Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Analisis Risiko Keamanan Website Kompetisi Nasional Menggunakan Metode Vulnerability Assessment dan CVSS 4.0

Security Risk Analysis of National Competition Website Using Vulnerability Assessment Method and CVSS 4.0

Fajar Ramadhan[1], Febri Pratama[2], Yunan Yuga Pratama[3], Ilham Albana[4]
[1,2,3,4] Program Studi Teknologi Informasi, Universitas Amikom Purwokerto
*Email: [1] 23SA31A065@students.amikompurwokerto.ac.id

ABSTRACT

The national IITC competition website manages participant registration and personal data at scale, requiring a measurable and objective security evaluation, particularly in the post-event phase. This study analyzes the security risk of the IITC website using a Vulnerability Assessment approach combined with manual Proof of Concept (PoC) validation and risk scoring based on CVSS version 4.0. The assessment followed structured stages, including planning and scoping, reconnaissance, vulnerability scanning, analysis and validation, risk scoring, and reporting. Reconnaissance results indicate that the target employs a modern web architecture using Cloudflare and Netlify services with the Next.js 13.4.4 framework and React, alongside critical endpoints such as /admin, /login, and redirected /dashboard paths. Automated vulnerability scanning using OWASP ZAP 2.15.0 identified 27 alert categories, dominated by informational and low-risk findings related to security header configuration and cookie management. Initial high-risk findings, including SQL Injection and SQL Injection–SQLite, were subsequently validated through PoC and classified as false positives. Risk scoring using CVSS 4.0 confirms that all validated vulnerabilities fall within the medium-risk category, with the highest score of 6.9 observed for Content Security Policy Header Not Set and Application Error Disclosure. No high or critical exploitable vulnerabilities were identified. These results indicate that the post-event security posture of the IITC website is at a moderate risk level, with mitigation priorities focused on improving preventive security configurations to reduce potential future attack escalation.

Keywords : Vulnerability Assessment, CVSS 4.0, OWASP ZAP, Proof of Concept, Web Security

ABSTRAK

Website kompetisi nasional IITC mengelola pendaftaran dan data pribadi peserta dalam skala besar sehingga memerlukan evaluasi keamanan yang objektif dan terukur, khususnya pada fase pasca-*event*. Penelitian ini menganalisis risiko keamanan website IITC menggunakan metode *Vulnerability Assessment* yang dikombinasikan dengan validasi manual *Proof of Concept* (PoC) serta penilaian risiko berbasis CVSS versi 4.0. Tahapan pengujian meliputi p*lanning and scoping, reconnaissance, vulnerability scanning,* analisis dan validasi, *risk scoring*, serta *reporting*. Hasil *reconnaissance* menunjukkan bahwa website target menggunakan arsitektur web modern dengan layanan Cloudflare dan Netlify serta framework Next.js 13.4.4 dan React, dengan beberapa *endpoint* penting seperti /admin, /login, dan mekanisme redirect /dashboard. Pemindaian otomatis menggunakan OWASP ZAP 2.15.0 menghasilkan 27 kategori peringatan yang didominasi oleh temuan tingkat informasional dan *low*, terutama terkait konfigurasi *header* keamanan dan manajemen *cookie*. Temuan awal berisiko tinggi berupa SQL Injection dan SQL Injection–SQLite setelah dilakukan validasi PoC terbukti sebagai *false positive*. Hasil penilaian risiko menggunakan CVSS 4.0 menunjukkan bahwa seluruh kerentanan yang tervalidasi berada pada kategori risiko sedang, dengan skor tertinggi sebesar 6,9 pada kerentanan *Content Security Policy Header Not Set* dan *Application Error Disclosure*. Tidak ditemukan kerentanan dengan tingkat risiko tinggi maupun kritis yang dapat dieksploitasi secara langsung. Dengan demikian, postur keamanan website IITC pada fase pasca event berada pada tingkat risiko sedang, dengan fokus mitigasi diarahkan pada perbaikan konfigurasi keamanan preventif untuk mencegah potensi eskalasi serangan di masa mendatang.

Kata kunci: *Vulnerability Assessment*, CVSS 4.0, OWASP ZAP, *Proof of Concept*, Keamanan Website

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

I. PENDAHULUAN

Isu mengenai keamanan data privasi menjadi isu yang sangat krusial di tengah perkembangan teknologi yang semakin masif ini. Data privasi merupakan suatu informasi yang digunakan untuk mengidentifikasi atau mengenali seseorang. Keamanan data privasi berarti perlindungan terhadap data privasi yang menjadi identitas otentik seseorang agar bebas dari segala bentuk bahaya [1]. Indonesia menjadi negara yang tercatat menempati urutan ke 9 dari 10 negara teratas dengan kasus kebocoran data terbanyak di kuartal 3 tahun 2025 dengan 943,742 total kebocoran serta 332 kebocoran per 100,000 orang [2].

Gambar 1. Top 10 Negara Dengan Kebocoran Data Terbanyak

Data privasi ini menjadi sangat penting dengan perkembangan teknologi yang ada, data pribadi sudah sangat umum digunakan untuk berbagai macam proses layanan sistem informasi yang memerlukan identitas otentik penggunanya seperti untuk layanan akademik, kesehatan, dan transaksi elektronik [3][4][5]. Sistem informasi berbasis website menjadi pilihan utama dalam pengembangan sistem informasi karena dianggap dapat mendukung model pengembangan cepat (*rapid)* serta kemudahannya untuk proses *deployment* lintas platform [6].

Dalam bidang akademik, sistem informasi berbasis website tidak hanya digunakan sebagai sarana belajar mengajar saja, namun menjadi sistem yang digunakan untuk berbagai macam event yang kerap diadakan dalam lingkungan akademik [7]. Pada penelitian milik Dila Afriani (2025), sistem informasi digunakan sebagai media kegiatan mahasiswa yang menyentralisasi seluruh informasi kegiatan secara terstruktur dan *real-time*. Sistem informasi berbasis web juga diimplementasikan oleh Firdhayati (2025) sebagai sistem registrasi kegiatan Pekan Olahraga dan Seni (PORSENI) yang meningkatkan efisiensi dalam penanganan data peserta serta pembayaran secara daring, khususnya bagi peserta luar kota. Perkembangan aktivitas event berbasis web menempatkan data pribadi peserta pada risiko yang nyata sehingga identifikasi dan penilaian keamanan sistem website menjadi kebutuhan penting. Hal ini harus menjadi SOP dan Kebijakan Privasi yang diterapkan pengembang sistem [1].

Beragam metode penilaian dan analisis keamanan informasi dapat digunakan untuk mengevaluasi tingkat kerentanan serta efektivitas pengendalian keamanan yang ada. Salah satunya adalah metode analisis Vulnerability Assessment dan CVSS (*Common Vulnerability Scoring System*). *Vulnerability Assessment* (VA) berperan sebagai pendekatan preventif yang sistematis untuk mengidentifikasi, mengukur, dan mengklasifikasikan celah keamanan dalam infrastruktur teknologi informasi sebelum celah tersebut dieksploitasi oleh ancaman siber [9]. Temuan dari proses VA kemudian diperkuat dengan penerapan CVSS, yang berfungsi sebagai standar industri terbuka untuk menilai tingkat keparahan (*severity*) suatu kerentanan. Melalui metrik CVSS, karakteristik kerentanan dikuantifikasi menjadi skor numerik (0.0 hingga 10.0) yang merepresentasikan urgensi risiko, mulai dari tingkat rendah (*low*) hingga kritis (*critical*) [10]. Integrasi kedua metode ini memungkinkan pengelola sistem untuk memprioritaskan mitigasi risiko secara efektif berdasarkan dampak potensial terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data peserta. Oleh karena itu, penerapan metode ini sangat relevan untuk menganalisis postur keamanan pada website kompetisi nasional yang mengelola data sensitif dalam skala masif.

IITC (Intermedia *Information Technology Information*) adalah event nasional yang diselenggarakan setiap tahun oleh Unit Kegiatan Mahasiswa (UKM) Intermedia Universitas Amikom Purwokerto yang memiliki rangkaian kegiatan berupa seminar dan webinar serta lomba yang menjadi acara utama *event* tersebut [11]. Penyelenggaraan IITC memanfaatkan platform berbasis website sebagai sistem informasi dan manajemen pendaftaran peserta. Dengan cangkupan pengguna berskala nasonal,

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

website resmi IITC yang bisa diakses pada https://iitc.intermediaamikom.org memproses berbagai aktivitas penting, termasuk input data pribadi peserta dan proses transaksi terkait pelaksanaan event. Kondisi tersebut menjadikan website IITC sebagai aset kritis yang rentan terhadap risiko kebocoran data dan penyalahgunaan informasi. Selain itu pergantian tim pengembang pada setiap periode kepengurusan UKM menyebabkan terjadinya perubahan dan penyesuaian sistem secara berulang, sehingga penilaian keamanan informasi perlu dilakukan secara berkala untuk memastikan konsistensi postur keamanan sistem.

Penelitian asesmen keamanan informasi website IITC yang telah dilakukan oleh Khairunnisak (2021) menggunakan metode DREAD dan ISO 27005:2018 [11]. Hasil penelitian menunjukan bahwa secara keseluruhan website IITC berada pada kategori risiko sedang dengan nilai rata-rata 11,5. Risiko tertinggi ditemukan pada aspek ketersediaan (*availability)*, khususnya pada mekanisme unggah berkas yang menyebabkan data peserta periode sebelumnya yang tidak dihapus secara menyeluruh. Temuan tersebut menunjukkan bahwa meskipun tidak bersifat kritis, kelemahan pengelolaan sistem tetap berpotensi berdampak terhadap keamanan dan kendala layanan.

Penelitian lanjutan oleh Zahraini dkk. (2025) melakukan asesmen keamanan website IITC pada fase pra-event menggunakan metode *Vulnerability Assessment* dengan distribusi risiko terdiri dari 1 risiko tinggi, 4 risiko sedang, 9 risiko rendah, dan 9 bersifat informasional, dimana 15 temuan termasuk dalam kategori OWASP Top 10 tahun 2021. Kerentanan utama yang disoroti meliputi penggunaan pustaka Javascript yang rentan serta temuan *Broken Access Control* berupa akses halaman dashboard admin tanpa proses otentikasi. Hasil ini mengindikasikan bahwa website IITC memiliki permukaan serangan yang signifikan sebelum event diselenggarakan

Berdasarkan beberapa penelitian terdahulu tersebut, diperlukan pemetaan yang lebih sistematis untuk melihat perbedaan objek, metode, serta pendekatan pengujian keamanan yang digunakan, sekaligus untuk memperjelas posisi dan kontribusi penelitian ini dibandingkan studi sebelumnya.

Tabel 1 State of the Art Penelitian Terdahulu

Peneliti	**Objek Penelitian**	**Metode**	**Tools**
Khairunnisak (2021)	Website IITC	DREAD, ISO 27005	Analisis Risiko
Zahrani dkk (2025)	Website IITC (Pra-event)	Vulnerability Assessment	OWASP ZAP
Penelitian ini	Website IITC (Post-event)	VA + PoC + CVSS 4.0	OWASP ZAP, Nmap

Tabel tersebut menunjukkan bahwa sebagian besar penelitian sebelumnya masih mengandalkan pemindaian otomatis atau metode penilaian risiko yang bersifat subjektif. Selain itu, validasi teknis melalui Proof of Concept serta penggunaan skema penilaian risiko terstandar versi terbaru seperti CVSS 4.0 masih terbatas, khususnya pada evaluasi keamanan website event pada fase pasca-event.

Dari kedua penelitian utama yang melakukan *assessment* keamanan terhadap website IITC didapati bahwa Metode DREAD sebagai salah satu pendekatan kualitatif dalam penilaian risiko siber memiliki kelemahan utama pada tingginya tingkat subjektivitas dalam proses penilaiannya. Hal ini disebabkan karena evaluasi risiko sangat bergantung pada pengalaman, latar belakang, serta sudut pandang individu yang melakukan analisis, sementara lingkungan ancaman siber sendiri bersifat dinamis dan terus berkembang. Akibatnya, penilaian risiko terhadap sistem yang sama dapat menghasilkan hasil yang berbeda secara signifikan apabila dilakukan oleh pakar yang berbeda, sehingga konsistensi dan reliabilitas hasil menjadi sulit dijamin. Kelemahan ini semakin kontras jika dibandingkan dengan bidang *reliability* engineering yang memiliki basis data kegagalan dan probabilitas yang relatif stabil. Oleh karena itu, penggunaan DREAD sering dikritik karena kurang mampu memberikan hasil yang objektif dan terstandarisasi dalam konteks manajemen risiko siber modern [14].

Kemudian, hasil penilaian yang mengandalkan pemindaian otomatis menggunakan OWASP ZAP tanpa proses validasi manual maupun pembuktian melalui *Proof of Concept* (PoC) memiliki keterbatasan fundamental yang perlu diperhatikan secara kritis.

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

pemindaian otomatis seperti ZAP terbukti memiliki tingkat *false positive* yang relatif tinggi serta cakupan deteksi yang terbatas, khususnya terhadap kerentanan modern dan kerentanan yang membutuhkan interaksi logis untuk dapat dieksploitasi. ZAP memiliki akurasi deteksi terendah dibandingkan alat komersial lainnya, dengan *false positive rate* mencapai 18,4%, sehingga hasil temuan scanner tidak dapat langsung diinterpretasikan sebagai kerentanan nyata tanpa validasi lanjutan. [15]. Penelitian [16] menegaskan bahwa perangkat otomatis cenderung menghasilkan laporan temuan yang tidak menggambarkan tingkat *exploitability* yang sesungguhnya karena tidak mampu menggantikan proses pembuktian teknis melalui PoC.

Oleh karena itu, penelitian ini mengusulkan penerapan metode *Vulnerability Assessment* (VA) yang disertai validasi manual (*Proof of Concept*) dan penilaian risiko terukur menggunakan CVSS sebagai solusi atas keterbatasan subjektivitas dan akurasi alat otomatis. Penelitian ini secara spesifik bertujuan untuk memvalidasi temuan kerentanan dari dua penelitian utama sebelumnya serta memperluas cakupan analisis dengan observasi status keamanan sistem pada fase pasca event (*Post-Event*), guna menjamin perlindungan data privasi peserta tetap terjaga bahkan setelah rangkaian kegiatan IITC berakhir.

Kebaruan penelitian ini terletak pada penerapan metode *Vulnerability Assessment* yang dikombinasikan dengan validasi manual *Proof of Concept* (PoC) serta penilaian risiko terukur menggunakan Common Vulnerability Scoring System (CVSS) versi 4.0 pada website event nasional pada fase pasca-event (post-event). Berbeda dengan penelitian sebelumnya yang umumnya mengandalkan pemindaian otomatis atau metode penilaian risiko yang bersifat subjektif, penelitian ini menekankan verifikasi teknis terhadap temuan kerentanan untuk mengeliminasi *false positive* dan menghasilkan penilaian risiko yang lebih objektif serta representatif. Selain itu, penggunaan CVSS 4.0 sebagai versi terbaru memberikan kontribusi metodologis dalam pengukuran tingkat keparahan kerentanan aplikasi web modern yang masih terbatas penerapannya pada konteks website event berbasis akademik.

II. LANDASAN TEORI

A. *CIA Triade*

Dalam konteks keamanan informasi, kerangka CIA (*Confidentiality, Integrity, Availability*) berperan sebagai landasan teoretis utama yang menjelaskan tujuan perlindungan informasi, menjamin integritas agar informasi dan hasil tidak dimodifikasi secara tidak sah, serta memastikan ketersediaan layanan agar sistem tetap dapat diakses saat dibutuhkan pengguna.

Gambar 2. CIA Triad

Dalam praktik vulnerability assessment, setiap kerentanan dianalisis berdasarkan dampaknya terhadap ketiga elemen CIA, misal kebocoran kredensial menurunkan *Confidentiality*, injeksi data merusak *Integrity*, sementara serangan volumetrik mengancam *Availability* dan hasil penilaian tersebut biasanya dipetakan ke metrik CVSS sehingga prioritas perbaikan dapat ditentukan secara kuantitatif berdasarkan besaran dampak terhadap CIA. Dengan demikian, penerapan CIA bukan hanya kerangka konseptual, tetapi juga alat operasional untuk menghubungkan temuan teknis pada assessment dengan keputusan manajemen risiko dan mitigasi yang terukur. [17].

B. *Vulnerabillity Assessment (VA)*

Vulnerability Assessment (VA) merupakan proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi kelemahan atau kerentanan pada sistem informasi, jaringan, maupun aplikasi web. Tujuan utama dari VA adalah menemukan potensi risiko keamanan sebelum kerentanan tersebut dapat dieksploitasi oleh penyerang. Proses VA dilakukan dengan cara pemindaian, pengujian, dan analisis struktur keamanan dari sistem yang diuji, sehingga dapat memberikan gambaran menyeluruh mengenai tingkat ancaman dan langkah mitigasi yang dibutuhkan..

Menurut Darojat (2022), *Vulnerability Assessment* merupakan metode penilaian kerentanan dengan melakukan pengujian celah keamanan untuk mengetahui seluruh potensi kelemahan kritis pada suatu website, terutama pada konteks aplikasi *e-government*. Selain itu, VA juga mencakup evaluasi konfigurasi sistem, kesadaran keamanan pengguna, serta aspek teknis seperti enkripsi, otentikasi, dan integritas data. Dalam penelitian lain, *vulnerability assessment* dipandang sebagai upaya untuk mencari dan menemukan kelemahan dalam sistem atau jaringan komputer untuk mencegah potensi serangan melalui identifikasi kerentanan yang ada [19].

Secara keseluruhan, *Vulnerability Assessment* memegang peranan penting dalam menjaga keamanan aplikasi web dan sistem informasi modern. Evaluasi rutin perlu dilakukan untuk menghadapi ancaman siber yang terus berkembang, memastikan sistem berada dalam kondisi aman, serta membantu organisasi mengambil langkah preventif secara tepat. Dengan mengimplementasikan metode dan standar penilaian yang baik, organisasi dapat meminimalkan risiko keamanan dan memperkuat ketahanan sistem terhadap serangan.

C. Common Vulnerabillity Scoring System (CVSS)

kerangka penilaian yang digunakan untuk mengukur tingkat keparahan kerentanan pada sistem informasi. Dalam penelitian Bardian (2024), CVSS dijelaskan sebagai metode yang memberikan skor numerik untuk menunjukkan tingkat kritis suatu kerentanan, sehingga memudahkan proses prioritisasi perbaikan. CVSS bekerja dengan memanfaatkan sejumlah metrik yang mencerminkan faktor teknis dan konteks operasional dari kerentanan, sehingga proses penilaian menjadi lebih objektif dan dapat diterapkan konsisten pada berbagai jenis celah keamanan.

Kerangka CVSS modern terdiri atas beberapa kelompok metrik, yaitu Base, Threat, Environmental, dan Supplemental. Metrik Base menggambarkan karakteristik mendasar dari kerentanan yang tidak berubah seiring waktu, seperti tingkat kerumitan eksploitasi dan dampaknya terhadap kerahasiaan, integritas, dan ketersediaan sistem[20]. Sementara itu, metrik Threat digunakan untuk menilai kondisi ancaman aktual yang mungkin meningkatkan urgensi penanganan suatu kerentanan, misalnya keberadaan eksploit publik atau bukti eksploitasi aktif. Metrik Environmental berfungsi menyesuaikan skor berdasarkan konteks organisasi, seperti nilai aset dan tingkat sensitivitas data. Terakhir, metrik Supplemental memberikan informasi tambahan yang dapat mendukung proses pengambilan keputusan[20].

CVSS sangat efektif bila digunakan dalam proses analisis risiko karena hasil skoringnya dapat dipadukan dengan kerangka keamanan lain seperti OWASP dan APPI[21]. Dengan integrasi ini, penilaian risiko menjadi lebih komprehensif, terutama dalam menentukan prioritas mitigasi setelah tahap Vulnerability Assessment. Penggunaan skor CVSS membantu organisasi memahami tingkat keparahan suatu celah dalam konteks operasional sehingga pengelolaan risiko dapat dilakukan secara lebih terarah dan terukur[21].

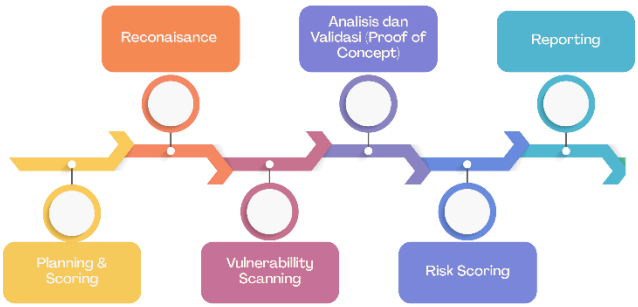
Secara keseluruhan, penggunaan CVSS dalam penelitian keamanan jaringan dan aplikasi web memberikan nilai tambah karena menyediakan sistem penilaian yang baku, terukur, dan dapat direplikasi oleh peneliti maupun praktisi keamanan. Pemanfaatan metrik-metrik pada CVSS memungkinkan analisis kerentanan tidak hanya terfokus pada aspek teknis, tetapi juga mempertimbangkan aspek ancaman dan kondisi spesifik suatu organisasi.

III. METODE PENELITIAN

Penelitian ini mengadopsi metode Vulnerability Assessment (VA) untuk mengidentifikasi dan menganalisis celah keamanan situs web kompetisi nasional. Metode VA bersifat sistematis dan preventif, melibatkan pemindaian otomatis untuk menemukan potensi kerentanan aplikasi web secara menyeluruh. Penelitian yang dilakukan akan menggunakan beragam alat pengujian keamanan, seperti Nmap (pemindaian jaringan), OWASP ZAP (pemindaian aplikasi web) untuk memperoleh data kerentanan. Setiap kerentanan yang terdeteksi kemudian divalidasi secara manual (Proof-of-Concept) untuk memastikan akurasinya dan mengurangi laporan positif palsu. Setelah verifikasi, risiko dari setiap kerentanan dihitung menggunakan Common Vulnerability Scoring System (CVSS) versi 4.0 Skor CVSS ini berdasarkan metrik Base (ciri intrinsik kerentanan) dan dapat disesuaikan dengan metrik Threat/Environmental sesuai konteks organisasi. Dengan demikian, setiap celah keamanan akan diberi nilai numerik (0,0–10,0) yang menunjukkan tingkat

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

keparahannya, sehingga memudahkan prioritisasi mitigasi risiko. Batasan metode pada penelitian ini adalah pengujian difokuskan pada satu domain website event pada lapisan aplikasi (application layer) menggunakan pendekatan vulnerability assessment berbasis pemindaian dan validasi manual (Proof of Concept), tanpa akses ke kode sumber maupun konfigurasi infrastruktur internal/server, sehingga temuan yang dihasilkan merepresentasikan kondisi keamanan dari sisi permukaan layanan (externally observable) dan tidak mencakup kerentanan yang hanya dapat diidentifikasi melalui audit internal serta tidak merusak data yang ada pada sistem aplikasi.



Gambar 3 Alur Metode Penelitian

A. Planning and Scoping

Tahapan ini menjadi langkah awal yang krusial dengan mencangkup aspek-aspek seperti batasan ruang lingkup dan domain website yang akan diuji, serta persetujuan terhadap pihak yang memiliki otoritas, sehingga dapat meningkatkan efektivitas dan meminimalisir risiko yang mungkin terjadi terhadap target yang akan diuji [22][18]. Batasan yang disetujui berupa domain yang diuji adalah hanya domain utama event yaitu https://iitc.intermediaamikom.org, kemudian pengujian dan kegiatan asesment harus dipastikan tidak akan mengubah atau merusak data pada sistem.

B. Reconnaisance

Tahap reconnaissance bertujuan untuk mengumpulkan informasi awal terkait target guna memahami karakteristik sistem, teknologi yang digunakan, serta memperkirakan permukaan serangan (attack surface) sebelum dilakukan pemindaian kerentanan. Aktivitas pada tahap ini dilakukan secara pasif dan semi-aktif untuk meminimalkan dampak terhadap ketersediaan layanan. Reconnaissance juga membantu menyusun strategi pemindaian agar lebih terarah dan efisien dalam mengidentifikasi endpoint yang berpotensi rentan [23] [24].

Pada penelitian ini, *reconnaissance* dilakukan melalui beberapa aktivitas. Pertama, identifikasi dilakukan pada domain dan resolusi DNS/IP untuk mengetahui keterkaitan domain, kemungkinan penggunaan CDN/load balancer, serta perubahan IP yang bersifat dinamis. Informasi ini penting karena dapat memengaruhi interpretasi hasil pemindaian (misalnya hasil berasal dari edge network/proxy, bukan origin server). Dari hasil identifikasi, selanjutnya akan dilakukan enumerasi teknologi (technology fingerprinting) untuk mengidentifikasi web framework, library frontend/backend, server, dan layanan pihak ketiga yang digunakan. Hasil fingerprinting dipakai untuk mengarahkan pencarian kerentanan berdasarkan komponen yang terdeteksi (misalnya kesesuaian versi dan konfigurasi) [24]. Terakhir, enumerasi direktori dan endpoint untuk menemukan path sensitif, file konfigurasi yang terpapar, halaman admin, maupun endpoint yang tidak terindeks. Enumerasi ini berguna sebagai input awal pada tahap pemindaian kerentanan agar cakupan endpoint lebih optimal [23]. Output dari tahap reconnaissance adalah daftar temuan informasi awal (IP/hosting pattern, teknologi utama, serta daftar endpoint) yang digunakan sebagai dasar konfigurasi pemindaian pada tahap berikutnya.

C. Vulnerability Scanning

Tahap ini bertujuan untuk mendeteksi kerentanan secara sistematis pada domain yang telah ditetapkan melalui proses pemindaian otomatis dan pengujian terstruktur. Pemindaian dilakukan dengan mengacu pada praktik pengujian keamanan aplikasi web yang umum digunakan, termasuk pengujian terhadap misconfiguration, kelemahan autentikasi/sesi, validasi input, kontrol akses, dan potensi paparan data [25]. Pada penelitian ini, pemindaian dimulai dengan memindai Konfigurasi target dan scope pemindaian sesuai batasan domain yang telah disepakati pada tahap planning dan scoping. Lalu dari hasil pemindaian tersebut, akan dilanjutkan dengan melakukan Crawling/Spidering untuk mengumpulkan URL, parameter, form, dan request yang dapat diuji lebih lanjut. Kemudian dengan memanfaatkan Automated scanning pada OWASP-ZAP pemindai kerentanan aplikasi web dilakkan untuk menghasilkan daftar potensi kerentanan beserta bukti

awal (request/response, parameter, dan indikasi pola serangan). Pemindaian otomatis membantu memperluas cakupan uji dan mempercepat identifikasi awal [24]. Berdasarkan hasil Automates Scanning, daftar temuan kerentanan akan di klasifikasi berdasarkan kategori kerentanan (misalnya OWASP Top 10) untuk memudahkan analisis, prioritisasi, dan penyusunan rekomendasi mitigasi [24]. Hasil tahap ini berupa daftar finding awal (termasuk yang berpotensi false positive), yang kemudian tidak langsung dianggap final karena akan dilanjutkan pada tahap validasi.

D. Analisis dan Validasi (*Proof of Concept*)

Tahapan ini akan berisi validasi dari hasil temuan dari pemindaian otomatis diuji ulang secara manual untuk memastikan keabsahan. Kerentanan yang dianggap kritis atau tinggi diuji (misalnya eksploitasi terbatas) pada lingkungan uji terisolasi. Proses ini menurunkan tingkat false positive dan memberikan bukti teknis (PoC) bahwa kerentanan tersebut benar adanya [23]. Dengan demikian, hanya kerentanan valid yang dibawa ke tahap penilaian risiko.

E. Risk Scoring

Pada tahap ini, kerangka penilaian yang digunakan untuk mengukur tingkat keparahan kerentanan pada sistem informasi menggunakan CVSS. Dalam penelitian Bardian (2024), CVSS dijelaskan sebagai metode yang memberikan skor numerik untuk menunjukkan tingkat kritis suatu kerentanan, sehingga memudahkan proses prioritisasi perbaikan. CVSS bekerja dengan memanfaatkan sejumlah metrik yang mencerminkan faktor teknis dan konteks operasional dari kerentanan, sehingga proses penilaian menjadi lebih objektif dan dapat diterapkan konsisten pada berbagai jenis celah keamanan.

Kerangka CVSS modern terdiri atas beberapa kelompok metrik, yaitu Base, Threat, Environmental, dan Supplemental. Metrik Base menggambarkan karakteristik mendasar dari kerentanan yang tidak berubah seiring waktu, seperti tingkat kerumitan eksploitasi dan dampaknya terhadap kerahasiaan, integritas, dan ketersediaan sistem[20]. Sementara itu, metrik Threat digunakan untuk menilai kondisi ancaman aktual yang mungkin meningkatkan urgensi penanganan suatu kerentanan, misalnya keberadaan eksploit publik atau bukti eksploitasi aktif. Metrik Environmental berfungsi menyesuaikan skor berdasarkan konteks organisasi, seperti nilai aset dan tingkat sensitivitas data. Terakhir, metrik Supplemental memberikan informasi tambahan yang dapat mendukung proses pengambilan keputusan[20].

CVSS sangat efektif bila digunakan dalam proses analisis risiko karena hasil skoringnya dapat dipadukan dengan kerangka keamanan lain seperti OWASP dan APPI[21]. Dengan integrasi ini, penilaian risiko menjadi lebih komprehensif, terutama dalam menentukan prioritas mitigasi setelah tahap Vulnerability Assessment. Penggunaan skor CVSS membantu organisasi memahami tingkat keparahan suatu celah dalam konteks operasional sehingga pengelolaan risiko dapat dilakukan secara lebih terarah dan terukur[21].

Secara keseluruhan, penggunaan CVSS dalam penelitian keamanan jaringan dan aplikasi web memberikan nilai tambah karena menyediakan sistem penilaian yang baku, terukur, dan dapat direplikasi oleh peneliti maupun praktisi keamanan. Pemanfaatan metrik-metrik pada CVSS memungkinkan analisis kerentanan tidak hanya terfokus pada aspek teknis, tetapi juga mempertimbangkan aspek ancaman dan kondisi spesifik suatu organisasi.

F. Reporting

Tahap reporting merupakan tahap akhir yang mendokumentasikan keseluruhan proses pengujian dan hasil yang diperoleh. Laporan disusun sebagai bentuk pertanggungjawaban ilmiah sekaligus menjadi acuan pihak pengelola website dalam melakukan perbaikan keamanan. Pada tahap ini dirangkum ruang lingkup pengujian, metode yang digunakan, temuan kerentanan yang tervalidasi, skor keparahan, serta rekomendasi mitigasi yang dapat diterapkan[22].

Dalam penelitian ini, laporan berisi ringkasan temuan utama, detail kerentanan (lokasi endpoint/parameter dan deskripsi singkat), bukti validasi PoC ringkas, serta hasil penilaian CVSS 4.0 untuk setiap temuan yang valid. Skor CVSS dan temuan CIA dianalisis untuk menyusun rekomendasi mitigasi. Kerentanan dengan skor tinggi (misalnya di atas 7.0) direkomendasikan diperbaiki segera[26]. Pelaporan akhir mencakup deskripsi kerentanan, nilai CVSS, serta dampaknya pada kerahasiaan, integritas, dan ketersediaan data [20]. Dengan pendekatan ini, analisis risiko menjadi terukur dan transparan, memudahkan manajemen sistem merencanakan perbaikan secara efektif.

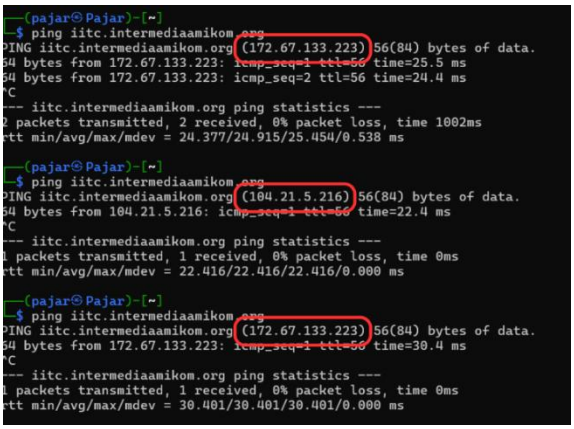
Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

IV. HASIL PENELITIAN DAN PEMBAHASAN

Pada tahapan ini dipaparkan hasil dari seluruh rangkaian proses pengujian keamanan yang telah dilakukan. Pemaparan hasil dilakukan dari tahap awal hingga analisis risiko dan scoring berdasarkan CVSS. Setiap temuan dipaparkan secara berurutan mengikuti tahapan pada metodologi penelitian, sehingga alur pembahasan lebih mudah dipahami. Proses analisis yang dipaparkan tidak hanya memaparkan langsung hasil temuan pemindaian otomatis, namun mencangkup validasi dengan PoC untuk memastikan akurasi temuan dan mengeliminasi kemungkinan *false positive.* Dengan demikian, hasil yang disajikan dapat menggambarkan kondisi keamanan aktual dari situs web target.

A. *Reconnaissance*

Hasil pengujian konektivitas menggunakan protokol ICMP (Ping), ditemukan bahwa target tidak merespon dari satu alamat IP statis, melainkan menghasilkan perilaku respon yang dinamis melalui beberapa alamat IP yang berbeda dalam rentang waktu yang singkat seperti yang ditunjukan pada Gambar 4. Perubahan alamat IP yang dinamis ini mengindikasikan bahwa target tidak menggunakan arsitektur situs web tradisional yang terkespos langsung ke internet. Namun, ini adalah karakteristik teknis dari penggunaan sistem Load Balancer atau Content Delivery Network (CDN) yang mendistribusikan permintaan pengguna ke berbagai server terdekat (*edge nodes*).



Gambar 4. Hasil Pengujian Konektivitas Target

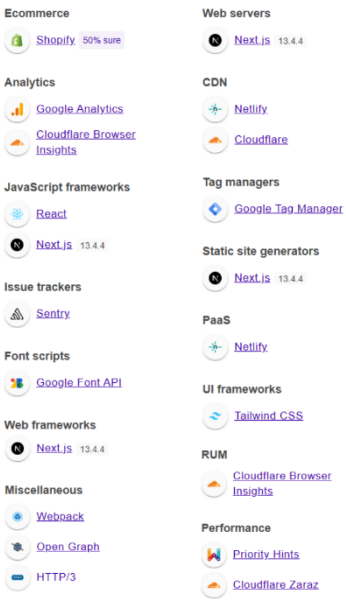
Langkah selanjutnya adalah dilakukan penelusuran informasi domain dengan menggunakan WHOIS yang bertujuan mengidentifikasi pemilik dan penyedia layanan infrastruktur dari situs web yang dikembangkan. Hasil temuan yang didapatkan adalah sebagai berikut:

Tabel 2 Hasil Informasi Domain WHOIS

Atribut Informasi	**Data Temuan**	**Analaisis Keamanan**
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com	Penyedia layanan pendaftaran domain.
Registrant Name	Zae*** Roc****	Identitas pemilik terekspos publik; fitur *WHOIS Privacy Protection* tidak diaktifkan.
Registrant Contact	Email: zae***.***98@gmail.com Phone: +62.815-****-****	Penggunaan email pribadi (Gmail) dan nomor seluler untuk aset organisasi meningkatkan risiko serangan *Social Engineering* (*Phishing*).
Organization	Intermedia	Memvalidasi target adalah organisasi yang dimaksud
Name Servers	andronicus.ns.cloudflare.com, olivia.ns.cloudflare.com	Mengonfirmasi penggunaan layanan *Reverse Proxy* / WAF dari Cloudflare.
Domain Status	clientTransferProhibited	Status ini mencegah transfer domain yang tidak sah (perlindungan terhadap *Domain Hijacking*).

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

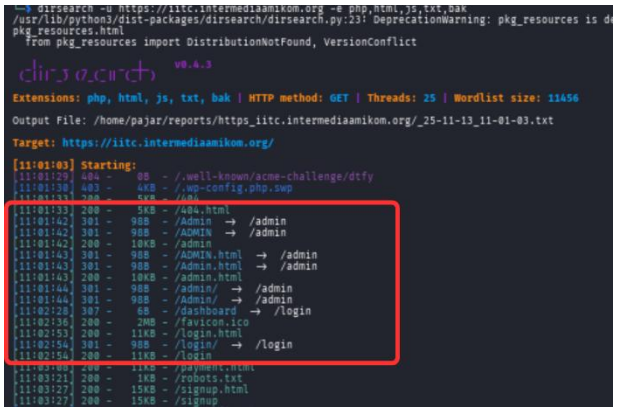
Langkah selanjutnya adalah mengidentifikasi *Technology Stack* yang digunakan situs web target. Langkah ini penting untuk menentukan vektor pengujian yang spesifik, mengingat kerentanan aplikasi modern memiliki karakteristik yang berbeda dibanding aplikasi *server-side* tradisional. Pemindaian dilakukan menggunakan Wappalyzer dengan hasil pada



Gambar 5. Hasil Pemindaian Wappalyzer

Hasilnya ditemukan framework aplikasi yang digunakan adalah Next.js versi 13.4.4 dan pustaka React Js yang mengindikasikan bahwa aplikasi ini memiliki pemrosesan di sisi klien sehingga fokus keamanan berbeda. Jenis kerentanan seperti injeksi sisi server konvensional menjadi kurang relevan yang kemudian kerentanan lebih relevan dengan jenis serangan sisi klien seperti *Cross-Site Scripting* (XSS) Informasi penting selanjutnya yang dapat diidentifikasi adalah Cloudflare dan Netlify sebagai layanan CDN serta PaaS (Platform as a Service) yang mengkonfirmasi temuan di awal bahwa situs web target memiliki arsitektur modern yang terdistribusi dan *serverless* sehingga memiliki kecenderungan serangan keamanan pada server fisik yang minim, namun disisi lain meningkatkan risiko pada miskonfigurasi API dan Eksposur secret keys pada kode frontend.

Langkah terakhir pada tahap ini adalah melakukan pemetaan struktur URL tersembunyi menggunakan alat Dirsearch dengan teknik *directory bruteforce.* Proses ini bertujuan mengidentifikasi direktori sensitif atau halaman administratif yang tidak terindeks secara publik namun dapat diakses melalui permintaan HTTP langsung.



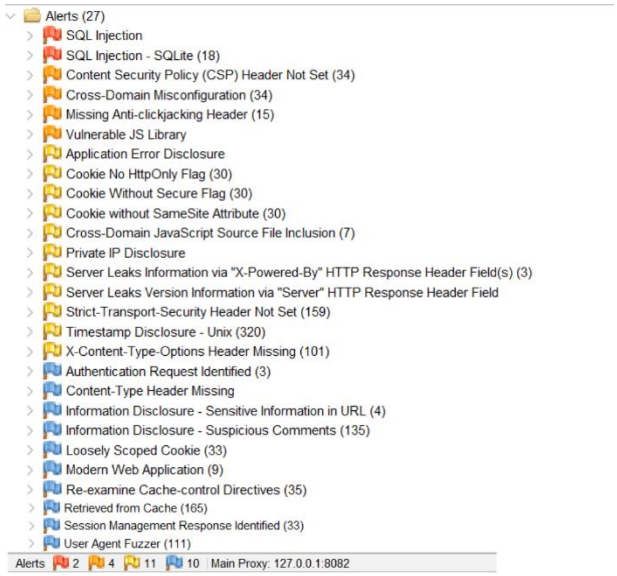
Gambar 6. Hasil Dirsearch

Hasilnya ditemukan beberapa *endpoint* krusial dengan status HTTP 200 (OK) dan 301/307 (*Redirect*) yang menjadi indikator adanya halaman tersembunyi. Temuan berupa direktori /admin dan /login yang dapat diakses secara langsung yang secara eksplisit memetakan lokasi pintu masuk autentikasi sistem tanpa pembatasan akses IP (*IP Whitelist*) yang meningkatkan risiko serangan berbasis identitas seperti *Bruteforce* dan *Credential Stuffing*. Kemudian adanya respon status *Redirect* pada *endpoint* /dashboard yang mengarah ke /login dengan status 307. Temuan ini mengidentifikasi bahwa memang ada halaman administratif yang untuk otoritas tertentu sekaligus meninjau ulang temuan [12] yang dikategorikan sebagai *Broken Access Control* dimana endpoin /admin/dashboard sudah diproteksi dengan membutuhkan proses *login* dengan otoritas administrator.

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

B. *Vulnerability Scanning*

Tahap pemindaian kerentanan dilakukan menggunakan OWASP ZAP versi 2.15.0 dengan ATTACK mode pada Automated Scanning yang dikombinasi Manual Spidering untuk memastikan seluruh endpoint aplikasi terpetakan dengan baik. Berdasarkan hasil pemindaian yang ditunjukan pada gambar, ditemukan total 27 kategori peringatan (alert) yang terbagi ke dalam berbagai tingkat risiko.



Gambar 7. Hasil ZAP

Berdasarkan hasil pemindaian yang dilakukan, ditemukan total 27 jenis peringatan (*alerts*). Temuan tersebut diklasifikasikan berdasarkan tingkat keparahan risiko (*severity*) yang mengacu pada standar OWASP, yaitu high, Medium, Low, dan Informational yang diklasifikasikan pada Tabel 3. Total peringatan yang dapat di identifikasi meningkat dibandingkan dengan penelitian sebelumnya dengan total sebanyak 21 peringatan (*alert)* [12].

.

Tabel 3. Klasifikasi Hasil OWASP ZAP

Tingkat Risiko	Jenis Kerentanan	Jumlah
High	Sql Injection	1
High	SQL Injection – SQLite	18
Medium	Content Security Policy (CSP) Header Not Set	34
Medium	Cross-Domain Misconfiguration	34
Medium	Missing Anti-clickjacking Header	15
Medium	Vulnerable JS Library	1
Medium	Application Error Disclosure	1
Medium	Cross-Domain JS Source File Inclusion	7
Low	Strict-Transport-Security Header Not Set	159
Low	Cookie Misconfiguration (No HttpOnly/Secure)	60
Info	Information Disclosure (Suspicious Comments)	139
Info	User Agent Fuzzer	111

Secara statistik, distribusi risiko didominasi oleh peringatan bersifat informational dan Low yang umumnya berkaitan dengan konfigurasi header keamanan manajemen cookie. Temuan yang diperoleh menghasilkan jumlah alerts yang lebih banyak dibandingkan penelitian [12], yang dilakukan sebelum event diselenggarakan (Pra-Event) yang hanya mengandalkan hasil Automated Scanning. Hal ini menunjukan bahwa kombinasi pemindaian manual

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

dan otomatis dapat mencangkup jangkauan pemindaian yang lebih luas sehingga mengekspos banyak endpoint dan parameter dalam aplikasi. Meskipun scanner mendeteksi sejumlah besar kerentanan, hasil ini masih bersifat indikatif dan memiliki kemungkinan *false positive*. Oleh karena itu , temuan berisiko tinggi (*High*) dan sedang (*Medium*) akan divalidasi pada tahap selanjutnya

C. Analisis dan Validasi

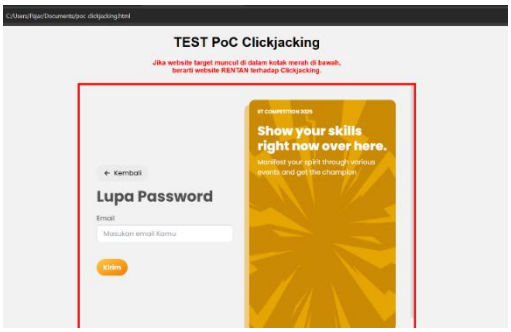
Hasil pemindaian otomatis yang dipaparkan memberikan indikasi awal mengenai postur keamanan aplikasi, namun belum merepresentasikan risiko yang sesungguhnya. Alat pemindai kerentanan seperti OWASP ZAP bekerja dengan mekanisme pencocokan pola (pattern matching) yang sering kali menghasilkan temuan positif yang kurang tepat (*false positive*), terutama pada aplikasi web modern berbasis *client-side rendering*. Oleh karena itu, tahap analisis dan validasi manual PoC menjadi langkah krusial untuk memverifikasi apakah temuan tersebut benar-benar dapat dieksploitasi (*exploitable*). Pada tahap ini, validasi tidak dilakukan terhadap seluruh peringatan, melainkan difokuskan pada kerentanan dengan tingkat risiko High dan Medium yang memiliki dampak signifikan terhadap aspek CIA.

Pemindaian ZAP mendeteksi indikasi SQL Injection (termasuk variansi "SQL Injection – SQLite") pada beberapa parameter input pengguna. Validasi manual dilakukan dengan memasukkan payload injeksi SQL ke endpoint terkait untuk menguji apakah query database dapat dimanipulasi. Hasil pengujian menunjukkan tidak ada satupun payload yang berhasil mengeksekusi perintah SQL tak terotorisasi atau mendapatkan data sensitif. Sebagian besar percobaan injeksi menghasilkan respons error umum atau ditolak oleh aplikasi, menandakan bahwa input tersebut tidak dieksekusi di database. Pada satu skenario, pemasukan karakter khusus memang memicu pesan kesalahan SQL yang menampilkan jejak galat (stack trace) basis data SQLite di halaman web. Munculnya pesan error internal ini mengonfirmasi adanya kelemahan sanitasi input (temuan *Application Error Disclosure*), karena informasi teknis seperti tipe DB dan struktur query terekspos di output. Meski demikian, tidak terdapat bukti bahwa injeksi SQL dapat dieksploitasi lebih lanjut, misalnya upaya klasik seperti 'OR '1'='1 untuk bypass login ataupun union query tidak menghasilkan akses ilegal. Dengan kata lain, temuan SQL Injection diklasifikasikan sebagai *false positive* secara exploitability. Kemungkinan besar mekanisme keamanan tambahan di sisi server atau WAF berhasil mencegah upaya injeksi berbahaya tersebut, sehingga walaupun scanner mengidentifikasi celah ini, serangan tidak dapat dilakukan hingga tuntas.

Validasi manual terhadap temuan *Content Security Policy* (CSP) dilakukan dengan melakukan inspeksi header http pada respons halaman utama dengan menggunakan *curl*. Hasil pengujian menunjukan bahwa respons HTTP tidak menyertakan header CSP. Kondisi ini mengindikasikan bahwa tidak terdapat kebijakan pembatasan eksekusi *script* pada sisi klien sehingga hasil temuan scanner dapat dianggap valid.

Gambar 8. Hasil Curl CSP

Kemudian tahap validasi dilakukan pada kerentanan Missing Anti-Clickjacking Protection dengan membuat halaman uji eksternal yang memuat situs target kedalam elemen *iframe.* Hasilnya menunjukan bahwa halaman target berhasil dimuat. Kondisi ini membuka potensi serangan manipulasi antarmuka pengguna apabila dikombinasikan dengan rekayasa sosial.

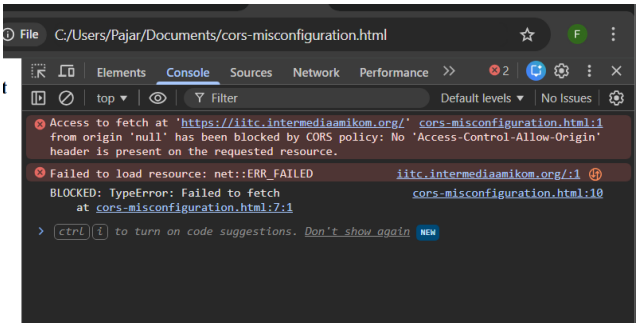


Gambar 10. Hasil Pengujian Iframe Clickjacking

Validasi pada kerentanan kebijakan *Cross-Origin Resource Sharing (CORS)* dilakukan dengan menjalankan permintaan Javascript lintas origin menggunakan metode dari hasil halaman html yang

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

dibuat mandiri. Hasil pengujian menunjukan bahwa browser memblokir akses lintas domain dengan pesan "*No Access-Control-Allow-Origin header is present*", sehingga respons tidak dapat dibaca *script* pihak ketiga. Temuan ini menjadi bukti *false positive* terhadap kerentanan CORS yang dideteksi *scanner.*



Gambar 11. Hasil Pengujian CORS

Temuan *Vulnerable JavaScript Library* dengan analisis berkas JavaScript pada *Network tab,* dan pemindaian menggunakan Retire.js. Hasilnya menunjukan bahwa aplikasi dibangun menggunakan Next.js didukung pustaka (*library)* Tailwind CSS sebagai *framework* Antarmuka pengguna yang demikian sudah terdeteksi sebelumnya pada saat pemindaian menggunakan Wappalyzer. Tidak ditemukan penggunaan pustaka Javascript *legacy* seperti jQuery maupun pihak ketiga lain yang memiliki kerentanan terdokumentasi dalam basis data CVE. *Script* tambahan Javascript yang terdeteksi sebagian besar berasal dari layanan CDN/infra pihak ketiga (Cloudflare) dan tidak termasuk dalam *dependency* aplikasi. Dengan demikian , temuan *Vulnerable JavaScript Library* diklasifikasikan sebagai *false positive*.

D. *Risk Scoring*

Penilaian tingkat risiko pada penelitian ini menggunakan *Common Vulnerability Scoring System* (CVSS) versi 4.0. Skoring hanya diterapkan pada temuan yang telah tervalidasi pada tahap sebelumnya. Pendekatan ini bertujuan memastikan bahwa skor yang dihasilkan merepresentasikan risiko aktual, serta bukan sekedar indikasi dari hasil temuan pemindaian otomatis. Penilaian difokuskan pada *Base Metric Group* CVSS 4.0 dengan mempertimbangkan karakteristik intrinsik dari setiap kerentanan yang meliputi vektor serangan, kompleksitas, eksploitasi, kebutuhan hak akses, interaksi pengguna, serta dampak terhadap aspek CIA. Untuk meningkatkan transparansi analisis risiko, seluruh temuan kerentanan berisiko tinggi dan sedang, yang teridentifikasi pada tahap pemindaian. Skoring kerentanan tervalidasi dilakukan menggunakan parameter Skor CVSS dihitung menggunakan Base Metric Group CVSS v4.0 berdasarkan hasil validasi PoC untuk setiap kerentanan yang terbukti dapat dieksploitasi.

Tabel 4. Hasil Validasi dan *Risk Scoring* Kerentanan

No.	Nama Kerentanan	Hasil PoC	Dampak CIA	Skor CVSS 4.0	Kategori Risiko
1.	SQL Injection (termasuk SQLite)	*False Positive*	-	-	-
2.	Content Security Policy (CSP) Header Not Set	Valid	C: Low I: Low A: None	6.9	*Medium*
3.	Missing Anti-Clickjacking Protection	Valid	C: Low I: Low A: None	5.1	*Medium*
4.	Cross-Origin Resource Sharing (CORS) Misconfiguration	*False Positive*	-	-	-

Jurnal EEMISAS, Vol. 4, No.2, Desember 2025, Hal. 12-28
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

No.	Nama Kerentanan	Hasil PoC	Dampak CIA	Skor CVSS 4.0	Kategori Risiko
5.	Application Error Disclosure	Valid	C: Low I: None A: None	6.9	*Medium*
6.	Vulnerable JavaScript Library	False Positive	-	-	-

Berdasarkan hasil skoring CVSS 4.0, seluruh kerentanan yang tervalidasi berada pada rentang risiko rendah hingga sedang. Temuan dengan indikasi risiko tinggi pada tahap pemindaian awal, yaitu SQL Injection, setelah dilakukanvalidasi PoC terbukti sebagai *false positive* sehingga tidak memiliki skor CVSS. Kerentanan dengan skor tertinggi adalah CSP dan *Application Error Disclosure* dengan skor 6,9 yang termasuk kategori medium. Tidak ditemukan kerentanan dengan tingkat risiko tinggi maupun kritis yang dapat dieksploitasi secara langsung. Hasil ini menunjukkan bahwa postur keamanan website IITC pasca-event berada pada tingkat risiko sedang, dengan fokus mitigasi diarahkan pada perbaikan konfigurasi keamanan untuk mencegah potensi eskalasi serangan di masa mendatang.

E. Perbandingan Hasil Penelitian dengan Studi Sebelumnya

Hasil penelitian ini menunjukkan perbedaan yang cukup signifikan apabila dibandingkan dengan studi-studi sebelumnya yang mengkaji keamanan website IITC maupun website sejenis. Penelitian Khairunnisak (2021) menggunakan metode DREAD dan ISO 27005:2018 menyimpulkan bahwa website IITC berada pada tingkat risiko sedang, namun penilaian risiko tersebut bersifat kualitatif dan sangat bergantung pada subjektivitas analis. Akibatnya, tingkat exploitability dari setiap kerentanan belum dapat diukur secara objektif.

Penelitian selanjutnya oleh Zahrani (2025) melakukan Vulnerability Assessment pada fase pra-event menggunakan OWASP ZAP dan menemukan beberapa kerentanan dengan kategori risiko tinggi dan sedang. Namun, seluruh temuan tersebut didasarkan pada hasil pemindaian otomatis tanpa disertai validasi manual melalui *Proof of Concept*. Pendekatan ini berpotensi menghasilkan *false positive*, terutama pada aplikasi *web* modern yang menggunakan arsitektur client-side rendering dan layanan pihak ketiga.

Tabel 5. Perbandingan Pendekatan dan Implikasi Hasil Penelitian Keamanan Website

Aspek Perbandingan	Penelitian Terdahulu	Penelitian Ini
Objek evaluasi	Website IITC (pra-event) dan website sejenis	Website IITC pada fase *pasca-event*
Metode utama	DREAD dan VA berbasis pemindaian otomatis	VA dengan validasi *Proof of Concept*
Validasi temuan	Tidak dilakukan	Dilakukan secara manual
Potensi *false positive*	Relatif tinggi	Ditekan melalui validasi teknis
Skema penilaian risiko	Kualitatif / CVSS versi lama	CVSS versi 4.0
Fokus interpretasi risiko	Indikasi teknis kerentanan	Exploitability dan dampak aktual
Kontribusi praktis	Identifikasi kerentanan	Prioritisasi mitigasi berbasis risiko

Berdasarkan Tabel 5, perbedaan utama penelitian ini terletak pada proses validasi teknis dan cara interpretasi risiko. Penelitian ini tidak hanya mengidentifikasi kerentanan berdasarkan hasil pemindaian otomatis, tetapi juga memastikan apakah kerentanan tersebut benar-benar dapat dieksploitasi. Hasil validasi menunjukkan bahwa beberapa temuan dengan indikasi risiko tinggi, seperti *SQL Injection*,

terbukti sebagai *false positive* dan tidak dapat dieksploitasi secara teknis.

Secara konseptual, temuan ini memperkuat pandangan bahwa asesmen keamanan aplikasi web modern perlu mengombinasikan pemindaian otomatis, validasi berbasis bukti teknis, serta penilaian risiko terstandar seperti CVSS versi 4.0. Pendekatan ini memungkinkan pengelola *website event* untuk memahami postur keamanan sistem secara lebih akurat dan menetapkan prioritas mitigasi berdasarkan tingkat risiko yang terukur, bukan semata-mata berdasarkan jumlah temuan teknis.

F. Reporting

Tahap reporting menyajikan ringkasan akhir hasil pengujian keamanan yang telah tervalidasi melalui Proof of Concept dan penilaian risiko menggunakan CVSS 4.0. Pelaporan difokuskan pada kerentanan yang terbukti valid secara teknis serta rekomendasi mitigasi yang dapat diterapkan untuk memperbaiki postur keamanan sistem, sebagaimana pendekatan pelaporan pada penelitian VAPT sebelumnya.

Tabel 6. Hasil *Reporting*

Jenis Kerentanan	Status Validasi	Dampak Utama	Rekomendasi Mitigasi
Content Security Policy (CSP) Header Not Set	Valid	Potensi eksekusi skrip berbahaya pada sisi klien (XSS)	Menerapkan header Content-Security-Policy untuk membatasi sumber script, style, dan object hanya dari domain tepercaya
Missing Anti-Clickjacking Protection	Valid	Risiko manipulasi antarmuka pengguna (clickjacking)	Menambahkan header X-Frame-Options: DENY atau kebijakan frame-ancestors pada CSP
Application Error Disclosure	Valid	Kebocoran informasi teknis internal aplikasi	Menonaktifkan pesan error detail pada lingkungan produksi dan menerapkan mekanisme generic error handling
SQL Injection (termasuk SQLite)	False Positive	Tidak terbukti dapat dieksploitasi	Mempertahankan mekanisme validasi input dan prepared statement serta melakukan pengujian berkala
Cross-Origin Resource Sharing (CORS) Misconfiguration	False Positive	Tidak terjadi akses lintas origin ilegal	Mempertahankan konfigurasi CORS saat ini dan melakukan audit berkala
Vulnerable JavaScript Library	False Positive	Tidak ditemukan pustaka rentan	Melakukan dependency audit rutin dan pembaruan pustaka frontend

Berdasarkan hasil reporting, kerentanan yang teridentifikasi didominasi oleh miskonfigurasi keamanan pada sisi aplikasi dan header HTTP, tanpa ditemukannya kerentanan kritis yang dapat dieksploitasi secara langsung. Rekomendasi mitigasi yang diberikan berfokus pada perbaikan konfigurasi keamanan preventif untuk menurunkan potensi eskalasi serangan di masa mendatang serta meningkatkan postur keamanan website secara keseluruhan.

V. KESIMPULAN

Penelitian ini berhasil melakukan analisis risiko keamanan pada website kompetisi nasional IITC menggunakan metode Vulnerability Assessment yang dikombinasikan dengan validasi manual Proof of Concept dan penilaian risiko terukur menggunakan

CVSS versi 4.0. Hasil pemindaian otomatis menggunakan OWASP ZAP menghasilkan sejumlah besar temuan dengan dominasi tingkat informational dan low, serta beberapa indikasi risiko medium dan high. Melalui tahap analisis dan validasi, temuan dengan indikasi risiko tinggi berupa SQL Injection dan variannya terbukti sebagai false positive dan tidak dapat dieksploitasi secara teknis. Kerentanan yang tervalidasi seluruhnya berada pada kategori risiko sedang, dengan skor CVSS tertinggi sebesar 6,9 pada kerentanan Content Security Policy Header Not Set dan Application Error Disclosure. Tidak ditemukan kerentanan dengan tingkat risiko tinggi maupun kritis yang berdampak langsung terhadap kerahasiaan, integritas, maupun ketersediaan data peserta.

Hasil penelitian ini menunjukkan bahwa postur keamanan website IITC pada fase pasca-event berada pada tingkat risiko sedang, dengan kelemahan utama berasal dari aspek miskonfigurasi keamanan aplikasi web, khususnya pada pengaturan header keamanan dan mekanisme penanganan error. Dengan demikian, prioritas mitigasi difokuskan pada perbaikan konfigurasi keamanan sebagai langkah preventif untuk mencegah potensi eskalasi serangan di masa mendatang.

Selain itu, penelitian ini menegaskan pentingnya validasi manual terhadap hasil pemindaian otomatis untuk mengurangi false positive serta menghasilkan penilaian risiko yang lebih objektif dan representatif. Pendekatan ini diharapkan dapat menjadi acuan dalam evaluasi keamanan website event berbasis web yang mengelola data pribadi peserta dalam skala besar.

Meskipun penelitian ini memberikan gambaran objektif mengenai postur keamanan *website* IITC pada fase pasca-event, terdapat beberapa keterbatasan yang perlu diperhatikan. Penelitian ini hanya dilakukan pada satu domain website dan menggunakan satu alat pemindaian utama, yaitu OWASP ZAP, sehingga hasil yang diperoleh belum sepenuhnya merepresentasikan kondisi keamanan *website event* secara umum. Selain itu, pengujian difokuskan pada aspek aplikasi web tanpa mencakup evaluasi infrastruktur internal maupun pengujian keamanan API secara mendalam. Oleh karena itu, penelitian selanjutnya disarankan untuk memperluas objek penelitian pada beberapa *website event* dengan karakteristik yang berbeda, mengombinasikan lebih dari satu tools pemindaian, serta mengintegrasikan metode *penetration testing* lanjutan dan pengujian keamanan API agar diperoleh evaluasi keamanan yang lebih komprehensif dan mendalam.

REFERENSI

[1] M. B. Yel, M. K. M. Nasution, I. Technology, and U. S. Utara, "Keamanan informasi data pribadi pada media sosial," vol. 6, no. 1, pp. 92–101, 2022.

[2] Surfshark, "Data Breach Monitoring: Quarterly Analysis," Surfshark.

[3] J. Tahsinia, A. A. Zulfa, T. Ibrahim, and O. Arifudin, "PERAN SISTEM INFORMASI AKADEMIK BERBASIS WEB," vol. 6, no. 1, pp. 115–134, 2025.

[4] P. Bontonyeleng and B. Web, "SISTEM INFORMASI PELAYANAN KESEHATAN PADA PUSKESMAS BONTONYELENG BERBASIS WEB," *Amm. J. Syst. Inf. Comput. Inst. Teknol. Dan Bisnis Bina Adinata*, vol. 1, no. 1, pp. 47–67, 2023.

[5] S. B. Lampung, A. Firdhayanti, M. Agarina, A. Suryadi, and M. R. F. M, "PEMANFAATAN INTEGRASI PAYMENT GATEWAY DI," vol. 7, no. 2, pp. 156–164, 2024.

[6] D. Hariyanto *et al.*, "Implementasi Metode RapidApplication Development Pada Sistem Informasi Perpustakaan," vol. 13, no. 1, pp. 110–117, 2021.

[7] U. Nurhasan, D. H. Subhi, A. N. Rahmanto, T. Informasi, P. N. Malang, and P. N. Malang, "Inovasi Pengelolaan Lomba Pramuka Berbasis Website dalam Rangka Penerapan Konsep Smart School fleksibilitas pengelolaan (' Perancangan Sistem Informasi Registrasi Lomba Pekan Olahraga Dan Seni Berbasis Web ,' 2021 ; Setiawan & Lestari , 2023 ; Yunita & Ru," vol. 11, no. 3, pp. 326–340, 2025, doi: 10.30997/qh.v11i3.21316.

[8] D. Afriani, D. Sihombing, L. Romadani, and K. Kunci, "Sistem Informasi Media Kegiatan Jurusan Teknik Informatika Politeknik Negeri Bengkalis : Sentralisasi Informasi Event Mahasiswa," vol. 01, no. 01, pp. 1–5, 2025.

[9] F. C. Islami, "Analisis Kerentanan Website XYZ Menggunakan Metode Vulnerability Assessment Penetration Testing Dan OWASP

WSTG (Studi Kasus: XYZ)," *J. Apl. dan Teor. Ilmu Komput.*, vol. 7, no. 2, pp. 93–99, 2025, doi: 10.17509/jatikom.v7i2.80934.

[10] R. marta Dinata, M. Alzril, M. I. Yamin, H. Effendi, and M. Febriansyah, "Analisis Keamanan Situs Web Rumah Sakit Menggunakan Metode Penetration Testing OWASP," *Sainstech J. Penelit. Dan Pengkaj. Sains Dan Teknol.*, vol. 35, no. 2, pp. 99–100, 2025, doi: 10.37277/stch.v35i2.2383.

[11] Gina Cahya Utami, Aden Bahtiar Supramaji, and Khairunnisak Nur Isnaini, "Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 8, no. 1, pp. 47–56, 2023, doi: 10.32528/justindo.v8i1.219.

[12] Aura Arnelia Zahrani, Dzihni Safwa Alifah, Yulia Cahyani, and Ilham Albana, "Analisis Vulnerability Assessment pada Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP," *Bridg. J. Publ. Sist. Inf. dan Telekomun.*, vol. 3, no. 2, pp. 55–68, 2025, doi: 10.62951/bridge.v3i2.425.

[13] A. A. Zahrani, D. S. Alifah, Y. Cahyani, and I. Albana, "Analisis Vulnerability Assessment pada Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP," 2025.

[14] N. Papakonstantinou, D. L. Van Bossuyt, B. Hale, R. Arlitt, J. Salonen, and J. Suomalainen, "CyberRiskDELPHI: Towards Objective Cyber Risk Assessment for Complex Systems," in International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, vol. Volume 2: 2023, p. V002T02A049. doi: 10.1115/DETC2023-114783.

[15] A. Aliyu, U. Ilyasu, and A. Zakariya, "Comparative Analysis and Evaluation of Web Application Security Tools for Enhanced Cyber security," vol. 3, no. 5, pp. 230–238, 2023.

[16] D. Dumaniya, "An Automated Web Vulnerability Scanner for Detecting Common Security Flaws in Modern Web Applications," pp. 372–378, 2025.

[17] B. Milosavljević, Z. Bogićević, and B. Prlinčević, "CYBER SECURITY , THREATS AND PROTECTION MECHANISMS," pp. 90–97, 2025.

[18] E. Zakia, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," vol. 01, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.

[19] I. G. J. E. P. I Made Adi Surya Permana, I Gede Putu Krisna Juliharta, "Analisis Keamanan Sistem Informasi Menggunakan Metode Vulnerability Assesment pada Aplikasi Web Karangasem. go.id," *Remik Ris. dan E-Jurnal Manaj. Inform. Komput.*, vol. 9, no. 2, pp. 466–473, 2025.

[20] H. Albani Bardian and I. Sutanto, "Pengembangan Aplikasi Vulnerability Scanner Untuk Mendeteksi Celah Keamanan Siber Pada Website," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 3, pp. 4404–4411, 2025, doi: 10.36040/jati.v9i3.13656.

[21] M. K. Adrian, P. D. Ibnugraha, and H. H. Nuha, "Integrating CVSS , OWASP , and APPI for a Comprehensive Risk Analysis of SQL Injection Vulnerabilities in E-Commerce," vol. 7, no. 1, pp. 17–23, 2025.

[22] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," vol. 09, pp. 118–125, 2024.

[23] M. A. Nurrizki, E. Iman, and H. Ujianto, "Analisis Keamanan Website Desa Budaya DIY Dengan Metode Penetration Testing (Pentest) dan OWASP ZAP," vol. 5, no. 1, pp. 22–27, 2024.

[24] R. Farismana and D. Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," vol. 3, no. 2, pp. 26–33, 2023.

[25] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, pp. 853–860, 2020, doi:

10.25126/jtiik.2020701928.

[26] D. Rohmaniah, W. M. Ashari, L. Lukman, and A. D. Putra, "Enhancing Website Security Using Vulnerability Assessment and Penetration Testing (VAPT) Based on OWASP Top Ten," *J. Appl. Informatics Comput.*, vol. 9, no. 2, pp. 404–411, 2025, doi: 10.30871/jaic.v9i2.9069.