BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

Seiring dengan perkembangan teknologi informasi yang semakin pesat dan dinamis, tingkat kejahatan siber juga semakin meningkat dewasa ini. Kejahatan siber (*cyber crime*) yang dimaksud ialah percobaan serangan terhadap suatu keamanan sistem informasi. Menurut Ditjen Aptika Kominfo, aktivitas yang dilakukan oleh sekelompok orang yang ingin menembus suatu sistem keamanan bertujuan untuk mendapatkan, mengubah, mencari, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan [1].

Pelaku kejahatan siber biasanya menyerang suatu sistem keamanan informasi yang memuat data-data penting dan rahasia. Biasanya penyerangan yang sering terjadi dilakukan terhadap aplikasi *web*. Banyak pengembang aplikasi *web* yang kurang memperhatikan sisi keamanan aplikasi *web* sehingga banyak dieksploitasi oleh para *hacker*. Menurut hasil *Web Security Report* SiteLock pada tahun 2022, didapatkan 172 serangan dalam sehari untuk satu *website* dan *website* diakses oleh *bot* sebanyak 2306 kali per minggu. *Bot* digunakan oleh hacker untuk mencari kelemahan situs web. Jumlah serangan di tahun 2022 meningkat sebanyak 210% dibandingkan tahun 2020. Terdapat 2 jenis kerentanan tertinggi yang tercatat yaitu *Cross Site Scripting* (XSS) sebanyak 1 juta halaman *website*, dan SQL *Injection* sebanyak 332 ribu halaman *website*. Untuk mengatasi berbagai permasalahan terkait keamanan aplikasi *web* diperlukan suatu sistem yang dapat mencegah serangan berbahaya [11]-[14].

WAF atau *Web Application Firewall* adalah perangkat keamanan yang digunakan untuk melindungi aplikasi *web* dari serangan jaringan yang tidak sah. WAF menganalisis lalu lintas jaringan yang masuk ke aplikasi web dan mengeliminasi lalu lintas yang tidak diinginkan atau merusak sebelum lalu lintas tersebut sampai ke aplikasi. WAF dapat digunakan sebagai sistem yang dapat mencegah serta mendeteksi serangan *SQL injection*, *Cross Site Scripting* (XSS), dan *Local File Inclusion* (LFI) dengan menggunakan *detection rules* yang telah ditetapkan untuk dapat memblokir akses bagi penyerang ke dalam *website* [2].

SIEM (*Security Information and Event Management*) adalah sistem yang digunakan untuk mengumpulkan, menganalisis, dan memantau aktivitas keamanan dari sebuah jaringan atau sistem. SIEM dapat digunakan untuk mengidentifikasi ancaman keamanan seperti serangan jaringan, aktivitas tidak sah, atau kerentanan keamanan yang tidak terdeteksi sebelumnya. Penerapan SIEM sangat membantu dalam melakukan analisis *log* dari suatu *server* yang sedang

berjalan. SIEM memiliki beberapa *tools* yang dapat membantu dalam menganalisis *log* dengan mengumpulkan semua informasi yang mengakses *server* yang sedang berjalan [3].

OWASP atau *Open Web Application Security Project* adalah organisasi nirlaba yang bertujuan untuk membantu para pengembang perangkat lunak dalam membangun aplikasi *web* yang aman. OWASP menyediakan berbagai sumber daya keamanan *web* yang berguna, termasuk dokumentasi, *tools*, dan proyek *open source* yang dapat digunakan oleh para pengembang untuk membangun aplikasi *web* yang aman. Salah satu bentuk penilaian tingkat risiko kerentanan keamanan aplikasi berbasis *website* adalah OWASP *Risk Rating Methodology*. Langkah besar dalam mengukur tingkat risiko adalah menentukan dampak buruk yang dihasilkan dari analisa kerentanan [4].

1.2 Informasi Pendukung Masalah

Pada jurnal berjudul "Implementasi Dan Analisis *Open Source ModSecurity WAF* pada Aplikasi Berbasis *Web* dengan Standar OWASP" (Kirana Dhiatama Ayunda, Adityas Widjajarto, Avon Budiyono) menyatakan bahwa Penggunaan *web application firewall* menjadi kebutuhan untuk melindungi aplikasi berbasis *web* dari serangan. Penerapan *web application firewall* pada aplikasi berbasis *web* dapat mengurangi serangan yang terjadi. Dari aspek keamanan, perlu diketahui seberapa efektif penerapan *web application firewall* untuk melindungi dan meminimalkan serangan berbahaya dari aplikasi berbasis *web* [3].

Penelitian ini menggunakan metode ilmiah dengan standar OWASP dengan memanfaatkan aplikasi berbasis *web* yang dilindungi atau tidak dilindungi oleh *web application firewall*. Dari enam percobaan yang dilakukan, *web application firewall* efektif dalam melindungi aplikasi *web* yang rentan sebesar 83% dan dapat melindungi lima kerentanan dengan risiko level high. Langkah kerentanan yang dapat dilakukan sebagai upaya pencegahan dan penilaian tingkat keamanan berdasarkan *Common Vulnerability and Exposures* (CVE) [5].

1.3 Analisis Umum

Masalah analisis umum dapat disampaikan dalam aspek:

1.3.1 Aspek Teknologi

Teknologi internet bukan lagi Bahasa asing bagi masyarakat. Dalam perkembangan internet terdapat berbagai macam teknologi baru di internet seperti *cloud* dan VPN. Namun,

ada teknologi baru yang menjadi aspek yang sangat penting sejak munculnya internet yakni *webserver*. *Server web* merupakan alat untuk menerima permintaan untuk mengakses situs web melalui *browser*.

Untuk *request, server* memberikan respons berupa halaman *website.* Oleh karena itu *server* merupakan tonggak untuk mengakses *website*. Banyaknya organisasi dan bisnis yang menggunakan *webserver* yang mana setiap masing-masing *web* memiliki keunggulan masing-masing. Pada perencanaan *capstone* ini dirancang sebuah *webserver* yang mana penggunaan *server* dapat di monitoring menggunakan SIEM dan *firewall security* menggunakan *web application firewall*.

1.3.2 Aspek Keamanan

Secara umum *cyber security* merpakan perlindungan digital sistem komputer terhadap berbagai serangan dan akses tidak sah yang dapat mengganggu keamanan data dan informasi pada jaringan. Serangan ini biasa disebut serangan siber atau *crimecyber*. Aktivitas keamanan siber mencakup alat, konsep keamanan dan kebijakan yang membantu melindungi bisnis, organisasi dan set berharga mereka. Perlindungan di sisi lain mencakup layanan, perangkat komputasi, aplikasi data atau informasi di dunia digital. Dengan menerapkan keamanan siber, organisasi dan bisnis dapat mengurangi risiko serangan pada sistem jaringan.

1.4 Kebutuhan yang Harus Dipenuhi

Kebutuhan yang harus dipenuhi yaitu WAF dapat memblokir dan mendeteksi serangan serta SIEM memonitor *log report*. Kemudian, membuat *Wordpress Plugin* kemudian memastikan *wordpress* tersebut dapat mengambil *log* data dari SIEM dan WAF. Setelah itu dilakukan penyerangan pada untuk mengevaluasi WAF.

1.5 Solusi Sistem yang Diusulkan

Berdasarkan masalah di atas maka diusulkan solusi sistem *website* yang dapat mendeteksi serangan dengan menggunakan keamanan *web application firewall* berbasis *proxy* dan *penetration testing* untuk memenuhi kebutuhan serta mencapai tujuan yang diharapkan. Dari sistem yang diusulkan diharapkan mampu mengatasi permasalahan rentan keamanan *website* yang ada. Sehingga pengguna dapat menjaga data-data penting yang ada pada *web server*.

Solusi sistem *website* yang lainnya yaitu dengan ditambahkan sistem pendeteksi serangan menggunakan, IDS, atau *machine learning.*

Sistem ini dirancang dengan beberapa fitur yang mampu mengatasi permasalahan yang telah dijelaskan pada poin sebelumnya. Berikut ini adalah fitur yang diusulkan pada sistem ini sebagai berikut:

1. Menampilkan data pada *plugin WordPress.*
2. Aplikasi *web application firewall* menggunakan *proxy* berbasis *website*.
3. Analisa hasil *log* serangan menggunakan SIEM.

1.5.1 Karakteristik Produk

1.5.1.1 Aplikasi *Web Application Firewall* menggunakan *proxy* berbasis *website*

Fitur ini berfungsi untuk meningkatkan sisi keamanan pada *website* yaitu dengan cara pengecekan terhadap *request* berbahaya berdasarkan *rule proxy*, dapat mendeteksi dan mengidentifikasi serangan berdasarkan OWASP, melakukan pemblokiran terhadap ip *address* yang melakukan *request* berbahaya, melakukan pencatatan dan menyimpan setiap ip *address* yang melakukan *request* berbahaya, aplikasi *web application firewall* menggunakan *proxy* yang berbentuk *prototype.*

1.5.1.2 *Security Information and Event Management* (SIEM)

SIEM akan mengumpulkan data keamanan dari berbagai sumber seperti *log* kejadian yang mencakup data informasi tentang aktivitas jaringan, IP *sources,* IP *destination* dan *severity*. SIEM akan mengubah format data tersebut menjadi data yang mudah dipahami.

1.5.1.3 *WordPress Plugin*

Fitur ini berfungsi untuk mengambil data dari WAF dan SIEM, data yang diambil adalah data relevan dan penting seperti *log* kejadian, aktivitas pengguna yang mencurigakan dan informasi tentang ancaman terdeteksi. Setalah data semua diambil, *plugin* akan menyajikan data tersebut dalam bentuk tabel dan grafik. Tabel untuk menyajikan data yang terstruktur sedangkan grafik untuk memvisualisasikan data-data agar lebih mudah dipahami.

1.5.2 Skenario Penggunaan

Penelitian ini diharapkan dapat bekerja sesuai dengan fungsi yang telah jelaskan pada poin sebelumnya. Adapun cara penggunaan dari sistem yang akan kami rancang adalah sebagai berikut:

1.5.2.1 Skema WAF

Ketika *request* akan mengakses *web server*, maka *request* tersebut akan difilter terlebih dahulu oleh WAF. Jika *request* tersebut tidak terindikasi berbahaya maka akan diteruskan, jika *request* tersebut berbahaya maka akan diblokir secara otomatis.

1.5.2.2 Skema SIEM

Mengakses antarmuka *web* melalui *browser* dengan alamat IP yang telah ditentukan saat *install*. Kemudian dapat melihat daftar kejadian yang terdeteksi oleh snorby. Data yang terenkripsi akan dideskripsi akan diubah ke format JSON yang akan dikirimkan ke *plugin.*

1.5.2.3 Skema *Plugin*

Ketika data telah terdeteksi pada SIEM dan WAF maka *plugin* akan mengambil data tersebut kemudian akan data akan di tampilkan dan divisualisasikan dalam bentuk tabel dan grafik.

1.6 Kesimpulan dan Ringkasan CD-1

Web Application Firewall (WAF) menjadi kebutuhan penting dalam melindungi aplikasi berbasis *web* dari serangan. Penerapan WAF dapat mengurangi serangan yang terjadi dan melindungi aplikasi *web* yang rentan. Dalam analisis umum, teknologi internet seperti *server web* menjadi elemen penting dalam mengakses situs *web* melalui *browser*. Kebutuhan akan keamanan siber juga diperhatikan untuk melindungi data dan informasi dalam jaringan.

Dalam memenuhi kebutuhan, sistem yang diusulkan adalah menggunakan WAF berbasis *proxy* dan SIEM untuk memblokir, mendeteksi dan melaporkan serangan. Selain itu, penggunaan *plugin WordPress* untuk menampilkan dan menganalisis data serangan menjadi solusi yang diusulkan. Karakteristik produk yang diusulkan termasuk aplikasi WAF berbasis *proxy*, SIEM untuk pemantauan keamanan dan *plugin WordPress* untuk tampilan data dan visualisasi. Skenario penggunaan sistem mencakup filtrasi dan pemblokiran *request* berbahaya oleh WAF, pemantauan dan analisis kejadian melalui SIEM, serta tampilan dan visualisasi data melalui *plugin WordPress.*