DOI: XXXXXXXXXX

ANALISIS KEAMANAN SISTEM AUTENTIKASI LOGIN BERBASIS FRAMEWORK LARAVEL

[1]M. Gema Maulana
[1]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri,
Email: [1]mgemamaulana04@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem autentikasi login pada aplikasi web berbasis framework Laravel. Sistem autentikasi merupakan komponen penting yang berfungsi sebagai gerbang utama dalam melindungi data dan akses pengguna dari berbagai ancaman keamanan. Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan metode deskriptif-analitis melalui studi literatur, observasi, dan pengujian langsung terhadap sistem. Pengujian dilakukan dengan beberapa skenario seperti validasi input, simulasi login berulang, serta analisis pengelolaan session dan proteksi CSRF. Hasil penelitian menunjukkan bahwa Laravel telah menyediakan fitur keamanan dasar yang cukup baik, seperti hashing password, middleware autentikasi, dan manajemen session yang aman. Namun demikian, masih ditemukan beberapa kelemahan dalam implementasi, seperti belum diterapkannya pembatasan percobaan login (rate limiting) dan kontrol akses berbasis peran yang belum optimal. Oleh karena itu, diperlukan peningkatan pada aspek tersebut untuk meminimalisir potensi serangan seperti brute force dan akses tidak sah. Penelitian ini diharapkan dapat menjadi acuan dalam pengembangan sistem autentikasi yang lebih aman dan andal.

Kata Kunci: keamanan sistem, autentikasi, Laravel, login, web.

ABSTRACT

This study aims to analyze the security level of a login authentication system in a web application based on the Laravel framework. Authentication systems play a crucial role as the primary gateway to protect user data and access from various security threats. The research employs a qualitative approach using a descriptive-analytical method through literature study, observation, and direct system testing. The testing scenarios include input validation, repeated login attempts simulation, as well as session management and CSRF protection analysis. The results indicate that Laravel provides adequate built-in security features, such as password hashing, authentication middleware, and secure session management. However, several weaknesses were identified in the implementation, including the absence of rate limiting and suboptimal role-based access control. Therefore, improvements in these aspects are necessary to minimize potential attacks such as brute force and unauthorized access. This study is expected to serve as a reference for developing more secure and reliable authentication systems.

Keywords: system security, authentication, Laravel, login, web.

1 PENDAHULUAN

Perkembangan teknologi informasi saat ini berlangsung sangat pesat dan telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Hampir semua aktivitas modern kini terhubung dengan sistem berbasis digital, mulai dari komunikasi, transaksi keuangan, pendidikan, hingga layanan pemerintahan. Salah satu bentuk implementasi teknologi yang paling umum digunakan adalah aplikasi berbasis web. Aplikasi web memungkinkan pengguna untuk mengakses layanan secara fleksibel melalui internet tanpa batasan perangkat maupun lokasi. Seiring dengan meningkatnya penggunaan aplikasi web, kebutuhan akan sistem keamanan yang baik juga menjadi semakin penting. Salah satu aspek keamanan yang paling krusial dalam aplikasi web adalah sistem autentikasi atau login. Sistem login berfungsi sebagai

DOI: XXXXXXXXXX

gerbang utama untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses suatu sistem. Jika mekanisme login tidak dirancang dengan baik, maka aplikasi akan rentan terhadap berbagai serangan seperti pencurian data, brute force attack, SQL injection, hingga session hijacking.

Framework Laravel sebagai salah satu framework PHP yang populer saat ini banyak digunakan dalam pengembangan aplikasi web modern. Laravel menyediakan berbagai fitur keamanan bawaan yang mendukung pengembangan sistem yang lebih aman dan efisien, seperti enkripsi password menggunakan bcrypt, proteksi CSRF (Cross-Site Request Forgery), middleware autentikasi, serta sistem manajemen session yang terstruktur. Dengan fitur-fitur tersebut, Laravel menjadi pilihan utama bagi banyak pengembang dalam membangun sistem autentikasi login yang aman. Namun demikian, meskipun Laravel telah menyediakan berbagai mekanisme keamanan, implementasi yang dilakukan oleh pengembang tetap sangat menentukan tingkat keamanan sistem secara keseluruhan. Kesalahan dalam konfigurasi, kurangnya pemahaman terhadap konsep keamanan, atau penggunaan kode yang tidak sesuai standar dapat menyebabkan celah keamanan yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan adanya analisis mendalam terhadap sistem autentikasi login berbasis Laravel untuk memastikan bahwa implementasi yang digunakan telah sesuai dengan prinsip keamanan yang baik. Dalam dunia keamanan siber, sistem autentikasi merupakan target utama dari berbagai jenis serangan. Hal ini disebabkan karena sistem login merupakan pintu masuk ke dalam aplikasi yang berisi data penting pengguna. Apabila sistem autentikasi berhasil ditembus, maka seluruh data dan fungsi dalam aplikasi dapat diakses tanpa izin. Beberapa serangan yang umum terjadi pada sistem login antara lain brute force attack, di mana penyerang mencoba berbagai kombinasi username dan password secara berulang; credential stuffing, yaitu penggunaan data login yang bocor dari sistem lain; serta session hijacking, yaitu pencurian sesi login pengguna yang masih aktif. Selain itu, terdapat juga ancaman lain seperti SQL injection yang memanfaatkan kelemahan dalam query database, serta phishing yang menargetkan pengguna untuk mencuri kredensial login mereka. Meskipun Laravel telah menyediakan perlindungan terhadap beberapa jenis serangan tersebut, implementasi yang tidak tepat tetap dapat membuka celah keamanan. Sebagai contoh, tidak mengaktifkan rate limiting dapat membuat sistem rentan terhadap brute force attack, atau penggunaan session yang tidak aman dapat menyebabkan pencurian identitas pengguna.

Berdasarkan kondisi tersebut, diperlukan suatu kajian yang mampu mengevaluasi sejauh mana sistem autentikasi login pada Laravel telah diterapkan dengan aman. Analisis ini penting untuk memberikan gambaran mengenai kekuatan dan kelemahan sistem, serta memberikan rekomendasi perbaikan untuk meningkatkan tingkat keamanan aplikasi. Dengan adanya penelitian ini, diharapkan pengembang dapat lebih memahami pentingnya penerapan prinsip keamanan dalam setiap tahap pengembangan aplikasi web. Penelitian ini juga relevan dengan perkembangan industri teknologi informasi yang semakin menuntut sistem yang tidak hanya fungsional, tetapi juga aman. Keamanan data pengguna menjadi salah satu prioritas utama dalam pengembangan aplikasi modern, terutama di era digital saat ini di mana kebocoran data dapat menimbulkan dampak yang sangat besar. Oleh karena itu, pemahaman terhadap sistem autentikasi yang aman menjadi sangat penting bagi para pengembang perangkat lunak.

Dalam konteks akademik, penelitian mengenai analisis keamanan sistem login berbasis Laravel juga dapat memberikan kontribusi dalam bidang rekayasa perangkat lunak dan keamanan sistem informasi. Hasil penelitian ini dapat digunakan sebagai referensi bagi penelitian selanjutnya yang berkaitan dengan pengembangan sistem autentikasi yang lebih kompleks dan aman, seperti penggunaan multi-factor authentication (MFA), OAuth, atau JSON Web Token (JWT). Selain itu, penelitian ini juga dapat membantu dalam memberikan edukasi kepada pengembang pemula mengenai pentingnya penerapan praktik keamanan yang baik dalam pengembangan aplikasi web. Banyak kasus keamanan terjadi bukan karena keterbatasan teknologi, tetapi karena kurangnya pemahaman pengembang terhadap aspek keamanan itu sendiri. Oleh karena itu, analisis terhadap sistem autentikasi ini diharapkan dapat meningkatkan kesadaran akan pentingnya keamanan aplikasi sejak tahap perancangan.

DOI: XXXXXXXXXX

Berdasarkan latar belakang tersebut, maka penelitian ini mengambil judul "Analisis Keamanan Sistem Autentikasi Login Berbasis Framework Laravel". Penelitian ini akan berfokus pada bagaimana sistem login diimplementasikan menggunakan Laravel, serta bagaimana tingkat keamanannya terhadap berbagai potensi ancaman yang ada. Selain itu, penelitian ini juga akan membahas rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan sistem autentikasi.

Dengan demikian, penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis. Secara teoritis, penelitian ini dapat memperkaya kajian ilmu di bidang keamanan sistem informasi. Sedangkan secara praktis, hasil penelitian ini dapat digunakan sebagai acuan dalam pengembangan sistem login yang lebih aman dan andal pada aplikasi berbasis web.

2 METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis. Metode ini dipilih karena penelitian bertujuan untuk menggambarkan serta menganalisis tingkat keamanan sistem autentikasi login berbasis framework Laravel secara mendalam berdasarkan kondisi nyata pada sistem yang diuji. Selain itu, penelitian ini juga termasuk dalam jenis penelitian terapan (applied research), karena hasil penelitian diharapkan dapat memberikan rekomendasi praktis untuk meningkatkan keamanan sistem login pada aplikasi web berbasis Laravel.

Objek dalam penelitian ini adalah sistem autentikasi login yang dibangun menggunakan framework Laravel. Sistem yang dianalisis mencakup proses autentikasi pengguna seperti login dan logout, pengelolaan session, serta mekanisme keamanan yang telah diterapkan di dalam sistem, seperti hashing password, proteksi CSRF (Cross-Site Request Forgery), penggunaan middleware autentikasi, dan pembatasan percobaan login (rate limiting).

Penelitian ini dilakukan pada lingkungan pengembangan atau development environment menggunakan perangkat komputer pribadi peneliti. Waktu pelaksanaan penelitian disesuaikan dengan proses penyusunan skripsi, mulai dari tahap pengumpulan data, pengujian sistem, hingga analisis hasil penelitian.

Sumber data yang digunakan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh melalui hasil pengujian langsung terhadap sistem login berbasis Laravel, termasuk hasil uji login dengan data valid maupun tidak valid, pengujian terhadap keamanan sistem seperti brute force attack, pengujian session, serta pengamatan terhadap kode program yang digunakan. Sementara itu, data sekunder diperoleh dari berbagai referensi seperti buku, jurnal ilmiah, artikel, serta dokumentasi resmi Laravel yang berkaitan dengan sistem autentikasi dan keamanan aplikasi web.

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa cara. Pertama, studi literatur dilakukan dengan mempelajari berbagai sumber yang relevan mengenai keamanan sistem informasi, autentikasi login, serta framework Laravel. Kedua, observasi dilakukan dengan mengamati secara langsung implementasi sistem login pada Laravel untuk memahami mekanisme yang digunakan. Ketiga, pengujian sistem dilakukan untuk mengetahui tingkat keamanan sistem login melalui beberapa skenario pengujian seperti percobaan login berulang untuk menguji brute force, pengujian validasi input untuk melihat potensi SQL injection sederhana, serta pengujian session management dan proteksi CSRF.

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif, yaitu dengan cara mengidentifikasi dan menjelaskan mekanisme autentikasi pada Laravel. Setelah itu, dilakukan analisis terhadap kelebihan dan kekurangan sistem login yang diuji, serta memberikan penilaian terhadap tingkat keamanannya berdasarkan hasil pengujian yang telah dilakukan.

Alur penelitian dimulai dari tahap identifikasi masalah yang berkaitan dengan keamanan sistem login berbasis Laravel. Setelah itu dilakukan studi literatur untuk memperkuat landasan teori. Tahap selanjutnya adalah implementasi atau penyiapan sistem login yang akan dianalisis. Kemudian dilakukan pengujian terhadap sistem untuk mengetahui tingkat keamanannya. Hasil

DOI: XXXXXXXXXX

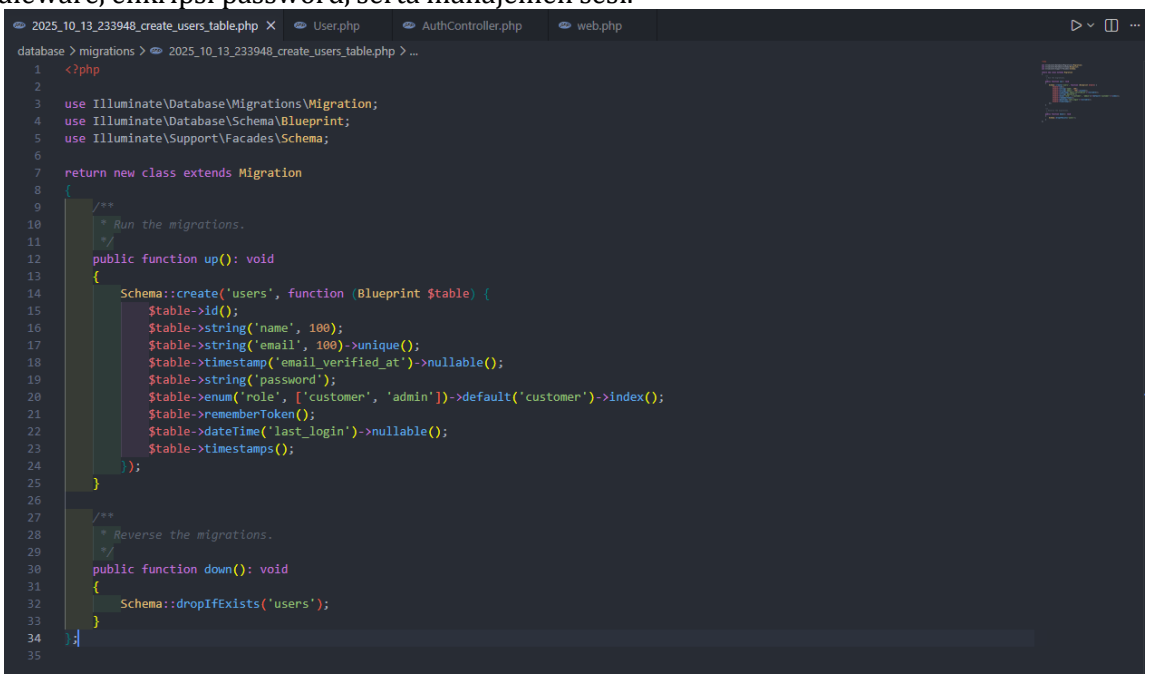
pengujian tersebut dianalisis secara mendalam, dan pada tahap akhir disusun kesimpulan serta rekomendasi untuk meningkatkan keamanan sistem autentikasi.

Dalam penelitian ini digunakan beberapa perangkat dan tools pendukung seperti framework Laravel sebagai objek utama penelitian, MySQL sebagai database, serta XAMPP atau Laragon sebagai local server. Selain itu, digunakan juga VS Code sebagai text editor dan browser atau Postman untuk melakukan pengujian terhadap sistem login.

3 HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas hasil implementasi sistem autentikasi login yang dikembangkan menggunakan framework Laravel, serta analisis terhadap kinerja dan mekanisme yang diterapkan. Proses autentikasi merupakan salah satu komponen krusial dalam sebuah sistem berbasis web, karena berfungsi untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat masuk ke dalam sistem. Oleh karena itu, perancangan dan implementasi fitur login harus memperhatikan aspek keamanan, efisiensi, serta kemudahan penggunaan.

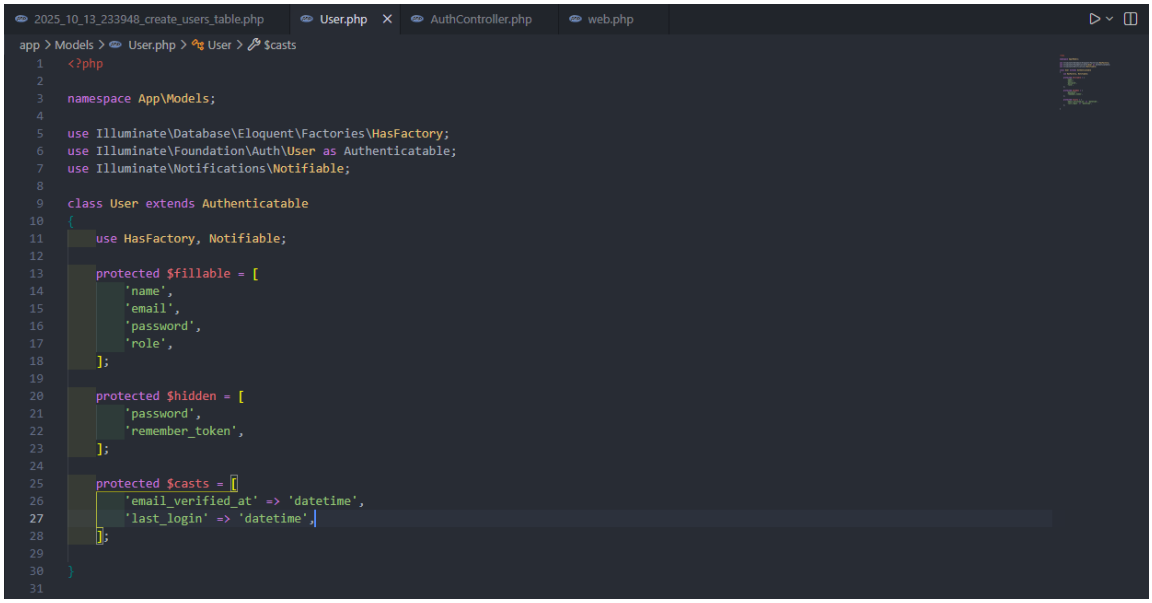
Dalam penelitian ini, fitur autentikasi dibangun dengan memanfaatkan fasilitas bawaan Laravel yang telah menyediakan struktur keamanan yang terstandarisasi, seperti penggunaan middleware, enkripsi password, serta manajemen sesi.



Gambar 1. Source Code Migrasi Tabel Users

File migration menunjukkan bahwa struktur tabel `users` telah dirancang dengan cukup baik untuk mendukung sistem autentikasi yang aman. Penggunaan kolom `email` dengan constraint `unique` membantu mencegah duplikasi akun, yang merupakan langkah penting dalam menjaga integritas data pengguna. Penyimpanan password menggunakan tipe string yang nantinya di-hash oleh Laravel juga sudah sesuai dengan praktik keamanan modern. Penambahan kolom `email_verified_at` memungkinkan implementasi verifikasi email, yang dapat meningkatkan keamanan akun pengguna. Selain itu, penggunaan `rememberToken()` mendukung fitur "remember me" pada login, meskipun fitur ini perlu dikontrol dengan baik agar tidak menjadi celah keamanan. Kolom `role` dengan tipe enum (`customer` dan `admin`) memberikan dasar untuk kontrol akses berbasis peran, namun pendekatan ini masih sederhana dan berpotensi kurang fleksibel jika sistem berkembang. Adanya kolom `last_login` juga menjadi nilai tambah untuk keperluan audit aktivitas pengguna. Secara keseluruhan, struktur database sudah cukup aman, namun belum mencakup fitur tambahan seperti penyimpanan log aktivitas atau proteksi terhadap percobaan login berulang secara langsung di level database.

DOI: XXXXXXXXXX



Gambar 2. Source Code Model User

Model `User` telah mengimplementasikan fitur dasar Laravel untuk autentikasi dengan mewarisi class `Authenticatable`, yang secara otomatis menyediakan berbagai mekanisme keamanan seperti pengelolaan session dan autentikasi berbasis guard. Penggunaan properti `$fillable` menunjukkan bahwa hanya atribut tertentu yang dapat diisi secara mass assignment, sehingga membantu mencegah serangan mass assignment vulnerability. Selain itu, properti `$hidden` digunakan untuk menyembunyikan atribut sensitif seperti `password` dan `remember_token` dari output JSON, yang merupakan praktik keamanan yang baik. Casting pada `email_verified_at` dan `last_login` ke tipe `datetime` juga meningkatkan konsistensi data. Namun demikian, model ini belum menerapkan fitur tambahan seperti enkripsi atribut tertentu atau penggunaan accessor dan mutator untuk kontrol lebih lanjut terhadap data sensitif. Selain itu, tidak terdapat implementasi fitur keamanan lanjutan seperti multi-factor authentication (MFA) atau pembatasan akses berbasis kebijakan (policy), sehingga masih bergantung pada implementasi di level controller atau middleware.

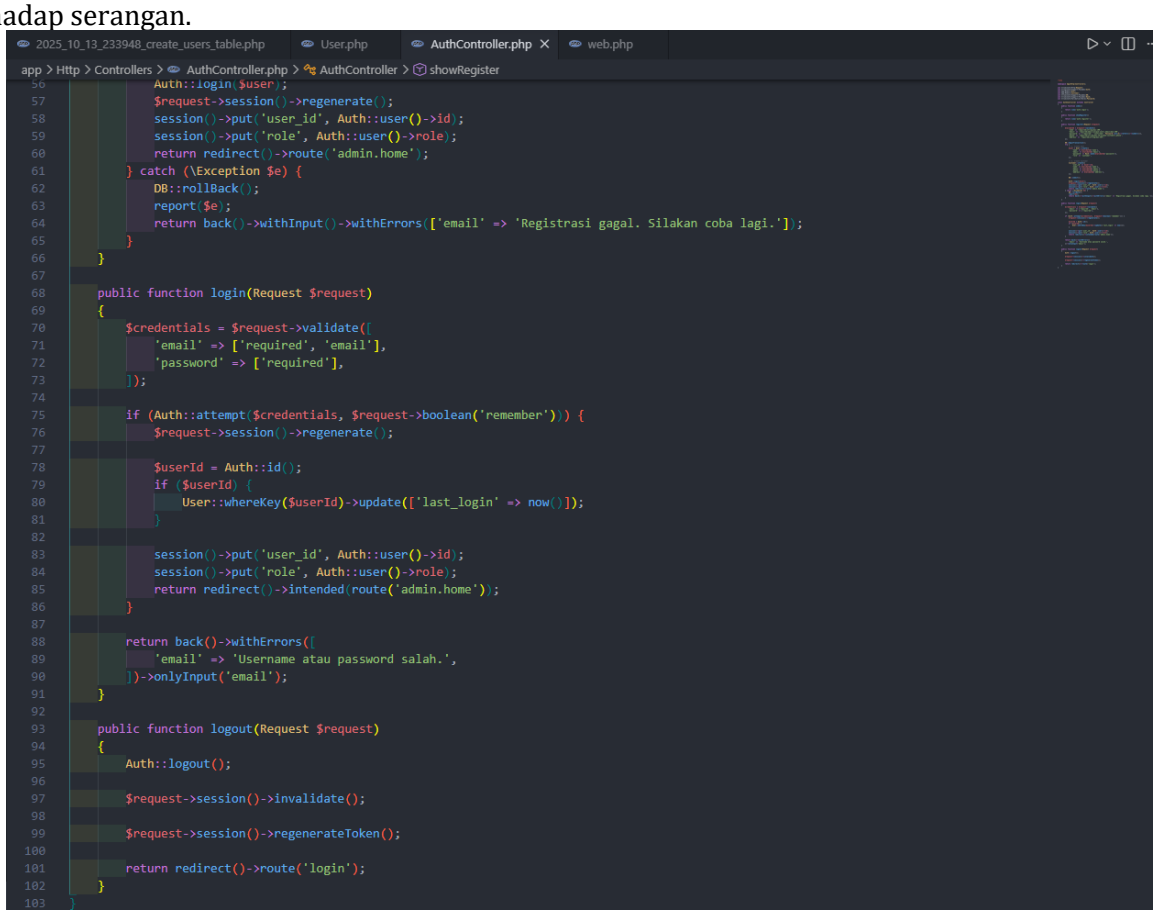
Gambar 3. Source Code Routing

Konfigurasi routing menunjukkan pemisahan akses yang cukup jelas antara pengguna yang belum login (`guest`) dan yang sudah login (`auth`). Penggunaan middleware `guest` pada route login dan register memastikan bahwa hanya pengguna yang belum terautentikasi yang dapat mengakses halaman tersebut, sehingga mencegah akses yang tidak perlu oleh pengguna yang

DOI: XXXXXXXXXX

sudah login. Selain itu, route logout dilindungi dengan middleware `auth`, yang memastikan hanya pengguna yang telah login yang dapat melakukan logout.

Namun demikian, terdapat potensi kelemahan pada route utama (`/`) yang langsung mengarahkan ke `admin.home` setelah login tanpa pengecekan role pengguna. Hal ini dapat menyebabkan pengguna dengan role `customer` mengakses halaman yang seharusnya hanya diperuntukkan bagi admin. Oleh karena itu, diperlukan middleware tambahan untuk membatasi akses berdasarkan role (role-based access control). Selain itu, tidak terlihat adanya penerapan middleware khusus untuk proteksi tambahan seperti rate limiting (`throttle`) pada route login, yang penting untuk mencegah brute force attack. Secara umum, struktur routing sudah baik, tetapi perlu ditingkatkan dengan kontrol akses yang lebih spesifik dan proteksi tambahan terhadap serangan.



Gambar 4. Source Code Controller Autentifikasi

Controller autentikasi menunjukkan implementasi yang cukup baik dalam menangani proses registrasi, login, dan logout pengguna. Pada proses registrasi, validasi input sudah diterapkan dengan ketat, termasuk validasi email unik, password minimal 8 karakter dengan kombinasi huruf dan angka, serta konfirmasi password. Penggunaan `Hash::make()` memastikan bahwa password disimpan dalam bentuk terenkripsi (bcrypt), sehingga aman dari kebocoran data plaintext. Implementasi transaksi database (`DB::beginTransaction`) juga merupakan langkah yang tepat untuk menjaga konsistensi data antara tabel `users` dan `customers`.

Pada proses login, penggunaan `Auth::attempt()` sudah sesuai dengan standar Laravel, dan diikuti dengan `session()->regenerate()` untuk mencegah serangan session fixation. Selain itu, pencatatan waktu login terakhir (`last_login`) merupakan praktik yang baik untuk monitoring aktivitas pengguna. Namun, terdapat beberapa kelemahan yang perlu diperhatikan. Sistem belum menerapkan rate limiting secara eksplisit, sehingga masih berpotensi terhadap serangan brute force. Selain itu, penyimpanan `user_id` dan `role` secara manual ke dalam session

sebenarnya redundan karena Laravel sudah mengelola session autentikasi secara otomatis, dan jika tidak dikelola dengan baik dapat meningkatkan risiko manipulasi session.

Pada proses logout, sistem telah menghapus session dengan `invalidate()` dan membuat token baru dengan `regenerateToken()`, yang merupakan praktik keamanan yang baik untuk mencegah penyalahgunaan session lama. Secara keseluruhan, controller sudah cukup aman, namun masih perlu peningkatan pada aspek proteksi terhadap serangan otomatis dan penyederhanaan manajemen session.

4 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai analisis keamanan sistem autentikasi login berbasis framework Laravel, dapat disimpulkan bahwa Laravel telah menyediakan berbagai fitur keamanan bawaan yang cukup kuat dalam mendukung implementasi sistem autentikasi yang aman. Fitur tersebut meliputi hashing password menggunakan bcrypt, middleware autentikasi, manajemen session yang aman, proteksi CSRF, serta mekanisme validasi input yang membantu mengurangi risiko serangan terhadap sistem login.

Hasil pengujian menunjukkan bahwa sistem autentikasi yang dikembangkan sudah mampu menangani proses login, registrasi, dan logout dengan baik serta memberikan perlindungan dasar terhadap beberapa ancaman keamanan seperti SQL injection sederhana dan session hijacking. Penggunaan Auth::attempt() serta session()->regenerate() juga terbukti meningkatkan keamanan dalam proses autentikasi pengguna.

Namun demikian, masih ditemukan beberapa kelemahan dalam implementasi sistem, terutama pada aspek pembatasan percobaan login (rate limiting) yang belum diterapkan secara optimal, serta kontrol akses berbasis peran (role-based access control) yang masih sederhana. Hal ini berpotensi membuka celah terhadap serangan brute force maupun akses tidak sah ke halaman tertentu.

Oleh karena itu, diperlukan pengembangan lebih lanjut pada aspek keamanan tambahan seperti penerapan rate limiting, implementasi middleware berbasis role yang lebih ketat, serta penggunaan mekanisme autentikasi lanjutan seperti Multi-Factor Authentication (MFA) untuk meningkatkan tingkat keamanan sistem secara keseluruhan. Dengan adanya peningkatan tersebut, diharapkan sistem autentikasi login berbasis Laravel dapat menjadi lebih aman, andal, dan sesuai dengan standar keamanan aplikasi web modern.

REFERENSI

[1] F. Prasetyo, E. Putra, A. Zulfikri, A. Rohman, And R. Alim, “Analysis Comparative Of Performance Optimization Techniques For Php Framework Testing : Laravel , Codeigniter , Symfony,” Vol. 5, No. 1, Pp. 242–248, 2025.

[2] R. Laipaka, “Penerapan Jwt Untuk Authentication Dan Authorization Pada Laravel 9 Menggunakan Thunder Client,” Pp. 450–455.

[3] F. Patria, B. A. Saputra, And M. Setiyawan, “Rancang Bangun Sistem Manajemen Inventori Berbasis Web Menggunakan Framework Laravel Pada Enuma Technology,” No. November, Pp. 742–752, 2025.

[4] P. A. Pratama, T. Informasi, U. P. Sakti, And P. Korespondensi, “Pengembangan Sistem Arsip Digital Berbasis Website Dengan Framework Laravel Untuk Efisiensi Penyimpanan Website-Based Digital Archiving System Development With Laravel Framework For Storage Efficiency And Data Security,” Vol. 3, No. 2, Pp. 9–12, 2024.

[5] A. E. Setyawan *Et Al.*, “Perancangan Sistem Pemesanan Tiket Pendakian Di Gunung Pulosari Menggunakan Framework Laravel,” Vol. 9, No. 6, Pp. 10245–10251, 2025.

[6] A. P. Abdjul And U. I. Indonesia, “Rancang Bangun Aplikasi Monitoring Akademik Berbasis,” Vol. 9, No. 6, Pp. 10333–10339, 2025.

[7] S. Salsabila And H. Maulana, “Pengembangan Sistem Penggajian Berbasis Web Laravel : Studi Kasus Pt Inti Pindad Mitra Sejati,” Vol. 16, No. 1, 2024.

[8] N. September, R. D. Risanty, M. Sutrisno, R. Mujiastuti, And S. N. Ambo, "Society : Jurnal Pengabdian Masyarakat , Testing Society : Jurnal Pengabdian Masyarakat ," Vol. 4, No. 5, Pp. 698–710, 2025.

[9] R. Y. Endra, Y. Aprilinda, Y. Y. Dharmawan, And W. Ramadhan, "Analisis Perbandingan Bahasa Pemrograman Php Laravel Dengan Php Native Pada Pengembangan Website," Vol. 8, No. 200, Pp. 48–55, 2022.

[10] A. Natasa, D. Samba, And P. Sukanta, "Informatics Today Rancang Bangun Sistem Presensi Pegawai Berbasis Website Menggunakan Framework Laravel Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Kuantan Singingi," Vol. 1, No. 1, Pp. 48–58, 2026.

[11] M. R. Ramadhan And G. Testiana, "Pengembangan Website Profil Politeknik Pariwisata Palembang Menggunakan Framework Laravel," Vol. 4, No. 4, Pp. 5749–5762, 2025.

[12] C. Jumlyacob, J. Edison, A. S. Affandi, And S. Informasi, "Implementasi Laravel Untuk Digitalisasi Umkm : Studi Kasus E- Commerce Kerajinan Tradisional Harpa Mulut," Pp. 6364–6374, 2025.

[13] M. Soeharto, A. Karim, And A. Supriady, "Perancangan Sistem Informasi Pembayaran Spp Dan Pembayaran Pendaftaran Peserta Didik Baru Sekolah Dasar Dalam Bentuk Website Menggunakan Framework Laravel," Vol. 1, No. 1, Pp. 1–11, 2025.

[14] O. Technology, "Hibahqu Education Monitoring Platform Based On Human-Centric Orange Technology Laravel 12 Vue . Js Platform Monitoring Pendidikan Hibahqu Berbasis Human-Centric," Vol. 6, No. 2, Pp. 204–219, 2025.

[15] P. Studi And T. Informatika, "File Encryption, Advanced Encryption Standard (Aes), Laravel, Id Card, Waterfall," Vol. 13, No. 2, 2025.