BAB I
PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi yang semakin pesat di era revolusi industri 4.0, menyebabkan akses internet dan pencarian informasi melalui website semakin meningkat. Peningkatan permintaan informasi tersebut membuat pengembang dan pemilik informasi mengumpulkan banyak data dan informasi di server, sehingga tuntutan keamanan server juga ikut meningkat karena semakin banyak data penting yang terdapat pada *server, maka* semakin tinggi pula resiko terjadinya peretasan data oleh pihak yang tidak bertanggung jawab atau biasa disebut *hacker*. Sehingga diperlukan *reverse proxy* untuk melindungi web server dengan menyaring, menganalisis, dan memblokir permintaan berbahaya sebelum mencapai server.

Salah satu serangan terhadap aplikasi web adalah serangan *Sql Injection (SQLi)*. Serangan ini menjadi salah satu ancaman yang paling umum yang mengancam keamanan database dari sebuah website [1]. Keamanan *web server* sangat berperan penting dalam menjaga data dan *privasi user* yang ada dalam server. Pemantauan sistem penuh tidak mungkin dilakukan secara manual. Perlu adanya bantuan sistem pengganti manusia untuk pemantauan terus menerus, yang diharapkan dapat mendeteksi dan mencegah serangan terhadap jaringan *web server*.

Berdasarkan pemaparan yang disampaikan diatas maka peneliti akan menganalisis penggunaan *reverse proxy* yang bertujuan untuk meningkatkan keamanan *web server* terhadap ancaman *Sql Injection* yang berjudul "Analisis Keamanan Web Server Menggunakan *Reverse proxy* dari Serangan *Sql Injection*".

1.2 Rumusan Masalah

Berdasar permasalahan yang diuraikan di latar belakang, rumusan masalah dalam penelitian ini, yaitu :

1. Bagaimana cara kerja *reverse proxy* dalam melindungi *web server* dari

serangan *Sql Injection*?

2. Seberapa efektif penggunaan *reverse proxy* dalam meningkatkan keamanan *web server* dari serangan *Sql Injection* pada web server?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang ada maka:

1. Penelitian ini dibatasi dalam ruang lingkup keamanan web server dengan *reverse proxy* dari serangan *Sql Injection*.
2. Fokus utamanya adalah konfigurasi dan implementasi *reverse proxy* sebagai lapisan pertahanan pertama, dimana pengujian *Sql Injection* akan dilakukan pada web server sebelum dan sesudah integrasi *reverse proxy* untuk membandingkan efektivitasnya.
3. Evaluasi diukur melalui simulasi serangan *Sql Injection* menggunakan perangkat lunak *penetration testing*, lingkupnya hanya akan menganalisis prinsip kerja dan konfigurasi *reverse proxy* dalam mendeteksi serta memblokir serangan *Sql Injection*.
4. Pembahasan tidak mencakup praktik pengkodean pada aplikasi, pengembangan algoritma baru, atau jenis serangan diluar *Sql Injection*.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai peneliti dalam penelitiannya, yaitu :

1. Mengetahui bagaimana cara kerja *reverse proxy* dalam melindungi *web server* dari serangan *Sql Injection*?
2. Mengetahui seberapa efektif penggunaan *reverse proxy* dalam meningkatkan keamanan *web server* dari serangan *Sql Injection* pada web server?

1.5 Manfaat Penelitian

1. Manfaat Akademik
   a. Penelitian ini berkontribusi pada literatur keamanan siber, khususnya dalam bidang perlindungan aplikasi web dari serangan *Sql Injection*.
2. Manfaat Praktis

a. Peningkatan Keamanan Aplikasi Web

3. Manfaat untuk Pengembangan Keamanan Jaringan dan Web

a. Memperkuat Perlindungan Jaringan Web: Penelitian ini memberikan wawasan mengenai pentingnya penerapan *reverse proxy* dalam mengamankan komunikasi antara pengguna dan server web