

## Efisiensi dan Produktivitas Pengembangan Aplikasi Web sebagai Nilai Ekonomi: Studi Komparatif Framework Laravel dan PHP Native

Alini Syawalia Riski Fenanda<sup>1</sup>, Richardus Eugene Tija<sup>2</sup>, Liah siti Komariah<sup>3</sup>, Rexxy Andrew Gunawan<sup>4</sup>, Devi Muawatul Mukaromah<sup>5</sup>

<sup>1,2,3,4,5,6</sup> Universitas Siber Asia, Indonesia

Korespondensi: [alinfenanda2@gmail.com](mailto:alinfenanda2@gmail.com)

---

### Informasi Artikel

#### Riwayat artikel:

Diterima Januari 31<sup>th</sup>, 2026

Direvisi Februari 04<sup>th</sup>, 2026

Diterima Februari 07<sup>th</sup>, 2026

---

#### Kata kunci:

Keamanan Aplikasi Web, *Laravel*, PHP, Efisiensi ekonomi, Produktivitas, Kerangka Kerja.

---

### ABSTRAK

Perkembangan aplikasi web modern menuntut sistem yang tidak hanya fungsional, tetapi juga aman, efisien, dan mudah dikembangkan. Ancaman keamanan seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan *Cross-Site Request Forgery (CSRF)* masih menjadi permasalahan utama dalam pengembangan aplikasi web berbasis PHP, khususnya pada sistem yang dibangun menggunakan PHP Native tanpa kerangka kerja terstandar. Penelitian ini bertujuan untuk menganalisis efektivitas *framework Laravel* dibandingkan PHP Native dalam meningkatkan keamanan, efisiensi pengembangan, serta kemudahan pemeliharaan aplikasi web. Metodologi yang digunakan adalah studi literatur dan analisis komparatif terhadap beberapa jurnal ilmiah yang membahas implementasi *Laravel*, fitur keamanan bawaan, serta penerapan pengujian penetrasi. Hasil kajian menunjukkan bahwa *Laravel* memiliki keunggulan signifikan dalam aspek keamanan melalui penerapan *middleware*, parameter binding, proteksi *CSRF*, enkripsi data, dan struktur *MVC* yang terstandarisasi. Selain itu, *Laravel* mampu meningkatkan produktivitas pengembang dan konsistensi kode, yang secara tidak langsung berkontribusi pada efisiensi biaya pengembangan dan pemeliharaan aplikasi web dalam jangka panjang. Meskipun memiliki kebutuhan konfigurasi dan optimasi performa yang lebih kompleks dibandingkan PHP Native, penggunaan *Laravel* memberikan nilai ekonomi tambahan melalui percepatan waktu pengembangan dan pengurangan risiko kesalahan sistem. Dengan demikian, *Laravel* dinilai lebih efektif untuk pengembangan aplikasi web modern yang menuntut tingkat keamanan dan skalabilitas tinggi.



© 2025 Para Penulis. Diterbitkan oleh Riset Anak Bangsa. Ini adalah artikel akses terbuka di bawah lisensi CC BY (<https://creativecommons.org/licenses/by/4.0/>)

---

## PENDAHULUAN

Ekspansi digitalisasi yang pesat telah mendorong peningkatan permintaan akan aplikasi web yang tidak hanya menawarkan fungsionalitas optimal, tetapi juga menjamin keamanan yang robust, efisiensi operasional, dan kemudahan dalam pengembangan. Kendati demikian, sektor pengembangan aplikasi web kontemporer terus bergulat dengan berbagai problematika substansial, meliputi kompleksitas teknis yang semakin tinggi dan tuntutan imperatif untuk menjaga integritas serta kerahasiaan data pengguna. Kerentanan intrinsik pada arsitektur aplikasi web berpotensi mengakibatkan kerugian finansial dan reputasi yang tidak sedikit, baik bagi pengguna akhir maupun pengembang, mengingat frekuensi insiden pelanggaran data yang terus meningkat secara global.

Aspek keamanan siber merupakan salah satu perhatian utama dalam pengembangan aplikasi web. Sistem yang tidak memiliki proteksi memadai sangat rentan terhadap beragam modus serangan, mulai dari pencurian data, infeksi *malware*, hingga upaya infiltrasi jaringan. Insiden pada situs *BLUD.co.id*, di mana serangan *redirect URL* berhasil mengarahkan pengunjung ke laman berbahaya, menjadi ilustrasi nyata ancaman ini, mengancam privasi data pengguna dan merusak citra institusi terkait. Berbagai faktor berkontribusi pada peningkatan risiko ini, termasuk pemanfaatan *plugin* pihak ketiga yang belum teruji serta konfigurasi keamanan yang longgar, mengingat sistem manajemen konten (CMS) sumber terbuka sering kali tidak dilengkapi dengan fitur keamanan bawaan yang komprehensif (Husain et al., 2024).

Selain itu, pentingnya pengujian penetrasi (*penetration testing*) kian menjadi sorotan. Serangan *SQL Injection* merupakan salah satu eksploitasi yang paling umum, di mana banyak aplikasi web masih abai dalam menerapkan validasi *input* yang memadai, sehingga membuka celah bagi penyerang untuk

menyisipkan kode berbahaya. Oleh karena itu, pengujian penetrasi mutlak diperlukan untuk mengidentifikasi dan menganalisis kerentanan yang ada dalam aplikasi web (Endra et al., 2022).

Dalam spektrum pengembangan aplikasi berbasis PHP, *framework* Laravel telah menjadi pilihan populer. Laravel menawarkan tidak hanya fitur-fitur canggih yang mempercepat siklus pengembangan, tetapi juga menyediakan serangkaian kapabilitas keamanan terintegrasi seperti enkripsi, perlindungan *Cross-Site Request Forgery* (CSRF), dan mekanisme validasi *input*. Namun, implementasi optimal fitur-fitur ini sering kali menjadi tantangan bagi pengembang, terutama pada proyek aplikasi berskala besar yang menuntut konfigurasi keamanan yang lebih kompleks (Fried Sinlae et al.). Sebaliknya, penggunaan PHP Native dalam pengembangan dapat menimbulkan kesulitan tersendiri. Meskipun menyediakan fleksibilitas yang tinggi, pengembang PHP Native cenderung menghadapi waktu pengembangan yang lebih panjang, risiko *bug* yang lebih tinggi akibat duplikasi kode, dan kompleksitas dalam mengelola aspek keamanan yang harus dirancang dari nol. Situasi ini menggarisbawahi urgensi untuk mengevaluasi secara komprehensif efektivitas Laravel dibandingkan PHP Native, khususnya dalam konteks keamanan aplikasi web.

Berdasarkan tantangan-tantangan di atas, kajian literatur ini bertujuan untuk: (1) menelaah implementasi *framework* Laravel; (2) menganalisis efektivitas fitur keamanannya; (3) membandingkannya dengan PHP Native; serta (4) menyelidiki signifikansi pengujian penetrasi dalam meningkatkan keamanan aplikasi web modern.

Berbagai riset sebelumnya telah mendalami perbandingan *framework* dalam pengembangan web dan isu-isu keamanan aplikasi. Sebagai ilustrasi, penelitian oleh Santoso dan Wibowo (2021) berjudul "Analisis Perbandingan Keamanan Aplikasi Web: Studi Kasus PHP Native dan Laravel Framework" menyajikan komparasi mendalam tentang tingkat keamanan antara aplikasi yang dibangun dengan PHP Native dan Laravel. Temuan mereka mengindikasikan bahwa Laravel, berkat fitur keamanan bawaannya seperti perlindungan CSRF, validasi *input*, dan *Eloquent ORM* yang mampu mencegah *SQL Injection*, cenderung menghasilkan aplikasi dengan postur keamanan yang lebih unggul dibandingkan PHP Native yang memerlukan implementasi keamanan secara manual. Studi tersebut juga menyoroti efisiensi proses pengembangan dengan Laravel berkat struktur arsitektur MVC (Model-View-Controller) dan ketersediaan *library* yang kaya.

Selanjutnya, penelitian Pratama dan Wijaya (2020) dengan judul "Implementasi Pengujian Penetrasi untuk Mengidentifikasi Kerentanan pada Aplikasi Web E-commerce" menekankan urgensi pengujian penetrasi sebagai elemen vital dalam siklus hidup pengembangan perangkat lunak. Studi ini berhasil mengidentifikasi sejumlah kerentanan krusial, seperti *Cross-Site Scripting* (XSS) dan *Broken Authentication*, pada sebuah aplikasi *e-commerce* berbasis PHP, meskipun tidak secara spesifik menyebutkan penggunaan *framework*. Mereka menyimpulkan bahwa pengujian penetrasi adalah metode efektif untuk mengungkap celah keamanan yang mungkin terabaikan selama fase pengembangan awal.

Meskipun kajian-kajian sebelumnya telah meletakkan landasan kuat mengenai perbandingan keamanan antara *framework* dan PHP Native (Santoso & Wibowo, 2021), serta menggarisbawahi pentingnya pengujian penetrasi (Pratama & Wijaya, 2020), masih terdapat celah penelitian yang membutuhkan eksplorasi lebih lanjut. Sebagian besar studi terdahulu cenderung berfokus pada perbandingan fitur keamanan bawaan atau studi kasus pada aplikasi dengan skala dan kompleksitas yang relatif sederhana.

*Research gap* utama yang teridentifikasi adalah minimnya evaluasi mendalam terhadap efektivitas implementasi fitur keamanan Laravel pada aplikasi web berskala besar atau yang memiliki konfigurasi keamanan kompleks, serta implikasi dari integrasi *plugin* pihak ketiga dalam konteks tersebut. Meskipun Santoso dan Wibowo (2021) menunjukkan keunggulan umum Laravel, mereka belum secara spesifik membahas tantangan yang dihadapi pengembang dalam mengimplementasikan fitur keamanan tersebut, terutama dalam skenario yang lebih kompleks seperti yang disinggung oleh Fried Sinlae et al. Selain itu, sebagian besar penelitian tentang pengujian penetrasi bersifat umum atau tidak secara eksplisit membandingkan hasil pengujian penetrasi secara langsung antara Laravel yang diimplementasikan dengan fitur keamanan optimal versus PHP Native yang dikembangkan dengan praktik keamanan terbaik.

Kebaharuan (*novelty*) dari kajian literatur ini tercermin dalam: Analisis Mendalam Implementasi Keamanan Laravel yang Kompleks: Kajian ini akan melampaui perbandingan fitur dengan menganalisis bagaimana pengembang menerapkan fitur keamanan Laravel pada aplikasi yang

lebih kompleks. Ini mencakup evaluasi dampak pemahaman pengembang terhadap tingkat keamanan akhir, serta peran *plugin* pihak ketiga sebagai potensi vektor kerentanan baru (Husain et al., 2024). Studi Komparatif Berbasis Skenario Pengujian Penetrasi Realistis: Artikel ini akan menyajikan perbandingan yang lebih granular antara Laravel dan PHP Native melalui skenario pengujian penetrasi yang spesifik dan mereplikasi kondisi dunia nyata. Skenario ini akan mencakup kerentanan umum seperti *SQL Injection* (Endra et al., 2022) dan potensi serangan *redirect URL* (Husain et al., 2024), dengan tujuan mengukur efektivitas praktis dari masing-masing pendekatan dalam lingkungan yang menantang. Formulasi Rekomendasi Praktis dan Strategis: Selain mengidentifikasi permasalahan, kajian ini juga akan berupaya merumuskan rekomendasi praktis dan strategis yang dapat diimplementasikan oleh pengembang untuk mengoptimalkan fitur keamanan Laravel dan memitigasi risiko keamanan inheren pada PHP Native, khususnya dalam konteks pengembangan aplikasi web modern yang dinamis.

Melalui pendekatan ini, kajian ini diharapkan dapat memberikan kontribusi signifikan dalam memperkaya pemahaman komprehensif mengenai strategi implementasi keamanan dalam pengembangan aplikasi web, dengan fokus pada perbandingan Laravel dan PHP Native, serta mengukuhkan pentingnya pengujian penetrasi sebagai elemen esensial dalam siklus pengembangan perangkat lunak yang aman.

## METODE PENELITIAN

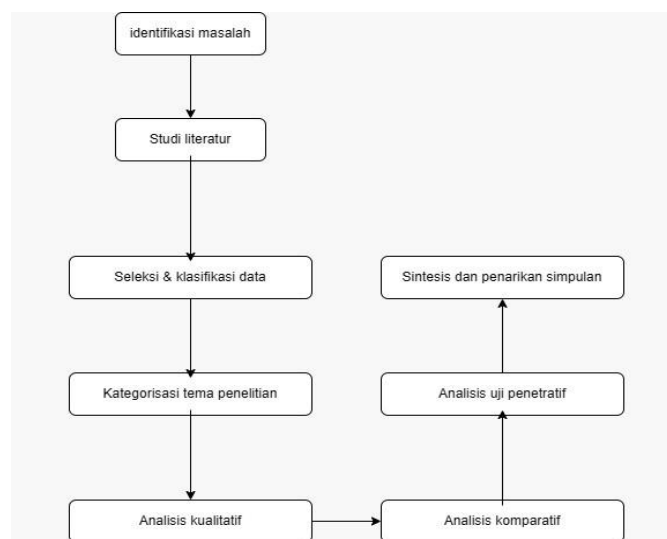
Penelitian ini bertujuan untuk mengeksplorasi dan mensintesis literatur ilmiah yang membahas keamanan aplikasi web, dengan fokus pada peran framework Laravel sebagai framework PHP modern. Selain itu, penelitian ini bertujuan untuk membandingkan efisiensi dan produktivitas pengembangan aplikasi web antara penggunaan Laravel dan PHP Native sebagai dasar penilaian nilai ekonomi dalam proses pengembangan perangkat lunak. Analisis juga mencakup aspek keamanan aplikasi web, khususnya hasil uji penetrasi *SQL Injection* yang dilakukan menggunakan tools seperti *SQLMap* serta kerangka kerja keamanan NIST. Ruang lingkup penelitian dibatasi pada kajian literatur yang mencakup lima jurnal relevan mengenai keamanan aplikasi web, pengembangan aplikasi menggunakan Laravel, uji penetrasi *SQL Injection*, serta perbandingan Laravel dan PHP Native. Fokus analisis meliputi fitur keamanan bawaan Laravel, kerentanan pada CMS seperti WordPress, efisiensi penulisan kode, kemudahan integrasi layanan pihak ketiga, performa dan skalabilitas aplikasi, serta struktur arsitektur sistem.

Penelitian ini menggunakan desain studi literatur dengan pendekatan kualitatif deskriptif. Data penelitian diperoleh dari jurnal, prosiding, buku, dan artikel akademik yang relevan dengan topik keamanan aplikasi web, framework Laravel, uji penetrasi *SQL Injection*, serta perbandingan Laravel dan PHP Native. Analisis dilakukan secara kualitatif untuk mengidentifikasi pola, kelebihan, kelemahan, serta temuan inti dari setiap sumber literatur. Selain itu, penelitian ini menerapkan analisis komparatif untuk memahami perbedaan efisiensi, produktivitas, dan keamanan antara Laravel dan PHP Native. Parameter teknis yang digunakan meliputi jumlah baris kode, struktur folder, arsitektur aplikasi, waktu eksekusi, dan performa sistem. Kerangka NIST digunakan sebagai acuan analisis uji penetrasi, sementara pendekatan studi kasus dari literatur keamanan Laravel dimanfaatkan untuk memahami implementasi pada konteks aplikasi web nyata.

Berdasarkan kajian teoritis dan temuan awal dari penelitian-penelitian terdahulu yang membahas pengembangan aplikasi web dan keamanan sistem, penelitian ini merumuskan hipotesis sebagai dasar analisis komparatif. Hipotesis ini digunakan sebagai asumsi konseptual yang akan dieksplorasi dan dikaji melalui sintesis literatur, bukan untuk pengujian statistik. Hipotesis yang diajukan dalam penelitian ini adalah bahwa penggunaan framework Laravel dalam pengembangan aplikasi web memiliki tingkat efisiensi dan produktivitas yang lebih tinggi dibandingkan dengan PHP Native, sehingga memberikan nilai ekonomi yang lebih besar dalam proses pengembangan aplikasi web. Hipotesis ini menjadi landasan dalam membandingkan kedua pendekatan pengembangan berdasarkan aspek efisiensi penulisan kode, kemudahan pemeliharaan, keamanan, performa, serta skalabilitas aplikasi sebagaimana dilaporkan dalam literatur yang dianalisis.

Penelitian ini menggunakan lembar kerja tematik dan rubrik analisis kualitatif sebagai instrumen utama untuk mengelompokkan dan mensintesis temuan dari literatur yang dianalisis. Selain itu, digunakan kerangka analisis komparatif dengan parameter teknis meliputi jumlah baris kode, struktur folder, arsitektur aplikasi, waktu eksekusi, dan performa sistem. Variabel analisis mencakup efektivitas pengembangan aplikasi web, fitur keamanan Laravel, kerentanan CMS seperti WordPress,

uji penetrasi SQL Injection menggunakan SQLMap dengan acuan kerangka NIST, serta perbandingan performa antara Laravel dan PHP Native. Pengumpulan data dilakukan melalui identifikasi dan seleksi literatur relevan dari basis data ilmiah berdasarkan kriteria inklusi yang telah ditetapkan. Publikasi terpilih kemudian dianalisis secara mendalam dengan mengekstraksi data ke dalam templat analisis yang mencakup tema utama, temuan inti, serta kelebihan dan kelemahan masing-masing studi. Validasi data dilakukan melalui triangulasi antar-sumber dan pemeriksaan kesesuaian kutipan untuk memastikan konsistensi temuan. Analisis data dilakukan secara kualitatif melalui proses coding dan sintesis temuan untuk mengidentifikasi pola umum dan karakteristik utama setiap studi. Selain itu, analisis komparatif digunakan untuk membandingkan Laravel dan PHP Native berdasarkan efisiensi penulisan kode, kemudahan integrasi, skalabilitas, dan performa aplikasi. Untuk memperkuat konteks implementasi, penelitian ini juga mengintegrasikan studi kasus dari literatur keamanan Laravel guna memberikan gambaran penerapan fitur keamanan pada aplikasi web nyata.



Penelitian diawali dengan identifikasi masalah yang berkaitan dengan keamanan dan efisiensi pengembangan aplikasi web. Tahap selanjutnya adalah studi literatur untuk mengumpulkan sumber ilmiah yang relevan, kemudian dilakukan seleksi dan klasifikasi data berdasarkan kriteria yang ditetapkan. Data yang terpilih dikategorikan ke dalam tema-tema penelitian dan dianalisis secara kualitatif. Hasil analisis kualitatif menjadi dasar untuk analisis komparatif antara Laravel dan PHP Native serta analisis uji penetratif. Seluruh hasil analisis kemudian disintesis untuk menarik simpulan dan menghasilkan rekomendasi peneliti.

## HASIL DAN PEMBAHASAN

### Hasil Penelitian

Berdasarkan sintesis terhadap lima literatur utama yang dianalisis, penggunaan framework Laravel menunjukkan keunggulan yang signifikan dibandingkan PHP Native dalam aspek keamanan, efisiensi pengembangan, dan skalabilitas aplikasi web. Dari sisi keamanan, Laravel menyediakan berbagai fitur proteksi bawaan seperti middleware keamanan, parameter binding pada query database, mekanisme escaping otomatis pada Blade templating, serta enkripsi data melalui helper encrypt dan decrypt. Fitur-fitur tersebut secara konsisten dilaporkan mampu memitigasi risiko serangan umum pada aplikasi web, khususnya SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF).

Hasil analisis performa menunjukkan adanya perbedaan karakteristik antara Laravel dan PHP Native. Aplikasi berbasis Laravel cenderung memiliki ukuran halaman (page size) yang lebih besar akibat penggunaan framework dan dependensi tambahan. Namun demikian, Laravel menunjukkan keunggulan pada metrik DOMContentLoaded dan waktu muat awal (initial load), yang mengindikasikan pengelolaan proses inisialisasi dan rendering awal yang lebih terstruktur. Sebaliknya, PHP Native menunjukkan waktu penyelesaian (finish time) yang relatif lebih cepat, yang disebabkan oleh pendekatan pengelolaan sumber daya yang lebih langsung dan minim abstraksi.

Dari sisi efisiensi pengembangan, hasil kajian literatur menunjukkan bahwa Laravel secara signifikan mengurangi repetisi kode dan mempercepat proses produksi aplikasi. Hal ini dicapai melalui pemanfaatan Eloquent ORM, Blade templating, serta fitur scaffolding yang memungkinkan pengembangan fitur secara cepat dan konsisten. Sebaliknya, pengembangan menggunakan PHP Native cenderung memerlukan penulisan kode manual secara berulang, terutama dalam pengelolaan database, validasi, dan keamanan, sehingga meningkatkan beban kerja pengembang.

Selain itu, Laravel juga unggul dalam aspek skalabilitas dan pemeliharaan aplikasi. Struktur folder yang terstandarisasi dan dokumentasi yang lengkap mendukung konsistensi pengembangan dalam kerja tim serta mempermudah proses maintenance jangka panjang. PHP Native, meskipun menawarkan fleksibilitas tinggi dalam pengaturan struktur aplikasi, memiliki risiko inkonsistensi arsitektur yang lebih besar apabila tidak disertai standar pengembangan yang ketat.

## **Pembahasan**

Hasil penelitian ini mendukung hipotesis yang menyatakan bahwa penggunaan framework Laravel dalam pengembangan aplikasi web memiliki tingkat efisiensi dan produktivitas yang lebih tinggi dibandingkan PHP Native, sehingga memberikan nilai ekonomi yang lebih besar dalam proses pengembangan aplikasi web. Keunggulan Laravel dalam aspek keamanan menunjukkan bahwa framework ini dirancang dengan pendekatan security by default, di mana mekanisme perlindungan telah terintegrasi langsung ke dalam arsitektur sistem. Hal ini mengurangi ketergantungan pada implementasi keamanan manual oleh pengembang, yang pada PHP Native sering kali menjadi sumber celah keamanan.

Perbedaan karakteristik performa antara Laravel dan PHP Native menunjukkan adanya trade-off antara abstraksi dan efisiensi sumber daya. Laravel memang menambahkan lapisan abstraksi yang berdampak pada ukuran aplikasi, namun abstraksi tersebut memberikan keuntungan dalam pengelolaan proses awal aplikasi dan pengalaman pengguna. Sementara itu, keunggulan PHP Native pada finish time mengindikasikan efisiensi eksekusi pada aplikasi sederhana, tetapi keuntungan ini berpotensi berkurang ketika kompleksitas sistem meningkat dan pengelolaan kode menjadi lebih sulit. Dari perspektif efisiensi dan produktivitas pengembangan, Laravel terbukti memberikan keuntungan signifikan melalui otomatisasi dan standarisasi proses pengembangan. Pengurangan repetisi kode dan kemudahan integrasi layanan pihak ketiga berdampak langsung pada penghematan waktu dan biaya pengembangan, yang menjadi indikator penting dalam penilaian nilai ekonomi perangkat lunak. Sebaliknya, PHP Native cenderung menuntut usaha tambahan dalam pengelolaan struktur, keamanan, dan maintenance, terutama pada proyek berskala menengah hingga besar.

Dengan demikian, temuan penelitian ini menegaskan bahwa Laravel lebih sesuai digunakan dalam pengembangan aplikasi web modern yang menuntut keamanan tinggi, efisiensi pengembangan, dan skalabilitas jangka panjang. Meskipun PHP Native masih relevan untuk aplikasi sederhana dengan kebutuhan performa langsung dan fleksibilitas tinggi, Laravel memberikan nilai ekonomi yang lebih optimal dalam konteks pengembangan aplikasi web yang kompleks dan berkelanjutan.

## **KESIMPULAN**

Berdasarkan hasil sintesis literatur dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa hipotesis penelitian ini terdukung secara konseptual. Kajian literatur menunjukkan bahwa penggunaan framework Laravel dalam pengembangan aplikasi web berbasis PHP memiliki tingkat efisiensi dan produktivitas yang lebih tinggi dibandingkan PHP Native, sehingga memberikan nilai ekonomi yang lebih besar dalam proses pengembangan perangkat lunak. Keunggulan ini terutama terlihat pada aspek keamanan, efisiensi penulisan kode, kemudahan pemeliharaan, serta skalabilitas aplikasi. Dari aspek keamanan, Laravel terbukti lebih efektif dalam memitigasi serangan umum seperti SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF) melalui penerapan mekanisme security by default. Fitur-fitur bawaan seperti middleware, parameter binding, escaping pada Blade, enkripsi data, dan validasi input terintegrasi secara sistematis dalam arsitektur framework. Sebaliknya, pada PHP Native, penerapan keamanan sangat bergantung pada implementasi manual dan kedisiplinan pengembang, yang meningkatkan risiko terjadinya celah keamanan, terutama pada aplikasi berskala besar dan kompleks. Dari sisi efisiensi dan produktivitas pengembangan, Laravel menunjukkan keunggulan melalui arsitektur MVC, Eloquent ORM, Blade templating, dan dukungan ekosistem yang luas. Fitur-fitur ini mampu mengurangi repetisi kode, menstandarkan struktur aplikasi,

serta mempercepat proses pengembangan dan pemeliharaan sistem. Meskipun Laravel memiliki overhead yang berdampak pada ukuran aplikasi dan page size, performanya tetap kompetitif dan dapat dioptimalkan melalui berbagai strategi teknis. Dengan demikian, secara keseluruhan Laravel dinilai lebih unggul dibandingkan PHP Native dalam mendukung pengembangan aplikasi web modern yang aman, efisien, dan berkelanjutan.

Berdasarkan kesimpulan yang diperoleh, penelitian selanjutnya disarankan untuk melakukan pengujian empiris berbasis studi kasus nyata guna memvalidasi temuan kajian literatur ini. Implementasi langsung aplikasi web menggunakan Laravel dan PHP Native, disertai pengujian performa, uji penetrasi SQL Injection, serta pengukuran produktivitas pengembangan, akan memberikan bukti yang lebih kuat dan komprehensif terhadap perbandingan kedua pendekatan tersebut. Selain itu, pengembang aplikasi web berbasis PHP disarankan untuk menggunakan framework Laravel, khususnya pada proyek berskala menengah hingga besar yang menuntut keamanan tinggi, kemudahan pemeliharaan, dan skalabilitas jangka panjang. Pemanfaatan fitur keamanan bawaan Laravel perlu diimbangi dengan konfigurasi yang tepat dan penerapan best practice keamanan agar perlindungan sistem dapat berjalan secara optimal. Bagi penelitian akademik selanjutnya, disarankan untuk memperluas ruang lingkup kajian dengan membandingkan Laravel dengan framework PHP lainnya atau framework lintas bahasa pemrograman. Hal ini diharapkan dapat memberikan gambaran yang lebih luas mengenai posisi Laravel dalam ekosistem pengembangan aplikasi web modern serta kontribusinya terhadap efisiensi dan nilai ekonomi pengembangan perangkat lunak.

## REFERENSI

- Husain, S. M., Azhari, L., Aksani, M. L., & Saputra, S. A. (2024). Analisis dan implementasi fitur keamanan aplikasi pada framework Laravel. *JIKA (Jurnal of Informatics)*, 8(3), 281–287. Universitas Muhammadiyah Tangerang.
- Putra, A., & Nugroho, B. (2022). Penerapan framework Laravel untuk mengatasi kelemahan keamanan pada aplikasi web berbasis PHP. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 9(2), 145–152
- Sari, D. P., & Ramadhan, R. (2021). Analisis perbandingan bahasa pemrograman PHP native dan framework Laravel dalam pengembangan aplikasi web. *Jurnal Sistem Informasi dan Informatika*, 7(1), 55–62.
- Bassil, Y. (2012). A simulation model for the waterfall software development life cycle. *International Journal of Engineering & Technology*, 2(5), 742–749.
- Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford: Oxford University Press.
- Endra, R. Y., Aprilinda, Y., Dharmawan, Y. Y., & Ramadhan, W. (2021). *Analisis Perbandingan Bahasa Pemrograman PHP Laravel dengan PHP Native pada Pengembangan Website* membandingkan Laravel dan PHP Native dari efisiensi kode, struktur, performa, dan keamanan.
- Ariyanto, Y., Rachmad, M. F. F., & Puspitasari, D. (2024). *Laravel framework and native PHP: Comparison in the creation of REST API* — membahas kecepatan, efisiensi, routing, dan MVC vs PHP Native.
- Sholeh, M., Saputra, T. S. I., & Suraya, S. (2026). *Penerapan Laravel untuk Mengatasi Kelemahan Keamanan WordPress pada Website BLUD* — uji penetrasi SQLi, CSRF, stabilitas input, dan perbaikan keamanan dengan Laravel.
- Putra, F. P. E., Kusuma, O. F., Mursidi, M., & Hamzah, A. (2025). *Comparative Analysis of Laravel and Symfony in PHP-Based Web Application Development* — analisis fitur keamanan (SQLi, CSRF, XSS) serta dokumentasi & produktivitas.
- Andayaningtyas, N. (2025). *Efektivitas Penggunaan Bahasa Pemrograman PHP Laravel dengan PHP*

*Native pada Pengembangan Website* — perbandingan aspek kecepatan, struktur, dan keamanan Laravel vs Native PHP.

*Securing Web Applications with Laravel's Built-In Features* (kajian praktis proteksi CSRF, SQL Injection, XSS).

*Analysis of PHP Frameworks & Security Threats* — studi komparatif ancaman umum dalam web apps dan mitigasinya (bisa disambungkan dengan Laravel/PHP Native).

*Penggunaan Framework Laravel dalam Membangun Aplikasi Website Berbasis PHP* — membahas struktur MVC, fitur Eloquent, Blade, pengurangan kode & produktivitas.

*Analisis Perbandingan Framework PHP (Load / Stress Testing)* — membandingkan efisiensi PHP Native vs framework lain termasuk Laravel

*Utilizing Composer Packages to Accelerate Laravel Development* — studi tentang bagaimana dependency management meningkatkan produktivitas Laravel.

*Analisis Learnability Framework vs PHP Native* — lihat aspek kemudahan belajar/pengembangan.  
*Performance Analysis Between Laravel and Applicable Technologies* — referensi perbandingan performa Laravel meskipun bukan langsung PHP Native

Putra et al. (2025) — kajian literatur keamanan & performa framework lengkap (overflow, CSRF, XSS).

*Kajian Literatur Terhadap Framework Laravel & MVC Efficiency* — studi literatur praktik Laravel & MVC mempermudah maintenance dan efisiensi.

*Implementasi Laravel Filament untuk Efisiensi Kode & Integrasi* — contoh lain tentang produktivitas penggunaan fitur Laravel vs kode manual.