REVIEW JURNAL

WEB SECURITY: EMERGING THREATS AND DEFENSE

Judul	Web Security: Emerging Threats and Defense
Nama Jurnal	CSSE (Clareus Scientific Sciencea and Engineering
Volume dan Halaman	Vol.40, No.3, Halaman 1234 - 1248
Tahun	2022
Penulis	Almutairi, A, A., Mishra, S., Alshehri, m
Link Download	https://www.researchgate.net/profile/Shailendra-Mishra-5/publication/354879360_Web_Security_Emerging_Threats_and_Defense/links/61529300154b3227a8b3e7da/Web-Security-Emerging-Threats-and-Defense.pdf
Reviewer	Syaif Kishanif
Tanggal Reviewer	21 SEPTEMBER 2025
Latar Belakang	*Web Applications* telah menjadi metode yang banyak digunakan untuk mendukung internet selama satu dekade terakhir. Karena telah berhasil diterapkan dalam aktivitas bisnis dan adanya kebutuhan akan fungsionalitas yang lebih canggih, konfigurasi aplikasi web menjadi semakin kompleks
Permasalahan	Bagaimana Kerentanan aplikasi web memungkinkan penyusup membobol aplikasi web untuk menjalankan hal-hal yang tidak diinginkan pada situs korban tertentu. Kerentanan keamanan yang paling canggih banyak ditemukan dalam sistem, jaringan, dan program aplikasi masa kini
Tujuan penelitian	Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis empat vulnerability paling umum dan kritis dalam aplikasi web berbasis *PHP* dan *JAVA*. Deskripsi komprehensif mengenai kerentanan, eksploitasi,
Sumber data	Penelitian ini menganalisis celah kode pada *PHP* dan *JAVA* yang sengaja digunakan untuk pengujian, serta memanfaatkan laporan hasil pemindaian dari berbagai *Vulnerability scanner*, baik statis maupun dinamis

Metode penelitian	Penelitian ini dilakukan dengan membangun aplikasi web berbasis *PHP* dan *Java* yang mengandung kerentanan, kemudian diuji menggunakan berbagai vulnerability scanner baik statis maupun dinamis di lingkungan Windows dan Linux, lalu hasil pemindaian dibandingkan untuk menganalisis efektivitas masing-masing alat dalam mendeteksi *SQL Injection*, *XSS*, *Path Traversal, dan Command Injection.*
Objek penelitian	Objek penelitian ini adalah aplikasi web berbasis PHP dan Java yang mengandung celah keamanan, dengan fokus pada empat jenis utama: *SQL Injection, Cross-Site Scripting (XSS), Path Traversal,* dan *Command Injection.* yang diuji menggunakan berbagai vulnerability scanner statis dan dinamis.
Hasil penelitian	Hasil penelitian menunjukkan bahwa SQL Injection (*SQLi*) dan Cross-Site Scripting (*XSS*) paling sering ditemukan, sedangkan Path Traversal dan Command Injection lebih jarang. Penggunaan vulnerability scanner secara static dan dynamic menunjukkan perbedaan efektivitas: scanner dynamic lebih akurat tetapi lebih lambat, sedangkan scanner static lebih cepat namun cenderung melewatkan beberapa celah.
Kelebihan penelitian	Kelebihan penelitian ini adalah penggunaan metode eksperimen langsung dengan scanner static dan dynamic pada aplikasi berbasis PHP dan Java, sehingga hasilnya relevan dan aplikatif.
Kekurangan penelitian	Kekurangan penelitian ini adalah objek yang terbatas (hanya PHP & Java dengan 4 vulnerability), hasil sangat bergantung pada scanner yang digunakan, serta pengujian dilakukan pada aplikasi buatan di lab sehingga jika diterapkan pada kondisi nyata kemungkinan kurang efektif.
Diskusi / Rekomendasi	Rekomendasi dari penelitian ini adalah pentingnya mengombinasikan penggunaan static dan dynamic vulnerability scanner karena keduanya saling melengkapi. Selain itu, penelitian selanjutnya disarankan untuk memperluas objek ke bahasa dan vulnerability lain, serta melakukan pengujian pada aplikasi nyata agar hasil lebih representatif. Developer juga perlu

	meningkatkan awareness dalam praktik coding yang aman, dan vulnerability scanner sebaiknya diintegrasikan ke proses pengembangan aplikasi.