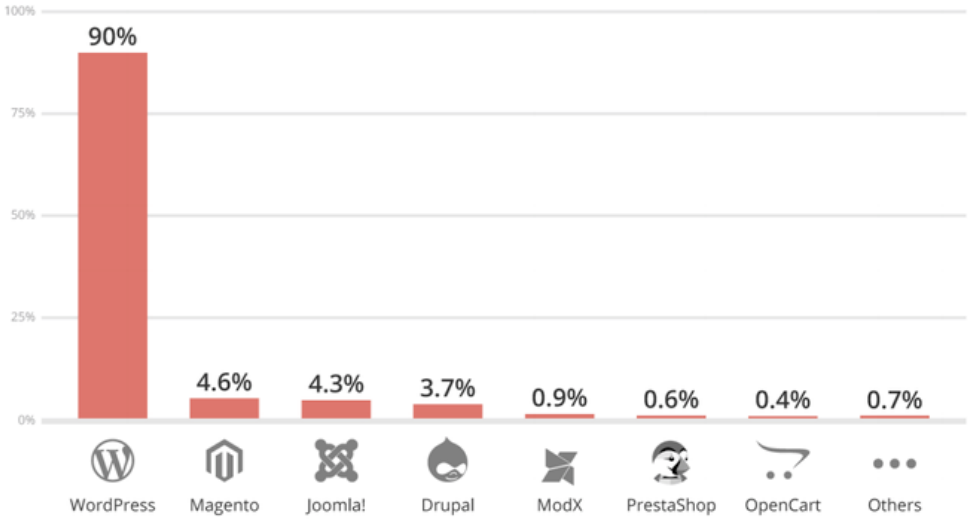
BAB I PENDAHULUAN

I.1 Latar Belakang

Kemajuan teknologi informasi telah memungkinkan informasi diakses, komunikasi dilakukan, dan berbagai tugas sehari-hari dijalankan dengan lebih mudah dalam transformasi dunia *modern*. Menurut Haag dan Keen (1996), teknologi informasi adalah seperangkat alat yang membantu dalam bekerja dengan informasi serta melakukan pemrosesan informasi. Namun, di balik kemajuan ini, terdapat potensi bahaya yang harus diwaspadai. Peretasan data, privasi yang terancam, dan ketergantungan yang berlebihan pada teknologi adalah beberapa masalah yang mendampingi perkembangan ini. Oleh karena itu, penting bagi risiko yang terkait dengan teknologi informasi untuk terus dipahami dan dikelola guna memastikan manfaatnya dapat dirasakan sambil meminimalkan dampak negatifnya.

Keamanan merupakan salah satu aspek krusial dalam pengelolaan sistem informasi, terutama dalam konteks *Content Management System* (CMS). CMS digunakan secara luas untuk mengelola konten di berbagai jenis situs web, mulai dari *blog* hingga situs web perusahaan besar. Namun, penggunaan CMS juga membawa risiko keamanan jika tidak diatur dengan baik. Oleh karena itu, pentingnya mekanisme keamanan CMS berdasarkan aspek sistem untuk mengatasi tantangan keamanan yang dihadapi oleh pengguna CMS.

WordPress merupakan salah satu *platform* CMS yang paling populer digunakan di seluruh dunia untuk membuat berbagai jenis situs *web*, mulai dari *blog* pribadi hingga situs *e-commerce* skala besar. Namun, popularitas WordPress juga menjadikannya sasaran utama bagi penyerang siber yang mencari celah keamanan.



Gambar I. 1 Laporan Peretasan dari GoDaddy

(Sumber: https://infokomputer.grid.id/)

Berdasarkan laporan yang diterima oleh penyedia *web hosting* terkenal asal Amerika Serikat yaitu GoDaddy, data menunjukkan bahwa terdapat 18.302 laporan peretasan yang terjadi pada klien GoDaddy sepanjang tahun 2018. Dari laporan tersebut, 90% diantaranya merupakan kasus peretasan pada WordPress. GoDaddy juga menemukan fakta menarik yaitu meskipun 63,3% situs WordPress yang diretas telah menggunakan versi terbaru, situs dengan CMS lain umumnya diretas karena menggunakan versi yang sudah usang. (Nugroho, 2019)

Penerapan desain kontrol merupakan langkah yang sangat penting untuk mengatasi berbagai risiko keamanan yang muncul pada *platform* CMS seperti WordPress. Desain kontrol merupakan pendekatan sistematis yang dirancang untuk mengidentifikasi, mencegah, dan memitigasi ancaman keamanan sebelum eksploitasi terjadi. Selain itu, desain kontrol yang efektif harus mengacu pada standar keamanan yang diakui secara global, seperti OWASP *Top Ten*, yang memberikan panduan tentang ancaman keamanan paling kritis dalam aplikasi *web*. Mengikuti standar ini membantu memastikan bahwa semua aspek keamanan, mulai dari pengelolaan akses hingga mitigasi kerentanan, diterapkan secara konsisten dan menyeluruh.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana cara mengidentifikasi dan mengevaluasi kerentanan pada sistem WordPress.org versi 6.4.3?
b. Bagaimana penyusunan desain kontrol untuk mengatasi kerentanan yang telah diidentifikasi pada sistem CMS WordPress.org versi 6.4.3?
c. Bagaimana mengelola langkah-langkah pengamanan berdasarkan kerentanan yang telah diidentifikasi pada sistem WordPress.org versi 6.4.3?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengidentifikasi dan mengevaluasi kerentanan pada sistem WordPress.org versi 6.4.3 yang dapat dieksploitasi melalui berbagai teknik serangan dan menggunakan berbagai *attack tools* seperti Gobuster versi 3.6, WPScan versi 3.8.25, Metasploit versi 6.4.2, serta Pyhton 3.
b. Menyusun desain kontrol keamanan yang sesuai dengan standar OWASP *Top Ten* untuk mengatasi kerentanan yang ditemukan pada aspek sistem CMS WordPress.org versi 6.4.3.
c. Menentukan urutan prioritas penerapan langkah-langkah pengamanan berdasarkan tingkat keparahan kerentanan yang telah diidentifikasi, guna meminimalkan risiko eksploitasi pada sistem WordPress.org versi 6.4.3.

I.4 Batasan Penelitian

Adapun batasan pada penelitian ini adalah sebagai berikut:

a. Penelitian ini tidak mengimplementasikan desain kontrol.
b. Analisis dilakukan berdasarkan hasil pengujian eksperimen pada sistem WordPress.org versi 6.4.3 dengan mempertimbangkan tingkat keparahan eksploitasi.
c. Penelitian ini menggunakan standar OWASP *Top* 10:2021 dan kategori tingkat keparahan untuk merancang desain kontrol serta mekanisme kontrol yang diberikan hanya berupa rekomendasi.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis, penelitian ini menyediakan panduan komprehensif dalam merancang dan menerapkan mekanisme keamanan untuk WordPress.
2. Secara praktis, penelitian ini dapat mengetahui mekanisme keamanan untuk WordPress dari aspek sistem.