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

HELMI 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

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	:	S1 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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PERSAMAAN