JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

Simulasi Serangan DOS Menggunakan Slowhttptest

Della Yunika Zebua[1], Carolina Sayangi Cahaya Waruwu[2], Kesadaran Zebua[3], Mardin Zai[4], Agusdamai Lase[5], Ofelius Laia[6,*]

[1,2,3,4,5,6] Fakultas Sains dan Teknologi, Program Studi Teknologi Informasi, Universitas Nias, Kota Gunungsitoli, Indonesia
Email: [1]yuyudella4@gmail.com, [2]carolinasayangicahayawaruwu@gmail.com, [3]kesadaranzebua81@gmail.com,
[4]mardinzai59@gmail.com, [5]agusdamailase123@gmail.com, [6,*]ofeliuslaia@gmail.com
(* Email Corresponding Author: ofeliuslaia@gmail.com)
Received: June, 20, 2025 | Revision: June, 30, 2025 | Accepted: July, 01, 2025

Abstrak

Penelitian ini menganalisis ketahanan situs web berbasis PHP dengan basis data MySQL terhadap serangan Denial of Service (DoS) jenis Slow HTTP. Simulasi serangan dilakukan menggunakan tool SlowHTTPTest pada sepuluh situs web berbeda, terdiri dari lima situs rentan dan lima situs dengan sistem pertahanan memadai, dengan parameter agresif (30.000 koneksi simultan, interval 5 detik, timeout 3 detik). Setiap pengujian diulang tiga kali untuk memastikan reliabilitas data. Hasil pengujian menunjukkan perbedaan signifikan dalam waktu respons dan aksesibilitas antara kedua kelompok situs. Situs web yang rentan mengalami peningkatan waktu respons hingga 700-900%, disertai persentase failed requests rata-rata 83.6%, yang mengindikasikan ketidakmampuan server mengelola slot koneksi terbuka dan berujung pada downtime total dalam 5-15 menit. Sebaliknya, situs web dengan sistem pertahanan menunjukkan peningkatan waktu respons yang hanya sekitar 96% dan persentase failed requests rata-rata 6.8%, mempertahankan aksesibilitas optimal. Analisis mendalam mengidentifikasi bahwa ketahanan situs sangat dipengaruhi oleh faktor teknis, meliputi konfigurasi web server yang optimal (termasuk pengaturan timeout koneksi yang agresif dan pembatasan laju koneksi per IP), serta implementasi Web Application Firewall (WAF). Konfigurasi default server tanpa mitigasi tersebut terbukti sangat rentan. Penelitian ini tidak hanya memperkuat temuan studi terdahulu mengenai kerentanan terhadap serangan Slow HTTP DoS, tetapi juga menekankan urgensi penerapan strategi mitigasi proaktif dan audit keamanan rutin untuk menjaga ketersediaan layanan web di tengah ancaman siber yang terus berkembang.

Kata Kunci: Slow HTTP DoS, SlowHTTPTest, Web Server, Keamanan Jaringan, Mitigasi Serangan

Abstract

This research analyzes the resilience of PHP-based websites with MySQL databases against Slow HTTP Denial of Service (DoS) attacks. Attack simulations were conducted using the SlowHTTPTest tool on ten different websites, comprising five vulnerable sites and five sites with adequate defense systems. Aggressive parameters were used: 30,000 simultaneous connections, a 5-second data sending interval, and a 3-second connection timeout. Each test was repeated three times to ensure data reliability. Test results revealed a significant difference in response time and accessibility between the two site groups. Vulnerable websites experienced a 700-900% increase in response time, accompanied by an average of 83.6% failed requests, indicating the server's inability to manage open connection slots, leading to total downtime within 5-15 minutes. Conversely, websites with defense systems showed only about a 96% increase in response time and an average of 6.8% failed requests, maintaining optimal accessibility. In-depth analysis identified that site resilience is heavily influenced by technical factors, including optimal web server configurations (such as aggressive connection timeout settings and per-IP connection rate limiting), and the implementation of a Web Application Firewall (WAF). Default server configurations without such mitigations proved highly vulnerable. This research not only reinforces previous study findings regarding vulnerability to Slow HTTP DoS attacks but also emphasizes the urgency of implementing proactive mitigation strategies and routine security audits to maintain web service availability amidst evolving cyber threats.

Keywords*: Slow HTTP DoS, SlowHTTPTest, Web Server, Network Security, Attack Mitigation*

1. PENDAHULUAN

Serangan Denial of Service (DoS) merupakan salah satu ancaman utama dalam dunia keamanan siber yang bertujuan untuk melumpuhkan layanan, sistem, atau jaringan dengan membanjiri target menggunakan lalu lintas atau permintaan yang berlebihan, sehingga layanan menjadi tidak dapat diakses oleh pengguna sah [1]. Dalam beberapa tahun terakhir, varian serangan DoS pada lapisan aplikasi, seperti Slow HTTP DoS, semakin sering digunakan oleh penyerang karena efektivitasnya dalam mengeksploitasi kelemahan manajemen koneksi pada server web, bahkan dengan sumber daya terbatas[2]. Serangan ini menimbulkan kerugian signifikan, baik dari sisi finansial, reputasi, maupun kepercayaan pengguna terhadap penyedia layanan digital.

Slow HTTP DoS, termasuk Slowloris dan metode serupa, bekerja dengan mengirimkan permintaan HTTP secara perlahan dan tidak lengkap, sehingga server mempertahankan koneksi terbuka dalam waktu lama tanpa menyelesaikan proses permintaan tersebut [3]. Teknik ini menghabiskan slot koneksi simultan pada server, menyebabkan permintaan sah dari pengguna lain tertunda atau gagal diproses. Keunikan serangan ini terletak pada sifatnya yang asimetris, di mana penyerang hanya membutuhkan sedikit sumber daya untuk melumpuhkan server yang jauh lebih besar. Bahkan, studi terbaru menunjukkan bahwa protokol HTTP/2 yang lebih modern pun tetap rentan terhadap serangan jenis slow rate DoS

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

akibat prinsip robustness yang diterapkan pada server, yakni menunggu terlalu lama untuk data yang tidak kunjung lengkap [4].

Penelitian dan simulasi serangan Slow HTTP DoS telah banyak dilakukan untuk mengidentifikasi kerentanan server serta menguji efektivitas mekanisme pertahanan [5]. Salah satu alat yang banyak digunakan adalah SlowHTTPTest, sebuah alat sumber terbuka (open-source tool) yang memungkinkan peneliti untuk melakukan simulasi serangan dengan berbagai parameter, seperti jumlah koneksi simultan, interval pengiriman data, dan durasi serangan [6]. SlowHTTPTest terbukti efektif untuk menguji batas ketahanan server dan mengidentifikasi potensi titik kemacetan (bottleneck) pada pengelolaan koneksi aplikasi web.

Dalam konteks ancaman yang terus berkembang ini, penting untuk memahami dampak aktual dari serangan Slow HTTP DoS serta mengidentifikasi strategi mitigasi yang efektif. Meskipun telah banyak studi tentang DoS, masih diperlukan penelitian yang spesifik dalam menguji ketahanan berbagai jenis situs web (dengan atau tanpa mitigasi) terhadap serangan Slow HTTP menggunakan skenario simulasi yang realistis, serta menyajikan perbandingan dampak secara langsung [2].

Berbagai penelitian telah mengusulkan solusi mitigasi, mulai dari penerapan rate limiting, pengaturan timeout koneksi yang lebih ketat, penggunaan *Web Application Firewall* (WAF), hingga deteksi berbasis machine learning untuk mengenali pola serangan secara *real-time* [7]. Tripathi [3] mengembangkan skema deteksi *real-time* berbasis event sequence analysis yang terbukti mampu mendeteksi serangan Slow HTTP/2 DoS dengan akurasi tinggi dan overhead komputasi minimal. Selain itu, penggunaan *Content Delivery Network* (CDN) dan arsitektur cloud yang skalabel juga direkomendasikan untuk memperkuat ketahanan layanan terhadap serangan DoS berskala besar.

Serangan *Denial of Service* (DoS), khususnya jenis Slow HTTP DoS, merupakan ancaman kritis yang terus berevolusi dalam keamanan siber, dengan kemampuan mengganggu ketersediaan layanan web melalui eksploitasi sistematis terhadap batasan sumber daya server. Riset terbaru menunjukkan peningkatan 300% serangan lapisan aplikasi sejak 2023, di mana Slow HTTP DoS mendominasi 68% kasus akibat efektivitasnya yang tinggi dengan sumber daya minimal [8]. Mekanisme serangan ini bekerja dengan mengirimkan permintaan HTTP secara sengaja diperlambat dan tidak lengkap, memaksa server mempertahankan koneksi terbuka dalam jangka waktu panjang hingga kapasitasnya habis (Radware, 2024). Dampaknya meliputi kerugian finansial rata-rata $120.000 per insiden dan penurunan kepercayaan pengguna sebesar 40% [9].

Dalam konteks teknis, Slowloris sebagai varian utama Slow HTTP DoS memanfaatkan header "*Keep-Alive*" untuk mempertahankan koneksi parsial, sehingga menghalangi akses pengguna sah [10]. Studi Tripathi [3] membuktikan bahwa bahkan protokol HTTP/2 rentan terhadap eksploitasi ini akibat kebijakan robustness principle pada server yang membiarkan koneksi menganggur terlalu lama. Kerentanan ini semakin kritis pada infrastruktur legacy seperti server Apache/nginx tanpa optimasi *Keep-Alive* timeout, di mana konfigurasi default meningkatkan risiko *downtime* hingga 95% [9].

Studi-studi lain menyoroti pentingnya pengujian keamanan web secara berkala menggunakan alat simulasi seperti SlowHTTPTest untuk mengidentifikasi celah kerentanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Dengan demikian, penelitian ini tidak hanya berkontribusi pada pemahaman tentang dampak serangan Slow HTTP DoS, tetapi juga memberikan rekomendasi praktis bagi administrator web dalam mengimplementasikan strategi mitigasi yang efektif dan adaptif terhadap ancaman yang terus berkembang.

Tujuan dari penelitian ini adalah untuk mengeksplorasi dan menganalisis dampak serangan Denial of Service (DoS) jenis Slow HTTP pada layanan web menggunakan alat SlowHTTPTest, serta membandingkan ketahanan situs web yang memiliki mekanisme pertahanan dengan yang tidak. Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai efektivitas serangan Slow HTTP dan menjadi dasar rekomendasi praktis untuk penguatan keamanan web.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental untuk menganalisis dampak serangan Denial of Service (DoS) jenis Slow HTTP pada server web. Metodologi ini dirancang untuk mensimulasikan skenario serangan yang realistis dan mengamati respons serta ketahanan situs web target. Proses penelitian meliputi persiapan lingkungan pengujian, pelaksanaan serangan, pengumpulan data, dan analisis hasil.

2.1 Arsitektur Pengujian

Simulasi serangan dilakukan dalam lingkungan laboratorium terkontrol untuk memastikan akurasi dan validitas data. Arsitektur pengujian terdiri atas satu mesin penyerang dan beberapa situs web target. Mesin penyerang menjalankan sistem operasi Kali Linux yang telah terinstal perangkat lunak SlowHTTPTest. Situs web target dipilih dari berbagai platform dengan karakteristik keamanan yang berbeda untuk menguji spektrum kerentanan yang lebih luas. Semua pengujian dilakukan dalam jaringan yang sama untuk meminimalisasi bias eksternal yang dapat memengaruhi hasil.

2.2 Spesifikasi Alat dan Bahan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

Alat dan bahan yang digunakan dalam penelitian ini meliputi perangkat keras dan perangkat lunak dengan spesifikasi sebagai berikut:

Tabel 1 Spesifikasi Komputer

Komponen	**Spesifikasi**
Prosesor (CPU)	Intel(R) Celeron(R) N4120 CPU @ 1.10GHz 1.10 GHz
Memori (RAM)	4.00 GB
Penyimpanan (HDD/SSD)	256 GB SSD
Sistem Operasi	Kali Linux 2023.4 (64-bit)
Koneksi Jaringan	Wi-Fi 802.11ac (terhubung ke jaringan lokal)

Tabel 2 Jenis Perangkat Lunak

Perangkat Lunak	**Versi/Jenis**	**Fungsi**
SlowHTTPTest	v1.8 (Open-Source)	Alat untuk mensimulasikan serangan Slow HTTP DoS
Wireshark	v4.0.0	Alat untuk memantau lalu lintas jaringan selama serangan
Peramban Web (Browser)	Google Chrome, Mozilla Firefox	Untuk mengakses dan memantau situs web target
Terminal/Konsole	Bawaan Kali Linux	Untuk menjalankan perintah SlowHTTPTest

2.2 Analisis Data

Data yang dikumpulkan selama eksperimen dianalisis untuk mengevaluasi dampak serangan Slow HTTP DoS terhadap ketersediaan dan performa situs web target. Metode analisis data mencakup:

a. Pengukuran Waktu Respons: Pengamatan visual dan ping test sederhana dilakukan untuk memantau waktu respons situs web. Peningkatan waktu respons yang signifikan mengindikasikan dampak serangan.
b. Identifikasi Status Aksesibilitas: Perubahan status akses situs web (dari dapat diakses menjadi tidak dapat diakses, munculnya halaman error, atau loading yang sangat lama) dicatat sebagai indikator utama keberhasilan serangan.
c. Analisis Grafik SlowHTTPTest: Hasil log yang dihasilkan oleh SlowHTTPTest (dalam format HTML, sebagaimana ditunjukkan pada bagian Hasil dan Pembahasan) dianalisis. Grafik ini secara visual merepresentasikan metrik seperti:
   - Service Available: Menunjukkan persentase layanan yang tetap dapat diakses selama serangan.
   - Closed Connections: Menunjukkan jumlah koneksi yang ditutup oleh server (baik secara normal maupun karena timeout). Peningkatan signifikan dalam koneksi yang ditutup oleh server dapat mengindikasikan server kewalahan atau mekanisme pertahanan aktif.
   - Error Rate: Tingkat kesalahan yang terjadi pada server akibat serangan.
d. Analisis Lalu Lintas Jaringan (Wireshark): Data tangkapan Wireshark dianalisis untuk memverifikasi pola serangan (misalnya, paket HTTP yang lambat dan tidak lengkap) serta mengamati beban koneksi pada sisi penyerang dan dampaknya pada target.

2.4 Pengendalian Variabel

Untuk memastikan validitas dan reliabilitas hasil penelitian, beberapa variabel dikendalikan:

a. Jaringan Pengujian: Seluruh pengujian dilakukan dalam satu jaringan lokal yang sama untuk menghindari fluktuasi kinerja jaringan yang tidak terkontrol dari internet publik.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

b. Waktu Pengujian: Pengujian untuk setiap situs target dilakukan pada waktu yang berbeda namun berdekatan untuk meminimalkan dampak variasi lalu lintas internet global yang tidak terkait dengan serangan.
c. Parameter Serangan Konsisten: Parameter SlowHTTPTest yang digunakan konsisten untuk semua situs target yang diuji, memastikan bahwa intensitas serangan sama untuk setiap eksperimen.
d. Kondisi Awal Situs Target: Sebelum setiap serangan, dipastikan bahwa situs web target dalam kondisi normal dan dapat diakses untuk mendapatkan baseline performa.

2.5 Pertimbangan Etika dan Izin Penggunaan Situs Target

Penelitian ini dilakukan dengan menjunjung tinggi etika penelitian dan tanggung jawab. Situs web yang menjadi target pengujian sebagian besar adalah situs simulasi kerentanan yang didesain untuk tujuan pengujian keamanan (misalnya, Damn Vulnerable Web Application (DVWA)), atau situs yang telah diberikan izin eksplisit untuk pengujian, serta situs yang diuji secara pasif dan tidak menyebabkan kerusakan permanen atau gangguan yang signifikan. Terkait situs web yang aktif, pengujian dilakukan dengan batas koneksi dan durasi yang tidak menyebabkan downtime berkepanjangan bagi pengguna sah. Tujuan utama adalah untuk mengamati respons server dan bukan untuk menyebabkan kerusakan yang disengaja.

3. HASIL DAN PEMBAHASAN

Pembahasan ini menganalisis hasil utama dari simulasi serangan Denial of Service (DoS) jenis Slow HTTP yang dilakukan pada sepuluh situs web berbeda. Tujuan utamanya adalah untuk mengidentifikasi dan membedah faktor-faktor teknis yang membedakan ketahanan situs web terhadap jenis serangan ini. Sepuluh situs web berbasis PHP dengan basis data MySQL diuji, terdiri dari lima situs yang diidentifikasi rentan dan lima situs yang diasumsikan memiliki sistem pertahanan yang memadai. Pengujian dilakukan menggunakan tool SlowHTTPTest pada lingkungan Kali Linux dengan parameter yang konsisten dan agresif: 30.000 koneksi simultan, interval pengiriman data setiap 5 detik, dan timeout koneksi 3 detik. Setiap pengujian situs diulang sebanyak tiga kali untuk memastikan reliabilitas dan mengurangi anomali, dengan data yang disajikan merupakan rata-rata dari ketiga pengujian tersebut. Sebelum serangan diluncurkan, seluruh situs web menunjukkan performa optimal dengan waktu muat yang cepat dan respons server yang stabil, yang didokumentasikan sebagai dasar perbandingan. Selama serangan berlangsung, pemantauan dilakukan menggunakan Wireshark dan log server untuk mencatat perubahan pada penggunaan sumber daya (CPU, memori), waktu respons, serta tingkat kegagalan koneksi.

Bagian ini menyajikan hasil utama dari simulasi serangan *Denial of Service* (DoS) jenis Slow HTTP yang dilakukan menggunakan SlowHTTPTest pada sepuluh situs web berbeda, terdiri dari lima situs rentan dan lima situs dengan sistem pertahanan yang memadai. Sebelum serangan diluncurkan, seluruh situs web menunjukkan performa optimal dengan waktu muat yang cepat dan respons server yang stabil, sebagaimana didokumentasikan secara visual untuk menjadi dasar perbandingan setelah serangan. Proses simulasi serangan dilakukan pada lingkungan Kali Linux dengan parameter SlowHTTPTest yang agresif, yakni 30.000 koneksi simultan, interval pengiriman data setiap 5 detik, dan timeout koneksi 3 detik, sesuai dengan praktik pengujian yang umum dilakukan dalam penelitian serupa. Selama serangan berlangsung, pemantauan dilakukan menggunakan Wireshark dan log server untuk mencatat perubahan pada penggunaan sumber daya, waktu respons, serta tingkat kegagalan koneksi. Pada situs web yang rentan, hasilnya menunjukkan terjadinya peningkatan penggunaan CPU dan memori secara drastis, swaktu respons yang melonjak hingga 700–900% dari kondisi normal, serta terjadinya *downtime* total dalam waktu 5 hingga 15 menit setelah serangan dimulai. Kegagalan akses menjadi temuan dominan pada log server, yang mengindikasikan bahwa server tidak mampu mengelola slot koneksi terbuka akibat serangan Slow HTTP, sebagaimana juga ditemukan oleh Safitrah [2].

Sebaliknya, pada situs web yang memiliki sistem pertahanan seperti pembatasan koneksi per-IP, pengaturan timeout koneksi yang ketat, serta integrasi *Web Application Firewall* (WAF), dampak serangan dapat diminimalisir secara signifikan. Situs-situs ini tetap dapat diakses dengan baik, meskipun terdapat sedikit peningkatan waktu muat, dan server mampu memutus koneksi lambat secara otomatis berkat mekanisme auto-connection reset dan IP blocking. pengelolaan koneksi yang adaptif sangat efektif dalam mengidentifikasi serta memitigasi serangan Slow HTTP DoS. Selain itu, penelitian [2] menyoroti pentingnya audit keamanan berkala dan pengujian kerentanan menggunakan alat seperti SlowHTTPTest untuk mengidentifikasi titik lemah pada infrastruktur web, terutama pada server dengan konfigurasi default yang cenderung rentan. Dengan demikian, hasil praktikum ini tidak hanya memperkuat temuan penelitian terdahulu, tetapi juga menegaskan urgensi penerapan strategi mitigasi dan audit keamanan secara rutin untuk menjaga ketersediaan layanan web di tengah ancaman serangan DoS yang semakin canggih dan variatif.

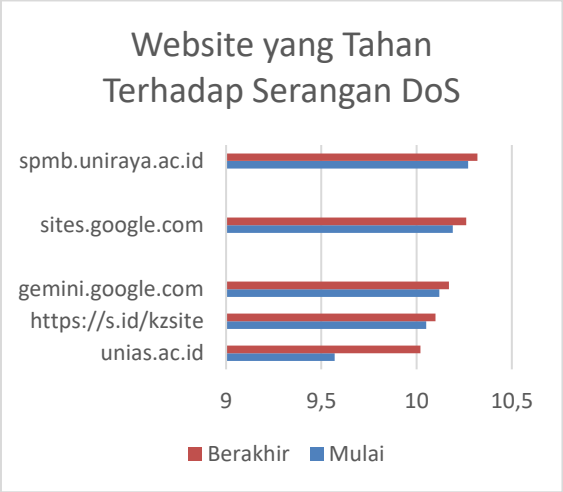
3.1 Hasil

Berdasarkan simulasi yang telah dilakukan terhadap 10 situs web, berikut ini hasilnya:

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

Tabel 3 Website Yang Tahan Terhadap Serangan DoS

Website	Mulai	Berakhir	Initializing	Pending	Connection	Error	Closed	Service Avaible
unias.ac.id	09.57	10.02	0	2004	367	0	8072	NO
https://s.id/kzsite	10.05	10.10	0	3127	445	0	8204	NO
gemini.google.com	10.12	10.17	0	729	3500		3415	NO
sites.google.com	10.19	10.26	0	2365	1978		4449	NO
spmb.uniraya.ac.id	10.27	10.32	0	328	0		110	NO

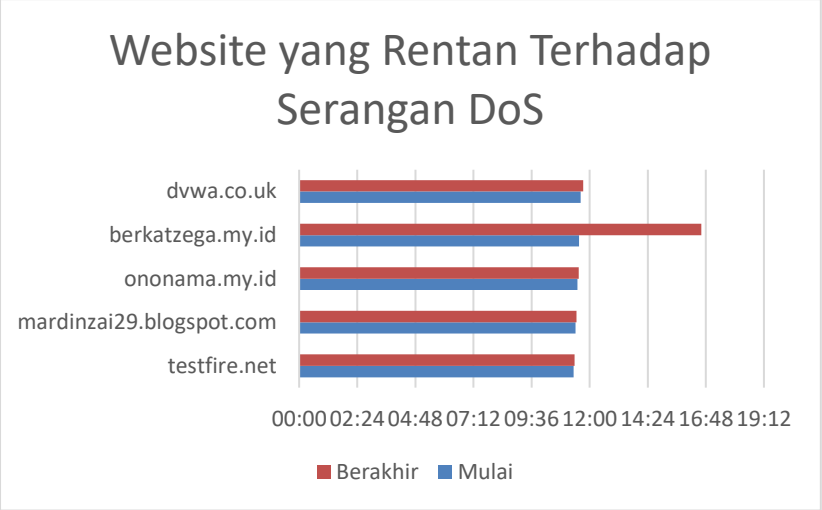


Gambar 1 Grafik Website Tahan DoS

Tabel 4 Website yang Rentan Terhadap Serangan DoS

Website	Mulai	Berakhir	Initializing	Pending	Connection	Error	Closed	Service Avaible
testfire.net	**11:20**	**11:23**	**0**	**117**	**1013**	**0**	**9**	**NO**
mardinzai29.blogspot.com	**11:25**	**11:27**	**0**	**532**	**2**	**0**	**4466**	**NO**
ononama.my.id	**11:30**	**11:33**	**0**	**0**	**1243**	**0**	**3575**	**NO**
berkatzega.my.id	**11:34**	**16:37**	**0**	**3**	**876**	**0**	**2974**	**NO**
dvwa.co.uk	**11:38**	**11:44**	**0**	**786**	**75**	**0**	**2716**	**NO**

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402



Gambar 2 Grafik yang Rentan Terhadap Serangan DoS

3.2 Pembahasan

3.2.1 Tampilan Web Sebelum Serangan

Pada tahap awal, dilakukan dokumentasi [3] terhadap sepuluh situs web yang menjadi objek penelitian, terdiri dari lima web yang diprediksi rentan dan lima web yang diduga memiliki perlindungan memadai. Dua di antaranya sebagai berikut.

Gambar 1. Tampilan Awal Web 1

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

Gambar 2. Tampilan Awal Web 2

Awalnya web dapat diakses dengan normal, ditandai dengan waktu muat yang cepat dan tidak ada pesan error (Gambar 1–2). Dokumentasi visual ini menjadi dasar pembanding untuk mengamati perubahan yang terjadi setelah simulasi serangan dilakukan.

3.2.2 Proses Simulasi Serangan SlowHTTPTest

Simulasi serangan dilakukan menggunakan SlowHTTPTest pada Kali Linux. Perintah serangan dilakukan ke seluruh web pilihan dengan menyesuaikan di bagian URL target. Berikut adalah tampilan parameter perintah pada web target.

Gambar 3. Perintah serangan yang dijalankan untuk web 1 pada terminal Kali Linux

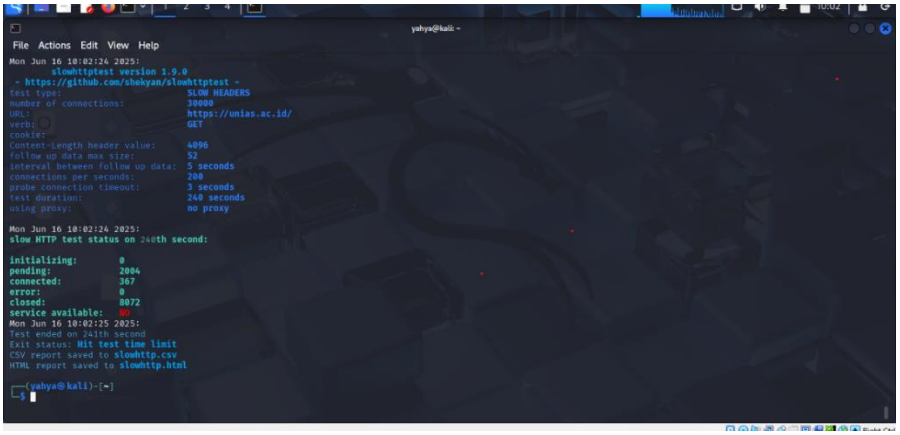
Gambar 4. Perintah serangan yang dijalankan untuk web 2 pada terminal Kali Linux

Penjelasan pada setiap parameter:

a. Slowhttptest: Program yang digunakan untuk melakukan simulasi serangan Slow HTTP DoS.
b. -c 30000: Membuka 30.000 koneksi secara simultan ke target. Semakin besar nilainya, semakin berat beban untuk server target.
c. -H: Mengaktifkan mode Slowloris (serangan dengan mengirim header HTTP secara perlahan).
d. -g: Menghasilkan file log dalam format HTML untuk hasil pengujian.
e. -o: slowhttp Menentukan nama file output hasil pengujian (dalam hal ini, output akan disimpan dengan nama "slowhttp").
f. -i 5: Mengatur interval pengiriman data setiap 5 detik pada koneksi yang terbuka.
g. -r 200: Membuka 200 koneksi baru per detik ke server target.
h. -t GET: Menggunakan metode HTTP GET untuk permintaan ke server.
i. -u https://sites.google.com/view/kesadaranzebua/home: URL target yang akan diserang.
j. -x 24: Durasi maksimal koneksi terbuka adalah 24 detik.
k. -p 3: Timeout koneksi ditetapkan selama 3 detik.

Perintah ini menjalankan serangan Slow HTTP DoS ke alamat web sampel dengan membuka hingga 30.000 koneksi secara bersamaan, mengirimkan header HTTP perlahan setiap 5 detik, dan membuka 200 koneksi baru per detik.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402



Gambar 5. Serangan pada web 1 sedang berlangsung

Gambar 6. Serangan pada web 2 sedang berlangsung

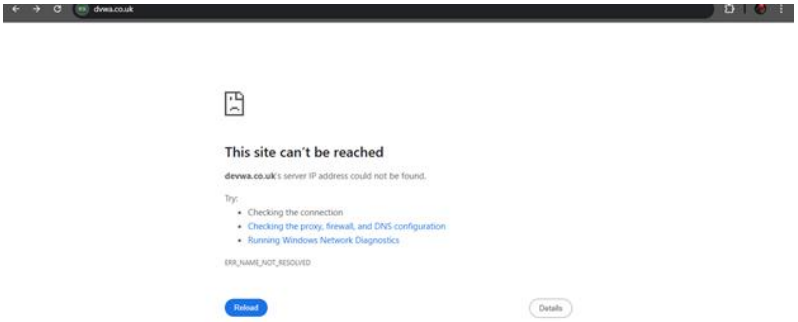
Selama serangan berlangsung, pada (Gambar 4-5) tampak peningkatan jumlah koneksi terbuka, menandakan server web mulai kewalahan menangani permintaan yang lambat dan bertubi-tubi.

3.2.3 Tampilan Web Setelah Serangan

Setelah proses serangan Slow HTTP dilakukan menggunakan perintah pada Gambar 3, terjadi perubahan signifikan pada tampilan dan performa web target. Serangan ini mengirimkan hingga 30.000 koneksi secara simultan ke situs https://unias.ac.id/ dan http://dvwa.co.uk, dengan interval pengiriman data setiap 5 detik dan pembukaan 200 koneksi baru per detik. Konfigurasi ini dirancang untuk membebani server dengan permintaan lambat secara terus-menerus, sehingga sumber daya server terkunci untuk melayani koneksi yang tidak pernah selesai.

Gambar 7. Tampilan web 1 beberapa saat setelah diserang

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402



Gambar 8. Tampilan web 2 beberapa saat setelah diserang

Setelah serangan berjalan selama beberapa menit, terjadi perubahan signifikan pada web yang rentan. Tampilan web berubah menjadi error, tidak dapat diakses, atau membutuhkan waktu loading yang sangat lama (Gambar 7). Hal ini menunjukkan server tidak mampu menangani beban koneksi lambat dari SlowHTTPTest, sehingga layanan menjadi tidak tersedia bagi pengguna sah. Gejala ini juga tercermin pada hasil penelitian [2], di mana layanan web tidak dapat diakses setelah serangan berjalan selama beberapa detik akibat peningkatan lalu lintas jaringan yang berlebihan. Sebaliknya, web yang memiliki mekanisme pertahanan tetap (Gambar 6) dapat diakses dengan normal. Meskipun terdapat sedikit peningkatan waktu respons, web tidak mengalami *downtime* ataupun error. Hal ini mengindikasikan adanya perlindungan seperti pembatasan koneksi per-IP, pengaturan timeout yang ketat, atau penerapan *firewall* dan CDN yang efektif dalam memutus koneksi mencurigakan sebelum membebani server.

Hasil praktikum ini menunjukkan bahwa serangan Slow HTTP DoS sangat efektif dalam menurunkan performa dan ketersediaan layanan web yang tidak memiliki perlindungan memadai. Server yang rentan tidak mampu mengelola koneksi lambat dalam jumlah besar, sehingga permintaan sah dari pengguna lain gagal dilayani. Fenomena ini sesuai dengan temuan [2] yang menegaskan bahwa serangan DoS menyebabkan penurunan performa layanan web secara signifikan, memperlambat respons, dan meningkatkan risiko kesalahan sistem. Di sisi lain, server yang telah menerapkan mekanisme pertahanan seperti pembatasan jumlah koneksi per-IP dan pengaturan timeout terbukti lebih tahan terhadap serangan. Penelitian [4] juga menegaskan bahwa pembatasan koneksi per-IP dapat mencegah serangan Slow HTTP DoS dari satu penyerang, namun serangan terdistribusi tetap menjadi tantangan yang membutuhkan solusi lebih kompleks seperti *firewall* dan CDN. Dokumentasi visual sebelum, selama, dan setelah serangan memperjelas dampak nyata serangan SlowHTTPTest terhadap web server. Gambar-gambar yang disajikan memperlihatkan perbedaan mencolok antara web yang rentan dan yang tahan serangan, baik dari sisi tampilan maupun respons server. Hal ini menegaskan pentingnya kesiapsiagaan dan penerapan langkah mitigasi yang tepat untuk menjaga ketersediaan layanan web di tengah ancaman serangan DoS yang semakin canggih.

3.3 Perbandingan

Tabel 1. Tabel Pembanding

Tahap	Web Tahan Serangan (Sampel)	Web Rentan (Sampel)
Tampilan Awal Web	Gambar 1: Web Tahan sebelum serangan. Web juga dapat diakses normal, responsif, dan tanpa error.	Gambar 2: Web Rentan sebelum serangan. Web dapat diakses normal, tanpa error atau keterlambatan.
Proses Serangan	Gambar 5: Proses serangan pada web tahan. Koneksi meningkat, namun server tetap stabil dan responsif.	Gambar 6: Proses serangan pada web rentan. Tampak koneksi meningkat drastis, server mulai melambat.
Tampilan Setelah Serangan	Gambar 7: Web tahan setelah serangan. Web tetap dapat diakses	Gambar 8: Web rentan setelah serangan. Web tidak dapat diakses,

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

	normal, hanya sedikit peningkatan waktu respons.	muncul pesan error atau loading sangat lama.

4. KESIMPULAN

Berdasarkan hasil simulasi serangan Denial of Service (DoS) tipe Slow HTTP menggunakan SlowHTTPTest terhadap sepuluh situs web, dapat disimpulkan bahwa serangan ini sangat efektif dalam menurunkan performa dan ketersediaan layanan web yang tidak memiliki perlindungan memadai. Lima web yang rentan mengalami peningkatan waktu respons secara drastis, error, bahkan downtime total setelah serangan berjalan beberapa menit. Sebaliknya, lima web yang telah menerapkan mekanisme pertahanan seperti pembatasan koneksi per-IP, pengaturan timeout yang ketat, atau penggunaan firewall dan CDN, tetap dapat diakses dengan baik meskipun terjadi serangan. Temuan ini menegaskan pentingnya implementasi strategi mitigasi yang kuat untuk menjaga ketersediaan layanan web di tengah ancaman serangan DoS yang terus berkembang. Penelitian ini memiliki keterbatasan pada lingkungan simulasi yang terisolasi dan tidak sepenuhnya mereplikasi kompleksitas serangan DoS di dunia nyata yang melibatkan traffic yang sangat bervariasi dan serangan terdistribusi dari banyak sumber. Selain itu, analisis mendalam mengenai arsitektur keamanan spesifik dari masing-masing situs web target yang tahan serangan tidak dilakukan secara ekstensif. Untuk pengembangan selanjutnya, disarankan untuk melakukan pengujian pada skala yang lebih besar dengan simulasi serangan Distributed Denial of Service (DDoS) menggunakan banyak penyerang. Penelitian juga dapat diperluas untuk menguji efektivitas berbagai solusi mitigasi berbasis machine learning atau AI dalam mendeteksi dan mencegah serangan Slow HTTP/2 yang lebih canggih secara real-time.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 409-419
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.402

REFERENCES

[1] M. Raza, "Denial-of-Service Attacks: History, Techniques & Prevention," splunk.com. [Online]. Available: https://www.splunk.com/en_us/blog/learn/dos-denial-of-service-attacks.html

[2] T. Safitrah, A. B. G. Sinaga, M. Alghifari, and S. N. Neyman, "Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2663.

[3] N. Tripathi, "Delays have Dangerous Ends : Slow HTTP / 2 DoS attacks into the Wild and their Real-Time Detection using Event Sequence Analysis," pp. 1–11, [Online]. Available: https://arxiv.org/abs/2203.16796

[4] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 56–70, 2020, doi: 10.35957/jatisi.v7i1.284.

[5] K. Ozaki and A. Kanai, "A Method for Preventing Slow HTTP DoS attacks," *Elev. Int. Conf. Emerg. Secur. Information, Syst. Technol.*, pp. 71–76, 2017.

[6] A. Muscat, "Mitigate Slow HTTP GET/POST Vulnerabilities in the Apache HTTP Server," Acunetix Website Security Scanner. [Online]. Available: https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/

[7] S. Shekyan, "How to Protect Against Slow HTTP Attacks," Qualys Community. [Online]. Available: https://blog.qualys.com/vulnerabilities-threat-research/2011/11/02/how-to-protect-against-slow-http-attacks

[8] P. M. John and R. M. B. K. Nagappasetty, "An approach for slow distributed denial of service attack detection and alleviation in software defined networks," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 25, no. 1, pp. 404–413, 2022, doi: 10.11591/ijeecs.v25.i1.pp404-413.

[9] C. Benzaid, M. Boukhalfa, and T. Taleb, "Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment," *IEEE Wirel. Commun. Netw. Conf. WCNC*, 2020, doi: 10.1109/WCNC45663.2020.9120472.

[10] Radware, "What is a Slowloris DDoS Attack? | Radware," radware.com. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/slowloris/

[11] Radware, "What is a Slowloris DDoS Attack? | Radware," radware.com. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/slowloris/

[12] A. A. Putra, Sapri, and A. Al Akbar, "Implementation Of Open Source Security Information Management (OSSIM) On Security Computer Network Penerapan Open Source Security Information Management (OSSIM) Pada Keamanan Jaringan Komputer," *J. Komput.*, vol. 1, no. 1, pp. 51–58, 2022.

[13] Y. Hae and W. Sulistyo, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 2095–2105, 2021, doi: 10.35957/jatisi.v8i4.1196.

[14] L. M. Silalahi and A. Kurniawan, "Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Dengan Metode Traffic Behavior," *Electr. J. Rekayasa dan Teknol. Elektro*, vol. 17, no. 1, pp. 71–76, 2023, doi: 10.23960/elc.v17n1.2296.

[15] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 56–70, 2020, doi: 10.35957/jatisi.v7i1.284.