BAB I
USULAN GAGASAN

1.1. Deskripsi Umum Masalah

1.1.1. Latar belakang masalah

Kejahatan tidak hanya terjadi secara fisik di dunia nyata, namun dapat terjadi di dunia maya melalui teknologi. Kejahatan di dunia maya disebut dengan kejahatan siber yang merupakan salah satu bentuk penyalahgunaan teknologi informasi dan komunikasi hingga menjadi isu prioritas seluruh negara [1]. Berdasarkan data dari Statista tentang *Number of Cyber Attack Cases in Indonesia from 2019 to 2022*, pada tahun 2022 tercatat sekitar 976 juta kasus serangan siber di Indonesia yang mengakibatkan penurunan lebih dari 600 juta kasus dibandingkan tahun sebelumnya. Menurut *National Cyber Security Index Ranking*, skor Indonesia terkait kebijakan keamanan siber masih relatif rendah. Hal ini menunjukkan adanya ruang untuk dilakukan perbaikan pada keamanan siber negara secara keseluruhan [2].

Pelaku kejahatan siber umumnya menyerang suatu sistem keamanan informasi yang memuat data-data penting dan rahasia. Salah satu media digital yang sering menjadi target adalah aplikasi web dengan angka mencapai sekitar 75% serangan siber [3]. Pada tahun 2023 sebanyak 30.000 situs web diretas setiap hari. Aplikasi web sangat rentan terhadap serangan karena aplikasi web harus tersedia untuk semua orang setiap saat. Hal ini menjadi celah bagi pelaku kejahatan siber untuk mencoba mengeksploitasi [4].

Salah satu jenis ancaman keamanan aplikasi web adalah adanya *request* berisi *payload* berbahaya seperti *SQL Injection* (SQLi) dan *Cross-Site Scripting* (XSS) ke aplikasi web. SQLi adalah jenis serangan injeksi, dimana perintah SQL dimasukkan ke dalam *form input* data untuk memengaruhi eksekusi perintah SQL yang telah ditentukan. SQLi memungkinkan penyerang untuk memalsukan identitas *user* atau administrator sistem, merusak data yang ada, atau membuatnya tidak tersedia [5]. Seperti SQLi, XSS merupakan jenis serangan injeksi. Pada XSS, serangan terjadi melalui kode berbahaya berupa *script*. Dampak dari serangan ini adalah penyerang dapat menyamar sebagai pengguna dan mengambil alih akun. Jika pengguna memiliki hak administratif, maka penyerang dapat melakukan *code execution* di server [6].

Jenis ancaman keamanan aplikasi web lainnya adalah *Distributed Denial of Service* (DDoS). Berbeda dengan SQLi dan XSS, DoS dan DDoS umumnya mengirimkan *request* tanpa *payload* berbahaya dalam jumlah besar karena tujuan utamanya adalah memenuhi *bandwidth* pada web aplikasi. Pada tahun 2022, terjadi peningkatan serangan ini hingga 1,6

juta serangan. Serangan DDoS mengakibatkan fungsionalitas situs web menjadi buruk atau membuatnya tidak dapat diakses (*offline*) [7]. Untuk itu, dalam mengatasi serangan SQLi, XSS, dan DDoS ditawarkan sebuah solusi berupa desain dan implementasi *Web Application Firewall* (WAF) dan *rate limiting* pada keamanan aplikasi web.

WAF merupakan perangkat keamanan untuk melindungi aplikasi web dengan cara memfilter, memantau dan memblokir permintaan jaringan yang tidak sah. Berdasarkan definisi WAF, sistem perlindungan yang dilakukan adalah membatasi akses dari IP address yang dicurigai sebagai bentuk serangan. Selain itu, WAF juga dapat membatasi akses berdasarkan *payload* yang dikirimkan pada permintaan (*request*). WAF dapat mendeteksi serangan berupa XSS, SQLi, *Cross-Site Forgery*, *File Inclusion*, dan sebagainya. WAF bekerja berdasarkan sekumpulan *rules* yang bertujuan untuk mengatasi kerentanan dan memfilter trafik berbahaya [8].WAF bersifat manual, yang berarti *rules* harus di-*update* secara berkala ketika serangan terjadi. WAF diintegrasikan dengan *rate limiting* untuk membatasi jumlah request yang dapat digunakan oleh seluruh IP client atau IP yang dicurigai sebagai anomali. Dalam memastikan kinerja dari WAF dan *rate limiting*, dilakukan pengujian berupa pengukuran akurasi dan *Quality of Service* (QoS). Akurasi diukur menggunakan persamaan *true-positive/false-positive*. Kemudian, QoS dari web akan dibandingkan pada saat *rate limiting* belum diimplementasikan dan sedang diimplementasikan. WAF dan *rate limiting* diharapkan dapat menjadi solusi untuk *cyber defense*.

1.1.2. Analisa Masalah

Masalah terkait keamanan aplikasi web dapat mengarah ke berbagai jenis aspek seperti aspek teknologi, aspek bisnis, hingga aspek hukum. Lingkup pada masing-masing aspek saling mempengaruhi karena terkait dengan produk berupa aplikasi web. Produk tersebut dapat mewakili berbagai bidang mulai dari web sederhana, web pendidikan, web berita, hingga web jual beli. Adapun permasalahan pada aspek-aspek tersebut adalah sebagai berikut.

1. Aspek Teknologi

Melakukan serangan SQLi pada aplikasi web dapat membuat data server berisiko dieksploitasi, sedangkan serangan XSS mengakibatkan penyerang dapat mengambil data penting, mengambil *cookie* dari *user* atau mengirimkan suatu program yang dapat merusak [9]. Aplikasi web terindikasi terjadinya serangan DDoS ketika situs atau layanan tiba-tiba menjadi lambat atau tidak tersedia. Serangan ini berupa banyaknya permintaan yang ditunjukkan pada suatu sistem sehingga mengakibatkan sistem *overload*. Sulit untuk memblokir serangan ini karena beberapa perangkat mengirim paket dan menyerang di berbagai lokasi [10] .

2. Aspek Bisnis

Serangan SQLi dapat merugikan bagi perusahaan karena penyerang dapat mengambil alih dan mendapatkan hak administratif atas *database* perusahaan [11]. Serangan XSS juga dapat memengaruhi dalam reputasi bisnis. Penyerang dapat merusak situs web perusahaan dengan cara mengubah kontennya, sehingga dapat merusak citra perusahaan atau menyebarkan informasi yang salah [12]. Sedangkan DDoS bertujuan untuk membuat layanan atau aplikasi web target tidak dapat diakses oleh pengguna yang sah. Hal ini menyebabkan layanan tidak dapat diakses atau terjadinya kegagalan total dalam menyediakan layanan. Dalam bisnis, buruknya layanan mengakibatkan hilangnya pendapatan, kesulitan dalam mengakses media belajar, penurunan produktivitas dan lain sebagainya [13].

3. Aspek Hukum

Menurut hukum yang berlaku di Indonesia, melakukan serangan aplikasi web yang mengakibatkan aplikasi web tidak dapat diakses atau digunakan sebagaimana mestinya, merupakan sebuah pelanggaran hukum. Peraturan ini dimuat dalam Undang-Undang (UU) 11/2008 Pasal 30 ayat 1,2, dan 3 tentang Informasi dan Transaksi Elektronik (ITE). Aturan lainnya terdapat pada Pasal 22 hurif B Undang-Undang (UU) 36/1999 tentang Telekomunikasi [14].

1.1.3 Tujuan Capstone

Adapun tujuan dari capstone adalah mendesain dan mengimplementasikan *Web Application Firewall* (WAF), *rate limiting*, dan *Intrusion Detection System* (IDS) untuk *cyber defense* berupa serangan SQL *Injection* (SQLi), *Cross-Site Scripting* (XSS), DDoS, serta penambahan notifikasi (*alerting*) ketika terjadi serangan.

1.2. Analisa Solusi yang Ada

Dalam mengatasi permasalahan keamanan aplikasi web berupa SQLi, XSS, DoS, dan DDoS, solusi yang dapat ditawarkan yaitu melakukan desain dan implementasi *Web Application Firewall* (WAF), *rate limiting* dan *Intrusion Detection System* (IDS) untuk *cyber defense*. Pada penelitian ini, aplikasi web yang menjadi target serangan dan keamanan adalah *Damn Vunerable Web Applicantion* (DVWA). Berikut merupakan fitur-fitur dari produk yang didesain dan diimplementasikan.

1.2.1. *Web Application Firewall*

Keamanan siber selalu menjadi perhatian utama untuk aplikasi internet, dan permintaan perlindungan situs web terus meningkat. Saat ini *Web Application Firewalls* (WAF) umum digunakan oleh pemilik situs web, karena memberikan perlindungan terhadap berbagai jenis

serangan dengan menyaring permintaan jaringan yang masuk. Berdasarkan penelitian tentang Web Application Firewall Using Machine Learning and Features Engineering tahun 2022, merupakan sebuah penelitian untuk menganalisis permintaan yang masuk ke web server dan memfilter permintaan yang berupa URL, *payload* dan *header*. Penelitian ini mengembangkan keterbatasan penelitian sebelumnya yang hanya menggunakan URL dan *payload* dalam klasifikasinya. Fitur yang dikembangkan pada penelitian ini adalah *request length*, persentase karakter yang diizinkan, persentase karakter khusus dan bobot serangan. Fitur ini menggunakan empat dataset yaitu CSIC 2010, HTTPParams 2015, Hybrid dataset (CSIC 2010 and HTTPParams) dan real logs. Keempat dataset ini diklasifikasikan dengan algoritma *Naive Bayes, Logistic Regression, Decision Tree*, dan *Support Vector Machine* dengan dua metode *train test split dan cross validation* untuk menghindari kemungkinan *overfitting* dan memastikan bahwa fitur-fitur tersebut efektif. Dari hasil penelitian ini akurasi klasifikasi sebesar 99,6% dengan dataset yang digunakan pada penelitian ini dan akurasi klasifikasi 98,8% dengan dataset real web server [15].

Penelitian lain tentang Improving Web Application Firewalls with Automatic Language Detection pada tahun 2022, penelitian ini mencoba mengkategorikan permintaan jaringan dan menentukan apakah setiap permintaan yang masuk normal atau tidak normal. Output dari penelitian ini merupakan kombinasi dari rule-based WAF dan ModSecurity yang merupakan *generic opensource* yang dapat menyimpulkan apakah permintaan yang masuk harus di blok atau tidak. Penelitian ini memberikan hasil yang baik dengan hampir tidak ada notifikasi palsu dan tingkat deteksi yang dapat diterima [16].

Berdasarkan penelitian-penelitian ini dapat disimpulkan bahwa WAF berfungsi untuk melindungi aplikasi web dengan menyaring, memantau, dan memblokir trafik HTTP atau HTTPS berbahaya yang mengarah ke aplikasi web serta mencegah terjadinya kebocoran privasi data. Fungsi tersebut membuat WAF dapat mengidentifikasi kemungkinan terjadinya sebuah serangan. WAF bertindak berdasarkan *rule* atau kebijakan yang diberikan secara manual.

1.2.2. *Rate Limiting*

Rate limiting mengontrol jumlah request yang dapat diterima server selama periode tertentu. *Rate limiting* bekerja dengan cara menetapkan threshold untuk sejumlah *request* yang masuk ke server, lalu traffic yang melebihi *threshold* dapat secara otomatis akan diperlambat atau mengantre sementara sehingga menjaga kestabilan server. *Rate limiting* sangat efektif untuk melindungi titik akhir tertentu yang rentan menjadi target serangan DDoS [17].

Berdasarkan penelitian tentang RateGuard: *A Robust Distributed Denial of Service* (DDoS) *Defense System*, yang merupakan sebuah penelitian tentang solusi inovatif untuk menangani serangan DDoS, dimana DDoS (*Distributed Denial of Service*) merupakan salah satu ancaman utama terhadap keamanan siber. DDoS dapat melumpuhkan sistem atau jaringan dengan *flood attack* melalui *traffic* internet yang tidak diinginkan. Sehingga dapat membuat layanan tidak tersedia bagi pengguna yang sah. Penelitian ini fokus pada tiga jenis serangan DDoS yaitu *Fast Adaptive Attacks* (FAAs), yaitu penyerang secara adaptif menyesuaikan pola serangan berdasarkan *Round Trip Time* (RTT) korban. Kemudian *Adaptive Attacks with statistical filtering rules Scanning* (AAS), yaitu penyerang mengidentifikasi dan mengeksploitasi sistem pertahanan untuk menghasilkan *traffic flood* yang kemudian menyerupai *traffic* normal. Terakhir ada *Low-Rate TCP Attack* (LRA), yaitu solusi untuk menangani permasalahan ini dinamai dengan RateGuard, yaitu sistem pertahanan terhadap DDoS berbasis *Leaky Bucket* (LB). RateGuard mampu melawan tiga jenis serangan DDoS tersebut secara *real time* dengan membatasi *traffic* berlebihan berdasarkan *traffic* nominal korban [18].

Dari penelitian tersebut dapat disimpulkan bahwa jumlah *request* yang dapat diterima oleh server dapat menjadi objek serangan yang sangat rentan. *Rate limiting* dapat membatasi *request* dan mengidentifikasi pola lalu lintas yang tidak normal atau mencurigakan. Dengan membatasi jumlah *request* per detik dari satu atau beberapa sumber, kapasitas *traffic* server atau jaringan dapat tetap stabil dan terjaga.

1.2.3. *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) adalah sebuah teknologi yang sangat penting untuk mencegah terjadinya serangan siber. Setiap transaksi dan pemrosesan informasi terjadi melalui internet yang sangat rentang terhadap berbagai aktivitas berbahaya. Oleh karena itu, perlu adanya perhatian lebih terhadap keamanan informasi [19]. Berdasarkan penelitian tentang Intrusion detection system for cyberattacks in the Internet of Vehicles environment tahun 2023, membahas tentang *framework* baru IDS yang dirancang khusus untuk serangan siber seperti DoS, DDoS, Brute Force, Botnets dan Sniffing. Penelitian tersebut membuat sistem IDS berbasis *machine learning* yang mampu mendeteksi perilaku tidak normal dengan memeriksa lalu lintas jaringan untuk menemukan aliran data yang tidak biasa. Penelitian ini memresentasikan IDS melalui evaluasi dan pemilihan teknik yang paling efektif yaitu pemrosesan data menggunakan Z-*score normalization* yang mempertahankan distribusi data, melakukan seleksi fitur menggunakan model regresi yang menyederhanakan kompleksitas

model dan mengurangi waktu eksekusi, dan terakhir pemilihan *model machine* yang digunakan dengan optimasi *hyperparameter* untuk mengontrol perilaku pada saat pengujian dan mencegah o*verfitting*. Efektifitas solusi tersebut dilakukan melalui pengujian yang menggunakan dataset standar yaitu CIC-IDS-2017, CSE-CIC-IDS-2018, dan CIC-DDoS-2019. Dari hasil penelitian yang telah dilakukan, didapatkan hasil akurasi tinggi sebesar 99,8% dalam waktu eksekusi 46,9 detik dan waktu deteksi 0,24 detik untuk ketiga dataset IDS yang digabungkan [20].

Penelitian lain tentang Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning tahun 2023, membuat sebuah sistem yang dapat menganalisis, mendeteksi dan pemantauan serangan siber menggunakan *Security Information & Event Management* (SIEM) yang dianalisis langsung menggunakan *machine learning pada Intrusion Detection System* (IDS). Pengujian yang dilakukan berfokus pada pengukuran konsumsi sumber daya (CPU dan RAM). Sistem diuji dengan serangan DoS dengan hasil 344,1 paket/detik, dari hasil pengujian *Elasticsearch* adalah komponen yang paling banyak menghabiskan kapasitas CPU dan RAM dengan penggunaan CPU sebesar 78% dan penggunaan RAM sebesar 2300 Mb. Zeek adalah komponen yang paling sedikit menghabiskan kapasitas CPU yaitu sebesar 3,5% dan penggunaan RAM sebesar 225 Mb. Sistem ini juga dapat mendeteksi serangan DoS pada jaringan [21].

Dari kedua penelitian tersebut dapat disimpulkan bahwa *Intrusion Detection System* (IDS) merupakan sistem keamanan yang efektif untuk digunakan. IDS dapat mendeteksi, memantau dan menganalisis serangan siber yang terjadi. IDS dapat memberikan peringatan kepada user, sehingga user dapat menentukan langkah yang tepat untuk mengatasi masalah yang ada.