ABSTRAK

Penelitian ini mengkaji kerentanan keamanan pada WordPress, sebuah *Content Management System* (CMS) yang sangat populer namun sering menjadi target serangan siber. Tujuan utama penelitian ini adalah untuk mengidentifikasi kerentanan pada WordPress.org versi 6.4.3, merancang kontrol keamanan berdasarkan standar OWASP *Top Ten*, serta menentukan prioritas pengamanan yang efektif berdasarkan tingkat keparahan kerentanan. Melalui pendekatan eksperimental dan simulasi, lima kerentanan utama berhasil diidentifikasi. Pertama, kategori *Broken Access Control* mengungkapkan eksploitasi pada PHP 8.1.0-dev dan Apache 2.4.49 dengan tingkat kerentanan "*High*" dan ancaman "*Alteration*", yang dapat diatasi menggunakan *Web Application Firewall* (WAF) dan pembatasan akses direktori. Kedua, kerentanan SQL *Injection* dalam kategori *Injection* teridentifikasi sebagai "*Critical*" dengan ancaman "*Disclosure*", yang diatasi melalui penerapan *parameterized queries*. Ketiga, dalam kategori *Insecure Design*, eksploitasi *Path Traversal* ditemukan dengan tingkat kerentanan "*Medium*" yang dapat diatasi menggunakan *plugin* keamanan seperti Wordfence. Keempat, kerentanan pada *Plugin Social Warfare* dalam kategori *Vulnerable and Outdated Components* diatasi melalui pembaruan rutin dan penggunaan WAF. Prioritas pengamanan difokuskan pada kerentanan "*Critical*" untuk mengurangi risiko eksploitasi. Penelitian ini menekankan pentingnya penerapan kontrol keamanan yang sesuai dengan standar OWASP *Top Ten* guna mengurangi risiko pada WordPress.org versi 6.4.3, khususnya terhadap kerentanan dengan tingkat risiko tinggi.

Kata kunci — **WordPress, keamanan, kerentanan, eksploitasi, OWASP**