ANALISIS KOMPARATIF EFEKTIVITAS OWASP ZAP DAN WAPITI DALAM VULNERABILITY ASSESSMENT WEBSITE BERBASIS FRAMEWORK OWASP TOP 10

TUGAS AKHIR

Diajukan oleh :

NABILA SYAKIVE

220705083

Mahasiswa Fakultas Sains dan Teknologi

Program Studi Teknologi Informasi

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI AR-RANIRY

BANDA ACEH

2026 M / 1447 H

LEMBAR PERSETUJUAN

ANALISIS KOMPARATIF EFEKTIVITAS OWASP ZAP DAN WAPITI DALAM VULNERABILITY ASSESSMENT WEBSITE BERBASIS FRAMEWORK OWASP TOP 10

TUGAS AKHIR

Diajukan kepada Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana (S1) dalam
Ilmu/Program Studi Teknologi Informasi

Oleh:
NABILA SYAKIVE
220705083
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi Informasi

Disetujui untuk Dimunaqasyahkan Oleh:

Pembimbing I,	Pembimbing II,
Mulkan Fadhli, M.T.	Aulia Syarif Aziz, S.Kom., M.Sc.
NIP. 198811282020121006	NIP. 199305212022031001

Mengetahui,
Ketua Program Studi Teknologi Informasi

Malahayati, M.T
NIP. 198301272015032003

LEMBAR PENGESAHAN

ANALISIS KOMPARATIF EFEKTIVITAS OWASP ZAP DAN WAPITI DALAM VULNERABILITY ASSESSMENT WEBSITE BERBASIS FRAMEWORK OWASP TOP 10

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 (S1)
Dalam Program Studi Teknologi Informasi

Pada Hari/Tanggal: Selasa, 03 Februari 2026
15 Sya'ban 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,
Dr. Hendri Ahmadian, M.I.M	Nizam Akbar, S.T., M.T.
NIP. 198301042014031002	NUPTK. 2849779680130032

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	:	Nabila Syakive
NIM	:	220705083
Program Studi	:	Teknologi Informasi
Fakultas	:	Sains dan Teknologi
Judul	:	Analisis Komparatif Efektivitas OWASP Zap Dan Wapiti Dalam Vulnerability Assessment Website Berbasis Framework OWASP Top 10

Dengan ini menyatakan bahwa dalam penulisan tugas akhir ini, saya:

1. Tidak menggunakna ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakna 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 bertanggung jawab 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, 09 Februari
Yang menyatakan

Nabila Syakive

ABSTRAK

Nama	: Nabila Syakive
NIM	: 220705083
Program Studi	: Teknologi Informasi
Fakultas	: Sains dan Teknologi (FST)
Judul	: Analisis Komparatif Efektivitas Owasp Zap dan Wapiti Dalam Vulnerability Assessment Website Berbasis Framework Owasp Top 10
Tanggal Sidang	: 03 Februari 2026 / 15 Sya'ban 1447 H
Jumlah Halaman	: 81 Halaman
Pembimbing I	: Mulkan Fadhli, M.T.
Pembimbing II	: Aulia Syarif Aziz, S.Kom., M.Sc.

Penelitian ini bertujuan menganalisis dan membandingkan efektivitas serta kinerja OWASP ZAP dan Wapiti pada infrastruktur web Universitas Islam Negeri Ar-Raniry. Metode yang digunakan adalah *Dynamic Application Security Testing* (DAST) dengan pendekatan *Black Box* melalui tiga tahap iterasi pengujian pada tiga situs target dengan karakteristik berbeda. Hasil penelitian menunjukkan bahwa OWASP ZAP unggul dalam kuantitas temuan dengan total 43 *alert* yang mencakup 5-6 kategori OWASP Top 10. Sebaliknya, Wapiti menunjukkan sensitivitas lebih tinggi dalam mendeteksi celah berisiko tinggi secara konsisten dengan efisiensi waktu rata-rata 4,3 menit per situs, jauh lebih cepat dibandingkan OWASP ZAP yang memerlukan 10 menit. Penelitian ini menyimpulkan bahwa integrasi hasil dari kedua instrumen tersebut merupakan pendekatan paling optimal untuk menghasilkan profil risiko keamanan yang komprehensif bagi infrastruktur sistem informasi.

Kata Kunci: *Vulnerability Assessment*, OWASP ZAP, Wapiti, DAST, OWASP Top 10.

ABSTRACT

Name : Nabila Syakive

NIM : 220705083

Department : Information Technology

Faculty : Science and Technology

Title : Comparative Analysis of OWASP ZAP and Wapiti Effectiveness in Website Vulnerability Assessment Based on the Owasp Top 10 Framework

Date : 03 February 2026 / 15 Sya'ban 1447 H

Total Pages : 81 Pages

Suoervisor I : Mulkan Fadhli, M.T.

Supervisor II : Aulia Syarif Aziz, S.Kom., M.Sc.

This research aims to analyze and compare the effectiveness and performance of OWASP ZAP and Wapiti on the web infrastructure of Universitas Islam Negeri Ar-Raniry. The methodology employed is Dynamic Application Security Testing (DAST) using a Black Box approach across three testing iterations on three target sites with distinct characteristics. The research results indicate that OWASP ZAP is superior in the quantity of findings, with a total of 43 alerts covering 5-6 categories of the OWASP Top 10. In contrast, Wapiti demonstrated higher sensitivity in consistently detecting high-risk vulnerabilities with an average time efficiency of 4.3 minutes per site, significantly faster than OWASP ZAP, which required 10 minutes. This research concludes that integrating the results from both instruments represents the most optimal approach for generating a comprehensive security risk profile for information system infrastructure.

Keywords: *Vulnerability Assessment*, OWASP ZAP, Wapiti, DAST, OWASP Top 10.

KATA PENGANTAR

Puji syukur senantiasa penulis panjatkan ke hadirat Allah SWT, atas rahmat dan karunia-Nya yang melimpah, sehingga Proposal Skripsi dengan judul : "Analisis Komparatif Efektivitas Owasp Zap Dan Wapiti Dalam Vulnerability Assessment Website Berbasis Framework Owasp Top 10" dapat diselesaikan dengan baik dan tepat waktu.

Proposal ini disusun sebagai salah satu syarat akademis untuk menyelesaikan studi pada Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi di Universitas Islam Negeri Ar-Raniry Banda Aceh.

Penulis menyadari sepenuhnya bahwa proposal ini masih memiliki banyak kekurangan, baik dari segi materi maupun tata bahasa, mengingat keterbatasan pengetahuan dan pengalaman yang dimiliki. Oleh karena itu, kritik dan saran yang membangun dari pembaca sangat penulis harapkan demi perbaikan dan penyempurnaan di masa mendatang.

Kesempatan ini penulis gunakan untuk menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada berbagai pihak yang telah memberikan dukungan, bimbingan, dan kontribusi tak ternilai :

1. Orang tua dan keluarga tercinta yang selalu memberikan semangat, dukungan moral, dan doa yang tiada henti dari awal perkuliahan hingga tahap penyusunan proposal ini.
2. Bapak Mulkan Fadhli, M.T., dan Bapak Aulia Syarif Aziz, S.Kom., M.Sc selaku dosen pembimbing yang telah meluangkan waktu memberikan arahan, masukan dan bimbingan yang sangat berharga selama proses penyusunan proposal.
3. Kepala, Staf, dan Seluruh Jajaran Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas Islam Negeri Ar-Raniry, atas persetujuan, izin dan fasilitas yang diberikan sebagai objek penelitian yang mendukung kelancaran studi dan penelitian ini.
4. Ibu Malahayati, M.T., selaku Ketua Program Studi Teknologi Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry Banda Aceh.

5. Bapak Khairan AR, M.Kom., selaku Sekretaris Program Studi Teknologi Informasi Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh.
6. Bapak Dr. Hendri Ahmadian, M.I.M., yang bertindak sebagai pembimbing akademik penulis dan secara terus-menerus memberikan arahan dan nasihat sejak awal perkuliahan hingga saat ini.
7. Ibu Cut Ida Rahmadiana, S.Si., sebagai staf Program Studi Teknologi Informasi yang telah memberi bantuan dan dukungan dalam berbagai mata kuliah akademik.
8. Penghargaan tulus kepada para sahabat, Muhammad Aufa Faisal, Lady Dwi Ulfa, Khairunnisak, Nadya Putri, dan Fitri Mulya, serta seluruh rekan lainnya yang tidak dapat disebutkan satu per satu, atas segala semangat dan dukungan moral yang telah diberikan selama proses penyusunan proposal ini.

Sebagai penutup, besar harapan penulis agar hasil laporan ini tidak hanya memenuhi syarat akademis, tetapi juga memberikan kontribusi nyata dan bermanfaat sebagai referensi bagi pengembangan kajian keamanan siber di masa depan. Tak lupa, semoga amal baik semua pihak yang telah membantu dibalas dengan limpahan rahmat oleh Allah SWT.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan pesat teknologi informasi menjadikan website sebagai komponen vital penyedia layanan digital, memicu peningkatan risiko ancaman keamanan siber serius seperti *Structured Query Language Injection*, *Cross-Site Scripting* (XSS), dan *Broken Authentication*. Untuk mengantisipasi kerentanan tersebut, *Vulnerability Assessment* merupakan langkah krusial dalam mitigasi celah keamanan. OWASP Top 10 ditetapkan sebagai standar acuan global yang berisi sepuluh kategori kerentanan paling kritis pada aplikasi website.

Proses *Vulnerability Assessment* sangat bergantung pada efektivitas *tools* yang digunakan. Banyak *open-source scanner* seperti OWASP ZAP dan Wapiti dipilih karena kemampuan deteksinya. Namun, evaluasi komprehensif mengenai efektivitas *tool* pemindaian spesifik terhadap setiap kategori risiko OWASP Top 10 2021 masih minim (Qadir et al, 2025). Studi literatur Alazmi & De Leon (2022) menunjukkan bahwa meskipun banyak website *vulnerability scanner* tersedia, belum ada satu pun yang benar-benar mampu mendeteksi seluruh jenis kerentanan secara konsisten dan komprehensif. Penelitian Yarphel (2025) juga menyatakan masing-masing *scanner* memiliki keunggulan dan keterbatasan dalam cakupan deteksi, efisiensi, serta akurasi hasil.

Kekosongan data inilah yang mendasari urgensi penelitian ini. Studi ini berfokus pada analisis komparatif efektivitas OWASP ZAP dan Wapiti melalui pengujian pada tiga website kampus nyata, yaitu uinarraniry.siakadcloud.com, student.mahad.ar-raniry.ac.id, dan pusatbahasa.ar-raniry.ac.id.

Pemilihan ketiga website tersebut didasarkan pada perbedaan karakteristik dan struktur sistem yang dimilikinya. Website uinarraniry.siakadcloud.com merepresentasikan sistem informasi akademik dengan autentikasi pengguna dan pengelolaan data sensitif. Website student.mahad.ar-raniry.ac.id merepresentasikan portal layanan mahasiswa dengan fitur interaktif dan manajemen akun pengguna. Sementara itu, website pusatbahasa.ar-raniry.ac.id merepresentasikan website

layanan institusi dengan struktur informasi publik yang lebih statis. Variasi karakteristik tersebut memungkinkan evaluasi efektivitas OWASP ZAP dan Wapiti dalam mendeteksi celah keamanan pada berbagai tipe website secara lebih komprehensif.

Analisis ini dibutuhkan untuk menjawab secara eksplisit beberapa pertanyaan kunci yang menjadi landasan studi, yaitu : Pertama, bagaimana perbandingan efektivitas kedua *scanner* dalam mendeteksi jumlah temuan kerentanan dan tingkat risikonya; kedua sejauh mana cakupan deteksi keduanya terhadap kategori OWASP Top 10 2021; ketiga, bagaimana stabilitas kedua *scanner* tersebut; keempat, kinerja OWASP ZAP dan Wapiti berdasarkan waktu pemindaian pada target situs website kampus tersebut.

Berdasarkan kondisi tersebut, penelitian ini bertujuan melakukan analisis komparatif untuk mengetahui efektivitas kedua alat tersebut dalam mendeteksi kerentanan berdasarkan framework OWASP Top 10. Analisis komparatif ini sangat penting dilakukan untuk mengetahui efektivitas kedua alat tersebut.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana perbandingan efektivitas OWASP ZAP dan Wapiti dalam mendeteksi kerentanan pada website uinarraniry.siakadcloud.com, student.mahad.ar-raniry.ac.id, dan pusatbahasa.ar-raniry.ac.id, ditinjau dari jumlah temuan, tingkat risiko, cakupan OWASP Top 10 2021, serta stabilitas hasil deteksi?
2. Bagaimana perbandingan kinerja OWASP ZAP dan Wapiti berdasarkan waktu pemindaian pada ketiga website tersebut?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan penelitian ini adalah :

1. Menganalisis dan membandingkan efektivitas OWASP ZAP dan Wapiti dalam mendeteksi kerentanan pada website uinarraniry.siakadcloud.com, student.mahad.ar-raniry.ac.id, dan pusatbahasa.ar-raniry.ac.id, berdasarkan jumlah temuan, tingkat risiko, cakupan kategori OWASP Top 10 2021, serta stabilitas hasil deteksi.

2. Menganalisis dan membandingkan kinerja OWASP ZAP dan Wapiti berdasarkan waktu yang dibutuhkan dalam proses pemindaian pada ketiga website tersebut.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Secara akademik, penelitian ini dapat menjadi referensi dalam pengembangan kajian mengenai *vulnerability assessment* berbasis OWASP Top 10 serta menambah literatur terkait analisis komparatif alat uji keamanan web.
2. Secara praktis, hasil penelitian ini dapat membantu praktisi keamanan informasi dalam menentukan *tool* yang lebih efektif dan efisien untuk melakukan analisis kerentanan pada website.
3. Bagi institusi pendidikan, hasil penelitian ini dapat menjadi bahan evaluasi dan dasar pengambilan keputusan dalam meningkatkan keamanan sistem informasi serta website kampus.

1.5 Batasan Penelitian

Batasan dalam penelitian ini adalah sebagai berikut :

1. Penelitian hanya menggunakan OWASP ZAP versi 2.16.1 dan Wapiti versi 3.0.4
2. Objek penelitian terbatas pada tiga website Universitas Islam Negeri Ar-Raniry, yaitu website uinarraniry.siakadcloud.com, student.mahad.ar-raniry.ac.id, dan pusatbahasa.ar-raniry.ac.id.
3. *Assessment* hanya melakukan *automated scanning* tanpa eksploitasi.

BAB II
LANDASAN TEORI

2.1 Penelitian Terdahulu

Sehubungan dengan penelitian yang akan dilakukan, diperlukan sejumlah referensi dan hasil penelitian terdahulu guna menghindari adanya unsur plagiarisme maupun duplikasi. Penelitian-penelitian sebelumnya berfungsi sebagai acuan, panduan, serta dasar perbandingan bagi penelitian ini. Untuk meninjau perbedaan dan relevansi, pada bagian ini disajikan beberapa hasil penelitian terdahulu yang memiliki keterkaitan dengan topik yang dibahas. Adapun ringkasan penelitian terdahulu yang relevan dengan topik penelitian ini disajikan dalam Tabel 2.1 guna menunjukkan posisi dan kebaruan penelitian yang dilakukan.

Tabel 2. 1 Penelitian Terdahulu

Peneliti (Tahun)	Judul Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
(Rand, 2024)	*Evaluating Web Application Vulnerability Scanners: Introducing the RD-Score for Comprehensive Performance Assessment*	Memperkenalkan metrik baru "*RD-Score*" yang menggabungkan akurasi deteksi dan efisiensi sumber daya untuk menilai *scanner* web aplikasi secara komprehensif.	Persamaan : Melakukan perbandingan alat pemindai kerentanan terhadap aplikasi web. Perbedaan : Tidak spesifik membandingkan OWASP ZAP dan Wapiti langsung. Alat-alat yang diuji berbeda, dan fokusnya bukan khusus *framework* OWASP Top 10.
(Savova et al., 2021)	*Automated Web Application Scanning with*	Wapiti mendeteksi berbagai tipe kerentanan	Persamaan: Mengevaluasi alat pemindaian otomatis untuk aplikasi web dan membahas efektivitas

	Wapiti, Selenium, and SQLMap	dengan akurasi baik tetapi kadang *false positives*. Selenium berguna untuk otomasi dan *coverage* dinamis namun memiliki cakupan *vulnerabilitas* terbatas tanpa integrasi *tool* lain. SQLMap sangat spesialis dan sangat akurat untuk SQL *injection*. Disertakan tabel perbandingan performa tiap *tool*	deteksi kerentanan yang relevan dengan OWASP Top 10. Perbedaan: Fokus penelitian ini membandingkan Wapiti (DAST) dengan alat berbeda. Selenium untuk otomasi & SQLMap khusus SQLi. Bukan membandingkan langsung OWASP ZAP vs Wapiti.
(Jarupunphol et al., 2023)	*Measuring Vulnerability Assessment Tools' Performance on the University Web Application*	Hasil : Burp Suite mendeteksi lebih banyak kerentanan & *alert* dibanding ZAP, dengan proporsi kerentanan risiko tinggi	Persamaan : Mengevaluasi alat pemindai kerentanan aplikasi web menggunakan kerangka OWASP Top 10 sebagai salah satu acuan. Perbedaan : Fokus tidak mencakup Wapiti — hanya ZAP dan Burp Suite.

		lebih besar. ZAP punya proporsi kerentanan "*medium-confidence*" lebih banyak. Juga ditemukan bahwa ranking kerentanan dalam OWASP Top 10 berbeda antara alat.	
(Arnefia & Alam, 2025)	Perbandingan Efektivitas OWASP ZAP, Acunetix, Nikto Menggunakan Vulnerability Scanning Untuk Deteksi Kerentanan Aplikasi Web	Acunetix ditemukan sebagai alat paling komprehensif dengan total 20 kerentanan (75% risiko tinggi/menengah). OWASP ZAP mendeteksi 13 kerentanan dengan fokus pada kebijakan keamanan dasar seperti CSP dan header HTTP. Nikto mendeteksi 5 kerentanan yang	Persamaan: Melakukan perbandingan efektivitas alat pemindai kerentanan otomatis terhadap aplikasi web . Perbedaan: Membandingkan tiga alat (OWASP ZAP, Acunetix, dan Nikto). Objek penelitian adalah website opendata.tasikmalayakab.go.id

		berfokus pada konfigurasi server.	
(Setiawan & Fachri, 2025)	Pengujian dan Mitigasi Kerentanan Website Sistem Informasi Akademik Universitas Ma'arif Nahdlatul Ulama Kebumen dengan OWASP ZAP	Ditemukan tiga kerentanan utama: *Content Security Policy* (CSP) *Header Not Set*, HTTP to HTTPS *Insecure Transition in Form Post*, dan *Missing Anti-clickjacking Header*. Pengujian menunjukkan tidak ada celah XSS aktif dan seluruh transmisi data login telah terenkripsi melalui HTTPS.	Persamaan: Menggunakan alat bantu OWASP ZAP dan metodologi OWASP Web Security Testing Guide (WSTG) untuk menguji keamanan website akademik. Perbedaan: Hanya menggunakan satu alat pemindai (OWASP ZAP) dan tidak melakukan perbandingan dengan Wapiti. Objek penelitian spesifik pada website Sistem Informasi Akademik UMNU Kebumen
(Aziz, 2025)	Analisis Kinerja Web Server Apache, Nginx, Open Litespeed, dan Open Resty	OpenLiteSpeed menempati posisi pertama dengan performa terbaik (Response Time 45.75 ms dan Error Rate	Persamaan: Melakukan pengujian terhadap infrastruktur sistem informasi di lingkungan UIN Ar-Raniry menggunakan metode pengujian otomatis dalam lingkungan virtual. Perbedaan: Fokus penean

		0.00%), diikuti oleh Nginx, OpenResty, dan terakhir Apache dengan performa paling rendah.	adalah analisis kinerja (performance) web server menggunakan tool JMeter, bukan analisis celah keamanan (vulnerability assessment) menggunakan OWASP ZAP atau Wapiti

2.2 Landasan Teori

Adapun teori-teori yang mendukung penelitian ini adalah sebagai berikut :

2.2.1 *Vulnerability Assessment*

Gambar 2. 1 Vulnerability Assessment. Sumber : Imperva (2025)

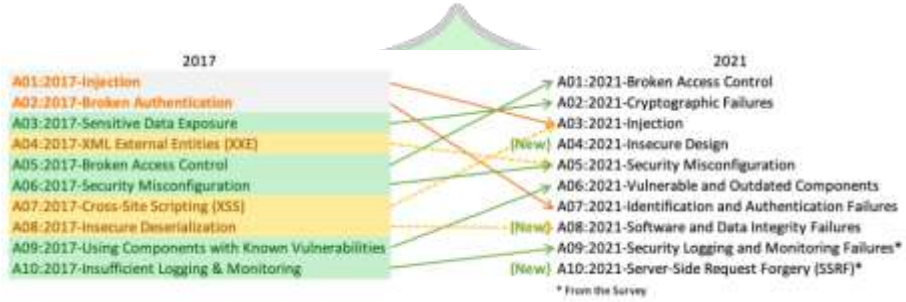
Vulnerability Assessment merupakan sebuah proses sistematis yang krusial dalam keamanan siber. Tujuan utamanya adalah untuk mengidentifikasi, mengukur, dan memprioritaskan kerentanan yang ada pada sebuah sistem. Dengan melakukan ini, *Vulnerability Assessment* berperan penting dalam menemukan celah keamanan yang berpotensi untuk dieksploitasi oleh pihak yang tidak berwenang, sebelum serangan tersebut benar-benar terjadi. Selain itu, penggunaan aplikasi pemindai kerentanan secara dini sangat diperlukan guna meminimalisir risiko eksploitasi serta menjaga ketersediaan layanan pada sebuah website (Bardian et al., 2025).

Proses *Vulnerability Assessment* merupakan sebuah siklus berkelanjutan yang terdiri dari beberapa tahapan *fundamental*. Seperti yang diilustrasikan pada Gambar 2.2.1, alur kerja metodis ini umumnya dimulai dari *Vulnerability Identification* (identifikasi kerentanan), dilanjutkan dengan *Analysis* (analisis), penilaian *Risk*

Assessment (risiko), dan diakhiri dengan *Remediation* (perbaikan). Ini memperjelas bahwa keempat tahapan ini saling terhubung dan membentuk sebuah siklus yang berulang untuk menjaga keamanan sistem secara proaktif.

Penting untuk dipahami bahwa terdapat perbedaan mendasar antara *Vulnerability Assessment* dengan *penetration testing* (uji penetrasi). Fokus utama Vulnerability Assessment adalah pada identifikasi, pengukuran, dan dokumentasi kerentanan. Berbeda dengan penetration testing, Vulnerability Assessment tidak melibatkan upaya eksploitasi aktif untuk menyimulasikan serangan secara nyata terhadap sistem.

2.2.2 OWASP Top 10 2021



Gambar 2. 2 Kategori OWASP Top 10. Sumber : Foundation (2021)

Pada gambar 2.2 terdapat 10 kategori cakupan OWASP Top 10 merupakan standar acuan keamanan aplikasi web global yang ditetapkan oleh Open Web Application Security Project. *Framework* ini mengelompokkan sepuluh kategori risiko keamanan paling kritis yang menimbulkan dampak tertinggi pada aplikasi web. Standar ini secara luas digunakan oleh pengembang dan praktisi keamanan sebagai titik awal yang paling efektif untuk mengukur postur keamanan dan meningkatkan kualitas kode. Penerapan standar ini dalam proses audit keamanan institusi terbukti krusial untuk memberikan pemahaman mendalam mengenai kondisi keamanan serta memetakan risiko pada aplikasi berbasis web secara komprehensif (Elanda & Buana, 2021).

OWASP Top 10 2021, sebagai versi terbaru, diperbaharui secara berkala sekitar tiga tahunan yang menjadi keunggulan utama untuk memastikan relevansi terhadap tren ancaman siber terkini. Namun, *framework* ini memiliki keterbatasan mendasar, standar ini bersifat terlalu umum dan minim detail pengujian untuk setiap kategori risiko.

Sebagai praktik awal yang paling efektif, penggunaan OWASP Top 10 sangat penting untuk mendorong pengembang menciptakan kode yang terjamin keamanannya dan rendah risiko (Maniraj et al., 2024).

Tabel 2. 2 Kategori OWASP Top 10

Kode	Kategori Risiko	Deskripsi Singkat
A01	*Broken Access Control*	Kesalahan dalam pembatasan hak akses pengguna terhadap data atau fungsi aplikasi.
A02	*Cryptographic Failures*	Kegagalan penerapan enkripsi yang aman sehingga data sensitif dapat terekspos.
A03	*Injection*	Serangan akibat input pengguna yang tidak divalidasi dengan baik (contoh: SQL *Injection*).
A04	*Insecure Design*	Kelemahan yang timbul akibat perancangan arsitektur aplikasi yang tidak memperhatikan prinsip keamanan.
A05	*Security Misconfiguration*	Pengaturan keamanan yang salah atau tidak sesuai *best practice* (konfigurasi default yang rentan).
A06	*Vulnerable and Outdated Components*	Penggunaan komponen atau *library* yang sudah usang dan memiliki kerentanan publik.
A07	*Identification and Authentication Failures*	Kegagalan dalam mekanisme autentikasi dan manajemen sesi.
A08	*Software and Data Integrity Failures*	Ketidakmampuan sistem menjaga integritas data dan perangkat lunak.
A09	*Security Logging and Monitoring Failures*	Tidak adanya mekanisme logging dan monitoring yang efektif untuk mendeteksi serangan.
A10	*Server-Side Request Forgery* (SSRF)	Serangan yang mengeksploitasi kemampuan server untuk melakukan permintaan ke sumber eksternal tanpa validasi.

Kategori-kategori yang terangkum dalam Tabel 2.2 menjadi kerangka acuan utama dalam penelitian ini. Secara spesifik, penelitian ini akan membandingkan kemampuan deteksi OWASP ZAP dan Wapiti terhadap jenis kerentanan yang sering muncul dalam konteks *black-box scanning*, seperti A03 *Injection* dan A07 *Identification and Authentication Failures*.

2.2.3 OWASP ZAP (Zed Attack Proxy) v2.16.1

Gambar 2. 3 OWASP ZAP. Sumber : OWASP ZAP Project (2025)

Gambar 2.2 menampilkan logo OWASP ZAP (Zed Attack Proxy), sebuah *tool open-source* terkemuka dari OWASP Foundation, berperan vital dalam metodologi *Dynamic Application Security Testing* (DAST). Alat uji ini secara spesifik dikembangkan untuk tujuan pemindaian kerentanan sehingga menjadi pilihan ideal untuk mengidentifikasi keberadaan celah keamanan pada sistem.

Guna melakukan pengujian dan analisis kerentanan, ZAP diperkuat dengan serangkaian fitur kunci yang terintegrasi. Kemampuan dasarnya mencakup *automated scanner* (pemindaian otomatis) yang berfungsi memetakan seluruh aplikasi web, serta fitur *spidering* yang secara aktif menelusuri struktur internal untuk mengungkap *endpoint* tersembunyi. Sejalan dengan hal tersebut, penelitian oleh Amirul et al (2024) menegaskan bahwa alat ini juga menawarkan kemampuan pengujian manual serta fungsionalitas pelaporan yang komprehensif untuk mendukung hasil analisis. Selain itu, ZAP juga dibekali *passive scanning* (pemindaian pasif), untuk menganalisis *traffic* (lalu lintas) tanpa perlu memodifikasi atau mengirimkan permintaan baru. Seluruh fungsionalitas ini memungkinkan pengguna membangun *assessment* keamanan yang berlapis, sesuai standar OWASP Top 10.

Dalam aksinya, OWASP ZAP dapat mengidentifikasi kerentanan seperti SQL *Injection, Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, dan Cross Site Scripting* (XSS) sehingga

menjadikannya *scanner* yang kredibel untuk mengukur postur keamanan aplikasi web modern (Umar et al., 2024).

2.2.4 Wapiti

Gambar 2. 4 Wapiti

Gambar 2.4 menunjukan *command prompt* untuk menginstal Wapiti. Wapiti adalah sebuah alat pemindai kerentanan aplikasi web yang bersifat *open-source*. Alat ini dirancang untuk beroperasi sebagai pemindai *black-box*, yang berarti Wapiti melakukan pengujian dari luar tanpa memerlukan akses ke kode sumber aplikasi, sama seperti cara kerja seorang penyerang.

Berbeda dengan OWASP ZAP yang menyediakan antarmuka pengguna grafis (GUI), Wapiti murni berbasis *command-line* (CLI). Gambar tersebut memberikan visual mengenai antarmuka operasionalnya, di mana seluruh interaksi dan eksekusi perintah dilakukan melalui terminal teks. Dalam praktiknya, alat ini secara efektif menguji berbagai titik injeksi pada aplikasi web dengan cara menyuntikkan beragam *payload* (muatan uji) melalui permintaan HTTP untuk menemukan celah keamanan.

Keunggulan utama yang membuat Wapiti sering digunakan dalam assessment adalah performanya yang tinggi dan efisiensi dalam penggunaan sumber daya sistem. Selain itu, Wapiti dikenal memiliki dukungan komprehensif untuk mendeteksi berbagai kategori serangan umum—seperti SQL *Injection, Cross-Site Scripting* (XSS), dan *File Inclusion*—serta menawarkan fleksibilitas bagi pengguna untuk menghasilkan laporan hasil pemindaian dalam beragam format misalnya HTML, XML, atau JSON.

2.2.5 Perbandingan Vulnerability Scanner

Dunia keamanan aplikasi web menawarkan beragam *vulnerability scanner*, baik yang bersifat *open-source* maupun komersial. Setiap alat dikembangkan

dengan filosofi desain, fokus, dan arsitektur yang berbeda. Akibatnya, tidak ada satu pun scanner yang dapat dianggap superior dalam segala aspek, masing-masing memiliki keunggulan dan keterbatasan yang unik, terutama dalam hal akurasi, kecepatan, dan jenis kerentanan yang dapat dideteksinya. elaksanaan vulnerability assessment menggunakan berbagai perangkat lunak pemindaian otomatis terbukti mampu memberikan hasil identifikasi celah keamanan yang lebih komprehensif serta selaras dengan standar keamanan global dibandingkan hanya mengandalkan satu metode pengujian saja (Sampurno, 2025).

Perbedaan fokus inilah yang menjadikan analisis komparatif antara OWASP ZAP dan Wapiti sangat relevan untuk dilakukan dalam penelitian ini. Untuk mengevaluasi keduanya secara objektif, efektivitas komparatif akan dinilai berdasarkan kriteria utama, yaitu Cakupan (sejauh mana kemampuan deteksi kerentanan) dan Kinerja (seberapa efisien waktu pemindaian yang dibutuhkan). Penilaian berdasarkan metrik ini sangat krusial untuk memetakan efektivitas kedua tool dalam konteks spesifik kerentanan yang diuraikan oleh *framework* OWASP Top 10.

2.2.6 *Web Application Security*

Gambar 2. 5 Web Application Security. Sumber : Jit.io (2024)

Web Application Security (Keamanan Aplikasi Web) adalah serangkaian praktik dan proses yang bertujuan melindungi data serta fungsionalitas sistem dari akses atau modifikasi ilegal. Fokus utamanya adalah memberikan perlindungan terhadap berbagai ancaman siber, seperti serangan *injection, cross-site scripting*, dan berbagai kelemahan terkait otentikasi.

Gambar 2.5 merupakan gambaran dari *Key Component of Website*. Untuk membangun pertahanan yang efektif, keamanan aplikasi web mengandalkan beberapa komponen kunci yang saling mendukung. Gambar tersebut mengilustrasikan pilar-pilar utama dalam keamanan web modern, yang mencakup *Authentication, Testing, Data Protection, Vulnerability Management,* dan *Monitoring* & *Response*. Komponen-komponen visual ini mewakili tindakan praktis yang harus diambil, seperti penjaminan *validitas input*, pengelolaan sesi yang aman, enkripsi data, konfigurasi server yang optimal, dan pemantauan berkelanjutan.

Seluruh praktik dan komponen pencegahan ini idealnya harus berlandaskan pada kerangka kerja standar industri. Penggunaan *framework* seperti OWASP Top 10 menjadi sangat penting untuk memastikan bahwa seluruh potensi risiko keamanan dapat diidentifikasi, diprioritaskan, dan dicegah secara efektif.

2.2.7 Framework OWASP

OWASP yang merupakan singkatan dari Open Web Application Security Project adalah sebuah organisasi nirlaba global. Organisasi ini berfokus pada upaya peningkatan keamanan perangkat lunak dengan menghasilkan dan memelihara berbagai kerangka kerja fundamental.

Kerangka kerja yang disediakan OWASP sangat beragam, mencakup panduan pengujian seperti OWASP Testing Guide, daftar peringkat risiko OWASP Top 10, dan alat pengujian seperti OWASP ZAP. Seluruh sumber daya ini telah diakui dan digunakan secara luas sebagai rujukan utama oleh para pengembang aplikasi dan peneliti keamanan. Berdasarkan peran sentralnya sebagai standar acuan dalam industri, *framework* OWASP ini dijadikan landasan utama dalam penelitian. *Framework* ini digunakan secara spesifik untuk membandingkan efektivitas antara OWASP ZAP dan Wapiti dalam melakukan *vulnerability assessment*.

Penelitian pada institusi pendidikan menunjukkan bahwa banyak website universitas masih memiliki kerentanan pada tingkat Medium hingga High berdasarkan standar OWASP (Hidayatulloh & Saptadiaji, 2021).

2.2.8 Antarmuka Penggunaan *Tools* Pengujian (GUI dan CLI)

OWASP ZAP dan Wapiti merupakan *tools* pengujian keamanan aplikasi web yang sama-sama digunakan untuk melakukan *vulnerability scanning*, namun

memiliki pendekatan antarmuka yang berbeda. OWASP ZAP menggunakan *Graphical User Interface* (GUI) yang memungkinkan konfigurasi pemindaian, *monitoring* proses, serta analisis hasil dilakukan secara visual dan interaktif. Pendekatan ini memudahkan pengguna dalam mengatur parameter scanning dan meninjau detail temuan kerentanan, termasuk klasifikasi tingkat risiko dan pemetaan terhadap OWASP Top 10.

Di sisi lain, Wapiti menggunakan *Command Line Interface* (CLI) yang mengeksekusi proses pemindaian melalui perintah teks. Pendekatan CLI memungkinkan proses *scanning* berjalan lebih ringan serta mendukung otomatisasi eksekusi. Hasil pemindaian disajikan dalam bentuk laporan tekstual yang memuat daftar temuan kerentanan beserta parameter teknisnya.

Perbedaan antarmuka ini tidak menjadi objek perbandingan utama, melainkan merupakan karakteristik operasional masing-masing *tools*. Penelitian ini tetap melakukan perbandingan secara setara dengan menyamakan ruang lingkup target, metode pengujian *black-box scanning*, serta parameter analisis, yaitu jumlah temuan, tingkat risiko, cakupan OWASP Top 10 2021, stabilitas hasil deteksi, dan waktu pemindaian. Dengan penyamaan parameter tersebut, perbedaan antarmuka GUI dan CLI justru menjadi konteks yang menjelaskan variasi kinerja masing-masing *tools*, tanpa memengaruhi validitas perbandingan efektivitas deteksinya.

2.2.9 Klasifikasi Tingkat Risiko Kerentanan

Klasifikasi risiko digunakan untuk menentukan prioritas penanganan kerentanan berdasarkan tingkat bahaya dan kemudahan eksploitasi. Klasifikasi tingkat risiko dalam penelitian ini mengadopsi standar OWASP Risk Rating Methodology yang membagi kerentanan berdasarkan tingkat bahaya dan kemudahan eksploitasi Umumnya, kategori risiko dibagi menjadi 4. Diantaranya:

1) *High Risk* (Risiko Tinggi): Celah kritis yang memungkinkan penyerang mengambil alih kontrol sistem atau mencuri data sensitif secara langsung. Wajib segera diperbaiki. Contoh: SQL *Injection* dan *Path Traversal*.
2) *Medium Risk* (Risiko Sedang): Kerentanan yang memiliki dampak signifikan namun lebih sulit dieksploitasi karena membutuhkan interaksi pengguna atau kondisi tertentu. Contoh: *Cross-Site Scripting* (XSS).

3) *Low Risk* (Risiko Rendah): Kerentanan dengan dampak minimal yang biasanya hanya memberikan akses informasi terbatas atau merupakan miskonfigurasi ringan. Contoh: *Missing Security Headers*.
4) *Informational*: Temuan yang tidak memiliki risiko eksploitasi langsung, melainkan hanya memberikan informasi teknis atau metadata mengenai sistem. Contoh: *Server Version Disclosure*.

BAB III
METODOLOGI PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen komparatif dengan pendekatan kuantitatif karena melibatkan proses pengumpulan dan analisis data numerik yang dapat diukur secara objektif. Metode pengujian yang digunakan dalam penelitian ini adalah *Dynamic Application Security Testing* (DAST). Sejalan dengan penelitian Lubis et al (2025), pendekatan DAST memungkinkan peneliti untuk melakukan perbandingan keamanan yang mendalam pada sistem yang sedang berjalan guna menemukan celah eksploitasi yang mungkin tidak terdeteksi pada tahap pengembangan. Rancangan penelitian berupa testing langsung terhadap tiga website target menggunakan dua *tools* yang berbeda, kemudian membandingkan hasilnya berdasarkan aspek dan parameter yang telah ditetapkan.

3.2 Objek dan Subjek Penelitian

Objek penelitian adalah tiga website Universitas Islam Negeri Ar-Raniry :

1. uinarraniry.siakadcloud.com
2. student.mahad.ar-raniry.ac.id
3. pusatbahasa.ar-raniry.ac.id

Subjek penelitian adalah *tools* OWASP ZAP 2.16.1 dan Wapiti 3.0.4.

3.3 Tempat dan Waktu Penelitian

Penelitian ini dilakukan selama 3 bulan, mulai dari Oktober hingga Desember 2025, bertempat di Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry Banda Aceh.

3.4 Alur Penelitian

Tahapan penelitian ini dirancang secara sistematis dan terstruktur untuk memastikan pelaksanaan eksperimen komparatif yang terukur dan efisien. Untuk mengorganisir dan menjamin efektivitas jadwal pengerjaan, Tabel 3.2 memvisualisasikan alokasi waktu yang direncanakan untuk setiap kegiatan penelitian. Jadwal ini menjadi panduan utama bagi peneliti dalam menyelesaikan

setiap tahapan secara tepat waktu, dengan fokus utama pada periode Oktober hingga Desember.

Tabel 3. 1 Alur Penelitian

No	Kegiatan	Oktober	November	Desember
1	Studi Literatur dan Pengumpulan Referensi			
2	Observasi Awal dan Penentuan Objek Uji			
3	Analisis Kebutuhan dan Perancangan Pengujian			
4	Pelaksanaan Vulnerability Assessment			
5	Analisis Hasil dan Perbandingan Efektifitas			
6	Penyusunan Kesimpulan dan Rekomendasi			
7	Penyusunan Laporan Akhir			

3.5 Alat dan Bahan Penelitian

Alat dan bahan untuk penelitian komparatif ini adalah serangkaian perangkat keras dan lunak yang digunakan dalam lingkungan simulasi yang terisolasi, meliputi :

1. Spesifikasi Perangkat Keras

Tabel 3. 2 Spesifikasi Perangkat Keras

Komponen	
Laptop	LENOVO (System Model: 20AMS1WW0X)
Sistem Operasi Host	Windows 10 Home Single Language 64-bit (Build 19045)
Prosesor (Processor)	Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz (4 CPUs), ≈ 2.5GHz
Memori (Random Access Memory)	8192MB (8 GB)

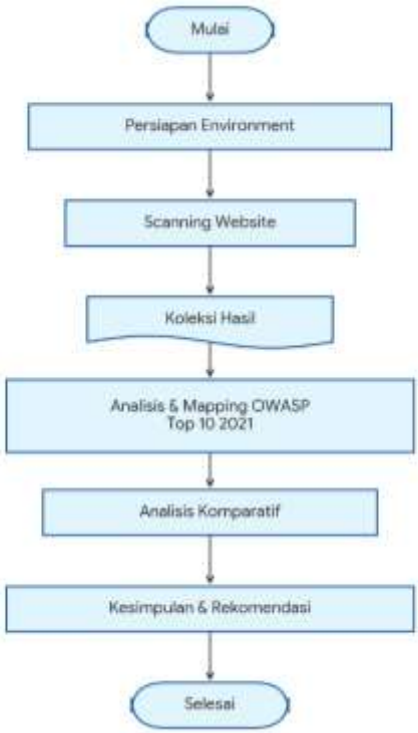
2. Sistem Operasi dan Lingkungan Virtual

   Pengujian *vulnerability scanner* dilakukan dalam lingkungan simulasi virtual untuk menciptakan isolasi dan konsistensi. Konfigurasi yang digunakan meliputi :

Tabel 3. 3 Sistem Operasi dan Lingkungan Virtual

Komponen	Versi	Fungsi
Oracle Virtual Box	7.1.10	Sistem Operasi
Kali Linux	6.12.33+kali-amd64	Sistem Operasi
OWASP ZAP	2.16.1	Web Application Vulnerability Scanner (WVS)
Wapiti	3.0.4	Web Application Vulnerability Scanner (WVS)
Website Target 1	uinarraniry.siakadcloud.com	Target simulasi
Website Target 2	student.mahad.ar-raniry.ac.id	Target simulasi
Website Target 3	pusatbahasa.ar-raniry.ac.id	Target simulasi

3.6 Diagam Alir Penelitian



Gambar 3. 1 Diagram Alir Penelitian

Diagram alir penelitian pada gambar 3.1 merupakan visualisasi dari seluruh alur kerja sistematis yang dimulai dengan Persiapan Environment, yaitu inisialisasi Virtual Machine dan penyiapan target aplikasi rentan untuk menciptakan lingkungan pengujian yang terisolasi. Setelah setup berhasil, penelitian dilanjutkan dengan fase eksekusi, yaitu *Scanning Website* dengan ZAP dan Wapiti. Hasil dari pemindaian independen ini kemudian dikumpulkan dan dicatat pada tahap Koleksi Hasil. Data yang terkumpul selanjutnya memasuki fase analisis, diawali dengan Analisis & Mapping OWASP Top 10 untuk mengklasifikasikan temuan ke dalam standar risiko global. Setelah pemetaan selesai, dilakukan Analisis Komparatif berdasarkan metrik efektivitas (Jumlah dan Tingkat Risiko, *Coverage*, Stabilitas) dan matrik *performance* (Kinerja waktu pemindaian) yang pada akhirnya menghasilkan kesimpulan dan rekomendasi sebagai luaran utama dari penelitian ini.

3.7 Tahapan Penelitian

Untuk mencapai tujuan penelitian, serangkaian langkah sistematis telah dirancang dan akan dilaksanakan secara berurutan. Proses ini dimulai dari fondasi teoritis melalui studi literatur, dilanjutkan dengan persiapan teknis lingkungan dan objek uji, kemudian masuk ke tahap inti yaitu perancangan dan eksekusi *vulnerability assessment*.

3.7.1 Studi Literatur dan Pengumpulan Referensi

Aktivitas pada tahap ini difokuskan untuk membangun landasan teoritis yang kuat melalui perolehan referensi relevan. Pendalaman dilakukan terhadap konsep kunci seperti *Vulnerability Assessment* termasuk identifikasi fungsi dan cara kerja spesifik dari *tool* pemindaian OWASP ZAP dan Wapiti.

3.7.2 Observasi Awal dan Penentuan Objek Uji

Tahap ini diawali dengan observasi teknis mendalam yang diarahkan untuk menetapkan seluruh kebutuhan *environment* pengujian. Fokus utama melibatkan penentuan spesifikasi perangkat keras dan lunak. Selain itu, riset ini mewajibkan pemilihan dan penetapan Website sebagai objek uji.

3.7.3 Analisis Kebutuhan dan Perancangan Pengujian

Tahap ini adalah inti penelitian, diawali dengan Analisis dan Perancangan Pengujian yang bertujuan memastikan seluruh prosedur eksperimen dapat dieksekusi secara terukur dan sistematis. Analisis kebutuhan berfokus pada penentuan spesifikasi minimal perangkat keras dan lunak yang akan digunakan, termasuk konfigurasi jaringan Virtual Machine untuk menciptakan lingkungan pengujian yang terisolasi. Sementara itu, Perancangan Pengujian mencakup penetapan Skenario Penelitian (Fase ZAP dan Wapiti) dan mendefinisikan kerangka waktu pengerjaan. Tahap ini juga krusial untuk merumuskan metrik perhitungan kuantitatif (Jumlah dan Tingkat Risiko, *Coverage*, Stabilitas dan Kinerja Waktu Pemindaian) yang akan digunakan untuk mengolah dan membandingkan hasil temuan kerentanan di Bab I.

3.7.4 Pelaksanaan *Vulnerability Assessment*

Tahap ini merupakan fase eksekusi pemindaian yang dilaksanakan secara paralel dan independen dalam lingkungan simulasi yang terisolasi sesuai

perancangan. Proses diawali dengan menjalankan OWASP ZAP untuk pemindaian otomatis, dan dilanjutkan dengan eksekusi *command-line* Wapiti pada target aplikasi rentan yang sama. Seluruh output data mentah, termasuk temuan kerentanan dan durasi waktu pemindaian, dicatat secara teliti. Pencatatan ini krusial untuk Koleksi Hasil Data Kerentanan yang akan digunakan sebagai bahan baku pada fase analisis.

3.7.5 Analisis Hasil dan Perbandingan Efektifitas

Setelah data mentah terkumpul, dilakukan proses Analisis Hasil dan Perbandingan Efektifitas yang terbagi menjadi tiga langkah utama. Pertama, setiap temuan kerentanan dari ZAP dan Wapiti diolah. Kedua, dilakukan pemetaan ke dalam kategori OWASP Top 10, semua temuan dari ZAP dan Wapiti diklasifikasikan ke dalam 10 kategori risiko OWASP (A01 hingga A10). Terakhir, dilakukan Analisis Komparatif dengan menghitung metrik kuantitatif: Jumlah dan tingkat risiko pada ketiga website, *Coverage* ke OWASP Top 10 2021, Stabilitas dan *Performance*, untuk mendapatkan gambaran objektif mengenai kemampuan deteksi masing-masing *tool*.

3.7.6 Penyusunan Kesimpulan dan Rekomendasi

Tahap terakhir dari penelitian adalah Penyusunan Kesimpulan dan Rekomendasi. Kesimpulan dirumuskan berdasarkan hasil Analisis Komparatif, menjawab secara eksplisit alat mana (OWASP ZAP atau Wapiti) yang menunjukkan efektivitas terbaik sesuai metrik yang telah ditetapkan. Selanjutnya, disusun Rekomendasi praktis dan akademis, memberikan saran teknis mengenai pemilihan *tools scanner* yang paling optimal untuk *vulnerability assessment* berbasis standar OWASP Top 10.

3.8 Skenario Penelitian

Penelitian ini menggunakan metodologi *Vulnerability Assessment* eksternal dengan pendekatan *Black Box*. Pengujian dilakukan sepenuhnya dari perspektif luar melalui jaringan internet publik, tanpa menggunakan informasi internal sistem, source code, maupun kredensial akses. Proses pengujian berfokus pada identifikasi potensi kerentanan tanpa melakukan *non-destructive* (eksploitasi aktif), sehingga tidak mengganggu operasional website yang diuji. Metode pengujian black box atau

yang dikenal sebagai pengujian berbasis perilaku (behavioral testing) berfokus pada luaran sistem tanpa memerlukan pengetahuan khusus mengenai struktur kode internal atau bahasa pemrograman yang digunakan oleh aplikasi target (Putri et al., 2024)

Pengujian metode Black Box menggunakan OWASP ZAP pada Kali Linux terbukti efektif dalam memberikan gambaran keamanan website secara objektif (Aryadi et al., 2026).

Pendekatan *Black Box* ini mensimulasikan kondisi nyata di mana seorang penyerang hanya mengandalkan informasi yang tersedia secara publik untuk melakukan pengujian keamanan. Ketiga website kampus diuji dari perspektif tersebut, sejalan dengan karakteristik website yang dapat diakses oleh pengguna umum dari jaringan eksternal.

Pengujian *Vulnerability Assessment* Eksternal ini akan dilaksanakan pada periode *low-traffic* (akhir pekan atau pukul 23:00 hingga 03:00 WIB) untuk meminimalisir dampak pada layanan akademik. *Vulnerability Assessment* akan menggunakan dua *tools* utama, OWASP ZAP versi 2.16.1 akan digunakan untuk melakukan automated scanning (pemindaian otomatis) dan Wapiti versi 3.0.4 akan digunakan untuk melakukan pemindaian *black-box* berbasis *command-line*.

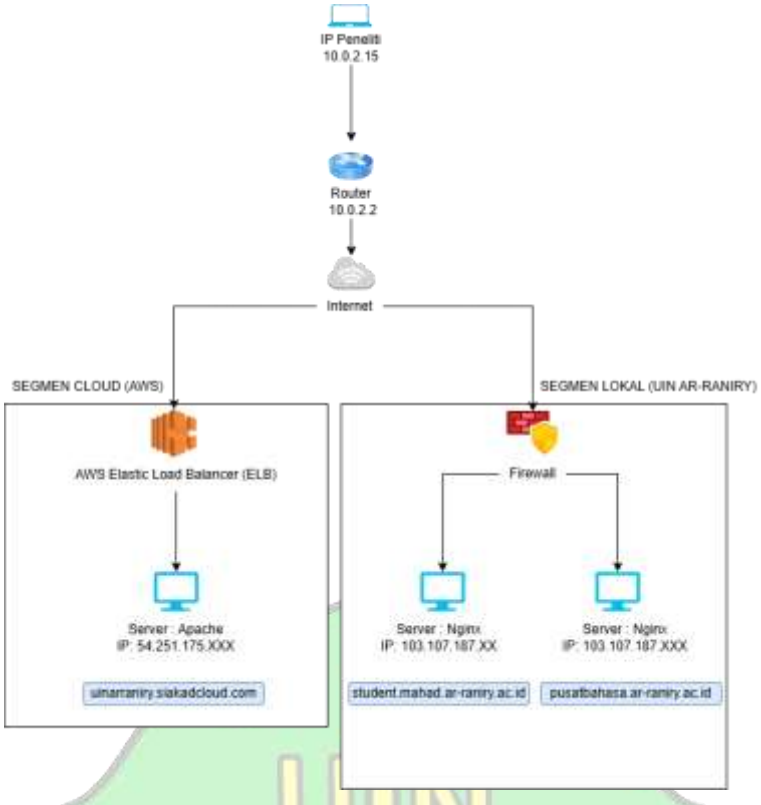
Kedua *tools* ini tidak akan dijalankan secara bersamaan pada target yang sama, melainkan menggunakan strategi *Serial Scanning*. Peneliti akan menyelesaikan *scanning* penuh pada satu target menggunakan satu *tool* terlebih dahulu, saat sudah mencapi 3 target yang ditentukan baru kemudian melanjutkan dengan tool kedua.

Infrastruktur website target dirangkum pada Tabel 3.4 untuk memfokuskan pengujian *Vulnerability Assessment* pada area yang paling relevan.

Tabel 3. 4 Infrastruktur dan Jaringan Target Penelitian

Domain Website	Hosting & Jaringan	Server Web & Backend
uinarraniry.siakadcloud.com	Eksternal (Cloud Pihak Ketiga). Lokasi server di luar negeri (AWS). IP 54.251.175.XXX Pengujian	Server Web: Apache. Infrastruktur: AWS Elastic Load Balancer (ELB). Backend/Autentikasi:

	Vulnerability Assessment Wajib Eksternal.	Menggunakan *Single Sign-On* (SSO) Sevima.
student.mahad.ar-raniry.ac.id	Internal/Lokal UIN Ar-Raniry. IP lokal (103.107.187.XX). Pengujian *Vulnerability Assessment* Prioritas Eksternal.	Server Web: Nginx versi 1.22.1. Status Akses: Memblokir akses (403 *Forbidden* / *Connection refused*), mengindikasikan adanya *firewall* atau mekanisme keamanan aktif.
pusatbahasa.ar-raniry.ac.id	Internal/Lokal UIN Ar-Raniry. IP lokal (103.107.187.XXX). Pengujian *Vulnerability Assessment* Prioritas Eksternal.	Server Web: Nginx. Backend: Dibangun menggunakan *framework* Laravel (PHP). *Vulnerability Assessment* harus fokus pada kerentanan aplikasi *framework*.



Gambar 3. 2 Topologi Jaringan

Berdasarkan Tabel 3.4 dan Gambar 3.2 di atas, menunjukkan topologi jaringan dalam proses pengujian keamanan aplikasi web. Peneliti bertindak sebagai penguji keamanan yang menggunakan perangkat dengan alamat IP 10.0.2.15 untuk melakukan scanning dan pengujian terhadap target website. Perangkat peneliti terhubung ke router dengan IP 10.0.2.2 sebagai gateway untuk mengakses jaringan internet. Melalui jaringan internet, pengujian diarahkan ke dua segmen target, yaitu:

1. Segmen Cloud (Eksternal): Terdiri dari website uinarraniry.siakadcloud.com yang dihosting di infrastruktur AWS dengan IP 54.251.175.XXX. Akses dari peneliti melewati internet menuju AWS *Elastic Load Balancer* (ELB) yang meneruskan trafik ke server Apache. Sistem ini juga terintegrasi dengan SSO Sevima untuk autentikasi pengguna.
2. Segmen Lokal (Internal UIN Ar-Raniry): Mencakup domain student.mahad.ar-raniry.ac.id (IP 103.107.187.XX) dan pusatbahasa.ar-raniry.ac.id (IP 103.107.187.XXX. Kedua website ini dihosting pada server Nginx dan berada di bawah perlindungan firewall lokal kampus. Akses dari internet harus melewati firewall UIN Ar-Raniry terlebih dahulu

sebelum diteruskan ke server, yang menunjukkan bahwa sistem menerapkan mekanisme penyaringan dan pembatasan akses jaringan untuk meningkatkan keamanan layanan.

Dalam penelitian ini, pengujian dilakukan dari sisi eksternal (internet) menuju kedua segmen server. Pendekatan ini bertujuan mensimulasikan potensi serangan nyata yang berasal dari luar jaringan kampus. Dengan topologi tersebut, peneliti dapat mengidentifikasi potensi kerentanan sistem secara lebih objektif.

BAB IV
HASIL DAN PEMBAHASAN

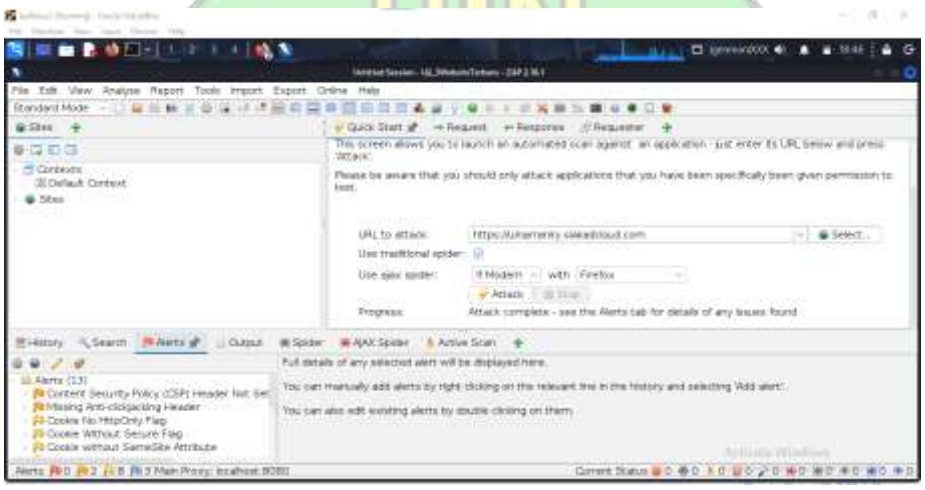
Pada bab ini, peneliti menyajikan hasil pengujian keamanan aplikasi web pada tiga target website menggunakan dua *tools vulnerability scanner*, yaitu OWASP ZAP dan Wapiti. Pengujian dilakukan untuk mengidentifikasi potensi kerentanan yang terdapat pada masing-masing website. Data hasil pemindaian *vulnerability assessment* yang diperoleh dari kedua *tools* selanjutnya dianalisis secara komparatif, guna melihat perbedaan kemampuan deteksi kerentanan, tingkat risiko yang dihasilkan, serta karakteristik temuan dari masing-masing *tools*.

4.1 Hasil *Vulnerability Assessment*

Berikut hasil temuan *vulnerability assessment* yang telah dilakukan:

4.1.1 Hasil Pengujian pada Website uinarraniry.siakadcloud.com

1. OWASP ZAP



Gambar 4. 1 OWASP ZAP uinarraniry.siakadcloud.com

Vulnerability Assessment pada website uinarraniry.siakadcloud.com dilakukan menggunakan *tool* OWASP ZAP dengan metode *automated scanning*. Gambar 4.1 menampilkan proses pemindaian yang berhasil dijalankan sepenuhnya hingga selesai. Pengujian ini menghasilkan sejumlah temuan kerentanan yang tercatat pada menu *Alerts*.

Tabel 4. 1 OWASP ZAP uinarraniry.siakadcloud.com

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Content Security Policy* (CSP) *Header Not Set*	*Medium*	2	Website belum menerapkan header CSP untuk membatasi sumber konten yang diperbolehkan dimuat oleh browser. Kondisi ini berpotensi meningkatkan risiko serangan *Cross-Site Scripting* (XSS).
2	*Missing Anti-clickjacking Header*	*Medium*	1	Tidak terdapat *header anti-clickjacking* sehingga website berpotensi disusupi melalui *frame* berbahaya.
3	*Cookie No HttpOnly Flag*	*Low*	1	*Cookie* dapat diakses melalui JavaScript dan berpotensi dimanfaatkan pada serangan XSS.
4	*Cookie Without Secure Flag*	*Low*	1	*Cookie* dapat dikirim tanpa enkripsi, berisiko disadap pada koneksi tidak aman.
5	*Cookie without SameSite Attribute*	*Low*	1	*Cookie* tidak memiliki atribut *SameSite*, berpotensi dimanfaatkan untuk serangan *Cross-Site*

				Request Forgery (CSRF).
6	*Cross-Domain JavaScript Source File Inclusion*	*Low*	7	Website memuat JavaScript dari domain eksternal yang berpotensi membawa skrip berbahaya.
7	*Server Leaks Version Information via "Server"* HTTP *Response Header Field*	*Low*	1	Server menampilkan informasi versi yang dapat dimanfaatkan untuk *fingerprinting* sistem.
8	*Strict-Transport-Security Header Not Set*	*Low*	3	Tidak diterapkan HSTS sehingga koneksi HTTPS tidak dipaksa secara penuh.
9	*X-Content-Type-Options Header Missing*	*Low*	1	Browser dapat menebak tipe konten, berpotensi mengeksekusi konten berbahaya.
10	*ZAP is Out of Date*	*Low*	1	OWASP ZAP yang digunakan perlu diperbarui, namun tidak berdampak langsung pada keamanan website.
11	*Modern Web Application*	*Informational*	1	Website menggunakan teknologi web modern.

12	*Session Management Response Identified*	*Informational*	1	Sistem merespon mekanisme manajemen sesi dengan baik.
13	*User Agent Fuzzer*	*Informational*	48	Server merespon variasi *user-agent.* Bersifat informasi tambahan.
Total			**13**	

Hasil pemindaian OWASP ZAP pada website uinarraniry.siakadcloud.com yang terangkum dalam Tabel 4.1 memperlihatkan total temuan sebanyak 13 jenis temuan. Temuan-temuan tersebut terdeteksi didominasi oleh kelemahan konfigurasi keamanan pada sisi server serta browser protection. Secara spesifik, celah ini mencakup absennya sejumlah security headers krusial seperti Content Security Policy (CSP), serta pengaturan atribut *cookie* yang belum optimal untuk memitigasi risiko serangan.

OWASP ZAP banyak menemukan ketidakhadiran *security headers* seperti *Content Security Policy* (CSP), *Anti-clickjacking Header*, *Strict-Transport-Security* (HSTS), serta *X-Content-Type-Options*. Selain itu, ditemukan pula kelemahan pada atribut *cookie*, yaitu tidak diterapkannya *HttpOnly*, *Secure, dan SameSite.* Di samping itu, OWASP ZAP juga mendeteksi pemanggilan JavaScript dari domain eksternal dan pengungkapan informasi versi server, yang termasuk kategori potensi *information disclosure.*

Temuan-temuan tersebut menunjukkan bahwa OWASP ZAP lebih fokus pada identifikasi kelemahan konfigurasi keamanan dasar dan perlindungan *browser-side* (*security header & cookie setting*). Hal ini akan menjadi dasar pembanding dengan hasil pemindaian menggunakan Wapiti, untuk melihat apakah kedua *tools* menghasilkan jenis temuan yang serupa atau memiliki fokus deteksi yang berbeda.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (7.7%)	1 (7.7%)	0 (0.0%)	2 (15.4%)
	Low	0 (0.0%)	3 (23.1%)	5 (38.5%)	0 (0.0%)	8 (61.5%)
	Informational	0 (0.0%)	0 (0.0%)	3 (23.1%)	0 (0.0%)	3 (23.1%)
	Total	0 (0.0%)	4 (30.8%)	9 (69.2%)	0 (0.0%)	13 (100%)

Gambar 4. 2 Tingkat Risiko uinnarraniry.siakadcloud.com

Berdasarkan Gambar 4.2 hasil pemindaian OWASP ZAP pada website uinarraniry.siakadcloud.com diperoleh matriks *Risk and Confidence Summary*. Matriks ini menggambarkan jumlah temuan kerentanan berdasarkan *Risk* (tingkat risiko**)** dan *Confidence* (tingkat kepercayaan deteksi) dari *tool* OWASP ZAP. Dari total 13 temuan kerentanan (100%), distribusi tingkat risiko yaitu *Medium Risk* sebanyak 2 temuan (15,4%) *Low Risk* sebanyak 8 temuan (61,5%), *Informational Risk* sebanyak 3 temuan (23,1%), *High Risk* sebanyak 0 temuan (0%).

Hasil ini menunjukkan bahwa tidak ditemukan kerentanan dengan kategori *High Risk*, sehingga secara umum website tidak memiliki celah keamanan kritis yang dapat langsung dieksploitasi untuk mengambil alih sistem. Namun, mayoritas temuan berada pada kategori *Low Risk* (61,5%), yang umumnya berkaitan dengan konfigurasi keamanan *header* HTTP dan pengaturan atribut *cookie*. Walaupun berdampak rendah, kerentanan ini tetap dapat dimanfaatkan dalam skenario serangan tertentu apabila tidak segera diperbaiki.

Sementara itu, *Medium Risk* (15,4%) menunjukkan adanya kelemahan konfigurasi keamanan yang berpotensi membuka peluang serangan seperti *clickjacking* dan *cross-site scripting* (XSS) apabila dikombinasikan dengan celah lain. Adapun kategori *Informational* (23,1%) bersifat informasi tambahan yang tidak berdampak langsung, namun tetap bermanfaat sebagai bahan evaluasi untuk meningkatkan keamanan sistem secara menyeluruh. Dari sisi *Confidence*, sebagian besar temuan tingkat *Medium* (69,2%) dan High (30,8%), yang menunjukkan bahwa OWASP ZAP cukup yakin terhadap validitas kerentanan yang terdeteksi.

2. WAPITI

Gambar 4. 3 Wapiti uinarraniry.siakadcloud.com

Berdasarkan visualisasi yang disajikan pada Gambar 4.3, laporan ini menampilkan hasil pemindaian keamanan menggunakan *tools* Wapiti pada website uinarraniry.siakadcloud.com. Melalui aktivitas *scanning* tersebut, Wapiti secara efektif mengidentifikasi sejumlah kelemahan pada konfigurasi keamanan sistem. Fokus utama temuan ini terletak pada beberapa aspek krusial, yaitu *security header*, pengamanan *cookie*, serta konfigurasi TLS/SSL

Temuan yang berhasil dipetakan mencakup tidak diterapkannya beberapa *header* keamanan penting, antara lain CSP, *X-Frame-Options*, dan HSTS. Selain itu, hasil pengujian juga menunjukkan ketiadaan atribut *HttpOnly* serta *Secure Flag* pada *cookie* yang digunakan. Di samping masalah pada sisi aplikasi, Wapiti turut mendeteksi kelemahan pada konfigurasi enkripsi TLS/SSL yang berpotensi memengaruhi keamanan komunikasi data antara *client* dan *server*.

Tabel 4. 2 Wapiti uinarraniry.siakadcloud.com

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Content Security Policy Configuration*	*Medium*	1	CSP belum dikonfigurasi dengan baik sehingga berpotensi membuka celah XSS.
2	*Clickjacking Protection*	*Medium*	1	Proteksi *anti-clickjacking* tidak

				diterapkan, memungkinkan halaman dimuat dalam *frame* berbahaya.
3	HTTP *Strict Transport Security* (HSTS)	*Low*	1	Website belum memaksa penggunaan HTTPS secara penuh.
4	*MIME Type Confusion*	*Low*	1	Browser berpotensi salah mengenali tipe file dan mengeksekusi konten berbahaya.
5	*HttpOnly Flag cookie*	*Low*	1	*Cookie* dapat diakses melalui JavaScript, berisiko pada serangan XSS.
6	*Secure Flag cookie*	*Low*	1	*Cookie* dapat dikirim melalui koneksi tidak terenkripsi.
7	TLS/SSL *misconfigurations*	*High*	14	Ditemukan konfigurasi enkripsi TLS/SSL yang lemah atau tidak optimal, berpotensi memungkinkan penyadapan komunikasi data.
Total			**7**	

Hasil pemindaian keamanan menggunakan *tools* Wapiti menunjukkan bahwa mayoritas kerentanan yang terdeteksi berkaitan erat dengan konfigurasi pada sisi *server*. Selain itu, temuan tersebut juga mencakup kelemahan dalam aspek koneksi komunikasi jaringan yang digunakan oleh sistem. Jenis kerentanan yang paling dominan ditemukan adalah TLS/SSL *misconfiguration* dengan angka mencapai persentase sekitar 70% dari keseluruhan total temuan.

TLS/SSL merupakan protokol yang berfungsi untuk mengenkripsi komunikasi antara *browser client* dan *server* website, sehingga data seperti *username, password,* dan informasi pribadi tidak dapat dibaca oleh pihak lain selama proses transmisi. Adanya temuan TLS/SSL *misconfiguration* menandakan bahwa pengaturan enkripsi pada *server* belum dikonfigurasi secara optimal, misalnya masih menggunakan protokol lama, sertifikat yang tidak sepenuhnya valid, atau konfigurasi *cipher* yang lemah. Kondisi ini berpotensi membuka peluang bagi penyerang untuk melakukan penyadapan komunikasi (*man-in-the-middle attack*) atau menurunkan tingkat kerahasiaan data pengguna.

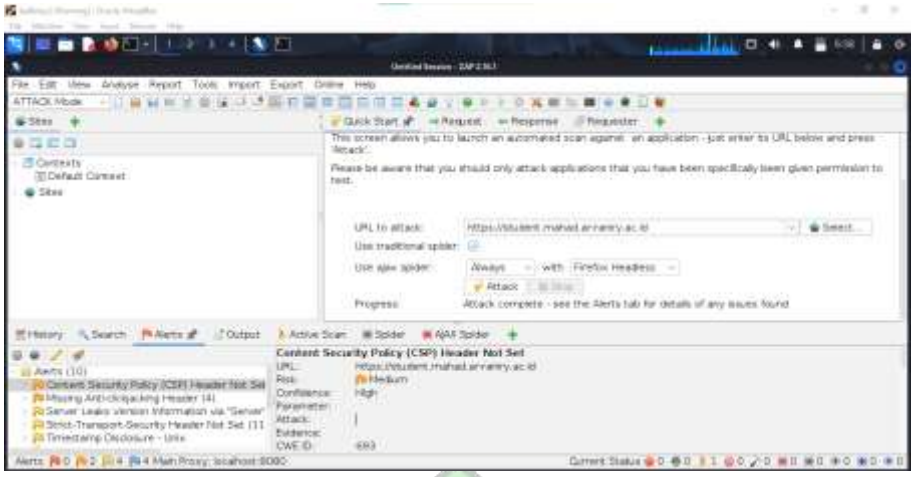
Selain itu, Wapiti juga menemukan kelemahan pada penerapan *security header*, seperti *Content Security Policy* (CSP), *Clickjacking Protection*, dan HTTP *Strict Transport Security* (HSTS). *Security header* ini berfungsi sebagai lapisan perlindungan tambahan pada browser untuk mencegah serangan berbasis web, seperti penyisipan skrip berbahaya dan pemuatan halaman palsu. Tidak diterapkannya *header-header* tersebut menunjukkan bahwa perlindungan dari sisi *browser* belum maksimal.

Temuan berikutnya berkaitan dengan atribut keamanan *cookie*, yaitu *HttpOnly Flag* dan *Secure Flag*. *Cookie* digunakan untuk menyimpan informasi sesi pengguna. Jika atribut ini tidak diterapkan, *cookie* dapat lebih mudah diakses oleh skrip berbahaya atau dikirim melalui koneksi yang tidak terenkripsi, sehingga meningkatkan risiko pencurian sesi pengguna.

Secara keseluruhan, hasil pemindaian Wapiti menunjukkan bahwa fokus utama temuan berada pada kelemahan konfigurasi keamanan infrastruktur dan komunikasi data, bukan pada celah logika aplikasi atau serangan injeksi *database*. Dengan demikian, Wapiti pada pengujian ini lebih menyoroti keamanan lapisan *transport* dan konfigurasi *server*, yang sangat penting untuk menjamin kerahasiaan dan integritas data pengguna saat mengakses website.

4.1.2 Hasil Pengujian pada Website student.mahad.ar-raniry.ac.id

1. OWASP ZAP



Gambar 4. 4 OWASP ZAP student.mahad.ar-raniry.ac.id

Merujuk pada visualisasi yang ditampilkan pada Gambar 4.4, hasil pemindaian menggunakan OWASP ZAP mendeteksi sebanyak 10 jenis *alert* kerentanan pada website student.mahad.ar-raniry.ac.id. Pengujian keamanan tersebut dilakukan melalui metode *automated scanning*. Meskipun situs web tersebut telah dapat diakses secara fungsional, hasil pemindaian tetap mengidentifikasi adanya sejumlah celah keamanan, terutama pada tingkat konfigurasi *header* respons HTTP.

Tabel 4. 3 OWASP ZAP student.mahad.ar-raniry.ac.id

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Content Security Policy (CSP) Header Not Set*	*Medium*	4	Website belum menerapkan CSP *Header* sehingga berpotensi rentan terhadap XSS.
2	*Missing Anti-clickjacking Header*	*Medium*	4	Tidak terdapat *header anti-clickjacking*, berpotensi disusupi melalui *frame* berbahaya.

3	*Server Leaks Version Information via "Server" HTTP Response Header Field*	*Low*	11	Server menampilkan informasi versi yang dapat dimanfaatkan untuk *fingerprinting*.
4	*Strict-Transport-Security Header Not Set*	*Low*	11	Tidak diterapkannya HSTS sehingga koneksi HTTPS tidak dipaksa penuh.
5	*Timestamp Disclosure - Unix*	*Low*	1	Website menampilkan informasi timestamp yang dapat dimanfaatkan untuk analisis sistem.
6	*X-Content-Type-Options Header Missing*	*Low*	11	Browser dapat menebak tipe konten, berpotensi mengeksekusi konten berbahaya.
7	*Information Disclosure - Suspicious Comments*	*Informational*	1	Ditemukan komentar mencurigakan pada *source code* yang berpotensi membocorkan informasi.
8	*Modern Web Application*	*Informational*	4	Website menggunakan teknologi web modern.

9	*Re-examine Cache-control Directives*	*Informational*	4	Pengaturan *cache* belum dikonfigurasi optimal.
10	*Retrieved from Cache*	*Informational*	1	Respon halaman terdeteksi berasal dari *cache*.
Total			**10**	

Data yang disajikan dalam 4.3 menunjukkan adanya 10 jenis *alert* kerentanan yang berhasil dideteksi, di mana temuan tersebut didominasi oleh kategori risiko *Medium* dan *Low*. Temuan utama pada tingkat Medium mencakup tidak diterapkannya *Content Security Policy* (CSP) serta *Anti-clickjacking Header* pada konfigurasi sistem. Ketiadaan komponen perlindungan tersebut dianggap krusial karena dapat membuka peluang terjadinya serangan *Cross-Site Scripting* (XSS) dan *clickjacking* yang membahayakan keamanan data pengguna.

Sebagian besar temuan pada tingkat *Low* berkaitan erat dengan *misconfiguration security header* serta potensi *information disclosure*, seperti pengungkapan versi *server* dan pengaturan HSTS yang belum optimal. Selain itu, ditemukan pula header perlindungan browser yang belum diterapkan secara menyeluruh, sementara temuan kategori *Informational* hanya bersifat sebagai referensi tambahan mengenai teknologi website serta konfigurasi *cache*. Secara keseluruhan, hasil pengujian OWASP ZAP pada objek ini lebih banyak menitikberatkan pada identifikasi kelemahan konfigurasi keamanan sisi *server* dan aspek *browser protection*.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (10.0%)	1 (10.0%)	0 (0.0%)	2 (20.0%)
	Low	0 (0.0%)	2 (20.0%)	1 (10.0%)	1 (10.0%)	4 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (20.0%)	2 (20.0%)	4 (40.0%)
	Total	0 (0.0%)	3 (30.0%)	4 (40.0%)	3 (30.0%)	10 (100%)

Gambar 4. 5 Tingkat Risiko student.mahad.ar-raniry.ac.id

Berdasarkan hasil pemindaian menggunakan OWASP ZAP pada website student.mahad.ar-raniry.ac.id, diperoleh matriks *Risk and Confidence Summary* sebagaimana ditunjukkan pada Gambar 4.5. Matriks tersebut menyajikan data komprehensif mengenai distribusi temuan kerentanan yang berhasil diidentifikasi selama proses pengujian keamanan berlangsung. Visualisasi ini secara spesifik merepresentasikan klasifikasi temuan berdasarkan tingkat *Risk* (risiko) dan tingkat *Confidence* (kepercayaan deteksi) yang dihasilkan oleh *tool* OWASP ZAP.

Dari total 10 temuan kerentanan (100%), diperoleh distribusi tingkat risiko mencakup *Medium Risk* sebanyak 2 temuan (20%), *Risk Low* sebanyak 4 temuan (40%), *Risk Informational* sebanyak 4 temuan (40%) dan *High Risk* sebanyak 0 temuan (0%). Hasil tersebut menunjukkan bahwa tidak ditemukan kerentanan dengan tingkat risiko tinggi, sehingga tidak terdapat celah keamanan kritis yang dapat langsung dimanfaatkan untuk eksploitasi sistem.

Mayoritas temuan berada pada kategori *Low* dan *Informational* dengan masing-masing hasil 40%, yang umumnya berkaitan dengan informasi konfigurasi sistem dan penerapan *security header* dasar. Walaupun tidak berdampak langsung, temuan ini tetap penting sebagai bahan evaluasi peningkatan keamanan aplikasi web. Sementara itu, temuan dengan risiko *Medium* (20%) mengindikasikan adanya kelemahan konfigurasi. Dari sisi *Confidence*, sebagian besar temuan berada pada tingkat *Medium* (40%) dan *High* (30%), yang menunjukkan bahwa OWASP ZAP cukup yakin terhadap validitas hasil deteksinya.

2. WAPITI

Gambar 4. 6 Wapiti student.mahad.ar-raniry.ac.id

Visualisasi pada Gambar 4.6 memperlihatkan hasil pemindaian menggunakan *tool* Wapiti terhadap website student.mahad.ar-raniry.ac.id guna menguji ketahanan konfigurasinya. Melalui pemindaian ini, ditemukan indikasi kerentanan akibat absennya beberapa *security headers* krusial seperti CSP, *X-Frame-Options*, *X-Content-Type-Options*, dan *Strict-Transport-Security*. Selain itu, Wapiti juga mendeteksi *misconfiguration* pada sektor TLS/SSL yang mencakup sertifikat kedaluwarsa, ketidaksesuaiayn *hostname*, serta kerentanan *server* terhadap eksploitasi OpenSSL CCS.

Tabel 4. 4 Wapiti student.mahad.ar-raniry.ac.id

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Content Security Policy Configuration*	*Medium*	1	CSP belum dikonfigurasi optimal sehingga berpotensi membuka peluang serangan XSS.
2	*Clickjacking Protection*	*Medium*	1	Proteksi *anti-clickjacking* belum diterapkan, memungkinkan halaman dimuat dalam *frame* berbahaya.
3	*HTTP Strict Transport Security (HSTS)*	*Low*	1	Website belum menerapkan pemaksaan akses HTTPS secara penuh.
4	*MIME Type Confusion*	*Low*	1	Browser berpotensi salah mengenali tipe konten dan mengeksekusi *file* berbahaya.
5	*TLS/SSL misconfigurations*	*High*	16	Ditemukan konfigurasi enkripsi TLS/SSL yang

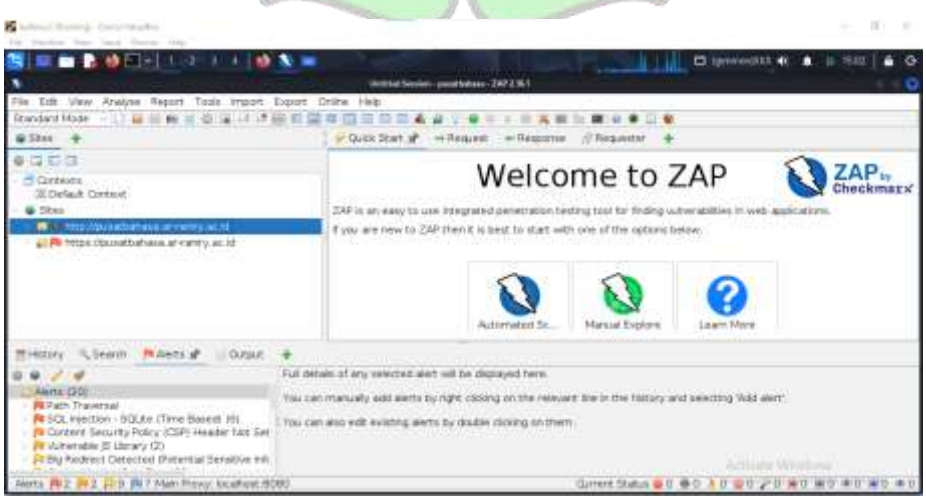
				tidak optimal, berpotensi melemahkan keamanan komunikasi data.
Total			**5**	

Berdasarkan data yang tersaji dalam Tabel 4.4, tercatat total lima temuan kerentanan yang berhasil diidentifikasi melalui pemindaian menggunakan Wapiti. Hasil pengujian tersebut menunjukkan bahwa jenis temuan yang paling dominan adalah TLS/SSL *misconfigurations* yaitu 16 temuan. Tingginya angka pada kategori ini mengindikasikan bahwa konfigurasi enkripsi komunikasi antara *client* dan *server* belum diatur secara optimal, sehingga berisiko melemahkan aspek keamanan pada proses transmisi data.

Selain temuan utama tersebut, laporan juga mencatat beberapa temuan lain yaitu *Content Security Policy*, *Clickjacking Protection*, HSTS, dan MIME *Type Confusion*. Munculnya temuan-temuan ini memberikan gambaran bahwa implementasi beberapa *security header* serta pengaturan proteksi *browser* pada sistem belum diterapkan secara sempurna demi memitigasi risiko serangan berbasis web. Secara keseluruhan, data ini menegaskan bahwa fokus utama kerentanan yang dideteksi oleh Wapiti terletak pada kelemahan konfigurasi koneksi serta keamanan *server*, alih-alih pada celah logika aplikasi.

4.1.3 Hasil Pengujian pada Website pusatbahasa.ar-raniry.ac.id

1. OWASP ZAP



Gambar 4. 7 OWASP ZAP pusatbahasa.ar-raniry.ac.id

Merujuk pada visualisasi hasil pemindaian yang disajikan dalam Gambar 4.7, *tool* OWASP ZAP berhasil mengidentifikasi sebanyak 20 jenis *alert* kerentanan pada website tersebut. Temuan-temuan yang muncul tersebut menunjukkan bahwa sistem memiliki variasi celah keamanan yang mencakup berbagai tingkat risiko. Klasifikasi kerentanan tersebut terbagi secara sistematis mulai dari kategori tingkat *High, Medium, Low*, hingga *Informational* sesuai dengan dampaknya terhadap sistem.

Tabel 4. 5 OWASP ZAP pusatbahasa.ar-raniry.ac.id

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Path Traversal*	*High*	1	Ditemukan indikasi akses file di luar direktori web yang seharusnya dibatasi.
2	*SQL Injection - SQLite (Time Based)*	*High*	6	Terdapat indikasi parameter rentan terhadap serangan SQL *Injection* berbasis waktu.
3	*Content Security Policy (CSP) Header Not Set*	*Medium*	69	Website belum menerapkan CSP *Header* sehingga berpotensi rentan terhadap XSS.
4	*Vulnerable JS Library*	*Medium*	2	Ditemukan penggunaan library JavaScript dengan versi rentan.
5	*Big Redirect Detected (Potential Sensitive Information Leak)*	*Low*	11	Terdeteksi *redirect* besar yang berpotensi

				membocorkan informasi sensitif.
6	*Cookie No HttpOnly Flag*	*Low*	60	*Cookie* dapat diakses melalui JavaScript, berpotensi dimanfaatkan pada XSS.
7	*Cookie Without Secure Flag*	*Low*	120	*Cookie* dikirim tanpa enkripsi, berisiko disadap pada koneksi tidak aman.
8	*Cookie without SameSite Attribute*	*Low*	120	Berpotensi dimanfaatkan untuk CSRF.
9	*Cross-Domain JavaScript Source File Inclusion*	*Low*	194	Website memuat JavaScript dari domain eksternal yang berpotensi berbahaya.
10	*Secure Pages Include Mixed Content*	*Low*	1	Halaman HTTPS memuat konten HTTP, berpotensi menurunkan keamanan koneksi.
11	*Strict-Transport-Security Header Not Set*	*Low*	90	Tidak diterapkannya HSTS sehingga koneksi HTTPS tidak dipaksa penuh.

12	*Timestamp Disclosure - Unix*	*Low*	2	Website menampilkan timestamp sistem yang dapat dimanfaatkan untuk analisis target.
13	*ZAP is Out of Date*	*Low*	1	Versi *tool* yang digunakan perlu diperbarui.
14	*Authentication Request Identified*	*Informational*	1	Ditemukan mekanisme autentikasi pada sistem.
15	*Charset Mismatch (Header Versus Meta Content-Type Charset)*	*Informational*	63	Terdapat ketidaksesuaian *charset* antara *header* dan meta tag.
16	*Information Disclosure - Suspicious Comments*	*Informational*	3	Ditemukan komentar mencurigakan pada *source code*.
17	*Modern Web Application*	*Informational*	66	Website teridentifikasi menggunakan teknologi web modern.
18	*Re-examine Cache-control Directives*	*Informational*	51	Pengaturan *cache* belum dikonfigurasi optimal.

19	*Session Management Response Identified*	*Informational*	60	Sistem merespon mekanisme manajemen sesi.
20	*User Controllable HTML Element Attribute (Potential XSS)*	*Informational*	4	Ditemukan atribut HTML yang dapat dikontrol *user* dan berpotensi XSS.
Total			**20**	

Hasil pemindaian OWASP ZAP pada website ini berhasil mengidentifikasi sebanyak 20 jenis alert kerentanan yang mencakup tingkat risiko *High*, *Medium*, *Low*, hingga *Informational*. Temuan utama yang menjadi perhatian serius adalah adanya kerentanan kritis pada sisi *server*, yaitu *Path Traversal* dan *SQL Injection* (*time-based*). Temuan tersebut secara langsung mengindikasikan adanya kelemahan pada sistem validasi input serta mekanisme *query database* yang digunakan oleh aplikasi. Selain itu, terdeteksi pula potensi kerentanan XSS yang dipicu oleh absennya implementasi *Content Security Policy* (CSP) serta keberadaan atribut HTML yang masih dapat dikontrol oleh user secara bebas.

Sebagian besar temuan lainnya berkaitan dengan kelemahan konfigurasi keamanan web, terutama pada aspek *security header* yang belum diimplementasikan secara lengkap. Hal ini diperburuk dengan pengaturan *cookie* yang dinilai kurang aman karena belum menerapkan atribut penting seperti *HttpOnly*, *Secure*, *SameSite*, serta konfigurasi HSTS yang belum optimal. Berdasarkan hasil tersebut, OWASP ZAP mengelompokkan temuan ke dalam dua kategori utama, yakni kerentanan sisi *server* terkait *injection* dan file *access*, serta kerentanan sisi *client* yang berkaitan dengan konfigurasi keamanan. Seluruh jenis temuan ini nantinya akan dibandingkan dengan hasil pemindaian Wapiti guna menganalisis perbedaan fokus deteksi antara pengujian *injection backend* dengan analisis konfigurasi keamanan aplikasi web secara menyeluruh.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (5.0%)	1 (5.0%)	2 (10.0%)
	Medium	0 (0.0%)	1 (5.0%)	1 (5.0%)	0 (0.0%)	2 (10.0%)
	Low	0 (0.0%)	2 (10.0%)	6 (30.0%)	1 (5.0%)	9 (45.0%)
	Informational	0 (0.0%)	1 (5.0%)	3 (15.0%)	3 (15.0%)	7 (35.0%)
	Total	0 (0.0%)	4 (20.0%)	11 (55.0%)	5 (25.0%)	20 (100%)

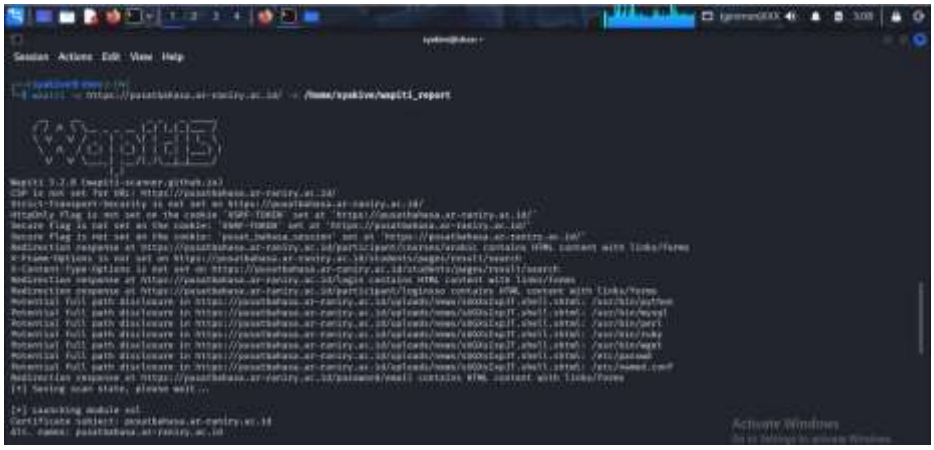
Gambar 4. 8 Tingkat Risiko pusatbahasa.ar-raniry.ac.id

Pada gambar 4.8 menampilkan dari total 20 temuan kerentanan (100%), diperoleh distribusi tingkat *Medium Risk* sebanyak 2 temuan (10%), *Low Risk* sebanyak 9 temuan (45%), *Informational Risk* sebanyak 7 temuan (35%) dan *High Risk* sebanyak 2 temuan (10%). Distribusi ini menunjukkan bahwa sebagian besar temuan berada pada kategori *Low Risk* (45%), yang umumnya berkaitan dengan kelemahan konfigurasi keamanan dasar seperti pengaturan *cookie* dan *security header*.

Meskipun persentase *High Risk* hanya 10%, temuan pada level ini bersifat kritis, karena mencakup kerentanan seperti *Path Traversal* dan *SQL Injection*, yang berpotensi memungkinkan penyerang mengakses file sensitif atau memanipulasi *database*. Sementara itu, *Medium Risk* (10%) menunjukkan adanya kelemahan konfigurasi yang dapat membuka peluang serangan seperti XSS apabila dikombinasikan dengan celah lain. Adapun *Informational Risk* (35%) bersifat informasi tambahan mengenai konfigurasi sistem dan teknologi yang digunakan, yang tidak berdampak langsung tetapi tetap penting sebagai bahan evaluasi peningkatan keamanan.

Hasil ini menunjukkan bahwa website memiliki beberapa celah kritis yang perlu segera diperbaiki, disertai banyak kelemahan konfigurasi keamanan dasar. Dengan kata lain secara umum sistem belum sepenuhnya aman, meskipun mayoritas celah berada pada tingkat risiko rendah.

2. WAPITI



Gambar 4. 9 Wapiti pusatbahasa.ar-raniry.ac.id

Visualisasi pada Gambar 4.9 menampilkan hasil pemindaian keamanan menggunakan tool Wapiti terhadap website pusatbahasa.ar-raniry.ac.id. Berdasarkan hasil pemindaian tersebut, Wapiti berhasil mengidentifikasi adanya sejumlah kelemahan konfigurasi pada bagian *security header* serta pengaturan atribut *cookie*. Selain itu, laporan ini juga mendeteksi adanya potensi *information disclosure* berupa kemungkinan akses *terhadap path internal* pada sisi *server*.

Tabel 4. 6 Wapiti pusatbahasa.ar-raniry.ac.id

No	Jenis Kerentanan	Risiko	Jumlah	Deskripsi
1	*Content Security Policy Configuration*	*Medium*	1	CSP belum dikonfigurasi optimal, berpotensi membuka celah XSS.
2	*Clickjacking Protection*	*Medium*	1	Proteksi *anti-clickjacking* tidak diterapkan.
3	*HTTP Strict Transport Security (HSTS)*	*Low*	1	Website belum menerapkan memksakan HTTPS penuh.

4	*MIME Type Confusion*	*Low*	1	*Browser* dapat salah mengenali tipe konten.
5	*HttpOnly Flag cookie*	*Low*	1	*Cookie* dapat diakses melalui JavaScript.
6	*Inconsistent Redirection*	*Low*	4	Ditemukan pola *redirect* tidak konsisten yang berpotensi disalahgunakan.
7	*Information Disclosure - Full Path*	*Low*	7	Sistem menampilkan *path* direktori *internal server*.
8	*Secure Flag cookie*	*Low*	2	Cookie dapat dikirim tanpa koneksi terenkripsi.
9	TLS/SSL *misconfigurations*	*High*	14	Konfigurasi enkripsi TLS/SSL tidak optimal, berpotensi melemahkan keamanan komunikasi data.
Total				**9**

Tabel 4.6 menampilkan hasil pemindaian Wapiti pada website ini menemukan 32 temuan kerentanan, dengan dominasi TLS/SSL *misconfigurations* yang menunjukkan lemahnya konfigurasi enkripsi komunikasi data. Selain itu, ditemukan beberapa kelemahan pada *cookie security* dan *information disclosure*, seperti bocornya *path internal server*. Temuan lainnya berkaitan dengan *security header* yang belum diterapkan optimal. Secara umum, hasil ini menegaskan bahwa fokus utama temuan Wapiti berada pada kelemahan konfigurasi *server* dan keamanan koneksi,

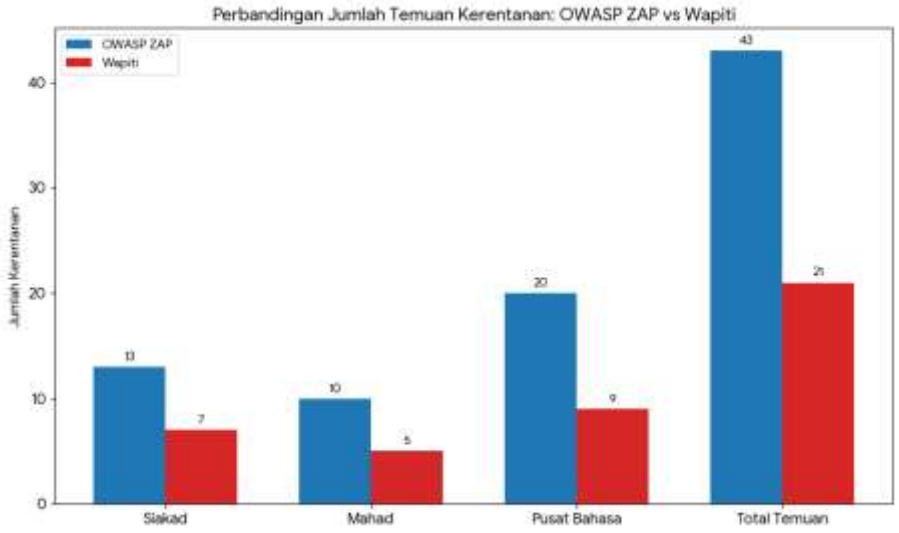
4.2 Analisis Efektivitas OWASP ZAP dan Wapiti

4.2.1 Jumlah Temuan

Merujuk pada hasil pemindaian yang telah dilakukan terhadap tiga website target di lingkungan UIN Ar-Raniry, diperoleh data kuantitatif mengenai total kerentanan yang dideteksi oleh kedua *tool* tersebut. Angka-angka yang terhimpun mencerminkan perbandingan jumlah temuan otomatis yang dihasilkan oleh OWASP ZAP dan Wapiti selama proses pengujian keamanan berlangsung. Akumulasi data ini berfungsi sebagai parameter awal yang krusial untuk menganalisis tingkat sensitivitas masing-masing alat dalam memetakan titik-titik kelemahan pada sistem yang diuji.

Tabel 4. 7 Jumlah Temuan

WEBSITE	JUMLAH TEMUAN	
	OWASP ZAP	WAPITI
uinarraniry.siakadcloud.com	13	7
student.mahad.ar-raniry.ac.id	10	5
pusatbahasa.ar-raniry.ac.id	20	9
Total	**43**	**21**



Gambar 4. 10 Jumlah Temuan Kerentanan

Berdasarkan Tabel 4.7 dan Gambar 4.10, dapat ditarik beberapa kesimpulan singkat mengenai jumlah temuan kerentanan. OWASP ZAP menemukan total 43

kerentanan, dua kali lipat lebih banyak dibandingkan Wapiti yang hanya menemukan 21 kerentanan. Hal ini menunjukkan mekanisme pemindaian ZAP lebih mendalam dalam mengidentifikasi celah keamanan. Website pusatbahasa.ar-raniry.ac.id memiliki jumlah temuan terbanyak yaitu ZAP 20 temuan dan Wapiti 9 temuan, yang mengindikasikan bahwa situs ini memiliki *attack surface* (permukaan serangan) paling luas dibandingkan target lainnya.

4.2.2 Tingkat Risiko

Analisis tingkat risiko dilakukan untuk mengelompokkan setiap celah keamanan yang ditemukan berdasarkan potensi dampak dan tingkat bahaya yang ditimbulkan terhadap target penelitian. Pengklasifikasian ini sangat penting guna memberikan panduan prioritas mitigasi bagi praktisi keamanan maupun pihak pengelola sistem informasi dalam menangani temuan secara efektif. Dalam analisis ini, setiap temuan dipetakan ke dalam empat kategori tingkat risiko, yaitu *High Risk* (Risiko Tinggi), *Medium Risk* (Risiko Sedang), *Low Risk* (Risiko Rendah), dan *Informational* (Informasi Konfigurasi).

Melalui perbandingan ini, penelitian bertujuan untuk mengukur sensitivitas antara OWASP ZAP dan Wapiti dalam mengidentifikasi ancaman yang paling kritis pada ketiga website target, yaitu uinarraniry.siakadcloud.com, student.mahad.ar-raniry.ac.id, dan pusatbahasa.ar-raniry.ac.id.

Tabel 4. 8 Tingkat Risiko

Website	Tools	High	Medium	Low	Info
uinarraniry.siakadcloud.com	OWASP ZAP	0	2	8	3
	Wapiti	1	2	4	0
student.mahad.ar-raniry.ac.id	OWASP ZAP	0	2	4	4
	Wapiti	1	2	2	0
pusatbahasa.ar-raniry.ac.id	OWASP ZAP	2	2	9	7
	Wapiti	1	2	6	0
JUMLAH TEMUAN	OWASP ZAP	2	6	21	14
	Wapiti	3	6	12	0
TOTAL	**OWASP ZAP**	**43**			
	Wapiti	**21**			

Berdasarkan rekapitulasi temuan pada Tabel 4.8 tercatat secara keseluruhan, OWASP ZAP menemukan total celah yang jauh lebih banyak yaitu 43 temuan dibandingkan Wapiti yang hanya menemukan 21 temuan. Hal ini didominasi oleh kemampuan OWASP ZAP dalam mendeteksi *Low Risk* dan *Informational* yang sangat detail. Sebaliknya, Wapiti cenderung lebih ringkas dan tidak menampilkan temuan kategori *Informational* pada ketiga website tersebut. Pada tingkat *Medium Risk*, kedua alat menunjukkan hasil yang identik karena masing-masing menemukan 2 celah di setiap website.

Mengenai alat mana yang lebih sensitif dalam menemukan celah *High Risk*, berikut adalah poin analisisnya:

1. Konsistensi Wapiti: Wapiti terbukti lebih sensitif pada dua dari tiga website target. Pada website Siakad dan Mahad, Wapiti berhasil menemukan masing-masing 1 celah High Risk, sedangkan OWASP ZAP tidak menemukan satu pun.
2. Keunggulan Spesifik ZAP: Meskipun secara total kalah jumlah pada dua website awal, OWASP ZAP menunjukkan performa sangat tinggi pada website Pusat Bahasa dengan menemukan 2 celah *High Risk*, unggul dari Wapiti yang hanya menemukan 1.
3. Kesimpulan Sensitivitas: Secara kuantitas total pada seluruh objek penelitian, Wapiti sedikit lebih sensitif dengan total 3 temuan High Risk, dibandingkan OWASP ZAP yang mengumpulkan 2 temuan. Wapiti mampu mendeteksi potensi bahaya kritis pada website yang dianggap "bersih" dari celah tinggi oleh ZAP. Namun, ZAP memiliki kedalaman pemindaian yang lebih baik pada target tertentu, seperti pada website Pusat Bahasa.

4.2.3 Cakupan OWASP Top 10 2021

Analisis cakupan dilakukan untuk mengevaluasi sejauh mana perangkat lunak pemindaian OWASP ZAP dan Wapiti mampu menjangkau berbagai kategori kerentanan sesuai dengan standar internasional OWASP Top 10 2021. Pemetaan ini bertujuan untuk mengidentifikasi kemampuan spesifik dari masing-masing alat dalam mendeteksi risiko keamanan yang paling relevan dan kritis bagi aplikasi web saat ini. Melalui pendekatan tersebut, penilaian tidak hanya berfokus pada aspek

kuantitatif temuan, tetapi juga meninjau kedalaman serta keluasan spektrum deteksi masing-masing perangkat lunak dalam memetakan ancaman keamanan di tingkat global.

Dengan merujuk pada kerangka kerja ini, setiap alert yang berhasil diidentifikasi akan diklasifikasikan secara sistematis ke dalam sepuluh kategori ancaman utama. Pengelompokan tersebut mencakup spektrum kerentanan yang luas, mulai dari kategori *Broken Access Control* hingga *Server-Side Request Forgery* (SSRF). Perbandingan cakupan ini menjadi indikator penting dalam menentukan efektivitas alat pemindaian guna memberikan gambaran keamanan yang menyeluruh pada ketiga website target penelitian di lingkungan UIN Ar-Raniry.

1. Pemetaan Temuan OWASP ZAP ke OWASP Top 10 2021

Tabel 4. 9 Cakupan OWASP ZAP ke OWASP Top 10

uinarraniry.siakadcloud.com			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Content Security Policy (CSP) Header Not Set*	A05:2021	*Security Misconfiguration*
2	*Missing Anti-clickjacking Header*	A05:2021	*Security Misconfiguration*
3	*Cookie No HttpOnly Flag*	A01:2021	*Broken Access Control*
4	*Cookie Without Secure Flag*	A01:2021	*Broken Access Control*
5	*Cookie without SameSite Attribute*	A01:2021	*Broken Access Control*
6	*Cross-Domain JavaScript Source File Inclusion*	A05:2021	*Security Misconfiguration*
7	*Server Leaks Version Information via "Server" Header*	A05:2021	*Security Misconfiguration*

8	*Strict-Transport-Security Header Not Set*	A05:2021	*Security Misconfiguration*
9	*X-Content-Type-Options Header Missing*	-	Bukan kerentanan sistem target
10	*ZAP is Out of Date*	-	Bukan kerentanan sistem target
11	*Modern Web Application*	-	*Informational / Metadata*
12	*Session Management Response Identified*	-	*Informational / Metadata*
13	*User Agent Fuzzer*	-	*Informational / Metadata*
student.mahad.ar-raniry.ac.id			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Content Security Policy (CSP) Header Not Set*	A05:2021	*Security Misconfiguration*
2	*Missing Anti-clickjacking Header*	A05:2021	*Security Misconfiguration*
3	*Server Leaks Version Information via Header*	A05:2021	*Security Misconfiguration*
4	*Strict-Transport-Security (HSTS) Header Not Set*	A05:2021	*Security Misconfiguration*
5	*Timestamp Disclosure - Unix*	A05:2021	*Security Misconfiguration*

6	*X-Content-Type-Options Header Missing*	A05:2021	*Security Misconfiguration*
7	*Information Disclosure - Suspicious Comments*	A05:2021	*Security Misconfiguration*
8	*Modern Web Application*	-	*Informational* (Bukan Celah)
9	*Re-examine Cache-control Directives*	A05:2021	*Security Misconfiguration*
10	*Retrieved from Cache*	-	*Informational* (Bukan Celah)
pusatbahasa.ar-raniry.ac.id			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Path Traversal*	A01:2021	*Broken Access Control*
2	*SQL Injection - SQLite (Time Based)*	A03:2021	*Injection*
3	*Content Security Policy (CSP) Header Not Set*	A05:2021	*Security Misconfiguration*
4	*Vulnerable JS Library*	A06:2021	*Vulnerable and Outdated Components*
5	*Big Redirect Detected*	A05:2021	*Security Misconfiguration*
6	*Cookie No HttpOnly Flag*	A01:2021	*Broken Access Control*
7	*Cookie Without Secure Flag*	A01:2021	*Broken Access Control*
8	*Cookie without SameSite Attribute*	A01:2021	*Broken Access Control*
9	*Cross-Domain JavaScript Source File Inclusion*	A05:2021	*Security Misconfiguration*

10	*Secure Pages Include Mixed Content*	A05:2021	*Security Misconfiguration*
11	*Strict-Transport-Security (HSTS) Not Set*	A05:2021	*Security Misconfiguration*
12	*Timestamp Disclosure - Unix*	A05:2021	*Security Misconfiguration*
13	*ZAP is Out of Date*	-	Peringatan Tool
14	*Authentication Request Identified*	A07:2021	*Identification and Authentication Failures*
15	*Charset Mismatch*	A05:2021	*Security Misconfiguration*
16	*Information Disclosure - Suspicious Comments*	A05:2021	*Security Misconfiguration*
17	*Modern Web Application*	-	*Informasi Teknologi*
18	*Re-examine Cache-control Directives*	A05:2021	*Security Misconfiguration*
19	*Session Management Response Identified*	A01:2021	*Broken Access Control*
20	*User Controllable HTML Element (Potential XSS)*	A03:2021	*Injection*

Tabel 4.9 menyajikan pemetaan komprehensif temuan kerentanan oleh OWASP ZAP yang diselaraskan dengan standar internasional OWASP Top 10 2021. Proses pemetaan ini dilakukan pada ketiga website target guna mengevaluasi relevansi temuan otomatis terhadap kategori ancaman yang dianggap paling kritis secara global. Melalui hasil klasifikasi tersebut, dapat ditarik beberapa poin inti sebagai berikut:

1. Dominasi Kategori A05:2021 (*Security Misconfiguration*): Kategori ini muncul secara konsisten dan menjadi temuan terbanyak di ketiga website (Siakad, Mahad, dan Pusat Bahasa). Hal ini mencakup absennya *security headers* seperti CSP, HSTS, dan *X-Content-Type-Options*. Ini

menunjukkan bahwa kerentanan umum pada infrastruktur web UIN Ar-Raniry terletak pada konfigurasi keamanan *server* yang belum optimal. Studi literatur yang dilakukan oleh Arief et al (2025) mengidentifikasi dua kerentanan utama, yaitu *Security Misconfiguration* dan *Identification and Authentication Failures.*

2. Keamanan Manajemen Sesi (A01:2021 - *Broken Access Control*): OWASP ZAP sangat efektif dalam mengidentifikasi kelemahan pada atribut *cookie* (*HttpOnly, Secure, dan SameSite*). Temuan ini muncul pada website Siakad dan Pusat Bahasa, yang mengindikasikan adanya risiko pencurian sesi pengguna melalui serangan *side-channel* atau skrip berbahaya.
3. Identifikasi Kerentanan Kritis pada Website Kompleks: Website pusatbahasa.ar-raniry.ac.id menunjukkan tingkat kerentanan yang paling kompleks dibandingkan dua website lainnya. ZAP berhasil mendeteksi celah berisiko tinggi seperti A01:2021 (*Path Traversal*) dan A03:2021 (SQL *Injection*), serta penggunaan pustaka yang usang pada A06:2021 (*Vulnerable and Outdated Components).*
4. Kedalaman Deteksi: Secara keseluruhan, OWASP ZAP mampu memetakan temuan ke dalam 5 hingga 6 kategori dari OWASP Top 10 2021 (A01, A03, A05, A06, dan A07). Hal ini menunjukkan bahwa OWASP ZAP memiliki cakupan deteksi yang luas, mulai dari *misconfiguration* sederhana hingga celah injeksi yang bersifat kritis pada sistem yang memiliki lebih banyak parameter *input*.

Hasil pengujian ini menunjukkan bahwa OWASP ZAP memiliki tingkat sensitivitas yang signifikan dalam mendeteksi berbagai jenis kerentanan pada sistem target. Fokus utama deteksi alat tersebut terletak pada aspek pengujian berbasis *header* serta mekanisme manajemen sesi yang diterapkan pada *website*. Temuan komprehensif ini nantinya akan dibandingkan secara mendalam dengan hasil pemetaan dari *tool* Wapiti guna menganalisis perbedaan karakteristik serta efektivitas deteksi di antara kedua perangkat lunak tersebut.

2. Pemetaan Temuan Wapiti ke OWASP Top 10 2021

Tabel 4. 10 Cakupan Wapiti ke OWASP Top 10

uinarraniry.siakadcloud.com			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Content Security Policy Configuration*	A05:2021	*Security Misconfiguration*
2	*Clickjacking Protection*	A05:2021	*Security Misconfiguration*
3	*HTTP Strict Transport Security (HSTS)*	A05:2021	*Security Misconfiguration*
4	*MIME Type Confusion*	A05:2021	*Security Misconfiguration*
5	*HttpOnly Flag cookie*	A01:2021	*Broken Access Control*
6	*Secure Flag cookie*	A01:2021	*Broken Access Control*
7	*TLS/SSL misconfigurations*	A02:2021	*Cryptographic Failures*
student.mahad.ar-raniry.ac.id			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Content Security Policy Configuration*	A05:2021	*Security Misconfiguration*
2	*Clickjacking Protection*	A05:2021	*Security Misconfiguration*
3	*HTTP Strict Transport Security (HSTS)*	A05:2021	*Security Misconfiguration*
4	*MIME Type Confusion*	A05:2021	*Security Misconfiguration*
5	*TLS/SSL misconfigurations*	A02:2021	*Cryptographic Failures*
pusatbahasa.ar-raniry.ac.id			
No	**Jenis Temuan**	**Kode OWASP**	**Nama Kategori**
1	*Content Security Policy Configuration*	A05:2021	*Security Misconfiguration*
2	*Clickjacking Protection*	A05:2021	*Security Misconfiguration*

3	*HTTP Strict Transport Security (HSTS)*	A05:2021	*Security Misconfiguration*
4	*MIME Type Confusion*	A05:2021	*Security Misconfiguration*
5	*HttpOnly Flag cookie*	A01:2021	*Broken Access Control*
6	*Inconsistent Redirection*	A05:2021	*Security Misconfiguration*
7	*Information Disclosure - Full Path*	A05:2021	*Security Misconfiguration*
8	*Secure Flag cookie*	A01:2021	*Broken Access Control*
9	*TLS/SSL misconfigurations*	A02:2021	*Cryptographic Failures*

Tabel 4.10 menampilkan hasil pemetaan temuan Wapiti pada ketiga website target (Siakad, Mahad, dan Pusat Bahasa). Dapat disimpulkan beberapa poin utama sebagai berikut:

1. Konsistensi pada Kategori A02:2021 (Cryptographic Failures): Berbeda dengan alat pembandingnya, Wapiti menunjukkan konsistensi yang sangat tinggi dalam mendeteksi kategori ini di seluruh objek penelitian. Temuan TLS/SSL *Misconfigurations* muncul di ketiga *website*, menunjukkan bahwa Wapiti memiliki modul pemindaian yang sangat peka terhadap konfigurasi enkripsi dan sertifikat pada *transport layer*.
2. Dominasi Miskonfigurasi Keamanan (A05:2021): Kategori *Security Misconfiguration* tetap menjadi penyumbang jenis temuan terbanyak. Wapiti tidak hanya mendeteksi absennya *security headers* standar (CSP, HSTS, *Clickjacking*), tetapi juga mampu menemukan celah spesifik lainnya seperti *Inconsistent Redirection* dan *Information Disclosure - Full Path* pada *website* Pusat Bahasa. Hal ini mengindikasikan kemampuan Wapiti dalam mendeteksi kebocoran informasi teknis *server* secara mendalam.
3. Fokus pada Kerentanan Akses (A01:2021 - *Broken Access Control*): Wapiti berhasil memetakan celah pada manajemen cookie (HttpOnly dan *Secure Flag)* pada *website* Siakad dan Pusat Bahasa. Ini menunjukkan bahwa Wapiti efektif dalam mengidentifikasi titik lemah pada kontrol akses yang dapat dieksploitasi untuk serangan pembajakan sesi.
4. Karakteristik Deteksi yang Ringkas dan Spesifik: Secara keseluruhan, Wapiti memetakan temuan ke dalam 3 kategori utama dari OWASP Top 10

2021 (A01, A02, dan A05). Meskipun jumlah kategori yang dideteksi lebih sedikit dibandingkan ZAP, Wapiti terbukti lebih fokus pada celah yang berkaitan langsung dengan konfigurasi teknis *server* dan enkripsi, tanpa menghasilkan banyak data *informational* atau metadata yang tidak relevan dengan kerentanan sistem.

Tabel 4. 11 Perbandingan Cakupan OWASP Top 10

Parameter Efektivitas	**CAKUPAN OWASP TOP 10**		**Unggul**
	OWASP ZAP	**Wapiti**	
Cakupan Kategori (Broadness)	Berhasil mendeteksi rata-rata 5 kategori OWASP Top 10 2021 (A01, A03, A05, A06, A07).	Berhasil mendeteksi rata-rata 3 kategori OWASP Top 10 2021 (A01, A02, A05).	OWASP ZAP
Sensitivitas High Risk	Menemukan total 2 celah *High Risk* (hanya pada *website* Pusat Bahasa).	Menemukan total 3 celah *High Risk* (tersebar di ketiga *website*).	Wapiti

Berdasarkan Tabel 4.11 dapast disimpulkan jika OWASP ZAP terbukti lebih unggul dalam mendeteksi variasi jenis kerentanan. Dengan jangkauan rata-rata 5 kategori OWASP Top 10, ZAP mampu memetakan spektrum ancaman yang lebih luas, mulai dari masalah kontrol akses (A01) hingga kegagalan autentikasi (A07). Dalam hal ini, OWASP ZAP bekerja seperti "jaring yang lebar" yang mampu menangkap banyak jenis ikan atau kerentanan dari berbagai kategori yang berbeda secara mendetail. Hal ini menunjukkan bahwa ZAP sangat efektif digunakan untuk audit keamanan menyeluruh karena kemampuannya "menyisir" berbagai jenis celah yang berbeda.

Sementara wapiti terbukti lebih unggul dalam mendeteksi celah yang bersifat kritis, *High Risk*. Meskipun secara jumlah kategori lebih sedikit dibandingkan ZAP, Wapiti lebih konsisten menemukan ancaman berbahaya di ketiga website target, tidak hanya terfokus pada satu website saja. Ini menunjukkan bahwa Wapiti memiliki akurasi tinggi dalam mendeteksi lubang keamanan yang paling fatal, menjadikannya alat yang sangat berguna untuk pengujian penetrasi cepat yang berfokus pada risiko berat. Secara analogi, Wapiti bekerja seperti "tombak yang tajam" di mana meskipun jangkauannya tidak selebar ZAP, alat ini jauh lebih efektif dalam mengenai sasaran yang paling besar dan berbahaya.

4.2.4 Stabilitas Hasil

Evaluasi stabilitas hasil melalui tiga tahap iterasi yaitu Cek 1, Cek 2, dan Cek 3 merupakan langkah krusial untuk memvalidasi reliabilitas data dan memastikan bahwa setiap alert yang terdeteksi bukan merupakan anomali teknis, melainkan representasi nyata dari celah keamanan. Konsistensi hasil pemindaian ini menjadi indikator utama bahwa algoritma pemindaian otomatis pada OWASP ZAP dan Wapiti bekerja dengan performa yang dapat diprediksi, sehingga mampu menyajikan analisis objektif mengenai ketahanan fungsional kedua *tool* dalam menghadapi struktur website yang kompleks serta respon dinamis dari server target.

Tabel 4. 12 Rekapitulasi Stabilitas Hasil Pemindaian Berdasarkan Pengujian Berulang

Website Target	**Tools**	**Jumlah Temuan**			**Status Stabilitas**
		Cek 1	**Cek 2**	**Cek 3**	
uinarraniry.siakadcloud.com	Owasp Zap	13	13	13	Stabil
	Wapiti	7	7	7	Stabil
student.mahad.ar-raniry.ac.id	Owasp Zap	10	6	6	Kurang Stabil
	Wapiti	5	5	5	Stabil
pusatbahasa.ar-raniry.ac.id	Owasp Zap	20	22	22	Kurang Stabil
	Wapiti	9	9	9	Stabil

Berdasarkan data pada Tabel 4.12, *tool* Wapiti menunjukkan tingkat stabilitas mutlak di seluruh objek penelitian dengan jumlah temuan yang konsisten sejak iterasi pertama. Hal ini mengindikasikan bahwa algoritma pemindaian pada Wapiti memiliki pola deteksi yang sangat ajek terhadap infrastruktur website di lingkungan

UIN Ar-Raniry. Keteguhan angka tersebut memberikan jaminan validitas bagi praktisi keamanan dalam memetakan prioritas mitigasi tanpa perlu melakukan pengujian berulang yang ekstensif.

Tool OWASP ZAP memperlihatkan karakteristik hasil yang fluktuatif pada situs Mahad dan Pusat Bahasa sebelum akhirnya mencapai titik stabil pada pemindaian kedua dan ketiga. Fenomena ini menunjukkan bahwa OWASP ZAP memiliki sensitivitas yang lebih dinamis dan memerlukan waktu sinkronisasi yang lebih mendalam terhadap respon *server* pada sesi awal pengujian. Meskipun sempat mengalami perubahan jumlah *alert* di tahap awal, konsistensi angka pada Cek 2 dan Cek 3 memberikan dasar yang kuat bahwa temuan akhir perangkat lunak tersebut telah terverifikasi secara stabil.

4.3 Analisis Kinerja Berdasarkan Waktu Pemindaian

Analisis kinerja ini difokuskan pada efisiensi waktu yang dibutuhkan oleh setiap *tool* dalam menyelesaikan proses pemindaian keamanan dari awal hingga akhir. Pengukuran waktu merupakan parameter krusial dalam operasional keamanan siber, karena berkaitan dengan kecepatan respons terhadap potensi ancaman. Dalam penelitian ini, waktu pemindaian diukur dalam satuan menit pada kondisi jaringan yang stabil untuk memastikan perbandingan yang adil antara OWASP ZAP dan Wapiti. Pemindaian dilakukan terhadap tiga objek penelitian utama di lingkungan UIN Ar-Raniry, yaitu portal akademik uinarraniry.siakadcloud.com, sistem asrama student.mahad.ar-raniry.ac.id, dan website pusatbahasa.ar-raniry.ac.id.

Tabel 4. 13 Kinerja Berdasarkan Waktu Pemindaian

WEBSITE	DURASI PEMINDAIAN		SELISIH WAKTU
	OWASP ZAP	WAPITI	
uinarraniry.siakadcloud.com	10	3	7 Menit
student.mahad.ar-raniry.ac.id	15	3	12 Menit
pusatbahasa.ar-raniry.ac.id	138	7	131 Menit

Data hasil pengukuran durasi pemindaian sebagaimana tercantum dalam Tabel 4.13 menjadi dasar utama dalam mengevaluasi efisiensi pengerjaan pengujian keamanan. Berdasarkan akumulasi waktu tersebut, dapat ditarik poin analisis

mengenai perbandingan performa masing-masing *tool* dalam menyelesaikan tugas pemindaian pada karakteristik sistem yang berbeda:

1. Kecepatan Unggul Wapiti: Secara konsisten di ketiga target website, Wapiti menunjukkan performa waktu yang jauh lebih cepat dibandingkan OWASP ZAP. Pada website Siakad dan Mahad, Wapiti hanya membutuhkan waktu masing-masing 3 menit untuk menyelesaikan proses pemindaian.
2. Efisiensi pada Website Kompleks: Perbedaan waktu yang paling mencolok terlihat pada pemindaian website pusatbahasa.ar-raniry.ac.id. OWASP ZAP membutuhkan waktu hingga 138 menit (2 jam 18 menit), sementara Wapiti mampu menyelesaikannya hanya dalam waktu 7 menit. Hal ini menunjukkan selisih efisiensi waktu yang sangat signifikan, mencapai lebih dari 18 kali lipat.
3. Korelasi Kedalaman Pemindaian dengan Waktu: Lamanya waktu yang dibutuhkan oleh OWASP ZAP berkorelasi dengan temuan pada sub-bab sebelumnya, di mana ZAP menemukan lebih banyak kategori *Informational* dan *Low Risk* dengan total 43 temuan dibandingkan Wapiti dengan total 21 temuan. Hal ini mengindikasikan bahwa mekanisme *spidering* dan *active scan* pada OWASP ZAP melakukan penelusuran parameter dan direktori secara lebih mendalam dan detail, namun berdampak pada durasi pemindaian yang jauh lebih lama.
4. Kinerja Rata-Rata: Secara rata-rata, Wapiti menyelesaikan tugasnya dalam waktu 4,3 menit per website, sedangkan OWASP ZAP memerlukan waktu rata-rata 10 menit per website. Data ini menunjukkan bahwa Wapiti memiliki keunggulan dari sisi kecepatan operasional (kinerja waktu), sementara OWASP ZAP lebih unggul dari sisi ketelitian hasil deteksi meskipun memakan waktu lebih lama.

Perbedaan durasi pemindaian yang sangat kontras ditemukan pada website pusatbahasa.ar-raniry.ac.id, di mana OWASP ZAP memerlukan waktu 138 menit sementara Wapiti hanya membutuhkan waktu 7 menit. Berdasarkan analisis terhadap karakteristik target, besarnya selisih waktu tersebut kemungkinan besar

disebabkan oleh kompleksitas struktur tautan dan jumlah halaman yang jauh lebih masif pada website tersebut dibandingkan dengan dua target lainnya.

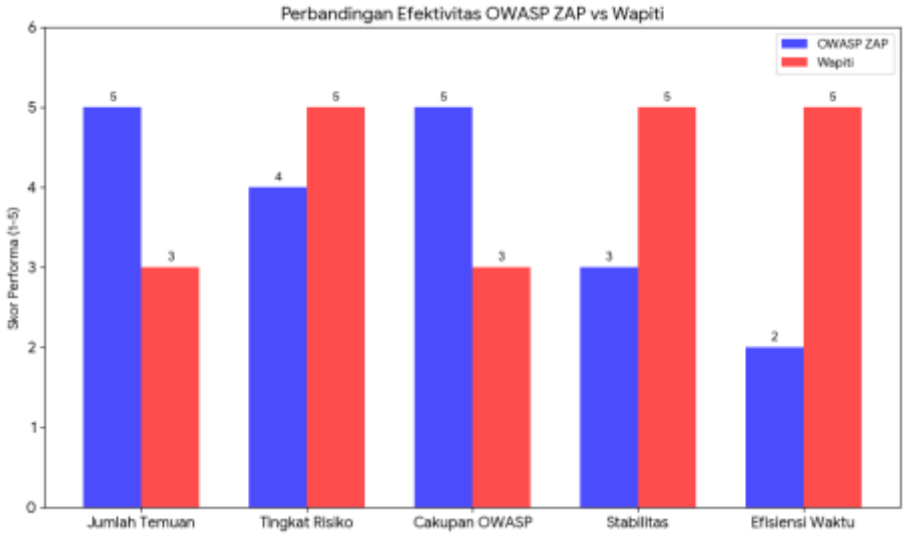
Fitur *crawler* atau *spidering* pada OWASP ZAP bekerja secara rekursif dan lebih intensif untuk memetakan seluruh permukaan aplikasi web sebelum melakukan *active scanning*. Hal ini mengakibatkan mesin pemindaian pada ZAP bekerja jauh lebih keras dalam menelusuri setiap direktori, parameter, dan skrip yang tertanam di dalam website Pusat Bahasa untuk memastikan cakupan deteksi yang menyeluruh. Di sisi lain, Wapiti memiliki mekanisme *crawling* yang lebih ringkas dan terfokus, sehingga mampu menyelesaikan pemindaian dalam waktu yang jauh lebih singkat. Meskipun performa waktu Wapiti unggul secara signifikan, durasi pemindaian yang lebih lama pada OWASP ZAP berbanding lurus dengan kemampuannya dalam mendeteksi total temuan yang lebih banyak (20 temuan) dibandingkan Wapiti (9 temuan) pada website yang sama.

4.4 Ringkasan Hasil Perbandingan

Ringkasan akhir dari penelitian ini disajikan dalam bentuk tabel dan diagram batang guna memaparkan kelebihan serta kekurangan masing-masing *tool* secara mendalam. Penyajian data tersebut bertujuan untuk memberikan gambaran komprehensif mengenai kapabilitas fungsional dari perangkat lunak pemindaian yang telah diuji pada sistem target. Melalui hasil perbandingan ini, analisis yang dihasilkan dapat dijadikan sebagai dasar rekomendasi objektif dalam pemilihan instrumen pengujian keamanan aplikasi web yang paling efektif.

4.4.1 Analisis Hasil

Visualisasi dalam bentuk diagram batang di bawah ini digunakan untuk memberikan perbandingan performa OWASP ZAP dan Wapiti. Grafik ini memetakan lima parameter utama: Jumlah Temuan, Tingkat Risiko, Cakupan OWASP Top 10, Stabilitas Hasil Deteksi, dan Waktu Pemindaian. Secara visual, performa kedua *tool* menunjukkan pola yang saling melengkapi. Berdasarkan grafik radar tersebut dapat dilihat performa kedua *tool* menunjukkan pola yang saling melengkapi.



Gambar 4. 11 Perbandingan Efektivitas

Gambar 4.11 menyajikan visualisasi perbandingan efektivitas antara OWASP ZAP dan Wapiti melalui format diagram batang berkelompok yang eksplisit. Batang berwarna biru mencerminkan dominasi OWASP ZAP yang sangat kuat pada parameter jumlah temuan serta luasnya cakupan kategori kerentanan yang terdeteksi pada sistem target. Namun, alat tersebut mencatatkan skor yang rendah pada efisiensi waktu dikarenakan durasi pemindaian otomatis yang relatif jauh lebih lama dibandingkan dengan alat pembandingnya.

Batang berwarna merah menunjukkan keunggulan mutlak *tool* Wapiti pada aspek efisiensi waktu serta konsistensi dalam mengidentifikasi celah keamanan tingkat tinggi (*High Risk*). Berbeda dengan parameter lainnya, kriteria stabilitas kini menunjukkan keunggulan bagi Wapiti yang mampu mempertahankan angka temuan secara ajek sejak iterasi pengujian pertama. Skor stabilitas OWASP ZAP berada di bawah Wapiti sebagai konsekuensi dari adanya fluktuasi jumlah *alert* yang ditemukan pada tahap pemindaian awal atau Cek 1.

Perbedaan pola capaian ini memberikan gambaran objektif bagi praktisi keamanan mengenai karakteristik fungsional dari masing-masing perangkat lunak tersebut. Integrasi hasil dari kedua *tool* ini sangat disarankan guna menutupi keterbatasan cakupan kategori pada Wapiti serta keterbatasan efisiensi waktu pada OWASP ZAP. Dengan demikian, pengelola sistem informasi di lingkungan UIN Ar-Raniry dapat memperoleh profil risiko keamanan yang lebih akurat dan menyeluruh untuk mendukung langkah mitigasi yang tepat sasaran.

4.4.2 Perbandingan Kelebihan dan Kekurangan

Subbab ini menyajikan perbandingan mendalam mengenai karakteristik operasional antara OWASP ZAP dan Wapiti sebagai instrumen pengujian keamanan. Analisis difokuskan pada keunggulan teknis serta keterbatasan yang ditemukan selama proses pemindaian pada ketiga website target di lingkungan UIN Ar-Raniry. Tabel 4.14 merangkum karakteristik utama masing-masing *tool* sebagai dasar rekomendasi strategis bagi praktisi keamanan siber dalam menentukan perangkat lunak yang paling sesuai dengan kebutuhan.

Tabel 4. 14 Perbandingan Kelebihan dan Kekurangan

Fitur	OWASP ZAP	Wapiti
Kelebihan Utama	Sangat detail dalam mendeteksi *security headers* dan manajemen sesi, serta memiliki cakupan kategori OWASP yang luas (A01-A07).	Memiliki efisiensi waktu yang tinggi, konsisten menemukan celah *High Risk*, serta menunjukkan stabilitas hasil yang sangat tinggi di setiap pemindaian.
Kekurangan Utama	Membutuhkan durasi pemindaian yang lama dan memiliki stabilitas hasil yang cenderung fluktuatif pada tahap pemindaian awal (Cek 1).	Memiliki cakupan kategori yang lebih terbatas dan cenderung mengabaikan temuan detail pada kategori *Informational*.
Rekomendasi Penggunaan	Digunakan untuk audit keamanan menyeluruh atau proses pemindaian mendalam yang digunakan untuk audit keamanan menyeluruh atau proses pemindaian mendalam yang dilakukan secara berkala.	Digunakan untuk *quick penetration testing* atau pemeriksaan harian yang mengutamakan kecepatan dan stabilitas hasil temuan detail pada kategori *Informational*.

Sebagai penutup diskusi pada bab ini, hasil evaluasi terhadap kedua tool secara menyeluruh menunjukkan bahwa tidak terdapat instrumen tunggal yang mampu mengungguli seluruh parameter pengujian secara mutlak. OWASP ZAP menunjukkan kapabilitas yang unggul dalam kedalaman deteksi serta luasnya spektrum kategori risiko (A01-A07) melalui mekanisme pemindaian yang mendetail. Di sisi lain, Wapiti menawarkan efisiensi waktu operasional yang sangat tinggi serta menunjukkan sensitivitas yang lebih konsisten dalam mengidentifikasi celah keamanan kritis (*High Risk*) pada seluruh objek penelitian.

Analisis ini juga menegaskan bahwa perbedaan durasi pemindaian yang kontras sangat dipengaruhi oleh kedalaman mekanisme penelusuran (*crawling*) serta intensitas analisis parameter dari masing-masing perangkat lunak terhadap infrastruktur sistem target. Selain itu, adanya fluktuasi data pada tahap awal pemindaian membuktikan krusialnya pengujian berulang guna memvalidasi reliabilitas temuan sebelum mencapai titik stabilitas. Dengan demikian, integrasi hasil dari kedua instrumen tersebut merupakan pendekatan paling optimal untuk menghasilkan profil risiko keamanan yang komprehensif bagi infrastruktur sistem informasi yang diuji.

BAB V
KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai analisis perbandingan efektivitas serta kinerja antara OWASP ZAP dan Wapiti pada tiga website UIN Ar-Raniry, maka dapat ditarik kesimpulan sebagai berikut:

1. Perbandingan Efektivitas Deteksi Kerentanan: OWASP ZAP terbukti lebih unggul secara kuantitas dengan total 43 temuan dan cakupan kategori yang lebih luas (5 kategori) dibandingkan Wapiti. Namun, Wapiti menunjukkan sensitivitas kualitas risiko yang lebih tinggi melalui temuan 3 celah High Risk secara konsisten serta memiliki tingkat stabilitas hasil yang lebih baik di setiap iterasi.
2. Perbandingan Kinerja Berdasarkan Waktu Pemindaian: Wapiti mencatatkan rata-rata waktu pemindaian 4,3 menit, jauh lebih efisien daripada OWASP ZAP yang memerlukan 10 menit. Keunggulan efisiensi ini mencapai puncaknya hingga 18 kali lipat saat memindai situs dengan struktur yang kompleks.

5.2 Saran

Berdasarkan hasil penelitian ini, peneliti merumuskan beberapa saran strategis sebagai berikut :

1. Pengelola IT UIN Ar-Raniry disarankan untuk segera memitigasi celah *High Risk* (terutama SQL *Injection* dan *Open*SSL CCS).
2. Perlu adanya integrasi metode pengujian manual di masa mendatang untuk memverifikasi temuan *false positive* yang mungkin muncul dari hasil pemindaian otomatis guna meningkatkan validitas data untuk peningkatan akurasi pengujian.
3. Penelitian selanjutnya diharapkan dapat memperluas cakupan objek pada aplikasi berbasis mobile serta menambahkan parameter analisis kinerja perangkat lunak yang lebih teknis, seperti konsumsi sumber daya CPU dan RAM saat proses pemindaian berlangsung

DAFTAR PUSTAKA

Alazmi, S., & De Leon, D. C. (2022). A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. *IEEE Access*, *10*, 33200–33219. https://doi.org/10.1109/ACCESS.2022.3161522

Amirul, M., Tristanti, N., Pramuja, G., & Fanani, I. (2024). *Analisis dan Pengujian Kerentanan Website Menggunakan OWASP ZAP Website Vulnerability Analysis and Testing Using OWASP ZAP*. *3*(1), 36–50.

Arief, M. I., Anwar, D. S., & Supriatman, A. (2025). *ANALISIS KERENTANAN WEBSITE MELALUI PENDEKATAN PENETRATION TESTING BERDASARKAN STANDAR OWASP TOP 10 STUDI KASUS SIMPELMAS UNIVERSITAS XYZ*. *05*.

Arnefia, Y., & Alam, R. (2025). *PERBANDINGAN EFEKTIVITAS OWASP ZAP , ACUNETIX , NIKTO MENGGUNAKAN VULNERABILITY SCANNING UNTUK*. *9*(2), 2975–2982.

Aryadi, T., Ridho, M., Hafizh, A., & Dani, I. (2026). *Pengujian Keamanan Website Menggunakan Metode Black Box dengan OWASP ZAP pada Kali Linux*. *2*(8), 1482–1491.

Aziz, S. (2025). *ANALISIS KINERJA WEB SERVER APACHE , NGINX , OPEN LITESPEED , DAN OPEN RESTY Apache , Nginx , Open Litespeed , And Open Resty Web Server Performance Analysis*. *11*(1), 1–9.

Bardian, H. A., Sutanto, I., Informatika, T., Unggul, U. E., Scanner, V., & Scripting, C. (2025). *PENGEMBANGAN APLIKASI VULNERABILITY SCANNER UNTUK*. *9*(1), 1–8.

Elanda, A., & Buana, R. L. (2021). *ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10*. *6*(2), 185–191.

Hidayatulloh, S., & Saptadiaji, D. (2021). *Penetration Testing pada Website*

Universitas ARS Menggunakan Open Web Application Security Project (OWASP). 77–86.

Jarupunphol, P., Seatun, S., & Buathong, W. (2023). Measuring Vulnerability Assessment Tools' Performance on the University Web Application. *Pertanika Journal of Science and Technology*, *31*(6), 2973–2993. https://doi.org/10.47836/pjst.31.6.19

Lubis, D. L., Nisa, F., & Ulya, A. (2025). *ANALISIS PERBANDINGAN KEAMANAN APLIKASI WEB PADA PLATFORM E-COMMERCE STUDI KASUS : SHOPEE , TIKTOK SHOP DAN FACEBOOK MARKETPLACE MENGGUNAKAN DYNAMIC APPLICATION SECURITY TESTING (DAST)*. *9*(6), 9240–9246.

Maniraj, S. P., Ranganathan, C. S., & Sekar, S. (2024). Securing Web Applications With Owasp Zap for Comprehensive Security Testing. *International Journal Of Advances In Signal And Image Sciences*, *10*(2), 12–23. https://doi.org/10.29284/ijasis.10.2.2024.12-23

Putri, S. J., Galih, D., Putri, P., Hayuhardhika, W., Putra, N., Elektro, D., Vokasi, S., & Mada, U. G. (2024). *Analisis Komparasi pada Teknik Black Box Testing (Studi Kasus : Website Lars)*. *5*(1), 23–28.

Qadir, S., Waheed, E., Khanum, A., & Jehan, S. (2025). Comparative evaluation of approaches & tools for effective security testing of Web applications. *PeerJ Computer Science*, *11*, 1–42. https://doi.org/10.7717/peerj-cs.2821

Rand, D. (2024). *Evaluating Web Application Vulnerability Scanners: Introducing the RD-Score for Comprehensive Performance Assessment*. *12*(11), 20–24.

Sampurno, W. (2025). *Vulnerability Assessment Web Instansi A Menggunakan*. 1–6.

Savova, Z., Atanasov, S. D., & Bogdanov, R. (2021). *Automated Web Application Scanning with Wapiti, Selenium, and SQLMap*. *60*(2), 57–60. www.nvu.bg.

Setiawan, E., & Fachri, F. (2025). *Pengujian dan Mitigasi Kerentanan Website*

Sistem Informasi Akademik Universitas Ma ' arif Nahdlatul Ulama Kebumen dengan OWASP ZAP Testing and Mitigation of Website Vulnerabilities in the Academic Information System of Universitas Ma ' arif Nahdlatul Ulama Kebumen using OWASP ZAP. *8*(1), 25–33.

Umar, R., Riadi, I., & Wicaksono, S. A. (2024). APPLICATION OF OWASP ZAP FRAMEWORK FOR SECURITY ANALYSIS OF LMS USING PENTEST METHOD. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *10*(2), 224–230. https://doi.org/10.33480/jitk.v10i2.5534

Yarphel, T. (2025). Comparative Performance Analysis of Web Vulnerability Scanners. *International Journal of Information Security*, *4*(1), 98–110. https://doi.org/10.34218/ijis_04_01_005