Analisis keamanan website instansi Y menggunakan *passive footprinting* dan penilaian risiko berbasis CVSS

Belia Putri Salsabila, Henni Endah Wahanani*, Achmad Junaidi

Program Studi Informatika, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur
Email: 22081010311@student.upnjatim.ac.id; henniendah@upnjatim.ac.id; achmadjunaidi.if@upnjatim.ac.id

Abstrak
Penelitian ini menganalisis keamanan website Instansi Y menggunakan metode passive footprinting berbasis Open-Source Intelligence (OSINT) dan penilaian risiko Common Vulnerability Scoring System (CVSS) v3.1. Pengumpulan data dilakukan secara non-intrusif melalui instrumen Wappalyzer, Whois, dan Nslookup. Hasil penelitian menunjukkan website menggunakan framework Angular versi 20.3.9 dan layanan Cloudflare. Berdasarkan skor CVSS, ditemukan profil risiko pada kategori rendah hingga sedang (low to medium), dengan skor tertinggi 5.3 akibat eksposur versi perangkat lunak dan rincian DNS. Meskipun tidak ditemukan kerentanan kritis, informasi teknis yang terbuka ini memperluas permukaan serangan (attack surface) pada fase pengintaian. Strategi mitigasi yang direkomendasikan meliputi header hardening, de-identifikasi infrastruktur, dan penerapan Content Security Policy (CSP). Penelitian ini menyimpulkan bahwa audit pasif sangat efektif sebagai langkah preventif awal untuk mengidentifikasi kebocoran informasi teknis pada instansi pemerintah.

Kata Kunci: keamanan website; passive footprinting; OSINT; CVSS v3.1; attack surface

Security analysis of agency Y's website using passive footprinting and CVSS-based risk assessment

Abstract
Abstract This research analyzes the security of the Y Agency's website using the passive footprinting method based on Open-Source Intelligence (OSINT) and the risk assessment of the Common Vulnerability Scoring System (CVSS) v3.1. Data collection was conducted non-intrusively using the Wappalyzer, Whois, and Nslookup instruments. The research results show that the website uses the Angular framework version 20.3.9 and Cloudflare services. Based on the CVSS score, a risk profile was found in the low to medium category, with the highest score being 5.3 due to the exposure of software versions and DNS details. Although no critical vulnerabilities were found, this open technical information expands the attack surface during the reconnaissance phase. The recommended mitigation strategies include header hardening, infrastructure de-identification, and the implementation of a Content Security Policy (CSP). This study concludes that passive audits are very effective as an initial preventive step to identify technical information leaks in government agencies.

Keywords: *website security; passive footprinting; OSINT; CVSS v3.1; attack surface*

1. Pendahuluan
Website merupakan infrastruktur utama dalam penyelenggaraan layanan digital di sektor pemerintahan, berfungsi sebagai media informasi publik, layanan administrasi, serta sarana interaksi masyarakat. Namun, keterbukaan akses ini menjadikan website pemerintah target potensial serangan siber seperti pencurian data dan gangguan layanan (OWASP, 2021). Insiden keamanan sering kali tidak diawali oleh eksploitasi tingkat lanjut, melainkan dipicu oleh kebocoran informasi teknis dan kesalahan konfigurasi sistem yang tidak teridentifikasi (Kuehn et al., 2023; CISA, 2024). Hal ini menunjukkan bahwa visibilitas terhadap *attack surface* (permukaan serangan) sangat krusial dalam membentuk postur pertahanan siber yang kokoh (Stallings, 2023; Brooks, 2021).

Meskipun metode *penetration testing* aktif umum digunakan, teknik tersebut berisiko menimbulkan gangguan operasional pada layanan publik yang membutuhkan stabilitas tinggi (Akbar et al., 2025; Putra & Sari, 2023). Oleh karena itu, pendekatan *passive footprinting* berbasis *Open-Source Intelligence* (OSINT) menjadi solusi alternatif yang aman dan non-intrusif (Allo & Widiasari, 2024;

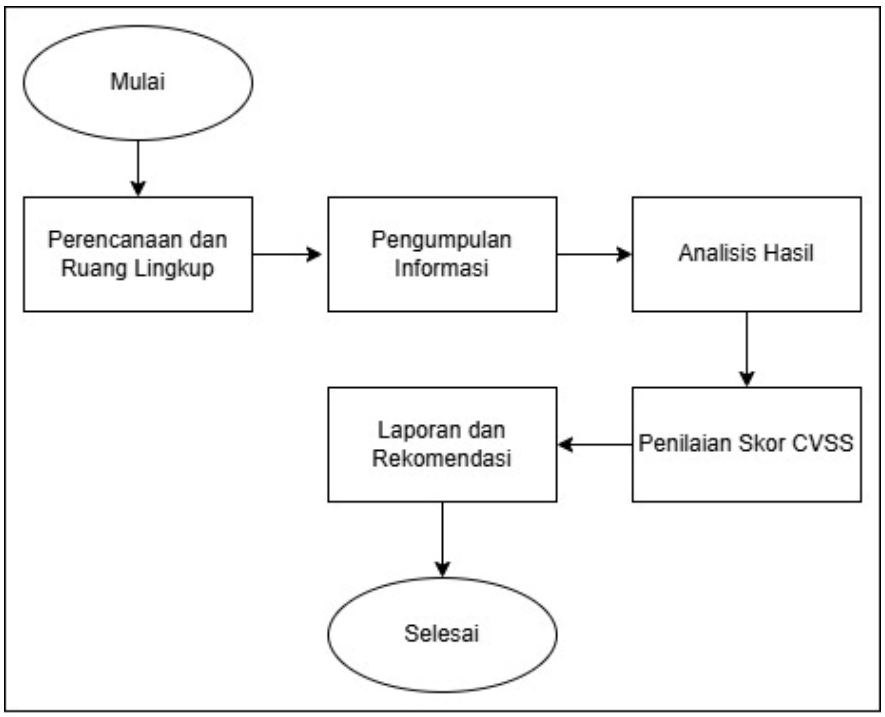
Ahmad & Fitriani, 2022). Teknik ini memanfaatkan data publik seperti *DNS record*, WHOIS, dan metadata tanpa melakukan interaksi langsung dengan sistem target (Bazzell, 2022; Ramadan, 2023). Studi menunjukkan bahwa informasi pasif sangat efektif dalam mengungkap detail teknis sensitif yang dapat dimanfaatkan dalam rantai serangan siber (Sanjaya, 2024; Hidayat et al., 2024).

Agar hasil pengintaian dapat dianalisis secara objektif, diperlukan mekanisme penilaian risiko yang terukur. *Common Vulnerability Scoring System* (CVSS) v3.1 merupakan standar internasional dari FIRST (2023) yang mengukur tingkat keparahan berdasarkan aspek *Confidentiality, Integrity,* dan *Availability* (CIA). Integrasi antara *passive footprinting* dan penilaian CVSS mampu menghasilkan model analisis keamanan yang komprehensif bagi instansi pemerintah (Pratama et al., 2025; Wijaya, 2022). Berdasarkan urgensi tersebut, penelitian ini bertujuan untuk menganalisis keamanan website Instansi Y menggunakan pendekatan integratif guna memperoleh pemetaan risiko yang valid sebagai dasar rekomendasi mitigasi.

2. Metode

Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan metode analisis keamanan berbasis passive footprinting dan penilaian risiko menggunakan *Common Vulnerability Scoring System* (CVSS). Pendekatan ini dipilih karena penelitian bertujuan untuk mengidentifikasi dan mengukur tingkat risiko keamanan website Instansi Y tanpa melakukan eksploitasi atau interaksi langsung terhadap sistem target.

Objek penelitian adalah website resmi Instansi Y yang dapat diakses secara publik melalui jaringan internet. Ruang lingkup penelitian dibatasi pada pengumpulan dan analisis informasi yang bersifat terbuka (*open information*), tanpa mencakup aktivitas eksploitasi, penetrasi, maupun akses ke dalam sistem internal. Seluruh proses penelitian dilakukan secara daring dengan memanfaatkan sumber informasi publik.



Gambar 1. *Flowchart* Penelitian

Pada Gambar 1. menunjukkan alur atau tahapan penelitian untuk menganalisis keamanan website, yang terdiri dari beberapa tahapan utama:

1. Perencanaan dan Ruang Lingkup
   Pada tahap pertama meliputi penetapan objek penelitian, yaitu website Instansi Y, serta penentuan batasan aktivitas analisis yang dilakukan agar penelitian tetap berada pada ruang lingkup yang telah ditetapkan.

2. Pengumpulan Informasi (*Passive Footprinting*)
   Selanjutnya pada tahap teknik *passive footprinting* berbasis *open-source intelligence* (OSINT) untuk memperoleh data teknis, seperti informasi domain, DNS, teknologi server, aplikasi web, serta metadata website, tanpa melakukan interaksi langsung dengan sistem target.
3. Analisis Hasil
   Pada tahap ini dilakukan proses identifikasi terhadap informasi teknis yang diperoleh untuk menentukan potensi risiko keamanan, seperti versi perangkat lunak yang digunakan, konfigurasi layanan, serta eksposur informasi publik yang dapat dimanfaatkan oleh pihak tidak berwenang.
4. Penilaian Skor CVSS
   Tahap ini dilakukan dengan memetakan potensi kerentanan yang teridentifikasi ke dalam skema *Common Vulnerability Scoring System* (CVSS) dan memberikan skor berdasarkan parameter *Attack Vector, Attack Complexity, Privileges Required,* serta dampaknya terhadap aspek *Confidentiality, Integrity, dan Availability*.
5. Laporan dan Rekomendasi
   Tahap akhir berupa penyusunan laporan yang memuat ringkasan hasil analisis keamanan, klasifikasi tingkat risiko (*Low*, *Medium*, *High*, dan *Critical*), serta rekomendasi mitigasi yang dapat diterapkan oleh pengelola website Instansi Y.

3. Hasil dan Pembahasan

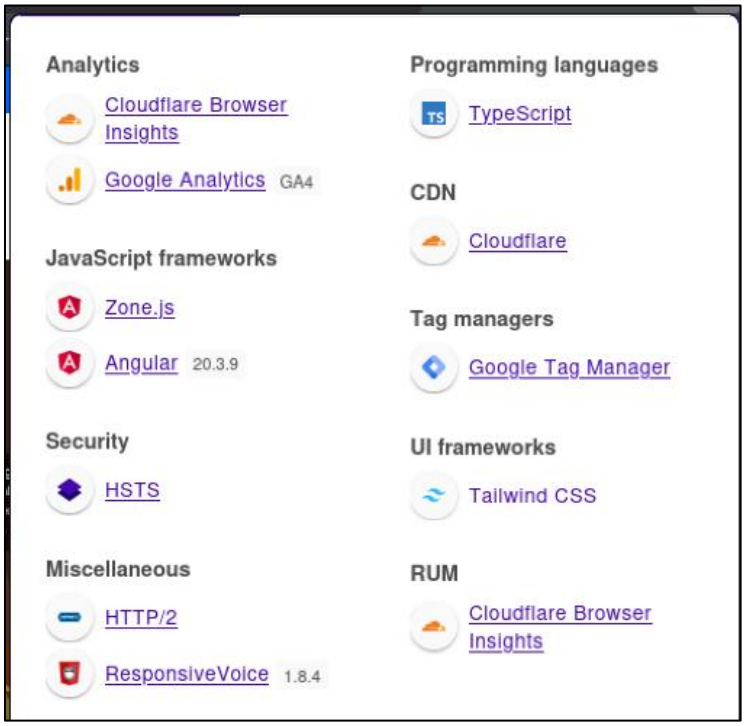
3.1. Hasil *Passive Footprinting*

Tahap *passive footprinting* bertujuan untuk mengumpulkan informasi teknis mengenai website Instansi Y melalui sumber terbuka (*open-source intelligence*/OSINT) tanpa melakukan interaksi langsung dengan sistem target. Proses ini dilakukan menggunakan beberapa tools, yaitu Wappalyzer, Whois, dan Nslookup, yang masing-masing memiliki fungsi berbeda dalam mengidentifikasi karakteristik infrastruktur website.

Penggunaan beberapa tools ini dimaksudkan untuk memperoleh gambaran menyeluruh terkait teknologi aplikasi, kepemilikan domain, serta konfigurasi DNS dan jaringan. Informasi yang diperoleh kemudian dianalisis untuk mengidentifikasi potensi risiko keamanan yang mungkin muncul akibat eksposur informasi teknis tersebut.

3.1.1. Hasil Wapplayzer

Wappalyzer merupakan instrumen analisis berbasis *open-source intelligence* (OSINT) yang digunakan untuk melakukan identifikasi serta pemetaan tumpukan teknologi (*technology stack*) pada suatu aplikasi berbasis web secara pasif. Alat ini bekerja dengan melakukan dekonstruksi terhadap komponen perangkat lunak melalui analisis pola pada *HTTP response headers*, struktur kode sumber HTML, variabel JavaScript, serta *cookies* yang terekspos ke publik. Secara fungsional, Wappalyzer mampu mengklasifikasikan berbagai entitas teknis yang meliputi *framework* aplikasi, sistem manajemen konten (CMS), bahasa pemrograman sisi klien maupun server, layanan analitik, hingga infrastruktur keamanan jaringan seperti *Content Delivery Network* (CDN). Dalam kerangka kerja *passive footprinting*, penggunaan alat ini sangat krusial untuk mengidentifikasi permukaan serangan (*attack surface*) tanpa melakukan interaksi langsung yang bersifat intrusif terhadap sistem target, sehingga integritas dan stabilitas operasional sistem tetap terjaga.



Gambar 2. Hasil Wapplayzer

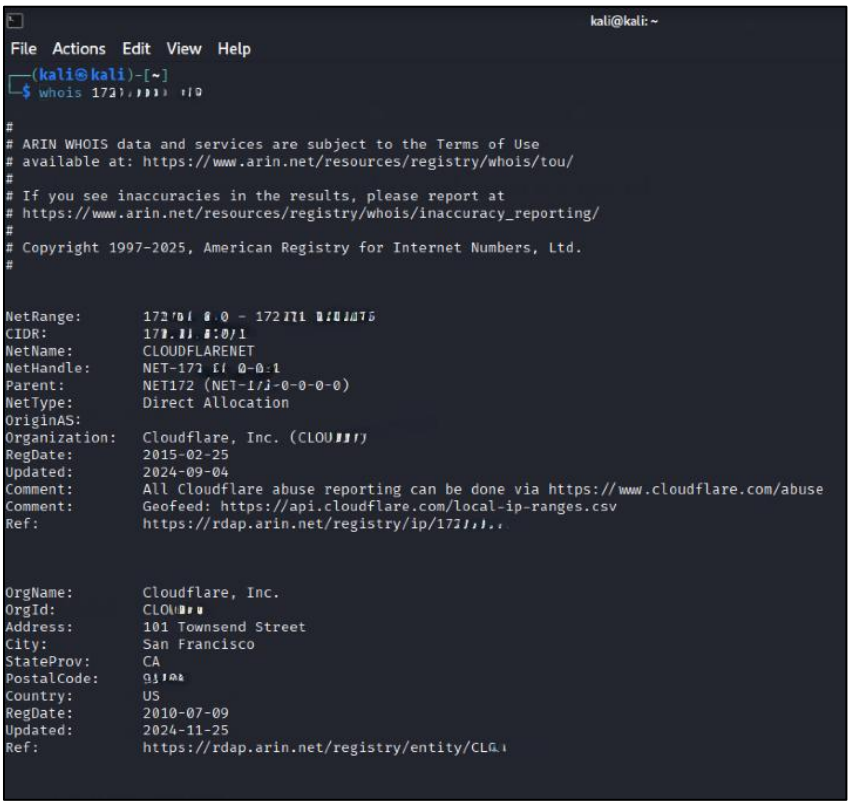
Pada Gambar 2. Berdasarkan hasil pengujian menggunakan Wappalyzer menunjukkan bahwa website Instansi Y menggunakan beberapa teknologi utama, antara lain:

1. Framework JavaScript Angular (versi 20.3.9),
2. Bahasa pemrograman TypeScript,
3. Content Delivery Network (CDN) Cloudflare,
4. Layanan analitik Google Analytics (GA4) dan Cloudflare Browser Insights,
5. UI framework Tailwind CSS,
6. Implementasi keamanan HSTS (HTTP Strict Transport Security),
7. Protokol komunikasi HTTP/2.

Penggunaan Angular dan TypeScript menunjukkan bahwa website dibangun menggunakan arsitektur aplikasi web modern berbasis *single-page application* (SPA). Selain itu, penggunaan Cloudflare sebagai CDN mengindikasikan adanya mekanisme proteksi dasar terhadap trafik, seperti DDoS *mitigation* dan *traffic filtering*. Namun, informasi teknologi yang terungkap ini juga dapat dimanfaatkan oleh pihak tidak berwenang untuk melakukan *technology fingerprinting* sebagai tahap awal serangan.

3.1.2. Hasil Whois

Whois adalah protokol kueri basis data yang digunakan untuk mengidentifikasi informasi administratif dan teknis terkait kepemilikan domain serta alamat IP target. Melalui instrumen ini, peneliti dapat memperoleh data krusial seperti identitas organisasi pendaftar, tanggal pendaftaran dan kedaluwarsa domain, serta konfigurasi *nameserver* yang digunakan. Dalam tahap *passive footprinting*, Whois berfungsi untuk memetakan kepemilikan infrastruktur digital secara non-intrusif guna menentukan batasan aset dan ruang lingkup audit keamanan tanpa melibatkan interaksi langsung dengan server operasional.

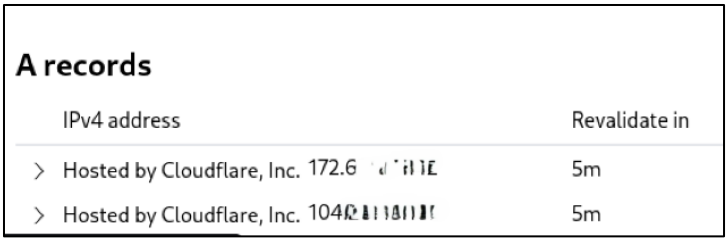


Gambar 3. Hasil Whois

Pada Gambar 3. Berdasarkan hasil Whois menunjukkan bahwa alamat IP website Instansi Y berada dalam rentang jaringan yang dimiliki oleh Cloudflare, Inc., dengan netname CLOUDFLARENET. Informasi ini menunjukkan bahwa server website berada di balik infrastruktur Cloudflare dan tidak langsung mengungkap alamat IP server asli (*origin server*). Penggunaan layanan pihak ketiga seperti Cloudflare memberikan keuntungan dari sisi keamanan, namun di sisi lain juga menunjukkan ketergantungan pada layanan eksternal. Selain itu, informasi organisasi dan lokasi yang terbuka tetap dapat digunakan sebagai bagian dari pemetaan infrastruktur oleh pihak yang melakukan pengintaian.

3.1.3. Hasil Nslookup

Nslookup *(Name Server Lookup)* merupakan instrumen baris perintah (*command-line*) yang digunakan untuk melakukan kueri terhadap sistem penamaan domain (*Domain Name System*/DNS) guna memetakan nama domain ke alamat IP atau sebaliknya. Secara teknis, alat ini berfungsi untuk mengekstraksi rekaman DNS (*DNS records*) yang krusial, seperti rekaman A (*Address*), CNAME (*Canonical Name*), dan MX (*Mail Exchanger*). Dalam kerangka *passive footprinting*, *Nslookup* berperan penting untuk mengidentifikasi infrastruktur jaringan server dan mendeteksi penggunaan layanan pihak ketiga, seperti *reverse proxy* atau CDN, yang bertujuan untuk menyamarkan alamat IP asli server target.



Gambar 4. Hasil Nslookup

Pada Gambar 4. Berdasarkan hasil Nslookup menunjukkan bahwa domain website Instansi Y memiliki beberapa *A records* yang semuanya mengarah ke alamat IP milik Cloudflare, Inc. Hal ini menunjukkan bahwa sistem DNS website dikonfigurasi untuk menggunakan layanan reverse proxy Cloudflare. Konfigurasi ini memberikan keuntungan dari sisi keamanan karena alamat IP server asli tidak terekspos secara langsung ke publik. Namun demikian, keberadaan beberapa A record juga memperluas permukaan serangan (attack surface) apabila salah satu konfigurasi DNS tidak dikelola dengan baik.

3.2. Analisis Hasil Risiko Keamanan

Berdasarkan hasil passive footprinting, teridentifikasi sejumlah informasi teknis yang berpotensi Berdasarkan tahapan *passive footprinting*, teridentifikasi sejumlah informasi teknis pada website Instansi Y yang memiliki implikasi terhadap postur keamanan sistem. Temuan-temuan tersebut dianalisis lebih lanjut untuk memahami potensi risiko yang muncul akibat eksposur informasi publik:

1. Eksposur Teknologi Inti dan *Fingerprinting*: Terdeteksinya penggunaan *framework* Angular versi 20.3.9, bahasa TypeScript, dan Tailwind CSS melalui Wappalyzer memungkinkan pihak tidak berwenang melakukan *technology fingerprinting*. Informasi versi yang sangat spesifik ini berpotensi mempercepat tahap *reconnaissance* karena penyerang dapat mencari basis data kerentanan (CVE) yang relevan dengan versi perangkat lunak tersebut.
2. Ketergantungan Infrastruktur Jaringan Eksternal: Hasil analisis Whois dan Nslookup mengonfirmasi bahwa seluruh trafik website diarahkan melalui jaringan Cloudflare, Inc.. Meskipun penggunaan *reverse proxy* dan CDN ini memberikan proteksi terhadap serangan DDoS, kondisi ini menciptakan ketergantungan pada pihak ketiga yang dapat menjadi *single point of failure* jika terjadi kesalahan konfigurasi atau gangguan layanan pada penyedia.
3. Eksposur Metadata Analitik dan Layanan Pihak Ketiga: Ditemukannya *tracking script* dari Google Analytics (GA4), Google Tag Manager, serta Cloudflare Browser Insights menunjukkan adanya aliran data metadata ke layanan eksternal. Jika tidak dikelola dengan ketat, integrasi layanan pihak ketiga ini dapat menjadi vektor serangan *supply chain* yang mengeksploitasi kepercayaan antara website utama dan penyedia layanan analitik.
4. Konfigurasi DNS dan Permukaan Serangan: Keberadaan beberapa *A records* yang terdeteksi melalui Nslookup, walaupun semuanya mengarah ke IP Cloudflare, tetap memperluas *attack surface* (permukaan serangan) secara administratif. Hal ini menuntut manajemen konfigurasi DNS yang sangat presisi guna menghindari risiko pembajakan subdomain atau kesalahan rute trafik jika terdapat rekaman DNS yang tidak lagi digunakan.

Secara keseluruhan, eksposur informasi teknis ini menempatkan website pada risiko terkait aspek Confidentiality (Kerahasiaan) karena struktur internal dan spesifikasi teknologi sistem dapat dipetakan secara jelas dari luar. Oleh karena itu, diperlukan penilaian kuantitatif menggunakan skema CVSS v3.1 untuk menentukan prioritas mitigasi yang tepat.

3.3 Penilaian Risiko CVSS

Penilaian risiko keamanan pada penelitian ini dilakukan menggunakan standar Common Vulnerability Scoring System (CVSS) versi 3.1, yang bertujuan untuk mengkuantifikasi tingkat risiko dari setiap temuan hasil passive footprinting. CVSS digunakan karena mampu memberikan skor numerik yang objektif berdasarkan karakteristik kerentanan serta dampaknya terhadap sistem.

Dalam penilaian ini, parameter utama yang digunakan meliputi *Attack Vector* (AV*), Attack Complexity* (AC), dan *Privileges Required* (PR), serta dampak terhadap tiga aspek keamanan utama, yaitu *Confidentiality* (C), *Integrity* (I), dan *Availability* (A). *Attack Vector* menunjukkan dari mana serangan dapat dilakukan, *Attack Complexity* menggambarkan tingkat kesulitan eksploitasi, dan *Privileges Required* menunjukkan apakah penyerang memerlukan hak akses khusus. Sementara itu, aspek CIA digunakan untuk mengukur sejauh mana dampak kerentanan terhadap kerahasiaan, keutuhan, dan ketersediaan sistem.

	Temuan	Vektor Serangan (CVSS v3.1 Vector)	Skor CVSS	Kategori
1	Eksposur Versi Framework (Angular 20.3.9)	AV:N/AC:L/PR:N/UI:N/S:U/C:L /I:N/A:N	5.3	Medium
2	Eksposur Metadata Analitik (GA4/GTM)	AV:N/AC:H/PR:N/UI:R/S:U/C:L /I:N/A:N	3.1	Low
3	Keterbukaan Rincian DNS (Nslookup Records)	AV:N/AC:L/PR:N/UI:N/S:U/C:L /I:N/A:N	5.3	Medium
4	Informasi Infrastruktur CDN (Cloudflare)	AV:N/AC:H/PR:N/UI:N/S:U/C: N/I:N/A:N	0.0	None

Berdasarkan data yang disajikan pada Tabel 1, hasil kueri dan pemindaian pasif menunjukkan bahwa profil risiko keamanan website Instansi Y secara agregat berada pada tingkat rendah hingga sedang (*low to medium*). Risiko pada kategori sedang (*medium*) dengan skor 5.3 didominasi oleh eksposur versi spesifik *framework* Angular serta rincian rekaman DNS. Secara teknis, temuan ini memiliki vektor serangan berbasis jaringan (*network*) dengan tingkat kompleksitas rendah (*low complexity*), yang mengindikasikan bahwa informasi tersebut dapat diakses oleh pihak eksternal tanpa memerlukan hak akses khusus maupun interaksi pengguna. Dalam kerangka kerja keamanan siber, keterbukaan informasi teknologi yang mendetail memfasilitasi aktivitas *vulnerability mapping*, di mana penyerang dapat secara presisi mengidentifikasi celah keamanan pada pangkalan data CVE (*Common Vulnerabilities and Exposures*) yang relevan dengan versi perangkat lunak yang digunakan.

Analisis lebih lanjut menunjukkan bahwa dampak utama dari temuan ini terkonsentrasi pada aspek kerahasiaan (*confidentiality*). Meskipun tidak ditemukan bukti kebocoran data sensitif pengguna secara langsung, eksposur metadata teknis dan struktur arsitektur jaringan memberikan keuntungan asimetris bagi penyerang dalam merancang strategi serangan yang lebih terarah. Di sisi lain, temuan mengenai implementasi infrastruktur Cloudflare dan protokol HSTS yang memperoleh skor 0.0 mencerminkan efektivitas kontrol keamanan yang telah diterapkan guna memitigasi risiko serangan *Man-in-the-Middle* serta proteksi terhadap ancaman pada lapisan transportasi data. Secara keseluruhan, walaupun tidak ditemukan celah yang sangat berbahaya, informasi teknis yang terekspos ini perlu segera dirapikan atau disembunyikan agar tidak menjadi langkah awal bagi serangan yang lebih serius di masa mendatang.

3.4 Laporan dan Rekomendasi

Berdasarkan hasil analisis dan penilaian risiko menggunakan kerangka kerja CVSS v3.1, rekomendasi mitigasi diprioritaskan pada temuan dengan skor 5.3 (Medium) yang memiliki dampak langsung terhadap aspek kerahasiaan informasi teknis. Strategi mitigasi difokuskan pada pengurangan eksposur informasi melalui teknik obfuscation (pengaburan) dan penguatan konfigurasi pada lapisan aplikasi serta jaringan guna mempersempit permukaan serangan (attack surface).

Tabel 2. Rekomendasi Mitigasi Keamanan

	Temuan	Tingkat Risiko	Rekomendasi Mitigasi	Sasaran Keamanan
1	Eksposur Versi Angular	*Medium*	Melakukan *header hardening* dengan menghapus informasi *X-Powered-By* atau *Server* header, serta melakukan *minification* kode produksi untuk menyembunyikan versi *framework*.	Mencegah *technology fingerprinting* dan pencarian CVE yang relevan dengan versi perangkat lunak.
2	Eksposur Metadata Analitik	*Low*	Mengatur kebijakan keamanan konten (*Content Security Policy*/CSP) untuk membatasi domain pihak ketiga yang diizinkan berinteraksi dengan website.	Meminimalisir risiko serangan *supply chain* dan kebocoran metadata melalui skrip analitik.
3	Keterbukaan Rekaman DNS	*Medium*	Mengaktifkan fitur *Proxy Status* (awan oranye) pada Cloudflare untuk seluruh rekaman DNS dan membatasi akses ke alamat IP asli melalui *firewall*.	Mengaburkan lokasi infrastruktur fisik dan mencegah serangan langsung ke alamat IP server (*origin IP*).
4	Efektivitas Kontrol	*None*	Melakukan audit berkala pada masa berlaku sertifikat SSL/TLS dan memperbarui daftar *preload* HSTS secara konsisten.	Mempertahankan resiliensi terhadap serangan *Man-in-the-Middle* yang telah terdeteksi baik.

Berdasarkan tabel 2, strategi perbaikan keamanan untuk website Instansi Y difokuskan pada penguatan pertahanan melalui dua pendekatan utama, yakni pengaburan informasi teknis dan penguatan kebijakan internal.

Pertama, untuk mengatasi temuan dengan risiko Sedang (*Medium*), prioritas utama adalah meminimalkan jejak digital teknis. Langkah *header hardening* berfungsi untuk menghapus identitas perangkat lunak (seperti versi Angular) dari lalu lintas data publik. Hal ini sangat penting karena jika versi perangkat lunak diketahui, penyerang dapat dengan mudah mencari daftar celah keamanan yang sudah ada di internet. Selain itu, penggunaan fitur *Proxy* pada Cloudflare secara menyeluruh akan menyembunyikan alamat IP asli server. Dengan cara ini, penyerang tidak dapat menargetkan serangan langsung ke pusat data instansi, melainkan harus melewati sistem penyaring terlebih dahulu.

Kedua, untuk risiko tingkat Rendah (*Low*) dan Nihil (*None*), rekomendasi ditekankan pada penguatan kebijakan internal. Implementasi *Content Security Policy* (CSP) berperan sebagai filter yang memastikan hanya skrip dari sumber terpercaya yang boleh dijalankan oleh website. Ini adalah langkah preventif agar metadata atau data analitik tidak disalahgunakan oleh pihak ketiga. Sementara itu, audit berkala pada sertifikat SSL/TLS dan pembaruan daftar HSTS bertujuan untuk memastikan saluran komunikasi antara pengguna dan website tetap terenkripsi dengan standar terbaru, sehingga kebal terhadap upaya penyadapan data di tengah jalan (*Man-in-the-Middle attack*).

Secara keseluruhan, seluruh rekomendasi ini bertujuan untuk mempersulit fase awal serangan (*reconnaissance*). Dengan mengurangi informasi teknis yang terekspos secara pasif, instansi dapat menciptakan lingkungan digital yang lebih aman dan tangguh terhadap berbagai upaya eksploitasi di masa mendatang.

4. Kesimpulan

Berdasarkan hasil analisis keamanan yang dilakukan pada website Instansi Y menggunakan pendekatan *passive footprinting* dan penilaian risiko berbasis CVSS v3.1, dapat ditarik beberapa kesimpulan utama. Pertama, integrasi teknik *Open-Source Intelligence* (OSINT) melalui instrumen Wappalyzer, Whois, dan Nslookup berhasil memetakan tumpukan teknologi dan infrastruktur jaringan target secara non-intrusif tanpa mengganggu stabilitas operasional layanan. Temuan menunjukkan adanya eksposur informasi teknis yang mendetail, mencakup penggunaan *framework* Angular versi 20.3.9, bahasa TypeScript, serta konfigurasi DNS yang diarahkan melalui layanan *reverse proxy* Cloudflare.

Kedua, hasil penilaian risiko menggunakan kerangka kerja CVSS v3.1 menunjukkan bahwa profil risiko keamanan website Instansi Y secara agregat berada pada tingkat rendah hingga sedang (*low to medium*). Risiko pada kategori sedang (*medium*) dengan skor 5.3 menjadi temuan paling krusial, yang bersumber dari keterbukaan versi perangkat lunak spesifik dan rincian rekaman DNS. Meskipun tidak ditemukan celah keamanan kritikal yang memungkinkan eksploitasi langsung terhadap integritas data, eksposur metadata teknis ini secara signifikan memperluas permukaan serangan (*attack surface*) dan memberikan keuntungan strategis bagi aktor ancaman dalam fase *reconnaissance* atau pengintaian.

Sebagai langkah tindak lanjut, penelitian ini merekomendasikan strategi mitigasi yang berfokus pada teknik pengaburan melalui *header hardening* serta de-identifikasi infrastruktur untuk menyembunyikan alamat IP asli server. Implementasi *Content Security Policy* (CSP) dan pemeliharaan protokol keamanan seperti HSTS juga menjadi prioritas untuk memperkuat pertahanan berlapis. Secara keseluruhan, penelitian ini menegaskan bahwa audit keamanan berkala berbasis metode pasif sangat efektif sebagai langkah preventif bagi instansi pemerintah untuk mengidentifikasi kebocoran informasi teknis sebelum dimanfaatkan dalam rantai serangan siber yang lebih kompleks.

5. Ucapan terimakasih

Penulis menyampaikan terima kasih banyak atas dukungannya kepada Ibu Henni Endah Wahanani, S.Kom., M.T., dan Bapak Achmad Junaidi, S.Kom., M.Kom., selaku dosen pembimbing atas arahan dan bimbingan konstruktif yang telah diberikan. Ucapan terimakasih juga disampaikan kepada instansi Y sebagai objek studi, serta Tim Seminar UNISAYOGYA atas kontribusinya dalam penyediaan standar publikasi ilmiah.

Akhirnya, terima kasih kepada semua pihak yang telah memberikan dukungan moral maupun teknis selama proses penelitian ini, dengan harapan hasil karya ilmiah ini dapat memberikan manfaat nyata bagi penguatan keamanan aplikasi web di berbagai instansi.

Daftar Pustaka

Ahmad, S., & Fitriani, D. (2022). Implementasi OSINT untuk pemetaan attack surface pada server pemerintah. *Jurnal Keamanan Informasi Nasional*, *4*(1), 22–34. https://ejournal.unhan.ac.id/index.php/pkn/article/view/1020

Akbar, I., Nur Isnaini, K., & Putranto, B. D. (2025). Penetration testing through NIST SP800-115 and OWASP Top 10 with risk analysis using CVSS on the XY Diskominfo website. *Journal of Innovation Information Technology and Application*, *3*(1), 45–55. https://journal.unesa.ac.id/index.php/jiita

Allo, A. K., & Widiasari, I. R. (2024). Analisis keamanan website SIASAT menggunakan teknik footprinting dan vulnerability scanning. *Jurnal Teknologi Informasi dan Komunikasi*, *8*(2), 316–323. https://doi.org/10.35870/jtik.v8i2.1723

Bazzell, M. (2022). Open source intelligence techniques: Resources for searching and analyzing online information (9th ed.). IntelTechniques. https://inteltechniques.com/

Brooks, C. J. (2021). Cybersecurity essentials. Wiley Publishing. https://www.wiley.com/

CISA. (2024). Mitigating risks in web infrastructure. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/resources-tools/

FIRST. (2023). *Common Vulnerability Scoring System v3.1: Specification document*. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v3.1/specification-document

Hidayat, T., et al. (2024). Risk assessment on government web application using CVSS framework.

Prosiding Seminar Nasional Informatika (SEMNASIF), *5*(1), 88–95. http://jurnal.upnyk.ac.id/index.php/semnasif

Kuehn, P., Relke, D. N., & Reuter, C. (2023). Common vulnerability scoring system prediction based on open source intelligence information sources. *Computers & Security*, *131*, 103286. https://doi.org/10.1016/j.cose.2023.103286

OWASP. (2021). *OWASP Top 10:2021 - The ten most critical web application security risks*. https://owasp.org/www-project-top-ten/

Pratama, Y. Y., Ramadhan, F., Albana, I., & Pratama, F. (2025). Analisis risiko keamanan website kompetisi nasional menggunakan metode vulnerability assessment dan CVSS 4.0. *Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science*, *7*(1), 12–20. https://journal.adpbi.or.id/index.php/JEEMIS

Putra, A., & Sari, M. (2023). Evaluasi kerentanan web menggunakan kerangka kerja CVSS v3.1. *Jurnal Sistem Informasi Terapan*, *9*(3), 210–225. https://jsi.cs.ui.ac.id/

Ramadan, M. (2023). Optimizing OSINT for cybersecurity reconnaissance. *Proceedings of the IEEE International Conference on Information Technology*, 302–309. https://ieeexplore.ieee.org/

Salsabila, B. P. (2025). *Analisis kerentanan dan penilaian risiko berbasis passive footprinting pada infrastruktur web publik* [Skripsi tidak dipublikasikan]. UPN "Veteran" Jawa Timur.

Sanjaya, R. (2024). Techniques of passive footprinting in modern web architecture. *In Proceedings of the International Conference on Cyber Security and Tech (ICCST)*, 145–152. https://iccst.org/

Stallings, W. (2023). Effective cybersecurity: A guide to help professionals and business managers establish a cybersecurity program. Addison-Wesley Professional.

Wijaya, K. (2022). *Analisis komparasi penilaian risiko keamanan menggunakan CVSS v3.0 dan v3.1 pada aplikasi e-government* [Tesis, Universitas Indonesia]. UI Library. https://lib.ui.ac.id/