TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

Analisis Komparatif OWASP ZAP dan Nuclei pada Vulnerability Scanning Non-Intrusive Aplikasi Web E-Commerce Publik

Bambang Harie Wiyono, Rintan Madi Sari*, Lukman Rosyidi

Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Depok, Indonesia
Email: [1]bambang.harie@nurulfikri.ac.id, [2,*]rint22156ti@student.nurulfikri.ac.id, [3]lukman@nurulfikri.ac.id
Email Penulis Korespondensi: rint22156ti@student.nurulfikri.ac.id

Abstrak–Penelitian ini membahas analisis komparatif hasil *vulnerability scanning non-intrusive* pada aplikasi web *e-commerce* publik menggunakan OWASP ZAP dan Nuclei. Penelitian ini tidak diarahkan untuk membuktikan eksploitasi kerentanan secara langsung, melainkan untuk mengevaluasi karakteristik keluaran pemindaian berdasarkan jumlah temuan agregat, temuan unik setelah deduplikasi, distribusi *severity* CVSS v3.1, pemetaan OWASP Top 10, *overlap*, serta temuan prioritas yang memerlukan validasi manual. Pengujian dilakukan dengan pendekatan *black-box* dan *non-intrusive* pada lima target yang diberi kode E1 sampai E5. Pemberian kode dilakukan untuk menjaga etika pengujian pada target publik, sedangkan pemilihan target didasarkan pada akses aplikasi web yang terbuka, relevansi terhadap konteks *e-commerce*, serta variasi karakteristik layanan yang dapat diamati dari sisi eksternal. Hasil penelitian menunjukkan terdapat 83 temuan agregat yang terdiri atas 68 temuan OWASP ZAP dan 15 temuan Nuclei. Setelah proses normalisasi dan deduplikasi, diperoleh 81 temuan unik dengan 2 temuan *overlap*. OWASP ZAP menghasilkan keluaran yang lebih konsisten pada beberapa target dan dominan pada kategori *Security Misconfiguration*, khususnya *security header*, *Content Security Policy*, *cache-control*, dan atribut *cookie*. Sementara itu, Nuclei menghasilkan jumlah temuan lebih sedikit, tetapi memberikan kontribusi penting karena mendeteksi 5 temuan *Critical* dan 3 temuan *High*, terutama pada target E4. Keterbatasan penelitian terdapat pada kendala *output* beberapa target, sehingga hasil pemindaian tidak dapat ditafsirkan sebagai kondisi keamanan final dari target, melainkan sebagai indikasi teknis awal yang perlu divalidasi lebih lanjut. Penelitian ini tidak mengukur *precision*, *recall*, *false positive rate*, maupun efisiensi waktu pemindaian karena pengujian dilakukan pada target publik dengan batasan *non-intrusive* dan tanpa *Proof of Concept*. Hasil penelitian menunjukkan bahwa kombinasi OWASP ZAP dan Nuclei memberikan cakupan analisis yang lebih lengkap dibandingkan penggunaan satu *scanner*, karena keduanya memiliki karakteristik deteksi yang berbeda dan saling melengkapi.

Kata Kunci: Keamanan *Web*; *E-Commerce*; *Vulnerability Scanning*; OWASP ZAP; Nuclei

Abstract–This study discusses a comparative analysis of non-intrusive vulnerability scanning results on public e-commerce web applications using OWASP ZAP and Nuclei. This study is not intended to directly prove vulnerability exploitation, but rather to evaluate the characteristics of scanning outputs based on the number of aggregate findings, unique findings after deduplication, CVSS v3.1 severity distribution, OWASP Top 10 mapping, overlap, and priority findings that require manual validation. Testing was conducted using a black-box and non-intrusive approach on five targets coded E1 to E5. The coding was applied to maintain testing ethics on public targets, while target selection was based on open web application access, relevance to the e-commerce context, and variations in service characteristics that could be observed externally. The results showed 83 aggregate findings, consisting of 68 OWASP ZAP findings and 15 Nuclei findings. After the normalization and deduplication process, 81 unique findings were obtained with 2 overlapping findings. OWASP ZAP produced more consistent outputs across several targets and was dominant in the Security Misconfiguration category, particularly security headers, Content Security Policy, cache-control, and cookie attributes. Meanwhile, Nuclei produced fewer findings but made an important contribution by detecting 5 Critical findings and 3 High findings, especially on target E4. The limitation of this study lies in output constraints on several targets; therefore, the scanning results cannot be interpreted as the final security condition of the targets, but rather as initial technical indications that require further validation. This study does not measure precision, recall, false positive rate, or scanning time efficiency because the testing was conducted on public targets under non-intrusive limitations and without Proof of Concept. The results indicate that the combination of OWASP ZAP and Nuclei provides more complete analysis coverage than the use of a single scanner because both have different and complementary detection characteristics.

Keywords: Web Security; E-Commerce; Vulnerability Scanning; OWASP ZAP; Nuclei

1. PENDAHULUAN

Dalam lima tahun terakhir, eskalasi ancaman siber terhadap aplikasi web semakin menonjol, terutama pada layanan digital yang mengelola transaksi finansial, data pribadi, dan aktivitas pengguna dalam skala besar. Analisis berbasis data historis menunjukkan bahwa tren dan modus *cybercrime* berkembang dari waktu ke waktu, mencakup ragam serangan seperti *phishing* dan *ransomware*, serta mendorong organisasi memperkuat strategi mitigasi secara adaptif (Abdullah et al., 2025). Pada konteks *e-commerce*, peningkatan ancaman tersebut menjadi relevan karena platform *e-commerce* memproses data bernilai ekonomi tinggi dan memiliki risiko penyalahgunaan yang dapat berdampak pada kepercayaan pengguna, reputasi bisnis, serta keberlangsungan layanan. Oleh karena itu, evaluasi keamanan aplikasi web perlu dilakukan secara terukur untuk membantu mengidentifikasi indikasi kerentanan sebelum dimanfaatkan oleh pihak tidak berwenang. Dalam konteks *e-commerce*, risiko kebocoran data menjadi perhatian penting karena layanan ini memproses informasi akun, riwayat transaksi, aktivitas pengguna, serta data finansial yang bernilai tinggi.

Untuk menekan risiko sebelum terjadi eksploitasi, organisasi perlu melakukan identifikasi celah secara sistematis. Salah satu pendekatan yang umum digunakan untuk mengidentifikasi potensi kerentanan pada aplikasi *web* adalah *vulnerability scanning*, yaitu pemeriksaan terstruktur untuk menemukan indikasi kelemahan sebelum dimanfaatkan pihak tidak berwenang. Kerentanan pada aplikasi *web*, seperti *SQL Injection*, *Cross-Site Scripting*, dan


TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

Security Misconfiguration, sering dilaporkan sebagai vektor serangan dominan karena dapat berujung pada pengambilalihan sesi, pencurian data, atau manipulasi transaksi. Studi evaluasi *black-box web application security scanner* menunjukkan bahwa pengujian pada sistem menyerupai layanan nyata masih menghadapi tantangan akurasi deteksi, terutama pada kategori injeksi tertentu (Althunayyan et al., 2022). Selain itu, pemetaan literatur *security testing* aplikasi *web* menunjukkan bahwa teknik dan *scanner* yang digunakan dapat menghasilkan keluaran berbeda karena variasi cakupan uji, aturan deteksi, dan cara pelaporan (Aydos et al., 2022).

Perkembangan platform *e-commerce* publik menjadikan aplikasi *web* sebagai infrastruktur utama untuk mendukung transaksi, autentikasi, pencarian produk, hingga proses pembayaran yang melibatkan data pribadi dan finansial pengguna. Seiring bertambahnya kompleksitas fitur, integrasi antarlayanan, serta pemanfaatan layanan pihak ketiga, *attack surface* pada sistem *e-commerce* cenderung meluas. Konsekuensinya, peluang eksploitasi celah keamanan turut meningkat dan berpotensi menimbulkan gangguan layanan, penyalahgunaan akun, maupun kebocoran data. Literatur menegaskan bahwa ancaman keamanan siber pada *e-commerce* merupakan tantangan yang terus berkembang karena penyerang terus menemukan kelemahan baru pada manusia, organisasi, dan teknologi yang digunakan (Liu et al., 2022). Keamanan aplikasi *web* juga perlu dipahami melalui hubungan antara *threat*, *vulnerability*, dan *protection*, karena eksploitasi sering memanfaatkan kelemahan *input validation*, konfigurasi, atau kontrol akses yang kurang ketat (Mohammed et al., 2021).

Dengan demikian, evaluasi keamanan berbasis data menjadi penting agar organisasi tidak hanya melakukan pemindaian, tetapi juga memperoleh gambaran kualitas temuan secara lebih terukur. Dataset deret waktu ancaman siber terbaru menunjukkan bahwa ancaman dapat dianalisis secara kuantitatif untuk memahami korelasi maupun pola tertentu yang pada akhirnya memperkuat urgensi evaluasi keamanan berbasis bukti atau *evidence-based security* (Sufi, 2024). Dalam konteks *e-commerce* publik, evaluasi yang terukur diperlukan untuk mendukung penentuan strategi pengujian keamanan yang relevan terhadap karakteristik target yang kompleks, berlapis kontrol, dan berpotensi memiliki pembatasan akses. Oleh karena itu, penelitian pada area evaluasi efektivitas *vulnerability scanning* menjadi penting untuk mendukung pengambilan keputusan keamanan yang lebih akuntabel.

Pada penelitian sebelumnya terkait evaluasi *web vulnerability scanner*, ditemukan bahwa hasil pemindaian dapat sangat bervariasi antar pendekatan maupun antar *scanner*, baik dari sisi jumlah temuan maupun tingkat keberhasilan mendeteksi kategori kerentanan tertentu. *Systematic literature review* menunjukkan bahwa evaluasi kuantitatif yang tersedia masih terbatas dan bahkan cenderung fokus pada jenis kerentanan tertentu, sementara variasi tingkat deteksi yang dilaporkan antarstudi juga tinggi (Alazmi & De Leon, 2022). Penelitian lain menunjukkan perbedaan performa antar *scanner* dalam skenario pengujian aplikasi *web*, sehingga pemilihan pendekatan pemindaian dan metodologi pengujian memengaruhi keluaran analisis keamanan (Kondraciuk et al., 2022). Studi terbaru oleh (Yuzar & Rahmatulloh, 2025) juga menunjukkan bahwa perbandingan alat vulnerability scanning seperti OWASP ZAP, Acunetix, dan Nikto dapat menghasilkan perbedaan jumlah temuan, jenis kerentanan, serta efisiensi pemindaian. Perbedaan tersebut juga berkaitan dengan parameter keamanan *web* yang harus dievaluasi secara komprehensif, termasuk kualitas temuan, *false positive*, dan relevansi hasil terhadap risiko aplikasi (Shahid et al., 2022). Evaluasi pada *scanner open-source* berbasis OWASP *Benchmark* turut menunjukkan bahwa *precision* dan *recall* dapat berbeda bergantung pada target serta kategori kerentanan yang diuji (Sarpong et al., 2021).

Namun, sebagian besar studi komparatif masih berfokus pada aplikasi uji, benchmark, atau sistem tertentu yang berada dalam lingkungan terkontrol. Kondisi tersebut belum sepenuhnya merepresentasikan tantangan pemindaian pada *e-commerce* publik yang berjalan di lingkungan nyata, memiliki mekanisme proteksi berlapis, serta dapat memberikan respons berbeda terhadap *scanner* eksternal. Selain itu, penelitian yang menggunakan lebih dari satu *scanner* belum selalu menjelaskan proses penyamaan *output*, deduplikasi, pemetaan kategori, maupun pemilihan temuan prioritas secara rinci. Dengan demikian, gap penelitian ini bukan hanya pada penggunaan multi-*scanner*, tetapi pada kebutuhan evaluasi *non-intrusive* yang menerapkan prosedur seragam, normalisasi, deduplikasi, pemetaan OWASP Top 10, penilaian CVSS v3.1, analisis *overlap*, dan identifikasi temuan unik pada beberapa target *e-commerce* publik. Kebutuhan evaluasi pada lingkungan modern juga terlihat pada penelitian tentang vulnerability assessment untuk arsitektur microservices yang kompleks (Izzat et al., 2025), serta studi implementasi OWASP ZAP dan Nuclei yang menunjukkan perbedaan fokus deteksi pada sistem web tertentu (Rahman et al., 2025).

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk membandingkan karakteristik keluaran OWASP ZAP dan Nuclei dalam proses *vulnerability scanning non-intrusive* pada aplikasi web *e-commerce* publik. Perbandingan dilakukan dengan melihat jumlah temuan agregat, temuan unik setelah deduplikasi, *overlap*, cakupan kategori OWASP Top 10, tingkat keparahan berdasarkan CVSS v3.1, serta temuan prioritas yang membutuhkan validasi manual. Dengan demikian, efektivitas *scanner* tidak hanya dinilai dari banyaknya temuan, tetapi juga dari cakupan deteksi, konsistensi *output*, relevansi risiko, dan karakter teknis masing-masing alat. Kontribusi penelitian ini terletak pada penyusunan alur evaluasi yang membantu membedakan hasil scanning sebagai indikasi teknis awal dari kerentanan yang telah terbukti melalui eksploitasi manual.

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

2. METODOLOGI PENELITIAN

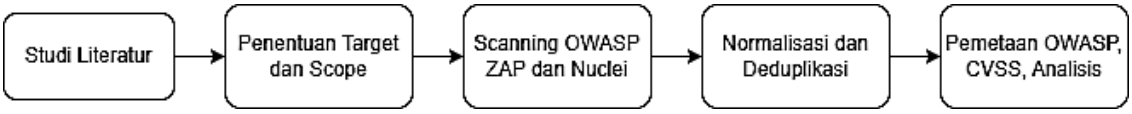
2.1 Kerangka Dasar Penelitian

Penelitian ini menggunakan rancangan komparatif-kuantitatif untuk membandingkan keluaran dua vulnerability *scanner*, yaitu OWASP ZAP dan Nuclei, pada pengujian keamanan aplikasi web *e-commerce* publik. Pengujian dilakukan secara *black-box* dari sisi eksternal dan bersifat *non-intrusive*, sehingga penelitian hanya mengamati respons dan indikasi teknis yang diberikan sistem tanpa melakukan eksploitasi manual, perubahan data, brute force, *credential attack*, transaksi nyata, *stress testing*, atau tindakan yang dapat mengganggu layanan target. Unit analisis penelitian adalah temuan yang dihasilkan masing-masing *scanner* pada setiap target dan *endpoint* yang berada dalam ruang lingkup uji. Rancangan komparatif dipilih karena OWASP ZAP dan Nuclei memiliki mekanisme deteksi, format laporan, dan jenis temuan yang berbeda, sehingga hasilnya perlu dibandingkan menggunakan indikator yang sama agar lebih adil dan dapat ditelusuri. Pembatasan ruang lingkup, dokumentasi prosedur, dan batas otorisasi tersebut sejalan dengan prinsip vulnerability assessment and penetration testing yang menempatkan *scope*, metode, serta kontrol etika sebagai bagian penting dalam pengujian keamanan aplikasi web (Wardana et al., 2022).

Objek penelitian berupa lima aplikasi web *e-commerce* publik yang diberi kode E1, E2, E3, E4, dan E5. Penggunaan kode dilakukan sebagai pertimbangan etis karena target merupakan layanan publik yang tidak berada dalam kontrol peneliti, sehingga identitas target tidak ditampilkan untuk menghindari penyalahgunaan informasi hasil pemindaian. Meskipun identitas target tidak dibuka, pemilihan target tetap didasarkan pada kriteria metodologis, yaitu memiliki akses web publik, relevan dengan konteks *e-commerce*, dapat diuji dari sisi eksternal, dan memiliki variasi karakteristik layanan yang memungkinkan perbandingan keluaran *scanner*. Dengan demikian, anonimisasi target tidak dimaksudkan untuk mengurangi transparansi prosedur, tetapi untuk menjaga batas etika pengujian pada sistem publik. Untuk memperkuat keterulangan proses, konfigurasi pengujian, status pelaksanaan scanning, dan kriteria validasi *output* tetap dijelaskan dalam metode dan hasil penelitian.

Karena penelitian dilakukan secara *non-intrusive*, seluruh temuan *scanner* diperlakukan sebagai indikasi teknis awal, bukan sebagai bukti eksploitasi final. Untuk mengurangi risiko *false positive*, hasil pemindaian disaring melalui beberapa tahap, yaitu pemeriksaan kelengkapan *output*, normalisasi nama temuan, penyamaan kategori risiko, deduplikasi berdasarkan target dan *endpoint*, pemetaan ke OWASP Top 10, serta penilaian *severity* menggunakan CVSS v3.1 atau padanan skor yang relevan. Temuan dianggap duplikat apabila dua keluaran dari *scanner* berbeda memiliki kesamaan pada target, *endpoint* atau parameter yang diuji, kategori kerentanan, dan bukti teknis yang ekuivalen. Temuan dengan kategori *Critical* dan *High* ditempatkan sebagai temuan prioritas yang membutuhkan validasi manual lebih lanjut. Dengan pendekatan ini, istilah temuan yang dianalisis dalam penelitian tidak dimaknai sebagai kerentanan yang telah berhasil dieksploitasi, melainkan sebagai *output scanner* yang memenuhi kriteria verifikasi awal dan layak dipertimbangkan dalam evaluasi keamanan.

2.2 Tahapan Penelitian



Gambar 1. Tahapan Penelitian

Gambar 1 menunjukkan tahapan operasional penelitian yang disusun agar proses pengumpulan dan analisis data dapat ditelusuri. Tahap pertama adalah studi pustaka untuk menetapkan landasan teori, indikator evaluasi, dan dasar pembanding dari penelitian terdahulu. Tahap kedua adalah analisis kebutuhan dan reconnaissance awal untuk menentukan target, ruang lingkup URL, batasan pengujian, serta parameter pelaksanaan yang dijaga konsisten. Tahap ketiga adalah scanning menggunakan OWASP ZAP dan Nuclei pada target yang sama dengan batas *non-intrusive*. Tahap keempat adalah ekstraksi hasil mentah dari laporan OWASP ZAP, *output* Nuclei, dan artefak bukti pemindaian. Tahap kelima adalah normalisasi dan deduplikasi agar temuan yang sama tidak dihitung ganda. Tahap keenam adalah pemetaan temuan ke OWASP Top 10 dan penilaian *severity* menggunakan CVSS v3.1. Tahap terakhir adalah analisis deskriptif-komparatif untuk membandingkan jumlah temuan, cakupan kategori, distribusi *severity*, *overlap*, temuan unik, serta temuan prioritas.

Instrumen utama penelitian terdiri dari OWASP ZAP sebagai *scanner* DAST berbasis proxy dan Nuclei sebagai *scanner* berbasis *template*. OWASP ZAP digunakan untuk melakukan *crawling*, *passive scanning*, dan *active scanning* terbatas pada ruang lingkup yang ditentukan. Alat ini lebih banyak berinteraksi dengan respons HTTP aplikasi sehingga relevan untuk mendeteksi kelemahan konfigurasi seperti *security header*, *Content Security Policy*, *cache-control*, *cookie attributes*, dan informasi aplikasi yang terekspos. Nuclei digunakan untuk mendeteksi indikator kerentanan berdasarkan *template* yang mencocokkan pola tertentu, termasuk CVE, *exposure*, Injection, *Server-Side Request Forgery*, *missing-sri*, dan *external-service-interaction*. Perbedaan mekanisme tersebut menjadi dasar metodologis mengapa kedua *scanner* dibandingkan dan dikombinasikan dalam penelitian ini. Penggunaan lebih dari satu *scanner* dipilih karena studi multi-*scanner* menunjukkan bahwa kombinasi alat dapat membantu memperluas cakupan deteksi dibandingkan penggunaan *scanner* tunggal (Abdulghaffar et al., 2023), sedangkan penggunaan OWASP ZAP dalam evaluasi

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

keamanan web juga telah digunakan pada studi implementasi keamanan aplikasi untuk mengidentifikasi kelemahan konfigurasi dan kebutuhan perbaikan kode (Fandier Saragih et al., 2023).

Pengolahan data dilakukan dengan menggabungkan hasil mentah tiap *scanner* ke dalam dataset terstruktur. Setiap *output* dicatat berdasarkan kode target, alat, status pelaksanaan, jenis temuan, kategori OWASP Top 10, *severity*, dan catatan validasi. Hasil yang tidak memiliki *output* akhir terstruktur tidak langsung ditafsirkan sebagai target aman, tetapi dicatat sebagai keterbatasan cakupan deteksi. Setelah itu, proses normalisasi dilakukan untuk menyamakan istilah temuan yang berbeda namun memiliki makna teknis serupa. Deduplikasi dilakukan menggunakan rumus total temuan unik = temuan OWASP ZAP + temuan Nuclei - temuan *overlap*. Indikator evaluasi digunakan secara deskriptif-komparatif, bukan sebagai model statistik inferensial, karena penelitian ini bertujuan membandingkan karakter keluaran *scanner* pada kondisi pengujian publik yang dibatasi secara etis. Penetapan indikator ini juga mengacu pada gagasan evaluasi *scanner* yang tidak hanya menilai jumlah temuan, tetapi juga *functionality*, *effectiveness*, kualitas laporan, *usability*, serta cakupan kategori pengujian (Koman & Janiszewski, 2025).

Untuk menjaga validitas interpretasi, hasil pemindaian tidak langsung dinyatakan sebagai kerentanan yang terbukti, melainkan sebagai indikasi teknis awal. Pengendalian potensi *false positive* dilakukan melalui pemeriksaan kelengkapan *output*, normalisasi nama temuan, penyamaan kategori risiko, deduplikasi berdasarkan target dan *endpoint*, pemetaan ke OWASP Top 10, serta penilaian *severity* menggunakan CVSS v3.1 atau skor yang relevan dari *scanner*. Temuan yang berasal dari CVE atau *template* Nuclei tetap diberi status "perlu validasi manual" karena penelitian tidak melakukan *Proof of Concept*, eksploitasi manual, atau pengujian destruktif. Dengan demikian, penelitian ini tidak bertujuan mengukur *false positive rate*, *precision*, atau *recall*, melainkan membandingkan karakter keluaran OWASP ZAP dan Nuclei dalam batas pengujian *non-intrusive* pada aplikasi web *e-commerce* publik.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Bagian ini menyajikan hasil pelaksanaan *vulnerability scanning* terhadap lima aplikasi web *e-commerce* publik yang diberi kode E1, E2, E3, E4, dan E5. Pengujian dilakukan menggunakan OWASP ZAP dan Nuclei dengan pendekatan *black-box* dan *non-intrusive* sesuai batasan penelitian. Data hasil pengujian diperoleh dari laporan OWASP ZAP, keluaran Nuclei, serta bukti gambar hasil pemindaian yang terdapat pada artefak penelitian. Seluruh hasil kemudian direkap, dinormalisasi, dipetakan ke kategori OWASP Top 10, dan diberi tingkat keparahan berdasarkan CVSS v3.1 agar hasil dari kedua alat dapat dibandingkan secara lebih terukur. Karena proses dilakukan pada target publik, hasil yang ditampilkan diposisikan sebagai indikasi teknis awal dan tetap membutuhkan validasi manual untuk temuan prioritas.

Pada target E1, OWASP ZAP menampilkan beberapa temuan keamanan pada aplikasi yang diuji. Temuan tersebut meliputi tidak adanya header keamanan seperti *Content Security Policy*, *Strict-Transport-Security*, *X-Content-Type-Options*, serta *Missing Anti-clickjacking Header*. Selain itu, terdapat peringatan terkait konfigurasi *cookie* seperti *Cookie No HttpOnly Flag* dan *Cookie without SameSite Attribute* yang dapat meningkatkan risiko penyalahgunaan sesi apabila tidak dikonfigurasi dengan baik. Sementara itu, pemindaian Nuclei terhadap target E1 berhasil dijalankan dengan memuat ribuan *template* keamanan, tetapi hasil akhirnya menunjukkan tidak ada kerentanan yang cocok dengan *template* yang digunakan pada saat pengujian.

Pada target E2, OWASP ZAP menampilkan 24 *alert* dengan beberapa temuan utama, seperti *PII Disclosure*, *Absence of Anti-CSRF Tokens*, kelemahan konfigurasi *Content Security Policy*, *Application Error Disclosure*, serta konfigurasi *cookie* yang belum optimal. Nuclei juga menemukan beberapa *match*, yaitu *external-service-interaction*, *cookies-without-httponly*, *missing-sri*, *cookies-without-secure*, dan *waf-detect cloudfront*. Hasil pemindaian E2 menunjukkan bahwa OWASP ZAP dan Nuclei sama-sama mendeteksi potensi kelemahan konfigurasi keamanan, khususnya pada aspek *cookie*, header keamanan, penggunaan sumber daya eksternal, serta keberadaan mekanisme perlindungan WAF pada target.

Pada target E3, OWASP ZAP mendeteksi tujuh *alert* yang berkaitan dengan konfigurasi keamanan, seperti *Content Security Policy* Header Not Set, *Missing Anti-clickjacking Header*, *Strict-Transport-Security header* Not Set, *X-Content-Type-Options* Header Missing, serta *Timestamp Disclosure-Unix*. Selain itu, terdapat temuan *Re-examine Cache-control Directives* dan *User agent Fuzzer* yang mengindikasikan perlunya pemeriksaan lebih lanjut terhadap konfigurasi cache dan respons aplikasi terhadap variasi user agent. Nuclei terlihat menjalankan pemindaian terhadap target yang sama, tetapi bukti yang tersedia hanya menampilkan proses hingga tahap pemuatan *template* sehingga hasil akhir jumlah temuan belum dapat direkap sebagai data terstruktur.

Pada target E4, OWASP ZAP mendeteksi 12 *alert*, di antaranya *Application Error Disclosure*, *Content Security Policy* Header Not Set, *Missing Anti-clickjacking Header*, *Big Redirect Detected*, *Cross-Domain JavaScript Source File Inclusion*, *Strict-Transport-Security header* Not Set, *Timestamp Disclosure-Unix*, serta *X-Content-Type-Options* Header Missing. Nuclei berhasil menjalankan pemindaian dan menampilkan beberapa temuan, termasuk kerentanan dengan label *Critical* dan *High* seperti *Common Vulnerabilities and Exposures* (CVE), antara lain CVE-2014-3206, CVE-2019-2767, CVE-2020-7796, CVE-2021-32305, serta CVE-2021-33544. Hasil ini memperlihatkan bahwa OWASP ZAP lebih banyak menyoroti masalah konfigurasi header, redirect, cache, dan informasi aplikasi, sedangkan Nuclei

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

mendeteksi temuan berbasis *template* CVE serta konfigurasi tambahan seperti *external-service-interaction* dan *missing-sri*.

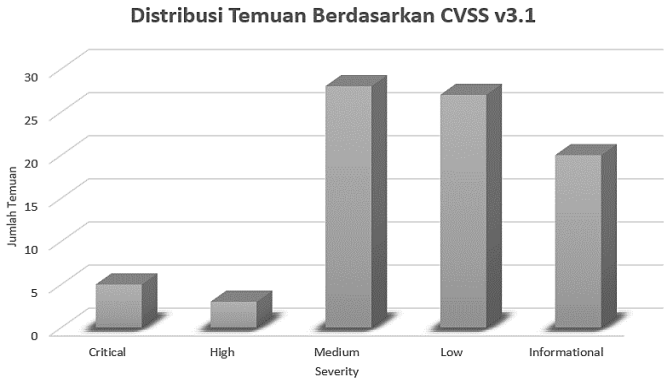
Pada target E5, proses *automated scan* OWASP ZAP tidak berhasil dijalankan karena target memberikan *response code* 529, sementara ZAP mengharapkan respons dengan status 2xx agar proses pemindaian dapat dilanjutkan. Kondisi ini tidak ditafsirkan sebagai tidak adanya kerentanan, tetapi sebagai keterbatasan akses dan ketersediaan *output* pada proses pemindaian eksternal. Nuclei juga mulai menjalankan pemindaian dengan memuat ribuan *template* keamanan, tetapi hasil akhir pemindaian tidak cukup tersedia untuk direkap sebagai data terstruktur. Hambatan tersebut dapat dipengaruhi oleh respons target, mekanisme proteksi seperti WAF/IPS, *rate limiting*, perubahan stabilitas layanan, atau keterbatasan *scanner* dalam membaca struktur layanan publik. Oleh karena itu, hasil E5 dicatat sebagai keterbatasan cakupan deteksi, bukan sebagai dasar untuk menyimpulkan bahwa target aman dari kerentanan.

Kendala *output* pada beberapa target tidak ditafsirkan sebagai tidak adanya kerentanan, melainkan sebagai keterbatasan proses pemindaian eksternal pada target publik. Respons HTTP tertentu, pembatasan akses, mekanisme proteksi seperti WAF/IPS, *rate limiting*, atau perubahan stabilitas layanan dapat memengaruhi kemampuan *scanner* dalam menghasilkan *output* terstruktur. Oleh karena itu, hasil pada target yang tidak menghasilkan laporan lengkap tetap dicatat sebagai bagian dari evaluasi cakupan deteksi, bukan sebagai dasar untuk menyimpulkan bahwa target tersebut aman dari kerentanan.

Tabel 1. Status Pelaksanaan *Scanning*

Kode Target	Tool	Status	Catatan
E1	OWASP ZAP	Selesai	Laporan tersedia dan temuan direkap
E1	Nuclei	Selesai	Pemindaian selesai, tetapi tidak menghasilkan *match* yang dapat direkap
E2	OWASP ZAP	Selesai	Laporan tersedia dan temuan direkap
E2	Nuclei	Selesai	*Output* tersedia dan temuan direkap
E3	OWASP ZAP	Selesai	Laporan tersedia dan temuan direkap
E3	Nuclei	Parsial	Hanya tersedia bukti proses scan
E4	OWASP ZAP	Selesai	Laporan tersedia dan temuan direkap
E4	Nuclei	Selesai	*Output* tersedia dan beberapa temuan perlu validasi manual
E5	OWASP ZAP	Gagal	Tidak menghasilkan *output* terstruktur karena kendala respons HTTP
E5	Nuclei	Tidak direkap	Bukti proses tersedia, tetapi *output* akhir tidak cukup untuk direkap

Tabel 1 memperlihatkan status pelaksanaan scanning pada setiap target dan setiap alat. Berdasarkan Tabel 1, OWASP ZAP berhasil menghasilkan laporan pada target E1, E2, E3, dan E4, tetapi tidak menghasilkan data yang dapat direkap pada E5 karena kendala respons HTTP. Pada Nuclei, target E2 dan E4 menghasilkan *output* yang dapat direkap, target E1 tidak menghasilkan *match* yang sesuai dengan *template* pada saat pengujian, sedangkan target E3 dan E5 hanya memiliki bukti proses tanpa *output* akhir yang cukup untuk dimasukkan sebagai data terstruktur. Dengan demikian, Tabel 1 tidak hanya menunjukkan keberhasilan pemindaian, tetapi juga memperlihatkan keterbatasan data yang perlu dipertimbangkan dalam pembahasan efektivitas *scanner*.



Gambar 2. Grafik Distribusi Temuan Berdasarkan *Severity*

Hasil rekapitulasi pada Gambar 2 menunjukkan bahwa total temuan agregat dari seluruh artefak pengujian adalah 83 temuan, terdiri atas 68 temuan dari OWASP ZAP dan 15 temuan dari Nuclei. Setelah proses normalisasi dan deduplikasi, ditemukan 2 temuan *overlap* sehingga total temuan unik atau union dalam penelitian ini adalah 81 temuan. Gambar 2 memperlihatkan bahwa kategori *Medium* menjadi kategori terbanyak dengan 28 temuan, disusul kategori *Low* sebanyak 27 temuan dan *Informational* sebanyak 20 temuan. Meskipun jumlah *Critical* dan *High* lebih sedikit, yaitu 5 *Critical* dan 3 *High*, kedua kategori tersebut tetap menjadi prioritas karena memiliki potensi risiko lebih besar

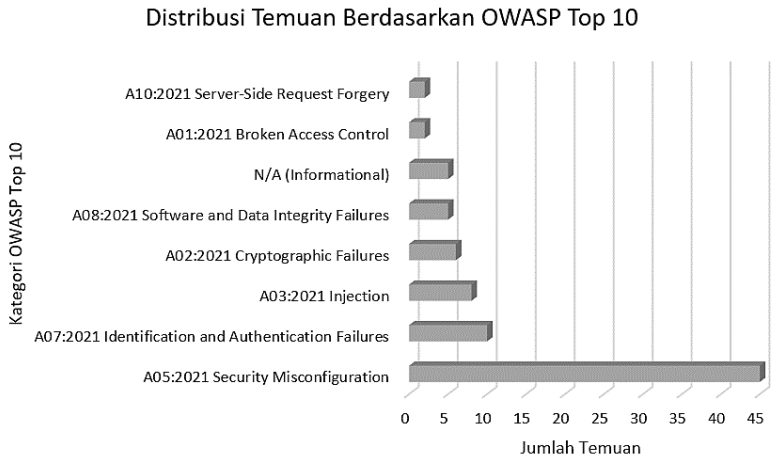
TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

apabila hasilnya terkonfirmasi melalui pemeriksaan lanjutan. Oleh sebab itu, jumlah temuan agregat tidak digunakan sebagai satu-satunya ukuran efektivitas, melainkan dipadukan dengan *severity*, *overlap*, cakupan kategori, dan kebutuhan validasi manual.

Tabel 2. Klasifikasi *Severity* dan Prioritas Tindakan

Severity	Karakter Risiko	Prioritas Tindakan	Peran dalam Analisis
Critical	Risiko sangat tinggi dan berpotensi berdampak besar apabila terkonfirmasi	Validasi dan mitigasi sangat segera	Prioritas utama analisis
High	Risiko tinggi dan dapat berdampak signifikan terhadap keamanan aplikasi	Validasi cepat dan rencana perbaikan	Masuk temuan prioritas
Medium	Risiko sedang, dapat menjadi celah pendukung atau memperlemah konfigurasi	Dianalisis setelah prioritas tinggi	Pendukung cakupan deteksi
Low	Risiko rendah, umumnya terkait konfigurasi atau praktik keamanan	Perbaikan bertahap	Indikator kualitas konfigurasi
Informational	Informasi teknis dan belum tentu kerentanan langsung	Dokumentasi dan pemantauan	Konteks tambahan

Pada Tabel 2, klasifikasi tingkat keparahan digunakan sebagai dasar untuk menentukan prioritas analisis terhadap temuan kerentanan. Kategori *Critical* menunjukkan temuan dengan potensi dampak sangat besar terhadap kerahasiaan, integritas, atau ketersediaan sistem sehingga membutuhkan tindakan validasi dan mitigasi paling cepat. Kategori *High* menunjukkan risiko tinggi yang juga perlu segera diperiksa karena berpotensi berdampak signifikan apabila benar-benar dapat dieksploitasi. Kategori *Medium* menunjukkan risiko sedang yang tetap perlu dianalisis karena dapat menjadi celah pendukung terhadap serangan lain atau menurunkan kualitas konfigurasi keamanan. Kategori *Low* menunjukkan risiko rendah yang umumnya berkaitan dengan kelemahan konfigurasi atau praktik keamanan yang belum optimal, sedangkan *Informational* tidak selalu menunjukkan kerentanan langsung, tetapi berguna sebagai informasi teknis untuk memahami *attack surface* dan kondisi konfigurasi target.



Gambar 3. Grafik Distribusi Temuan Berdasarkan OWASP Top 10

Gambar 3 menunjukkan bahwa kategori A05:2021 *Security Misconfiguration* menjadi kategori dengan jumlah temuan terbanyak, yaitu 45 temuan atau sekitar 54,2% dari total temuan agregat. Dominasi kategori ini memperlihatkan bahwa sebagian besar indikasi kerentanan yang ditemukan berkaitan dengan konfigurasi aplikasi web, seperti *Content Security Policy*, *security header*, *cache-control*, dan atribut *cookie*. Kategori A03:2021 Injection juga perlu diperhatikan karena muncul pada temuan prioritas dari Nuclei yang memiliki rating *Critical*. Dengan demikian, Gambar 3 memperjelas bahwa analisis efektivitas *scanner* tidak hanya didasarkan pada distribusi jumlah temuan, tetapi juga pada jenis kategori yang memiliki dampak risiko lebih besar.

3.2 Pembahasan

Secara keseluruhan, hasil pengujian menunjukkan bahwa OWASP ZAP menghasilkan 68 temuan atau sekitar 81,9% dari 83 temuan agregat, sedangkan Nuclei menghasilkan 15 temuan atau sekitar 18,1%. Setelah deduplikasi, total temuan unik menjadi 81 karena terdapat 2 temuan *overlap*. OWASP ZAP lebih banyak mendeteksi isu pada lapisan aplikasi web, terutama konfigurasi respons HTTP, *Content Security Policy*, *security header*, *cache-control*, dan atribut *cookie*. Nuclei menghasilkan temuan yang lebih sedikit, tetapi beberapa temuannya memiliki tingkat keparahan lebih tinggi karena berkaitan dengan pola CVE, potensi Injection, dan *Server-Side Request Forgery*. Perbedaan ini menunjukkan bahwa kedua alat memiliki karakteristik deteksi yang berbeda dan saling melengkapi, tetapi hasilnya tetap perlu dibaca sebagai indikasi awal karena penelitian tidak melakukan eksploitasi manual.

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

Pemilihan temuan prioritas pada pembahasan ini didasarkan pada klasifikasi *severity*. Temuan dengan kategori *Critical* dan *High* dipilih sebagai fokus analisis utama karena memiliki potensi dampak terbesar dan membutuhkan validasi manual lebih cepat dibandingkan kategori lainnya. Dalam penelitian ini, temuan prioritas berasal dari dua alat, yaitu OWASP ZAP dan Nuclei. Dari OWASP ZAP, temuan yang masuk prioritas adalah *PII Disclosure* pada target E2 karena memiliki *rating High* dan berkaitan dengan potensi kegagalan perlindungan informasi sensitif. Dari Nuclei, temuan prioritas sebagian besar muncul pada target E4, yaitu CVE-2014-3206, CVE-2019-2767, CVE-2020-7796, CVE-2021-32305, CVE-2021-33544, *sar2html-rce*, dan CVE-2018-15517.

Tabel 3. Rangkuman Temuan Prioritas

Target	Tool	ID Kerentanan	Kategori OWASP	CVSS	*Rating*	Status Validasi
E2	OWASP ZAP	*PII Disclosure*	A02:2021 *Cryptographic Failures*	7,5	*High*	Perlu validasi manual segera
E4	Nuclei	CVE-2014-3206	A03:2021 *Injection*	9,8	*Critical*	Perlu validasi manual
E4	Nuclei	CVE-2019-2767	A03:2021 *Injection*	8,8	*High*	Perlu validasi manual
E4	Nuclei	CVE-2020-7796	A10:2021 *Server-Side Request Forgery*	9,1	*Critical*	Perlu validasi manual
E4	Nuclei	CVE-2021-32305	A03:2021 *Injection*	9,8	*Critical*	Perlu validasi manual
E4	Nuclei	CVE-2021-33544	A03:2021 *Injection*	9,8	*Critical*	Perlu validasi manual
E4	Nuclei	*sar2html-rce*	A03:2021 *Injection*	9,8	*Critical*	Perlu validasi manual
E4	Nuclei	CVE-2018-15517	A10:2021 *Server-Side Request Forgery*	8,8	*High*	Perlu validasi manual

Tabel 3 memperlihatkan terdapat delapan temuan prioritas yang terdiri dari lima temuan *Critical* dan tiga temuan *High*. Sebagian besar temuan prioritas berasal dari Nuclei pada target E4, sedangkan satu temuan *High* berasal dari OWASP ZAP pada target E2. Temuan prioritas tersebut mencakup kategori A03:2021 *Injection*, A10:2021 *Server-Side Request Forgery*, dan A02:2021 *Cryptographic Failures* sehingga perlu diperhatikan karena memiliki potensi risiko lebih besar dibandingkan temuan *Medium*, *Low*, dan *Informational*. Namun, karena beberapa temuan berasal dari deteksi berbasis *template* dan CVE, hasil tersebut tetap perlu diperlakukan sebagai indikasi awal yang membutuhkan validasi manual sebelum dinyatakan sebagai kerentanan yang benar-benar terkonfirmasi.

Efektivitas *vulnerability scanning* dalam penelitian ini dilihat dari kemampuan masing-masing *scanner* menghasilkan *output* yang dapat direkap, dibandingkan, dan dianalisis menggunakan indikator yang sama. OWASP ZAP menunjukkan efektivitas yang lebih kuat dari sisi keluasan temuan karena hasilnya tersebar pada target E1, E2, E3, dan E4. Sebaliknya, Nuclei menghasilkan temuan yang lebih terbatas dari sisi jumlah target yang dapat direkap, terutama pada E2 dan E4. Namun, keterbatasan *output* Nuclei pada beberapa target tidak langsung berarti target aman, melainkan menunjukkan adanya hambatan pemindaian eksternal atau tidak adanya *match* dengan *template* yang digunakan. Oleh karena itu, efektivitas kedua *scanner* tidak berada pada aspek yang sama: OWASP ZAP unggul pada jumlah dan konsistensi temuan konfigurasi, sedangkan Nuclei lebih selektif dalam menghasilkan indikasi berbasis *template*.

Jika efektivitas dilihat dari kualitas risiko yang teridentifikasi, Nuclei tetap memiliki kontribusi penting meskipun jumlah temuannya lebih sedikit. Pada target E4, Nuclei menghasilkan beberapa temuan dengan *rating Critical* dan *High* yang tidak muncul pada hasil OWASP ZAP. Temuan tersebut tidak langsung dinyatakan sebagai kerentanan final, tetapi menjadi sinyal prioritas yang perlu divalidasi karena berkaitan dengan CVE dan pola serangan tertentu. Dengan demikian, efektivitas *vulnerability scanning* pada penelitian ini tidak dapat disimpulkan hanya dari banyaknya temuan, tetapi perlu dipahami melalui gabungan jumlah temuan, tingkat keparahan, konsistensi *output*, cakupan kategori, *overlap*, temuan unik, dan kebutuhan validasi manual.

Jenis kerentanan yang ditemukan menunjukkan adanya perbedaan karakter deteksi antara OWASP ZAP dan Nuclei. OWASP ZAP bekerja sebagai *scanner* DAST yang berinteraksi dengan respons HTTP, *crawling*, *passive scanning*, dan *active scanning* terbatas sehingga lebih banyak menemukan isu konfigurasi aplikasi web seperti *security header*, *Content Security Policy*, *Strict-Transport-Security*, *X-Content-Type-Options*, *cache-control*, dan atribut *cookie*. Sementara itu, Nuclei bekerja berdasarkan *template* untuk mencocokkan pola kerentanan tertentu seperti CVE, Injection, *exposure*, *external-service-interaction*, *missing-sri*, dan *Server-Side Request Forgery*. Perbedaan mekanisme tersebut menjelaskan mengapa OWASP ZAP menghasilkan temuan lebih banyak, sedangkan Nuclei menghasilkan temuan lebih sedikit tetapi beberapa di antaranya memiliki *severity* lebih tinggi.

Berdasarkan tingkat keparahan, sebagian besar temuan berada pada kategori *Medium*, *Low*, dan *Informational*. Komposisi tersebut menunjukkan bahwa hasil pemindaian didominasi oleh isu konfigurasi dan informasi teknis yang perlu diperbaiki, tetapi tidak selalu menunjukkan risiko kritis secara langsung. Meskipun demikian, terdapat temuan *Critical* dan *High* yang menjadi perhatian utama karena berpotensi memiliki dampak lebih besar apabila terkonfirmasi melalui pemeriksaan lanjutan. Target E4 menjadi target paling menonjol dari sisi *severity* karena menjadi satu-satunya

TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

target yang memiliki temuan *Critical*. Oleh karena itu, penilaian risiko tidak cukup dilakukan berdasarkan jumlah temuan, melainkan perlu mempertimbangkan tingkat keparahan dan bukti teknis dari setiap temuan.

Cakupan deteksi kedua *scanner* juga menunjukkan karakteristik yang berbeda. OWASP ZAP memiliki cakupan yang lebih luas pada target yang dapat dipindai secara stabil, terutama E1, E2, E3, dan E4. Hal ini terlihat dari banyaknya temuan konfigurasi keamanan yang muncul secara konsisten pada beberapa target. Nuclei memiliki cakupan yang lebih terbatas dari sisi jumlah target yang menghasilkan *output* terstruktur, karena temuan yang dapat direkap hanya muncul pada E2 dan E4, sedangkan E1 tidak menghasilkan *match* serta E3 dan E5 tidak memiliki *output* akhir yang cukup untuk dianalisis. Kondisi tersebut menjadi keterbatasan dataset, tetapi juga menjadi bagian penting dari evaluasi efektivitas karena menunjukkan bahwa *scanner* berbasis *template* sangat bergantung pada ketersediaan respons target dan kecocokan *template*.

Berdasarkan perbandingan tersebut, pendekatan yang lebih relevan dalam penelitian ini adalah penggunaan kombinasi OWASP ZAP dan Nuclei, bukan penggunaan salah satu *scanner* secara tunggal. Alasan teknisnya adalah karena OWASP ZAP memberikan cakupan luas terhadap konfigurasi aplikasi web dan respons HTTP, sedangkan Nuclei memberikan tambahan visibilitas terhadap pola kerentanan spesifik berbasis *template* dan CVE. Apabila hanya menggunakan OWASP ZAP, penelitian berpotensi melewatkan indikasi prioritas seperti CVE, Injection, atau *Server-Side Request Forgery* yang ditemukan oleh Nuclei. Sebaliknya, apabila hanya menggunakan Nuclei, penelitian akan kehilangan banyak temuan konfigurasi keamanan aplikasi web yang secara konsisten terdeteksi oleh OWASP ZAP. Oleh karena itu, keunggulan kombinasi bukan sekadar karena memakai dua alat, tetapi karena keduanya menutup *blind spot* yang berbeda.

Penerapan kombinasi *scanner* tetap perlu disertai proses normalisasi, deduplikasi, pemetaan OWASP Top 10, penilaian CVSS v3.1, dan validasi manual terhadap temuan prioritas. Proses tersebut diperlukan karena keluaran OWASP ZAP dan Nuclei memiliki format, istilah, serta karakter bukti teknis yang berbeda. Dalam konteks pengujian *e-commerce* publik yang dilakukan secara *non-intrusive*, kombinasi OWASP ZAP dan Nuclei dapat digunakan sebagai pendekatan evaluasi awal yang memberikan gambaran luas mengenai konfigurasi aplikasi web sekaligus menampilkan indikasi risiko prioritas. Namun, rekomendasi mitigasi tetap harus didasarkan pada validasi lanjutan di lingkungan yang memiliki izin penuh, karena penelitian ini tidak melakukan pembuktian eksploitasi atau pengujian destruktif.

Hasil penelitian ini mendukung penelitian-penelitian terdahulu yang menyatakan bahwa keluaran *web vulnerability scanner* dapat berbeda antar alat karena perbedaan teknik deteksi, cakupan pengujian, dan cara pelaporan. (Alazmi & De Leon, 2022) menjelaskan bahwa evaluasi efektivitas *scanner* masih memiliki variasi tinggi karena kemampuan deteksi tiap *scanner* tidak selalu sama pada kategori kerentanan tertentu. Temuan penelitian ini sejalan dengan kondisi tersebut karena OWASP ZAP dan Nuclei menghasilkan keluaran berbeda meskipun diuji pada target yang sama. Hasil ini juga mendukung (Rahman et al., 2025) yang menunjukkan perbedaan fokus deteksi antara OWASP ZAP dan Nuclei, serta (Abdulghaffar et al., 2023) yang menekankan bahwa penggunaan beberapa *vulnerability scanner* dapat meningkatkan cakupan deteksi dibandingkan pendekatan tunggal. Selain itu, (Altulaihan et al., 2023) menegaskan bahwa penetration testing aplikasi *web* perlu menilai celah, dampak, dan kontrol pertahanan agar hasil pengujian dapat ditindaklanjuti secara realistis.

Keterbatasan hasil perlu diperhatikan agar interpretasi penelitian tetap objektif. Pada target E5, OWASP ZAP tidak menghasilkan data terstruktur karena kendala respons HTTP, sedangkan Nuclei pada E5 tidak memiliki *output* akhir yang dapat direkap. Pada target E3, Nuclei hanya memiliki bukti gambar proses scan tanpa *output* akhir yang cukup untuk dimasukkan sebagai data terstruktur. Kondisi tersebut tidak dapat langsung ditafsirkan sebagai tidak adanya kerentanan, tetapi menunjukkan keterbatasan proses scanning eksternal pada target publik. Jumlah temuan yang relatif terbatas pada beberapa target juga dapat dipengaruhi oleh WAF/IPS, *rate limiting*, pembatasan akses, stabilitas layanan, atau perubahan respons target. Oleh karena itu, hasil penelitian ini lebih tepat dipahami sebagai evaluasi karakter keluaran *scanner* dalam kondisi *non-intrusive*, bukan sebagai representasi final keamanan seluruh target.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa OWASP ZAP dan Nuclei menghasilkan karakter keluaran yang berbeda ketika digunakan dalam *vulnerability scanning non-intrusive* pada aplikasi web *e-commerce* publik. OWASP ZAP menghasilkan temuan yang lebih banyak dan lebih konsisten pada aspek konfigurasi aplikasi web, seperti *security header*, *Content Security Policy*, *cache-control*, dan atribut *cookie*. Sebaliknya, Nuclei menghasilkan jumlah temuan yang lebih sedikit, tetapi memberikan indikasi risiko prioritas melalui deteksi berbasis *template*, CVE, Injection, dan *Server-Side Request Forgery*. Berdasarkan 83 temuan agregat yang berhasil direkap, 81 temuan unik setelah deduplikasi, dan 2 temuan *overlap*, kombinasi kedua *scanner* memberikan cakupan indikasi teknis yang lebih luas dibandingkan penggunaan satu *scanner* dalam konteks data penelitian ini. Namun, hasil tersebut tidak dapat ditafsirkan sebagai kondisi keamanan final target karena penelitian dilakukan tanpa eksploitasi manual dan beberapa target mengalami kendala *output*. Oleh karena itu, penelitian selanjutnya disarankan melakukan validasi lanjutan pada lingkungan yang memiliki izin penuh, seperti *staging environment* atau benchmark aplikasi rentan, serta menambahkan metrik akurasi seperti *precision*, *recall*, *false positive rate*, dan waktu pemindaian.


TIN: Terapan Informatika Nusantara
Vol 7, No 1, June 2026, page 306-314
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i1.10143

REFERENCES

Abdulghaffar, K., Elmrabit, N., & Yousefi, M. (2023). Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners. *Computers*, *12*(11). https://doi.org/10.3390/computers12110235

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. binte, & Muhammad, Z. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. In *Analytics* (Vol. 4, Number 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/analytics4030025

Alazmi, S., & De Leon, D. C. (2022). A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. In *IEEE Access* (Vol. 10, pp. 33200–33219). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2022.3161522

Althunayyan, M., Saxena, N., Li, S., & Gope, P. (2022). Evaluation of Black-Box Web Application Security Scanners in Detecting Injection Vulnerabilities. *Electronics (Switzerland)*, *11*(13). https://doi.org/10.3390/electronics11132049

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A Survey on Web Application Penetration Testing. In *Electronics (Switzerland)* (Vol. 12, Number 5). MDPI. https://doi.org/10.3390/electronics12051229

Aydos, M., Aldan, Ç., Coşkun, E., & Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. In *Journal of King Saud University - Computer and Information Sciences* (Vol. 34, Number 9, pp. 6775–6792). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2021.09.018

Kondraciuk, A., Bartos, A., & Pańczyk, B. (2022). Comparative analysis of the effectiveness of OWASP ZAP, Burp Suite, Nikto and Skipfish in testing the security of web applications. *Journal of Computer Sciences Institute*, *24*, 176–180. https://doi.org/10.35784/jcsi.2929

Fandier Saragih, N., Reinhard Tamalawe, & Indra M Sarkis. (2023). Analisis Dan Implementasi Secure Code Pada Pengembangan Sistem Keamanan Website Fikom-Methodist.Com Menggunakan Penetration Testing Dan OWASP ZAP. *Jurnal TIMES*, *12*(1), 28–39. https://doi.org/10.51351/jtm.12.1.2023690

Izzat, M., Saputra, F. A., & Syarif, I. (2025). Design and Implementation of Distributed Web Application Vulnerability Assessment Tools for Securing Complex Microservices Environment. *International Journal of Safety and Security Engineering*, *15*(2), 267–273. https://doi.org/10.18280/ijsse.150207

Koman, J., & Janiszewski, M. (2025). SCAnME - Scanner Comparative Analysis And Metrics For Evaluation. *International Journal of Information Security*, *24*(3). https://doi.org/10.1007/s10207-025-01054-8

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.927398

Mohammed, A., Alkhathami, J., Alsuwat, H., & Alsuwat, E. (2021). Security of Web Applications: Threats, Vulnerabilities, and Protection Methods. *IJCSNS International Journal of Computer Science and Network Security*, *21*(8), 167. https://doi.org/10.22937/IJCSNS.2021.21.8.22

Rahman, A., Indra, I., Zulkarnaim, N., Mukhram, M., & Rizaldi, A. (2025). Analisis Implementasi Nucklei Vulnerability Dan OWASP-ZAP Scanner Untuk Deteksi Kerentanan Keamanan (Secure System) Pada Platform Web Based. *Jurnal Komputer Terapan*, *11*(1), 10–15. https://doi.org/10.35143/jkt.v11i1.6430

Sarpong, P. A., Larbi, L. S., Paa, D. P., Abdulai, I. B., Amankwah, R., & Amponsah, A. (2021). Performance Evaluation of Open Source Web Application Vulnerability Scanners based on OWASP Benchmark. *International Journal of Computer Applications*, *174*(18), 15–22. https://doi.org/10.5120/ijca2021921070

Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *Applied Sciences (Switzerland)*, *12*(8). https://doi.org/10.3390/app12084077

Sufi, F. (2024). A New Time Series Dataset for Cyber-Threat Correlation, Regression and Neural-Network-Based Forecasting. *Information (Switzerland)*, *15*(4). https://doi.org/10.3390/info15040199

Wardana, W., Almaarif, A., & Widjajarto, A. (2022). Vulnerability Assessment and Penetration Testing On The XYZ Website Using NIST 800-115 Standard. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(1), 520. https://doi.org/10.36418/syntax-literate.v7i1.5800

Yuzar, A., & Rahmatulloh, A. (2025). Perbandingan Efektivitas OWASP ZAP, Acunetix, Nikto Menggunakan Vulnerability Scanning Untuk Deteksi Kerentanan Aplikasi Web. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 2975–2982. https://doi.org/10.36040/jati.v9i2.13227