ANALISIS KOMPARATIF KEAMANAN WEBSITE POLRES ACEH JAYA DAN POLRES ACEH SELATAN MENGGUNAKAN INTEGRASI OWASP TOP 10 2025, NIST SP 800-115, DAN CVSS 4.0

TUGAS AKHIR

Diajukan oleh :

FITRI MULIYA

220705088

Mahasiswa Fakultas Sains dan Teknologi

Program Studi Teknologi Informasi

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI AR-RANIRY

BANDA ACEH

2026

LEMBAR PERSETUJUAN

ANALISIS KOMPARATIF KEAMANAN WEBSITE POLRES ACEH JAYA DAN POLRES ACEH SELATAN MENGGUNAKAN INTEGRASI OWASP TOP 10 2025, NIST SP 800-115, DAN CVSS 4.0

TUGAS AKHIR

Diajukan Kepada Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana (S1)
dalam Program Studi Teknologi Informasi

Oleh:
FITRI MULIYA
220705088
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

Disetujui Untuk Dimunaqasyahkan Oleh:

Pembimbing I,

Mulkan Fadhli, M.T
NIP. 198811282020121006

Pembimbing II,

Aulia Syarif Aziz, S.Kom., M.Sc
NIP. 199305212022031001

Mengetahui,
Ketua Program Studi Teknologi Informasi

Malahayati, M.T
NIP. 198301272015032003

LEMBAR PENGESAHAN

ANALISIS KOMPARATIF KEAMANAN WEBSITE POLRES ACEH JAYA DAN POLRES ACEH SELATAN MENGGUNAKAN INTEGRASI OWASP TOP 10 2025, NIST SP 800-115, DAN CVSS 4.0

TUGAS AKHIR

Telah Diuji Oleh Panitia Ujian Munaqasyah Tugas Akhir
Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus
Serta Diterima Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
Dalam Prodi Teknologi Informasi

Pada Hari/Tanggal: Senin, 11 Mei 2026
23 Dzulqaidah 1447 H
di Darussalam, Banda Aceh

Panitia Ujian Munaqasyah Tugas Akhir:

Ketua,	Sekretaris,
Mulkan Fadhli, M.T.	**Aulia Syarif Aziz, S.Kom., M.Sc**
NIP. 198811282020121006	**NIP. 199305212022031001**
Penguji I,	Penguji II,
Nazaruddin Ahmad, M.T.	**Dr. Hendri Ahmadian, M.I.M**
NIP. 198206052014031002	**NIP. 198301042014031002**

Mengetahui:
Dekan Fakultas Sains dan Teknologi
UIN Ar-Raniry Banda Aceh

Prof. Dr. Ir. Muhammad Dirhamsyah, M.T., IPU
NIP. 196210021988111001

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	: Fitri Muliya
NIM	: 220705088
Program Studi	: Teknologi Informasi
Fakultas	: Sains dan Teknologi
Judul	: Analisis Komparatif Keamanan Website Polres Aceh Jaya dan Polres Aceh Selatan Menggunakan OWASP TOP 10 2025, NIST SP 800-115, dan CVSS 4.0

Dengan ini menyatakan bahwa dalam penulisan tugas akhir, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;
4. Tidak memanipulasi dan memalsukan data;
5. Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh. Demikian pernyataan ini saya buat dengan sesungguhnya dan tanpa paksaan dari pihak manapun.

Banda Aceh, 12 Mei 2026

Yang Menyatakan

(Fitri Muliya)

ABSTRAK

Nama	: Fitri Muliya
NIM	: 220705088
Program Studi	: Teknologi Informasi
Fakultas	: Sains dan Teknologi (FST)
Judul	: Analisis Komparatif Keamanan Website Polres Aceh Jaya dan Polres Aceh Selatan Menggunakan OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0
Tanggal Sidang	: 11 Mei 2026 / 23 Zulkaidah 1447 H
Jumlah Halaman	: 83 Halaman
Pembimbing I	: Mulkan Fadhli, M.T.
Pembimbing II	: Aulia Syarif Aziz, S.Kom., M.Sc
Kata Kunci	: *OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, Keamanan Website, Polres Aceh*

Penelitian ini menganalisis keamanan website Polres Aceh Jaya dan Polres Aceh Selatan secara komparatif menggunakan OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0. Pengujian dilakukan secara black box eksternal dengan tools WhatWeb, Nmap, OWASP ZAP, dan Burp Suite, berdasarkan izin resmi dari Polda Aceh. Hasil pengujian menunjukkan website Aceh Jaya memiliki 36 peringatan ZAP dengan 15 jenis kerentanan yang didominasi Security Misconfiguration (A02), sedangkan website Aceh Selatan memiliki 16 peringatan dengan temuan paling kritis berupa PHP 7.4.33 End of Life (A03) dengan skor CVSS 4.0 sebesar 8,2 (High). Lima kerentanan lainnya berada pada tingkat Medium (skor 4,8–5,9). Rekomendasi prioritas mencakup upgrade PHP, pemasangan header keamanan, pengamanan cookie, penyempurnaan CSP, dan perbaikan HTML Injection.

Kata Kunci: *OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, Keamanan Website, Polres Aceh*

ABSTRACT

Nama	: Fitri Muliya
NIM	: 220705088
Program Studi	: Information Technology
Fakultas	: Science and Technology

Judul	: Comparative Analysis Of Website Security For Aceh Jaya Police And Aceh Selatan Police Using The Integration Of OWASP Top 10 2025, NIST SP 800-115, and CVSS 4.0
Tanggal Sidang	: 11 May 2026 / 23 Zulkaidah 1447 H
Jumlah Halaman	: 83 Pages
Pembimbing I	: Mulkan Fadhli, M.T.
Pembimbing II	: Aulia Syarif Aziz, S.Kom., M.Sc
Kata Kunci	: *OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, Website Security, Polres Aceh*

This study comparatively analyzes the security of the Polres Aceh Jaya and Polres Aceh Selatan websites using OWASP Top 10 2025, NIST SP 800-115, and CVSS 4.0. Testing was conducted through an external black box approach using WhatWeb, Nmap, OWASP ZAP, and Burp Suite, with official permission from Polda Aceh. Results showed the Aceh Jaya website had 36 ZAP alerts with 15 relevant vulnerabilities, predominantly Security Misconfiguration (A02), while the Aceh Selatan website had 16 alerts, with the most critical finding being PHP 7.4.33 End of Life (A03) scoring 8.2 (High) on the CVSS 4.0 scale. Five other vulnerabilities were classified as Medium (scores 4.8–5.9). Priority recommendations include upgrading PHP, implementing security headers, securing cookies, refining CSP, and fixing HTML Injection.

Keywords: *OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, Website Security, Polres Aceh*

KATA PENGANTAR

Segala puji dan rasa syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir dengan judul "Analisis Komparatif Keamanan Website Polres Aceh Jaya dan Polres Aceh Selatan Menggunakan Integrasi OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0" tepat pada waktunya.

Tugas akhir ini disusun sebagai salah satu persyaratan akademis dalam menempuh mata kuliah Skripsi pada Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Ar-Raniry Banda Aceh.

Penulis menyadari sepenuhnya bahwa tugas akhir ini masih memiliki banyak keterbatasan dan kekurangan, baik dari sisi isi, penyajian, maupun penulisan. Untuk itu, segala bentuk masukan, kritik, dan saran yang membangun sangat penulis harapkan guna penyempurnaan tugas akhir ini di kemudian hari.

Ucapan terima kasih yang tulus penulis sampaikan kepada semua pihak yang telah memberikan bantuan, arahan, dan dukungan selama proses penyusunan tugas akhir ini, terutama kepada:

1. Keluarga saya tercinta, terutama Ayah, Ibu, serta kakak dan adik yang selalu mendoakan, memberi semangat, dan menjadi motivasi utama dalam setiap langkah studi penulis.
2. Bapak Mulkan Fadhli, M.T., selaku dosen pembimbing l yang telah dengan sabar membimbing, mengarahkan, dan memberikan banyak ilmu serta masukan berharga selama penyusunan tugas akhir ini.
3. Bapak Aulia Syarif Aziz, S.Kom., M.Sc., selaku Pembimbing II yang telah memberikan arahan, masukan, serta dukungan yang sangat berarti dalam penyempurnaan tugas akhir ini
4. Kasubbid Tekinfo Polda Aceh, Bapak M. Siddiq Amrullah, S.Kom., serta seluruh jajaran Kepolisian Daerah Aceh bidang Teknologi Informasi dan Komunikasi, atas izin, kepercayaan, dan fasilitas yang diberikan sehingga penelitian ini dapat dilaksanakan.
5. Ibu Malahayati, M.T., selaku Ketua Program Studi Teknologi Informasi yang telah memberikan kesempatan dan dukungan akademis.

6. Bapak Khairan AR, M.Kom., selaku Sekretaris Program Studi Teknologi Informasi yang selalu membantu dalam hal administrasi dan pengembangan akademik.
7. Bapak Nazaruddin Ahmad, M.T., selaku dosen pembimbing akademik yang senantiasa membimbing dan memotivasi penulis sejak awal perkuliahan hingga sekarang.
8. Ibu Cut Ida Rahmadiana, S.Si., selaku staf Program Studi Teknologi Informasi yang telah dengan ramah membantu berbagai keperluan administrasi selama perkuliahan.
9. Seluruh staf dan pegawai Program Studi Teknologi Informasi yang telah memberikan layanan terbaik dan suasana akademik yang kondusif.
10. Sahabat-sahabat saya, Nadya Putri, Khairunnisak, Nabila Syakive, dan Lady Dwi Ulfa, atas kebersamaan, motivasi, dan dukungan yang selalu menyemangati penulis dalam setiap tahap studi.
11. Seluruh teman-teman angkatan 2022 Program Studi Teknologi Informasi yang telah berjuang bersama dan saling berbagi ilmu serta pengalaman selama masa perkuliahan.

Penulis berharap tugas akhir ini dapat memberikan manfaat, baik bagi pengembangan ilmu keamanan informasi maupun bagi peningkatan keamanan sistem informasi di instansi pemerintah. Semoga segala kebaikan semua pihak yang telah membantu mendapat balasan yang terbaik dari Allah SWT.

Banda Aceh, 16 April 2026
Penulis,

Fitri Muliya

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong hampir seluruh instansi pemerintah untuk memanfaatkan website sebagai media utama dalam penyampaian informasi dan pelayanan publik. Website instansi pemerintah berperan penting sebagai sarana komunikasi resmi, transparansi informasi, serta peningkatan kualitas layanan kepada masyarakat. Oleh karena itu, aspek keamanan website menjadi faktor yang sangat krusial untuk menjaga kepercayaan publik dan keberlangsungan layanan.

Seiring dengan meningkatnya penggunaan website, ancaman terhadap keamanan sistem informasi juga semakin kompleks. Website pemerintah sering menjadi target serangan siber, baik berupa peretasan (defacement), pencurian data, maupun gangguan layanan. Kondisi ini menunjukkan bahwa masih terdapat kelemahan atau celah keamanan pada sistem yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Apabila tidak ditangani dengan baik, kelemahan keamanan tersebut dapat berdampak pada kerugian institusi, menurunnya kredibilitas, serta terganggunya pelayanan kepada masyarakat.

Website Polres Aceh Jaya dengan domain tribratanews-resacehjaya.aceh.polri.go.id dan website Polres Aceh Selatan dengan domain tribratanewspolresacehselatan.com merupakan dua website resmi kepolisian di wilayah Aceh yang memiliki peran strategis dalam menyampaikan informasi terkait keamanan dan pelayanan kepolisian kepada masyarakat. Kedua website ini mewakili dua jenis domain yang berbeda, yaitu domain .go.id yang merupakan domain resmi instansi pemerintah dan domain .com yang bersifat komersial umum, namun keduanya tetap berfungsi sebagai media komunikasi publik. Hal ini menunjukkan perlunya dilakukan evaluasi dan analisis keamanan secara menyeluruh untuk mengetahui tingkat kerentanan yang ada pada kedua website tersebut.

Analisis keamanan website merupakan langkah preventif yang bertujuan untuk mengidentifikasi celah keamanan sebelum dimanfaatkan oleh penyerang. Salah

satu pendekatan yang dapat digunakan adalah dengan mengintegrasikan beberapa framework dan standar keamanan yang telah diakui secara internasional. Open Web Application Security Project (OWASP) Top 10 2025 menyediakan daftar kerentanan aplikasi web yang paling umum dan berisiko tinggi. Sementara itu, NIST Special Publication 800-115 memberikan panduan teknis dalam melakukan pengujian keamanan sistem informasi secara sistematis. Untuk menilai tingkat keparahan risiko dari setiap kerentanan yang ditemukan, digunakan Common Vulnerability Scoring System (CVSS) 4.0 sebagai standar penilaian risiko terbaru.

Dengan mengintegrasikan framework OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0, analisis keamanan website dapat dilakukan secara lebih komprehensif, terstruktur, dan objektif. Pendekatan ini tidak hanya berfokus pada identifikasi kerentanan, tetapi juga memberikan penilaian tingkat risiko serta rekomendasi perbaikan yang dapat digunakan sebagai acuan dalam meningkatkan keamanan website. Dalam pelaksanaannya, penelitian ini menggunakan seperangkat tools pendukung yang terdiri dari WhatWeb untuk identifikasi teknologi website, Nmap untuk pemindaian port dan layanan, OWASP ZAP untuk pemindaian kerentanan otomatis, serta Burp Suite untuk validasi manual dan pengujian lebih mendalam.

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk menganalisis keamanan website Polres Aceh Jaya dan Polres Aceh Selatan secara komparatif menggunakan integrasi framework OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0. Pengujian keamanan dilakukan secara legal berdasarkan persetujuan resmi dari Polda Aceh sebagai upaya nyata dalam mendukung peningkatan keamanan sistem informasi instansi pemerintah. Hasil penelitian diharapkan dapat memberikan gambaran tingkat keamanan kedua website serta menjadi bahan evaluasi yang berguna bagi pengelola.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka rumusan masalah dalam penelitian ini disusun untuk memfokuskan arah dan tujuan penelitian. Rumusan masalah tersebut adalah sebagai berikut:

1. Apa saja jenis kerentanan keamanan yang terdapat pada website Polres Aceh Jaya dan Polres Aceh Selatan berdasarkan pengujian keamanan web menggunakan integrasi *framework* OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0?
2. Bagaimana tingkat risiko dari setiap kerentanan keamanan yang ditemukan pada kedua website tersebut berdasarkan penilaian CVSS 4.0 serta klasifikasi OWASP Top 10 2025?
3. Bagaimana rekomendasi perbaikan yang dapat diberikan untuk meningkatkan keamanan kedua website Polres tersebut berdasarkan hasil analisis yang dilakukan?

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah:

1. Mengidentifikasi jenis-jenis kerentanan keamanan yang terdapat pada website Polres Aceh Jaya dan Polres Aceh Selatan melalui proses analisis keamanan web menggunakan integrasi *framework* OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0.
2. Menilai tingkat risiko dari setiap kerentanan keamanan yang ditemukan pada kedua website tersebut berdasarkan penilaian CVSS 4.0 serta klasifikasi *framework* OWASP Top 10 2025.
3. Memberikan rekomendasi perbaikan yang dapat dijadikan acuan untuk meningkatkan keamanan kedua website Polres tersebut berdasarkan hasil analisis yang dilakukan.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis bagi berbagai pihak yang berkepentingan. Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat menambah wawasan dan pemahaman dalam bidang keamanan informasi, khususnya terkait analisis keamanan website instansi pemerintah. Selain itu, penelitian ini dapat menjadi rujukan akademik mengenai penerapan integrasi *framework* OWASP Top 10 2025, NIST SP 800-

115, dan CVSS 4.0 dalam melakukan analisis keamanan web secara terstruktur dan sistematis.

2. Manfaat Praktis

   a) Bagi Instansi Terkait

      Hasil penelitian ini diharapkan dapat memberikan gambaran mengenai kondisi keamanan website Polres Aceh Jaya dan Polres Aceh Selatan, termasuk jenis kerentanan dan tingkat risikonya, sehingga dapat digunakan sebagai bahan evaluasi dalam upaya peningkatan keamanan sistem.

   b) Bagi Akademisi dan Peneliti

      Penelitian ini dapat dijadikan sebagai referensi atau bahan rujukan bagi mahasiswa dan peneliti selanjutnya yang ingin melakukan penelitian di bidang keamanan website atau keamanan sistem informasi.

   c) Bagi Penulis

      Penelitian ini diharapkan dapat meningkatkan pemahaman serta keterampilan penulis dalam melakukan analisis keamanan website dan penerapan standar keamanan informasi yang diakui secara internasional.

1.5 Batasan Penelitian

Untuk menjaga agar penelitian ini tetap terfokus sesuai dengan tujuan yang telah ditetapkan, maka ditetapkan batasan penelitian sebagai ruang lingkup pembahasan sebagai berikut:

1. Objek penelitian dibatasi pada website resmi Polres Aceh Jaya (https://tribratanews-resacehjaya.aceh.polri.go.id) dan Polres Aceh Selatan (https://tribratanewspolresacehselatan.com) yang dapat diakses secara publik.
2. Penelitian difokuskan pada analisis keamanan aplikasi web, tidak mencakup keamanan jaringan secara mendalam, keamanan server fisik, maupun aspek sumber daya manusia.
3. Pengujian keamanan dilakukan dengan pendekatan *vulnerability assessment* menggunakan *tools* WhatWeb, Nmap, OWASP ZAP, dan Burp Suite.
4. Penelitian tidak melakukan eksploitasi aktif, perubahan data, maupun tindakan yang dapat mengganggu ketersediaan layanan website.

5. *Framework* yang digunakan dalam penelitian ini terbatas pada OWASP Top 10 2025 sebagai acuan klasifikasi kerentanan, NIST SP 800-115 sebagai panduan tahapan pengujian keamanan, dan CVSS 4.0 sebagai metode penilaian tingkat risiko.
6. *Tools* yang digunakan dibatasi pada WhatWeb untuk identifikasi teknologi website, Nmap untuk pemindaian *port* dan layanan, OWASP ZAP untuk pemindaian kerentanan otomatis, serta Burp Suite untuk validasi manual dan pengujian lebih mendalam.
7. Seluruh kegiatan pengujian dilakukan secara legal berdasarkan persetujuan dan ruang lingkup yang telah disetujui oleh Polda Aceh.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Sehubungan dengan penelitian yang akan dilakukan, diperlukan sejumlah referensi dan hasil penelitian terdahulu sebagai bahan acuan untuk memahami pendekatan, metode, serta hasil penelitian yang telah dilakukan sebelumnya. Penelitian terdahulu juga berfungsi sebagai dasar perbandingan agar penelitian ini memiliki arah yang jelas serta terhindar dari duplikasi penelitian. Oleh karena itu, pada bagian ini disajikan beberapa penelitian terdahulu yang relevan dengan topik analisis keamanan website.

Tabel 2.1 Penelitian Terdahulu

No	Penelitian (Tahun)	Fokus Penelitian	Metode / Framework	Temuan Utama
1	Anggraeni et al., 2022	Keamanan website institusi pendidikan	ISSAF, OWASP v4	Ditemukan kerentanan konfigurasi seperti robots.txt yang mengekspos sitemap dan komponen jQuery usang
2	Maherza et al., 2023	Pengujian keamanan website sekolah	NIST SP 800-115	Penerapan NIST mampu mengidentifikasi celah secara sistematis
3	Haeruddin et al., 2024	Analisis keamanan website institusi pendidikan	VA, OWASP ZAP	Ditemukan 11 kerentanan sedang–rendah beserta rekomendasi
4	Septiawan et al., 2022	Pengujian kerentanan aplikasi web	OWASP ZAP	OWASP ZAP efektif mendeteksi kerentanan umum
5	Khosiri et al., 2025	Analisis kerentanan website pendidikan	OWASP ZAP, Burp Suite, Nikto	Kombinasi scanner dan manual testing meningkatkan akurasi

6	Handaya & Islamadina, 2025	Pengujian penetrasi aplikasi web Polda Aceh	OWASP, NIST SP 800-115	Ditemukan kerentanan pada aplikasi web Sistem Evaluasi Data TIK Polda Aceh
7	Albalawi et al., 2023	Analisis kerentanan website	OWASP ZAP, Burp Suite, Nikto	Kombinasi automated dan manual testing meningkatkan akurasi
8	Salim, 2026	Assessment keamanan website institusi akademik	Nmap, OWASP ZAP, SQLMap	Nmap mempercepat identifikasi titik rentan di fase reconnaissance

Berdasarkan Tabel 2.1, dapat dianalisis bahwa penelitian-penelitian terdahulu menunjukkan beberapa pola dan temuan yang relevan dengan penelitian ini. Pertama, mayoritas penelitian menggunakan framework OWASP sebagai acuan utama, baik untuk klasifikasi kerentanan (Anggraeni et al., 2022) maupun sebagai tools pemindaian (Septiawan et al., 2022; Haeruddin et al., 2024). Kedua, penggunaan NIST SP 800-115 sebagai panduan metodologis terbukti efektif dalam memberikan struktur pengujian yang sistematis (Maherza et al., 2023; Handaya & Islamadina, 2025). Ketiga, kombinasi antara automated scanning (OWASP ZAP) dan manual testing (Burp Suite) secara konsisten menghasilkan deteksi kerentanan yang lebih akurat dengan minimal false positive (Khosiri et al., 2025; Albalawi et al., 2023). Keempat, penggunaan tools reconnaissance seperti Nmap pada fase awal pengujian terbukti mempercepat identifikasi titik rentan sebelum masuk ke pengujian yang lebih mendalam (Salim, 2026).

Namun, terdapat celah penelitian (*research gap*) yang dapat diidentifikasi. Belum ada penelitian terdahulu yang mengintegrasikan ketiga *framework* sekaligus (OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0) dalam konteks website kepolisian di Indonesia, khususnya pada website Polres Aceh Jaya dan Polres Aceh Selatan. Selain itu, penerapan CVSS 4.0 yang baru dirilis belum banyak digunakan dalam penelitian serupa di Indonesia.

Oleh karena itu, penelitian ini melanjutkan dan menyempurnakan penelitian terdahulu dengan mengintegrasikan tiga standar internasional (OWASP Top 10

2025, NIST SP 800-115, dan CVSS 4.0) dalam satu kerangka analisis yang koheren, serta menerapkan integrasi tersebut pada objek spesifik yaitu website Polres Aceh Jaya dan Polres Aceh Selatan sebagai representasi instansi kepolisian.

2.2 Keamanan Website

Keamanan *website* merupakan upaya untuk melindungi aplikasi *web* beserta data dan layanan yang disediakan agar terhindar dari ancaman, serangan, maupun akses yang tidak sah. *Website*, khususnya milik instansi pemerintah seperti kepolisian, memiliki peran penting sebagai media penyampaian informasi dan pelayanan publik sehingga harus dijaga kerahasiaan, keutuhan, dan ketersediaannya.

Keamanan *website* bertujuan untuk memastikan bahwa informasi yang disajikan tidak dapat diubah oleh pihak yang tidak berwenang, data pengguna terlindungi dari pencurian, serta layanan *website* tetap dapat diakses dengan baik oleh masyarakat. Apabila aspek keamanan tidak diperhatikan, *website* berpotensi mengalami berbagai serangan siber yang dapat merugikan instansi dan menurunkan kepercayaan publik.

Ancaman terhadap keamanan *website* dapat berasal dari berbagai teknik serangan, seperti eksploitasi celah keamanan pada aplikasi *web*, kesalahan konfigurasi sistem, lemahnya mekanisme autentikasi, maupun penggunaan perangkat lunak yang tidak diperbarui. Serangan tersebut dapat mengakibatkan kerusakan sistem, kebocoran data, hingga gangguan layanan.

Oleh karena itu, diperlukan analisis keamanan website secara berkala untuk mengidentifikasi potensi kerentanan yang ada. Analisis keamanan dilakukan sebagai langkah pencegahan agar celah keamanan dapat diketahui dan diperbaiki sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pendekatan analisis keamanan website umumnya mengacu pada standar dan framework keamanan yang telah diakui secara luas, sehingga hasil analisis bersifat sistematis dan dapat dipertanggungjawabkan.

Dalam konteks instansi kepolisian seperti Polres Aceh Jaya dan Polres Aceh Selatan, keamanan *website* tidak hanya melindungi aset digital, tetapi juga menjaga kredibilitas dan kepercayaan publik. Oleh karena itu, penelitian ini mengadopsi pendekatan analisis yang mengintegrasikan *framework* OWASP Top 10 2025 untuk

klasifikasi kerentanan, NIST SP 800-115 sebagai panduan teknis pengujian, dan CVSS 4.0 untuk penilaian tingkat risiko. Dengan demikian, analisis keamanan *website* dapat dilakukan secara terstruktur, terukur, dan sesuai dengan standar internasional..

2.3 Vulnerability Assessment dan Penetration Testing

Vulnerability assessment (VA) dan *penetration testing* (PT) adalah dua metode yang umum digunakan untuk menilai keamanan sebuah sistem, terutama aplikasi web. Meskipun sama-sama bertujuan menemukan kelemahan keamanan, cara kerja, tingkat kedalaman, dan hasil akhir dari kedua metode ini cukup berbeda. Untuk melihat perbedaannya secara langsung, berikut adalah tabel perbandingan yang merangkum poin-poin utamanya.

Tabel 2.2 Perbedaan Utama Vulnerability Assessment dan Penetration Testing

Aspek	Vulnerability Assessment (VA)	Penetration Testing (PT)
Tujuan Pokok	Mencari dan mendaftar semua kemungkinan celah keamanan yang ada di sistem	Mencoba menerobos sistem dengan meniru serangan sungguhan untuk menguji pertahanannya
Cara Pengerjaan	Lebih mengandalkan alat *scan* otomatis (seperti OWASP ZAP) yang bekerja berdasarkan daftar kerentanan yang sudah dikenal	Mengombinasikan alat dengan pendekatan manual dan cara pikir seorang penyerang untuk menemukan jalan masuk yang tak terduga
Tingkat Kedalaman	Cakupannya luas, bertujuan memindai semua area untuk mengumpulkan daftar kemungkinan celah sebanyak-banyaknya	Lebih mendalam, fokus mengeksplorasi beberapa celah terpilih hingga benar-benar bisa dimanfaatkan
Hasil Akhir	Laporan berupa daftar kerentanan yang sudah diberi nilai risiko (biasanya pakai CVSS) dan dilengkapi saran perbaikan	Laporan yang berisi bukti langkah-langkah peretasan yang berhasil, data yang bisa diakses, serta analisis dampak yang mungkin terjadi
Perumpamaan	Seperti *general check-up* di dokter, pakai alat untuk mendeteksi berbagai gejala penyakit	Seperti tindakan operasi simulasi, untuk menguji ketahanan tubuh terhadap prosedur tertentu

Penerapan dalam Penelitian Ini	Digunakan sebagai langkah utama untuk tahap awal pemindaian menyeluruh terhadap website	Digunakan dengan sangat hati-hati dan terbatas, hanya untuk memastikan kebenaran temuan penting tanpa merusak sistem

Berdasarkan Tabel 2.2, dapat diketahui bahwa vulnerability assessment (VA) adalah proses yang dilakukan secara sistematis untuk menemukan, mengelompokkan, dan menilai tingkat keparahan dari berbagai celah keamanan yang mungkin ada di dalam sistem. Proses ini banyak mengandalkan bantuan alat pemindaian otomatis seperti OWASP ZAP. VA tidak mencoba untuk membobol sistem, melainkan fokus pada pendeteksian dan pencatatan titik-titik lemah. Hasil dari proses ini berupa daftar kerentanan yang sudah diberi peringkat risiko, lengkap dengan rekomendasi teknis untuk memperbaikinya.

Pendekatan VA cocok digunakan sebagai langkah awal untuk mengevaluasi website kepolisian seperti Polres Aceh Jaya dan Polres Aceh Selatan.Sementara itu, *penetration testing* (PT) adalah metode yang mencoba meniru serangan sungguhan terhadap sistem. Tujuannya untuk mengetahui seberapa jauh sistem bisa ditembus dan seberapa efektif pertahanan yang sudah dibangun. PT membutuhkan pendekatan yang lebih mendalam dan sering melibatkan teknik manual. Dalam penelitian ini, PT dilakukan secara terbatas dan tidak merusak, di mana tindakan eksploitasi yang berisiko mengubah data atau mengganggu layanan akan dihindari. Hal ini penting untuk mematuhi etika penelitian dan menjaga keamanan website yang menjadi objek penelitian.

Dalam penelitian ini, kedua pendekatan tersebut digunakan secara bersamaan agar saling melengkapi. VA berperan sebagai tahap pencarian awal untuk mengumpulkan berbagai kemungkinan celah keamanan pada kedua website. Selanjutnya, dari daftar temuan VA, beberapa titik lemah yang tampaknya paling berisiko akan diverifikasi lebih lanjut dengan PT terbatas. Verifikasi ini bertujuan untuk memastikan bahwa temuan tersebut akurat dan bukan kesalahan deteksi (*false positive*). Dengan strategi gabungan ini, analisis keamanan yang dilakukan diharapkan lebih komprehensif dan bertanggung jawab.

Untuk menjalankan kedua pendekatan tersebut, penelitian ini menggunakan beberapa *tools*. *WhatWeb* digunakan untuk identifikasi teknologi website, *Nmap*

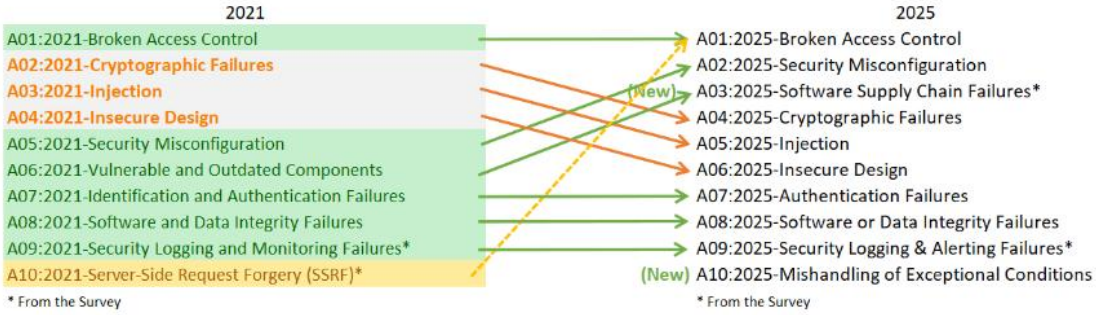
untuk pemindaian *port* dan layanan, OWASP ZAP sebagai alat utama *vulnerability assessment*, dan Burp Suite untuk validasi manual dan pengujian terbatas. Penggunaan kombinasi *tools* ini bertujuan agar proses pengujian bisa mencakup kecepatan dari pemindaian otomatis dan ketelitian dari analisis manual.

2.4 OWASP (Open Web Application Security Project)

OWASP (*Open Web Application Security Project*) merupakan organisasi nirlaba internasional yang berfokus pada peningkatan keamanan aplikasi web. OWASP menyediakan berbagai panduan, dokumentasi teknis, *tools*, serta standar terbuka yang dapat digunakan oleh pengembang, peneliti, maupun praktisi keamanan untuk meningkatkan keamanan aplikasi web. OWASP bersifat independen dan didukung oleh komunitas global, sehingga hasil dan rekomendasinya banyak dijadikan rujukan dalam penelitian akademik maupun praktik industri.

Salah satu kontribusi OWASP yang paling dikenal adalah OWASP Top 10 2025, yaitu daftar sepuluh jenis kerentanan keamanan aplikasi web yang paling sering ditemukan dan memiliki tingkat risiko tinggi. OWASP Top 10 2025 diperbarui secara berkala berdasarkan data insiden keamanan, laporan penelitian, serta kontribusi komunitas keamanan global. Pembaruan ini penting untuk memastikan daftar tersebut relevan dengan perkembangan ancaman yang terus berubah.

Untuk menggambarkan dinamika dan evolusi standar ini, Gambar 2.1 menampilkan diagram resmi dari OWASP *Foundation* yang membandingkan perubahan antara versi 2021 dan versi 2025. Diagram ini tidak hanya menunjukkan pergeseran peringkat, tetapi juga penyempurnaan kategori melalui visualisasi warna dan alur panah.



Gambar 2.1 OWASP Top 10
Sumber: OWASP Foundation (2025).

Berdasarkan Gambar 2.1 di atas menunjukkan pergeseran prioritas risiko keamanan aplikasi web. Warna pada setiap kategori membantu membedakan karakteristik risikonya, sementara perubahan warna dari satu versi ke versi lainnya menandakan adanya penyempurnaan definisi atau perubahan fokus. Panah yang menghubungkan kedua versi memperjelas pergerakan setiap kategori, seperti kenaikan peringkat, penggabungan, atau konsolidasi.

Berikut adalah ringkasan perubahan untuk semua 10 kategori pada OWASP Top 10 2025 dan relevansinya dengan penelitian ini:

1. **A01:2025 - *Broken Access Control***

   Tetap di peringkat #1. Ini menegaskan bahwa kesalahan kontrol akses adalah risiko terpenting yang harus diuji. Perubahan signifikan adalah masuknya *Server-Side Request Forgery* (SSRF) ke dalam kategori ini.

2. **A02:2025 - *Security Misconfiguration***

   Naik tajam dari #5 ke #2. Ini menunjukkan kesalahan konfigurasi menjadi masalah yang semakin kritis. Penelitian akan fokus memindai konfigurasi server dan aplikasi *website* Polres Aceh Jaya dan Polres Aceh Selatan.

3. **A03:2025 - *Software Supply Chain Failures***

   Adalah pengembangan dari kategori lama (*Vulnerable Components*). Kategori baru ini lebih luas, mencakup risiko dari seluruh rantai ketergantungan *software*. Penelitian akan memeriksa komponen pihak ketiga yang digunakan kedua *website*.

4. **A04:2025 - *Cryptographic Failures***

   Turun dari #2 ke #4. Meski turun, risiko kegagalan enkripsi yang menyebabkan kebocoran data tetap tinggi. Ini akan menjadi fokus pengujian.

5. **A05:2025 - *Injection***

   Turun dari #3 ke #5. Serangan injeksi (seperti SQL *Injection* dan XSS) tetap sangat umum dan berbahaya. *Tools* OWASP ZAP dan Burp Suite akan dioptimalkan untuk mendeteksi kerentanan jenis ini.

6. **A06:2025 - *Insecure Design***

   Turun dari #4 ke #6. Penurunan ini mengindikasikan industri mulai beralih ke desain yang lebih aman. Penelitian tetap akan mengidentifikasi kelemahan logika bisnis yang berasal dari desain.

7. **A07:2025 - *Authentication Failures***

   Tetap di #7, dengan penyempurnaan nama. Kelemahan manajemen sesi dan *login* tetap perlu diuji.

8. **A08:2025 - *Software or Data Integrity Failures***

   Tetap di #8. Risiko ini berfokus pada integritas kode dan data. Penelitian akan memeriksa mekanisme validasi dan keamanan *update* pada *website*.

9. **A09:2025 - *Security Logging & Alerting Failures***

   Tetap di #9, dengan penekanan baru pada fungsi peringatan (*alerting*). Penelitian akan mengevaluasi apakah *website* memiliki mekanisme pencatatan dan peringatan yang memadai.

10. **A10:2025 - *Mishandling of Exceptional Conditions***

    Adalah kategori baru di 2025. Ini berfokus pada penanganan *error* dan kondisi tak terduga yang salah. Pengujian akan mencoba memicu kondisi *error* untuk melihat respons sistem.

OWASP juga mengembangkan berbagai *tools* keamanan, salah satunya adalah OWASP ZAP yang digunakan dalam penelitian ini sebagai alat utama *vulnerability assessment*.

Dalam penelitian ini, OWASP Top 10 2025 digunakan sebagai acuan utama untuk mengklasifikasikan jenis kerentanan keamanan yang ditemukan pada *website* Polres Aceh Jaya dan Polres Aceh Selatan. Setiap temuan hasil pengujian keamanan

akan dipetakan ke dalam salah satu dari sepuluh kategori di atas. Dengan demikian, analisis dan pelaporan menjadi lebih terstruktur, memudahkan dalam penyusunan rekomendasi perbaikan yang terprioritaskan berdasarkan risiko tertinggi. Penggunaan standar OWASP dalam penelitian ini diharapkan dapat menghasilkan analisis keamanan *website* yang selaras dengan praktik internasional dan mudah dipahami oleh pihak pengelola sistem.

2.5 NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)

NIST SP 800-115 merupakan panduan teknis yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) sebagai acuan dalam pelaksanaan pengujian dan penilaian keamanan sistem informasi. Dokumen ini menyediakan kerangka kerja yang sistematis untuk membantu organisasi dalam mengidentifikasi, menganalisis, dan mengevaluasi kelemahan keamanan pada sistem informasi, termasuk aplikasi web.

Dalam penelitian ini, NIST SP 800-115 digunakan sebagai pedoman metodologis agar proses analisis keamanan website dilakukan secara terstruktur, terkontrol, dan sesuai dengan standar yang diakui secara internasional. Framework ini tidak hanya menekankan aspek teknis pengujian, tetapi juga mencakup tahapan perencanaan dan pelaporan hasil, sehingga mendukung pelaksanaan penelitian yang etis dan terdokumentasi dengan baik.

NIST SP 800-115 membagi proses pengujian keamanan ke dalam beberapa tahapan utama yang saling berkaitan. Tahapan-tahapan tersebut disajikan pada Tabel 2.3 berikut.

Tabel 2.3 Tahapan Pengujian Keamanan Berdasarkan NIST SP 800-115

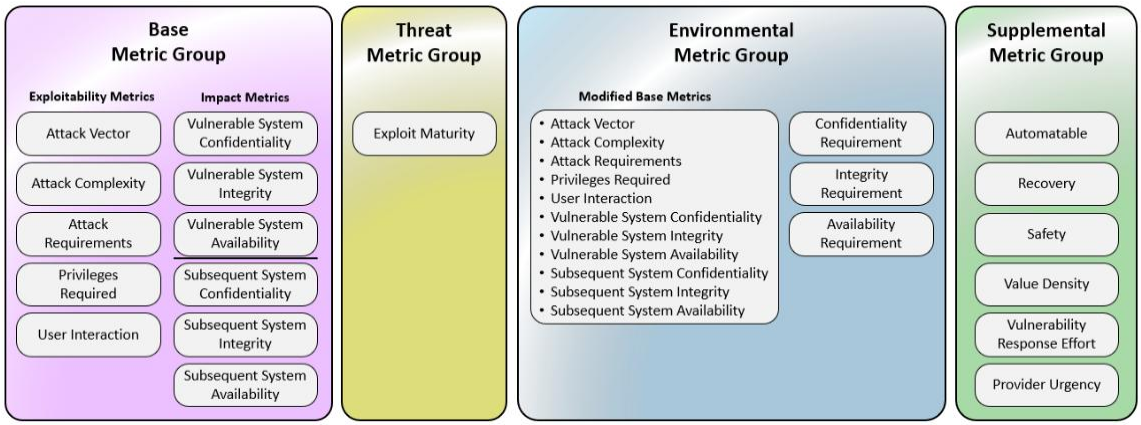
No	Tahapan	Deskripsi
1	*Planning* (Perencanaan)	Tahap awal untuk menentukan tujuan pengujian, ruang lingkup sistem yang diuji, metode yang digunakan, serta batasan dan aturan pengujian. Perencanaan dilakukan untuk memastikan pengujian berjalan terarah, aman, dan sesuai dengan izin yang diberikan.

2	*Discovery* (Pengumpulan Informasi)	Tahap pengumpulan informasi terkait sistem yang diuji, meliputi identifikasi teknologi, pemetaan aplikasi web, serta pencarian potensi kerentanan awal. Tahap ini bertujuan untuk memahami kondisi sistem sebelum dilakukan pengujian teknis.
3	*Attack* (Pengujian Kerentanan)	Tahap pengujian teknis terhadap kerentanan yang telah diidentifikasi untuk mengetahui tingkat keparahan dan dampaknya. Pengujian dilakukan secara terkendali sebagai simulasi serangan guna mengevaluasi efektivitas mekanisme keamanan sistem.
4	*Reporting* (Pelaporan)	Tahap dokumentasi seluruh hasil pengujian yang mencakup jenis kerentanan, tingkat risiko, serta rekomendasi perbaikan. Hasil pelaporan digunakan sebagai bahan evaluasi dan dasar pengambilan keputusan dalam peningkatan keamanan sistem.

Sebagaimana ditunjukkan pada Tabel 2.3, tahapan pengujian berdasarkan NIST SP 800-115 tersebut digunakan sebagai kerangka kerja pelaksanaan analisis keamanan *website* pada penelitian ini. Tahap *Discovery* dalam *framework* ini mendukung penggunaan *tools* seperti WhatWeb untuk identifikasi teknologi *website* dan Nmap untuk pemindaian *port* dan layanan. Sementara itu, tahap *Attack* sejalan dengan penggunaan OWASP ZAP untuk pemindaian otomatis dan Burp Suite untuk validasi manual kerentanan. *Framework* ini dikombinasikan dengan OWASP Top 10 2025 sebagai acuan klasifikasi kerentanan dan CVSS 4.0 sebagai metode penilaian tingkat risiko, sehingga menghasilkan analisis keamanan *website* yang lebih komprehensif dan sistematis pada *website* Polres Aceh Jaya dan Polres Aceh Selatan.

2.6 Common Vulnerability Scoring System (CVSS) 4.0

Common Vulnerability Scoring System (CVSS) merupakan standar terbuka yang digunakan untuk memberikan penilaian numerik (skor 0.0-10.0) terhadap tingkat keparahan suatu kerentanan keamanan. Dalam penelitian ini, CVSS 4.0 akan menjadi alat utama untuk mengukur dan memprioritaskan risiko dari setiap kerentanan yang ditemukan pada *website* Polres Aceh Jaya dan Polres Aceh Selatan. CVSS 4.0 menyempurnakan versi sebelumnya dengan struktur metrik yang lebih detail dan fleksibel, seperti yang diilustrasikan dalam gambar berikut.



Gambar 2.2 Kelompok Metrik CVSS 4.0 (CVSS Metric Groups)
Sumber: FIRST Organization (2023)

Berdasarkan Gambar 2.2, CVSS 4.0 mengorganisir penilaian risiko ke dalam empat kelompok metrik yang terstruktur secara hierarkis. Visualisasi ini menunjukkan alur penilaian yang dimulai dari analisis karakteristik dasar kerentanan, kemudian disesuaikan dengan faktor kontekstual untuk menghasilkan skor akhir yang lebih akurat dan relevan.

Base Metrics merupakan fondasi utama penilaian CVSS. Kelompok metrik ini mengukur karakteristik intrinsik sebuah kerentanan yang sifatnya tetap, terlepas dari waktu dan lingkungan pengguna. *Base Metrics* terbagi menjadi *Exploitability Metrics* yang menilai kemudahan dan cara eksploitasi, serta *Impact Metrics* yang mengukur dampak langsung terhadap kerahasiaan, integritas, dan ketersediaan data. Dalam penelitian ini, setiap kerentanan dari kedua *website* akan dinilai terlebih dahulu dengan metrik ini untuk mendapatkan skor dasar.

Supplemental Metrics berperan sebagai kelompok penjelas yang memberikan konteks tambahan terhadap kerentanan. Metrik ini mencakup aspek seperti dampak terhadap keselamatan (*Safety*), sifat kerentanan yang dapat diotomatisasi (*Automated*), atau kebutuhan pemulihan (*Recovery*). Meskipun tidak memengaruhi perhitungan skor akhir, informasi dari *Supplemental Metrics* sangat berharga untuk memberi prioritas tambahan dalam analisis.

Threat Metrics merepresentasikan lapisan penyesuaian dinamis berdasarkan keadaan ancaman aktual yang dapat berubah seiring waktu. Kelompok metrik ini menilai faktor seperti kematangan eksploit (*Exploit Maturity*), yaitu apakah sudah ada kode atau teknik eksploitasi yang beredar secara publik untuk kerentanan

tersebut. Dalam penelitian, kondisi ancaman terbaru untuk setiap kerentanan yang ditemukan akan diteliti guna menyesuaikan skor dengan situasi nyata.

Environmental Metrics merupakan kelompok penyesuaian akhir yang membuat skor CVSS lebih personal dan relevan dengan lingkungan spesifik pengguna. Metrik ini mempertimbangkan kondisi unik organisasi, seperti keberadaan kontrol keamanan yang dapat memitigasi serangan, serta nilai atau kepentingan kritis dari aset yang rentan. Untuk penelitian ini, *Environmental Metrics* akan disesuaikan dengan konteks Polres Aceh Jaya dan Polres Aceh Selatan sebagai *website* instansi kepolisian.

2.6.1 Tujuan Penggunaan CVSS 4.0 dalam Penelitian

Penggunaan CVSS 4.0 dalam penelitian ini bertujuan untuk:

1. Memberikan penilaian tingkat keparahan kerentanan secara objektif.
2. Membantu menentukan prioritas penanganan kerentanan keamanan.
3. Menyajikan hasil analisis risiko dalam bentuk yang terukur dan mudah dipahami.
4. Mendukung pengambilan keputusan dalam upaya peningkatan keamanan *website*.

2.6.2 Penerapan dan Alur Penilaian

Penerapan keempat kelompok metrik ini dalam konteks penelitian dirangkum dalam Tabel 2.4.

Tabel 2.4 Penerapan Kelompok Metrik CVSS 4.0 dalam Penelitian

Kelompok Metrik	**Fokus Penilaian**	**Contoh Penerapan untuk Analisis Website Polres Aceh Jaya dan Polres Aceh Selatan**
Base Metrics	Sifat tetap kerentanan (cara eksploitasi & dampak dasar)	Menganalisis apakah kerentanan bisa dieksploitasi dari jarak jauh (*Network*) dan apakah menyebabkan data korup (*High Integrity Impact*)
Threat Metrics	Keadaan ancaman aktual yang berubah waktu	Meneliti apakah ada laporan eksploit aktif di internet untuk jenis kerentanan yang ditemukan
Environmental Metrics	Kondisi khusus lingkungan kepolisian	Mempertimbangkan tingkat kepentingan website sebagai portal informasi publik kepolisian

Supplemental Metrics	Konteks tambahan (tidak memengaruhi skor)	Mencatat jika kerentanan berpotensi menyebabkan gangguan layanan yang panjang

2.6.3 Skala Keparahan dan Prioritas Tindakan

Skor akhir CVSS kemudian dipetakan ke dalam tingkat keparahan menggunakan Tabel 2.5. Tabel ini menjadi pedoman praktis untuk menentukan urgensi penanganan setiap kerentanan dalam rekomendasi akhir.

Tabel 2.5 Skala Tingkat Keparahan CVSS 4.0

Rentang Skor	Tingkat Keparahan	Keterangan
0.0	*None*	Tidak memiliki dampak keamanan yang signifikan
0.1 – 3.9	*Low*	Kerentanan berdampak rendah dan relatif sulit dimanfaatkan
4.0 – 6.9	*Medium*	Kerentanan berdampak sedang dan memerlukan perhatian pengelola sistem
7.0 – 8.9	*High*	Kerentanan berdampak tinggi dan berpotensi mengganggu sistem secara signifikan
9.0 – 10.0	*Critical*	Kerentanan sangat berbahaya dan memerlukan penanganan segera

Mengacu pada skala yang disajikan pada Tabel 2.5, tingkat keparahan kerentanan diklasifikasikan berdasarkan rentang skor CVSS 4.0 yang diperoleh dari hasil pengujian keamanan. Klasifikasi ini membagi kerentanan ke dalam beberapa tingkat keparahan, mulai dari kategori *none* hingga *critical*, sesuai dengan besarnya potensi dampak yang dapat ditimbulkan terhadap sistem. Pembagian tingkat keparahan tersebut digunakan sebagai dasar dalam menentukan prioritas penanganan kerentanan yang ditemukan.

2.6.4 Peran CVSS 4.0 dalam Analisis Keamanan Website

Dalam penelitian ini, CVSS 4.0 berperan sebagai alat pemberi skor dan penentu prioritas penanganan kerentanan. CVSS 4.0 menghubungkan temuan teknis dari pengujian dengan manajemen risiko yang terukur. Setiap kerentanan yang ditemukan pada website Polres Aceh Jaya dan Polres Aceh Selatan akan diberikan

skor numerik antara 0 hingga 10, sehingga tingkat keparahannya dapat diketahui secara objektif.

CVSS 4.0 melengkapi dua *framework* lainnya dalam penelitian ini. OWASP Top 10 2025 digunakan untuk mengklasifikasikan jenis kerentanan (misalnya *Injection* atau *Broken Access Control*), sementara NIST SP 800-115 menjadi panduan metodologis untuk menemukan kerentanan tersebut. Selanjutnya, CVSS 4.0 mengambil alih untuk menjawab pertanyaan "seberapa parah kerentanan ini dan kapan harus diperbaiki?"

Dengan integrasi ini, laporan akhir penelitian tidak hanya berisi daftar kerentanan, tetapi juga peta prioritas yang jelas dan dapat ditindaklanjuti. Contohnya, jika ditemukan kerentanan SQL Injection pada sebuah form login dengan skor CVSS 9,1 (kategori Critical), maka rekomendasi perbaikannya akan diberikan prioritas tinggi untuk segera ditangani. Pendekatan ini menjadikan analisis keamanan website lebih terstruktur, terukur, dan bermanfaat bagi pengelola sistem dalam mengambil keputusan.

2.7 Tools Pendukung dalam Pengujian Keamanan Web

Untuk mendukung proses pengujian keamanan website, penelitian ini menggunakan beberapa *tools* pendukung. Masing-masing *tools* memiliki fungsi yang berbeda dan saling melengkapi. Pemilihan *tools* didasarkan pada kebutuhan setiap tahap pengujian serta reputasinya sebagai alat standar dalam keamanan informasi.

Penggunaan kombinasi *tools* ini bertujuan agar proses pengujian dapat mencakup kecepatan dari pemindaian otomatis dan ketelitian dari analisis manual. Dengan pendekatan ini, hasil pengujian diharapkan lebih akurat dan komprehensif. Selain itu, setiap *tools* memiliki keunggulan spesifik yang tidak dimiliki oleh *tools* lainnya.

Secara garis besar, *tools* yang digunakan dalam penelitian ini terdiri dari WhatWeb untuk identifikasi teknologi, Nmap untuk pemindaian *port* dan layanan, OWASP ZAP untuk pemindaian kerentanan otomatis, serta Burp Suite untuk validasi manual dan pengujian lebih mendalam. Keempat *tools* ini diintegrasikan dalam alur pengujian berdasarkan kerangka NIST SP 800-115.

2.7.1 WhatWeb

WhatWeb adalah *tools open-source* yang digunakan untuk mengidentifikasi teknologi yang dipakai oleh sebuah *website*. *Tools* ini mampu mengenali berbagai komponen seperti *Content Management System* (CMS), *web server*, *framework*, hingga *plugin* dan tema yang terpasang. WhatWeb bekerja dengan mengirimkan permintaan HTTP ke server target lalu menganalisis respons yang diterima, seperti *header* HTTP, *cookie*, dan kode HTML.

Keunggulan utama *WhatWeb* terletak pada kemampuannya mengenali teknologi secara akurat dan cepat. *Tools* ini memiliki lebih dari 1.500 *plugin* yang dapat mendeteksi berbagai macam *software* dan aplikasi web. Selain itu, *WhatWeb* juga dapat melakukan *scanning* secara agresif atau pasif sesuai dengan kebutuhan pengujian.

Dalam penelitian ini, WhatWeb akan digunakan pada tahap awal (*Discovery Phase*) untuk mengetahui teknologi yang mendasari website Polres Aceh Jaya dan Polres Aceh Selatan. Informasi yang diperoleh, seperti jenis CMS, versi *web server*, dan komponen lainnya, menjadi dasar untuk menentukan strategi pengujian selanjutnya.

Dengan mengetahui teknologi yang digunakan sejak awal, pengujian dengan OWASP ZAP dan Burp Suite dapat lebih terarah. Peneliti dapat fokus pada kerentanan yang sering muncul pada teknologi tertentu, sehingga proses pengujian menjadi lebih efisien dan hasilnya lebih akurat.

2.7.2 Nmap (Network Mapper)

Nmap (*Network Mapper*) adalah *tools open-source* yang sangat populer untuk pemetaan jaringan dan audit keamanan. *Tools* ini pertama kali dirilis pada tahun 1997 dan hingga kini masih menjadi alat standar bagi para profesional keamanan siber. Kekuatan utama Nmap terletak pada kemampuannya untuk melihat dan memahami apa saja yang ada di dalam sebuah jaringan dengan detail yang tinggi.

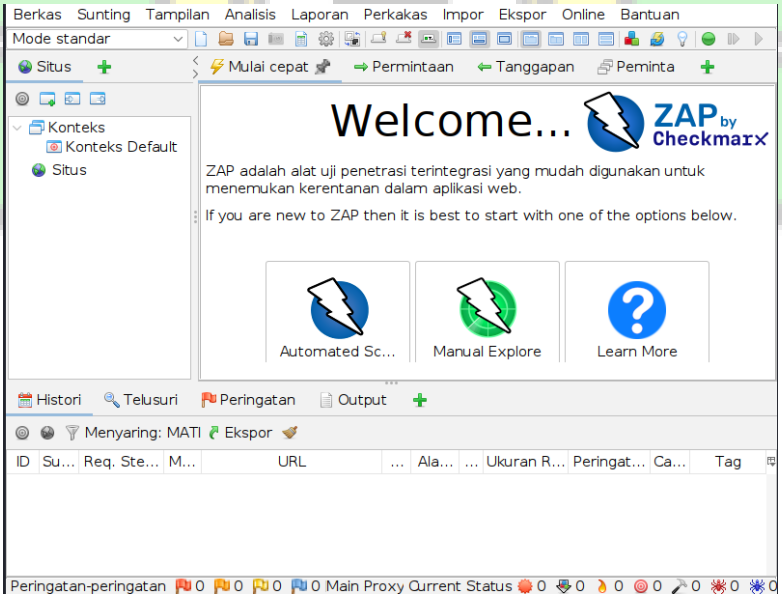
Secara teknis, Nmap bekerja dengan mengirimkan paket-paket khusus ke alamat target (misalnya alamat IP website) dan menganalisis respons yang diterima. Dari sini, Nmap dapat mendeteksi *host* (perangkat) yang aktif, mendaftar *port-port* jaringan mana yang terbuka, serta mengidentifikasi layanan (*service*) dan versi perangkat lunak yang berjalan di balik *port* tersebut.

Dalam penelitian ini, Nmap akan digunakan pada fase awal (*Discovery Phase*). Sebelum melakukan pengujian kerentanan aplikasi web pada website Polres Aceh Jaya dan Polres Aceh Selatan, perlu diketahui "pintu-pintu" (*port*) dan "ruangan" (*service*) apa saja yang tersedia pada server target. Informasi ini menjadi peta awal yang sangat berharga untuk memfokuskan pengujian dengan *tools* lain secara lebih efisien.

Data yang dikumpulkan Nmap akan menjadi landasan strategis untuk langkah pengujian selanjutnya. Selain itu, pola respons dari pemindaian Nmap juga dapat memberikan petunjuk tentang konfigurasi *firewall* atau mekanisme keamanan jaringan yang diterapkan oleh pihak pengelola website. Dengan demikian, pengujian dapat disesuaikan agar tetap sesuai dengan ruang lingkup dan etika penelitian.

2.7.3 OWASP ZAP (Zed Attack Proxy)

OWASP ZAP (Zed Attack Proxy) merupakan alat utama yang digunakan dalam penelitian ini untuk melakukan *automated vulnerability assessment*. *Tool* ini dikembangkan oleh komunitas OWASP dan secara khusus dirancang untuk menemukan kerentanan keamanan pada aplikasi web.



Gambar 2.3 Antarmuka OWASP ZAP

Sebagaimana ditunjukkan pada Gambar 2.3, antarmuka OWASP ZAP terdiri dari beberapa bagian utama yang mendukung proses pengujian keamanan aplikasi

web. Bagian kiri (*Sites Tree*) menampilkan struktur halaman website yang telah berhasil di-*crawl*. Bagian tengah utama digunakan untuk menampilkan permintaan dan respons HTTP secara detail, yang sangat penting untuk analisis manual. Sementara itu, tab bagian bawah (*Alerts*) menampilkan daftar kerentanan yang berhasil ditemukan oleh ZAP, yang sudah dikelompokkan berdasarkan tingkat risiko (*High*, *Medium*, *Low*, *Informational*). Antarmuka ini memungkinkan peneliti tidak hanya menjalankan pemindaian otomatis, tetapi juga melakukan investigasi manual terhadap temuan yang didapat.

OWASP ZAP bekerja dengan cara menyisipkan dirinya sebagai *proxy* antara peramban peneliti dan server web target. Dengan konfigurasi ini, semua lalu lintas HTTP dan HTTPS dapat dicegat, dianalisis, dan bahkan dimodifikasi. Berikut adalah fitur-fitur kunci yang akan dimanfaatkan dalam penelitian ini:

1. ***Spider* (Crawler)** : Secara otomatis menjelajahi seluruh halaman dan tautan pada website Polres Aceh Jaya dan Polres Aceh Selatan untuk memetakan seluruh titik yang dapat diuji (*attack surface*).
2. ***Active Scanner*** : Melakukan pemindaian aktif dengan mengirimkan berbagai *payload* atau pola input yang mencurigakan ke setiap titik yang ditemukan (seperti *form login*, kolom pencarian) untuk mendeteksi kerentanan seperti SQL *Injection*, *Cross-Site Scripting* (XSS), dan *Cross-Site Request Forgery* (CSRF).
3. ***Passive Scanner*** : Menganalisis lalu lintas yang lewat secara *real-time* tanpa mengirimkan input baru. Fitur ini efektif untuk mendeteksi masalah seperti *header* keamanan yang kurang (misal, CSP, HSTS) atau informasi sensitif yang terbawa dalam respons.
4. ***Fuzzer*** : Memungkinkan pengujian yang lebih intensif dengan menggabungkan daftar *payload* kustom ke parameter tertentu, berguna untuk menguji logika bisnis atau celah *input validation* yang kompleks.

Dalam penelitian ini, OWASP ZAP akan berperan sebagai *tools* inti untuk pemindaian otomatis pertama terhadap website Polres Aceh Jaya dan Polres Aceh Selatan. Pemindaian akan dikonfigurasi dengan mengacu pada OWASP Top 10 2025 sebagai standar acuan utama. Kombinasi fitur *spidering*, *active*, dan *passive*

scanning diharapkan dapat memberikan gambaran awal yang komprehensif tentang postur keamanan aplikasi web target.

2.7.4 Burp Suite

Burp Suite adalah perangkat lunak yang digunakan untuk menguji keamanan website secara manual. Di dunia keamanan siber, perangkat lunak ini dikenal sebagai alat standar untuk pengujian manual. Berbeda dengan OWASP ZAP yang banyak bekerja secara otomatis, Burp Suite memberikan kendali penuh kepada peneliti. Dengan kendali penuh ini, peneliti dapat melakukan pengujian yang lebih mendalam dan terarah.

Fitur paling dasar dari Burp Suite adalah Proxy, yang berfungsi menyadap komunikasi antara browser dan server website. Selain itu, terdapat fitur Repeater untuk mengulang dan mengedit satu perintah HTTP, serta Intruder untuk mengirimkan ribuan percobaan input secara otomatis. Fitur-fitur ini memungkinkan peneliti untuk menguji berbagai skenario serangan secara sistematis.

Dalam penelitian ini, Burp Suite memiliki peran yang sangat spesifik, yaitu untuk mengecek ulang atau memvalidasi semua temuan kerentanan yang didapat dari OWASP ZAP. Proses validasi manual ini sangat penting untuk memastikan bahwa laporan yang dihasilkan akurat dan bebas dari kesalahan deteksi (*false positive*). Validasi dilakukan dengan cara menguji ulang titik-titik yang terindikasi rentan menggunakan pendekatan manual.

Selain validasi, Burp Suite juga digunakan untuk pengujian yang lebih mendalam, seperti menguji kekuatan mekanisme *login*, memeriksa keamanan manajemen sesi pengguna, dan menganalisis logika bisnis aplikasi website Polres Aceh Jaya dan Polres Aceh Selatan. Semua aktivitas pengujian dengan Burp Suite dilakukan secara sangat terkontrol dan tidak merusak, sesuai dengan etika penelitian yang berlaku.

2.7.5 Integrasi Tools dalam Kerangka Penelitian

Tools-tools pendukung tersebut diintegrasikan secara sinergis dalam alur penelitian berdasarkan kerangka NIST SP 800-115, menciptakan pendekatan bertingkat yang mencakup berbagai aspek keamanan dari perspektif eksternal:

1. **Tahap Perencanaan (*Planning*)** : Semua *tools* dipersiapkan dan diuji coba dalam lingkungan laboratorium virtual di sisi peneliti untuk memastikan

konfigurasi dan fungsionalitasnya berjalan dengan baik sebelum digunakan terhadap target sesungguhnya.

2. **Tahap Penemuan (*Discovery*)** : WhatWeb digunakan untuk identifikasi teknologi website, sedangkan Nmap digunakan untuk pemindaian *port* dan layanan pada server target.
3. **Tahap Penilaian Kerentanan (*Vulnerability Assessment*)** : OWASP ZAP berperan sebagai alat utama *automated scanning* untuk mendeteksi kerentanan aplikasi web secara luas berdasarkan OWASP Top 10 2025.
4. **Tahap Serangan/Validasi (*Attack*)** : Burp Suite digunakan untuk pengujian manual dan validasi temuan kerentanan yang telah diidentifikasi oleh OWASP ZAP.
5. **Tahap Pelaporan (*Reporting*)** : Semua hasil dari setiap tahap dan *tools* dikonsolidasikan untuk dianalisis secara komprehensif berdasarkan OWASP Top 10 2025 dan dinilai tingkat risikonya dengan CVSS 4.0.

Pendekatan multi-tools ini memungkinkan cross-verifikasi temuan, mengurangi false positive, dan memberikan pemahaman yang lebih komprehensif tentang postur keamanan website. Setiap tools melengkapi kelemahan tools lainnya: automated scanner (OWASP ZAP) memberikan cakupan luas tetapi berpotensi false positive, sementara manual testing tools (Burp Suite) memberikan akurasi tinggi tetapi membutuhkan waktu lebih lama. Tools reconnaissance (WhatWeb dan Nmap) memberikan konteks infrastruktur yang penting untuk interpretasi hasil yang tepat.

Secara spesifik, integrasi ini dirancang untuk menilai website Polres Aceh Jaya dan Polres Aceh Selatan dari sudut pandang eksternal (*external assessment*). Pengujian dilakukan dari jaringan peneliti menuju alamat publik website target, mensimulasikan ancaman yang dapat dilakukan oleh pihak luar tanpa memerlukan akses ke dalam jaringan internal kepolisian. Rincian fungsi dan fase setiap *tools* dalam kerangka ini disajikan pada Tabel 2.6.

Tabel 2.6 Tools Pendukung dan Fungsinya dalam Penelitian

No	Tools	Fungsi Utama	Fase NIST SP 800-115	Contoh Penggunaan Spesifik
1	WhatWeb	Identifikasi teknologi website	*Discovery*	Mendeteksi CMS, web server, framework, plugin pada website target
2	Nmap	*Network discovery*, *port scanning*	*Discovery*	Pemindaian port 80/443, identifikasi layanan yang terbuka pada server
3	OWASP ZAP	*Automated vulnerability scanning*, *spidering*, *passive scanning*	*Vulnerability Assessment*	*Scanning* otomatis menyeluruh, deteksi kerentanan berdasarkan OWASP Top 10 2025, pemetaan struktur website
4	Burp Suite	*Manual testing*, validasi kerentanan	*Attack* (Validation)	Validasi manual temuan XSS atau SQLi, pengujian *session management*, analisis *business logic flaw*

2.7.6 Pertimbangan Etika dan Legalitas Penggunaan Tools

Seluruh penggunaan *tools* dalam penelitian ini dilandasi oleh aspek legalitas dan kepatuhan etika yang ketat. Dari segi perangkat lunak, semua *tools* yang digunakan (WhatWeb, Nmap, OWASP ZAP, dan Burp Suite *Community Edition*) merupakan perangkat berlisensi *open-source* atau tersedia secara legal dalam versi komunitas untuk penelitian akademik.

Landasan hukum dan etika yang paling utama adalah bahwa seluruh aktivitas pengujian dilakukan berdasarkan persetujuan dan izin observasi resmi dari Kepolisian Daerah (Polda) Aceh. Penelitian ini berkomitmen menjalankan prinsip-prinsip inti etika pengujian keamanan, yaitu pengujian yang diizinkan (*authorized testing*), meminimalkan gangguan terhadap layanan (*minimal disruption*), menjaga

integritas data (*data integrity*), serta melakukan pengujian secara terkendali (*controlled testing*).

Seluruh aktivitas pengujian akan dipantau dan *log* aktivitas akan dicatat untuk keperluan *audit* dan akuntabilitas. Lingkungan pengujian menggunakan *Virtual Machine* terisolasi di sisi peneliti untuk memastikan kontrol penuh. Tidak ada upaya untuk mengubah, menghapus, atau menambahkan data pada sistem target. Pengujian difokuskan pada identifikasi kerentanan secara pasif dan non-destruktif.

BAB III
METODOLOGI PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan campuran (*mixed methods*). Pendekatan ini dipilih karena penelitian tidak hanya mendeskripsikan fakta, tetapi juga membutuhkan analisis yang mendalam terhadap data yang beragam.

Pendekatan kuantitatif diterapkan untuk mengolah data yang dapat diukur secara numerik. Data tersebut mencakup skor keparahan dari CVSS 4.0, lama waktu pemindaian setiap *tools*, serta jumlah kerentanan yang ditemukan pada setiap kategori. Angka-angka ini akan memberikan gambaran yang objektif tentang tingkat risiko dan kinerja alat.

Secara paralel, pendekatan kualitatif digunakan untuk melakukan analisis yang lebih mendalam terhadap temuan. Pada pendekatan ini, setiap kerentanan akan diklasifikasikan berdasarkan jenisnya mengacu pada *framework* OWASP Top 10 2025. Selain itu, dilakukan analisis terhadap konteks, penyebab, dan potensi dampak dari setiap celah keamanan untuk menyusun rekomendasi perbaikan yang tepat.

Metode inti yang menjadi pelaksanaan kedua pendekatan tersebut adalah *Vulnerability Assessment* dan *Penetration Testing* (VAPT) Terbatas. Kerangka NIST SP 800-115 digunakan sebagai panduan tahapan pengujian, sementara standar OWASP Top 10 2025 menjadi acuan teknis. Seluruh proses pengujian bersifat legal, terkendali, dan non-destruktif karena dilaksanakan berdasarkan izin observasi resmi dari Polda Aceh. Pengujian dilakukan secara eksternal dari lingkungan peneliti menggunakan *Virtual Machine* (VM) yang terisolasi, tanpa memerlukan akses ke jaringan internal instansi target.

3.2 Objek Penelitian

Objek penelitian ini adalah dua website resmi milik Kepolisian Republik Indonesia yang berada di wilayah Aceh, yaitu website Polres Aceh Jaya dan website Polres Aceh Selatan. Kedua website tersebut dipilih karena memiliki fungsi yang sama sebagai media informasi dan komunikasi publik, namun menggunakan jenis

domain yang berbeda, yaitu domain .go.id dan domain .com. Perbedaan domain ini menjadi salah satu aspek yang menarik untuk dianalisis guna melihat kemungkinan perbedaan tingkat keamanan antara website yang menggunakan domain resmi pemerintah dengan domain komersial umum.

Secara teknis, kedua website dapat diakses secara publik tanpa perlu melakukan autentikasi atau login. Pengujian keamanan difokuskan pada seluruh halaman yang tersedia untuk umum, dengan menggunakan metode *vulnerability assessment* dan *penetration testing* terbatas. Seluruh kegiatan pengujian dilakukan secara legal berdasarkan izin resmi dari Polda Aceh. Rincian lebih lengkap mengenai objek penelitian disajikan pada Tabel 3.1 berikut.

Tabel 3.1 Deskripsi Objek Penelitian

No	Keterangan	Deskripsi
1	Nama Website	Website Polres Aceh Jaya
2	URL	https://tribratanews-resacehjaya.aceh.polri.go.id
3	Nama Website	Website Polres Aceh Selatan
4	URL	https://tribratanewspolresacehselatan.com
5	Jenis Website	Website Instansi Kepolisian (Polres)
6	Akses Website	Publik (tanpa login)
7	Objek Pengujian	Seluruh halaman yang dapat diakses umum pada kedua website
8	Metode Pengujian	*Vulnerability Assessment* menggunakan WhatWeb, Nmap, OWASP ZAP, dan Burp Suite
9	Batasan Pengujian	Tidak melakukan eksploitasi destruktif, perubahan data, atau gangguan layanan

Mengacu pada Tabel 3.1, objek penelitian ini terdiri dari dua website resmi kepolisian, yaitu website Polres Aceh Jaya dan website Polres Aceh Selatan. Kedua website tersebut dapat diakses secara publik tanpa autentikasi. Informasi yang disajikan dalam tabel mencakup aspek teknis dan nonteknis website yang menjadi dasar dalam menentukan ruang lingkup pengujian keamanan.

Penelitian ini membandingkan hasil analisis dari kedua website untuk memberikan gambaran keamanan yang lebih komprehensif. Dengan membandingkan dua website yang memiliki jenis domain berbeda namun fungsi yang sama, diharapkan dapat diketahui apakah terdapat perbedaan signifikan dalam tingkat kerentanan keamanan antara keduanya.

Pemilihan kedua website ini didasari oleh pengalaman penulis selama menjalani magang di Polda Aceh, di mana analisis keamanan website Polres merupakan bagian dari tugas yang diberikan. Pada saat penelitian dimulai, hampir seluruh website Polres jajaran yang menggunakan domain .go.id tidak dapat diakses, termasuk website resmi berita Polda Aceh yang sebelumnya direncanakan sebagai objek. Setelah berkonsultasi dengan Kepala Sub Bidang Teknologi Informasi dan Komunikasi (Kasubbid TIK) Polda Aceh, beliau menyarankan agar pengujian difokuskan pada dua website yang masih aktif dan dapat diakses publik, yaitu Polres Aceh Jaya dan Polres Aceh Selatan. Dari sinilah kemudian muncul pendekatan komparatif dalam penelitian ini, karena kedua website tersebut mewakili dua jenis domain yang berbeda namun sama-sama digunakan sebagai media komunikasi publik kepolisian.

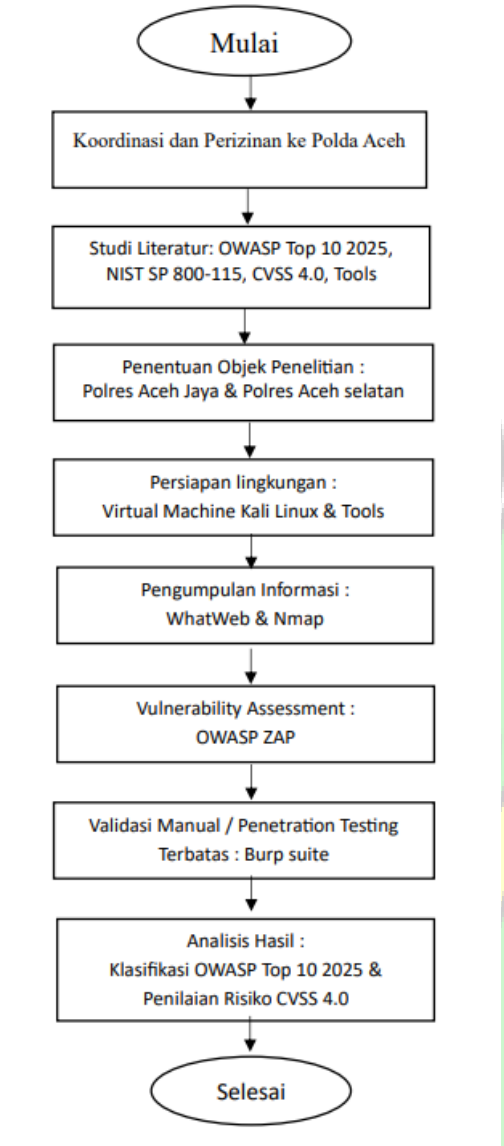
3.3 Waktu dan Tempat Penelitian

Penelitian ini dilaksanakan selama kurang lebih tujuh bulan, yaitu mulai dari Oktober 2025 hingga April 2026, dengan pengujian teknis terkonsentrasi pada April 2026. Pelaksanaan penelitian dilakukan di Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry Banda Aceh serta dari rumah peneliti, dengan objek penelitian berupa website yang dapat diakses secara daring.

Secara kronologis, tahap awal penelitian berupa koordinasi perizinan dan studi literatur dilakukan pada Oktober 2025. Selanjutnya pada November 2025, dilakukan persiapan alat dan pelaksanaan pengujian teknis. Proses analisis data dan penilaian risiko dilaksanakan pada Desember 2025, sedangkan penyusunan laporan serta finalisasi diselesaikan pada April 2026.

3.4 Alur Penelitian

Alur penelitian pada studi ini disusun secara sistematis untuk memastikan setiap tahap berjalan terstruktur dan terarah sesuai dengan tujuan penelitian. Secara visual, alur penelitian ditunjukkan dalam Gambar 3.1.



Gambar 3.1 Alur Penelitian

Alur penelitian dimulai dengan tahap koordinasi dan perizinan kepada Polda Aceh untuk memperoleh persetujuan resmi dan ruang lingkup pengujian. Setelah izin diperoleh, peneliti melakukan studi literatur yang mencakup kajian terhadap OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, serta *tools* yang akan digunakan yaitu WhatWeb, Nmap, OWASP ZAP, dan Burp Suite. Selanjutnya, dilakukan penentuan objek penelitian yaitu website Polres Aceh Jaya dan Polres Aceh Selatan sebagai target pengujian.

Tahap berikutnya adalah persiapan lingkungan, dimana peneliti menyiapkan *Virtual Machine* dengan sistem operasi Kali Linux dan menginstal

seluruh *tools* yang diperlukan. Setelah lingkungan siap, dilakukan pengumpulan informasi (*discovery*) menggunakan WhatWeb untuk identifikasi teknologi website dan Nmap untuk pemindaian *port* serta layanan. Kemudian dilanjutkan dengan *vulnerability assessment* menggunakan OWASP ZAP untuk melakukan pemindaian kerentanan otomatis.

Hasil pemindaian dari OWASP ZAP kemudian divalidasi secara manual melalui tahap validasi manual atau *penetration testing* terbatas menggunakan Burp Suite. Validasi ini bertujuan untuk memastikan akurasi temuan dan menghindari *false positive*. Setelah itu, dilakukan analisis hasil yang mencakup klasifikasi kerentanan berdasarkan OWASP Top 10 2025 dan penilaian tingkat risiko menggunakan CVSS 4.0. Tahap terakhir adalah penyusunan laporan yang berisi dokumentasi seluruh hasil penelitian beserta rekomendasi perbaikan. Setelah seluruh tahapan selesai dilaksanakan, maka penelitian dinyatakan selesai.

3.5 Alat dan Bahan Penelitian

Dalam pelaksanaan penelitian ini, diperlukan beberapa alat dan bahan untuk mendukung proses analisis kerentanan keamanan website. Alat dan bahan tersebut digunakan selama proses pengumpulan data, pengujian, serta analisis hasil penelitian agar penelitian dapat berjalan secara optimal dan sesuai dengan tujuan yang telah ditetapkan. Alat dan bahan yang digunakan dalam penelitian ini terdiri dari perangkat keras dan perangkat lunak yang dijelaskan sebagai berikut.

3.5.1 Perangkat Keras

Perangkat keras merupakan komponen fisik yang digunakan sebagai infrastruktur utama dalam menjalankan seluruh proses penelitian. Pemilihan spesifikasi perangkat keras perlu mempertimbangkan kebutuhan sumber daya untuk menjalankan *tools* pengujian keamanan secara bersamaan, seperti OWASP ZAP dan Burp Suite yang membutuhkan memori yang cukup besar. Selain itu, koneksi internet yang stabil juga diperlukan untuk mengakses website target dan melakukan pemindaian kerentanan secara *online*. Berikut adalah spesifikasi perangkat keras yang digunakan dalam penelitian ini.

Tabel 3.2 Spesifikasi Perangkat Keras

No	Keterangan	Deskripsi
1	Perangkat	Laptop
2	Prosesor	AMD Ryzen 5 7535HS with Radeon Graphics (~3.30 GHz)
3	RAM	16 GB
4	Sistem Operasi	Windows 11 Home Single Language 64-bit
5	Penyimpanan	SSD
6	Koneksi	Internet

Berdasarkan Tabel 3.2, spesifikasi perangkat keras yang digunakan tergolong cukup mumpuni untuk menjalankan proses pengujian keamanan. Prosesor dengan kecepatan 3.30 GHz dan kapasitas RAM 16 GB memungkinkan peneliti menjalankan *virtual machine* serta beberapa *tools* pengujian secara bersamaan tanpa mengalami kendala kinerja yang berarti. Selain itu, media penyimpanan SSD mempercepat proses *booting* dan akses data selama pengujian berlangsung.

3.5.2 Perangkat Lunak

Selain perangkat keras, penelitian ini juga memerlukan perangkat lunak yang berfungsi sebagai lingkungan pengujian dan *tools* untuk melakukan analisis keamanan. Perangkat lunak yang digunakan meliputi sistem operasi, *virtual machine*, *browser*, serta berbagai *tools* keamanan seperti WhatWeb, Nmap, OWASP ZAP, dan Burp Suite. Pemilihan perangkat lunak didasarkan pada kompatibilitas, ketersediaan lisensi *open-source*, serta reputasinya dalam pengujian keamanan website. Rincian lebih lengkap mengenai perangkat lunak dan *tools* yang digunakan disajikan pada Tabel 3.3.

Tabel 3.3 Spesifikasi Perangkat Lunak dan Tools Keamanan

No	Komponen	Versi	Fungsi
1	Sistem Operasi Host	Windows 11 Home	Sistem operasi utama

2	*Virtual Machine*	Oracle VirtualBox 7.0	Virtualisasi lingkungan pengujian
3	Sistem Operasi Virtual	Kali Linux 2024.1	*Environment* pengujian keamanan
4	*Web Browser*	Google Chrome	Akses dan eksplorasi website
5	*Technology Identifier*	WhatWeb 0.5.5	Identifikasi teknologi website (CMS, *web server*, dll.)
6	*Network Scanner*	Nmap 7.94	*Network discovery* dan *port scanning*
7	*Vulnerability Scanner*	OWASP ZAP 2.15.0	*Automated scanning* dan *vulnerability assessment*
8	*Penetration Testing Tool*	Burp Suite Community 2024.5	*Manual testing* dan validasi kerentanan

Mengacu pada Tabel 3.3, perangkat lunak yang digunakan dalam penelitian ini terdiri dari sistem operasi utama, lingkungan virtualisasi, serta berbagai *tools* keamanan yang mendukung proses pengujian keamanan website. Penggunaan sistem operasi Windows sebagai *host* dan Kali Linux sebagai sistem operasi virtual bertujuan untuk menciptakan lingkungan pengujian yang terisolasi dan terkontrol, sehingga proses pengujian dapat dilakukan secara aman tanpa mengganggu sistem utama.

Kombinasi *tools* keamanan yang digunakan memiliki fungsi yang saling melengkapi. WhatWeb digunakan untuk identifikasi teknologi website pada tahap awal, Nmap untuk pemindaian *port* dan layanan, OWASP ZAP untuk pemindaian kerentanan otomatis, serta Burp Suite untuk validasi manual. Dengan kombinasi ini, diharapkan hasil pengujian menjadi lebih akurat dan komprehensif. Seluruh *tools* yang digunakan bersifat *open-source* dan legal untuk keperluan penelitian akademik.

3.6 Tahapan Penelitian

Tahapan penelitian dirancang agar proses analisis berjalan terstruktur, terukur, dan dapat dipertanggungjawabkan. Tahapan ini mengintegrasikan kerangka NIST SP 800-115 dengan standar OWASP Top 10 2025 dan CVSS 4.0.

Tabel 3.4 Tahapan Pelaksanaan Penelitian

No	Tahapan Penelitian	Keterangan Singkat
1	Koordinasi dan Perizinan	Memperoleh persetujuan dan ruang lingkup pengujian dari Polda Aceh
2	Studi Literatur	Mengkaji teori dan standar keamanan (OWASP Top 10 2025, NIST SP 800-115, CVSS 4.0, *tools*)
3	Penentuan Objek Penelitian	Menetapkan website Polres Aceh Jaya dan Polres Aceh Selatan sebagai objek
4	Persiapan Alat dan Lingkungan	Menyiapkan perangkat keras, lunak, dan konfigurasi *tools* pengujian
5	Pengumpulan Informasi (*Discovery*)	Identifikasi teknologi dengan WhatWeb; pemindaian *port* dan layanan dengan Nmap
6	*Vulnerability Assessment*	Pemindaian otomatis mendalam dengan OWASP ZAP
7	Validasi Manual	Validasi temuan kerentanan menggunakan Burp Suite
8	Analisis dan Pengolahan Data	Klasifikasi kerentanan berdasarkan OWASP Top 10 2025 dan penilaian risiko CVSS 4.0
9	Penyusunan Laporan	Dokumentasi hasil penelitian dan rekomendasi perbaikan

Mengacu pada Tabel 3.4, tahapan pelaksanaan penelitian dimulai dari proses koordinasi dan perizinan hingga penyusunan laporan akhir. Setiap tahapan disusun secara berurutan untuk memastikan bahwa proses pengujian keamanan dilakukan secara sistematis, mulai dari persiapan, pengumpulan informasi, pemindaian kerentanan, hingga analisis dan dokumentasi hasil. Tahapan ini mengikuti kerangka NIST SP 800-115 yang telah disesuaikan dengan kebutuhan penelitian.

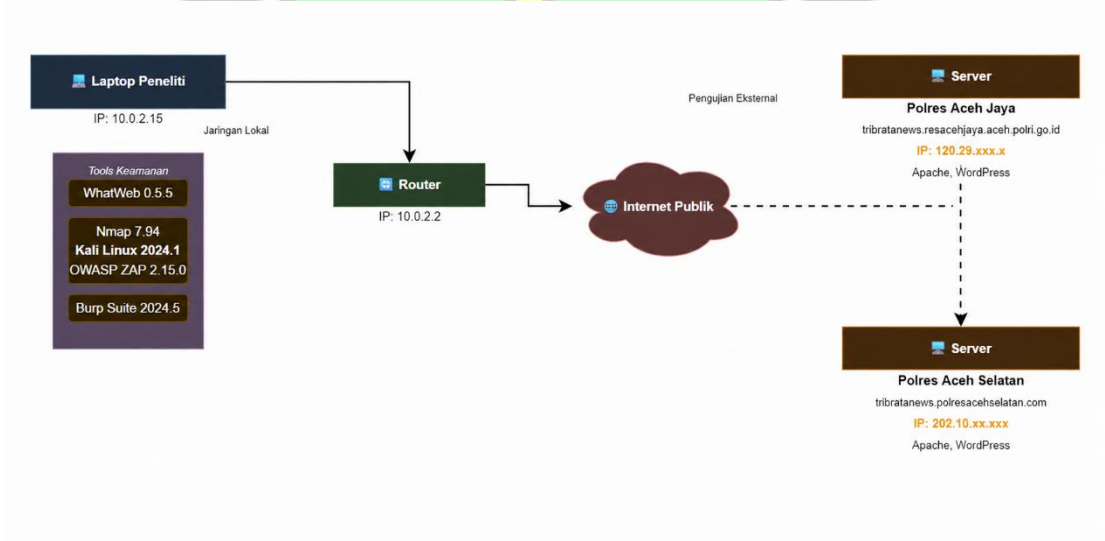
Seluruh tahapan penelitian dilaksanakan dengan mengacu pada prinsip pengujian yang legal, terbatas, dan non-destruktif. Pendekatan ini bertujuan untuk menjaga validitas hasil penelitian sekaligus memastikan bahwa proses pengujian tetap berada dalam ruang lingkup dan etika pengujian yang telah disetujui oleh pihak Polda Aceh. Dengan tahapan yang terstruktur, penelitian ini diharapkan dapat menghasilkan analisis keamanan yang akurat dan bermanfaat bagi peningkatan keamanan website Polres Aceh Jaya dan Polres Aceh Selatan.

3.7 Skenario Pengujian

Skenario pengujian disusun sebagai pedoman teknis untuk memastikan proses berjalan terarah, terkontrol, dan sesuai ruang lingkup yang telah disetujui Polda Aceh. Skenario ini mengadopsi metodologi *Vulnerability Assessment* Eksternal dengan pendekatan *Black Box*.

3.7.1 Topologi dan Lingkungan Pengujian

Pengujian dilakukan secara eksternal (*external assessment*) dari sisi peneliti menggunakan *virtual machine* (VM) terisolasi yang berisi seluruh *tools* pengujian. Topologi pengujian yang akan diterapkan digambarkan pada Gambar 3.2 berikut.



Gambar 3.2 Topologi Pengujian Keamanan Website Polres Aceh Jaya dan Polres Aceh Selatan

Gambar 3.2 menunjukkan topologi pengujian keamanan website yang dilakukan dari sisi peneliti menuju server target melalui jaringan internet. Pada sisi kiri gambar terdapat lingkungan peneliti yang menggunakan sebuah laptop dengan alamat IP 10.0.2.15. Di dalam laptop tersebut dijalankan sebuah *virtual machine* (VM) yang berfungsi sebagai lingkungan pengujian terisolasi. VM ini digunakan untuk menjalankan sistem operasi Kali Linux 2024.1 yang telah dilengkapi dengan berbagai *tools* pengujian keamanan web, seperti WhatWeb 0.5.5, Nmap 7.94, OWASP ZAP 2.15.0, dan Burp Suite 2024.5. Seluruh aktivitas pengujian dilakukan dari dalam VM untuk memastikan proses pengujian lebih terkontrol dan tidak memengaruhi sistem utama peneliti.

Dari lingkungan peneliti, koneksi jaringan diarahkan ke router dengan alamat IP 10.0.2.2 yang berfungsi sebagai *gateway*. Hubungan antara laptop peneliti dengan router digambarkan menggunakan garis lurus, yang menandakan bahwa koneksi ini bersifat langsung dan berada dalam kendali penuh peneliti di jaringan lokal. Router ini menjadi penghubung antara jaringan lokal peneliti dengan jaringan internet publik. Dari router, lalu lintas pengujian memasuki internet dan kemudian diteruskan menuju dua server target melalui jalur yang digambarkan dengan garis putus-putus. Penggunaan garis putus-putus ini menunjukkan bahwa koneksi menuju server dilakukan melalui jaringan internet publik yang tidak dapat dikontrol langsung oleh peneliti, sekaligus menandakan batas antara lingkungan pengujian internal dengan server target yang berada di luar. Percabangan garis putus-putus menuju masing-masing server menegaskan bahwa pengujian dilakukan secara paralel dari satu sumber ke dua target yang berbeda, tanpa interkoneksi langsung antara kedua server.

Pada sisi kanan gambar ditampilkan dua server target. Server pertama menghosting website Polres Aceh Jaya dengan domain tribratanews-resacehjaya.aceh.polri.go.id yang berjalan di atas Apache dan WordPress, dan server kedua menghosting website Polres Aceh Selatan dengan domain tribratanewspolresacehselatan.com yang juga menggunakan Apache dan WordPress. Kedua website ini dapat diakses secara umum melalui internet, sehingga menjadi objek pengujian untuk mengidentifikasi potensi kerentanan pada layanan web yang bersifat *public-facing*.

3.7.2 Ruang Lingkup dan Waktu Pengujian

Pengujian akan dilakukan pada website resmi Polres Aceh Jaya dengan domain tribratanews-resacehjaya.aceh.polri.go.id dan website Polres Aceh Selatan dengan domain tribratanewspolresacehselatan.com. Ruang lingkup pengujian terbatas pada halaman yang dapat diakses publik tanpa perlu autentikasi. Penelitian ini direncanakan berlangsung dalam periode Oktober 2025 hingga April 2026.

Aktivitas pengujian akan dilaksanakan pada jam kerja setelah memperoleh persetujuan resmi dan dilakukan dengan pemantauan dari pihak Polda Aceh guna memastikan tidak mengganggu ketersediaan layanan utama. Seluruh pengujian

bersifat non-destruktif, berfokus pada identifikasi dan validasi kerentanan tanpa melakukan eksploitasi aktif atau perubahan data.

3.7.3 Pendekatan dan Strategi Pengujian

Pengujian dilakukan dari perspektif eksternal (*external assessment*) dengan pendekatan *black box*, yaitu peneliti tidak memiliki pengetahuan awal mengenai struktur internal, kode sumber, atau konfigurasi detail dari kedua website target. Pengetahuan awal yang dimiliki hanya terbatas pada informasi yang dapat diakses publik, seperti alamat URL domain target (tribratanews-resacehjaya.aceh.polri.go.id dan tribratanewspolresacehselatan.com) serta hasil identifikasi awal menggunakan WhatWeb untuk mengetahui teknologi yang digunakan.

Strategi pengujian yang digunakan adalah *serial scanning*, di mana setiap *tools* dijalankan secara berurutan pada kedua website target dengan urutan yang sama. Strategi ini bertujuan untuk memastikan cakupan pengujian yang menyeluruh dan hasil yang saling melengkapi. WhatWeb digunakan terlebih dahulu untuk identifikasi teknologi, dilanjutkan dengan Nmap untuk pemindaian *port* dan layanan, kemudian OWASP ZAP untuk *automated scanning*, dan terakhir Burp Suite untuk validasi manual.

3.7.4 Tahapan Pengujian

Tahapan pengujian keamanan dalam penelitian ini disusun dengan mengacu pada alur pengujian yang sistematis dan terukur. Setiap fase pengujian dirancang untuk saling melengkapi, dimulai dari proses pengumpulan informasi awal, pemindaian kerentanan secara otomatis, hingga validasi manual dan analisis risiko. Pendekatan ini bertujuan untuk memperoleh gambaran menyeluruh mengenai kondisi keamanan kedua website yang menjadi objek penelitian.

Tabel 3.5 Rincian Skenario Pengujian

No	Fase	Tools Utama	Aktivitas Utama
1	*Discovery*	WhatWeb, Nmap	Identifikasi teknologi website, pemindaian *port*, enumerasi *service*
2	*Vulnerability Assessment*	OWASP ZAP	*Automated scanning*, *crawling*, *active scan* berdasarkan OWASP Top 10 2025

3	Validasi Manual	Burp Suite	Validasi manual kerentanan (XSS, SQLi, dll.), *input fuzzing*, *session analysis*
4	Analisis	Manual + *Spreadsheet*	Klasifikasi OWASP Top 10 2025, *scoring* CVSS 4.0, prioritisasi risiko

Mengacu pada Tabel 3.5, skenario pengujian keamanan dibagi ke dalam empat fase utama, yaitu *discovery*, *vulnerability assessment*, validasi manual, dan analisis. Setiap fase menggunakan *tools* yang berbeda sesuai dengan fungsi dan tujuan pengujian, sehingga proses identifikasi dan validasi kerentanan dapat dilakukan secara efektif dan terstruktur.

Hasil dari setiap fase pengujian kemudian dianalisis dengan mengacu pada klasifikasi OWASP Top 10 2025 dan dinilai tingkat risikonya menggunakan standar CVSS 4.0. Dengan skenario pengujian yang tersusun secara sistematis, penelitian ini diharapkan mampu menghasilkan temuan kerentanan yang akurat serta rekomendasi keamanan yang relevan untuk meningkatkan keamanan website Polres Aceh Jaya dan Polres Aceh Selatan.

Perlu dicatat bahwa tidak seluruh fitur dari setiap *tools* yang disebutkan di Bab II digunakan dalam penelitian ini. Pada OWASP ZAP, fitur *Fuzzer* tidak diaktifkan karena pengujian injeksi lebih mengandalkan validasi manual melalui Burp Suite *Repeater*. Pada Burp Suite, fitur *Intruder* tidak digunakan untuk menghindari lonjakan permintaan yang berpotensi membebani server *live*. Selain itu, pengujian terhadap mekanisme *login* dan manajemen sesi tidak dilakukan karena ruang lingkup pengujian dibatasi pada halaman yang dapat diakses publik tanpa otentikasi. Pembatasan-pembatasan ini merupakan bagian dari strategi pengujian yang terkendali dan non-destruktif sebagaimana telah disetujui oleh Polda Aceh.

3.7.5 Output yang Diharapkan

Hasil dari skenario pengujian ini adalah laporan komprehensif yang berisi:

1. Daftar kerentanan yang teridentifikasi pada website Polres Aceh Jaya dan Polres Aceh Selatan beserta tingkat risikonya.
2. Pemetaan kerentanan terhadap standar OWASP Top 10 2025.
3. Rekomendasi perbaikan yang terprioritaskan berdasarkan skor CVSS 4.0.

3.8 Teknik Analisis Data

Teknik analisis data digunakan untuk mengolah dan memahami data yang diperoleh dari hasil pengujian keamanan website. Analisis dilakukan agar hasil pemindaian dapat diinterpretasikan dengan baik dan disajikan secara sistematis sesuai tujuan penelitian.

Data yang dianalisis berasal dari hasil pemindaian menggunakan tools WhatWeb, Nmap, OWASP ZAP, dan Burp Suite. Data tersebut berupa temuan kerentanan keamanan yang kemudian dianalisis berdasarkan jenis kerentanan, tingkat risiko, dan dampak potensialnya.

Proses analisis dilakukan dengan mengelompokkan temuan berdasarkan kerangka kerja OWASP Top 10 2025, serta menilai tingkat risikonya menggunakan CVSS 4.0 dengan penyesuaian kontekstual terhadap lingkungan kepolisian. Pendekatan ini memudahkan penarikan kesimpulan mengenai postur keamanan website dan penyusunan rekomendasi perbaikan yang terprioritaskan.

3.8.1 Tahapan Analisis Data

Tahapan analisis data dalam penelitian ini mengikuti alur sistematis:

1. **Pengumpulan Data**: Menggabungkan hasil pemindaian dari semua *tools* (WhatWeb, Nmap, OWASP ZAP, Burp Suite) ke dalam satu basis data terpusat.
2. **Identifikasi dan Validasi**: Mengidentifikasi jenis kerentanan dan memvalidasi temuan melalui uji manual untuk meminimalkan *false positive*.
3. **Klasifikasi Berdasarkan OWASP Top 10 2025**: Mengelompokkan setiap kerentanan ke dalam salah satu dari sepuluh kategori OWASP Top 10 2025.
4. **Penilaian Risiko dengan CVSS 4.0**: Memberikan skor risiko menggunakan metode CVSS 4.0 melalui empat lapis analisis:
    1) *Base Metrics*: Menilai sifat intrinsik kerentanan (cara eksploitasi & dampak dasar)
    2) *Threat Metrics*: Menyesuaikan dengan kondisi ancaman terkini (kedewasaan eksploit)
    3) *Environmental Metrics*: Mempertimbangkan konteks spesifik lingkungan kepolisian (kepentingan aset, kontrol keamanan)

4) *Supplemental Metrics*: Mencatat konteks tambahan seperti dampak terhadap pelayanan publik

5. **Prioritisasi**: Mengurutkan kerentanan berdasarkan tingkat keparahan hasil skoring (*Critical*, *High*, *Medium*, *Low*).
6. **Penyajian Hasil**: Menyajikan hasil analisis dalam bentuk tabel, diagram distribusi, dan narasi deskriptif.

3.8.2 Teknik Analisis Spesifik

Teknik analisis data dalam penelitian ini dirancang untuk memastikan bahwa setiap temuan kerentanan yang diperoleh dari proses pengujian dapat dianalisis secara sistematis dan akurat. Analisis dilakukan dengan mengombinasikan pendekatan teknis dan standar internasional guna menghasilkan klasifikasi serta penilaian risiko yang objektif dan dapat dipertanggungjawabkan.

Tabel 3.6 Teknik Analisis Data Kerentanan Keamanan Website

No	Jenis Data	Teknik Analisis	Hasil yang Diharapkan
1	Hasil pemindaian OWASP ZAP & Burp Suite	Identifikasi dan validasi manual kerentanan	Daftar kerentanan yang telah divalidasi (bebas *false positive*)
2	Data temuan kerentanan	Klasifikasi berdasarkan OWASP Top 10 2025	Pemetaan kerentanan ke dalam 10 kategori standar OWASP
3	Karakteristik kerentanan	Penilaian risiko empat lapis CVSS 4.0 (*Base*, *Threat*, *Environmental*, *Supplemental*)	Skor risiko numerik (0.0–10.0) yang kontekstual
4	Skor CVSS hasil analisis	Kategorisasi tingkat keparahan	Prioritas penanganan: *Critical*, *High*, *Medium*, *Low*
5	Data keseluruhan hasil pengujian	Analisis deskriptif dan komparatif	Gambaran umum postur keamanan kedua website dan rekomendasi perbaikan terstruktur

Mengacu pada Tabel 3.6, teknik analisis data dilakukan secara bertahap mulai dari identifikasi dan validasi kerentanan hingga penilaian tingkat risiko dan penyusunan rekomendasi perbaikan. Setiap jenis data dianalisis menggunakan

teknik yang sesuai, sehingga hasil analisis yang diperoleh tidak hanya akurat secara teknis, tetapi juga relevan dalam konteks keamanan website kepolisian.

Hasil analisis kemudian digunakan untuk memetakan kerentanan ke dalam kategori OWASP Top 10 2025 serta menentukan tingkat keparahan berdasarkan skor CVSS 4.0. Pendekatan ini memungkinkan peneliti untuk menyusun prioritas penanganan kerentanan secara terstruktur, sekaligus memberikan gambaran umum mengenai postur keamanan kedua website yang menjadi objek penelitian.

3.8.3 Output Analisis

Hasil analisis akan disajikan dalam bentuk:

1. **Tabel Temuan Kerentanan** yang dilengkapi dengan: deskripsi kerentanan, kategori OWASP Top 10 2025, skor CVSS 4.0, tingkat keparahan, dan rekomendasi mitigasi.
2. **Diagram Distribusi Kerentanan** berdasarkan tingkat keparahan.
3. **Rekomendasi Perbaikan Terstruktur** yang disusun berdasarkan prioritas risiko (*Critical* → *High* → *Medium* → *Low*).
4. **Laporan Analisis Komprehensif** untuk Polda Aceh sebagai bahan evaluasi dan acuan peningkatan keamanan sistem informasi pada website Polres Aceh Jaya dan Polres Aceh Selatan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Fase Discovery: Identifikasi Teknologi dan Infrastruktur

Langkah awal yang diambil dalam penelitian ini adalah mengumpulkan informasi dasar mengenai teknologi dan konfigurasi jaringan dari kedua website. Informasi semacam ini diperlukan untuk memahami lingkungan tempat aplikasi berjalan, sekaligus menjadi petunjuk awal mengenai potensi kelemahan yang mungkin muncul dari komponen yang digunakan. Dua alat bantu yang dipakai pada tahap ini adalah *WhatWeb* untuk mengenali susunan perangkat lunak, dan *Nmap* untuk memindai port serta layanan yang terbuka.

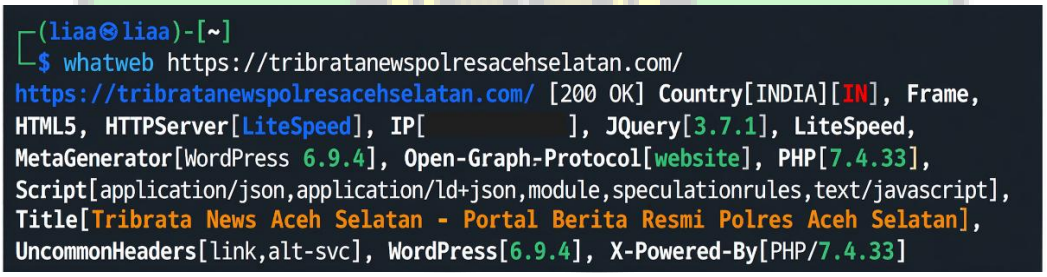
4.1.1 Identifikasi Teknologi dengan WhatWeb

WhatWeb dijalankan terhadap alamat utama kedua Polres. Hasilnya menunjukkan bahwa baik website Polres Aceh Jaya maupun Aceh Selatan sama-sama dibangun di atas CMS *WordPress*. Versi yang terdeteksi adalah 6.9.4, yang pada saat pengujian berlangsung merupakan rilis stabil terbaru. Ini bisa dinilai sebagai langkah pemeliharaan yang baik karena inti sistem tidak tertinggal versi lama yang rawan. Perbedaan mulai tampak ketika melihat komponen di lapisan server. Pada website Aceh Jaya, *web server* yang digunakan adalah *Apache*, namun tanpa keterangan versi lebih lanjut. Informasi bahasa pemrograman *PHP* juga tidak ditampilkan di *header* respons *HTTP*, sehingga tidak mudah diketahui dari luar. Sementara itu, website Aceh Selatan menggunakan *LiteSpeed* dan secara terbuka mengirimkan *header* X-Powered-By: PHP/7.4.33. Terlihat jelas bahwa versi *PHP* yang berjalan sudah cukup tua dan sebenarnya telah berakhir masa dukungannya sejak November 2022. Temuan kecil ini sebenarnya cukup berarti karena komponen usang semacam itu tidak lagi memperoleh tambalan keamanan dari pengembangnya.

Gambar 4.1 Hasil WhatWeb pada website Polres Aceh Jaya

Gambar 4.1 menampilkan keluaran *WhatWeb* untuk situs Aceh Jaya. Terlihat bahwa *Apache* terdeteksi sebagai server, namun tidak ada baris X-Powered-By yang mengungkap versi *PHP*. Ketidakhadiran informasi versi ini bisa jadi merupakan hasil dari konfigurasi sadar pihak pengelola untuk menyembunyikan jejak perangkat lunak yang dipakai. Dalam praktik keamanan, tindakan semacam ini dikenal sebagai *security through obscurity*, yang meskipun bukan pertahanan utama, setidaknya dapat memperlambat penyerang dalam mengidentifikasi kerentanan spesifik yang sesuai dengan versi tertentu.

Selain itu, *WhatWeb* juga mendeteksi penggunaan *Bootstrap* sebagai kerangka antarmuka, serta beberapa *plugin* umum *WordPress* seperti *Contact Form 7* dan *Elementor*. Informasi ini berguna untuk mempersempit dugaan mengenai titik-titik interaksi yang mungkin ada di situs, sekaligus menjadi petunjuk bahwa situs ini cukup aktif dikelola dan diperbarui. Tidak adanya indikasi komponen usang pada lapisan aplikasi menjadi nilai positif tersendiri bagi postur keamanan Polres Aceh Jaya.



Gambar 4.2 hasil WhatWeb pada website Polres Aceh Selatan

Berbeda dengan Gambar 4.1, Gambar 4.2 menyajikan pemandangan yang sedikit berbeda. *WhatWeb* berhasil mengidentifikasi bahwa server yang digunakan adalah *LiteSpeed*, dan yang paling mencolok adalah kemunculan informasi X-Powered-By: PHP/7.4.33. Informasi ini terpampang jelas di header respons *HTTP*, yang artinya setiap kali ada permintaan ke server, versi *PHP* yang digunakan akan

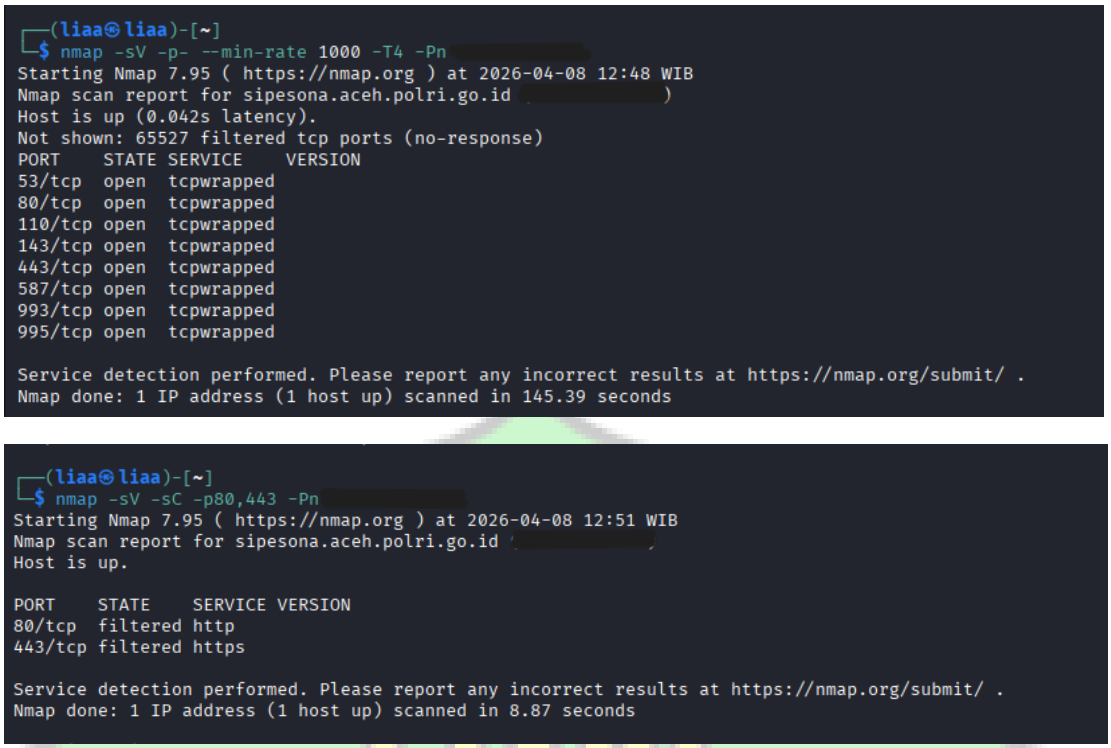
ikut dikirimkan sebagai bagian dari balasan. Dari sudut pandang keamanan, praktik ini kurang ideal karena memberikan informasi gratis kepada calon penyerang tentang versi perangkat lunak yang sedang berjalan.

Versi *PHP* 7.4 sendiri sudah tidak lagi didukung oleh pengembangnya sejak akhir tahun 2022. Ini berarti bahwa setiap kerentanan baru yang ditemukan pada versi tersebut tidak akan pernah diperbaiki secara resmi. Jika situs ini masih berjalan di atas *PHP* 7.4, maka seluruh aplikasi berada dalam kondisi rentan terhadap eksploitasi yang mungkin sudah diketahui publik. Temuan ini nantinya akan menjadi salah satu poin utama dalam penilaian risiko menggunakan *CVSS* 4.0, karena menyangkut aspek *Software Supply Chain* yang menjadi perhatian dalam OWASP Top 10 2025.

4.1.2 Pemetaan Port dan Layanan dengan Nmap

Setelah mengetahui susunan perangkat lunak, pengujian bergeser ke lapisan jaringan. *Nmap* dipakai untuk melihat port-port apa saja yang merespons permintaan dari internet. Hasil pemindaian penuh terhadap alamat IP Polres Aceh Jaya mendapati beberapa port dalam keadaan terbuka namun terbungkus oleh mekanisme tcpwrapped. Ini adalah teknik yang menyembunyikan *banner* asli layanan, sehingga alat pemindai tidak bisa langsung tahu aplikasi apa yang berjalan di balik port tersebut. Upaya ini cukup efektif untuk mempersulit pengintaian awal oleh penyerang.

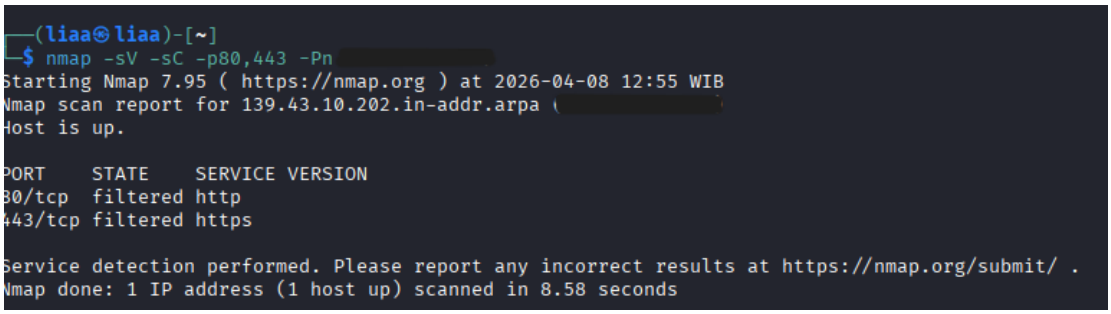
Hasil yang berbeda justru terlihat pada website Aceh Selatan. Saat dilakukan pemindaian menyeluruh, tidak ditemukan satu pun port yang memberikan respons berarti. Semua port dilaporkan dalam keadaan filtered. Konfigurasi semacam ini sering disebut sebagai mode senyap, di mana server seakan tidak terlihat di jaringan. Dari sisi perimeter, ini adalah postur yang lebih disukai karena mengurangi permukaan serangan secara drastis.



Gambar 4.3 hasil Nmap pada IP Polres Aceh Jaya

Gambar 4.3 memperlihatkan keluaran Nmap saat melakukan pemindaian terhadap alamat IP yang menaungi website Polres Aceh Jaya. Beberapa port seperti 53, 80, 110, 143, 443, dan lainnya dilaporkan dalam keadaan terbuka, namun dengan catatan tcpwrapped. Status tcpwrapped ini mengindikasikan bahwa ada lapisan tambahan biasanya berupa firewall atau TCP Wrapper yang menghalangi Nmap untuk menyelesaikan proses handshake dan membaca banner layanan. Alhasil, peneliti hanya tahu bahwa port tersebut terbuka, tetapi tidak bisa memastikan versi layanan apa yang berjalan di belakangnya.

Konfigurasi seperti ini cukup umum diterapkan pada server yang ingin tetap menyediakan layanan ke publik namun tidak ingin membeberkan detail teknis secara cuma-cuma. Bagi penyerang, informasi yang minim akan memperlambat proses pengintaian karena mereka harus menebak-nebak atau mencoba berbagai kemungkinan eksploitasi secara membabi buta. Meskipun tidak menjamin keamanan mutlak, langkah ini tetap patut diapresiasi sebagai bagian dari strategi pertahanan berlapis.



Gambar 4.4 hasil Nmap pada IP Polres Aceh Selatan

Gambar 4.4 menyajikan hasil pemindaian *Nmap* terhadap alamat IP website Polres Aceh Selatan. Berbeda dengan Gambar 4.3, tidak ada satu pun port yang dilaporkan sebagai terbuka. Seluruh 65.535 port yang dipindai berada dalam keadaan filtered, yang berarti *Nmap* tidak menerima balasan apa pun dari server, baik berupa penerimaan maupun penolakan. Paket yang dikirim seolah-olah hilang ditelan jaringan, tanpa jejak. Kondisi ini adalah contoh dari konfigurasi *firewall* dengan kebijakan *default deny* yang diterapkan secara ketat. Server hanya akan merespons jika permintaan datang dari sumber atau dengan kriteria tertentu yang sudah diizinkan. Bagi pemindai port, server seperti ini praktis tidak terlihat, sehingga sangat sulit untuk memetakan layanan apa saja yang sebenarnya tersedia. Dari sisi keamanan perimeter, Polres Aceh Selatan jelas unggul dalam hal ini, karena permukaan serangan yang terekspos ke internet publik nyaris tidak ada.

Secara keseluruhan, tahap pengumpulan informasi ini memberikan dua potret yang berbeda. Polres Aceh Jaya lebih terbuka di sisi jaringan namun cukup rapat dalam menyembunyikan jejak perangkat lunak. Sebaliknya, Polres Aceh Selatan sangat kokoh di perimeter namun menyisakan celah pada versi *PHP* lawas yang terekspos. Kedua karakteristik ini akan mempengaruhi fokus pengujian pada tahap berikutnya, terutama ketika masuk ke analisis kerentanan aplikasi dan penilaian risiko menyeluruh.

4.2 Fase Vulnerability Assessment: Pemindaian Otomatis dengan OWASP ZAP

Setelah mendapatkan gambaran awal mengenai teknologi dan kondisi jaringan dari kedua website, langkah berikutnya adalah melakukan pemindaian kerentanan secara otomatis menggunakan *OWASP ZAP*. Alat ini bekerja dengan cara

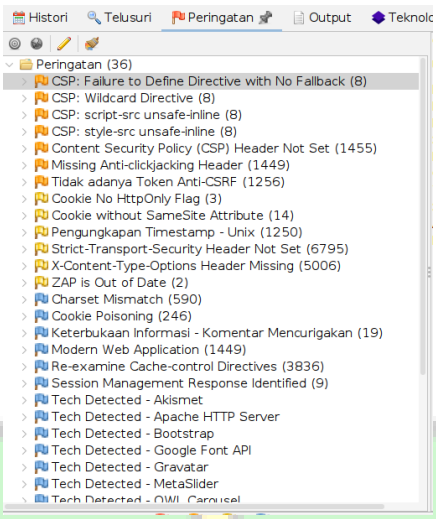
menjelajahi seluruh struktur situs yang dapat dijangkau, kemudian mengirimkan berbagai pola serangan standar ke setiap titik interaksi yang ditemukan, seperti formulir, parameter URL, dan elemen interaktif lainnya. Di saat yang sama, *ZAP* juga memantau lalu lintas secara pasif untuk mendeteksi kelemahan konfigurasi yang mungkin terlewat oleh pemindaian aktif. Proses pemindaian terhadap kedua website tidak berjalan sepenuhnya mulus. Pada website Polres Aceh Jaya, pemindaian sempat terhenti (*freeze*) di progres 3% dan 38% sehingga harus diulang beberapa kali hingga mencapai 100%. Kendala ini menyebabkan total waktu pemindaian mencapai sekitar 8 jam. Meskipun demikian, dari sisi cakupan, spidering berhasil menjangkau sekitar 120 halaman dengan total sekitar 850 permintaan. Pada website Polres Aceh Selatan, spidering menjangkau sekitar 95 halaman dengan total sekitar 720 permintaan. Perbedaan jumlah halaman ini wajar mengingat perbedaan volume konten dan struktur navigasi antara kedua website. Lamanya waktu pemindaian lebih disebabkan oleh faktor jaringan dan teknis di sisi peneliti, bukan karena ukuran atau kompleksitas website target..

Hasil pemindaian OWASP ZAP terhadap website Polres Aceh Jaya menghasilkan total 36 peringatan yang tersebar di berbagai tingkat risiko. Setelah mengeliminasi peringatan internal seperti ZAP is Out of Date serta peringatan informational murni terkait deteksi teknologi, diperoleh sekitar 15 jenis peringatan keamanan yang relevan. Pada tingkat Medium, ditemukan beberapa kelemahan konfigurasi Content Security Policy (CSP), yaitu CSP: Failure to Define Directive with No Fallback yang menunjukkan ketiadaan direktif default-src, serta CSP: Wildcard Directive yang menandakan penggunaan karakter liar dalam kebijakan. Selain itu, header X-Frame-Options tidak ditemukan (Missing Anti-clickjacking Header), dan pada formulir komentar publik tidak terdapat token anti-CSRF, meskipun yang terakhir ini berisiko rendah karena tidak melibatkan autentikasi pengguna. Pada tingkat Low, ZAP mencatat penggunaan script-src unsafe-inline dan style-src unsafe-inline dalam CSP, ketiadaan header Strict-Transport-Security (HSTS) dan X-Content-Type-Options, serta pengaturan cookie yang belum dilengkapi atribut HttpOnly dan SameSite. Sementara itu, peringatan informational mencakup pengungkapan timestamp Unix, komentar mencurigakan, charset

mismatch, serta deteksi teknologi seperti Akismet, Bootstrap, MetaSlider, Gravatar, Google Font API, dan Apache HTTP Server.

Banyaknya peringatan ini menunjukkan bahwa konfigurasi keamanan pada website Polres Aceh Jaya masih memerlukan perhatian serius, terutama pada aspek CSP dan HTTP security headers. Meskipun situs telah mulai menerapkan CSP, ketidaklengkapan direktif seperti ketiadaan default-src dan penggunaan wildcard justru melemahkan perlindungan yang seharusnya diberikan. Ketiadaan header HSTS dan X-Content-Type-Options juga menambah potensi risiko terhadap serangan downgrade HTTPS dan MIME sniffing. Namun, perlu dicatat bahwa sebagian besar temuan ini terkonsentrasi pada satu kategori OWASP, yaitu Security Misconfiguration, yang umumnya dapat diperbaiki melalui penyesuaian konfigurasi server tanpa perlu perubahan kode aplikasi yang rumit. Dibandingkan dengan website Polres Aceh Selatan yang memiliki 16 peringatan, jumlah peringatan di Aceh Jaya memang lebih banyak, namun jenisnya cenderung lebih ringan karena tidak melibatkan kerentanan high-risk seperti komponen usang yang sudah end of life. Hal ini memperkuat temuan bahwa postur keamanan kedua website memiliki kelemahan pada area yang berbeda, di mana Aceh Jaya perlu fokus pada penyempurnaan konfigurasi, sementara Aceh Selatan menghadapi risiko lebih serius pada rantai pasok perangkat lunak.

Kondisi yang sangat berbeda terlihat pada website Polres Aceh Selatan. Pemindaian di sini menghasilkan total enam belas peringatan, jumlah yang tepat dua kali lipat dari temuan pada website Aceh Jaya. Komposisi warnanya menunjukkan tingkat keragaman yang lebih tinggi, dengan empat peringatan kuning (*Medium*), empat peringatan biru (*Low*), dan delapan peringatan hijau (*Informational*). Keempat peringatan *Medium* yang muncul adalah Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, dan Cookie No HttpOnly Flag. Masing-masing dari peringatan ini menyoroti kelemahan yang berbeda, tetapi semuanya bermuara pada satu masalah mendasar: kurangnya perhatian terhadap konfigurasi keamanan dasar pada tingkat aplikasi.



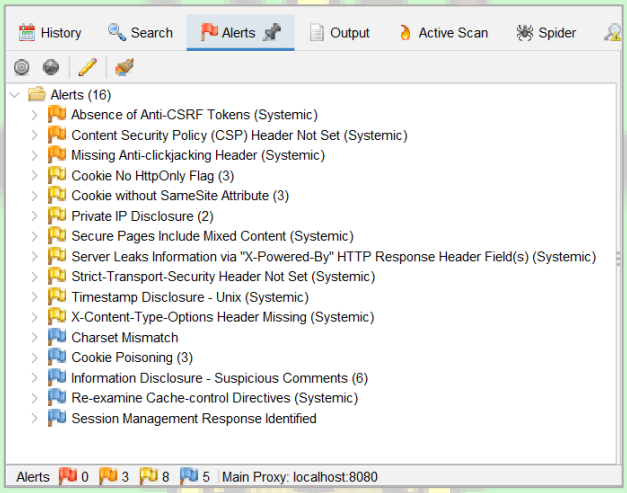
Gambar 4.5 Alerts OWASP ZAP pada website Polres Aceh Jaya

Gambar 4.5 menampilkan tampilan tab *Alerts* dari *OWASP ZAP* setelah menyelesaikan pemindaian terhadap situs Polres Aceh Jaya. Daftar peringatan yang muncul tidak terlalu panjang, dengan satu peringatan berwarna kuning yang langsung menarik perhatian di antara peringatan biru dan hijau lainnya. Peringatan kuning tersebut adalah CSP: Failure to Define Directive with No Fallback. *ZAP* mendeteksi bahwa situs ini telah memasang *header* Content-Security-Policy, namun isinya hanya sebatas frame-ancestors 'self' tanpa menyertakan direktif default-src. Aturan frame-ancestors 'self' sebenarnya sudah cukup baik untuk mencegah serangan *Clickjacking* karena hanya mengizinkan halaman ditampilkan dalam bingkai dari domain yang sama. Akan tetapi, persoalannya adalah tidak ada aturan lain yang membatasi dari mana skrip, gambar, atau stylesheet boleh dimuat.

Ketiadaan default-src berarti bahwa untuk semua jenis sumber daya yang tidak disebutkan secara eksplisit, peramban akan menerapkan kebijakan *allow-all*. Ini sama saja dengan tidak memiliki pagar untuk jenis-jenis konten tersebut. Sebagai ilustrasi, jika seorang penyerang berhasil menemukan celah untuk menyuntikkan tag gambar yang mengarah ke server asing, maka *CSP* yang longgar ini tidak akan menghalangi peramban untuk memuat gambar tersebut. Padahal, gambar itu bisa saja berisi pelacak yang memberitahu penyerang bahwa injeksi mereka berhasil. Oleh karena itu, meskipun *ZAP* hanya menempatkan temuan ini pada

tingkat *Medium* dengan warna kuning, penyempurnaan *CSP* tetap menjadi langkah yang sangat disarankan untuk memperkuat postur keamanan secara keseluruhan.

Perlu dijelaskan bahwa angka 36 yang tertera pada Gambar 4.5 merupakan jumlah keseluruhan *instance* peringatan yang dilaporkan oleh ZAP, mencakup peringatan yang muncul berulang di berbagai URL serta peringatan informatif seperti *Tech Detected*. Setelah dilakukan proses reduksi dengan menghilangkan duplikasi dan menghitung hanya peringatan unik berdasarkan jenisnya, diperoleh total delapan peringatan yang menjadi dasar analisis pada penelitian ini. Prosedur yang sama juga diterapkan pada hasil pemindaian untuk website Aceh Selatan, sehingga jumlah 16 peringatan yang dilaporkan pada Gambar 4.6 juga merupakan hasil reduksi dari total *instance* yang lebih besar.



Gambar 4.6 Alerts OWASP ZAP pada website Polres Aceh Selatan

Gambar 4.6 menyajikan situasi yang berbeda secara signifikan dari Gambar 4.5. Daftar peringatan di sini tampak lebih padat, dengan empat peringatan kuning berada di urutan teratas, disusul oleh beberapa peringatan biru dan hijau di bawahnya. Peringatan kuning pertama, Content Security Policy (CSP) Header Not Set, menunjukkan bahwa situs ini sama sekali tidak memiliki *header* CSP. Jika pada Aceh Jaya masalahnya adalah CSP yang belum sempurna, maka pada Aceh Selatan CSP-nya tidak ada sama sekali. Ini berarti tidak ada kebijakan yang membatasi sumber konten apa pun yang boleh dimuat oleh halaman. Peramban akan menerima dan mengeksekusi skrip dari mana pun, memuat gambar dari server asing mana pun, dan mengizinkan koneksi ke alamat mana pun. Kondisi ini memberikan

keleluasaan penuh bagi penyerang yang berhasil menyuntikkan konten berbahaya ke dalam halaman.

Peringatan kuning kedua, Missing Anti-clickjacking Header, berkaitan dengan ketiadaan *header* X-Frame-Options. Tanpa *header* ini, situs dapat ditampilkan di dalam bingkai (iframe) pada situs lain yang dikendalikan oleh penyerang. Serangan yang memanfaatkan teknik ini disebut *Clickjacking*, di mana pengguna dikelabui untuk mengklik sesuatu yang terlihat tidak berbahaya, padahal sebenarnya mereka sedang mengklik tombol atau tautan di situs yang asli. Untuk situs kepolisian yang mungkin memiliki halaman pengaduan atau pelaporan, serangan semacam ini bisa disalahgunakan untuk mengelabui masyarakat agar memberikan informasi pribadi tanpa sadar.

Peringatan kuning ketiga, Cookie No HttpOnly Flag, muncul karena ZAP mendeteksi adanya tiga cookie yang disetel tanpa atribut HttpOnly. Atribut HttpOnly adalah mekanisme keamanan yang mencegah cookie diakses oleh JavaScript yang berjalan di peramban. Ketika atribut ini tidak disetel, maka skrip apa pun yang berjalan di halaman termasuk skrip berbahaya yang disuntikkan melalui celah XSS dapat membaca isi cookie tersebut dan mengirimkannya ke server penyerang. Dalam kasus ini, cookie yang dimaksud adalah comment_author, comment_author_email, dan comment_author_url yang digunakan oleh WordPress untuk menyimpan data pengisi komentar. Meskipun data yang tersimpan bukanlah kredensial login, tetap saja informasi pribadi seperti nama dan alamat surel pengunjung menjadi terekspos jika terjadi serangan.

Peringatan kuning keempat, Absence of Anti-CSRF Tokens, sempat memicu kekhawatiran awal. Token *Anti-CSRF* adalah mekanisme yang mencegah serangan *Cross-Site Request Forgery*, di mana penyerang membuat permintaan berbahaya atas nama pengguna yang sedang login. Namun, setelah ditelusuri lebih lanjut pada fase validasi manual, ditemukan bahwa peringatan ini dipicu oleh formulir komentar publik. Formulir komentar tidak memerlukan otentikasi dan tidak melakukan tindakan sensitif apa pun atas nama pengguna, sehingga ketiadaan token *Anti-CSRF* pada formulir ini bukanlah sebuah kerentanan. Ini adalah contoh klasik *false positive* yang sering dihasilkan oleh pemindai otomatis, dan menjadi alasan mengapa validasi manual selalu diperlukan setelah pemindaian.

Selain peringatan kuning, terdapat juga empat peringatan biru yang memberikan gambaran tambahan tentang kelemahan konfigurasi server. Server Leaks Information via "X-Powered-By" mengonfirmasi bahwa server secara terbuka mengirimkan header X-Powered-By: PHP/7.4.33. Informasi ini memudahkan penyerang untuk langsung mengetahui versi *PHP* yang digunakan dan mencari kerentanan yang sesuai tanpa harus menebak-nebak. Strict-Transport-Security Header Not Set menunjukkan bahwa situs tidak memiliki mekanisme *HSTS* yang memaksa peramban untuk selalu menggunakan koneksi *HTTPS*. Tanpa *HSTS*, penyerang yang berada di jaringan yang sama dengan korban berpotensi melakukan serangan *downgrade* untuk mengalihkan koneksi ke *HTTP* yang tidak terenkripsi. X-Content-Type-Options Header Missing berarti peramban diizinkan untuk menebak tipe konten dari suatu berkas, sebuah praktik yang disebut *MIME-sniffing*. Jika penyerang berhasil mengunggah berkas dengan ekstensi yang tampak aman tetapi berisi konten berbahaya, peramban bisa saja menebak tipe konten yang salah dan mengeksekusinya. Cookie without SameSite Attribute menandakan bahwa *cookie* dapat dikirim dalam permintaan lintas situs, sehingga jika ada fitur sensitif yang tidak terlindungi, serangan *CSRF* bisa terjadi. Seluruh temuan ini, dari yang kuning hingga biru, melukiskan gambaran yang jelas bahwa konfigurasi keamanan di Polres Aceh Selatan memerlukan pembenahan yang menyeluruh dan mendesak.

4.3 Fase Attack: Validasi Manual dengan Burp Suite

Pemindaian otomatis menggunakan *OWASP ZAP* memang memberikan gambaran awal yang luas, namun hasilnya belum tentu sepenuhnya akurat. Beberapa peringatan bisa jadi merupakan *false positive*, sementara celah lain yang lebih samar mungkin lolos dari deteksi. Oleh karena itu, diperlukan tahap validasi manual untuk memastikan temuan mana yang benar-benar merupakan kelemahan dan untuk menggali kemungkinan adanya titik rentan lain yang tidak terdeteksi oleh alat. Pada fase ini, validasi dilakukan dengan bantuan *Burp Suite Community Edition*, yang berfungsi sebagai perantara antara peramban dan server sehingga setiap permintaan dan respons *HTTP* dapat diperiksa secara terperinci.

Tiga area utama menjadi sasaran validasi pada fase ini. Pertama, pengaturan keamanan pada *cookie* yang sebelumnya telah ditandai oleh *ZAP* pada kedua

website. Kedua, potensi serangan *Cross-Site Scripting* (XSS) pada titik-titik interaksi pengguna seperti kolom komentar dan kolom pencarian. Ketiga, kemungkinan adanya celah *SQL Injection* pada parameter yang menerima masukan dari pengguna. Seluruh pengujian dilakukan dalam batas-batas yang telah disetujui, tanpa melakukan tindakan yang dapat mengubah data atau mengganggu ketersediaan layanan.

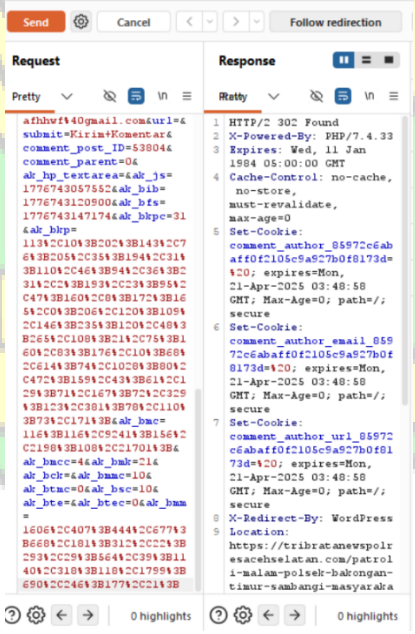
4.3.1 Validasi Keamanan Cookie

Validasi terhadap cookie diawali dengan mengamati lalu lintas HTTP saat fitur komentar digunakan. Dengan mengaktifkan fitur Intercept pada Burp Suite, permintaan yang dikirimkan ketika tombol "Kirim Komentar" ditekan dapat ditahan untuk diperiksa. Respons dari server kemudian dianalisis, terutama pada bagian header Set-Cookie. Pada website Polres Aceh Jaya, terlihat bahwa server menyetel beberapa cookie dengan nama seperti comment_author, comment_author_email, dan comment_author_url. Namun, tidak satu pun dari cookie tersebut yang dibekali dengan atribut HttpOnly ataupun Secure.

Gambar 4.7 Tangkapan layar Burp Suite yang menunjukkan respons HTTP dengan cookie tanpa flag HttpOnly pada website Polres Aceh Jaya

Gambar 4.7 menangkap momen ketika server mengirimkan balasan setelah sebuah komentar dikirim. Pada bagian Response Headers, terlihat beberapa baris Set-Cookie yang menetapkan nilai untuk cookie comment_author, comment_author_email, dan comment_author_url. Atribut yang menyertai hanya expires dan path, sementara atribut HttpOnly dan Secure sama sekali tidak muncul. Ini berarti bahwa cookie-cookie tersebut dapat diakses melalui JavaScript yang berjalan di sisi peramban, cukup dengan menggunakan perintah document.cookie.

Cookie comment_author, comment_author_email, dan comment_author_url pada kedua website disetel tanpa flag HttpOnly, sehingga tetap dapat diakses melalui JavaScript. Meskipun data yang tersimpan tidak tergolong sensitif, ketiadaan flag ini tetap menyisakan celah: jika sewaktu-waktu terjadi kerentanan Cross-Site Scripting (XSS), penyerang dapat mencuri cookie tersebut dan memanfaatkannya untuk phishing yang lebih meyakinkan atau membangun profil pengguna. Pada website Polres Aceh Selatan, kelemahan ini semakin terlihat karena server juga mengekspos header X-Powered-By: PHP/7.4.33, yang secara terbuka mengumumkan versi PHP yang sudah sangat usang dan tidak lagi didukung.



Gambar 4.8 Tangkapan layar Burp Suite yang menunjukkan respons HTTP dengan cookie tanpa flag HttpOnly dan header X-Powered-By pada website Polres Aceh Selatan

Gambar 4.8 menampilkan temuan ganda pada website Polres Aceh Selatan. Selain ketiadaan flag HttpOnly pada cookie komentar, terlihat pula baris X-

Powered-By: PHP/7.4.33 pada bagian Response Headers. Temuan ini mengonfirmasi dua hal sekaligus. Pertama, peringatan Cookie No HttpOnly Flag yang sebelumnya dilaporkan oleh OWASP ZAP adalah valid dan berlaku untuk kedua website, bukan hanya Aceh Selatan. Kedua, informasi versi PHP yang terekspos memperkuat dugaan awal pada fase Discovery bahwa situs ini berjalan di atas perangkat lunak yang sudah kedaluwarsa.

Paparan versi *PHP* seperti ini adalah contoh klasik dari kebocoran informasi yang tidak perlu. Bagi penyerang, mengetahui versi persis dari perangkat lunak yang digunakan akan sangat mempersempit pilihan eksploitasi yang mungkin dicoba. Mereka tidak perlu membuang waktu untuk menguji kerentanan yang hanya berlaku pada versi lain, melainkan bisa langsung mengarahkan serangan ke kelemahan yang sudah terdokumentasi untuk *PHP* 7.4. Dalam kasus ini, karena versi tersebut sudah *End of Life*, setiap kerentanan baru yang ditemukan tidak akan pernah diperbaiki, sehingga server akan terus rentan untuk selamanya. Menonaktifkan *header* X-Powered-By atau mengaturnya untuk tidak menampilkan versi adalah langkah mitigasi sederhana yang dapat segera dilakukan untuk mengurangi keterbukaan informasi ini.

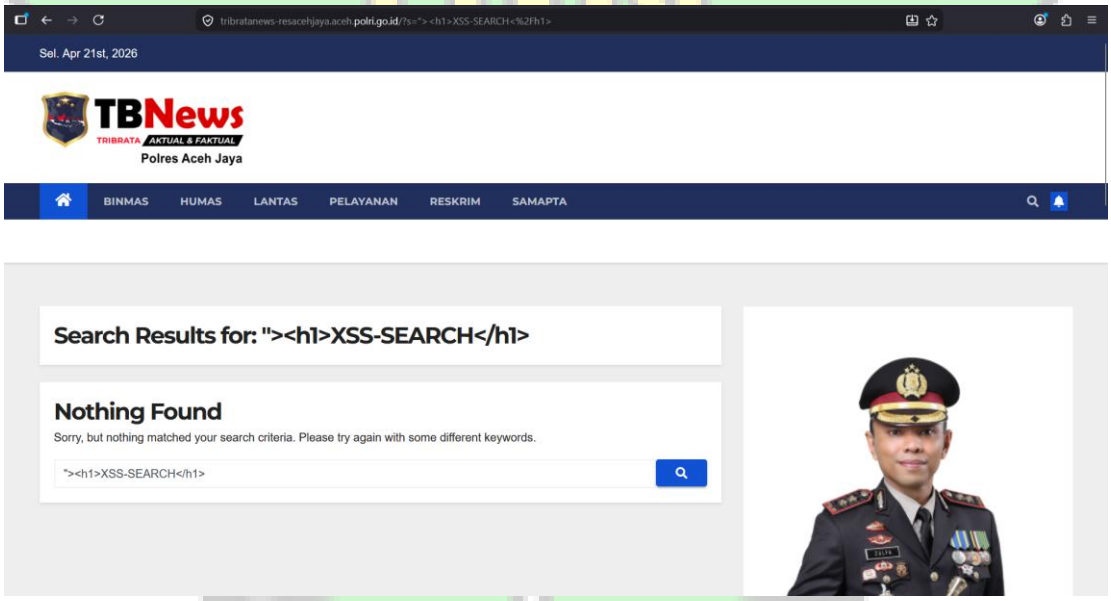
4.3.2 Validasi Cross-Site Scripting (XSS) dan HTML Injection

Setelah memeriksa aspek *cookie*, pengujian berlanjut ke titik-titik yang memungkinkan terjadinya serangan *Cross-Site Scripting*. Kolom komentar menjadi sasaran pertama karena merupakan salah satu fitur paling umum yang memungkinkan pengguna mengirimkan teks bebas. Pengujian dilakukan dengan menyisipkan muatan sederhana berupa tag *HTML* <h1>XSS-TEST-HEADING</h1> ke dalam isi komentar. Hasilnya, pada kedua website, muatan tersebut ditampilkan sebagai teks polos tanpa efek format apa pun. Ini menunjukkan bahwa *WordPress* telah melakukan *output encoding* dengan baik, mengubah karakter khusus seperti tanda kurang dari dan lebih dari menjadi entitas *HTML* yang aman.

Keberhasilan sistem dalam menangkal muatan *HTML* sederhana pada kolom komentar memberikan rasa aman, tetapi tidak berarti pengujian bisa dihentikan begitu saja. Seringkali, kerentanan *XSS* tidak muncul di fitur utama seperti komentar, melainkan di bagian-bagian lain yang kurang mendapatkan perhatian.

Oleh karena itu, pengujian perlu diperluas ke area lain yang juga menerima masukan dari pengguna.

Pengujian berikutnya menyasar kolom pencarian pada website Polres Aceh Jaya. Berbeda dengan Aceh Selatan yang tidak memiliki fitur pencarian publik, situs Aceh Jaya menyediakan kotak pencarian di bagian atas halaman. Muatan "><h1>XSS-SEARCH</h1> dimasukkan ke dalam kolom pencarian dan permintaan dikirim. Hasil yang muncul di halaman pencarian ternyata berbeda dari yang terjadi pada kolom komentar. Alih-alih menampilkan teks biasa, judul halaman hasil pencarian justru menampilkan muatan tersebut secara utuh, lengkap dengan tanda kutip dan tag-nya: *Search Results for: "<h1>XSS-SEARCH</h1>"*. Lebih jauh, tag <h1> benar-benar dirender oleh peramban sehingga teks "XSS-SEARCH" muncul dengan ukuran huruf yang jauh lebih besar, layaknya sebuah judul.



Gambar 4.9 hasil uji HTML Injection pada kolom pencarian website Polres Aceh Jaya

Gambar 4.9 merekam momen ketika muatan "><h1>XSS-SEARCH</h1> berhasil mempengaruhi tampilan halaman. Terlihat jelas bahwa teks "XSS-SEARCH" muncul dua kali: pertama pada judul halaman dengan ukuran besar, dan kedua pada bagian bawah sebagai teks biasa yang mengulangi kata kunci pencarian. Yang menjadi perhatian adalah tampilan judul yang besar tersebut. Ini membuktikan bahwa input pengguna pada parameter pencarian tidak melalui

proses *output encoding* yang memadai ketika ditempatkan di bagian judul halaman. Akibatnya, peramban menganggap tag <h1> sebagai perintah untuk mengubah gaya teks menjadi heading tingkat satu.

Fenomena ini sebenarnya lebih tepat dikategorikan sebagai HTML Injection ketimbang Cross-Site Scripting yang dapat mengeksekusi kode. Ketika pengujian dilanjutkan dengan muatan yang mengandung tag <script>alert('XSS')</script>, peramban tidak mengeksekusi skrip tersebut. Pop-up peringatan yang diharapkan tidak muncul, menandakan bahwa ada mekanisme lain yang mencegah eksekusi JavaScript, mungkin karena batasan keamanan peramban modern terhadap penyisipan skrip melalui innerHTML. Meskipun demikian, kemampuan untuk menyuntikkan tag HTML arbitrer tetaplah sebuah celah yang tidak bisa diabaikan begitu saja.

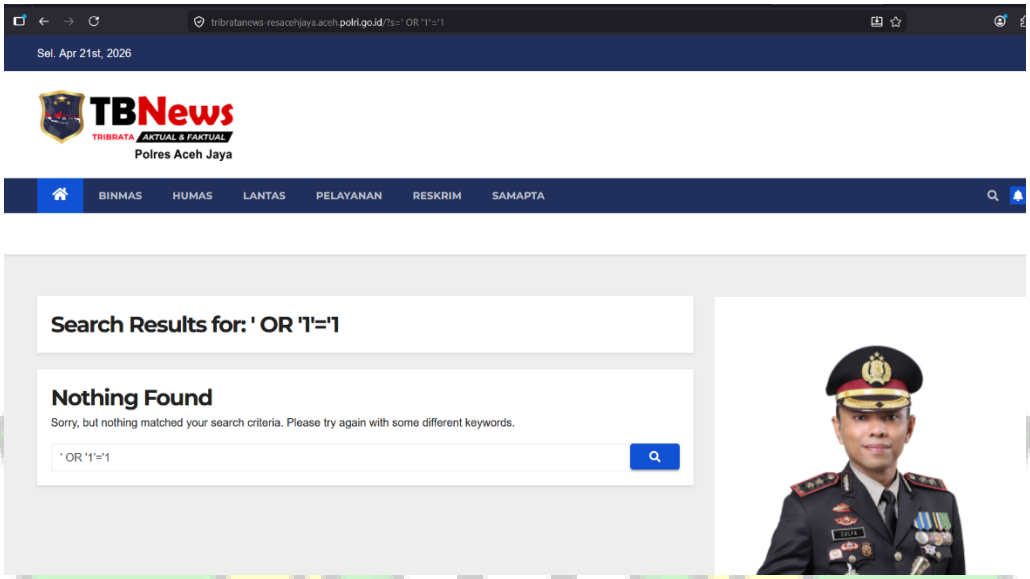
Dampak dari *HTML Injection* mungkin tidak seburuk *XSS* yang bisa mencuri sesi pengguna, tetapi tetap dapat dimanfaatkan untuk tujuan yang merugikan. Seorang penyerang dapat membuat tautan pencarian khusus yang ketika diklik akan menampilkan halaman dengan tampilan yang sudah diubah. Misalnya, mereka dapat menyisipkan gambar atau pesan palsu yang seolah-olah berasal dari pihak kepolisian, kemudian menyebarkan tautan tersebut melalui media sosial atau surel. Pengunjung yang tidak waspada mungkin akan mengira bahwa informasi tersebut resmi, padahal itu adalah hasil rekayasa. Dalam konteks situs kepolisian, kepercayaan publik adalah segalanya. Gangguan sekecil apa pun terhadap integritas tampilan dapat merusak kredibilitas institusi. Oleh karena itu, meskipun *OWASP ZAP* tidak melaporkan adanya kerentanan di sini, temuan manual ini tetap layak mendapatkan perhatian serius dari pengelola situs.

4.3.3 Validasi SQL Injection

Pengujian selanjutnya diarahkan pada potensi serangan *SQL Injection*, yaitu jenis serangan yang menyisipkan perintah *SQL* melalui parameter masukan untuk memanipulasi basis data. Titik yang diuji adalah parameter pencarian ?s= pada website Polres Aceh Jaya. Pengujian dilakukan dengan mengirimkan payload ' OR '1'='1 melalui *Burp Suite Repeater* dan mengamati respons server.

Hasil pengujian menunjukkan bahwa payload tersebut tidak menghasilkan pesan kesalahan basis data maupun perubahan perilaku halaman. Halaman hasil pencarian

tetap menampilkan "Nothing Found" seperti halnya pencarian biasa. Ini merupakan indikasi kuat bahwa aplikasi tidak rentan terhadap *SQL Injection*, karena masukan pengguna diperlakukan sebagai data, bukan sebagai perintah *SQL*. Mekanisme *prepared statements* yang digunakan oleh *WordPress* berperan penting dalam mencegah serangan injeksi jenis ini.



Gambar 4.10 hasil uji SQL Injection pada kolom pencarian website Polres Aceh Jaya

Gambar 4.10 menampilkan tangkapan layar pengujian *SQL Injection* pada parameter pencarian. Terlihat bahwa payload ' OR '1'='1 hanya menghasilkan halaman "Nothing Found" yang sama persis dengan pencarian kata kunci biasa. Tidak ada pesan *error*, tidak ada perubahan struktur halaman, dan tidak ada penundaan waktu. Temuan ini memperkuat kesimpulan bahwa situs Polres Aceh Jaya aman dari serangan *SQL Injection* pada titik yang diuji.

4.4 Fase Analisis: Klasifikasi, Penilaian Risiko, dan Rekomendasi

Sebelum masuk ke analisis, perlu dijelaskan bahwa dari total 24 peringatan unik yang dihasilkan OWASP ZAP pada kedua website (8 dari Aceh Jaya dan 16 dari Aceh Selatan), dilakukan proses konsolidasi untuk menghindari duplikasi dan memfokuskan analisis pada kerentanan yang memiliki dampak keamanan signifikan. Peringatan *Informational* dan beberapa peringatan *Low* yang bersifat minor seperti stempel waktu Unix atau pengungkapan informasi umum tidak dimasukkan dalam penilaian CVSS karena tidak memiliki bobot risiko yang

memadai. Selain itu, peringatan *CSRF* dieliminasi setelah validasi manual mengonfirmasi bahwa formulir yang dimaksud adalah formulir komentar publik yang tidak memerlukan token *CSRF*. Dengan demikian, diperoleh lima kerentanan utama yang menjadi fokus analisis risiko.

Fase terakhir ini mengintegrasikan seluruh data yang telah dikumpulkan dari ketiga fase sebelumnya. Setiap temuan, baik yang berasal dari pemindaian otomatis *OWASP ZAP* maupun validasi manual dengan *Burp Suite*, dianalisis dalam tiga langkah berurutan. Pertama, temuan diklasifikasikan ke dalam kategori OWASP Top 10 2025 untuk memahami jenis kelemahan yang dominan. Kedua, tingkat keparahan setiap kerentanan dinilai menggunakan CVSS 4.0 agar risiko dapat diukur secara kuantitatif. Ketiga, berdasarkan hasil klasifikasi dan penilaian tersebut, disusun rekomendasi perbaikan yang terprioritaskan untuk menjadi acuan bagi pengelola sistem.

4.4.1 Analisis Kerentanan Berdasarkan OWASP Top 10 2025

Dari keseluruhan proses pengujian, terdapat tiga kategori OWASP Top 10 2025 yang secara langsung bersinggungan dengan temuan pada kedua website. Kategori-kategori tersebut adalah A02:2025 – *Security Misconfiguration*, A03:2025 – *Software Supply Chain Failures*, dan A05:2025 – *Injection*. Pemetaan temuan ke dalam keempat kategori ini dirangkum dalam Tabel 4.1 berikut.

Tabel 4.1 Pemetaan Temuan ke dalam OWASP Top 10 2025

Kategori OWASP 2025	**Temuan Spesifik**	**Website Terdampak**	**Tingkat Risiko (CVSS)**
A02: *Security Misconfiguration*	Konfigurasi CSP tidak lengkap (tanpa *default-src*, gunakan *wildcard*, *unsafe-inline*) serta header *X-Frame-Options*, HSTS, dan *X-Content-Type-Options* tidak dipasang	Aceh Jaya	Medium
A02: *Security Misconfiguration*	CSP, HSTS, *X-Frame-Options* tidak dipasang sama sekali	Aceh Selatan	Medium

A02: *Security Misconfiguration*	*Cookie* tanpa flag *HttpOnly* dan *SameSite*	Aceh Jaya & Aceh Selatan	Medium
A02: *Security Misconfiguration*	*Directory listing* pada direktori *uploads*	Aceh Selatan	Low
A03: *Software Supply Chain Failures*	PHP 7.4.33 (*End of Life*)	Aceh Selatan	High
A05: *Injection*	HTML *Injection* pada kolom pencarian	Aceh Jaya	Medium

Tabel 4.1 memberikan gambaran sekilas mengenai sebaran temuan berdasarkan kategori OWASP. Terlihat bahwa kategori *Security Misconfiguration* mendominasi, dengan jumlah temuan terbanyak yang tersebar di kedua website. Sementara itu, temuan dengan tingkat risiko paling tinggi berada pada kategori *Software Supply Chain Failures*, yang hanya ditemukan pada website Polres Aceh Selatan. Pemetaan ini membantu dalam menentukan prioritas penanganan, karena perbaikan pada kategori dengan risiko tinggi tentu harus didahulukan. Berikut adalah pembahasan rinci untuk masing-masing kategori.

A. A02:2025 – Security Misconfiguration

Kategori ini menduduki peringkat kedua dalam daftar OWASP Top 10 2025, naik signifikan dari posisi kelima pada edisi sebelumnya. Kenaikan ini mencerminkan kenyataan bahwa kesalahan konfigurasi masih menjadi sumber utama kerentanan pada aplikasi web modern. *Security Misconfiguration* mencakup berbagai bentuk kelalaian, mulai dari penggunaan kredensial bawaan, pengaturan *header* keamanan yang tidak lengkap, hingga eksposur informasi sensitif melalui pesan kesalahan atau *banner* layanan. Inti dari kategori ini adalah adanya fitur keamanan yang tersedia tetapi tidak diaktifkan atau tidak dikonfigurasi dengan benar, sehingga pertahanan yang seharusnya ada menjadi tidak berfungsi sebagaimana mestinya.

Pada penelitian ini, kategori *Security Misconfiguration* menjadi yang paling dominan dan ditemukan pada kedua website, meskipun dengan karakteristik yang berbeda. Pada website Polres Aceh Jaya, meskipun beberapa *header* keamanan

sudah mulai diterapkan, konfigurasinya masih jauh dari optimal. *Content Security Policy* (CSP) telah diaktifkan, namun tidak menyertakan direktif *default-src* yang berfungsi sebagai aturan bawaan, sehingga setiap jenis sumber daya yang tidak diatur secara spesifik tetap diizinkan dimuat dari mana pun. Selain itu, CSP masih menggunakan *wildcard* (*) serta mengizinkan *unsafe-inline* untuk *script* dan *style*, yang secara signifikan melemahkan perlindungan terhadap serangan *Cross-Site Scripting* (XSS). Header *X-Frame-Options*, *Strict-Transport-Security* (HSTS), dan *X-Content-Type-Options* juga tidak ditemukan, membuat situs rentan terhadap *Clickjacking*, pembajakan koneksi HTTPS, dan *MIME sniffing*. Sementara itu, website Polres Aceh Selatan justru tidak memasang satu pun *header* keamanan dasar CSP, HSTS, *X-Frame-Options*, maupun *X-Content-Type-Options* sama sekali tidak ditemukan. Kondisi ini membuat situs kehilangan seluruh lapisan pertahanan tambahan di sisi peramban. Kedua website juga sama-sama mengekspos *cookie* tanpa atribut *HttpOnly* dan *SameSite*, yang memudahkan pencurian data melalui skrip jika sewaktu-waktu ditemukan celah XSS..

Jika ditarik benang merahnya, akar masalah dari semua temuan ini bukanlah pada kerentanan kode yang kompleks, melainkan pada kurangnya perhatian terhadap pengaturan keamanan dasar yang seharusnya menjadi lapisan pertahanan pertama sebuah aplikasi web. Pengelola situs, baik dari pihak kepolisian maupun penyedia layanan hosting, tampaknya lebih fokus pada ketersediaan konten dan fungsionalitas, sementara aspek penguatan server (*hardening*) belum menjadi prioritas. Padahal, menerapkan *header* keamanan yang direkomendasikan OWASP adalah langkah yang relatif mudah dan tidak memerlukan perubahan kode yang rumit, cukup dengan menambahkan beberapa baris konfigurasi pada server Apache atau LiteSpeed.

Selain pada header keamanan, kelemahan konfigurasi juga terlihat pada pengaturan cookie yang disetel oleh WordPress. Cookie comment_author, comment_author_email, dan comment_author_url yang digunakan untuk menyimpan data pengisi komentar tidak dilengkapi dengan atribut HttpOnly dan SameSite. Ketiadaan HttpOnly memungkinkan cookie ini diakses melalui JavaScript, yang membuka peluang pencurian data jika sewaktu-waktu ditemukan celah XSS. Sementara itu, ketiadaan SameSite membuat cookie ini rentan

dikirimkan dalam permintaan lintas situs. Meskipun cookie ini tidak menyimpan kredensial autentikasi, pengaturan yang longgar ini tetap merupakan kelalaian konfigurasi yang dapat memperbesar dampak dari kerentanan lain.

B. A03:2025 – Software Supply Chain Failures

Kategori ini merupakan evolusi dari kategori *Vulnerable and Outdated Components* pada edisi sebelumnya. Cakupannya kini diperluas, tidak hanya terbatas pada komponen yang memiliki kerentanan publik, tetapi juga mencakup risiko yang muncul dari seluruh rantai pasok perangkat lunak, termasuk ketergantungan terhadap pustaka pihak ketiga, penggunaan perangkat lunak yang sudah tidak didukung, hingga integrasi dengan layanan eksternal yang tidak tepercaya. Dalam konteks penelitian ini, temuan yang paling relevan dengan kategori ini adalah penggunaan *PHP* versi 7.4.33 pada website Polres Aceh Selatan.

Seperti yang telah diungkap pada fase *Discovery* dan dikonfirmasi kembali melalui *header* X-Powered-By pada respons *Burp Suite*, server yang menaungi situs Aceh Selatan masih berjalan di atas *PHP* 7.4.33. Versi ini telah resmi memasuki masa *End of Life* sejak 28 November 2022, yang berarti tidak ada lagi pembaruan keamanan, perbaikan *bug*, maupun tambalan untuk kerentanan baru yang ditemukan setelah tanggal tersebut. Meskipun inti *WordPress* yang digunakan sudah versi terbaru, fondasi tempat aplikasi itu berpijak tetaplah rapuh. Setiap kerentanan yang muncul pada *PHP* 7.4 setelah masa dukungannya berakhir akan tetap terbuka selamanya, tanpa ada perbaikan resmi dari pengembang.

Risiko yang ditimbulkan oleh komponen usang semacam ini tidak bisa dianggap enteng. Penyerang yang berhasil mengidentifikasi versi *PHP* yang digunakan dapat langsung merujuk ke basis data kerentanan publik seperti *CVE Details* untuk mencari eksploitasi yang sesuai. Jika ditemukan celah yang memungkinkan eksekusi kode dari jarak jauh, maka seluruh server bisa diambil alih. Dampaknya tidak lagi terbatas pada deface atau pencurian data kecil, melainkan dapat berujung pada kompromi total terhadap sistem. Dalam konteks situs kepolisian yang menyimpan informasi strategis dan menjadi wajah institusi di dunia maya, skenario semacam ini adalah risiko yang sama sekali tidak bisa ditoleransi. Oleh karena itu, temuan ini mendapatkan prioritas tinggi dalam rekomendasi perbaikan.

Selain pada tingkat runtime PHP, analisis terhadap komponen plugin WordPress juga dilakukan sejauh yang dimungkinkan oleh pendekatan black box. WhatWeb mendeteksi beberapa plugin yang terpasang, antara lain Contact Form 7, Elementor, MetaSlider, dan Akismet. Pemeriksaan terhadap basis data kerentanan publik seperti WPVulnDB dan CVE dilakukan pada April 2026, dan tidak ditemukan kerentanan kritis yang belum ditambal untuk versi-versi terbaru dari plugin tersebut. Namun, perlu dicatat bahwa tanpa akses ke panel administrasi, versi pasti setiap plugin tidak dapat diverifikasi secara langsung. Oleh karena itu, penilaian ini bersifat indikatif dan hanya berdasarkan asumsi bahwa plugin diperbarui secara rutin seiring dengan pembaruan inti WordPress. Pengecekan versi plugin secara akurat memerlukan pendekatan grey box atau white box yang berada di luar ruang lingkup penelitian ini.

C. A05:2025 – Injection

Kategori *Injection* tetap bertahan dalam daftar sepuluh besar, meskipun posisinya sedikit menurun ke peringkat kelima. Kategori ini mencakup berbagai bentuk serangan yang melibatkan penyisipan data tidak tepercaya ke dalam interpreter, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), *Command Injection*, dan sejenisnya. Pada penelitian ini, pengujian terhadap kerentanan injeksi dilakukan pada beberapa titik yang memungkinkan, dengan hasil yang cukup beragam.

Untuk *SQL Injection*, pengujian yang dilakukan pada parameter pencarian dan parameter URL artikel tidak membuahkan hasil yang mengkhawatirkan. Tidak ditemukan pesan kesalahan basis data, perubahan struktur halaman, maupun penundaan waktu yang mencurigakan. Hal ini mengindikasikan bahwa *WordPress* telah menggunakan mekanisme *prepared statements* atau sanitasi masukan yang memadai dalam menangani kueri ke basis data. Temuan ini adalah kabar baik dan menunjukkan bahwa inti CMS modern memang sudah cukup matang dalam menangkal serangan injeksi klasik.

Namun, cerita yang berbeda muncul pada pengujian *Cross-Site Scripting* terhadap kolom pencarian website Polres Aceh Jaya. Seperti yang telah diuraikan secara rinci pada Subbab 4.3, celah *HTML Injection* berhasil diidentifikasi. Meskipun muatan *JavaScript* tidak tereksekusi karena batasan

peramban, kemampuan untuk menyuntikkan tag *HTML* arbitrer tetaplah sebuah kelemahan yang termasuk dalam spektrum *Injection*. Ketiadaan *output encoding* pada bagian judul hasil pencarian memungkinkan penyerang untuk mengubah tampilan halaman, menyisipkan tautan palsu, atau melakukan serangan *phishing* yang lebih meyakinkan. Temuan ini menjadi pengingat bahwa kerentanan injeksi tidak selalu berbentuk *SQL Injection* yang dramatis. Kadang, celah kecil pada penanganan keluaran di antarmuka pengguna pun dapat menjadi pintu masuk bagi serangan yang merusak kepercayaan publik.

Keenam kategori OWASP Top 10 2025 lainnya—yaitu A01: *Broken Access Control*, A04: *Cryptographic Failures*, A06: *Insecure Design*, A08: *Software or Data Integrity Failures*, A09: *Security Logging & Alerting Failures*, dan A10: *Mishandling of Exceptional Conditions*—telah diperiksa dalam ruang lingkup pengujian ini namun tidak ditemukan kerentanan yang signifikan. Ketiadaan temuan pada A01 lebih disebabkan oleh keterbatasan pengujian *black box* yang tidak memiliki akses ke panel administrasi atau mekanisme otentikasi internal. Kategori A04 tidak terpicu karena kedua website telah menggunakan HTTPS secara penuh. Kategori A06, A08, A09, dan A10 lebih berkaitan dengan kelemahan desain, integritas data, pencatatan log, serta penanganan kesalahan yang memerlukan akses ke kode sumber atau konfigurasi internal untuk dapat dinilai secara menyeluruh. Dengan demikian, ketiadaan temuan pada kategori-kategori tersebut tidak serta-merta menjamin ketiadaannya, melainkan merefleksikan batasan pendekatan *black box* yang digunakan dalam penelitian ini.

Pemetaan temuan ke dalam kerangka OWASP Top 10 2025 ini memberikan perspektif yang lebih terang mengenai prioritas perbaikan. Kategori *Security Misconfiguration* dan *Software Supply Chain Failures* menjadi dua area yang paling mendesak untuk ditangani, terutama pada website Polres Aceh Selatan. Sementara itu, kategori *Injection* muncul dengan tingkat keparahan yang lebih rendah, tetapi tetap memerlukan perhatian karena dapat menjadi batu loncatan bagi serangan yang lebih besar.

Sebagai bagian dari analisis komparatif yang telah ditetapkan dalam metodologi penelitian, berikut disajikan perbandingan ringkas postur keamanan

kedua website. Tabel 4.2 merangkum perbedaan utama antara Polres Aceh Jaya dan Polres Aceh Selatan berdasarkan seluruh temuan yang telah dibahas sebelumnya.

Tabel 4.2 Perbandingan Postur Keamanan Kedua Website

Aspek	**Polres Aceh Jaya (.go.id)**	**Polres Aceh Selatan (.com)**
Total Alerts ZAP (unik)	36 (15 relevan)	16
Temuan High	0	1 (PHP *End of Life*)
Temuan Medium	4 (CSP *wildcard*, *no fallback*, *missing XFO*, *missing token CSRF*)	4
Versi PHP	Tersembunyi (*X-Powered-By* tidak ada)	7.4.33 (terekspos, *End of Life*)
Header Keamanan	Tidak lengkap (CSP dengan *wildcard*/*unsafe-inline*, tanpa *default-src*, HSTS, *X-Content-Type-Options*, *X-Frame-Options* tidak dipasang)	Tidak ada sama sekali
Postur Perimeter (Nmap)	Port terbuka + *tcpwrapped*	*Full stealth* (semua *filtered*)
Web Server	Apache	LiteSpeed
Keamanan Cookie	Tanpa *HttpOnly* & *SameSite*	Tanpa *HttpOnly* & *SameSite*
Kerentanan Injeksi	HTML *Injection* (pencarian)	Tidak ditemukan

Tabel 4.2 memperlihatkan perbandingan yang menarik antara kedua website. Polres Aceh Selatan unggul dalam keamanan perimeter dengan konfigurasi *full stealth*, namun memiliki kelemahan signifikan pada perangkat lunak usang dan ketiadaan *header* keamanan. Sebaliknya, Polres Aceh Jaya memiliki perimeter yang sedikit lebih terbuka, tetapi menunjukkan pengelolaan perangkat lunak yang lebih modern dengan versi PHP terkini. Meskipun demikian, konfigurasi keamanan aplikasinya masih memerlukan perbaikan signifikan, terutama pada kelengkapan *header* keamanan dan optimalisasi CSP. Menariknya, perbedaan jenis domain .go.id untuk instansi pemerintah dan .com untuk komersial tidak serta-

merta mencerminkan postur keamanan yang lebih baik pada domain pemerintah. Justru website dengan domain .com (Aceh Selatan) memiliki keamanan perimeter yang lebih ketat, meskipun lemah di sisi pemeliharaan perangkat lunak. Hal ini menunjukkan bahwa faktor pengelolaan dan pemeliharaan lebih menentukan keamanan sebuah website dibandingkan jenis domain yang digunakan.

4.4.2 Penilaian Risiko Menggunakan CVSS 4.0

Setelah seluruh kerentanan berhasil diidentifikasi dan diklasifikasikan ke dalam kategori OWASP Top 10 2025, langkah berikutnya adalah melakukan penilaian kuantitatif terhadap tingkat keparahan masing-masing temuan. Untuk keperluan ini, penelitian menggunakan standar *Common Vulnerability Scoring System* (CVSS) 4.0 yang dirilis secara resmi oleh *Forum of Incident Response and Security Teams* (FIRST) pada 1 November 2023. Standar ini dipilih karena kemampuannya dalam memberikan skor numerik yang tidak hanya didasarkan pada karakteristik bawaan kerentanan, tetapi juga mempertimbangkan faktor kematangan eksploitasi serta konteks lingkungan tempat sistem beroperasi.

CVSS 4.0 merupakan kerangka kerja terbuka untuk mengomunikasikan karakteristik dan tingkat keparahan kerentanan perangkat lunak. Skor yang dihasilkan berkisar antara 0 hingga 10, di mana nilai 0 menunjukkan tidak ada dampak keamanan yang signifikan, sedangkan nilai 10 merepresentasikan tingkat keparahan paling kritis. Secara kualitatif, skor tersebut dipetakan ke dalam empat tingkatan: *Low* (0,1–3,9), *Medium* (4,0–6,9), *High* (7,0–8,9), dan *Critical* (9,0–10,0). CVSS 4.0 terdiri dari empat kelompok metrik, yaitu *Base*, *Threat*, *Environmental*, dan *Supplemental*. *Base Metrics* mengukur karakteristik intrinsik kerentanan yang bersifat tetap sepanjang waktu. *Threat Metrics* menyesuaikan skor berdasarkan ketersediaan kode eksploitasi di dunia nyata. *Environmental Metrics* mempertimbangkan kontrol keamanan yang sudah ada serta tingkat kepentingan aset bagi organisasi. *Supplemental Metrics* memberikan informasi tambahan yang tidak memengaruhi skor akhir tetapi berguna untuk analisis lebih lanjut.

Dalam penelitian ini, penilaian risiko dilakukan dengan mengombinasikan *Base Metrics*, *Threat Metrics*, dan *Environmental Metrics* untuk menghasilkan skor akhir yang mencerminkan risiko aktual dalam konteks situs

kepolisian. Perhitungan dilakukan menggunakan kalkulator resmi CVSS 4.0 yang disediakan oleh FIRST di alamat https://www.first.org/cvss/calculator/4.0. Hasil penilaian untuk setiap kerentanan utama yang ditemukan pada kedua website dirangkum dalam Tabel 4.3.

Tabel 4.3 Penilaian Risiko CVSS 4.0 untuk Temuan Utama

No	Kerentanan	Objek	CVSS 4.0 Vector String	Final Score	Tingkat Keparahan
1	PHP 7.4.33 *End of Life* (A03)	Aceh Selatan	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/CR:H/IR:H/AR:M	8,2	*High*
2	*HTML Injection* pada Pencarian (A05)	Aceh Jaya	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:M/IR:H/AR:M	5,9	*Medium*
3	*Missing Security Headers* (A02)	Aceh Selatan	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/CR:M/IR:M/AR:M	5,6	*Medium*
4	*Cookie* tanpa *HttpOnly* & *SameSite* (A02)	Aceh Jaya & Aceh Selatan	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:M/IR:L/AR:L	5,1	*Medium*
5	*CSP Misconfiguration* (A02)	Aceh Jaya	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/CR:M/IR:M/AR:M	4,8	*Medium*
6	*Missing Security Headers (HSTS, X-Content-Type-Options, X-Frame-Options)*	Aceh Jaya	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/CR:M/IR:M/AR:M	5,1	*Medium*

Dari Tabel 4.3 terlihat bahwa hanya ada satu kerentanan yang mencapai tingkat *High*, yaitu penggunaan PHP 7.4.33 yang sudah tidak didukung pada website Polres Aceh Selatan, dengan skor 8,2. Sisanya berada pada

tingkat *Medium* dengan rentang skor 4,0 hingga 6,9. Meskipun sebagian besar temuan berada pada kategori *Medium*, bukan berarti dapat diabaikan begitu saja. Akumulasi dari beberapa kerentanan tingkat menengah dapat menciptakan rantai serangan yang dampaknya setara atau bahkan melebihi satu kerentanan kritis.

Sebagai penjelasan atas vector string yang tercantum pada Tabel 4.3, digunakan sejumlah singkatan metrik CVSS 4.0 yang menggambarkan karakteristik setiap kerentanan. AV (*Attack Vector*) menunjukkan dari mana serangan dapat dilakukan, dengan nilai N berarti melalui jaringan (*Network*). AC (*Attack Complexity*) menunjukkan tingkat kesulitan serangan, dengan L berarti rendah (*Low*) dan H berarti tinggi (*High*). AT (*Attack Requirements*) menandakan adanya syarat khusus untuk melancarkan serangan, dengan N berarti tidak ada (*None*). PR (*Privileges Required*) menunjukkan apakah penyerang memerlukan hak akses tertentu, dengan N berarti tidak diperlukan (*None*). UI (*User Interaction*) menunjukkan apakah korban perlu terlibat, dengan N berarti tidak perlu, P berarti pasif, dan A berarti aktif. Dampak terhadap sistem diukur melalui VC (*Confidentiality*), VI (*Integrity*), dan VA (*Availability*), dengan N berarti tidak berdampak (*None*), L berarti rendah (*Low*), dan H berarti tinggi (*High*). E (*Exploit Maturity*) menunjukkan ketersediaan kode eksploitasi, dengan A berarti sudah diserang (*Attacked*), P berarti baru sebatas bukti konsep (*Proof-of-Concept*), dan U berarti belum dilaporkan (*Unreported*). CR, IR, dan AR (*Confidentiality, Integrity, Availability Requirement*) menunjukkan tingkat kepentingan aset bagi organisasi, dengan L berarti rendah, M berarti sedang, dan H berarti tinggi.

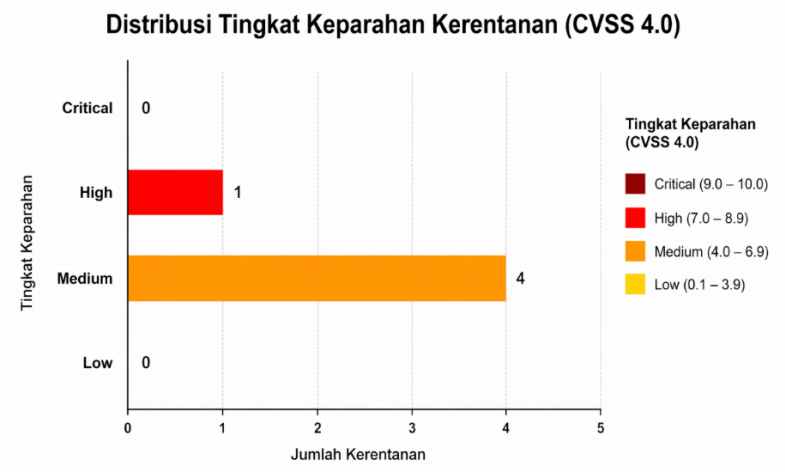
Kerentanan *PHP End of Life* pada Aceh Selatan mendapatkan skor akhir 8,2 yang menempatkannya pada batas atas kategori *High*. Skor ini diberikan karena kerentanan ini dapat dieksploitasi dari jaringan (AV:N), memiliki kompleksitas serangan yang rendah (AC:L), tidak memerlukan syarat khusus (AT:N), dan tidak memerlukan hak akses khusus (PR:N) serta tanpa perlu interaksi pengguna (UI:N). Dampak terhadap kerahasiaan, integritas, dan ketersediaan seluruhnya dinilai tinggi (VC:H/VI:H/VA:H) karena jika ditemukan eksploitasi yang sesuai, penyerang dapat mengambil alih server sepenuhnya. Skor ini telah mempertimbangkan *Threat Metrics* yang menunjukkan bahwa kode eksploitasi untuk kerentanan PHP 7.4 sudah tersedia secara publik (E:A), serta *Environmental Metrics* yang

menempatkan tingkat kepentingan data kepolisian pada level tinggi (CR:H/IR:H) dengan toleransi *downtime* pada level sedang (AR:M).

Sementara itu, kerentanan *HTML Injection* pada kolom pencarian Polres Aceh Jaya memperoleh skor akhir 5,9. Skor ini mencerminkan fakta bahwa serangan dapat dilakukan dari jaringan (AV:N) tanpa memerlukan otentikasi (PR:N), namun memerlukan interaksi pengguna untuk mengklik tautan (UI:P). Dampaknya terbatas pada perubahan tampilan tanpa mengubah data asli (VC:N/VI:L/VA:N). Penyesuaian *Environmental Metrics* sedikit menaikkan skor karena situs kepolisian memiliki persyaratan integritas yang tinggi (IR:H), sehingga perubahan tampilan sekecil apa pun dapat merusak kepercayaan publik. Sementara itu, *Threat Metric* ditetapkan sebagai *Proof-of-Concept* (E:P) karena belum ada laporan eksploitasi aktif tetapi konsep serangan sudah dipublikasikan. Ketiadaan *header* keamanan pada Aceh Selatan dan pengaturan *cookie* yang lemah pada kedua situs sama-sama berada di kisaran skor 5,1 hingga 5,6, yang mencerminkan bahwa meskipun bukan ancaman langsung, kelemahan-kelemahan ini secara signifikan mempermudah eskalasi serangan jika celah lain berhasil ditemukan. Untuk ketiga kerentanan dengan skor 5,1 hingga 5,6 tersebut, *Threat Metric* ditetapkan sebagai *Unreported* (E:U) karena belum ditemukan bukti eksploitasi publik, dengan *Environmental Metric* disesuaikan pada tingkat sedang (CR:M, IR:M, AR:M) sesuai dengan dampak masing-masing.

Sementara itu, ketiadaan *header* HSTS, *X-Content-Type-Options*, dan *X-Frame-Options* pada website Aceh Jaya menambah risiko *Clickjacking* dan *MIME sniffing* dengan skor 5,1 (*Medium*), sehingga pemasangannya disarankan bersamaan dengan perbaikan CSP.

Untuk memberikan gambaran visual mengenai distribusi tingkat keparahan kerentanan yang ditemukan, disajikan diagram yang mengelompokkan temuan berdasarkan tingkat keparahannya *High*, *Medium*, dan *Low* serta menunjukkan jumlah kerentanan pada masing-masing tingkat.



Gambar 4.11 Diagram Distribusi Tingkat Keparahan Kerentanan

Gambar 4.11 menampilkan diagram yang merangkum hasil penilaian CVSS 4.0. Sumbu horizontal menunjukkan tingkat keparahan, sementara sumbu vertikal menunjukkan jumlah kerentanan. Dari diagram tersebut, terlihat bahwa mayoritas kerentanan berada pada tingkat *Medium*, dengan satu kerentanan *High* pada website Polres Aceh Selatan. Tidak ditemukan kerentanan dengan tingkat *Critical* maupun *Low* yang signifikan dalam penilaian akhir.

Visualisasi ini menegaskan bahwa meskipun tidak ada ancaman yang bersifat sangat mendesak secara individual, akumulasi kelemahan pada tingkat menengah tetap memerlukan perhatian serius. Pengelola sistem dapat menggunakan diagram ini sebagai panduan cepat untuk memahami komposisi risiko yang dihadapi dan menentukan alokasi sumber daya yang tepat untuk penanganannya.

Hasil penilaian CVSS 4.0 ini memberikan panduan yang jelas mengenai urutan penanganan kerentanan. Perbaikan terhadap *PHP End of Life* pada website Aceh Selatan harus menjadi prioritas utama karena risikonya yang paling tinggi. Setelah itu, perhatian dapat dialihkan pada pemasangan *header* keamanan dan pengamanan *cookie*, yang meskipun skornya lebih rendah, merupakan langkah perbaikan yang relatif mudah dan memberikan peningkatan keamanan yang signifikan secara menyeluruh. Dengan mengikuti urutan prioritas ini, pengelola sistem dapat memastikan bahwa sumber daya yang terbatas dialokasikan secara optimal untuk mereduksi risiko yang paling mendesak terlebih dahulu.

4.4.3 Rekomendasi Perbaikan

Berdasarkan hasil klasifikasi OWASP Top 10 2025 dan penilaian CVSS 4.0 yang telah dilakukan, langkah selanjutnya adalah menyusun rekomendasi perbaikan yang dapat dijadikan acuan oleh pengelola sistem. Rekomendasi ini disusun berdasarkan urutan prioritas, dimulai dari kerentanan dengan skor risiko paling tinggi yang memerlukan penanganan segera, hingga perbaikan yang bersifat penguatan jangka panjang. Tabel 4.4 menyajikan ringkasan seluruh rekomendasi yang akan dijelaskan lebih rinci pada bagian selanjutnya.

Tabel 4.4 Ringkasan Rekomendasi Perbaikan Keamanan Website

No	Website	Kerentanan	Tingkat Risiko	Rekomendasi Singkat
1	Aceh Selatan	PHP 7.4.33 *End of Life*	*High*	Upgrade PHP ke versi 8.1/8.2/8.3
2	Aceh Selatan	*Header* keamanan tidak dipasang	*Medium*	Tambahkan HSTS, XFO, X-CTO, CSP di .htaccess
3	Aceh Selatan	*Directory listing* terbuka	*Low*	Tambahkan Options -Indexes di .htaccess
4	Aceh Selatan	Eksposur X-Powered-By	*Low*	Setel expose_php = Off di php.ini
5	Aceh Jaya	CSP tidak lengkap	*Medium*	Tambahkan default-src 'self' pada header CSP
6	Aceh Jaya	*Missing* HSTS, *X-Content-Type-Options*, *X-Frame-Options*	*Medium*	Tambahkan *header* HSTS, *X-Content-Type-Options*, dan *X-Frame-Options* di .htaccess
7	Aceh Jaya & Aceh Selatan	*Cookie* tanpa HttpOnly/SameSite	*Medium*	Tambahkan kode di wp-config.php dan functions.php
8	Aceh Jaya	*HTML Injection* pada pencarian	*Medium*	Lakukan *output escaping* pada search.php

Tabel 4.4 menyajikan ringkasan rekomendasi yang diurutkan berdasarkan prioritas risiko. Prioritas tertinggi diberikan pada upgrade PHP di website Polres Aceh Selatan mengingat skor CVSS-nya yang paling tinggi (8,2). Selanjutnya, pemasangan header keamanan pada server yang sama serta pengamanan cookie di kedua website menjadi langkah berikutnya karena relatif mudah diterapkan namun

memberikan dampak perlindungan yang signifikan. Untuk website Polres Aceh Jaya, fokus perbaikan diarahkan pada pemasangan header keamanan yang hilang (HSTS, X-Content-Type-Options, X-Frame-Options), penyempurnaan CSP, serta perbaikan HTML Injection pada fitur pencarian. Urutan ini memastikan bahwa sumber daya yang tersedia dialokasikan secara optimal untuk mereduksi risiko yang paling mendesak terlebih dahulu.

1. Prioritas High: Upgrade PHP pada Server WordPress Polres Aceh Selatan

Kerentanan dengan tingkat risiko paling tinggi ditemukan pada website Polres Aceh Selatan, yaitu penggunaan PHP versi 7.4.33 yang telah memasuki masa End of Life sejak November 2022. Skor CVSS 4.0 sebesar 8,2 menempatkan kerentanan ini pada kategori High, sehingga menjadi prioritas utama untuk segera ditangani. Risiko yang ditimbulkan tidak bisa dianggap ringan karena setiap kerentanan baru yang ditemukan pada PHP 7.4 tidak akan pernah menerima tambalan keamanan resmi dari pengembang. Jika terdapat celah yang memungkinkan eksekusi kode dari jarak jauh, penyerang dapat mengambil alih kendali server secara penuh.

Tindakan yang paling tepat untuk mengatasi masalah ini adalah melakukan pembaruan versi PHP ke rilis yang masih mendapatkan dukungan aktif. Saat ini, versi PHP yang direkomendasikan adalah 8.1, 8.2, atau 8.3. Sebelum melakukan pembaruan, sangat disarankan untuk melakukan pencadangan penuh terhadap seluruh berkas situs dan basis data. Setelah pencadangan selesai, pembaruan dapat dilakukan melalui panel kontrol *hosting* seperti cPanel atau Plesk, atau melalui baris perintah jika memiliki akses SSH. Khusus untuk pengguna LiteSpeed seperti yang terdeteksi pada server Aceh Selatan, proses pembaruan PHP biasanya tersedia melalui fitur *MultiPHP Manager* atau sejenisnya. Setelah pembaruan selesai, lakukan pengujian menyeluruh terhadap seluruh fitur situs untuk memastikan tidak ada masalah kompatibilitas dengan tema atau plugin yang terpasang. Apabila ditemukan kendala kompatibilitas, tim pengelola dapat mempertimbangkan untuk berkonsultasi dengan pengembang tema atau plugin terkait, atau mencari alternatif pengganti yang lebih mutakhir.

Sebagai langkah tambahan yang dapat segera dilakukan sambil menunggu proses upgrade, pengelola disarankan untuk menonaktifkan tampilan versi PHP pada header HTTP. Hal ini dapat dilakukan dengan menambahkan

baris expose_php = Off pada berkas php.ini, atau melalui panel kontrol hosting jika tersedia opsi tersebut. Dengan menyembunyikan informasi versi, setidaknya penyerang tidak dapat dengan mudah mengidentifikasi bahwa server menggunakan versi rentan.

2. Prioritas Medium: Pemasangan Header Keamanan pada Website Polres Aceh Selatan

Ketiadaan *header* keamanan dasar pada website Polres Aceh Selatan menjadi temuan dengan jumlah peringatan terbanyak dari OWASP ZAP. Skor CVSS 4.0 sebesar 5,6 menempatkannya pada tingkat Medium. Meskipun tidak secara langsung membuka celah eksploitasi, ketiadaan *header* ini membuat situs kehilangan lapisan pertahanan tambahan yang sangat penting untuk mencegah berbagai jenis serangan berbasis peramban.

Beberapa *header* yang perlu segera ditambahkan antara lain *Strict-Transport-Security* (HSTS) untuk memastikan koneksi selalu menggunakan HTTPS, *X-Frame-Options* untuk mencegah serangan *Clickjacking*, *X-Content-Type-Options* untuk mencegah *MIME-sniffing*, serta *Content-Security-Policy* (CSP) untuk membatasi sumber daya yang boleh dimuat oleh halaman. Pemasangan *header* ini dapat dilakukan dengan menambahkan beberapa baris konfigurasi pada berkas .htaccess di direktori utama WordPress. Untuk server LiteSpeed, konfigurasi yang sama juga berlaku karena LiteSpeed kompatibel dengan sintaks .htaccess milik Apache. Setelah berkas disimpan, pengujian dapat dilakukan dengan membuka situs dan memeriksa tab *Network* pada alat pengembang peramban untuk memastikan header telah muncul.

3. Prioritas Medium: Penyempurnaan Content Security Policy pada Website Polres Aceh Jaya

Website Polres Aceh Jaya telah memiliki header CSP, namun konfigurasinya belum lengkap karena tidak menyertakan direktif *default-src*, masih menggunakan *wildcard* (*), serta mengizinkan *unsafe-inline* untuk *script* dan *style*. Selain itu, header *Strict-Transport-Security* (HSTS), *X-Content-Type-Options*, dan *X-Frame-Options* juga tidak ditemukan. Skor CVSS 4.0 untuk kelemahan CSP

adalah 4,8, dan untuk ketiadaan header lainnya adalah 5,1—keduanya masih dalam kategori Medium.

Perbaikannya cukup dengan melengkapi header CSP yang sudah ada. Pengelola dapat menambahkan direktif *default-src 'self'* di awal baris CSP, menghapus *wildcard*, serta membatasi *unsafe-inline* hanya jika benar-benar diperlukan. Contoh nilai CSP yang disarankan adalah: *default-src 'self'; script-src 'self' 'unsafe-inline' https://www.google-analytics.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:;*. Konfigurasi ini akan membatasi semua sumber daya agar hanya dimuat dari domain situs itu sendiri, kecuali untuk skrip yang diizinkan dari Google Analytics dan gaya dari inline CSS. Sementara itu, header HSTS, *X-Content-Type-Options*, dan *X-Frame-Options* perlu ditambahkan melalui konfigurasi server agar situs terlindungi dari serangan *downgrade* HTTPS, *MIME sniffing*, dan *Clickjacking*. Seluruh perubahan ini dapat dilakukan pada berkas *.htaccess* atau melalui plugin keamanan yang menyediakan antarmuka pengaturan header.

4. Prioritas Medium: Pengamanan Cookie pada Kedua Website

Temuan mengenai cookie yang tidak memiliki flag HttpOnly dan SameSite terjadi pada kedua website. Skor CVSS 4.0 sebesar 5,1 menempatkannya pada tingkat Medium. Cookie yang dimaksud adalah comment_author, comment_author_email, dan comment_author_url yang disetel oleh WordPress saat pengunjung mengisi formulir komentar. Ketiadaan flag HttpOnly membuat cookie ini dapat diakses melalui JavaScript, sementara ketiadaan SameSite membuatnya rentan dikirimkan dalam permintaan lintas situs.

Perbaikan untuk masalah ini dapat dilakukan dengan menambahkan potongan kode pada berkas wp-config.php yang terletak di direktori utama WordPress. Kode @ini_set('session.cookie_httponly', true); dan @ini_set('session.cookie_secure', true); akan menginstruksikan PHP untuk menyetel flag HttpOnly dan Secure pada cookie sesi. Untuk atribut SameSite, dapat ditambahkan kode pada berkas functions.php tema yang aktif. Dengan menambahkan kode ini, setiap cookie yang dikirimkan akan secara otomatis menyertakan atribut SameSite=Lax, yang memberikan perlindungan memadai terhadap serangan CSRF tanpa mengganggu fungsionalitas normal situs.

5. Prioritas Medium: Perbaikan HTML Injection pada Pencarian Polres Aceh Jaya

Kerentanan *HTML Injection* yang ditemukan pada kolom pencarian website Polres Aceh Jaya memperoleh skor CVSS 5,9. Meskipun tidak dapat digunakan untuk mengeksekusi JavaScript, kemampuan untuk menyuntikkan tag HTML arbitrer tetap dapat disalahgunakan untuk mengubah tampilan halaman atau menyisipkan tautan palsu. Akar permasalahan terletak pada tidak adanya *output encoding* pada bagian judul hasil pencarian.

Perbaikan untuk masalah ini dilakukan pada tingkat kode tema yang menangani tampilan halaman pencarian. Berdasarkan pengujian, berkas yang bertanggung jawab atas halaman hasil pencarian adalah search.php. Pada berkas tersebut, bagian yang menampilkan judul halaman menggunakan fungsi yang mencetak langsung parameter pencarian tanpa melalui fungsi sanitasi. Untuk memperbaikinya, fungsi tersebut perlu diganti dengan fungsi yang telah melakukan *escaping*, seperti esc_html() atau esc_attr(). Sebagai contoh, kode echo get_search_query(); diubah menjadi echo esc_html(get_search_query());.

6. Prioritas Low: Menonaktifkan Directory Listing pada Website Polres Aceh Selatan

OWASP ZAP mendeteksi adanya *directory listing* pada direktori wp-content/uploads/ milik website Polres Aceh Selatan. Meskipun dampaknya tidak besar, fitur ini memudahkan penyerang untuk melihat daftar lengkap berkas yang diunggah, termasuk gambar dan dokumen yang mungkin bersifat internal. Perbaikan untuk masalah ini sangat sederhana, yaitu dengan menambahkan baris Options -Indexes pada berkas .htaccess di direktori tersebut. Setelah penambahan, akses ke direktori tanpa nama berkas spesifik akan menghasilkan halaman *forbidden* alih-alih daftar isi direktori.

7. Rekomendasi Umum untuk Peningkatan Keamanan Berkelanjutan

Di luar perbaikan spesifik yang telah dijabarkan, terdapat beberapa langkah penguatan yang dapat diterapkan untuk meningkatkan postur keamanan kedua website dalam jangka panjang. Pertama, mengaktifkan pembaruan otomatis untuk inti WordPress, tema, dan plugin. Langkah ini akan memastikan bahwa setiap

tambalan keamanan segera terpasang begitu dirilis, tanpa harus menunggu intervensi manual dari pengelola. Kedua, melakukan audit berkala terhadap akun pengguna yang memiliki akses ke panel administrasi WordPress. Hapus akun yang sudah tidak aktif, pastikan setiap akun menggunakan kata sandi yang kuat, dan aktifkan otentikasi dua faktor jika memungkinkan.

Ketiga, memasang plugin keamanan khusus seperti Wordfence atau Sucuri yang menyediakan fitur *firewall*, pemindaian malware, dan pencegahan serangan *brute force*. Keempat, melakukan pencadangan rutin terhadap seluruh berkas dan basis data, dan menyimpan hasil cadangan di lokasi yang terpisah dari server utama. Kelima, mengaktifkan pencatatan dan pemantauan aktivitas mencurigakan, baik melalui plugin keamanan maupun melalui konfigurasi server. Log aktivitas yang tercatat dapat menjadi sumber informasi berharga untuk mendeteksi upaya serangan sejak dini dan meresponsnya sebelum menimbulkan kerusakan. Terakhir, menjadwalkan asesmen keamanan secara berkala, minimal setiap enam bulan sekali, untuk mengevaluasi apakah ada kerentanan baru yang muncul akibat perubahan konfigurasi atau pembaruan perangkat lunak. Dengan menerapkan rekomendasi-rekomendasi ini, diharapkan kedua website Polres dapat mempertahankan tingkat keamanan yang optimal dan terus menjadi sarana informasi yang tepercaya bagi masyarakat.

4.5 Keterbatasan Penelitian

Setiap penelitian memiliki batasan-batasan yang perlu diakui agar hasil yang diperoleh dapat ditempatkan dalam konteks yang tepat. Keterbatasan ini tidak mengurangi validitas temuan, melainkan memberikan gambaran yang jujur mengenai ruang lingkup dan kondisi di mana penelitian ini dilaksanakan. Dengan menyadari keterbatasan yang ada, pembaca dapat memahami bahwa hasil yang disajikan merupakan potret keamanan pada suatu titik waktu tertentu dan dalam batasan-batasan metodologis yang telah ditetapkan sejak awal.

Keterbatasan pertama berkaitan dengan pendekatan pengujian yang digunakan. Penelitian ini dilakukan sepenuhnya dari perspektif eksternal atau yang sering disebut sebagai *black box testing*. Peneliti tidak memiliki akses ke kode sumber, konfigurasi server, maupun arsitektur internal dari kedua website yang menjadi objek penelitian. Seluruh informasi diperoleh melalui pengamatan dari luar,

sebagaimana yang dapat dilakukan oleh penyerang pada umumnya. Meskipun pendekatan ini realistis dan sesuai dengan tujuan penelitian, ada kemungkinan bahwa kerentanan tertentu yang hanya dapat diidentifikasi melalui akses internal seperti kesalahan logika bisnis yang kompleks atau kelemahan pada lapisan basis data yang tidak terekspos tidak dapat terdeteksi.

Keterbatasan kedua terletak pada cakupan pengujian injeksi yang dilakukan. Validasi manual dengan Burp Suite difokuskan pada titik-titik interaksi yang dapat diakses publik tanpa otentikasi, seperti kolom komentar, kolom pencarian, dan parameter URL artikel. Pengujian terhadap kerentanan *Cross-Site Scripting* dan *SQL Injection* tidak diperluas ke seluruh parameter yang mungkin ada, termasuk parameter yang hanya muncul setelah pengguna melakukan login atau berinteraksi dengan fitur tertentu. Selain itu, pengujian *SQL Injection* tidak menggunakan teknik *time-based blind* secara mendalam, melainkan terbatas pada pengamatan error dan perbedaan konten. Oleh karena itu, kemungkinan adanya kerentanan injeksi yang lebih tersembunyi tidak dapat sepenuhnya dikesampingkan.

Keterbatasan ketiga menyangkut sifat dinamis dari aplikasi web. Penelitian ini dilakukan dalam rentang waktu Oktober 2025 hingga April 2026, dengan pengujian teknis terkonsentrasi pada bulan April 2026. Website yang menjadi objek penelitian bersifat dinamis, dapat mengalami perubahan konfigurasi, pembaruan perangkat lunak, atau penambahan fitur baru sewaktu-waktu. Temuan yang dilaporkan dalam penelitian ini mencerminkan kondisi keamanan pada saat pengujian dilakukan. Tidak ada jaminan bahwa kondisi tersebut akan tetap sama di masa mendatang, terutama jika pengelola sistem melakukan perubahan tanpa disertai evaluasi keamanan yang memadai.

Keterbatasan keempat berkaitan dengan alat bantu yang digunakan. Meskipun OWASP ZAP dan Burp Suite merupakan perangkat lunak standar industri untuk pengujian keamanan, keduanya tetap memiliki keterbatasan dalam hal cakupan deteksi. OWASP ZAP, sebagai pemindai otomatis, dapat menghasilkan *false positive* maupun *false negative*. Penelitian ini telah berupaya meminimalkan *false positive* melalui validasi manual, namun kemungkinan adanya *false negative* yaitu kerentanan yang sebenarnya ada tetapi tidak terdeteksi tetap terbuka. Hal ini

terbukti dari temuan *HTML Injection* pada kolom pencarian yang sama sekali tidak dilaporkan oleh ZAP, namun berhasil diidentifikasi melalui pengujian manual.

Keterbatasan kelima adalah tidak dilakukannya pengujian terhadap aspek keamanan jaringan secara lebih mendalam. Meskipun Nmap digunakan untuk memetakan port dan layanan yang terbuka, penelitian ini tidak melakukan analisis terhadap kerentanan pada lapisan infrastruktur, seperti kemungkinan adanya serangan *Man-in-the-Middle*, kelemahan pada konfigurasi DNS, atau kerentanan pada perangkat keras jaringan yang digunakan. Fokus penelitian memang sengaja dibatasi pada lapisan aplikasi web, sehingga aspek keamanan jaringan yang lebih luas berada di luar ruang lingkup pembahasan.

Terakhir, penelitian ini tidak melibatkan wawancara atau survei terhadap pengelola sistem untuk memahami praktik keamanan dari sisi sumber daya manusia. Aspek seperti kesadaran keamanan, prosedur penanganan insiden, dan kebijakan pembaruan perangkat lunak tidak menjadi bagian dari analisis. Padahal, faktor manusia sering kali menjadi mata rantai terlemah dalam keamanan sistem informasi. Ketiadaan data kualitatif dari sisi pengelola membuat penelitian ini hanya mampu memberikan gambaran teknis, tanpa dapat menjelaskan akar penyebab organisasional dari kerentanan yang ditemukan.

Dengan menyadari seluruh keterbatasan ini, hasil penelitian hendaknya dipandang sebagai kontribusi awal yang dapat menjadi landasan bagi penelitian selanjutnya yang lebih mendalam dan komprehensif. Keterbatasan-keterbatasan tersebut juga membuka peluang bagi peneliti lain untuk melanjutkan eksplorasi pada aspek-aspek yang belum terjangkau, seperti pengujian *grey box* dengan akses terbatas, analisis kode sumber, atau evaluasi kebijakan keamanan organisasi.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis keamanan web pada website Polres Aceh Jaya dan Polres Aceh Selatan menggunakan integrasi OWASP Top 10 2025, NIST SP 800-115, dan CVSS 4.0, diperoleh kesimpulan sebagai berikut:

1. Kerentanan yang ditemukan pada kedua website mayoritas berkaitan dengan konfigurasi keamanan dasar. Berdasarkan klasifikasi OWASP Top 10 2025, kerentanan-kerentanan tersebut terpetakan ke dalam tiga kategori, yaitu A02 (*Security Misconfiguration*), A03 (*Software Supply Chain Failures*), dan A05 (*Injection*). Pada Polres Aceh Jaya ditemukan CSP yang belum optimal (tanpa *default-src*, menggunakan *wildcard* dan *unsafe-inline*), ketiadaan header HSTS, *X-Content-Type-Options*, dan *X-Frame-Options*, *cookie* tanpa *HttpOnly* dan *SameSite*, serta HTML *Injection* pada kolom pencarian. Pada Polres Aceh Selatan ditemukan PHP 7.4.33 yang sudah End of Life, ketiadaan header keamanan dasar, kebocoran versi PHP melalui X-Powered-By, directory listing terbuka, serta kelemahan cookie yang sama dengan Aceh Jaya.
2. Tingkat risiko berdasarkan CVSS 4.0 menempatkan PHP *End of Life* di *website* Aceh Selatan pada level *High* dengan skor 8,2. Empat kerentanan lainnya berada pada level *Medium* dengan skor 4,8 hingga 5,9, meliputi *HTML Injection*, ketiadaan *header* keamanan, kelemahan *cookie*, dan CSP tidak lengkap. Tidak ditemukan kerentanan level *Critical*.
3. Rekomendasi perbaikan diprioritaskan mulai dari upgrade PHP pada server WordPress di *website* Aceh Selatan, pemasangan header keamanan, pengamanan cookie di kedua website, penyempurnaan CSP di Aceh Jaya, serta perbaikan output encoding pada fitur pencarian. Dalam jangka panjang, Polda Aceh disarankan menyusun prosedur pemeliharaan keamanan yang seragam dan menjadwalkan audit berkala.
4. Sebagai temuan tambahan, perbandingan antara website dengan domain .go.id (Polres Aceh Jaya) dan domain .com (Polres Aceh Selatan)

menunjukkan bahwa jenis domain tidak serta-merta menentukan tingkat keamanan. Website dengan domain .com justru memiliki keamanan perimeter yang lebih ketat (*full stealth*), sementara website dengan domain .go.id lebih unggul dalam pemeliharaan perangkat lunak dan konfigurasi aplikasi. Hal ini mengindikasikan bahwa faktor pengelolaan teknis dan kebijakan pemeliharaan lebih berpengaruh terhadap postur keamanan dibandingkan jenis domain yang digunakan.

5.2 Saran

Berdasarkan hasil penelitian, saran yang dapat diberikan adalah sebagai berikut:

1. Bagi Polda Aceh dan jajaran Polres, prioritas utama adalah segera melakukan upgrade PHP pada server Polres Aceh Selatan. Selanjutnya, pasang *header* keamanan dasar seperti HSTS, CSP, dan X-Frame-Options, serta amankan *cookie* dengan menambahkan flag HttpOnly, Secure, dan SameSite pada kedua website. Untuk Polres Aceh Jaya, sempurnakan CSP dan perbaiki *output escaping* pada berkas search.php. Dalam jangka panjang, susun standar operasional prosedur pemeliharaan keamanan website yang seragam, mencakup pembaruan berkala, audit enam bulanan, dan peningkatan kapasitas SDM pengelola.
2. Bagi peneliti selanjutnya, disarankan untuk melakukan pengujian dengan pendekatan *grey box* atau *white box* jika memungkinkan, memperluas cakupan pengujian injeksi, menambahkan analisis kualitatif melalui wawancara dengan pengelola sistem, serta memperluas objek penelitian ke website Polres lain di wilayah Aceh.

DAFTAR PUSTAKA

Albalawi, N., Alamrani, N., Aloufi, R., Albalawi, M., Aljaedi, A., & Alharbi, A. R. (2023). The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities. *Electronics (Switzerland)*, *12*(12). https://doi.org/10.3390/electronics12122664

Angga Septiawan, G., Irawan, K. W. S., Mayasari, I., & Listartha, I. M. E. (2022). Analisis Kerentanan XSS dan Rate Limiting Pada Website SMAN 8 Denpasar Menggunakan Framework OWASP ZAP. *Jurnal Informatika Upgris*, *8*(1), 98–100. https://doi.org/10.26877/jiu.v8i1.10271

Anggraeni, D. P., Zen, B. P., & Pranata, M. (2022). *Jurnal Pertahanan SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB*. *8*(3), 497–506.

Haeruddin, Gautama Wijaya, Winata, H., Sukma Aji, & Muhammad Nur Faiz. (2024). Website Security Analysis Using Vulnerability Assessment Method. *Journal of Innovation Information Technology and Application (JINITA)*, *6*(2), 173–180. https://doi.org/10.35970/jinita.v6i2.2476

Handaya, S., & Islamadina, R. (2025). Imlementasi Penetration Testing Pada Aplikasi Web Sistem Evaluasi Data Bidang Tik Polda Aceh Menggunakan Metode Owasp Dan Nist Sp 800-115. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *9*(1), 27–41. https://doi.org/10.22373/cj.v9i1.27978

Iksal, Hayani, & A. (2024). Indonesian Journal of Education (INJOE). *Indonesian Journal of Education (INJOE)*, *4*(1), 761–774.

Khosiri, M., Hoiriyah, & Anwari. (2025). *Pengujian dan Analisis Kerentanan Keamanan Website Fakultas Teknik Universitas Islam Madura Menggunakan OWASP ZAP, Burp Suite, dan Nikto*. *11*(1), 10–16. https://ft.uim.ac.id

Maherza, S. A., Hananto, B., & Pradnyana, I. W. W. (2023). Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115. *Informatik : Jurnal Ilmu Komputer*, *19*(1), 11–27.

https://doi.org/10.52958/iftk.v19i1.4697

Salim, D. J. N. (2026). *Modeling and Simulating Cyber Attacks Using Attack Trees and Security Testing Tools : A Case Study of an ICT Department*. *5*(03), 698–708.

FIRST.org. (2023). Common Vulnerability Scoring System version 4.0 specification.

Hidayat, R., & Prasetyo, E. (2024). Evaluasi keamanan aplikasi web menggunakan OWASP ZAP dan Burp Suite pada instansi pemerintahan. *Jurnal Teknologi Informasi dan Ilmu Komputer, 11*(1), 67–76.

Isnaini, K. N., & Putranto, B. D. (2025). Penetration testing through NIST SP 800-115 and OWASP Top 10 with risk analysis using CVSS on the XY Diskominfo website. *Journal of Innovation Information Technology and Application*, 7(2).

Kurniawan, D., & Lestari, P. (2023). Analisis keamanan sistem informasi berbasis web menggunakan OWASP Top 10. *Jurnal RESTI, 7*(3), 450–458.

Maulana, A., & Fitriani, N. (2025). Pendekatan hybrid vulnerability assessment menggunakan WhatWeb, Nmap, dan OWASP ZAP pada website universitas. *Jurnal Keamanan Siber dan Teknologi Informasi, 5*(1), 1–12.

DARTAR LAMPIRAN