BAB I PENDAHULUAN

I.1 Latar Belakang

Pengelolaan dan penyediaan konten digital menjadi kunci dalam berbagai aspek kehidupan, termasuk bisnis, pendidikan, hiburan, dan komunikasi. Mengelola konten digital bukan hal yang sederhana, inilah saatnya *Content Management System* (CMS) berperan penting dalam hal ini. Subariah *et al*. (2021) mendefinisikan CMS sebagai system yang dapat membuat, mengelola, dan menerbitkan konten *web* tanpa perlu *skill* pemrograman. Contoh CMS seperti WordPress menawarkan *user interface* yang mudah dipahami, membantu efisiensi dalam penciptaan dan pengelolaan halaman *web*.

WordPress adalah salah satu *Content Management System* yang sangat terkenal dan sering digunakan untuk membuat berbagai jenis situs *web*. WordPress merupakan CMS yang serbaguna, yang mampu digunakan untuk menciptakan beragam jenis situs *web*, seperti *blog*, situs *web* perusahaan, dan *platform e-commerce* (Heera, 2019). Namun, kepopuleran WordPress juga berarti bahwa platform ini menjadi sasaran potensial bagi para *hacker* yang mencari celah keamanan untuk melancarkan peretasan pada situs *web*.

Pada tahun 2023, sekitar 4,3% dari situs web WordPress mengalami peretasan, artinya hampir 1 dari 25 situs terpengaruh. Ini setara dengan sekitar 13.000 situs yang diserang setiap hari. Dalam setahun, diperkirakan sekitar 4,7 juta situs WordPress mengalami serangan peretasan. Sebagian besar kerentanan keamanan pada WordPress disebabkan oleh plugin dan tema. Pada tahun 2021, 99,42% dari semua kerentanan keamanan ditemukan pada tema dan *plugin*, dengan rincian 92,81% disebabkan oleh *plugin* dan 6,61% oleh tema (MoonThemes, 2023).

Kontrol adalah proses yang dirancang untuk untuk meningkatkan keamanan aplikasi dengan mengurangi potensi kerentanan. Dalam konteks ini, kontrol melibatkan identifikasi risiko, penilaian dampaknya, dan penerapan langkah-langkah untuk mengurangi kemungkinan terjadinya insiden keamanan atau dampaknya jika insiden tersebut terjadi. salah satu panduan yang dapat digunakan adalah *Open Web Application Security Project* (OWASP) yaitu merupakan

komunitas global yang fokus pada penanganan risiko dan pemahaman keamanan aplikasi *web*.

Keamanan situs *web* menjadi semakin penting. Desain kontrol keamanan pada WordPress memiliki dampak signifikan dalam meningkatkan aspek keamanan. Dengan pendekatan ini, pengguna WordPress dapat mengidentifikasi kebutuhan keamanan yang sesuai dengan tujuan bisnis, mengelola risiko yang terkait dengan situs *web*, dan menyesuaikan kontrol keamanan yang tepat. Melalui pengaturan kontrol yang relevan, seperti manajemen akses dan perlindungan terhadap eksploitasi, dapat menjaga dan meningkatkan tingkat keamanan situs WordPress sesuai dengan kebutuhan dan risiko yang dihadapi.

Dengan merancang desain kontrol keamanan yang baik, pengguna WordPress dapat memperkuat keamanan situs *web* mencakup peningkatan lapisan keamanan yang dapat mengurangi kerentanan dan meminimalkan risiko terjadinya peretasan. Melalui pendekatan ini, situs *web* menjadi lebih tangguh dan dapat memberikan perlindungan yang lebih efektif terhadap serangan siber yang beragam. Dengan demikian, tindakan perancangan desain keamanan dengan panduan OWASP menjadi salah satu langkah dalam menjaga keamanan WordPress.

I.2 Perumusan Masalah

Permasalahan yang mendasari penelitian ini dapat dirumuskan sebagai berikut :

1. Apa saja tipe eksploitasi kerentanan yang dapat ditemukan pada *plugin* dan fungsi lainnya (*non plugin*)?
2. Bagaimana menyusun desain kontrol keamanan berdasarkan eksplotasi kerentanaan?
3. Bagaimana mengatur prioritas kontrol untuk melindungi CMS WordPress dari eksploitasi pada aspek aplikasi

I.3 Tujuan Penelitian

Berdasarkan fenomena yang telah dijelaskan pada latar belakang dan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut.

1. Mengidentifikasi dan mengklasifikasikan berbagai tipe eksploitasi kerentanan yang dapat ditemukan pada *plugin* serta *non-plugin* dalam Wordpress.
2. Menyusun desain kontrol keamanan yang efektif berdasarkan eksploitasi kerentanan yang telah diidentifikasi
3. Mengatur prioritas kontrol untuk melindungi CMS WordPress dari eksploitasi pada aspek aplikasi dengan mempertimbangkan standar OWASP dan tingkat keparahan kerentanan.

I.4 Batasan Penelitian

1. Pendekatan yang dilakukan berdasarkan eksperimen, dengan menggunakan metode *black-box*, tidak membahas aspek internal dari perangkat lunak dan sistem.
2. Penelitian ini difokuskan pada eksploitasi *target* WordPress.org versi 6.5.2 yang diinstal pada server dengan konfigurasi Nginx sebagai *web server* dan MySQL sebagai *database*.
3. Desain kontrol yang disusun berpedoman pada standar OWASP dan kategori *level* keparahan kerentanan serta mekanisme kontrol yang diberikan hanya berupa rekomendasi.

I.5 Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Secara teoritis, penelitian ini dapat menambah pengetahuan mengenai desain kontrol keamanan yang efektif pada CMS WordPress dari.aspek aplikasi.
2. Secara praktis, penelitian ini diharapkan dapat menyediakan panduan tentang perancangan dan perumusan desain kontrol keamanan yang efektif pada CMS WordPress, sesuai dengan standar keamanan yang ada.