



**ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS
DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB
SERVER**

SKRIPSI

**HELMI HASYIM
2110511046**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
JAKARTA
2025**



**ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS
DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB
SERVER**

**HELMY HASYIM
2110511046**

Skripsi
sebagai salah satu syarat untuk melaksanakan
penelitian oleh mahasiswa pada
Program Studi Informatika

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
JAKARTA
2025**

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Helmi Hasyim

NIM : 2110511046

Tanggal : 06 Juli 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 06 Juli 2025

Yang Menyatakan

A handwritten signature in black ink is written over a red 10000 Rupiah banknote stamp and a blue official stamp. The blue stamp contains the text "B22FCAMX402450019".

Helmi Hasyim

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta,
saya yang bertanda tangan di bawah ini:

Nama : Helmi Hasyim
NIM : 2110511046
Fakultas : Ilmu Komputer
Program Studi : S-1 Informatika

Demi Pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada
Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non
eksklusif (Non – exclusive Royalty Free Right) atas skripsi saya yang berjudul:

**ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY DENGAN DDOS
DEFLATE TERHADAP SERANGAN DDOS PADA WEB SERVER**

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta
berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk
pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama
tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada tanggal: 08 Juli 2025

Yang menyatakan,



Helmi Hasyim

LEMBAR PENGESAHAN

Judul : Analisis Efektivitas Kombinasi ModSecurity OWASP CRS dan DDoS
Deflate terhadap Serangan DDoS pada Web Server
Nama : Helmi Hasyim
NIM : 2110511046
Program Studi : SI Informatika

Disetujui oleh:

Penguji 1:

I Wayan Widi Pradnyana, S.Kom, MTI.

Penguji 2:

Nurhuda Maulana, S.T., M.T.

Pembimbing 1:

Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM.

Pembimbing 2:

Hamonangan Kinantan P., S.T, M.T.

Diketahui oleh:

Koordinator Program Studi:

Dr. Widya Cholil, M.I.T.

NIP. 2211122080

Dekan Fakultas Ilmu Komputer:

Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM

NIP. 197605082003121002

Tanggal Ujian Tugas Akhir:
03 Juli 2025



ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB SERVER

HELMI HASYIM

ABSTRAK

Serangan Distributed Denial of Service (DDoS) merupakan ancaman serius yang dapat mengganggu ketersediaan layanan web server. Penelitian ini bertujuan untuk menganalisis efektivitas kombinasi ModSecurity OWASP Core Rule Set (CRS) dan DDoS Deflate dalam mendeteksi dan memitigasi serangan DDoS. Penelitian dilakukan dalam lingkungan laboratorium menggunakan tiga skenario: tanpa perlindungan, hanya dengan ModSecurity, dan kombinasi ModSecurity dengan DDoS Deflate. Metode pengujian menggunakan simulasi serangan HTTP Flood dan SYN Flood selama 10 menit, dengan pengamatan terhadap performa server melalui Prometheus, Grafana, dan tcpdump. Hasil menunjukkan bahwa skenario tanpa perlindungan menyebabkan lonjakan penggunaan CPU hingga 97% dan tingginya trafik masuk tanpa pemblokiran. Penggunaan ModSecurity saja menunjukkan perlindungan terbatas, terutama pada layer aplikasi, dengan blokir sebagian permintaan HTTP. Sementara itu, kombinasi ModSecurity dan DDoS Deflate mampu meningkatkan efisiensi mitigasi secara signifikan, dengan pemblokiran lebih dari 5 juta koneksi berbahaya dan efisiensi bandwidth HTTP Flood sebesar 87,76%. Kesimpulannya, pendekatan mitigasi berlapis terbukti lebih efektif dalam menjaga kestabilan performa server dan layak diterapkan sebagai strategi perlindungan web server dari serangan DDoS.

Kata Kunci : ModSecurity, DDoS Deflate, HTTP Flood, SYN Flood, Mitigasi.

ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB SERVER

HELMI HASYIM

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability of web server services. This study aims to evaluate the effectiveness of combining ModSecurity OWASP Core Rule Set (CRS) and DDoS Deflate in detecting and mitigating DDoS attacks. The research was conducted in a controlled laboratory environment using three scenarios: without protection, with ModSecurity alone, and with a combination of ModSecurity and DDoS Deflate. The testing involved simulated HTTP Flood and SYN Flood attacks over a duration of 10 minutes, with performance metrics observed using Prometheus, Grafana, and tcpdump. The results indicate that in the unprotected scenario, server CPU usage spiked up to 97%, accompanied by a high volume of incoming traffic without any mitigation. The implementation of ModSecurity alone provided limited protection, primarily at the application layer, by partially blocking HTTP requests. In contrast, the combined use of ModSecurity and DDoS Deflate significantly improved mitigation effectiveness, successfully blocking over 5 million malicious connections and achieving a bandwidth efficiency of 87.76% against HTTP Flood attacks. In conclusion, the layered mitigation approach demonstrated a superior ability to maintain server performance stability and is highly recommended as a strategy for protecting web servers from DDoS attacks.

Keywords: ModSecurity, Deflate DDoS, HTTP Flood, SYN Flood, Mitigation.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah SWT, karena berkat rahmat dan hidayah-Nya penulis dapat menyelesaikan skripsi yang berjudul “Analisis Efektivitas Kombinasi ModSecurity OWASP CRS Dan DDoS Deflate Terhadap Serangan DDoS Pada Web Server”. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan tugas akhir perkuliahan dan untuk memperoleh gelar Sarjana Strata 1 di Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. Selain itu, skripsi ini juga merupakan bentuk penerapan dari ilmu yang penulis peroleh selama studi di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.

Terselesaikannya skripsi ini tidak lepas dari dukungan, bimbingan, dan masukan dari berbagai pihak. Untuk itu, dengan penuh rasa terima kasih, penulis menyampaikan penghargaan sebesar-besarnya kepada:

- a. Allah SWT. yang telah memberikan karunia, rahmat, rezeki, nikmat sehat, dan hidayah-Nya selama penelitian ini berlangsung.
- b. Ayah dan Ibu, yang selalu menjadi sumber inspirasi, doa, serta dukungan terbesar bagi penulis.
- c. Bapak Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM, sebagai Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta, serta sekaligus sebagai dosen pembimbing pertama yang telah memberikan dan membimbing peneliti sekaligus menjadi sosok yang menginspirasi peneliti untuk meneliti topik skripsi yang diangkat.
- d. Ibu Dr. Widya Cholil, S.Kom., M.I.T, selaku Koordinator Program Studi Informatika dan jajarannya yang telah memfasilitasi dan mendukung kelancaran proses penyelesaian skripsi penelitian ini.
- e. Bapak Hamonangan Kinantan Prabu, S.T, M.T. selaku dosen pembimbing kedua, yang telah meluangkan waktu untuk membantu penulis dalam melakukan penelitian dan memberikan masukan serta saran kepada

penulis dalam segi penulisan, maupun teknis proses penyusunan skripsi penelitian ini.

- f. Bapak Indra Permana Solihin, S.Kom, M.Kom., selaku dosen pembimbing akademik yang telah memberikan dukungan dalam proses penulisan ini.
- g. Saudara dan rekan-rekan penulis yang selalu memberikan dukungan dan bantuan dalam setiap langkah penulisan skripsi ini.
- h. Raisha Bianca Putri Bagus, Nayla Zayyannafisah Abida, dan Esterlita Nugraheni Praharningtyas atas izin dan kepercayaan yang diberikan kepada penulis untuk menggunakan proyek web “Portal Layanan Akademik” sebagai objek penelitian dalam tugas akhir ini. Izin dan kontribusi tersebut sangat berarti dalam keberhasilan proses pengujian dan pengambilan data.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis dengan senang hati menerima kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat dan kontribusi positif bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan jaringan.

Jakarta, 2 Mei 2025



Helmi Hasyim

DAFTAR ISI

PERNYATAAN ORISINALITAS.....	i
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
ABSTRACT.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN	xiii
DAFTAR PERSAMAAN	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan dan Manfaat Penelitian	4
1.5. Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA.....	7
2.1. OSI Model.....	7
2.1.1. Layer 7: Protokol Aplikasi	9
2.1.2. Layer 4 dan 3: Protokol Transport dan Jaringan	10
2.2. <i>Server</i>	11
2.2.1. Sistem Operasi Server	12
2.2.2. <i>Databases Server</i>	13
2.2.3. <i>Web Server</i>	15
2.3. Serangan Keamanan Web Server	16
2.4. <i>Distributed Denial of Service (DDoS)</i>	16

2.5.	DDoS Tools	20
2.6.	Sistem Keamanan Server	21
2.6.1.	Firewall	22
2.6.2.	<i>Web Application Firewall</i>	24
2.6.3.	ModSecurity OWASP Core Rule Set	25
2.6.4.	DDoS Deflate	26
2.6.5.	Monitoring Sistem dan Visualisasi.....	27
2.6.6.	Wafw00f.....	28
2.7.	Penelitian Terdahulu.....	29
BAB III	METODE PENELITIAN	33
3.1.	Tahapan Penelitian	33
3.1.1.	Identifikasi Masalah	33
3.1.2.	Pendefinisian Solusi	35
3.1.3.	Studi Literatur	35
3.1.4.	Perancangan Sistem	36
3.1.5.	Kebutuhan Sistem	37
3.1.6.	Pengujian Sistem.....	38
3.1.7.	Analisis Hasil	42
3.1.8.	Pembuatan Laporan.....	44
3.2.	Alat dan Bahan Penelitian.....	44
3.3.	Jadwal Penelitian.....	45
BAB IV	HASIL DAN PEMBAHASAN	47
4.1.	Profil Perusahaan	47
4.2.	Pemodelan dan Implementasi Sistem Mitigasi	48
4.2.1.	Arsitektur Sistem Mitigasi	48
4.2.2.	Alur Logika Mitigasi Serangan.....	49

4.2.3.	Konfigurasi ModSecurity OWASP CRS.....	50
4.2.4.	Konfigurasi DDoS Deflate.....	52
4.2.5.	Konfigurasi Log <i>tcpdump</i>	54
4.2.6.	Alur Monitoring dan Collecting Metric	55
4.3.	Metode Serangan dalam Pengujian Sistem Mitigasi.....	57
4.4.	Skenario Pengujian dan Hasil	58
4.4.1.	Skenario 1 Tanpa Perlindungan.....	58
4.4.2.	Skenario 2 Menggunakan ModSecurity.....	59
4.4.3.	Skenario 3 Kombinasi ModSecurity + DDoS Deflate	60
4.5.	Analisis Hasil	60
4.5.1.	Analisis Metrik Performa.....	60
4.5.2.	Analisis Log Keamanan	63
4.5.3.	Analisis Perbandingan dan Efektivitas Mitigasi	69
4.5.4.	Analisis Efisiensi Bandwith	72
4.6.	Rekomendasi Hasil.....	74
BAB V	PENUTUP.....	75
5.1.	Kesimpulan	75
5.2.	Saran.....	75
	DAFTAR PUSTAKA.....	77
	LAMPIRAN.....	80

DAFTAR GAMBAR

Gambar 2.1 OSI Model Layer.....	7
Gambar 2.2 Application Layer.....	9
Gambar 2.3 Transport Layer	10
Gambar 2.4 Network Layer	11
Gambar 2.5 SYN Flood Attack Example.....	17
Gambar 2.6 Proses Terjadinya SYN Flood	18
Gambar 2.7 HTTP Flood attack example	18
Gambar 2.8 Alur serangan Get Flood	19
Gambar 2.9 Cara kerja ModSecurity	25
Gambar 2.10 Alur diagram DDos Deflate.....	26
Gambar 3.1 Flow diagram penelitian.....	33
Gambar 3.2 Portal Layanan Akademik	33
Gambar 3.3 Pengujian WAF menggunakan Wafw00f	34
Gambar 3.4 Topologi Simulasi Lab	36
Gambar 3.5 Topologi Jaringan simulasi serangan dan Mitigasi DDoS	39
Gambar 3.6 Flow diagram pengujian serangan	41
Gambar 4.1 Arsitektur sistem Mitigasi DDoS	48
Gambar 4.2 Alur Logika Mitigasi DDoS	49
Gambar 4.3 Alur pengambilan data	56
Gambar 4.4 Perintah Serangan HTTP Flood	57
Gambar 4.5 Script hping3	57
Gambar 4.6 Log SYN Flood Skenario 3	65
Gambar 4.7 HTTP Flood Skenario 2	67
Gambar 4.8 SYN Flood Skenario 2	68
Gambar 4.9 HTTP Flood Skenario 3	68
Gambar 4.10 SYN Flood Skenario 3	69
Gambar 4.11 Diagram Rata- Rata CPU	70
Gambar 4.12 Diagram Rata-Rata RAM.....	70
Gambar 4.13 Diagram Response Time	71
Gambar 4.14 Diagram Total Serangan Vs Diblokir	72

DAFTAR TABEL

Tabel 2.1 Ringkasan Penelitian Terdahulu	29
Tabel 3.1 Skenario Serangan DDoS	38
Tabel 3.2 Perangkat Serangan	44
Tabel 3.2 Jadwal Kegiatan	45
Tabel 4.1 Parameter DDoS Deflate	52
Tabel 4.2 Hasil Pengujian Skenario 1 (Tanpa Perlindungan)	59
Tabel 4.3 Hasil Pengujian Skenario 2	59
Tabel 4.4 Hasil Pengujian Skenario 3	60
Tabel 4.5 Rekapitulasi Metrik Performa pada Tiga Skenario	61
Tabel 4.6 Total Bandwith Setiap Skenario Serangan	73

DAFTAR LAMPIRAN

Lampiran 1. Skenario1 HTTP Flood.....	80
Lampiran 2. Skenario1 SYN Flood.....	80
Lampiran 3. Skenario2 HTTP Flood.....	80
Lampiran 4. Skenario2 SYN Flood.....	81
Lampiran 5. Skenario3 HTTP Flood.....	81
Lampiran 6. Skenario3 SYN Flood.....	81
Lampiran 7. DDoS Config	82
Lampiran 8. Hasil Wawancara	83
Lampiran 9. Bukti Wawancara.....	84

DAFTAR PERSAMAAN

(3.1) Persamaan Efisiensi.....	43
--------------------------------	----