Original Article

e-XXXX-XXXX

Original Article

Analisis Keamanan Aplikasi Berbasis Web terhadap Serangan Directory Traversal

Nursaskia[1]✉, Iin Syafira[2] , Rakhmadi Rahman [3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: nursaskia.241031024@mahasiswa.ith.ac.id,
iinsyafira.241031012@mahasiswa.ith.ac.id, rakhmadi.rahman@ith.ac.id

Abstrak:

Keamanan aplikasi berbasis web merupakan aspek penting seiring meningkatnya penggunaan teknologi web dalam berbagai sektor. Salah satu ancaman keamanan yang masih sering ditemukan adalah serangan directory traversal, yaitu teknik eksploitasi yang memungkinkan penyerang mengakses file atau direktori di luar jalur yang diizinkan oleh sistem. Penelitian ini bertujuan untuk menganalisis tingkat keamanan aplikasi berbasis web terhadap serangan directory traversal serta mengidentifikasi faktor penyebab terjadinya kerentanan tersebut. Metode penelitian yang digunakan adalah vulnerability assessment dengan pendekatan penetration testing terbatas berdasarkan panduan OWASP Top 10. Pengujian dilakukan pada aplikasi web uji dengan memanipulasi parameter input untuk mensimulasikan serangan directory traversal. Hasil penelitian menunjukkan bahwa lemahnya validasi input dan konfigurasi direktori yang tidak aman menjadi penyebab utama terjadinya kerentanan. Penelitian ini diharapkan dapat memberikan pemahaman serta rekomendasi teknis dalam meningkatkan keamanan aplikasi berbasis web terhadap serangan directory traversal.

Keywords: keamanan aplikasi web, directory traversal, penetration testing, vulnerability assessment, OWASP Top 10.

Pendahuluan

Perkembangan teknologi informasi telah mendorong penggunaan aplikasi berbasis web secara luas di berbagai sektor, seperti pendidikan, pemerintahan, dan bisnis. Aplikasi web berperan penting sebagai media utama dalam pengelolaan, penyimpanan, dan pertukaran data, termasuk data yang bersifat sensitif. Oleh karena itu, aspek keamanan aplikasi web menjadi hal yang sangat penting dan tidak dapat diabaikan.

Seiring meningkatnya transformasi digital, aplikasi berbasis web menjadi fondasi

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

utama dalam penyediaan layanan informasi yang cepat, efisien, dan mudah diakses. Namun, meningkatnya ketergantungan terhadap sistem digital juga diiringi dengan bertambahnya risiko ancaman keamanan siber. Ancaman tersebut tidak hanya berasal dari serangan berskala besar, tetapi juga dari eksploitasi sederhana yang memanfaatkan kelemahan dalam proses pengembangan dan pengelolaan aplikasi web. Salah satu jenis serangan yang masih sering ditemukan adalah directory traversal. Serangan ini memanfaatkan kelemahan validasi input sehingga penyerang dapat mengakses file atau direktori di luar jalur yang diizinkan oleh sistem hanya dengan memanipulasi parameter input. Berdasarkan laporan OWASP Top 10, kegagalan dalam validasi input masih menjadi salah satu penyebab utama terjadinya kerentanan keamanan pada aplikasi web.

Serangan directory traversal berpotensi memberikan akses tidak sah terhadap file sistem yang bersifat sensitif, seperti file konfigurasi, kredensial sistem, file log, hingga source code aplikasi. Kerentanan ini termasuk dalam kategori tingkat menengah hingga tinggi karena dapat membuka peluang terjadinya serangan lanjutan yang lebih berbahaya. Selain itu, serangan ini sering kali sulit terdeteksi oleh pengguna awam karena tidak selalu menimbulkan perubahan tampilan pada aplikasi web. Meskipun teknologi web terus berkembang, berbagai kerentanan keamanan masih sering ditemukan akibat kesalahan dalam validasi input dan konfigurasi direktori yang tidak aman. Tanpa mekanisme pembatasan akses dan pengamanan yang memadai, aplikasi web dapat menjadi sasaran empuk bagi penyerang untuk mengeksploitasi kelemahan yang ada.

Berdasarkan permasalahan tersebut, diperlukan analisis keamanan aplikasi berbasis web untuk mengetahui sejauh mana sistem mampu melindungi diri dari serangan directory traversal. Oleh karena itu, penelitian ini bertujuan untuk menganalisis tingkat keamanan aplikasi berbasis web terhadap serangan directory traversal serta mengidentifikasi faktor-faktor penyebab terjadinya kerentanan. Selain itu, penelitian ini juga diharapkan dapat memberikan rekomendasi teknis sebagai upaya mitigasi guna meningkatkan keamanan aplikasi web.

Gambar 1. Arsitektur Aplikasi Web

Metode Penelitian

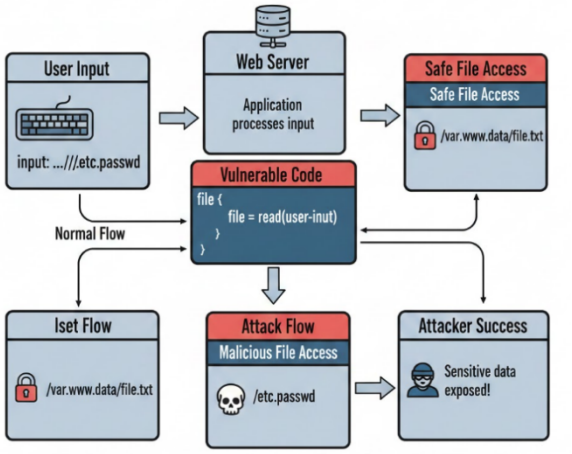
Penelitian ini menggunakan metode deskriptif dengan pendekatan vulnerability assessment dan penetration testing terbatas. Metode ini dipilih untuk memperoleh gambaran menyeluruh mengenai tingkat keamanan aplikasi berbasis web terhadap potensi kerentanan, khususnya serangan directory traversal. Objek penelitian berupa aplikasi berbasis web yang dijalankan pada lingkungan pengujian lokal. Tahapan penelitian dilakukan secara sistematis dan terstruktur, yang meliputi beberapa langkah sebagai berikut. Pertama, dilakukan studi literatur terkait keamanan aplikasi web, konsep directory traversal, serta panduan pengujian keamanan berdasarkan OWASP. Kedua, dilakukan identifikasi terhadap parameter-parameter pada aplikasi web yang berpotensi rentan terhadap serangan directory traversal. Ketiga, dilakukan pengujian keamanan dengan memanipulasi input menggunakan pola serangan directory traversal. Keempat, hasil pengujian dianalisis untuk menentukan tingkat kerentanan serta

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

dampak yang ditimbulkan terhadap keamanan aplikasi. Kelima, disusun rekomendasi mitigasi sebagai upaya peningkatan keamanan aplikasi web.

Pengujian dilakukan secara etis dan hanya pada aplikasi web uji yang berada dalam lingkungan pengujian tertutup, sehingga tidak menimbulkan dampak terhadap sistem nyata atau sistem produksi. Pendekatan penetration testing terbatas digunakan untuk mensimulasikan skenario serangan yang mungkin dilakukan oleh penyerang, namun tetap dalam ruang lingkup yang terkendali dan sesuai dengan prinsip etika pengujian keamanan. Teknik pengujian dilakukan dengan memanfaatkan pola serangan directory traversal, seperti penggunaan karakter khusus dan manipulasi jalur direktori, untuk menguji respons aplikasi web terhadap input yang tidak valid. Setiap hasil pengujian dicatat dan dianalisis guna menentukan tingkat risiko serta potensi dampak yang dapat ditimbulkan oleh kerentanan yang ditemukan.

Lingkungan pengujian dalam penelitian ini menggunakan server lokal dengan web server Apache, bahasa pemrograman PHP, serta sistem operasi berbasis Linux. Aplikasi web uji dijalankan sepenuhnya pada lingkungan pengujian tertutup untuk memastikan keamanan dan mencegah gangguan terhadap sistem produksi.



Gambar 2. Ilustrasi alur serangan directory traversal

Landasan Teori

Keamanan Aplikasi Web

Aplikasi berbasis web merupakan sistem informasi yang diakses melalui jaringan internet dengan memanfaatkan protokol HTTP atau HTTPS. Dalam operasionalnya, aplikasi web berfungsi sebagai media pertukaran data antara pengguna (client) dan server. Data yang dikelola oleh aplikasi web umumnya bersifat penting dan sensitif, seperti data pengguna, dokumen, serta konfigurasi sistem. Oleh karena itu, keamanan aplikasi web menjadi aspek yang sangat krusial untuk menjamin kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data.

Menurut Stallings (2018), keamanan sistem informasi harus dirancang untuk melindungi sumber daya digital dari berbagai bentuk ancaman dan eksploitasi. Pada aplikasi web, ancaman keamanan dapat muncul akibat kelemahan dalam pengkodean, kesalahan konfigurasi server, maupun kelalaian dalam memproses input pengguna. Zalewski (2011) menyatakan bahwa sebagian besar kerentanan pada aplikasi web disebabkan oleh kurangnya mekanisme validasi terhadap data yang dikirimkan oleh

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

pengguna. Tanpa perlindungan yang memadai, aplikasi web dapat dieksploitasi untuk mengakses bagian sistem yang seharusnya tidak dapat diakses secara publik. OWASP Foundation sebagai organisasi internasional yang berfokus pada keamanan aplikasi web telah mengelompokkan berbagai risiko keamanan ke dalam OWASP Top 10 Web Application Security Risks (2023). Salah satu risiko yang termasuk dalam kategori tersebut adalah kelemahan dalam pengelolaan akses file dan direktori, yang sering dieksploitasi melalui serangan Path Traversal atau Directory Traversal. Landasan teori ini menjadi dasar dalam penelitian untuk mengkaji bagaimana aplikasi web memproses jalur direktori serta menerapkan pembatasan akses terhadap sistem file.

Konsep dan Mekanisme Serangan Directory Traversal

Directory Traversal merupakan salah satu teknik serangan pada aplikasi web yang bertujuan untuk memperoleh akses ke direktori atau file di luar lokasi yang telah ditentukan oleh pengembang. Serangan ini dilakukan dengan memanipulasi parameter input yang berkaitan dengan lokasi file, seperti parameter URL file, path, atau page. Penyerang biasanya menyisipkan karakter traversal seperti ../, %2e%2e/, atau pola encoding lainnya untuk mencoba melewati pembatasan direktori aplikasi.

Scambray et al. (2011) menjelaskan bahwa serangan Directory Traversal terjadi ketika aplikasi menerima input pengguna secara langsung tanpa melakukan proses sanitasi atau normalisasi jalur (path) terlebih dahulu. Dalam banyak kasus pada aplikasi berbasis PHP, input tersebut diteruskan ke fungsi sistem seperti include(), readfile(), atau fopen(), sehingga memungkinkan penyerang membaca file sensitif yang tersimpan pada server. Zalewski (2011) juga menegaskan bahwa kesalahan dalam pengelolaan jalur relatif dan absolut dapat membuka peluang terjadinya kebocoran informasi.

Serangan Directory Traversal tidak selalu bertujuan untuk mengubah sistem, melainkan lebih sering digunakan untuk memperoleh informasi sensitif. Beberapa tujuan umum dari serangan ini antara lain membaca file konfigurasi, memperoleh kredensial basis data, mengunduh file penting, serta mempelajari struktur internal aplikasi. Informasi yang berhasil diperoleh selanjutnya dapat dimanfaatkan untuk melakukan serangan lanjutan, seperti Remote File Inclusion atau privilege escalation. Oleh karena itu, serangan Directory Traversal memiliki dampak yang serius karena berhubungan langsung dengan akses terhadap sistem file inti pada server.

Hasil dan Pembahasan

Hasil Pengujian Keamanan Aplikasi Web

Hasil pengujian menunjukkan bahwa aplikasi web uji memiliki parameter input yang tidak menerapkan validasi secara ketat terhadap karakter khusus. Kondisi ini memungkinkan terjadinya manipulasi jalur direktori, sehingga penyerang berpotensi mengakses file di luar direktori yang diizinkan oleh sistem. Temuan ini mengindikasikan bahwa mekanisme pengamanan pada aplikasi web uji belum diterapkan secara optimal, khususnya pada proses validasi input pengguna. Aplikasi tidak melakukan penyaringan terhadap karakter traversal, sehingga permintaan yang mengandung jalur direktori tidak valid tetap diproses oleh sistem.

Kondisi tersebut mencerminkan kelemahan yang masih sering ditemukan pada aplikasi web, terutama yang dikembangkan tanpa mengacu pada standar keamanan yang baku. Apabila kerentanan ini dieksploitasi oleh pihak yang tidak bertanggung jawab, maka aplikasi web berpotensi mengalami kebocoran data yang berdampak pada kerahasiaan, integritas, dan ketersediaan informasi. Kerentanan Directory Traversal

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

yang ditemukan berpotensi menyebabkan kebocoran informasi sensitif, seperti file konfigurasi dan struktur direktori aplikasi. Selain itu, apabila tidak segera ditangani, kerentanan ini dapat dimanfaatkan sebagai pintu masuk bagi serangan lain yang lebih kompleks dan berisiko tinggi.

Berdasarkan hasil analisis, faktor utama penyebab terjadinya kerentanan adalah lemahnya validasi input serta kesalahan konfigurasi sistem dalam membatasi akses direktori. Hal ini menunjukkan bahwa aspek keamanan sering kali belum menjadi prioritas utama dalam proses pengembangan aplikasi web. Hasil penelitian ini sejalan dengan beberapa penelitian sebelumnya yang menyatakan bahwa kesalahan konfigurasi sistem dan lemahnya validasi input merupakan penyebab utama terjadinya serangan Directory Traversal. Dengan demikian, temuan ini memperkuat pentingnya penerapan praktik keamanan sejak tahap perancangan aplikasi web.

Analisis Kerentanan Directory Traversal

Berdasarkan hasil pengujian yang telah diperoleh, dilakukan analisis lebih lanjut terhadap kerentanan keamanan aplikasi berbasis web. Analisis ini bertujuan untuk mengevaluasi kelemahan sistem yang ditemukan selama proses pengujian Directory Traversal serta menilai efektivitas mekanisme keamanan yang telah diterapkan.

Hasil analisis menunjukkan bahwa kerentanan utama terletak pada tidak adanya proses validasi dan sanitasi input pengguna, khususnya pada parameter yang digunakan untuk menentukan lokasi file atau direktori di sisi server. Pada kondisi awal, aplikasi belum menerapkan mekanisme pengamanan yang memadai, sehingga payload traversal seperti ../ dapat diteruskan langsung ke fungsi pemrosesan file. Akibat dari kondisi tersebut, sistem tidak memiliki pembatasan yang jelas terhadap direktori yang dapat diakses oleh pengguna. Kerentanan ini tergolong kritis karena memungkinkan penyerang membaca file sensitif, seperti file konfigurasi aplikasi, kredensial basis data, serta informasi internal sistem operasi.

Evaluasi Penerapan Mekanisme Keamanan

Setelah dilakukan penerapan mekanisme keamanan tambahan, terdapat perubahan respons sistem yang signifikan. Mekanisme keamanan berupa penyaringan karakter khusus, normalisasi jalur direktori (path normalization), serta pembatasan akses berbasis whitelist terbukti mampu meminimalkan potensi kerentanan.

Seluruh input yang mengandung pola Directory Traversal berhasil ditolak oleh aplikasi, sehingga akses terhadap file di luar direktori yang diizinkan dapat dicegah. Namun demikian, hasil evaluasi menunjukkan bahwa keamanan aplikasi tidak cukup hanya mengandalkan satu metode perlindungan. Pengamanan harus diterapkan secara menyeluruh, baik pada sisi aplikasi maupun pada sisi server.

Rekomendasi Perbaikan Keamanan Aplikasi Web

Berdasarkan hasil analisis dan evaluasi, terdapat beberapa rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan aplikasi web. Pertama, pengembang perlu menerapkan validasi input secara ketat dengan memeriksa setiap parameter yang berasal dari pengguna sebelum digunakan dalam proses pengelolaan file. Input pengguna tidak boleh langsung digabungkan dengan jalur direktori tanpa melalui proses sanitasi yang memadai.

Kedua, penggunaan fungsi pengelolaan file sebaiknya berbasis pada jalur absolut yang telah ditentukan oleh sistem. Pendekatan ini bertujuan untuk mencegah

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

manipulasi jalur relatif yang dapat dimanfaatkan dalam serangan Directory Traversal.

Ketiga, pengaturan hak akses file dan direktori pada server perlu diterapkan dengan prinsip least privilege. Web server hanya diberikan izin minimum untuk mengakses direktori tertentu, sedangkan direktori sensitif seperti konfigurasi dan log server sebaiknya ditempatkan di luar direktori publik.

Keempat, administrator server disarankan untuk menerapkan mekanisme pemantauan melalui pencatatan log guna mendeteksi adanya percobaan serangan sejak dini. Monitoring yang baik dapat membantu dalam melakukan respons cepat terhadap potensi ancaman keamanan.

Selain itu, hasil pengujian menunjukkan bahwa penggunaan payload dengan teknik encoding dapat melewati filter sederhana. Oleh karena itu, aplikasi disarankan untuk menerapkan metode validasi yang lebih kuat, seperti pengecekan basename file, pembatasan tipe ekstensi yang diizinkan, serta penggunaan daftar karakter input yang legal.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa serangan Directory Traversal masih menjadi ancaman nyata pada aplikasi web modern. Kerentanan tersebut umumnya bukan disebabkan oleh teknologi yang digunakan, melainkan oleh kesalahan pengembang dalam mengelola input pengguna dan jalur direktori.

Oleh karena itu, peningkatan kualitas pengembangan perangkat lunak yang memperhatikan aspek keamanan sejak tahap perancangan menjadi kunci utama dalam upaya pencegahan serangan siber. Penerapan standar keamanan yang konsisten diharapkan dapat mengurangi risiko kerentanan dan meningkatkan keandalan aplikasi web secara keseluruhan.

Tabel 1. Hasil Pengujian Serangan Directory Traversal pada Aplikasi Web

No	Parameter yang Diuji	Contoh Payload	Respon Sistem	Hasil
1	file	../etc/passwd	Aplikasi menampilkan isi file passwd	Rentan
2	file	../../config.php	File konfigurasi berhasil diakses	Rentan
3	file	../../../db.php	Kredensial database dapat terbaca	Rentan
4	download	../uploads/	Struktur direktori terbuka	Rentan
5	file	%2e%2e/%2e%2e/secret.txt	File sensitif dapat diakses melalui encoding	Rentan
6	file	images/../index.php	Akses ditolak oleh validasi input	Aman
7	file	basename(valid).pdf	Hanya file dalam whitelist yang diproses	Aman

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

8	upload_path	../includes/	Penyimpanan ke direktori tidak sah diblokir	Aman
9	url	....\windows.ini	Percobaan traversal Windows ditolak	Aman
10	file	..%2f..%2fadmin.log	Akses ke log berhasil diblokir setelah sanitasi	Aman

Kesimpulan

Berdasarkan hasil analisis dan pengujian keamanan yang telah dilakukan, dapat disimpulkan bahwa aplikasi berbasis web yang diuji masih memiliki kerentanan terhadap serangan Directory Traversal. Kerentanan ini disebabkan oleh lemahnya mekanisme validasi input pengguna serta tidak adanya pembatasan akses direktori yang memadai pada sisi server, sehingga permintaan yang tidak sah masih dapat diproses oleh aplikasi.

Kerentanan Directory Traversal memungkinkan penyerang mengakses file di luar direktori aplikasi yang seharusnya dilindungi. Kondisi tersebut berpotensi menyebabkan kebocoran informasi sensitif, mengganggu integritas data, serta membuka peluang terjadinya serangan lanjutan yang dapat berdampak pada keamanan sistem secara keseluruhan.

Penelitian ini memiliki keterbatasan karena pengujian hanya dilakukan pada satu aplikasi web uji dan difokuskan pada satu jenis serangan keamanan. Oleh karena itu, hasil penelitian ini belum dapat digeneralisasi untuk seluruh aplikasi berbasis web. Penelitian selanjutnya diharapkan dapat mencakup pengujian terhadap berbagai jenis serangan keamanan lainnya serta penerapan mekanisme pengamanan yang lebih komprehensif guna meningkatkan ketahanan aplikasi web terhadap ancaman siber.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar pengembang aplikasi web menerapkan validasi input secara ketat serta melakukan pembatasan akses terhadap direktori sistem untuk mencegah terjadinya serangan Directory Traversal. Selain itu, pengembang juga diharapkan mengikuti standar keamanan yang direkomendasikan oleh OWASP dalam proses perancangan dan pengembangan aplikasi web. Penelitian selanjutnya disarankan untuk mengembangkan dan menguji mekanisme deteksi otomatis terhadap serangan keamanan guna meningkatkan perlindungan aplikasi berbasis web secara lebih optimal dan menyeluruh.

Daftar Pustaka

OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks.https://owasp.org/www-project-top-ten/

Behl, A. (2017). Cybersecurity and Cyberwar. Oxford University Press.

Maizi, Z., Munawir, M., & Zainal, Z. (2023). Analisis log akses server web untuk mendeteksi anomali dan serangan siber.

Sutanto, H., & Wibowo, A. (2020). Implementasi vulnerability assessment pada aplikasi berbasis web. Jurnal Teknologi dan Sistem Komputer, 8(4), 312–319.

Nugraha, Y., & Pratama, R. (2021). Analisis kerentanan keamanan aplikasi web berbasis PHP. Jurnal Ilmiah Komputer dan Informatika, 10(2), 89–97.

Kurniawan, A., & Nugroho, A. (2020). Analisis keamanan aplikasi web menggunakan

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026

metode penetration testing berdasarkan OWASP Top 10. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(3), 523–530.
Gupta, S., & Sharma, P. (2022). Detection and Prevention of Directory Traversal Attacks in Web Applications. International Journal of Computer Applications, 184(12), 20–26.
Alenezi, M. (2021). Input Validation as a Defense Mechanism against Path Traversal Vulnerabilities. Journal of Information Security, 12(4), 215–223.
Engebretson, P. (2021).The Basics of Web Hacking: Tools and Techniques to Attack the Web. Elsevier Publishing.

Received: November 16, 2025 – Revised: November 23, 2025 - Accepted: Desember 18, 2025 - Published online: January 10, 2026