JUDUL:

ANALISIS *REVERSE PROXY* DAN NAXSI UNTUK PENCEGAHAN SERANGAN XSS DAN SQL INJECTION PADA *WEB SERVER*

SKRIPSI

RAFLI AKBAR AUDI PUTRA

1907422003

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

ANALISIS *REVERSE PROXY* DAN NAXSI UNTUK PENCEGAHAN SERANGAN XSS DAN SQL INJECTION PADA *WEB SERVER*

SKRIPSI

Dibuat Untuk Melengkapi Syarat-Syarat yang Diperlukan Untuk Memperoleh Diploma Empat Politeknik

RAFLI AKBAR AUDI PUTRA
1907422003

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Rafli Akbar Audi Putra

NIM : 1907422003

Jurusan/ProgramStudi : T.Informatika dan Komputer / TMJ

Judul skripsi : Analisis *Reverse proxy* dan Naxsi untuk pencegahan serangan Sql Injection dan XSS pada *web server*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, ...

Yang membuat pernyataan

(Rafli Akbar Audi Putra)

NIM 1907422003

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Rafli Akbar Audi Putra
NIM	:	1907422003
Program Studi	:	Teknik Multimedia Jaringan
Judul Skripsi	:	Analisis *Reverse Proxy* dan Naxsi untuk pencegahan serangan XSS dan Sql Injection pada *web server*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 4, Bulan Agustus, Tahun 2023 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom., M.T. ( )

Penguji I : Ayu Rosyida Zain, S.ST., M.T. ( )

Penguji II : Defiana Arnaldy, S.Tp., ( )

Penguji III : Ariawan Andi Suhandana S.Kom, M.T.I. ( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

KATA PENGANTAR

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa karena berkat dan rahmat-Nya penulis dapat menyelesaikan laporan skripsi ini. Laporan skripsi ini dibuat untuk memenuhi salah satu persyaratan gelar. Sarjana Terapan yang diterima di Politeknik Negeri Jakarta. Fokus penelitian ini akan melakukan Analisis *reverse proxy* dan Naxsi untuk pencegahan serangan XSS dan Sql injection pada *web server* sebelum dan sesudah menerapkan *reverse proxy* dan Naxsi, dengan metode penyerangan menggunakan *tools* Nmap, Nessus, Sql Map dan Xsser. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dan masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu terutama kepada:

1. Bapak Iik Muhamad Malik Matin, S.Kom., M.T., selaku pembimbing penulis yang telah banyak membantu, mendukung dan memberi masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai;
2. Bapak Defiana Arnaldy, S.Tp., M.Si., Ibu Ayu Rosyida Zain, S.ST., M.T. dan Bapak Ariawan Andi Suhandana S.Kom, M.T.I. selaku dosen penguji yang telah memberikan saran dan masukan penelitian;
3. Dr. Prihatin Oktivasari, S.Si., M.Si. selaku kepala program studi Teknik Multimedia dan Jaringan jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
4. Ibu, Ayah dan teteh yang selalu memberikan dukungan dan bantuan pada saat pengerjaan skipsi ini.
5. Teman-teman CCIT SEC 2019 yang sudah mendukung, membantu dan memberikan dorongan sesama perkuliahan hingga selesai skripsi Bersama.
6. Teman-teman semua yang tidak dapat disebutkan satu per satu, atas waktu, bantuan, dan dukungan dalam proses pengerjaan skripsi.
7. Rinda Eriska sebagai orang terdekat yang sudah memberikan semangat semasa pengerjaan skripsi

Akhir kata, penulis mengucapkan terima kasih banyak kepada Anda semua, dan semoga Allah SWT membalas semua kebaikan yang Anda berikan. Mohon maaf

apabila ada kesalahan atau kekurangan dalam skripsi ini. Semoga pembaca mendapatkan manfaat dari skripsi ini dan menjadi inspirasi untuk penelitian lebih lanjut. Sekian dan terimakasih Wassalamualaikum Warahmatullahi Wabarakatuh.

Depok,….

Rafli Akbar Audi Putra

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Rafli Akbar Audi Putra

NIM : 1907422003

Jurusan/ProgramStudi : T.Informatika dan Komputer / TMJ

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis *Reverse proxy* dan Naxsi untuk pencegahan serangan Sql Injection dan XSS pada *web server*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta..

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, ……..

Yang Menyetujui, Materai

(R. … …tra)

NIM. 1907422003

ANALISIS *REVERSE PROXY* DAN NAXSI UNTUK PENCEGAHAN SERANGAN XSS DAN SQL INJECTION PADA *WEB SERVER*

Abstrak

Dalam era digital saat ini, keamanan *web server* menjadi hal yang sangat penting. Banyak pihak dan Lembaga yang belum menyadari pentingnya keamanan pada sebuah *web sever*. Keamanan *web server* menjadi semakin penting mengingat meningkatnya serangan *cyber* terhadap *web server* dalam beberapa tahun terakhir. Analisis menerapkan *reverse proxy* dan Naxsi untuk pencegahan serangan XSS dan SQL Injection pada *web server* adalah sebuah penelitian yang bertujuan untuk mengevaluasi efektivitas penggunaan *reverse proxy* dan Naxsi sebagai *Web Application Firewall* dalam melindungi *web server* dari serangan XSS dan SQL Injection. Penetrasi ilegal ke dalam *web server* dapat mengakibatkan pencurian data, kehilangan akses, penyebaran malware, dan bahkan kerusakan *server*. Penelitian ini menggunakan metode pentesting dengan menerapkan *reverse proxy* dan Naxsi pada *web server*. Selanjutnya, dilakukan pengujian pentesting *web server* menggunkaan *tool* SQLmap dan Xsser. Untuk mengatasi jenis serangan Sql Injection dan XSS dilakukan pengujian sebelum dan sesudah menerapkan *reverse proxy* dan Naxsi, dengan metode penyerangan menggunakan *tools* Nmap, Nessus, Sql Map dan Xsser. Hasil Analisis pengujian menunjukkan bahwa penggunaan *reverse proxy* dan Naxsi memperoleh 554.961 pada serangan SQL Injection, 186.076 Pada serangan XSS dan 64.357 serangan pada serangan publik.

Kata Kunci: *Web server*, Naxsi, *Reverse proxy*, *SQL Injection*, *Cross-Site Scripting*.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada saat ini melaju dengan sangat pesat, kita banyak dimudahkan dalam melakukan berbagai hal. Saat ini, estimasi pengguna internet dan statistik populasi dunia berlaku hingga 30 Juni 2022 terdapat 7,932,791,734 poulasi (Internet World Stats, 2023). Internet menjadi suatu landasan untuk mencari informasi yang penting bagi semua aspek kehidupan. Indonesia menempati peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet di mana pada tahun 2017 diperkirakan *netter* Indonesia mencapai 112 juta orang (Kautsar, 2021).

Umumnya, di dalam sebuah *server* Linux terdapat keamanan kuat yang diberikan seperti hak akses yang memungkinkan administrator dapat mengelola dan mengontrol akses pengguna ke berbagai file dan direktori. Namun, pada *server* Linux maupun Nginx *web server* juga perlu dilakukan pembaharuan, konfigurasi dan *patching* secara teratur untuk mengatasi celah keamanan yang mungkin terjadi. *Web server* berguna sebagai tempat aplikasi web dan penerima request dari *klien*. Seiring dengan perkembangan teknologi informasi, jenis kejahatan dalam teknologi terkhusus pada *web server* juga marak timbul (ANSHOR, 2022).

Pada tahun 2021 menunjukan bahwa serangan berbasis injeksi masih menjadi sepuluh besar serangan yang paling banyak digunakan OWASP (OWASP, 2023). Serangan *SQL Injection* yang memanfaatkan celah keamanan pada lapisan antarmuka *database* untuk memasukkan kode berbahaya atau mengubah pernyataan SQL yang digunakan oleh aplikasi web. Serangan injeksi terjadi ketika seseorang yang tidak sah, mengirimkan perintah SQL berbahaya ke *server.* Hal ini cukup sering terjadi karena hampir semua aplikasi modern menggunakan *database* terpusat untuk menyampaikan informasi(Bastian et al., 2020). Serangan XSS (*Cross-Site Scripting*) merupakan serangan pada aplikasi web dimana penyerang untuk menyisipkan skrip berbahaya (seperti JavaScript) ke dalam halaman web yang ditampilkan oleh pengguna. XSS sering terjadi ketika aplikasi web tidak memvalidasi dengan benar masukan yang diberikan pengguna, seperti memasukkan

teks atau kode HTML(Dewangkara et al., 2022). Serangan ini dapat memungkinkan penyerang untuk mencuri informasi dari pengguna, seperti nama pengguna dan kata sandi, atau melakukan tindakan berbahaya seperti memodifikasi atau menghapus data. Berkaca dari masalah banyaknya serangan menuju *web server* menimbulkan pertanyaan bagaimana cara mencegah ancaman serangan sebelum terjadi. Salah satunya dengan memanfaatkan Naxsi sebagai *Web Application Firewall* (WAF) yang dikembangkan oleh Wargio (Wargio, 2023). Selain menggunakan Naxsi, *Reverse proxy* juga dapat dimanfaatkan dalam menghindari beban pada *web server*. *Reverse proxy* mengatur agar sebuah server dapat berperan menjadi perantara antara klien dengan server utama. Selain itu *Reverse proxy* berhasil mengoptimalisasi *web server* dengan mengakses *Reverse IP Proxy* layanan *Reverse proxy* pada saat terjadinya waktu permintaan, waktu transfer, dan waktu koneksi (Defiana Arnaldy, 2020). Salah satu WAF yang dapat digunakan adalah Naxsi. Naxsi berfungsi sebagai lapisan tambahan yang dapat memperkuat keamanan aplikasi *web server* yang dijalankan oleh Nginx.

Penerapan WAF Naxsi telah dilakukan di beberapa penelitian salah satunya oleh Feri Setiyawan (Setyawan, 2014) menerapkan *web application firewall* (WAF) menggunakan Naxsi untuk menangkal serangan SQL injection pada web server. Namun penggunaan Naxsi dalam menangkal serangan SQL injection dan XSS perlu dilakukan kajian mengenai performa Naxsi terhadap serangan SQL Injection dan XSS.

Untuk itu, pada penelitian ini dilakukan analisis *reverse proxy* dan Naxsi pada serangan XSS dan SQL Injection pada *web server*. Analisis dilakukan dengan menerapkan reverse proxy dan Naxsi pada sebuah VPS. Kemudian diuji berdasarkan serangan SQL injection dan XSS secara lokal dan publik. Pada skema lokal, serangan dilakukan menggunakan tools Nmap, Nessus, Sql Map, dan Xsser pada kondisi sebelum menggunakan reverse proxy dan setelah menggunakan reverse proxy. Hasil serangan akan dibandingkan pada saat sebelum menerapkan *reverse proxy* dan Naxsi di web server dan setelah menerapkan *reverse proxy* dan

Naxsi di web server. Selain itu, pada penyerangan publik dilakukan pengambilan data terhadap jenis dan target serangannya.

1.2 Perumusan Masalah

Berdasarkan uraian dari latar belakang tersebut maka perumusan masalahnya adalah sebagai berikut:

a. Bagaimana merancang *reverse proxy* dan NAXSI untuk mencegah serangan XSS dan SQL Injection pada *web server*?
b. Melakukan analisis serangan *reverse proxy* dan Naxsi terhadap Sql Injection dan XSS.

1.3 Batasan Masalah

Adapun batasan masalah yang dibuat agar pembahasan lebih terukur dan terfokus. Pembatasan masalah tersebut antara lain sebagai berikut:

a. Penelitian ini disimulasikan sebuah perangkat *reverse proxy* dan *server* secara *hosting* virtual private *server*.
b. WAF (*Web Application Firewall*) yang diterapkan adalah NAXSI.
c. Penelitian ini menggunakan *web server* Nginx untuk *proxy server*.
d. Penyerangan yang dilakukan adalah Sql Injection dan XSS (Cross-site Scriping).
e. *Tools* yang digunakan dalam pengujian penelitian ini adalah Nmap, Nessus, Sql Map, dan Xsser.

1.4 Tujuan dan Manfaat

Ada tujuan dan manfaat dari dilakukannya penelitian ini adalah:

1.4.1 Tujuan

1. Melakukan perancangan *reverse proxy* dan Naxsi untuk mencegah serangan XSS dan SQL Injection pada *web server*
2. Melakukan analisis pada *website* yang sudah di terapkan *reverse proxy* dan Naxsi menggunakan *tools* Nmap, Nessus, Sql Map dan Xsser.

1.4.2 Manfaat

1. Memberikan solusi dalam meningkatkan keamanan *web server* dari serangan XSS dan SQL Injection.
2. Meningkatkan kewaspadaan terhadap keamanan informasi bagi penulis, pekerja dan pembaca.
3. Memberikan rekomendasi mengenai penggunaan *reverse proxy* dan NAXSI secara bersamaan untuk memberikan keamanan yang lebih baik pada *web server*.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan proposal ini adalah sebagai berikut:

1. **BAB I PENDAHULUAN**

Bab ini berisi pembahasan tentang latar belakang, perumusan masalah, batasan masalah, tujuan, dan manfaat serta sistematika penulisan.

2. **BAB II TINJAUAN PUSTAKA**

Bab ini berisi pembahasan mengenai materi/teori yang mendukung membantu proyek yang dibuat pada proposal.

3. **BAB III PERENCANAAN DAN REALISASI ATAU RANCANG BANGUN**

Pada bab ini akan dijelaskan mengenai tahapan penelitian dan rancangan terkait kegiatan penelitian

4. **BAB IV HASIL DAN PEMBAHASAN**

Penulis akan menjabarkan hasil yang didapat dari penelitian yang sudah dilakukan

5. **BAB V PENUTUP**

Penulis akan memberikan kesimpulan dan saran dari penelitian.

BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil penelitian "Analisis *Reverse proxy* dan Naxsi untuk pencegahan serangan XSS dan Sql Injection pada *web server"* yang telah dilakukan oleh penulis, dapat ditarik kesimpulan sebagai berikut:

1. Pada penelitian ini berhasil merancang dan mengimplementasikan sistem *reverse proxy* dan Naxsi sebagai Web Application Firewall di dalam server. Prosesnya melibatkan konfigurasi server Ubuntu di dalam virtual private server (VPS) dan instalasi Nginx di dalam *web server* untuk pembuatan website yang digunakan untuk penyerangan. Selanjutnya, penulis melakukan konfigurasi modul *reverse proxy* dan menerapkan serta mengkonfigurasi Naxsi Web Application Firewall di dalam Nginx. Penulis juga menggunakan skrip Python yang digunakan untuk untuk menganalisis hasil dari acces.log, error.log dan naxsi.log pada setiap pengujian yang dilakukan.
2. Analisis tanpa menggunakan *reverse proxy* dan Naxsi, penulis berhasil mendapatkan akses ke isi database server melalui serangan SQL Injection. Selain itu, penulis juga berhasil menyisipkan sintaks berbahaya ke dalam *web server* menggunakan serangan XSS.
3. Setelah mengunakan *reverse proxy* dan Naxsi, ditemukan sebanyak 554.961 serangan pada Sql Injection dan 186.076 serangan pada XSS. Pada pengambilan data dari publik, ditemukan sebanyak 64.357 serangan. Dalam hasil analisis tersebut, ditemukan bahwa serangan Sql Injection merupakan jenis serangan yang paling banyak terjadi pada *web server.*
4. Pada penelitian ini berhasil melakukan penyerangan sebelum menerapkan *reverse proxy* dan Naxsi menggunakan Nmap, Nessus, Sql Injection dan XSS dan berhasil menemukan 17 kerentanan pada *tools* scanning dan mendapatkan isi dari *database server* dan *cookie* di dalam *web server* pada *exploitation tools*. Setelah menerapkan *reverse proxy* dan Naxsi, penulis berhasil menguji kembali dengan

menggunakan Nmap, Nessus, Sql Injection dan XSS. Hasil penelitian menunjukkan bahwa tidak ditemukan adanya kerentanan pada *scaning tools* yang digunakan, serta tidak ada akses yang berhasil diperoleh ke dalam *database server* maupun *cookie* yang berada di dalam *web server* menggunakan *exploitation tools*.

5.2 Saran

Berdasarkan pengujian yang telah dilakukan, berikut saran yang dapat diusulkan pada penelitian selanjutnya adalah :

1. Dapat menggunakan Web Application Firewall lain untuk melakukan penelitian seperti WAFNinja dan IronBee.
2. Menambahkan penyerangan selain Sql Injection dan XSS.
3. Menambahkan *tools* lain seperti loic dan sucuri untuk melakukan serangan ke dalam *web server*.