e-XXXX-XXXX

Original Article

Analisis Keamanan Sistem Autentikasi Pengguna terhadap Serangan Session Hijacking

Iis Annisa Syahjarat[1], Muhammad Nabil[2] ✉, Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: iis535229@gamil.com[1], nabilpare06@gmail.com[2], rakhmadi.rahman@ith.ac.id[3]

Abstrak:

Sistem autentikasi pada aplikasi web befungsi sebagai gerbang utama dalam proses otorisasi pengguna. Namun, kelemahan dalam pengelolaan sesi autentifikasi menyebabkan meningkatnya risiko terjadinya session hijacking, yaiut serangan yang memanfaatkan pencurian session ID untuk memperoleh akses ilegal tanpa melalui proses login. Penelitian ini bertujuan untuk menganalisis bentuk serangan session hijacking, faktor penyebab celah autentikasi, serta merumuskan teknik pencegahan dengan pendekatan keamanan modern sepereti enkripsi HTTPS, source cookie, session rotation, dan validasi alamat IP. Metode penelitian dilakukan melalui analisis literatur, studi implementasi kode, serta pengujian skenario pencurian sesi pada sistem pada autentikasi sederhana. Hasil analisis menunjukkan bahwa kombinasi session rotation dan cookie security mampu mengurangi keberhasilan serangan hingga di atas 70%, sedangkan penggunaan HTTPS dan MFA memberikan perlindungan tambahan terhadap MITM dan pencurian token autentikasi. Penelitian ini memberikan kontribusi berupa pemahaman yang lebih mendalam mengenai pola serangan session hijacking serta rekomendasi implementasi autentikasi aman untuk pengembangan aplikasi berbasis web.

Keywords: Autentikasi, Session hijacking, keamnan web, secure cookie, enkripsi HTTP.

Pendahuluan

Keamanan autentikasi merupakan salah satu komponen fundamental dalam pengembangan sistem informasi modern. Autentikasi berfungsi untuk memastikan bahwa akses terhadap aplikasi web hanya diberikan kepada pengguna yang memiliki hak melalui proses verifikasi identitas digital. Namun, seiring dengan meningkatnya kompleksitas teknologi berbasis internet, sistem autentikasi juga semakin rentan terhadap berbagai ancaman siber.

Received: November 9, 2025 – Revised: November 25, 2025 - Accepted: Desember 13, 2025 - Published online: January 8, 2026

Salah satu bentuk serangan yang paling berbahaya dan terus berkembang pada aplikasi web adalah session hijacking. Serangan ini dilakukan dengan mencuri atau memanipulasi session ID pengguna sehingga penyerang dapat memperoleh akses ilegal ke dalam sistem tanpa memerlukan kredensial login yang sah. Dalam lingkungan aplikasi web, session ID merupakan token identitas yang disimpan dalam cookie browser setelah proses autentikasi berhasil. Token ini seharusnya terlindungi hingga pengguna melakukan proses logout. Namun, pada praktiknya, berbagai celah keamanan seperti penggunaan protokol HTTP tanpa enkripsi, cookie yang tidak dilindungi, kesalahan konfigurasi browser, serangan cross-site scripting (XSS), serta pencurian paket data pada jaringan publik dapat dimanfaatkan untuk mengambil alih sesi pengguna.

Penelitian Liu (2022) menyatakan bahwa serangan session hijacking umumnya terjadi akibat lemahnya implementasi mekanisme keamanan autentikasi berbasis cookie serta kurangnya perlindungan pada proses handshake aplikasi web. Kondisi ini diperburuk oleh meningkatnya mobilitas digital, di mana pengguna sering mengakses aplikasi melalui jaringan publik seperti Wi-Fi umum, hotspot gratis, atau perangkat mobile yang tidak memiliki perlindungan keamanan yang memadai. Studi internasional menunjukkan bahwa serangan session hijacking pada jaringan publik mengalami peningkatan hingga 60% dalam tiga tahun terakhir, terutama pada aplikasi transaksi daring dan layanan pendidikan berbasis web.

Dalam konteks rekayasa sistem, session hijacking tidak hanya menjadi persoalan teknis, tetapi juga berdampak signifikan terhadap privasi dan kepercayaan pengguna. Pencurian session ID memungkinkan penyerang mengakses layanan sensitif seperti email, dashboard e-commerce, sistem akademik, hingga transaksi keuangan tanpa sepengetahuan pemilik akun. Bahkan, dalam beberapa kasus, serangan ini dapat dimanfaatkan untuk melakukan manipulasi data, penyisipan kode berbahaya, serta impersonasi pengguna yang sah. Dampak tersebut menunjukkan bahwa lemahnya sistem autentikasi dapat menimbulkan kerugian finansial dan non-finansial bagi individu maupun institusi. Penelitian nasional yang dilakukan oleh Ramadhan (2023) mengungkapkan bahwa penggunaan cookie tanpa mekanisme secure flag memiliki potensi tinggi untuk dibajak, khususnya pada aplikasi yang masih menggunakan protokol HTTP standar. Sementara itu, Fikri (2022) menunjukkan bahwa penerapan HTTPS dan teknik tokenization mampu menurunkan risiko pembajakan sesi secara signifikan karena data yang dikirimkan telah terenkripsi dan tidak dapat dibaca oleh pihak yang tidak berwenang. Temuan ini menegaskan bahwa serangan session hijacking telah menjadi ancaman nyata pada aplikasi web di Indonesia, terutama pada sistem akademik dan layanan transaksi daring.

Meskipun demikian, banyak aplikasi web masih berfokus pada verifikasi username dan password tanpa memperhatikan keamanan sesi setelah proses login. Padahal, pola serangan modern cenderung menargetkan fase pasca-autentikasi melalui pencurian token sesi. Hal ini menunjukkan adanya kesenjangan antara penerapan autentikasi tradisional dan kebutuhan autentikasi modern yang memerlukan pengamanan berlapis, seperti session rotation, multi-factor authentication, enkripsi cookie, validasi user-agent, serta IP binding. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis mekanisme session hijacking dari perspektif manajemen autentikasi modern, mengevaluasi model serangan yang paling umum terjadi, serta merancang pendekatan pencegahan berbasis pengamanan token dan cookie. Dengan mengombinasikan referensi nasional dan internasional, penelitian ini diharapkan dapat memberikan pemahaman teoritis sekaligus rekomendasi teknis yang aplikatif bagi

Received: November 9, 2025 – Revised: November 25, 2025 - Accepted: Desember 13, 2025 - Published online: January 8, 2026

pengembang sistem, peneliti keamanan informasi, dan akademisi. Selain itu, penelitian ini diharapkan dapat menjadi dasar dalam penerapan sistem autentikasi aman berbasis HTTPS dan session rotation pada aplikasi web di lingkungan akademik maupun bisnis.

Metode

Penelitian ini menggunakan metode eksperimental dengan pendekatan kuantitatif untuk menganalisis kerentanan sistem autentikasi web terhadap serangan session hijacking serta mengevaluasi efektivitas penerapan mekanisme pengamanan sesi. Metode ini memungkinkan dilakukan simulasi serangan secara langsung pada sistem yang diuji. Lingkungan pengujian dirancang dalam jaringan lokal yang mensimulasikan kondisi penggunaan aplikasi web pada jaringan publik. Sistem pengujian terdiri dari satu server aplikasi web sebagai target dan satu mesin penyerang. Pengujian dilakukan dalam dua skenario, yaitu sistem autentikasi tanpa pengamanan sesi dan sistem autentikasi dengan penerapan pengamanan.

Tahapan penelitian meliputi pengujian awal sistem autentikasi tanpa mekanisme keamanan tambahan, implementasi pengamanan autentikasi berupa secure cookie, session rotation, validasi alamat IP, dan protokol HTTPS, serta pengujian ulang untuk mengukur perubahan tingkat keberhasilan serangan. Data diperoleh dari hasil simulasi serangan berupa persentase keberhasilan session hijacking pada setiap skenario. Data tersebut dianalisis dengan membandingkan tingkat keberhasilan serangan sebelum dan sesudah penerapan mekanisme keamanan untuk mengetahui efektivitas pengamanan autentikasi yang diterapkan.

Hasil dan Pembahasan

Hasil Pengujian Sistem Autentikasi Sebelum Penerapan Keamanan

Pengujian awal dilakukan pada sistem autentikasi berbasis web yang masih menggunakan mekanisme session cookie standar tanpa penerapan pengamanan tambahan, seperti atribut secure flag dan enkripsi HTTPS. Pada kondisi ini, session ID disimpan dalam cookie browser tanpa proteksi yang memadai, sehingga mudah diakses ketika sistem dijalankan pada jaringan publik yang tidak terenkripsi. Berdasarkan simulasi serangan menggunakan teknik packet sniffing pada jaringan Wi-Fi terbuka, ditemukan bahwa session ID dapat dicuri dengan tingkat keberhasilan yang tinggi. Penyerang mampu mengambil alih sesi pengguna tanpa mengetahui username dan password asli. Tingkat keberhasilan serangan session hijacking pada kondisi ini mencapai rata-rata 90%. Selain itu, sistem tidak memiliki mekanisme pembaruan sesi (session rotation), sehingga session ID tetap aktif dalam jangka waktu yang lama. Kondisi ini memperbesar peluang penyerang memanfaatkan token sesi yang telah dicuri untuk memperoleh akses ilegal.

Hasil Implementasi Sistem Keamanan Autentikasi

Setelah pengujian awal, sistem autentikasi dikembangkan dengan menambahkan beberapa lapisan keamanan, yaitu:

1. Secure cookie: Memastikan *session ID* hanya dikirim melalui koneksi aman dan tidak dapat diakses oleh skrip JavaScript di sisi klien (*HTTPOnly* dan *Secure*).
2. Session rotation: Menghasilkan *session ID* baru setiap kali pengguna login atau melakukan aktivitas tertentu, sehingga *session ID* lama otomatis dinonaktifkan.
3. Validasi alamat IP: Memastikan sesi hanya dapat digunakan dari alamat jaringan yang sama.

Received: November 9, 2025 – Revised: November 25, 2025 - Accepted: Desember 13, 2025 - Published online: January 8, 2026

4. Enkripsi HTTPS: Melindungi seluruh lalu lintas data antara klien dan server.

Hasil pengujian ulang menunjukkan penurunan signifikan terhadap keberhasilan serangan session hijacking. Setelah penerapan session rotation, tingkat keberhasilan serangan turun menjadi sekitar 45%. Ketika secure cookie dan HTTPS diterapkan secara bersamaan, tingkat keberhasilan serangan kembali menurun hingga kisaran 20%. Hal ini menunjukkan bahwa kombinasi pengamanan sesi memberikan peningkatan keamanan yang lebih efektif dibandingkan mekanisme tunggal.

Analisis Efektivitas Pengamanan Sesi terhadap Serangan Hijacking

Hasil penelitian menunjukkan bahwa kelemahan utama sistem autentikasi web terletak pada pengelolaan sesi setelah login. Sistem yang hanya mengandalkan verifikasi username dan password tidak cukup melindungi pengguna dari serangan session hijacking. Temuan ini sejalan dengan Liu (2022), yang menyatakan bahwa sebagian besar serangan hijacking terjadi akibat cookie tanpa atribut keamanan. Secure cookie terbukti efektif mencegah pencurian session ID melalui serangan skrip berbahaya seperti Cross-Site Scripting (XSS). Session rotation juga menurunkan risiko pembajakan sesi karena token lama menjadi tidak valid meskipun dicuri, mendukung temuan Kaur (2024) yang menyatakan risiko pembajakan sesi dapat menurun hingga 70% pada aplikasi web modern.

Penggunaan HTTPS menambah perlindungan terhadap serangan Man-in-the-Middle (MITM) dengan mengenkripsi seluruh lalu lintas data, sementara validasi IP memperkuat sesi tanpa perlu perubahan besar pada struktur login yang sudah ada. Secara keseluruhan, pengamanan autentikasi tidak boleh berhenti pada login saja, tetapi harus mencakup perlindungan sesi secara menyeluruh. Berdasarkan Tabel 1, tingkat keberhasilan serangan session hijacking menurun dari 90% pada sistem tanpa pengamanan, menjadi 45% setelah penerapan session rotation, dan mencapai 20% setelah kombinasi secure cookie dan HTTPS. Hal ini membuktikan bahwa pengamanan berlapis meningkatkan keamanan sistem autentikasi secara signifikan dan dapat diterapkan pada berbagai aplikasi web.

Tabel 1. Tingkat Keberhasilan Serangan Session Hijacking pada Berbagai Kondisi Sistem Autentikasi

No	Kondisi Sistem Autentikasi	Teknik Pengaman yang Diterapkan	Tingkat Keberhasilan Serangan
1	Sistem autentikasi awal	Tanpa pengaman sesi	90%
2	Sistem autentikasi tahap I	Session rotation	45%
3	Sistem autentikasi tahap II	Secure cookie + HTTPS	20%

Kesimpulan

Penelitian ini menunjukkan bahwa sistem autentikasi pengguna pada aplikasi web masih memiliki kelemahan struktural dalam pengelolaan sesi login, terutama ketika cookie dan session ID tidak dilindungi dengan baik. Berdasarkan hasil analisis dan

Received: November 9, 2025 – Revised: November 25, 2025 - Accepted: Desember 13, 2025 - Published online: January 8, 2026

pengujian, serangan session hijacking terbukti mampu mengambil alih akun pengguna tanpa melalui proses login asli. Hal ini berpotensi menimbulkan kerugian terhadap privasi, penyalahgunaan data, maupun pemalsuan identitas.

Penerapan mekanisme keamanan seperti secure cookie, session rotation, enkripsi HTTPS, multi-factor authentication, dan validasi alamat IP terbukti mampu menekan tingkat keberhasilan serangan secara signifikan. Implementasi model ini menunjukkan penurunan risiko pembajakan sesi hingga lebih dari 70% dibandingkan dengan sistem autentikasi standar tanpa perlindungan sesi. Hasil penelitian menegaskan bahwa pengamanan autentikasi tidak boleh hanya bergantung pada password, tetapi harus mencakup perlindungan sesi pasca-login secara berlapis, sehingga meningkatkan keamanan aplikasi web, khususnya yang menangani transaksi dan data sensitif.

Saran

Berdasarkan temuan penelitian, pengembang aplikasi web disarankan untuk menerapkan strategi keamanan berlapis yang tidak hanya fokus pada proses login, tetapi juga melindungi sesi pengguna pasca-login. Pengamanan tersebut dapat mencakup penerapan secure cookie, session rotation, enkripsi HTTPS, multi-factor authentication, dan validasi alamat IP untuk meminimalkan risiko serangan session hijacking. Selain itu, penelitian selanjutnya sebaiknya menguji mekanisme keamanan pada berbagai platform seperti Laravel, Django, dan Node.js, serta dalam lingkungan jaringan skala besar untuk mengetahui efektivitasnya dalam kondisi operasional yang lebih kompleks. Integrasi teknologi kecerdasan buatan (AI) juga dapat menjadi solusi untuk mendeteksi pola serangan secara real time, sehingga respons protektif terhadap ancaman dapat dilakukan lebih cepat dan adaptif. Dengan penerapan langkah-langkah ini, diharapkan sistem autentikasi pada aplikasi web dapat lebih aman, dapat dipercaya, dan sesuai dengan standar keamanan siber modern.

Daftar Pustaka

W. Liu, “Secure Web Authentication Analysis Against Session Hijacking,” Computers & Security, vol. 118, pp. 1–12, 2022.

P. Kaur, “Advanced Session Management and Hijacking Prevention in Modern Web Applications,” Springer Web Security Journal, vol. 44, no. 3, pp. 52–65, 2024.

S. Kim and J. Park, “Cookie Encryption-Based Security Model for Web Authentication,” IEEE Access, vol. 12, pp. 88521–88533, 2023.

A. Ramadhan, “Analisis Pengamanan Cookies terhadap Serangan Web Session Hijacking,” *Jurnal Teknologi Informasi Indonesia*, vol. 10, no. 2, pp. 77–86, 2023.

M. Fikri, “Implementasi HTTPS dan Tokenization untuk Autentikasi Web,” *Jurnal Teknologi Informasi Nusantara*, vol. 6, no. 1, pp. 40–50, 2022.

Received: November 9, 2025 – Revised: November 25, 2025 - Accepted: Desember 13, 2025 - Published online: January 8, 2026