



JUDUL:

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

SKRIPSI

RAFLI AKBAR AUDI PUTRA

1907422003

**POLITEKNIK
NEGERI
JAKARTA**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER**

POLITEKNIK NEGERI JAKARTA

2023

© Hak Cipta milik Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**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

**POLITEKNIK
NEGERI
JAKARTA**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN**

JURUSAN TEKNIK INFORMATIKA DAN

KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Rafli Akbar Audi Putra

NIM : 1907422003

Jurusan/Program Studi : 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



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta



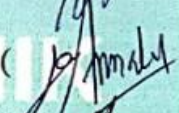

LEMBAR PENGESAHAN

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 Amaldy, 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

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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 skripsi 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



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



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/Program Studi : 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 pernyataan ini saya buat dengan sebenarnya.

Depok,

Yang Menandatangani Meterai



(R. tra)

NIM. 1907422003

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





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* menggunakan *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.*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat.....	3
1.4.1 Tujuan.....	4
1.4.2 Manfaat	4
1.5 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA	5
2.1 <i>Web server</i>	5
2.2 <i>Nginx Web server</i>	5
2.3 <i>Web Application Firewall</i>	6
2.4 <i>Reverse proxy</i>	7
2.5 NAXSI (Nginx anti XSS dan SQL Injection)	7
2.6 XSS (Cross site-scripting).....	8
2.7 SQL Injection	9
2.8 Virtual box.....	9
2.9 Ubuntu	10
2.10 Kali Linux.....	11
2.11 Nesus <i>Vulnerability Scanner</i>	13
2.12 BurpSuite.....	14
2.13 XSSER.....	14
2.14 SQLMAP.....	15
2.15 Visual Studio Code.....	16

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.16	Penelitian Sejenis	16
	BAB III METODE PENELITIAN.....	20
3.1	Rancangan Penelitian	20
3.1.1	Flowchart Alur Penelitian	20
3.2	Tahapan Penelitian.....	21
3.3	Objek Penelitian	22
	BAB IV HASIL DAN PEMBAHASAN.....	23
4.1	Analisis Kebutuhan	23
4.1.1	Spesifikasi Perangkat Penelitian	24
4.2	Perancangan Sistem.....	24
4.3	Implementasi Aplikasi Sistem.....	26
4.3.1	Instalasi dan konfigurasi <i>Virtual box</i>	26
4.3.2	Instalasi dan konfigurasi Windows 11	27
4.3.3	Konfigurasi <i>Server VPS</i>	29
4.4	Pengujian.....	44
4.4.1	Deskripsi Pengujian	44
4.4.2	Prosedur Pengujian	45
4.4.3	Data Hasil Pengujian.....	46
4.4.4	Analisis Data/Evaluasi Pengujian	64
	BAB V PENUTUP.....	186
5.1	Simpulan.....	186
5.2	Saran.....	187
	DAFTAR PUSTAKA.....	xvi
	Lampiran	xx

DAFTAR GAMBAR

Gambar 2.1 Nginx Logo.....	5
Gambar 2.2 Naxsi Logo.....	7
Gambar 2.3 Tampilan Virtual Box.....	10
Gambar 2.4 Tampilan Ubuntu	11
Gambar 2.5 Tampilan Kali Linux	13
Gambar 2.6 Nessus	13
Gambar 2.7 BurpSuite	14
Gambar 3.1 Flowchart Alur Penelitian	20
Gambar 4.1 Bagan perancangan.....	25
Gambar 4.2 Implementasi Virtual box.....	26
Gambar 4.3 Instalasi Kali Linux.....	27
Gambar 4.4 Instalasi Visual Studio Code	27
Gambar 4.5 Remote SSH.....	28
Gambar 4.6 Ubuntu Version	28
Gambar 4.7 Install Nessus dashboard.....	29
Gambar 4.8 Nginx version.....	29
Gambar 4.9 Nginx start	30
Gambar 4.10 Instalasi fpm.....	30
Gambar 4.11 Start php.....	31
Gambar 4.12 Konfigurasi php-fpm	31
Gambar 4.13 Instalasi Mysql-server	31
Gambar 4.14 mysql.....	32
Gambar 4.15 Koneksi.php	32
Gambar 4.16 Halaman login.....	33

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.17 Halaman utama	33
Gambar 4.18 <i>Reverse proxy</i> line script.....	34
Gambar 4.19 Web Proxy.....	35
Gambar 4.20 Custom.log.....	35
Gambar 4.21 Web reverse proxy port.....	36
Gambar 4.22 Aplikasi port.....	36
Gambar 4.23 Naxsi dependencies	37
Gambar 4.24 Naxsi Instal	37
Gambar 4.25 Naxsi compile	37
Gambar 4.26 Naxsi core rules	38
Gambar 4.27 Naxsi.rules	38
Gambar 4.28 Nginx.conf	40
Gambar 4.29 Sites konfigurasi	41
Gambar 4.30 Nginx-t.....	41
Gambar 4.31 Custom-access.log	42
Gambar 4.32 Hasil python custom	42
Gambar 4.33 Error.log	43
Gambar 4.34 Hasil python error.....	43
Gambar 4.35 Hasil Naxsi log	43
Gambar 4.36 Hasil python Naxsi	44
Gambar 4.37 Skenario Pengujian	46
Gambar 4.38 Nmap web.....	47
Gambar 4.39 Nmap web.....	47
Gambar 4.40 Nessus web	47
Gambar 4.41 Burpsuite web	48

Gambar 4.42 Sql Map web	48
Gambar 4.43 Instal Xsser	48
Gambar 4.44 Xsser web.....	49
Gambar 4.45 Nmap rp	51
Gambar 4.46 Nmap vuln rp	51
Gambar 4.47 Nmap vuln rp	52
Gambar 4.48 Sql map rp.....	52
Gambar 4.49 Sql map rp2.....	52
Gambar 4.50 Xsser rp.....	53
Gambar 4.51 Nmap n.....	55
Gambar 4.52 Nmap vuln n	55
Gambar 4.53 Nessus n	56
Gambar 4.54 Sql map n	56
Gambar 4.55 Sql map skrip n	57
Gambar 4.56 Xsser n	57
Gambar 4.57 Nmap scanning	60
Gambar 4.58 Nmap Vuln.....	60
Gambar 4.59 Nessus scan Naxsi.....	60
Gambar 4.60 Burpsuite Naxsi	61
Gambar 4.61 Sqlmap Naxsi.....	62
Gambar 4.62 Xsser Naxsi.....	62
Gambar 4.63 Nmap hasil web	65
Gambar 4.64 Nmap vuln web.....	66
Gambar 4.65 Hasil Nessus Vuln.....	67
Gambar 4.66 Penyerangan Sql lokal	73

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.67 Hasil Sql local.....	73
Gambar 4.68 Penyerangan Xsser local.....	74
Gambar 4.69 Payload xss	74
Gambar 4.70 Nmap hasil rp.....	75
Gambar 4.71 Nmap vuln hasil rp.....	77
Gambar 4.72 Nessus hasil rp	77
Gambar 4.73 Sql map hasil rp	83
Gambar 4.74 Xsser hasil rp	83
Gambar 4.75 Hasil Nmap n	85
Gambar 4.76 Hasil Nmap vuln n.....	85
Gambar 4.77 Hasil Nessus n.....	87
Gambar 4.78 Sql map n	92
Gambar 4.79 Sql param n.....	93
Gambar 4.80 Xsser n	93
Gambar 4.81 Nmap hasil.....	94
Gambar 4.82 Nmap Vuln.....	96
Gambar 4.83 Hasil Nessus.....	96
Gambar 4.84 Hasil sqlmap	100
Gambar 4.85 Parameter sqlmap.....	101
Gambar 4.86 Hasil Xsser.....	101
Gambar 4.87 Blocked by NAXSI.....	102
Gambar 4.88 Hasil access.log nmap -A	103
Gambar 4.89 Hasil access.log nmap vuln.....	104
Gambar 4.90 Hasil Nessus web.....	104
Gambar 4.91 Hasil error.log Nessus web	105

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.92 Hasil Sql map log web	105
Gambar 4.93 Hasil xsser web	106
Gambar 4.94 Hasil custom acces rp	107
Gambar 4.95 Garfik Hasil Acces.log rp	108
Gambar 4.96 Hasil custom acces rp	109
Gambar 4.97 Grafik nmap vuln rp.....	110
Gambar 4.98 Hasil Nessus rp	111
Gambar 4.99 Hasil Nessus rp	112
Gambar 4.100 Grafik Nessus rp	113
Gambar 4.101 Hasil analisis sqlmap rp	114
Gambar 4.102 Hasil analisis xsser rp	115
Gambar 4.103 Hasil analisis nmap-a nd.....	116
Gambar 4.104 Hasil analisis naxsi nmap-a nd	118
Gambar 4.105 Hasil nmap-vuln nd.....	119
Gambar 4.106 Grafik halaman error nd.....	120
Gambar 4.107 Nmap-vuln naxsi nd.....	121
Gambar 4.108 Grafik Naxsi nd.....	123
Gambar 4.109 Acces.log nessus nd	124
Gambar 4.110 Grafik laman error nd	125
Gambar 4.111 Hasil analisis naxsi nd.....	126
Gambar 4.112 Grafik rule naxsi nd	128
Gambar 4.113 Hasil analisis acces nd	129
Gambar 4.114 Hasil analisis naxsi nd.....	130
Gambar 4.115 Grafik rule sqlmap nd	132
Gambar 4.116 Hasil xsser nd.....	133

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.117 Hasil xsser nd.....	134
Gambar 4.118 Grafik hasil xsser nd	136
Gambar 4.119 Hasil custom access lokal	137
Gambar 4.120 Grafik error lokal	138
Gambar 4.121 Hasil nmap vuln lokal.....	139
Gambar 4.122 Grafik nmap vuln lokal.....	140
Gambar 4.123 Hasil error.log map -A	141
Gambar 4.124 Grafik request method lokal nmap -A	142
Gambar 4.125 Hasil vuln lokal.....	142
Gambar 4.126 Hasil python Naxsi lokal	143
Gambar 4.127 Grafik jumlah rule local nmap vuln.....	145
Gambar 4.128 Jumlah zona local nmap vuln	146
Gambar 4.129 Hasil Naxsi.log vuln lokal	146
Gambar 4.130 Grafik jumlah rule.....	148
Gambar 4.131 Grafik id 1 nmap vuln.....	149
Gambar 4.132 Grafik zona vuln nmap	150
Gambar 4.133 Error run.....	151
Gambar 4.134 Isi custom access nessus.....	151
Gambar 4.135 Hasil error nessus lokal.....	152
Gambar 4.136 Nessus request method lokal	153
Gambar 4.137 Hasil Naxsi lokal nessus	153
Gambar 4.138 Grafik rule 0 nessus lokal	157
Gambar 4.139 Jumlah rule id 1 nessus scan lokal.....	158
Gambar 4.140 Grafik zona nessus lokal.....	159
Gambar 4.141 Access log penuh sql lokal.....	159

Gambar 4.142 Hasil sql map lokal	160
Gambar 4.143 Hasil Naxsi log sql map lokal.....	161
Gambar 4.144 Grafik jumlah rule sql lokal.....	163
Gambar 4.145 Jumlah zona sql map lokal.....	164
Gambar 4.146 Hasil access.log Xsser lokal	165
Gambar 4.147 Hasil error xsser lokal.....	166
Gambar 4.148 Hasil Naxsi.log xsser lokal	167
Gambar 4.149 Grafik jumlah rule xsser lokal	170
Gambar 4.150 Grafik jumlah rule xsser lokal	172
Gambar 4.151 Hasil custom log	173
Gambar 4.152 Grafik laman error	174
Gambar 4.153 Jumlah OS dan browser klien.....	175
Gambar 4.154 Hasil error.log	176
Gambar 4.155 Grafik request method	177
Gambar 4.156 Grafik jumlah host.....	178
Gambar 4.157 Hasil Naxsi log	179
Gambar 4.158 Grafik jumlah rule klien.....	181
Gambar 4.159 Jumlah zona klien.....	183

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR TABEL

Tabel 2.1 Jenis Penelitian lain	17
Tabel 4.1 Software/ <i>Tools</i>	23
Tabel 4.2 Xss skrip manual.....	49
Tabel 4.3 Xss skrip rp.....	53
Tabel 4.4 Xss skrip n	57
Tabel 4.5 Xss skrip	63
Tabel 4.6 Hasil Scan web	65
Tabel 4.7 Hasil Nssus web	67
Tabel 4.8 Hasil XSS skrip web.....	74
Tabel 4.9 Nmap hasil rp.....	76
Tabel 4.10 Nessus hasil rp	78
Tabel 4.11 Hasil xss manual rp.....	84
Tabel 4.12 Hasil Nmap vuln n.....	86
Tabel 4.13 Hasil Nessus n.....	87
Tabel 4.14 Hasil XSS input n	93
Tabel 4.15 Hasil Nmap Naxsi.....	95
Tabel 4.16 Data hasil scanning Nessus ke dalam <i>web server</i>	97
Tabel 4.17 Hasil skrip xss Naxsi	102
Tabel 4.18 Hasil custom acces rp	107
Tabel 4.19 Hasil analisis nmap rp.....	108

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.20 Hasil custom acces rp	109
Tabel 4.21 Hasil OS nmap vuln rp	110
Tabel 4.22 Hasil Nessus rp	111
Tabel 4.23 Hasil os nessus rp.....	112
Tabel 4.24 Jumlah nessus rp.....	113
Tabel 4.25 Hasil sql map rp	114
Tabel 4.26 Hasil os sqlmap rp	115
Tabel 4.27 Hasil os xsser rp.....	115
Tabel 4.28 Hasil analisis nmap-a nd.....	116
Tabel 4.29 Hasil analisis browser nmap-a nd	117
Tabel 4.30 Hasil hostname nd.....	118
Tabel 4.31 Hasil Naxsi nd.....	118
Tabel 4.32 Hasil analisis halaman error nmap-vuln nd	119
Tabel 4.33 Hasil analisis browser nmap-vuln nd.....	120
Tabel 4.34 Hasil analisis naxsi nd	122
Tabel 4.35 Hasil Zona nd.....	123
Tabel 4.36 Error nessus nd	125
Tabel 4.37 Hasil analisis browser nessus nd.....	126
Tabel 4.38 Hasil naxsi nessus nd	127
Tabel 4.39 Hasil error nd sql	129

Tabel 4.40 Hasil os sql.....	129
Tabel 4.41 Hasil rule sqlmap nd	131
Tabel 4.42 Hasil laman error nd	133
Tabel 4.43 Hasil laman nd	133
Tabel 4.44 Hasil xsser naxsi nd	135
Tabel 4.45 Hasil custom access lokal	137
Tabel 4.46 OS Lokal nmap	138
Tabel 4.47 Hasil tabel nmap vuln lokal	139
Tabel 4.48 OS vuln nmap lokal	140
Tabel 4.49 Hasil request method nmap lokal	141
Tabel 4.50 Hasil request method vuln lokal	142
Tabel 4.51 Hasil host nmap	143
Tabel 4.52 Hasil rule nmap lokal.....	144
Tabel 4.53 Hasil Naxsi nmap zona	145
Tabel 4.54 Hasil hostname.....	147
Tabel 4.55 Jumlah rule nmap vuln lokal.....	147
Tabel 4.56 Tabel rule ID 1 vuln	149
Tabel 4.57 Jumlah zona vuln	150
Tabel 4.58 Hasil error.log Nessus lokal	152
Tabel 4.59 Naxsi host nessus lokal.....	154

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Tabel 4.60 Jumlah rule id 0 Naxsi nessus.....	154
Tabel 4.61 Jumlah rule id 1 nessus lokal scan	157
Tabel 4.62 Jumlah zona nessus lokal.....	158
Tabel 4.63 Hasil metode request sqlmap	160
Tabel 4.64 Hasil IP yang diserang sql lokal.....	162
Tabel 4.65 Hasil jumlah rule sql lokal.....	162
Tabel 4.66 Jumlah zona	164
Tabel 4.67 Hasil laman error xsser lokal	165
Tabel 4.68 Hasil OS xsser.....	165
Tabel 4.69 Hasil xsser request lokal	166
Tabel 4.70 Hasil IP xsser lokal	167
Tabel 4.71 Hasil IP xsser lokal	168
Tabel 4.72 Hasil rule ID 0 xsser	168
Tabel 4.73 Hasil rule id 1 xsser lokal	170
Tabel 4.74 Hasil zona xsser lokal	172
Tabel 4.75 Hasil laman error	173
Tabel 4.76 Jumlah OS klien.....	174
Tabel 4.77 Jumlah request klien	176
Tabel 4.78 Jumlah Host klien	177
Tabel 4.79 Hasil IP yang diserang klien	179

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Tabel 4.80 Hasil rule id 0 klien.....	180
Tabel 4.81 Jumlah rule id 1 klien	182
Tabel 4.82 Jumlah rule id 2 klien	182
Tabel 4.83 Jumlah zona klien	182
Tabel 4.84 Analisis parameter penyerangan	184



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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 penduduk (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 menunjukkan 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



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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 mengoptimalkan *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 (Setiyawan, 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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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 menganalisis hasil dari *aces.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 menggunakan *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 *scanning 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*.



POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

