BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan aplikasi berbasis web dapat melakukan banyak hal seperti mengakses informasi maupun berita. Dengan meningkatnya jumlah penggunaan aplikasi berbasis web ini menyebabkan banyak pengembang yang kurang memperhatikan keamanan aplikasi web. Terkait dengan celah pada aplikasi web, penggunaan *Common Vulnerabilities and Exposures* (CVE) yang berisi tentang daftar celah keamanan pada aplikasi berbasis web sehingga segera diperbarui oleh pengembang. Seiring dengan perkembangan aplikasi berbasis web menjadikan munculnya oknum-oknum yang ingin mengambil keuntungan pribadi. Dilansir dari situs imperva.com menyatakan bahwa jumlah kerentanan pada aplikasi berbasis web di tahun 2019 sebanyak 20.362 kasus meningkat sebanyak 17,6% dibandingkan tahun 2018 sebanyak 17.308 kasus. Dari beberapa jenis kerentanan yang dilaporkan, kerentanan yang paling umum ditemukan pada tahun 2019 yaitu *SQL Injection* meningkat sebanyak 21% dari tahun 2018 (Dima Bekerman, 2020). Untuk mengatasi permasalahan pada keamanan aplikasi berbasis web serta meminimalisir serangan yang dapat menyebabkan kerugian, maka perlu suatu sistem untuk mencegah serangan berbahaya.

Web Application Firewall (WAF) merupakan salah satu cara untuk mengurangi dan mencegah serangan berbahaya. *Web Application Firewall* memiliki beberapa fungsi diantaranya dapat melakukan *monitoring* lalu lintas jaringan, mendeteksi dan memblokir serangan berbahaya, serta melakukan penyaringan akses ke aplikasi berbasis web. Pada penelitian ini menggunakan *Web Application Firewall* ModSecurity untuk melindungi aplikasi berbasis web dari serangan. ModSecurity memiliki fungsi sama seperti *web application firewall* pada umumnya, yaitu melakukan pemblokiran lalu lintas jaringan yang dianggap berbahaya oleh *rule* yang telah ditentukan serta dapat melindungi aplikasi web dari serangan seperti *SQL Injection, Cross-Site Scripting, Remote File Inclusion,* dan *Brute Force*.

Akibat dari meningkatnya kerentanan pada aplikasi berbasis web maka pada penelitian ini membahas tentang efektivitas penggunaan *control* dalam melindungi aset IT yang rentan dari serangan. Pada penelitian ini standar OWASP digunakan sebagai tahapan *penetration testing*. Dari penelitian ini diharapkan *web application firewall* efektif melindungi aplikasi web yang rentan dari serangan.

Pada penelitian tentang ModSecurity WAF pada aplikasi berbasis web dengan standar OWASP karena tahapan OWASP mudah dipahami dan tahapan dari standar OWASP ringkas dan jelas. Penerapan standar OWASP dapat berguna untuk melindungi aplikasi web dari serangan seperti *SQL Injection, Cross-Site Scripting, Brute Force*, dan serangan lainnya.

I.2 Perumusan Masalah

Berdasarkan latar belakang di atas, perlu diketahui beberapa perumusan masalah terkait dengan penelitian kali ini sebagai berikut:

1. Bagaimana penggunaan *control* dalam melindungi aset IT?
2. Bagaimana tingkat efektivitas penggunaan *control* dalam melindungi aset IT?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, berikut merupakan tujuan dari penelitian Tugas Akhir ini sebagai berikut:

a. Menganalisis kemampuan *control* dengan mengeksploitasi aset IT sebelum dan setelah diproteksi oleh *control* berupa *web application firewall*.

b. Mengevaluasi penggunaan *control* dalam melindungi aset IT.

I.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian Tugas Akhir ini yaitu sebagai berikut:

1. Berfokus terhadap penggunaan *Web Application Firewall* dalam melindungi aplikasi berbasis web yang rentan.

2. Penelitian dilakukan berdasarkan eksperimen eksploitasi terhadap aset IT.
3. Penggunaan standar OWASP sebagai pedoman untuk melakukan proses eksploitasi.
4. Penelitian ini tidak menggunakan langkah *Maintaining Access* pada standar OWASP.

I.5 Manfaat Penelitian

Adapun manfaat bagi peneliti yang didapatkan dari penelitian Tugas Akhir ini yaitu sebagai berikut:

1. Secara teoritis, dapat menambah ilmu pengetahuan terkait dengan pengujian *control* pada sebuah aset IT dari serangan.
2. Secara praktis, dapat memberikan penguasaan materi maupun keahlian dalam melakukan proses *penetration testing* pada aplikas web.

I.6 Sistematika Penulisan

Adapun sistem penulisan pada Tugas Akhir ini sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai uraian latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan permasalahan yang diteliti dan dibahas pula hasil-hasil penelitian terdahulu.

Bab III Metodologi Penelitian

Bab ini berisikan tentang model konseptual yang digunakan pada penelitian serta tahapan pada penelitian yang dilakukan mulai dari tahap awal, tahap hipotesis, tahap eksperimen, tahap analisis,

tahap akhir atau kesimpulan.

Bab IV Perancangan Sistem dan Skenario Pengujian

Bab ini berisikan tentang perancangan *software* maupun *hardware* yang digunakan pada penelitian ini sebagai skenario pengujian.

Bab V Analisis dan Pengujian Sistem

Pada bab ini berisikan pengujian terhadap sistem serta analisis masalah yang telah ditemukan mengikuti skenario yang telah ditentukan pada BAB V.

Bab VI Kesimpulan dan Saran

Pada bab ini dijelaskan kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya.