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

Vulnerability Assessment Web Instansi A Menggunakan OWASP ZAP, Nmap, dan Analisis Konfigurasi SSL/TLS

Moch Wahyu Sampurno Utomo

Informatika, Universitas Pembangunan Nasional "Veteran" Jawa Timur
22081010046@student.upnjatim.ac.id

***Abstrak*— Keamanan aplikasi web merupakan salah satu faktor utama dalam menjaga kerahasiaan, integritas, dan ketersediaan data organisasi. Penelitian ini bertujuan untuk melakukan Vulnerability Assessment (VA) terhadap web Instansi A (nama disamarkan) dengan menggunakan kombinasi OWASP ZAP, Nmap, serta analisis konfigurasi SSL/TLS. Penelitian dilakukan secara non-destruktif dan meliputi perencanaan ruang lingkup, pengumpulan informasi, pemindaian kerentanan menggunakan OWASP ZAP dan Nmap, serta pemeriksaan manual terhadap konfigurasi SSL/TLS, HTTP header, dan domain menggunakan curl, openssl, dan whois.**

Hasil pengujian menunjukkan adanya beberapa potensi kerentanan, seperti header keamanan yang belum diterapkan, cookie tanpa atribut keamanan tambahan, serta versi server yang terdeteksi masih menggunakan konfigurasi lama. Analisis sertifikat SSL menunjukkan bahwa web telah menggunakan enkripsi modern, namun masih perlu optimasi pada sisi konfigurasi keamanan HTTP. Penelitian ini menegaskan bahwa kombinasi antara tools otomatis dan analisis manual mampu memberikan hasil asesmen keamanan web yang komprehensif, efisien, dan sesuai standar OWASP.

Kata Kunci— **Vulnerability Assessment, Web Security, OWASP ZAP, Nmap, SSL/TLS, HTTP Header**

I. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah menjadikan aplikasi web sebagai fondasi utama dalam penyediaan layanan digital bagi masyarakat. Berbagai instansi, baik pemerintah maupun swasta, mengandalkan aplikasi web untuk mendukung proses bisnis, distribusi informasi, dan interaksi layanan publik. Namun demikian, peningkatan penggunaan teknologi web juga menimbulkan tantangan serius dalam aspek keamanan informasi. Serangan siber seperti *injection*, *cross-site scripting*, *session hijacking*, dan *security misconfiguration* terus berkembang dan menjadi ancaman nyata bagi sistem informasi modern [1]. Serangan yang menargetkan aplikasi web berpotensi menyebabkan kebocoran data sensitif, gangguan layanan, hingga kerusakan reputasi organisasi.

Penelitian terdahulu menunjukkan bahwa kerentanan aplikasi web masih menjadi salah satu faktor dominan dalam insiden keamanan siber. Oppenheim [2] menekankan pentingnya penerapan *Vulnerability Assessment* (VA) sebagai pendekatan sistematis untuk mengidentifikasi dan memitigasi risiko sebelum dapat dieksploitasi. Berbagai studi yang memanfaatkan OWASP ZAP membuktikan bahwa alat ini efektif untuk mendeteksi kelemahan pada sisi aplikasi, seperti kesalahan validasi input, konfigurasi header keamanan, serta kendali sesi pengguna [3]. Sementara itu, penelitian lain memanfaatkan Nmap untuk pemetaan port dan layanan aktif, yang terbukti mampu mengidentifikasi eksposur jaringan serta potensi serangan awal berbasis port scanning [5].

Namun begitu, sebagian besar penelitian sebelumnya fokus pada pemindaian otomatis dan belum menggabungkan evaluasi konfigurasi enkripsi transport-layer secara mendalam. Padahal, keamanan saluran komunikasi melalui mekanisme SSL/TLS merupakan elemen penting dalam melindungi data selama proses transmisi [6]. Selain itu, beberapa studi belum memadukan verifikasi manual untuk memvalidasi hasil pemindaian, sehingga potensi *false positive* tidak tereliminasi sepenuhnya. Kondisi ini membuka ruang penelitian untuk pendekatan yang lebih komprehensif, yang tidak hanya mengandalkan automasi, tetapi juga verifikasi teknis secara langsung.

Berdasarkan kesenjangan penelitian tersebut, penelitian ini dilakukan untuk mengevaluasi keamanan web pada Instansi A (nama disamarkan) melalui kombinasi alat otomatis dan pengujian manual. OWASP ZAP digunakan untuk memindai kerentanan pada lapisan aplikasi web, sedangkan Nmap berfungsi untuk mendeteksi layanan dan port aktif. Analisis SSL/TLS dengan OpenSSL dilakukan untuk memeriksa validitas sertifikat digital, konfigurasi cipher, dan tingkat kekuatan enkripsi, sementara curl dimanfaatkan untuk mengonfirmasi konfigurasi header HTTP secara langsung. Proses ini diperkaya dengan analisis Whois untuk memvalidasi informasi administratif domain.

Dengan pendekatan yang bersifat non-destruktif, penelitian ini diharapkan dapat memberikan gambaran yang lebih akurat dan mendalam mengenai postur keamanan aplikasi web, sekaligus menyajikan model asesmen yang dapat direplikasi pada instansi lain. Hasil penelitian diharapkan memberi kontribusi terhadap penguatan praktik keamanan aplikasi web dan peningkatan kesadaran organisasi dalam melakukan pemantauan keamanan secara berkala, sesuai dengan standar keamanan modern berbasis OWASP.

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

II. TEORI PENDUKUNG

A. *Vulnerability Assessment (VA)*

Vulnerability Assessment (VA) adalah suatu proses sistematis yang digunakan untuk mengidentifikasi, menganalisis, dan memetakan kelemahan keamanan pada sistem, jaringan, maupun aplikasi tanpa melakukan eksploitasi aktif [2].

Pendekatan ini menjadi langkah awal yang sangat penting dalam siklus keamanan informasi karena membantu organisasi mengenali potensi risiko sejak dini sebelum terjadi pelanggaran atau serangan nyata.

B. *OWASP Top 10 Tahun 2021*

Open Web Application Security Project (OWASP) adalah organisasi nirlaba yang berfokus pada peningkatan keamanan perangkat lunak. Salah satu kontribusi utamanya adalah publikasi OWASP Top 10, yaitu daftar sepuluh kategori kerentanan aplikasi web yang paling sering ditemukan secara global [3].

OWASP Top 10 berfungsi sebagai standar de facto bagi peneliti keamanan, pengembang, dan auditor untuk memahami risiko paling umum pada aplikasi web.

C. *OWASP ZAP (Zed Attack Proxy)*

OWASP ZAP merupakan *web application scanner open-source* yang dikembangkan oleh OWASP untuk mendeteksi potensi kerentanan seperti *Cross-Site Scripting (XSS)*, *SQL Injection (SQLi)*, dan kesalahan konfigurasi HTTP. ZAP juga memiliki fitur *spidering* dan *passive scanning* untuk analisis non-destruktif terhadap aplikasi web [4].

D. *Nmap (Network Mapper)*

Nmap digunakan untuk melakukan pemetaan jaringan dan deteksi layanan (service detection) pada server. Nmap membantu mengetahui port terbuka, versi layanan yang berjalan, dan potensi celah akibat konfigurasi jaringan yang lemah [5].

E. *CURL*

CURL adalah alat baris perintah sederhana namun kuat yang digunakan untuk memeriksa HTTP header dan parameter komunikasi antara server dan klien. Dengan *curl*, peneliti dapat memverifikasi keberadaan header keamanan seperti Content-Security-Policy dan X-Frame-Options, serta memeriksa atribut cookie [6].

F. *OPENSSL*

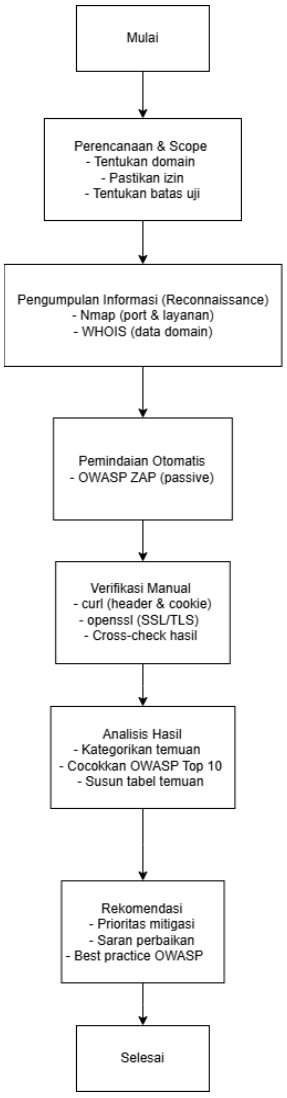
OPENSSL digunakan untuk menganalisis konfigurasi SSL/TLS, memeriksa validitas dan masa berlaku sertifikat, serta mengevaluasi dukungan protokol keamanan seperti TLS 1.2 atau TLS 1.3. Analisis ini penting untuk memastikan komunikasi data terenkripsi dengan aman [7].

G. *WHOIS*

WHOIS merupakan alat untuk memperoleh informasi registrasi domain, seperti tanggal pendaftaran, registrar, dan status privasi. Informasi ini berguna dalam tahap identifikasi awal dan konfirmasi kepemilikan domain yang diuji [8].

III. *METODOLOGI PENELITIAN*

Penelitian ini menggunakan pendekatan *Vulnerability Assessment* (VA) dengan metode non-destruktif, yaitu pengujian keamanan sistem tanpa melakukan eksploitasi aktif terhadap target. Pendekatan ini dipilih untuk memastikan proses analisis tidak menyebabkan gangguan layanan, kehilangan data, atau pelanggaran kebijakan keamanan dari pihak pemilik sistem.



gbr. 1 Flowchart

Metodologi penelitian terdiri dari beberapa tahap utama, mulai dari perencanaan hingga analisis hasil, yang dijelaskan secara rinci pada subbagian berikut.

A. *Perencanaan dan Penentuan Ruang Lingkup*

Tahapan pertama adalah perencanaan yang mencakup penentuan ruang lingkup (scope), waktu pelaksanaan, serta persetujuan etis dari pihak terkait. Objek penelitian adalah situs

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

web publik milik Instansi A (nama disamarkan) yang dipilih karena memiliki karakteristik sistem web dinamis dengan layanan berbasis HTTPS.

Langkah ini dilakukan untuk memastikan pengujian hanya mencakup komponen publik seperti domain utama, halaman web, serta endpoint yang dapat diakses oleh umum. Setiap aktivitas dilakukan secara terkontrol dan mematuhi prinsip *responsible disclosure*, sehingga tidak menimbulkan dampak negatif terhadap operasional sistem.

B. Pengumpulan Informasi (Reconnaissance)

Tahap kedua adalah pengumpulan informasi atau *reconnaissance*, yaitu proses awal dalam memahami karakteristik sistem yang akan diuji. Tahapan ini penting karena memberikan gambaran umum mengenai infrastruktur jaringan, layanan yang berjalan, serta teknologi yang digunakan pada server web. Dua alat utama digunakan pada tahap ini:

- Nmap (Network Mapper), Digunakan untuk melakukan pemindaian alamat IP dari domain target guna menemukan port terbuka, mendeteksi layanan yang aktif (seperti HTTP, HTTPS, SSH), serta mengidentifikasi versi perangkat lunak yang digunakan. Informasi ini membantu menentukan potensi celah keamanan di tingkat jaringan.
- WHOIS, Digunakan untuk memperoleh data registrasi domain, seperti registrar, organisasi pemilik, masa berlaku, serta detail DNS. Data tersebut berguna untuk memverifikasi legalitas domain dan memetakan hubungan infrastruktur jaringan yang digunakan.

Hasil dari tahap reconnaissance disusun dalam bentuk ringkasan struktur teknis target yang kemudian menjadi dasar untuk tahap pemindaian kerentanan berikutnya.

C. Pemindaian Otomatis (Automated Scanning)

Tahap ketiga merupakan inti dari proses Vulnerability Assessment, yaitu pemindaian otomatis terhadap komponen web aplikasi. Pada tahap ini digunakan OWASP ZAP sebagai alat utama karena bersifat open-source dan mendukung berbagai metode analisis tanpa perlu melakukan serangan destruktif.

OWASP ZAP beroperasi dalam mode passive scanning, di mana tool akan memantau lalu lintas HTTP/HTTPS antara klien dan server tanpa mengubah data atau mengirim payload berbahaya. Fitur utama yang digunakan meliputi:

- Spidering, untuk menelusuri seluruh halaman dan endpoint pada situs target,
- Passive Scan Rules, untuk mendeteksi kesalahan konfigurasi umum seperti ketiadaan *security header*, cookie tanpa atribut keamanan, atau penggunaan konten campuran (*mixed content*).

Hasil pemindaian otomatis disimpan dalam bentuk laporan (*scan report*) yang kemudian diverifikasi secara manual untuk memastikan keakuratan data.

D. Pemeriksaan Manual (Manual Verification)

Tahapan selanjutnya adalah pemeriksaan manual untuk memastikan hasil pemindaian otomatis benar-benar valid dan relevan dengan kondisi sistem. Tahap ini penting karena scanner otomatis sering kali menghasilkan *false positive* temuan yang tidak benar-benar berbahaya namun terdeteksi sebagai anomali. Beberapa alat digunakan dalam proses ini:

- curl, digunakan untuk melakukan permintaan HTTP secara langsung dan memeriksa tanggapan dari server. Dengan perintah ini, peneliti dapat meninjau *response header* untuk melihat keberadaan elemen keamanan seperti Content-Security-Policy, Set-Cookie, dan Server. Pemeriksaan ini juga membantu memastikan apakah situs sudah menggunakan HTTPS secara konsisten.
- openssl, digunakan untuk menganalisis konfigurasi SSL/TLS. Melalui alat ini, dapat diketahui versi protokol TLS yang didukung, jenis cipher suite yang digunakan, serta validitas dan masa berlaku sertifikat digital. Hasil dari pemeriksaan ini menjadi indikator kekuatan enkripsi dan kepatuhan terhadap praktik keamanan komunikasi data.

Kombinasi antara hasil otomatis dan manual ini memberikan gambaran yang lebih komprehensif terhadap kondisi keamanan web, baik di sisi aplikasi maupun lapisan transport (jaringan).

E. Analisis Hasil dan Rekomendasi

Tahap terakhir adalah analisis dan interpretasi hasil pengujian. Semua hasil dari proses pemindaian dan verifikasi manual dikompilasi menjadi tabel hasil pengujian yang berisi:

1) *Tool* yang digunakan,
2) Informasi atau jenis temuan,
3) Potensi dampak terhadap sistem, dan
4) Rekomendasi perbaikan.

Analisis dilakukan dengan membandingkan hasil temuan terhadap standar OWASP Top 10 untuk menentukan klasifikasi kerentanan dan tingkat risikonya. Rekomendasi yang diberikan disusun berdasarkan prinsip prioritas mitigasi, yaitu menekankan perbaikan pada temuan dengan tingkat risiko tertinggi terlebih dahulu.

Hasil dari tahap ini tidak hanya memberikan daftar celah keamanan, tetapi juga menghasilkan strategi peningkatan keamanan berkelanjutan (continuous improvement) yang dapat diterapkan oleh Instansi A guna memperkuat postur keamanan aplikasinya.

IV. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pengujian yang dilakukan terhadap situs web milik Instansi A (nama disamarkan) menggunakan pendekatan *Vulnerability Assessment* (VA) non-destruktif. Tujuan utama dari tahap ini adalah mengevaluasi konfigurasi keamanan jaringan, aplikasi web, serta sertifikat SSL/TLS dan informasi domain untuk memperoleh gambaran menyeluruh mengenai postur keamanan sistem web yang diuji.

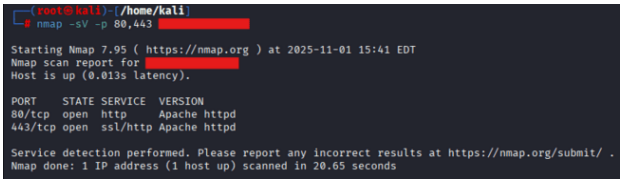
Proses pengujian dilakukan dengan kombinasi alat otomatis (OWASP ZAP dan Nmap) dan alat manual (curl, OpenSSL, dan Whois). Pendekatan ini memungkinkan identifikasi kelemahan dari berbagai lapisan mulai dari jaringan, aplikasi,

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

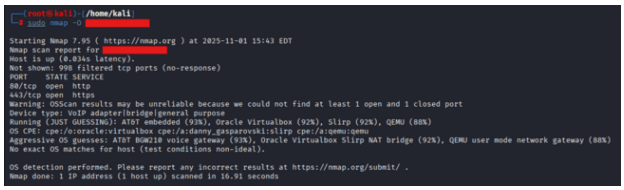
hingga manajemen identitas digital tanpa menyebabkan gangguan pada layanan.

A. Identifikasi Port dan Layanan Aktif (Nmap)

Pengujian pertama dilakukan dengan menggunakan Nmap, sebuah *network scanner* yang bertujuan untuk mengidentifikasi port terbuka, layanan yang berjalan, serta sistem operasi yang digunakan pada server web Instansi A.



Gbr. 2 nmap



Gbr. 3 Hasil nmap

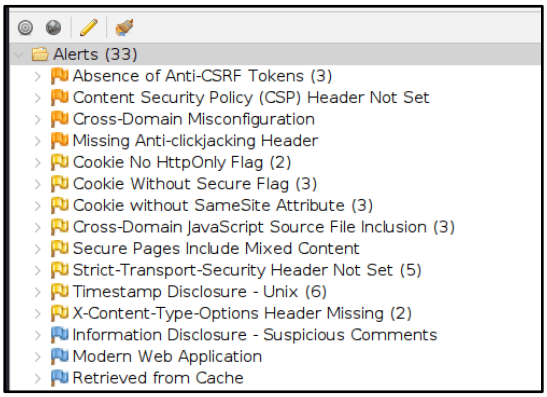
Dari gambar 1 dan 2 menunjukan hasil pengujian nmap sebagai berikut:

- Port 80 (HTTP) dan 443 (HTTPS) terdeteksi terbuka dan aktif digunakan untuk layanan web.
- Server menggunakan Apache HTTP Server versi 2.4.x yang berjalan pada lingkungan virtualisasi.
- Tidak ditemukan port lain yang terbuka, menunjukkan konfigurasi firewall cukup ketat.

Kondisi ini mengindikasikan bahwa lapisan jaringan telah dikonfigurasi dengan baik, namun versi server yang terdeteksi bukan versi terbaru. Hal ini dapat menjadi potensi risiko apabila terdapat kerentanan pada versi lama yang belum ditambal (*unpatched vulnerabilities*).

B. Evaluasi Keamanan Aplikasi Web (OWASP ZAP)

Selanjutnya dilakukan pengujian menggunakan OWASP ZAP (Zed Attack Proxy). Pengujian ini dilakukan dalam mode *passive scanning* untuk mendeteksi kelemahan konfigurasi tanpa mengirimkan payload eksploitasi.



Gbr. 4 OWASP ZAP

Dari gambar 3 menunjukan ZAP berhasil mengidentifikasi sejumlah temuan penting, antara lain:

- Header keamanan seperti Content-Security-Policy, X-Frame-Options, dan Strict-Transport-Security belum diterapkan.
- Terdapat cookie tanpa atribut keamanan seperti Secure dan HttpOnly.
- Ditemukan komentar internal dalam kode sumber HTML yang berpotensi membocorkan informasi sensitif.
- Form input tidak dilengkapi *token anti-CSRF*, yang membuka kemungkinan terjadinya serangan *Cross-Site Request Forgery*.

ZAP juga mendeteksi beberapa pustaka umum yang digunakan dalam situs, seperti *jQuery*, *Bootstrap*, dan *Font Awesome*, yang membantu proses analisis komponen aplikasi web. Sebagian besar temuan berasal dari konfigurasi keamanan yang belum optimal pada lapisan aplikasi. Ketiadaan header CSP dan X-Frame-Options dapat meningkatkan risiko serangan *clickjacking* dan *cross-site scripting (XSS)*, terutama jika halaman web mengizinkan pemuatan sumber eksternal.

C. Pemeriksaan Header dan Cookie (CURL)

Pengujian selanjutnya menggunakan curl bertujuan untuk meninjau secara langsung HTTP response header serta atribut keamanan pada cookie yang dikirim oleh server.

Gbr. 5 CURL

Dari gambar 4 menunjukan hasil pengujian curl dengan perintah dasar curl -s -D - -L https://[domain_instansi]/ -o /dev/null | sed -n '1,200p', diperoleh hasil sebagai berikut:

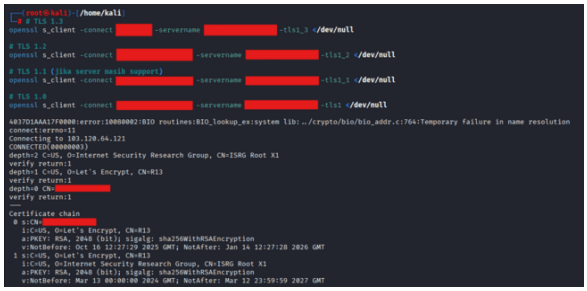
- Server melakukan pengalihan otomatis (redirect) dari HTTP ke HTTPS, menunjukkan penggunaan enkripsi sudah diterapkan secara default.
- Cookie sesi (PHPSESSID) hanya memiliki atribut HttpOnly, namun tidak disertai atribut Secure.
- Beberapa cookie tambahan terkait preferensi pengguna tidak memiliki flag keamanan (Secure, SameSite).

Ketiadaan atribut Secure memungkinkan cookie terkirim melalui koneksi yang tidak terenkripsi, sehingga meningkatkan risiko pencurian sesi (session hijacking) jika pengguna terhubung melalui jaringan publik.

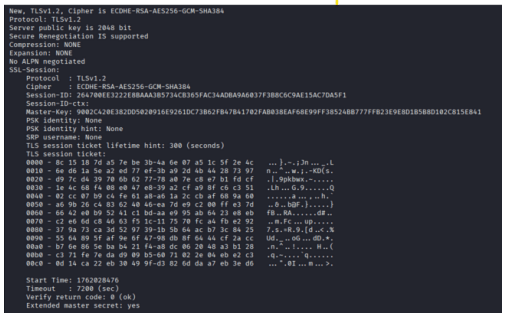
D. Pemeriksaan Sertifikat dan Konfigurasi SSL/TLS (OpenSSL)

Tahapan berikutnya menggunakan OpenSSL untuk memverifikasi konfigurasi SSL/TLS serta validitas sertifikat digital pada situs Instansi A.

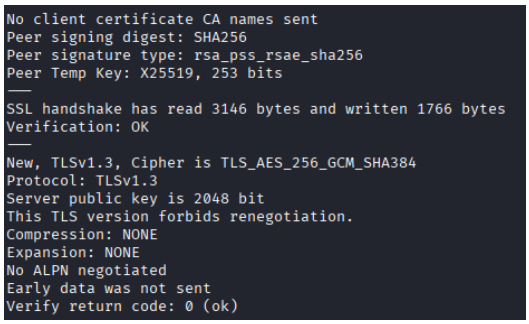
ISSN (Online) 2747-0563
Volume 5 No. 2 Tahun 2025



Gbr. 6 OpenSSL



Gbr. 7 Server Mendukung TLS



Gbr. 8 SHA 256

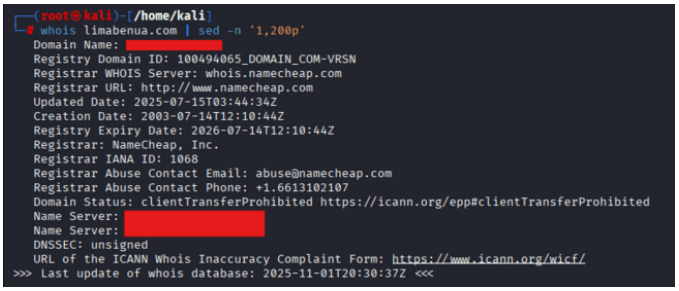
Dari gambar 5, 6 dan 7 menunjukan hasil pengujian dilakukan dengan perintah openssl s_client -connect [domain_instansi]:443 -servername https://[domain_instansi] -tls1_1 </dev/null dan hasil menunjukkan:

- Sertifikat diterbitkan oleh otoritas sertifikat terpercaya dan memiliki masa berlaku aktif.
- Server mendukung TLS 1.3 dan TLS 1.2, sementara versi lama seperti TLS 1.0 dan 1.1 telah dinonaktifkan.
- Cipher suite yang digunakan termasuk TLS_AES_256_GCM_SHA384, yang dianggap kuat dan sesuai standar keamanan modern.
- Panjang kunci enkripsi 2048-bit RSA dengan algoritma tanda tangan SHA256.

Hasil ini menunjukkan bahwa lapisan transport telah dikonfigurasi dengan baik dan mengikuti praktik keamanan terkini. Namun, pengujian juga menunjukkan belum adanya sistem pembaruan otomatis sertifikat (auto-renew) yang dapat menyebabkan sertifikat kadaluarsa jika tidak diawasi.

E. Pemeriksaan Informasi Domain (WHOIS)

Pengujian terakhir menggunakan WHOIS bertujuan untuk mengetahui status registrasi domain, masa aktif, serta perlindungan privasi pemilik domain.



Gbr. 9 WHOIS

Dari gambar 8 menunjukan hasil WHOIS sebagai berikut:

- Domain web Instansi A masih aktif dan dikelola melalui registrar resmi.
- Fitur perlindungan privasi WHOIS telah diaktifkan, sehingga informasi identitas pemilik domain tidak ditampilkan secara publik.
- Masa aktif domain masih panjang dan status administrasi "clientTransferProhibited" menunjukkan pencegahan pemindahan domain tanpa izin.

Hasil ini menunjukkan aspek manajemen domain sudah sesuai standar, dengan perlindungan data registrasi yang baik. Tidak ditemukan potensi penyalahgunaan informasi administratif.

F. Analisis dan Interpretasi Keseluruhan

No	Lapisan Keamanan	Tools Utama	Hasil Utama	Tingkat Risiko	Rekomendasi Utama
1	Jaringan	Nmap	Port 80 (HTTP) dan 443 (HTTPS) terbuka; firewall efektif, tidak ada port tambahan	Rendah	Perbarui versi Apache dan tutup port tidak digunakan
2	Aplikasi Web	OWASP ZAP, curl	Tidak ada header keamanan (CSP, HSTS, X-Frame-Options); cookie tanpa Secure & SameSite	Menengah	Tambahkan security header dan atur flag cookie dengan aman
3	Transport / Enkripsi	OpenSSL	TLS 1.3 aktif, cipher kuat, sertifikat valid	Rendah	Aktifkan auto-renew sertifikat dan nonaktifkan cipher lama
4	Identitas Domain	Whois	Domain aktif, perlindungan privasi WHOIS aktif, registrar resmi	Rendah	Pemantauan rutin masa berlaku domain

Gbr. 10 Tabel Hasil Analisis

Dari gambar 10 hasil analisis ini menunjukkan aspek manajemen domain sudah sesuai standar, dengan perlindungan data registrasi yang baik. Tidak ditemukan potensi penyalahgunaan informasi administratif.Berdasarkan hasil pengujian di atas, dapat disimpulkan bahwa konfigurasi keamanan web Instansi A secara umum cukup baik pada lapisan jaringan dan transport, tetapi masih terdapat kelemahan pada lapisan aplikasi yang perlu segera diperbaiki.

1) Lapisan Jaringan (Nmap): Server hanya membuka port penting (HTTP dan HTTPS), menandakan konfigurasi firewall efektif. Risiko rendah.
2) Lapisan Aplikasi (OWASP ZAP & curl): Tidak adanya header keamanan dan cookie tanpa atribut Secure serta SameSite menimbulkan risiko sedang terhadap serangan *XSS*, *clickjacking*, dan *session hijacking*. Risiko menengah.

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

3) Lapisan Transport (OpenSSL): Penggunaan TLS 1.3 dan cipher kuat menunjukkan tingkat keamanan tinggi. Risiko rendah.
4) Lapisan Identitas (Whois): Domain memiliki perlindungan privasi aktif dan status administratif aman. Risiko rendah.

Secara keseluruhan, hasil evaluasi menunjukkan tingkat risiko keseluruhan berada pada kategori menengah (medium risk). Fokus mitigasi diarahkan pada peningkatan konfigurasi keamanan aplikasi web, khususnya penerapan *HTTP Security Header* dan penguatan manajemen sesi pengguna. Pendekatan gabungan antara pemindaian otomatis dan verifikasi manual terbukti efektif dalam memberikan hasil yang komprehensif, akurat, dan tetap aman bagi sistem target.

V. KESIMPULAN

Penelitian ini berhasil melakukan evaluasi menyeluruh terhadap postur keamanan web Instansi A (nama disamarkan) menggunakan pendekatan *Vulnerability Assessment* berbasis kombinasi OWASP ZAP, Nmap, dan analisis SSL/TLS. Hasil pengujian menunjukkan bahwa lapisan jaringan dan transport telah memiliki konfigurasi yang cukup baik, dengan hanya port penting (HTTP dan HTTPS) yang terbuka serta penerapan enkripsi modern TLS 1.3 menggunakan cipher kuat. Hal ini menandakan penerapan keamanan jaringan yang efektif dan pengelolaan sertifikat digital yang sesuai standar.

Namun demikian, pada lapisan aplikasi masih ditemukan sejumlah kelemahan, terutama terkait ketiadaan header keamanan seperti Content-Security-Policy (CSP) dan X-Frame-Options, serta pengaturan cookie yang belum optimal karena tidak seluruhnya menggunakan atribut Secure, HttpOnly, dan SameSite. Kondisi ini dapat meningkatkan risiko terhadap serangan seperti Cross-Site Scripting (XSS), Clickjacking, dan Session Hijacking, yang pada akhirnya dapat mengancam kerahasiaan serta integritas data pengguna.

Pendekatan kombinasi antara tools otomatis dan verifikasi manual terbukti efektif dalam memberikan hasil asesmen yang komprehensif dan akurat, karena setiap temuan dari proses pemindaian otomatis dapat diverifikasi ulang untuk menghindari *false positive*. Metode ini juga bersifat non-destruktif, sehingga aman diterapkan tanpa mengganggu kinerja atau ketersediaan sistem yang diuji.

Secara keseluruhan, tingkat risiko keamanan web Instansi A berada pada kategori menengah (medium risk). Fokus perbaikan direkomendasikan pada peningkatan konfigurasi keamanan aplikasi web, khususnya melalui penerapan HTTP Security Header, penguatan manajemen sesi, dan pemeliharaan rutin terhadap sertifikat SSL/TLS.

Pendekatan ini dapat dijadikan model asesmen keamanan preventif bagi instansi lain, terutama dalam konteks peningkatan keamanan aplikasi web secara sistematis, terukur, dan sesuai dengan standar OWASP Top 10 serta praktik terbaik keamanan informasi.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Tim SANTIKA yang telah meluangkan waktu dan memberikan kontribusi dalam penyusunan serta penyediaan template jurnal ini. Dukungan tersebut sangat membantu dalam proses penulisan, penyusunan format, serta penyelarasan gaya penulisan agar sesuai dengan standar publikasi ilmiah.

Penulis juga berterima kasih kepada semua pihak yang telah memberikan dukungan moral dan teknis selama proses penelitian dan penyusunan karya ilmiah ini. Semoga hasil penelitian ini dapat memberikan manfaat bagi peningkatan kesadaran dan penerapan keamanan aplikasi web di berbagai instansi.

REFERENSI

[1] OWASP Foundation, *OWASP Top Ten 2021 – The Ten Most Critical Web Application Security Risks*, 2021.
[2] A. V. Oppenheim, *Vulnerability Assessment Methodology: An Overview*, SANS Institute, 2020.
[3] OWASP, *OWASP Testing Guide v5*, OWASP Foundation, 2023.
[4] OWASP, *Zed Attack Proxy (ZAP) User Guide*, 2023.
[5] G. Lyon, *Nmap Network Scanning*, Insecure.Org, 2009.
[6] OpenSSL Project, *OpenSSL User Guide*, 2024.
[7] Curl Project, *curl Command Line Tool Documentation*, 2024.
[8] ICANN, *WHOIS Protocol Specification*, RFC 3912, 2023