Vol 3 No. 2 April 2026 P-ISSN : 3047-9029 E-ISSN : 3047-9010, Hal 72 – 76

JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/7eb4g917

PENGUJIAN KEAMANAN APLIKASI BERBASIS WEB TERHADAP SERANGAN PARAMETER TAMPERING

Rakhmadi Rahman [a*], Yonatan Rannu [b], Marwa Dinda Muchtar [c]
[a] Jurusan Sistem Informasi; rakhmadi.rahman@ith.ac.id, Institut Teknologi BJ Habibie; JL. Balai Kota No. 1, Kota Parepare, Sulawesi Selatan
[b] Jurusan Sistem Informasi; yonatanrannu@gmail.com, Institut Teknologi BJ Habibie; JL. Balai Kota No. 1, Kota Parepare, Sulawesi Selatan
[c] Jurusan Sistem Informasi; muchtarmarwadinda@gmail.com, Institut Teknologi BJ Habibie; JL. Balai Kota No. 1, Kota Parepare, Sulawesi Selatan
[*] Penulis Korespondensi: Rakhmadi Rahman

ABSTRACT

The abstract contains a = Web application security is a critical aspect in ensuring the confidentiality and integrity of user data. One of the most common attack vectors is parameter tampering, which involves manipulating parameter values transmitted between the client and the server to alter application logic. This study aims to analyze the level of vulnerability of web applications to parameter tampering attacks and to identify the resulting security impacts. The research adopts a qualitative approach using a case study method through web application security testing based on black-box testing techniques. The testing process is conducted using tools such as Burp Suite and OWASP ZAP to observe application responses to parameter modifications. The results indicate that weaknesses in server-side parameter validation mechanisms still exist and may be exploited by attackers. Therefore, the implementation of strict server-side parameter validation and regular security testing is essential to enhance the overall security of web applications.

Keywords: *web application security; parameter tampering; security testing; OWASP*

Abstrak

Keamanan aplikasi berbasis web merupakan aspek penting dalam menjaga kerahasiaan dan integritas data pengguna. Salah satu bentuk serangan yang sering terjadi adalah *parameter tampering*, yaitu manipulasi nilai parameter yang dikirimkan antara klien dan server untuk memengaruhi logika aplikasi. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan aplikasi web terhadap serangan parameter tampering serta mengidentifikasi dampak keamanan yang ditimbulkan. Metode penelitian yang digunakan bersifat kualitatif dengan pendekatan studi kasus melalui pengujian keamanan aplikasi web menggunakan teknik *black-box testing*. Proses pengujian dilakukan dengan memanfaatkan alat bantu Burp Suite dan OWASP ZAP untuk mengamati respons aplikasi terhadap perubahan parameter. Hasil penelitian menunjukkan bahwa masih terdapat kelemahan dalam mekanisme validasi parameter pada sisi server yang berpotensi dimanfaatkan oleh penyerang. Oleh karena itu, penerapan validasi parameter yang ketat dan pengujian keamanan secara berkala menjadi langkah penting dalam meningkatkan keamanan aplikasi web.

Kata Kunci: keamanan aplikasi web; parameter tampering pengujian keamanan; OWASP

1. PENDAHULUAN

Aplikasi berbasis web telah menjadi komponen utama dalam penyelenggaraan sistem informasi modern. Pemanfaatan teknologi web memungkinkan akses informasi yang cepat, fleksibel, dan lintas platform, sehingga banyak diadopsi oleh organisasi pemerintahan, pendidikan, dan sektor bisnis. Seiring dengan

Naskah Masuk 7 Januari 2026; Revisi 9 Januari 2026; Diterima 14 Januari 2026; Tersedia 15 Januari 2026

meningkatnya ketergantungan terhadap aplikasi web, aspek keamanan menjadi faktor krusial yang tidak dapat diabaikan (Behl, 2023).

Ancaman terhadap keamanan aplikasi web terus berkembang, baik dari sisi teknik maupun kompleksitas serangan. Laporan OWASP secara konsisten menempatkan kelemahan validasi input dan manipulasi parameter sebagai risiko utama yang sering ditemukan pada aplikasi web. Salah satu bentuk serangan yang masih banyak terjadi adalah *parameter tampering*, yaitu upaya memodifikasi parameter permintaan HTTP untuk memanipulasi perilaku aplikasi di sisi server (OWASP, 2023).

Serangan parameter tampering dapat dilakukan dengan relatif mudah menggunakan alat bantu yang tersedia secara luas, seperti *web proxy* dan *interception tools*. Penyerang dapat mengubah nilai parameter harga, identitas pengguna, atau status transaksi tanpa terdeteksi apabila aplikasi tidak menerapkan mekanisme validasi yang memadai. Dampak dari serangan ini mencakup pelanggaran integritas data, kebocoran informasi sensitif, hingga penyalahgunaan hak akses sistem [4].

1.1. Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah sebagai berikut:
1. Bagaimana proses pengujian keamanan aplikasi berbasis web terhadap serangan parameter tampering?
2. Celah keamanan apa saja yang dapat ditemukan melalui pengujian parameter tampering pada aplikasi web?

1.2. Tujuan Penelitian

Tujuan penelitian ini meliputi:
a. Menguji tingkat keamanan aplikasi berbasis web terhadap serangan parameter tampering.
b. Mengidentifikasi kelemahan sistem yang berkaitan dengan validasi dan pengelolaan parameter.
c. Memberikan rekomendasi perbaikan keamanan aplikasi web berdasarkan hasil pengujian.

1.3. Manfaat Penelitian

Secara akademis, penelitian ini diharapkan dapat memperkaya kajian literatur terkait pengujian keamanan aplikasi web, khususnya pada aspek parameter tampering. Secara praktis, hasil penelitian dapat menjadi acuan bagi pengembang aplikasi web dalam meningkatkan mekanisme validasi input dan perlindungan terhadap manipulasi parameter

2. TINJAUAN PUSTAKA

2.1. Keamanan Aplikasi Web

Keamanan aplikasi web merupakan disiplin yang berfokus pada perlindungan aplikasi dari ancaman yang dapat merusak kerahasiaan, integritas, dan ketersediaan informasi. Prinsip dasar keamanan informasi dikenal sebagai CIA Triad, yang mencakup *Confidentiality*, *Integrity*, dan *Availability* (Stallings, 2022).

Dalam konteks aplikasi web, keamanan tidak hanya bergantung pada infrastruktur jaringan, tetapi juga pada implementasi logika aplikasi, pengelolaan sesi, serta mekanisme validasi input. Kegagalan dalam menerapkan kontrol keamanan pada lapisan aplikasi sering kali menjadi titik masuk bagi serangan siber (Behl, 2023).

2.2. Parameter Tampering

Parameter tampering adalah teknik serangan yang dilakukan dengan cara memodifikasi parameter yang dikirimkan oleh klien ke server melalui permintaan HTTP. Parameter tersebut dapat berupa parameter URL (*query string*), data formulir, *cookie*, maupun *hidden field* yang tersembunyi dalam halaman web (OWASP, 2023).

Jenis-jenis parameter tampering meliputi:
a. URL Parameter Tampering, yaitu manipulasi parameter pada alamat URL.
b. Form Parameter Tampering, yaitu perubahan nilai input formulir sebelum dikirim ke server.
c. Cookie Tampering, yaitu modifikasi nilai *cookie* untuk mempengaruhi sesi pengguna.
d. Hidden Field Tampering, yaitu perubahan nilai parameter tersembunyi dalam formulir HTML.

Serangan ini sering dimanfaatkan untuk melewati validasi klien, mengubah harga transaksi, atau melakukan eskalasi hak akses. Penelitian [4] menunjukkan bahwa banyak aplikasi web hanya mengandalkan validasi sisi klien, sehingga rentan terhadap manipulasi parameter.

2.3. Teknik Pengujian Keamanan Aplikasi Web

Pengujian keamanan aplikasi web bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan yang dapat dieksploitasi oleh pihak tidak berwenang. Teknik pengujian yang umum digunakan meliputi *black-box testing*, *white-box testing*, dan *gray-box testing* (OWASP, 2023).

Pengujian *black-box* sering digunakan dalam pengujian parameter tampering karena menyerupai skenario serangan nyata, di mana penguji tidak memiliki akses ke kode sumber aplikasi. Pengujian dapat dilakukan secara manual maupun otomatis dengan bantuan alat seperti Burp Suite, OWASP ZAP, dan teknik *fuzzing* [9].

2.4. Penelitian Terkait

Berbagai penelitian telah membahas deteksi dan mitigasi parameter tampering. [4] memperkenalkan *NoTamper*, sebuah metode *black-box* untuk mendeteksi kerentanan parameter tampering secara otomatis. Penelitian [9] mengusulkan pendekatan berbasis *machine learning* untuk meningkatkan akurasi deteksi kerentanan. Sementara itu, studi oleh OWASP menekankan pentingnya validasi sisi server sebagai kontrol utama dalam mencegah manipulasi parameter.

Penelitian ini memiliki kebaruan pada pendekatan kualitatif berbasis studi kasus aplikasi web nyata dengan fokus pada analisis mendalam proses pengujian dan implikasi keamanan.

3. METODOLOGI PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam mengenai karakteristik kerentanan parameter tampering dan respons aplikasi web terhadap manipulasi parameter. Beberapa indikator kuantitatif digunakan sebagai pendukung analisis, namun fokus utama penelitian tetap pada interpretasi hasil pengujian secara kualitatif.

3.2. Objek Penelitian

Objek penelitian berupa aplikasi berbasis web yang memiliki fitur autentikasi pengguna dan transaksi data. Pengujian dilakukan pada lingkungan pengujian terkontrol menggunakan peramban web dan *proxy interception tool*.

3.3. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

a. Observasi terhadap perilaku aplikasi saat menerima input.
b. Dokumentasi konfigurasi dan alur proses aplikasi.
c. Pengujian keamanan secara langsung dengan memodifikasi parameter.

3.4. Teknik Pengujian Parameter Tampering

Tahapan pengujian meliputi:

a. Identifikasi parameter kritis pada permintaan HTTP.
b. Modifikasi nilai parameter menggunakan Burp Suite.
c. Analisis respons sistem terhadap perubahan parameter.

3.5. Teknik Analisis Data

Analisis data dilakukan melalui reduksi data, penyajian hasil temuan dalam bentuk deskriptif, serta penarikan kesimpulan berdasarkan pola kerentanan yang ditemukan

4. HASIL DAN PEMBAHASAN

4.1. Proses Pengujuan Parameter Tampering

Pengujian dilakukan dengan menangkap permintaan HTTP menggunakan Burp Suite, kemudian memodifikasi nilai parameter seperti ID pengguna dan status transaksi. Pengujian difokuskan pada parameter yang tidak divalidasi ulang di sisi server.

4.2. Hasil Temuan Pengujian

Hasil pengujian menunjukkan adanya beberapa parameter yang dapat dimodifikasi tanpa memicu mekanisme keamanan. Dampak yang ditemukan meliputi perubahan data yang tidak sah dan potensi eskalasi hak akses.

Berdasarkan proses pengujian parameter tampering yang telah dilakukan menggunakan Burp Suite, diperoleh beberapa temuan terkait parameter yang rentan terhadap manipulasi. Ringkasan hasil pengujian disajikan pada Tabel 1.

Tabel 1. Hasil Pengujian Parameter Tampering pada Aplikasi Web

No	Parameter Yang Diuji	Lokasi Parameter	Teknik Manipulasi	Respons Aplikasi	Dampak Keamanan
1	user_id	URL (Query String)	Mengubah nilai ID pengguna	Aplikasi menerima perubahan	Eskalasi hak akses
2	price	Form Input	Mengubah harga sebelum submit	Transaksi tetap diproses	Manipulasi data transaksi
3	role	Cookie	Modifikasi nilai cookie	Hak akses berubah	Bypass otorisasi
4	status	Hidden Field	Mengubah status transaksi	Sistem tidak melakukan validasi ulang	Perubahan data tidak sah

Berdasarkan Tabel 1, terlihat bahwa beberapa parameter kritis seperti user_id, price, dan role tidak divalidasi ulang di sisi server. Kondisi ini memungkinkan penyerang untuk melakukan manipulasi data dan eskalasi hak akses. Temuan ini menunjukkan bahwa mekanisme validasi sisi klien saja tidak cukup untuk mencegah serangan parameter tampering

4.3. Pembahasan

Temuan penelitian sejalan dengan hasil penelitian sebelumnya yang menyatakan bahwa ketergantungan pada validasi sisi klien meningkatkan risiko parameter tampering (Bisht et al., 2010). Hal ini menunjukkan perlunya pendekatan keamanan berlapis dan validasi input yang konsisten.

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa aplikasi web yang diuji masih memiliki kerentanan terhadap serangan parameter tampering akibat lemahnya validasi sisi server. Keterbatasan penelitian terletak pada ruang lingkup objek yang diuji.

SARAN

Disarankan agar pengembang menerapkan validasi parameter di sisi server dan menggunakan mekanisme pengujian keamanan secara berkala. Penelitian selanjutnya dapat memperluas objek penelitian dan menggunakan pendekatan kuantitatif.

DAFTAR PUSTAKA

[1] Albestty I. Rafeli, Seta, H. B., & Widi, I. W. (2022). Pengujian celah keamanan menggunakan metode OWASP Web Security Testing Guide (WSTG) pada website XYZ. Jurnal Informatik. https://ejournal.upnvj.ac.id/informatik/article/view/4632

[2] Anugrah, R. D., & Alwi, E. I. (2025). Vulnerability assessment method for website security. International Journal of Open Information Technologies. https://jurnal.yoctobrain.org/index.php/ijonit/article/view/169

[3] Anonymous. (2024). Automated web security testing guide mapping to accelerate process on penetration testing. Procedia Computer Science, 235, 103–110. https://www.sciencedirect.com/science/article/pii/S1877050924004988

[4] Bisht, P., Hinrichs, T., Skrupsky, N., & Venkatakrishnan, V. N. (2010). NoTamper: Automatic black-box detection of parameter tampering vulnerabilities. In Proceedings of the ACM Conference on Computer and Communications Security (CCS) (pp. 607–618).
[5] Jose, L., Khanna, M. R., Meganathan, D., & B. T., P. (2022). Web-based parameter tampering on shopping site using Burp Suite testing. In Proceedings of the National Conference on Cyber Security. https://doi.org/10.52458/978-81-955020-5-9-51
[6] OWASP Foundation. (2014). OWASP testing guide v2.0 (Archived). https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v2.pdf
[7] OWASP Foundation. (2025). OWASP web security testing guide (WSTG). https://owasp.org/www-project-web-security-testing-guide/
[8] OWASP Foundation. (2025). Web parameter tampering. https://owasp.org/www-community/attacks/Web_Parameter_Tampering
[9] Yun, S. Y., & Cho, N.-W. (2025). A machine learning-based detection for parameter tampering vulnerabilities in web applications using BERT embeddings. Symmetry, 17(7), Article 985. https://doi.org/10.3390/sym17070985