikasi masuk ke dalam empat kategori OWASP Top 10. Dari ketujuh kerentanan tersebut, lima diklasifikasikan dalam kategori *disclosure* dan dua dalam kategori *alteration*. Setiap kerentanan diberikan CVE ID dan dinilai menggunakan sistem CVSS. seperti, CVE-2023-2732 pada *Plugin* MStore-API memiliki skor tertinggi yaitu 9.8 (*Critical*), sedangkan CVE-2021-29447 (XXE) memiliki skor terendah dengan nilai 6.5 (*Medium*). Desain kontrol keamanan yang didasarkan pada kategori OWASP Top 10 membantu menentukan prioritas dalam implementasi mekanisme keamanan. Misalnya, pada kategori *Identification and Authentication Failures* (A07:2021), MStore-API *Plugin* diklasifikasikan sebagai *critical* dengan ancaman *disclosure*, sehingga mekanisme keamanan seperti pemasangan *plugin* Wordfence harus menjadi prioritas. Sementara itu, mitigasi untuk serangan *Brute Force* dengan tingkat *medium*, seperti mengganti *URL login* dan mengaktifkan 2FA, sebaiknya dilakukan setelah menangani kerentanan *critical.*

Kata kunci **– Wordpress, desain kontrol keamanan, eksploitasi, kerentanan, *plugin,***