ABSTRAK

WordPress adalah *Content Management System* (CMS) yang paling populer di dunia untuk membuat dan mengelola situs web atau *blog*. Dengan populernya CMS ini, membuat WordPress juga menjadi target serangan para *hacker* untuk menemukan celah keamanan dan melancarkan eksploitasi yang tentunya berdampak kepada pengguna WordPress. Penelitian ini bertujuan untuk mendesain sebuah prioritas kontrol keamanan pada WordPress dari eksploitasi-eksploitasi yang diujikan, terutama yang berhubungan dengan jaringan. Eksploitasi yang dilakukan yaitu eksploitasi terhadap XML-RPC dengan *Brute Force*, DDoS, *Packet Sniffing*, *Packet Data Manipulation*, dan *Session Hijacking* dengan target utama eksploitasi yaitu WordPress. Hasil dari eksploitasi akan dianalisis menggunakan pendekatan ancaman terhadap keamanan data yang terdiri dari *Disclosure, Alteration*, dan *Denial* serta berdasarkan OWASP *Top Ten* yang dikeluarkan oleh OWASP. Kemudian, masing-masing eksploitasi akan dievaluasi tingkat keparahan kerentanannya berdasarkan kategori yang didapat dari skor CVSS serta merekomendasikan mekanisme keamanannya. Hasil dari penelitian ini berupa desain kontrol keamanan berdasarkan standar OWASP untuk prioritas mitigasi terhadap kerentanan yang dieksploitasi oleh ancaman di CMS WordPress dengan urutan prioritas pertamanya yaitu eksploitasi *Packet Sniffing* yang termasuk ke dalam kategori *Cryptographic Failures* dengan tingkat keparahan di level *High*, tipe ancamannya berupa *Disclosure* dan mekanisme keamanan yang diterapkan dapat berupa penggunaan sertifikat SSL/TLS pada *server* WordPress, *Force* HTTPS, dan HTTP *Strict Transport Security* (HSTS). Sedangkan, pada urutan terakhir diisi oleh eksploitasi DDoS yang tercakup dalam kategori *Security Logging and Monitoring Failures* dengan tingkat keparahan di level *High*, ancamannya bertipe *Denial* dan mekanisme keamanan yang bisa diterapkan berupa penggunaan *Web Application Firewall* (WAF) serta memasang *plugin* keamanan di WordPress. Kelanjutan penelitian ini dapat berupa penambahan variasi jenis eksploitasi atau analisis lebih lanjut terhadap sumber daya yang digunakan selama proses eksploitasi.

Kata kunci: Desain Kontrol, Eksploitasi, WordPress, Jaringan