ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

Analisis Kerentanan Keamanan Aplikasi Web pada Instansi Pemerintah X Menggunakan Pendekatan OWASP Top 10 dan Vulnerability Scanning Tools untuk Peningkatan *Web Security Awareness*

Belia Putri Salsabila

Jurusan Informatika, Universitas Pembangunan Nasional "Veteran" Jawa Timur

22081010311@student.upnjatim.ac.id

Abstrak*— Keamanan aplikasi web menjadi faktor penting dalam layanan digital pemerintahan karena sistem berbasis web sering mengelola data publik yang sensitif. Penelitian ini bertujuan untuk menganalisis kerentanan aplikasi web pada salah satu situs instansi pemerintah X menggunakan standar OWASP Top 10 Tahun 2021. Metode yang digunakan adalah black-box testing dengan bantuan OWASP ZAP untuk pemindaian aplikasi web dan Nessus untuk analisis konfigurasi server, serta didukung tahap reconnaissance melalui Nslookup, Whois, dan Wappalyzer. Setiap temuan dinilai menggunakan CVSS v3.1 untuk menentukan tingkat keparahan risiko. Hasil menunjukkan tidak terdapat kerentanan dengan tingkat *critical* maupun *high*, namun ditemukan beberapa risiko *medium* dan *low* terkait *Security Misconfiguration* dan *broken access control*, seperti absennya token CSRF dan kebijakan CSP yang belum optimal. Nilai CVSS berkisar antara 2.6 hingga 6.5, menandakan tingkat keamanan cukup baik namun tetap memerlukan peningkatan konfigurasi dan *web security awareness.

Kata Kunci— **OWASP Top 10, *Vulnerability Assessment, Web Security Awareness, Government Website*, Keamanan Aplikasi Web.**

I. PENDAHULUAN

Pemanfaatan aplikasi web pada instansi pemerintahan telah menjadi pilar utama dalam mendukung pelayanan publik yang efisien dan terintegrasi. Namun, penggunaan aplikasi web juga membawa risiko terhadap keamanan data karena sifatnya yang dapat diakses secara publik [1]. Berbagai insiden keamanan siber di sektor pemerintahan menunjukkan bahwa serangan dapat terjadi akibat konfigurasi server yang lemah, komponen perangkat lunak yang tidak diperbarui, atau rendahnya kesadaran keamanan dari pengelola sistem [2].

OWASP (*Open Web Application Security Project*) menyediakan standar OWASP Top 10, yang berisi daftar sepuluh risiko keamanan paling kritis pada aplikasi web [3]. Standar ini menjadi rujukan internasional dalam audit keamanan web, karena membantu organisasi memahami ancaman dan menetapkan prioritas pengamanan.

Selain itu, penggunaan alat pemindaian kerentanan seperti OWASP ZAP dan Nessus merupakan pendekatan efisien untuk melakukan identifikasi celah keamanan awal tanpa perlu melakukan eksploitasi langsung [4]–[5]. Dengan melakukan pemetaan hasil temuan terhadap kategori OWASP Top 10, instansi dapat memperoleh gambaran menyeluruh mengenai tingkat keamanan aplikasi web yang mereka kelola.

Penelitian ini difokuskan pada analisis dan klasifikasi kerentanan berdasarkan OWASP Top 10 pada situs web milik instansi pemerintah X. Tujuannya adalah untuk mendukung peningkatan *web security awareness* serta memberikan gambaran objektif mengenai kondisi keamanan aplikasi web pemerintah tanpa melibatkan proses eksploitasi aktif.

II. TEORI PENDUKUNG

A. *Keamanan Aplikasi Web*

Aplikasi web memiliki tingkat kerentanan tinggi karena Aplikasi web merupakan sistem yang sangat bergantung pada interaksi pengguna dan jaringan publik, sehingga memiliki tingkat paparan ancaman yang tinggi. Keamanan aplikasi web bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan (CIA) data terhadap akses tidak sah maupun gangguan eksternal [1]. Pada sektor pemerintahan, keamanan menjadi krusial karena aplikasi web sering memuat data pribadi dan administratif warga negara.

B. *OWASP Top 10 Tahun 2021*

OWASP Top 10 adalah daftar sepuluh risiko keamanan aplikasi web paling kritis yang dirilis oleh OWASP Foundation berdasarkan analisis data global [3]. Beberapa kategori yang sering muncul meliputi Broken Access Control, Cryptographic Failures, Security Misconfiguration, Vulnerable Components, dan Injection Attacks. Daftar ini tidak hanya menjadi acuan pengujian keamanan, namun juga berfungsi sebagai pedoman edukatif bagi pengembang dalam menerapkan praktik *secure coding* sejak tahap desain.

C. *Blackbox Testing*

Metode *black-box testing* adalah pendekatan pengujian keamanan tanpa akses ke kode sumber atau struktur internal sistem. Penguji hanya berinteraksi melalui antarmuka publik untuk mensimulasikan perilaku penyerang eksternal [7]. Pendekatan ini relevan digunakan dalam penelitian ini karena

ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

mencerminkan ancaman realistis terhadap sistem yang diakses publik, seperti situs web pemerintah.

D. Common Vulnerability Scoring System (CVSS)

CVSS merupakan standar internasional yang digunakan untuk mengukur tingkat keparahan suatu kerentanan keamanan. Sistem ini dikembangkan oleh *Forum of Incident Response and Security Teams* (FIRST) dan digunakan secara luas oleh lembaga keamanan serta *platform* keamanan siber global. Versi terbaru, CVSS v3.1, menilai kerentanan berdasarkan tiga metrik utama:

1) *Base Score*, menggambarkan tingkat keparahan mendasar (0–10).
2) *Temporal Score*, memperhitungkan faktor waktu, seperti ketersediaan eksploitasi.
3) *Environmental Score*, menyesuaikan dampak terhadap konteks lingkungan target [10].

Skor CVSS membantu peneliti dan pengembang menentukan prioritas penanganan kerentanan: nilai 0.1-3.9 tergolong *Low*, 4.0-6.9 *Medium*, 7.0-8.9 *High*, dan 9.0–10.0 *Critical*. Dalam penelitian ini, sistem CVSS digunakan untuk mengukur tingkat keparahan hasil pemindaian dari OWASP ZAP dan Nessus secara kuantitatif, sehingga penilaian lebih objektif dan terukur.

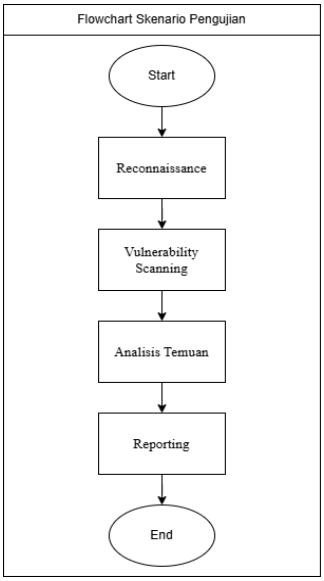
E. Web Security Awareness

Kesadaran keamanan atau *web security awareness* merupakan pemahaman pengembang dan administrator terhadap potensi ancaman siber serta penerapan kebijakan keamanan dalam siklus pengembangan sistem [6]. Meningkatkan kesadaran ini menjadi kunci utama dalam mencegah kesalahan konfigurasi dan mengurangi risiko kebocoran data pada sistem pemerintahan [9].

III. *METODOLOGI PENELITIAN*

Penelitian ini menggunakan pendekatan deskriptif dengan metode *vulnerability assessment* terhadap website instansi pemerintah X menggunakan pendekatan *black-box testing*, tanpa eksploitasi terhadap sistem dan hanya berfokus pada identifikasi serta klasifikasi kerentanan mengacu pada standar OWASP Top 10 tahun 2021 [3], [7]. Tujuan utama penelitian adalah memberikan gambaran tingkat risiko aplikasi web dan mendukung peningkatan *web security awareness* pengelola sistem [6].

Pada gambar 1, merupakan alur atau skenario pengujian. Pengujian dilakukan secara *non-intrusive,* yaitu hanya memanfaatkan informasi yang tersedia untuk publik dan interaksi standar layaknya pengguna umum, tanpa mengakses kode sumber atau kredensial internal. Pendekatan ini mencerminkan sudut pandang penyerang eksternal dan merupakan praktik umum pada proses *assessment* awal untuk sistem yang sedang beroperasi [9]. Tahapan pengujian terdiri dari:



Gambar 1. Skenario Pengujian.

1) *Reconnaissance*

Tahap ini bertujuan untuk mengidentifikasi teknologi, struktur, dan permukaan serangan (*attack surface*) dari website yang diuji. Proses dilakukan menggunakan teknik passive information gathering dan basic enumeration tanpa melakukan interaksi berlebihan terhadap sistem.

Pada tahap ini peneliti hanya menggunakan cara-cara yang aman dan bersifat pasif, seperti melihat informasi domain, server, dan halaman publik yang dapat diakses oleh semua pengguna. Hasil dari tahap ini berupa daftar teknologi, alamat website, dan halaman yang akan diperiksa pada tahap berikutnya.

2) *Vulnerability Scanning*

Pada tahap ini dilakukan pemindaian kerentanan (*automatic scanning tools*) untuk menemukan potensi kelemahan pada aplikasi web serta konfigurasi server. Proses dilakukan secara scripted scanning menggunakan dua alat utama:

a. OWASP ZAP digunakan untuk Untuk menemukan kerentanan aplikasi seperti header konfigurasi keamanan, parameter input, dan sesi pengguna, OWASP ZAP digunakan untuk *passive scanning* dan *limited active testing* [4].
b. Nessus digunakan untuk mengidentifikasi kerentanan server dan protokol jaringan, seperti port terbuka, konfigurasi TLS/SSL, serta kelemahan modul sistem [5].

Pemindaian dilakukan sesuai dengan *Rules of Engagement* (RoE) tanpa upaya untuk menjalankan muatan berbahaya, sehingga tidak menyebabkan gangguan atau perubahan pada sistem.

3) Analisis Temuan

Pada tahap ini dapat menjamin validitas dan mengurangi kemungkinan hasil *false positive*, setiap temuan dikonfirmasi

ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

secara manual. Setelah memetakan hasil ke OWASP Top 10 2021, tingkat risiko diukur menggunakan standar CVSS v3.1 yang mencakup nilai base score, impact, dan exploitability [3], [10]. Pada tahap ini, peneliti hanya menggunakan respons sistem untuk menentukan adanya kerentanan, daripada melakukan eksploitasi.

4) *Reporting*

Tahap ini peneliti membuat laporan dengan temuan penelitian dalam format tabel dan penjelasan singkat adalah langkah terakhir. Laporan tersebut akan mencakup daftar kerentanan, penilaian risiko berdasarkan CVSS, log atau screenshot, dan kategori OWASP Top 10 2021. Strategi ini sejalan dengan prosedur penilaian kerentanan kontemporer yang digunakan oleh lembaga pemerintah, yang memprioritaskan deteksi awal dan tindakan preventif terhadap potensi risiko keamanan siber[8].

IV. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan pada salah satu website layanan digital milik instansi pemerintah daerah. Proses pengujian mengikuti tahapan metodologi yang telah ditentukan, yaitu *reconnaissance*, *vulnerability scanning*, analisis temuan, dan pelaporan. Pengujian dilakukan tanpa akses langsung ke server dan tanpa eksploitasi aktif, sehingga hasil yang diperoleh murni berupa identifikasi indikator kerentanan dari sisi publik atau *black-box testing*.

A. Reconnaissance

Tahap *reconnaissance* dilakukan untuk mengidentifikasi teknologi dan komponen yang digunakan pada website target. Informasi dikumpulkan menggunakan teknik passive gathering seperti Nslookup, Whois, dan *technology fingerprinting* melalui Wappalyzer.

1) Nslookup

Nslookup digunakan untuk mengidentifikasi informasi DNS dari domain target penelitian.

Gambar 2. Hasil Nslookup

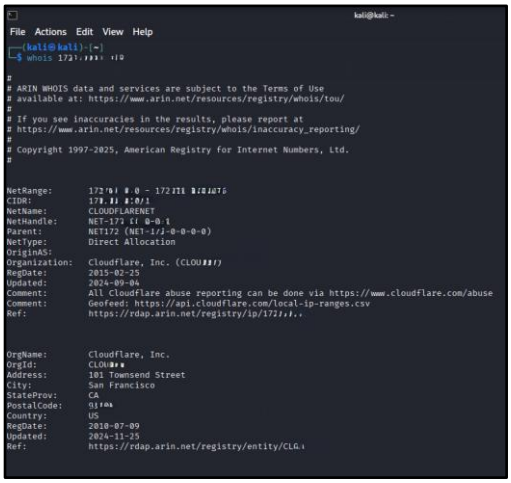
Dari hasil Nslookup pada gambar 2, diperoleh informasi bahwa:

a. Domain berhasil di-resolve dan terhubung ke dua alamat IP publik yang di-host oleh Cloudflare, Inc.
b. Sistem menggunakan layanan DNS berbasis cloud dengan revalidation time lima menit, menunjukkan konfigurasi DNS modern dan reliabel.
c. Infrastruktur memanfaatkan layanan Content Delivery Network (CDN) untuk mempercepat akses dan meningkatkan keamanan.

Hasil ini mengindikasikan bahwa situs instansi pemerintah tersebut menggunakan infrastruktur yang sudah terintegrasi dengan proteksi bawaan Cloudflare, seperti DDoS protection, traffic caching, dan web application firewall (WAF).

2) Whois

Detail jaringan dan informasi kepemilikan alamat IP domain target dapat ditemukan menggunakan whois.



Gambar 3. Hasil Whois.

Berdasarkan hasil Whois gambar 3, diperoleh informasi sebagai berikut:

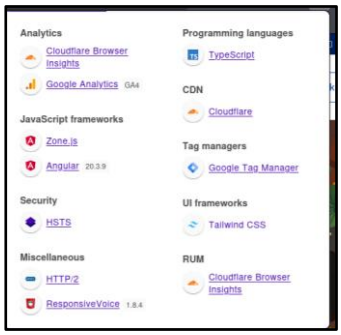
a. Alamat IP domain terdaftar di bawah penyedia layanan Cloudflare, Inc., yang berlokasi di San Francisco, Amerika Serikat.
b. Rentang jaringan yang digunakan termasuk dalam blok IP publik global dengan tipe alokasi Direct Allocation, menunjukkan bahwa domain menggunakan infrastruktur jaringan yang dikelola langsung oleh penyedia layanan internasional.
c. Informasi tambahan seperti abuse contact, organization ID, dan registry reference menunjukkan transparansi administrasi serta kepatuhan terhadap standar keamanan jaringan internasional (ARIN).

Hasil ini menunjukkan bahwa situs web instansi pemerintah memanfaatkan Cloudflare sebagai penyedia jaringan dan keamanan lapisan depan (edge network) untuk meningkatkan availability, latency, dan DDoS protection. Meskipun demikian, penggunaan layanan pihak ketiga perlu tetap diawasi agar tidak menimbulkan potensi kebocoran metadata atau kesalahan konfigurasi DNS publik.

ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

3) Wappalyzer

Wappalyzer digunakan untuk mengidentifikasi teknologi yang digunakan oleh website yang menjadi objek penelitian. Proses ini membantu memahami arsitektur aplikasi, framework, serta layanan pihak ketiga yang berpotensi memengaruhi keamanan sistem.



Gambar 4. Hasil Wappalyzer.

Berdasarkan hasil analisis pada Gambar 4, situs web tersebut menggunakan sejumlah teknologi modern, antara lain:

a. Angular (v20.3.9) dan TypeScript sebagai frontend framework utama yang mendukung pengembangan berbasis komponen dinamis.
b. Tailwind CSS sebagai UI framework yang mempercepat pembuatan antarmuka, namun perlu perhatian terhadap sanitasi inline style agar tidak membuka potensi cross-site scripting (XSS).
c. Cloudflare CDN digunakan untuk distribusi konten, optimasi performa, dan perlindungan terhadap serangan DDoS.
d. HSTS dan HTTP/2 diimplementasikan untuk memastikan koneksi terenkripsi serta mempercepat komunikasi antara klien dan server.
e. Google Analytics dan Cloudflare Browser Insights digunakan untuk pemantauan lalu lintas dan kinerja situs.
f. Google Tag Manager membantu dalam pengelolaan skrip analitik, namun apabila tidak dikonfigurasi dengan benar dapat menjadi vektor injeksi skrip eksternal.

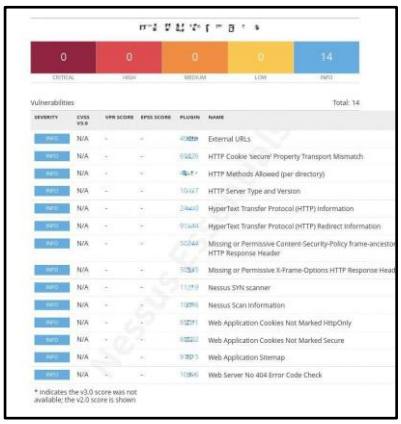
Dari hasil tersebut, dapat disimpulkan bahwa situs web instansi pemerintah ini menggunakan infrastruktur yang cukup modern dan aman. Namun, integrasi berbagai layanan pihak ketiga seperti Cloudflare dan Google Analytics perlu dikonfigurasi dengan hati-hati agar tidak membuka risiko kebocoran data atau security misconfiguration.

B. *Vulnerability Scanning*

Tahap ini bertujuan untuk mendeteksi potensi kelemahan keamanan pada aplikasi web dan konfigurasi server menggunakan alat vulnerability assessment otomatis tanpa melakukan eksploitasi langsung terhadap sistem. Dua alat utama yang digunakan adalah OWASP ZAP dan Nessus, yang masing-masing berfokus pada lapisan aplikasi web dan konfigurasi jaringan/server.

1) Nessus

Nessus bekerja dengan cara melakukan analisis otomatis terhadap respons sistem, memeriksa paket layanan, protokol komunikasi, dan konfigurasi jaringan, lalu memberikan klasifikasi tingkat risiko berdasarkan standar seperti CVSS (*Common Vulnerability Scoring System*).



Gambar 5. Hasil Nessus.

Dari Gambar 5 terlihat bahwa Nessus berhasil mengidentifikasi 14 temuan dengan tingkat risiko informational. Temuan tersebut menunjukkan adanya beberapa konfigurasi dan header keamanan yang belum optimal, di antaranya:

a. Header keamanan seperti Content-Security-Policy dan X-Frame-Options belum diterapkan, sehingga berpotensi membuka celah terhadap serangan seperti clickjacking dan cross-site scripting (XSS).
b. Cookie pada aplikasi web belum memiliki atribut Secure dan HttpOnly, yang dapat meningkatkan risiko pencurian sesi melalui koneksi tidak terenkripsi.
c. Server masih menampilkan informasi detail seperti HTTP Server Type dan Version, serta HTTP Methods yang diizinkan, yang dapat dimanfaatkan penyerang untuk melakukan fingerprinting.
d. Terdapat informasi tambahan seperti external URLs, HTTP redirect, dan web sitemap yang dapat memberikan gambaran struktur aplikasi kepada pihak luar.

Secara keseluruhan, hasil pemindaian Nessus menunjukkan bahwa konfigurasi keamanan situs masih perlu diperkuat pada sisi header HTTP dan

ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

manajemen cookie, meskipun belum ditemukan kerentanan yang bersifat kritis atau berpotensi langsung dieksploitasi.

2) OWASP ZAP

OWASP Zed Attack Proxy (ZAP) dirancang untuk membantu profesional keamanan dan pengembang dalam mengidentifikasi kelemahan keamanan.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	9
Low	9
Informational	8

Gambar 6. Summary Alert OWASP ZAP.

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	4
CSP: Failure to Define Directive with No Fallback	Medium	14
CSP: Wildcard Directive	Medium	14
CSP: script-src unsafe-eval	Medium	13
CSP: script-src unsafe-inline	Medium	1
CSP: style-src unsafe-inline	Medium	14
Content Security Policy (CSP) Header Not Set	Medium	6
Cross-Domain Misconfiguration	Medium	146
Missing Anti-clickjacking Header	Medium	3
CSP: Notices	Low	13
Cookie Without Secure Flag	Low	83
Cookie with SameSite Attribute None	Low	2
Cookie without SameSite Attribute	Low	85
Cross-Domain JavaScript Source File Inclusion	Low	8
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	31
Timestamp Disclosure - Unix	Low	72
X-Content-Type-Options Header Missing	Low	5
Information Disclosure - Sensitive Information in URL	Informational	2
Information Disclosure - Suspicious Comments	Informational	18
Loosely Scoped Cookie	Informational	2
Modern Web Application	Informational	4
Re-examine Cache-control Directives	Informational	33
Retrieved from Cache	Informational	8
Session Management Response Identified	Informational	68
User Controllable HTML Element Attribute (Potential XSS)	Informational	3

Gambar 7. Hasil OWASP ZAP.

Dari Gambar 6 dan 7 terlihat bahwa OWASP Zed Attack Proxy (ZAP) berhasil mengidentifikasi 26 temuan keamanan, terdiri dari 9 risiko tingkat medium, 9 risiko low, dan 8 bersifat informational.

Temuan dengan tingkat risiko medium umumnya berkaitan dengan penerapan kebijakan keamanan aplikasi yang belum optimal, seperti:

a. Tidak adanya token anti-CSRF (Cross-Site Request Forgery) pada form input, yang dapat memungkinkan serangan pemalsuan permintaan pengguna.
b. Header keamanan seperti Content-Security-Policy (CSP), X-Frame-Options, dan Strict-Transport-Security belum diterapkan dengan benar, sehingga berpotensi membuka celah terhadap serangan clickjacking dan cross-site scripting (XSS).
c. Ditemukan pula konfigurasi lintas domain (cross-domain misconfiguration) yang berisiko memperluas akses sumber daya antar domain tanpa pembatasan yang jelas.

Pada tingkat risiko low, ZAP mendeteksi bahwa cookie belum dilengkapi atribut keamanan Secure, HttpOnly, dan SameSite, serta belum diterapkannya beberapa header penting seperti Strict-Transport-Security dan X-Content-Type-Options. Hal ini menunjukkan masih adanya potensi penyadapan data pada lapisan transport dan risiko kebocoran informasi ringan.

Sementara itu, temuan pada kategori informational menunjukkan indikasi pengungkapan informasi sensitif, seperti komentar pada kode sumber HTML, URL yang memuat data penting, dan konfigurasi cache-control yang belum sesuai praktik terbaik.

C. Analisis Temuan dan Reporting

Tabel 1. Hasil Temuan dan Report.

No	Security Layer	Alat Bantu	Hasil Temuan	Skor Risiko	Tingkat Risiko	Kategori OWASP TOP 10	Rekomendasi Mitigasi
1	Reconnaissance – DNS & Infrastruktur	Nslookup, Whois	Domain menggunakan Cloudflare dengan DNS publik modern dan layanan CDN; proteksi DDoS & WAF aktif. Tidak ditemukan anomali DNS.	-	-	-	Lakukan pemantauan DNS & konfigurasi Cloudflare secara berkala untuk mencegah kesalahan publikasi atau kebocoran metadata.
2	Reconnaissance – Teknologi Web	Wappalyzer	Website menggunakan Angular, Tailwind CSS, TypeScript, Cloudflare CDN, dan Google Analytics. Potensi risiko pada integrasi skrip pihak ketiga.	-	-	-	Tinjau kembali integrasi pihak ketiga (Google Analytics/Tag Manager) agar tidak membuka potensi data leakage
3	Server Configuration & Header	Nessus	Header keamanan seperti CSP dan X-Frame-Options belum diterapkan; server menampilkan versi HTTP & metode yang diizinkan; cookie tanpa flag Secure/HttpOnly.	5.8	*Medium*	A05: Security Misconfiguration	Terapkan security headers (CSP, X-Frame-Options, X-Content-Type-Options), nonaktifkan informasi versi server, dan gunakan cookie Secure + HttpOnly.
4	Aplikasi Web	OWASP ZAP	Tidak terdapat token anti-CSRF; CSP menggunakan wildcard/unsafe-inline; X-Frame-Options & HSTS tidak diterapkan.	6.5	*Medium*	A01: Broken Access Control / A05: Security Misconfiguration	Implementasikan token anti-CSRF, perketat CSP (tanpa wildcard/unsafe-*), dan aktifkan X-Frame-Options & Strict-Transport-Security.
5	Cross-Domain & Scripting Policy	OWASP ZAP	Cross-domain misconfiguration ditemukan; sumber JS eksternal tidak dibatasi.	6.4	*Medium*	A08: Software and Data Integrity Failures	Terapkan whitelist domain pada konfigurasi CORS; batasi penanggalan JS eksternal dan gunakan integrity attribute.
6	Cookie & Session Management	OWASP ZAP	Cookie tanpa atribut Secure, HttpOnly, dan SameSite; berpotensi meningkatkan risiko hijacking dan CSRF.	3.4	*Low*	A02: Cryptographic Failures / A01: Broken Access Control	Implementasikan token anti-CSRF pada setiap form yang mengubah data pengguna
7	Information Disclosure	Nessus, OWASP ZAP	Server version disclosure, timestamp & sitemap masih terlihat di HTTP response.	2.8	*Low*	A06: Vulnerable Components	Sembunyikan metadata & versi server, nonaktifkan auto-indexing direktori, dan gunakan minimal response headers.

Berdasarkan hasil pada tabel 1, seluruh temuan memiliki skor CVSS antara 2.6 hingga 6.5, Skor CVSS ditentukan berdasarkan standar CVSS v3.1 [10] dan hasil pemindaian otomatis dari OWASP ZAP serta Nessus. Nilai tersebut merepresentasikan tingkat risiko relatif tanpa melakukan eksploitasi aktif terhadap sistem target. hasil menunjukkan tingkat risiko low hingga medium severity. Temuan terbanyak berasal dari kategori *Security Misconfiguration* (A05) dan *Broken Access Control* (A01), menandakan bahwa kelemahan utama website bukan berasal dari eksploitasi aktif, melainkan konfigurasi keamanan aplikasi dan server yang belum optimal.

ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025

Meskipun tidak ditemukan kerentanan critical atau high severity, temuan seperti ketiadaan token CSRF, CSP yang tidak ketat, serta cookie tanpa atribut keamanan berpotensi menjadi titik awal serangan *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), dan clickjacking apabila tidak segera dimitigasi.

Langkah mitigasi yang disarankan mencakup:

a. Mengaktifkan security headers (CSP, HSTS, X-Frame-Options, X-Content-Type-Options).
b. Menambahkan token anti-CSRF pada semua permintaan sensitif.
c. Mengamankan cookie dengan flag Secure, HttpOnly, dan SameSite.
d. Melakukan audit konfigurasi CORS dan skrip eksternal untuk membatasi akses antar domain.
e. Meninjau konfigurasi server dan DNS Cloudflare secara berkala.

V. KESIMPULAN

Penelitian ini telah melakukan analisis kerentanan keamanan aplikasi web pada salah satu situs instansi pemerintah X menggunakan metode external black-box testing dengan bantuan alat otomatis OWASP ZAP dan Nessus, serta didukung oleh analisis pasif menggunakan Nslookup, Whois, dan Wappalyzer.

Berdasarkan hasil pengujian, tidak ditemukan kerentanan dengan tingkat risiko critical maupun high. Namun, terdapat sejumlah temuan dengan tingkat risiko medium dan low, yang umumnya berkaitan dengan konfigurasi keamanan (security misconfiguration) dan pengendalian akses (broken access control). Beberapa kelemahan yang teridentifikasi meliputi ketiadaan token anti-CSRF, kebijakan Content Security Policy (CSP) yang belum optimal, cookie tanpa atribut keamanan (Secure, HttpOnly, SameSite), serta header HTTP seperti X-Frame-Options dan HSTS yang belum diterapkan. Nilai CVSS v3.1 dari temuan berkisar antara 2.6 hingga 6.5, yang menunjukkan bahwa tingkat risiko keseluruhan berada pada kategori low hingga medium severity. Kerentanan-kerentanan ini tidak secara langsung mengancam integritas atau ketersediaan sistem, namun berpotensi dimanfaatkan sebagai pintu masuk awal untuk serangan berbasis web seperti Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan Clickjacking apabila tidak segera dimitigasi.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa situs instansi pemerintah tersebut telah memiliki infrastruktur modern dan perlindungan jaringan yang baik melalui Cloudflare, namun masih memerlukan penyesuaian konfigurasi keamanan pada lapisan aplikasi web. Oleh karena itu, disarankan agar instansi terkait melakukan security hardening, penerapan kebijakan header keamanan yang ketat, serta pengujian kerentanan berkala mengacu pada panduan OWASP Top 10 2021. Langkah-langkah ini penting untuk menjaga keberlanjutan keamanan layanan digital dan meningkatkan web security awareness bagi pengembang maupun administrator sistem dalam menghadapi ancaman siber yang terus berkembang.

REFERENSI

[1] F. Cremer et al., “Cyber risk and cybersecurity: a systematic review of data and approaches,” Int. J. of Information Management, 2022.
[2] A. W. Kuncoro and F. Rahma, “Analisis Metode OWASP pada Pengujian Keamanan Website: Literature Review,” Automata, vol. 3, no. 1, 2022.
[3] OWASP Foundation, OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks, 2021.
[4] OWASP Foundation, Zed Attack Proxy (ZAP) Documentation – Getting Started / User Guide, 2022.
[5] Tenable Inc., Nessus Product Documentation, 2022.
[6] D. Rohmaniah et al., “Enhancing Website Security Using VAPT Based on OWASP Top Ten,” JAIC, vol. 9, no. 2, Apr. 2025.
[7] M. Althunayyan et al., “Evaluation of Black-Box Web Application Security Scanners,” Electronics, vol. 11, no. 13, 2022.
[8] H. Zhang et al., “ICVTest: A Practical Black-Box Penetration Testing Framework,” Applied Sciences, vol. 14, no. 1, 2024.
[9] M. A. Alzahrani and S. Alqahtani, “Web Application Vulnerabilities Assessment and Mitigation Using OWASP Top 10,” IJACSA, vol. 13, no. 8, 2022.
[10] S. Kumar and A. Kaur, “Risk-Based Vulnerability Assessment of Web Applications Using CVSS Metrics,” IEEE Access, vol. 9, 2021.
[11] H. J. Hong et al., “Automated Web Security Testing Framework Using OWASP ZAP,” J. of Information Security and Applications, vol. 75, 2023.