BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dianggap telah berkembang jauh dalam periode yang selalu berubah ini. Semuanya sangat bergantung pada layanan Internet. Mulailah dengan tugas-tugas sederhana seperti menonton acara hiburan, membaca berita, atau memesan makanan dari aplikasi internet. Internet mengubah segala aspek kehidupan kita menjadi lebih mudah. Segala pekerjaan yang ada bisa kita selesaikan lebih cepat dengan hadirnya internet contoh nya seperti pada masa pandemi covid-19. Pandemi covid-19 menjadi masa ketika orang-orang mengubah segala aktivitasnya menjadi serba online. Masyarakat tidak diperkenankan keluar rumah untuk menurunkan kasus penularan virus. Dampaknya yaitu masyarakat menjadi lebih sering membuka website dan segala hal online lainnya. Lalu lintas tiap website pun menjadi naik karena pada saat pandemi orang menjadi sulit jika harus beraktivitas keluar rumah. (Kusuma, 2021).

Aplikasi web kini menjadi bagian dari masyarakat saat ini karena seluruh kebutuhan diperoleh melalui aplikasi berbasis web dan aplikasi seluler, aplikasi web kini telah menjadi bagian mendasar dari kehidupan sehari-hari. Namun, tidak ada yang sempurna di dunia ini, berbagai kelebihan aplikasi web dalam dunia internet juga memiliki kelemahan yang berhubungan dengan aspek keamanan yaitu sangat rentan terhadap serangan dari pihak yang tidak bertanggung jawab. Keamanan pada sebuah aplikasi web merupakan aspek penting yang harus dimiliki (Riska & Alamsyah, 2021).

Banyaknya website yang ada pada saat ini membuat ia sering dijadikan sasaran berbagai jenis serangan web yang beragam seperti DoS (Denial of Service), Hacking, Cross-Site Scripting (XSS), SQL Injection. Sehingga diperlukan suatu sistem yang mampu memberikan solusi dalam pengamanan website. (Bangkit Wiguna et al., 2020). Berdasarkan permasalahan diatas, diperlukan penerapan konsep keamanan aplikasi web untuk melindungi data atau informasi dari serangan hacker. Salah satu solusinya adalah menerapkan web application firewall (WAF) pada aplikasi berbasis web secara open source (Rizal & Sumaryana, 2021). Jika keamanan dari suatu website tidak bagus maka bukan hal yang sulit bagi para penjahat bisa mendapatkan data-data dari website tersebut. Oleh karena itu, perlu adanya pengamanan yang terbaik untuk mencegah hal itu terjadi. Salah satunya yaitu dengan memanfaatkan teknologi firewall untuk bisa mem-filter lalu lintas pengunjung yang mengakses (Kusuma, 2021).

1.2 Perumusan Masalah

Dalam era teknologi yang sangat maju ini, banyak tindak kejahatan terutama pencurian data pada suatu website. Untuk menjaga keamanan website dari serangan yang tidak diinginkan, penulis menerapkan sistem keamanan website menggunakan Web Application Firewall (WAF) dengan Framework Open Web Application Security Project (OWASP). Langkah ini diambil untuk melindungi data-data penting di masa mendatang.

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian tersebut adalah sebagai berikut:

1. Mengidentifikasi kerentanan keamanan pada aplikasi web atau website: Melakukan pengujian keamanan dengan menggunakan Framework OWASP dapat membantu untuk mengidentifikasi kerentanan keamanan yang mungkin terdapat pada aplikasi web atau website, seperti kerentanan pada SQL injection dan cross-site scripting (XSS).
2. Menganalisis tingkat keamanan aplikasi web atau website: Dengan melakukan pengujian keamanan menggunakan Framework OWASP, dapat dilakukan analisis tingkat keamanan aplikasi web atau website yang digunakan, sehingga dapat diketahui apakah aplikasi web atau website tersebut memiliki tingkat keamanan yang cukup atau tidak.
3. Memberikan rekomendasi untuk memperbaiki kerentanan keamanan: Setelah melakukan pengujian keamanan dengan Framework OWASP, tujuan selanjutnya adalah memberikan rekomendasi untuk memperbaiki kerentanan keamanan yang ditemukan pada aplikasi web atau website, sehingga dapat meningkatkan keamanan aplikasi web atau website tersebut.
4. Melindungi informasi sensitif dari serangan cyber: Dengan meningkatkan keamanan aplikasi web atau website melalui pengujian keamanan menggunakan Framework OWASP, tujuannya adalah untuk melindungi informasi sensitif dari serangan cyber, sehingga data pengguna dan informasi penting pada aplikasi web atau website tetap aman.

1.4 Batasan Masalah

Dalam penelitian ini, untuk mencapai tujuan Penerapan Sistem Keamanan Website Menggunakan Waf (Web Application Firewall) Dengan Framework Owasp (Open Web Application Security Project) maka perlu dilakukan pembatasan masalah terhadap keamanan website yang akan dibuat, sebagai berikut;

a. Penelitian ini akan berfokus pada penerapan keamanan website menggunakan WAF berbasis teknologi dan pendekatan yang dianjurkan oleh OWASP. Lingkup teknologi yang akan dipelajari

mencakup konfigurasi, implementasi, dan manajemen WAF, serta integrasinya dengan framework OWASP.

b. Penelitian akan mengevaluasi efektivitas sistem keamanan ini dalam mencegah dan mendeteksi serangan berbasis aplikasi seperti cross-site scripting (XSS) dan serangan lainnya.
c. Penelitian akan mengidentifikasi dan menganalisis tantangan teknis yang mungkin muncul selama implementasi WAF dengan framework OWASP, serta memberikan solusi atau strategi penyelesaiannya.

1.5 Manfaat Peneltian

Adapun manfaat dari penilitan yang dilakukan:

1. Keamanan data pada website: Sistem keamanan website yang terintegrasi dengan OWASP dapat memberikan keamanan yang lebih terhadap data pengguna, sehingga pengguna dapat merasa lebih aman saat menggunakan website tersebut.
2. Perlindungan terhadap serangan: Dengan adanya sistem keamanan yang terintegrasi dengan OWASP, website akan lebih terlindungi dari serangan cyber, seperti serangan hacking, virus, malware, dan sejenisnya. Ini dapat melindungi data pengguna dari ancaman yang merugikan.
3. Peningkatan Keamanan Website: Penelitian ini akan membantu meningkatkan keamanan website melalui penerapan WAF yang dapat mendeteksi dan mencegah serangan siber yang berpotensi merusak aplikasi web.