BAB I PENDAHULUAN

I.1 Latar Belakang

Tidak bisa dipungkiri, keamanan adalah salah satu hal yang penting dan sering dibahas ketika berbicara mengenai teknologi di masa sekarang ini. Teknologi memainkan peranan penting di semua lini kehidupan, mulai dari penggunaan pribadi hingga organisasi berskala dunia. Keamanan menjadi aspek penting untuk melindungi data, sistem, layanan, dan semua jenis produk digital dari berbagai risiko yang mengancam. Salah satu bentuk produk digital tersebut adalah *Content Management System* atau biasa disingkat dengan CMS.

CMS adalah sistem yang memungkinkan pengguna untuk dapat membuat, mengelola, dan menyimpan konten digital seperti teks, gambar, video, dan audio tanpa harus memiliki pengetahuan teknis yang mendalam tentang pemrograman web. Banyak keuntungan yang bisa didapatkan ketika menggunakan CMS di antaranya mudah digunakan, memiliki banyak fitur tambahan yang bisa digunakan secara gratis, dan dapat digunakan untuk berbagai kebutuhan. Salah satu CMS yang paling populer dan banyak digunakan di dunia adalah WordPress.

WordPress adalah sebuah *Content Management System* (CMS) untuk membuat dan mengelola *website* atau *blog*. WordPress dibangun menggunakan bahasa pemrograman PHP dan basis data MySQL. WordPress digunakan hingga 43.4% situs yang ada di dunia pada tahun 2024. WordPress disukai oleh banyak pengguna karena WordPress memiliki tampilan antarmuka platform yang *user-friendly*, memiliki hingga 60 ribu *plugin* gratis yang bisa digunakan, 12 ribu tema gratis, dan yang terpenting WordPress bersifat *open-source* yang artinya WordPress bisa digunakan, dimodifikasi, dan disebarkan tanpa perlu khawatir mengenai pelanggaran hak cipta (Mauladhika, 2024).

Namun, bukan berarti WordPress tidak memiliki kekurangan. Sebagai salah satu CMS paling populer di dunia, WordPress menjadi sasaran serangan siber oleh para *hacker* untuk menemukan celah dan melancarkan peretasan yang bisa berdampak signifikan untuk penggunanya. Sebagian besar kerentanan disebabkan oleh kerentanan pada *plugin*, sedangkan faktor lainnya seperti serangan-serangan yang

dapat dilakukan melalui jaringan atau internet, sehingga memungkinkan para *hacker* untuk memanfaatkan celah-celah tersebut.

Penelitian ini bertujuan untuk mengembangkan desain kontrol pada CMS untuk platform WordPress dengan meningkatkan keamanannya berdasarkan standar keamanan dunia seperti *Open Web Application Security Project* (OWASP). Desain kontrol yang diusulkan bertujuan untuk memberikan rekomendasi dan prioritas mekanisme keamanan ketika ingin menggunakan CMS WordPress, serta eksploitasi yang diujikan pada penelitian ini berfokus pada eksploitasi-eksploitasi yang berbasis pada aspek jaringannya.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah sebagai berikut:

1. Bagaimana merancang pengujian eksploitasi pada CMS WordPress di aspek jaringan?
2. Bagaimana menganalisis eksploitasi berdasarkan ancaman dan tingkat kerentanannya pada CMS WordPress?
3. Bagaimana mengelola kontrol untuk CMS WordPress dari eksploitasi pada aspek jaringan?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Merumuskan rancangan pengujian eksploitasi sampai implementasinya pada CMS WordPress.
2. Merumuskan tujuan dan target eksploitasi berdasarkan hasil analisis ancaman dan tingkat keparahan kerentanannya.
3. Merancang desain kontrol keamanan jaringan pada eksploitasi yang diujikan.

I.4 Batasan Penelitian

Adapun batasan penelitian ini adalah sebagai berikut:

1. Penelitian ini berdasarkan uji coba eksploitasi pada eksperimen dan simulasi di aspek jaringannya menggunakan WordPress versi 6.5.5 yang diunduh dari *website* wordpress.org.

2. Analisis dilakukan berdasarkan hasil pengujian eksperimen dengan mempertimbangkan aspek *Disclosure*, *Alteration*, dan *Denial* serta level keparahan dari *Common Vulnerabilities and Exposures* (CVE).
3. Desain kontrol yang dirancang didasarkan pada standar OWASP dan kategori tingkat keparahan eksploitasi serta mekanisme kontrol yang diberikan hanya berupa rekomendasi.

I.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari hasil penelitian ini adalah sebagai berikut:

1. Secara teoritis, penelitian ini diharapkan dapat berkontribusi pada pengembangan pengetahuan terutama mengenai eksploitasi dan prioritas kontrol pada CMS dari aspek jaringan.
2. Secara Praktis, penelitian ini diharapkan dapat menyediakan panduan tentang perancangan dan pengimplementasian desain kontrol yang efektif pada CMS dengan standar keamanan yang ada.