PENGUJIAN KEAMANAN KONFIGURASI SERVER DAN LAYANAN (*SECURITY MISCONFIGURATION*) PADA DOMAIN UNPAS.DEV MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT* BERBASIS PTES

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik
Informatika, Universitas Pasundan Bandung

Disusun oleh :

Muhamad Rizki Maulana
NRP. 22.304.0167

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG

JUNI 2026

LEMBAR PENGESAHAN LAPORAN TUGAS AKHIR

Telah disetujui Laporan Tugas Akhir:

Nama : Muhamad Rizki Maulana

NRP : 22.304.0167

Dengan judul :

"Pengujian Keamanan Konfigurasi Server dan Layanan (*Security Misconfiguration)* Pada Domain unpas.dev Menggunakan Metode *Vulnerability Assessment* Berbasis PTES"

Bandung, 30 Juni 2026

Menyetujui,

Pembimbing Utama

(Doddy Ferdiansyah, S.T., M.T)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir yang berjudul "Pengujian Keamanan Konfigurasi Server dan Layanan (*Security Misconfiguration)* Pada Domain unpas.dev Menggunakan Metode *Vulnerability Assessment* Berbasis PTES" adalah benar-benar hasil saya sendiri, bukan merupakan plagiat, duplikasi, atau pengambilan karya orang lain, kecuali bagian-bagian yang secara eksplisit dirujuk sumbernya dan dicantumkan dalam Daftar Pustaka. Apabila di kemudian hari terbukti bahwa pernyataan ini tidak benar, saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh serta sanksi lain sesuai dengan peraturan yang berlaku di Universitas Pasundan.

Dalam proses penyusunan Tugas Akhir ini, saya menggunakan bantuan perangkat kecerdasan buatan (AI*)* untuk mendukung proses analisis hasil dari berbagai tools pengujian dan untuk membantu penyuntingan bahasa. Setiap indikasi dari AI saya periksa dan verifikasi ulang sendiri berdasarkan bukti teknis yang saya peroleh, sebelum ditetapkan sebagai temuan akhir. Pengambilan keputusan dan kesimpulan akhir tetap sepenuhnya menjadi tanggung jawab saya sebagai penulis.

Demikian pernyataan ini saya buat dengan sebenar-benarnya, tanpa paksaan dari pihak mana pun, untuk dapat dipergunakan sebagaimana mestinya.

Bandung, 30 Juni 2026

Yang membuat pernyataan,

Muhamad Rizki Maulana

NRP.22.304.0167

ABSTRAK

Keamanan informasi menjadi aspek penting dalam pengelolaan sistem informasi akademik, terutama pada layanan berbasis web yang terhubung dengan jaringan internet publik. Fakultas Teknik Universitas Pasundan menggunakan domain unpas.dev untuk mendukung beberapa layanan akademik, seperti remedial, penilaian dosen sejawat, *whistleblowing system,* serta manajemen Kerja Praktik dan Tugas Akhir. Namun, layanan yang berjalan pada lingkungan produksi memiliki potensi risiko keamanan apabila terdapat kesalahan konfigurasi pada server dan layanan yang belum teridentifikasi. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan konfigurasi server dan layanan pada domain unpas.dev berdasarkan kategori *Security Misconfiguration* dalam OWASP Top 10 Tahun 2025 menggunakan metode *Vulnerability Assessment* berbasis *Penetration Testing Execution Standard* (PTES). Pengujian dilakukan dengan pendekatan *black-box* dan bersifat non-destruktif. Berdasarkan rangkaian pengujian yang telah dilaksanakan, ditemukan 7 temuan celah keamanan yang teridentifikasi pada aspek konfigurasi server dan layanan. Melalui penilaian menggunakan standar CVSS v4.0, diperoleh hasil bahwa 3 temuan berada pada tingkat risiko *Medium* (skor 5,3 hingga 6,9), 2 temuan pada tingkat risiko *Low*. 1 temuan bernilai *None* (0,0), dan 1 temuan bersifat informational. Hasil penelitian ini menghasilkan dokumentasi teknis, analisis dampak secara mendalam terhadap prinsip CIA triad, serta penyusunan rekomendasi perbaikan sebagai panduan bagi pengelola sistem untuk meningkatkan keamanan layanan akademik pada domain unpas.dev.

Kata Kunci: *Security Misconfiguration, Vulnerability Assessment,* PTES, OWASP Top 10 Tahun 2025*, CVSS v4.0.*

ABSTRACT

Information security is an important aspect in managing academic information systems, especially in web-based services connected to the public internet network. The Faculty of Engineering, Pasundan University, uses the unpas.dev domain to support several academic services, such as remedial, peer assessment, whistleblowing system, and management of Practical Work and Final Projects. However, services running in a production environment have potential security risks if there are unidentified configuration errors on servers and services. This study aims to evaluate the security level of server and service configurations in the unpas.dev domain based on the Security Misconfiguration category in the OWASP Top 10 2025 *using the Vulnerability Assessment method based on the Penetration Testing Execution Standard* (PTES). *The testing was carried out with a black-box approach and is non-destructive. Based on the series of tests that have been carried out, 7 security vulnerabilities were identified in the server and service configuration aspects. Through an assessment using the* CVSS v4.0 *standard, the results showed that 3 findings were at the Medium risk level (score* 5.3 *to* 6.9*), 2 findings at the Low risk level. One finding was rated None* (0.0), *and one finding was informational. The results of this study produced technical documentation, an in-depth impact analysis of the* CIA *triad principle, and the development of improvement recommendations as a guide for system administrators to improve the security of academic services in the unpas.dev domain.*

Keywords: *Security Misconfiguration, Vulnerability Assessment,* PTES, OWASP Top 10 2025, CVSS v4.0.

KATA PENGANTAR

Puji dan Syukur penulis panjatkan ke hadirat Allah SWT karena atas rahmat, karunia, dan hidayah-Nya, penulis dapat menyelesaikan laporan tugas akhir ini dengan baik. Laporan tugas akhir ini disusun sebagai salah satu syarat dalam pelaksanaan tugas akhir program Studi Teknik Informatika, Fakultas Teknik, Universitas Pasundan. Penelitian ini membahas Pengujian keamanan konfigurasi server dan layanan dengan fokus pada *Security Misconfiguration* berdasarkan OWASP Top 10 Tahun 2025, serta menggunakan metode *Vulnerability Assessment* berbasis PTES.

Dalam proses penyusunan laporan tugas akhir ini, penulis menyadari bahwa penyelesaian laporan tidak terlepas dari bantuan, arahan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Kedua orang tua serta adik-adik penulis, yang doanya tidak pernah putus di setiap sujud dan yang selalu menjadi alasan penulis untuk terus bertahan meski di tengah rasa lelah dan keraguan. Terima kasih atas kasih sayang, kesabaran, dan pengorbanan yang tidak pernah bisa terbalas oleh apapun, termasuk oleh lembar-lembar laporan ini.
2. Bapak Doddy Ferdiansyah, S.T., M.T., selaku dosen pembimbing, yang dengan penuh kesabaran meluangkan waktu, memberikan arahan, serta masukan berharga di setiap tahap penyusunan tugas akhir ini. Terima kasih atas kepercayaan dan bimbingan yang diberikan, yang menjadikan proses ini bukan hanya tentang menyelesaikan sebuah laporan, tetapi juga proses belajar yang sangat berarti bagi penulis.
3. Bapak/Ibu dosen Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pasundan yang telah membekali penulis dengan ilmu, wawasan, dan nilai-nilai yang menjadi bekal berharga sepanjang masa perkuliahan hingga terselesaikannya tugas akhir ini.
4. Teman-teman penulis, yang senantiasa hadir memberi dukungan, semangat, dan pengertian, baik di saat suka maupun ketika proses ini terasa berat. Terima kasih telah menjadi tempat berbagi cerita dan menjadi pengingat bahwa penulis tidak pernah benar-benar berjalan sendiri dalam menyelesaikan tugas akhir ini.
5. Seseorang yang spesial bagi penulis, yang selalu berada di sisi penulis, menjadi tempat berbagi cerita, air mata, dan tawa sepanjang perjalanan ini, serta dengan tulus memahami setiap keluh kesah dan tak pernah berhenti percaya pada penulis untuk terus melangkah meski lelah, menjadi rumah yang selalu menyenangkan di tengah kesibukan menyusun tugas akhir ini, serta atas cinta, kesabaran, dan kehadiran yang menjadi kekuatan tak terlihat di balik selesainya laporan ini.

Penulis menyadari bahwa laporan tugas akhir ini masih memiliki kekurangan, baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun agar laporan ini dapat disempurnakan pada tahap penelitian selanjutnya.

Akhir kata, penulis berharap laporan tugas akhir ini dapat memberikan manfaat bagi penulis, pihak terkait, serta pembaca yang memiliki keterkaitan pada bidang keamanan informasi

Bandung, 30 Juni 2026

Penulis

DAFTAR ISI

DAFTAR ISTILAH

Daftar istilah berikut disusun berdasarkan istilah-istilah yang digunakan dalam penelitian ini. Penjelasan istilah bersifat ringkas untuk membantu pembaca memahami konteks penelitian.

No	Istilah	Keterangan
1	*Black-box Testing*	Pendekatan pengujian keamanan yang dilakukan tanpa mengetahui konfigurasi internal sistem, sehingga penguji bertindak seperti pihak luar yang hanya melihat sistem dari sisi publik.
2	CVSS	Singkatan dari *Common Vulnerability Scoring System,* yaitu sistem penilaian untuk menentukan tingkat keparahan suatu kerentanan.
3	*Database Server*	Server yang digunakan untuk menyimpan, mengelola, dan menyediakan akses terhadap data dalam basis data.
4	*Directory Listing*	Kondisi ketika direktori pada web server dapat terlihat oleh pengguna, sehingga berpotensi membuka informasi yang seharusnya tidak dapat diakses secara bebas.
5	Domain	Alamat unik yang digunakan untuk mengakses suatu layanan atau sistem melalui internet.
6	*Exploitation*	Tahap pengujian untuk membuktikan apakah suatu kerentanan dapat dimanfaatkan dalam skenario pengujian yang sah dan terkontrol.
7	*Grey-box Testing*	Pendekatan pengujian keamanan yang dilakukan dengan sebagian informasi internal sistem diberikan kepada penguji.
8	Hak Akses	Pengaturan yang menentukan pihak mana saja yang dapat membaca. mengubah, menjalankan, atau mengelola file, direktori, maupun layanan tertentu.
9	*Intelligence Gathering*	Tahap pengumpulan informasi awal mengenai target pengujian, seperti domain, subdomain, port terbuka, layanan aktif, dan teknologi yang digunakan.
10	Keamanan Informasi	Upaya untuk menjaga kerahasiaan, keutuhan, dan ketersediaan informasi agar tidak diakses, diubah, atau diganggu oleh pihak yang tidak berwenang.
11	Konfigurasi Default	Pengaturan bawaan pada sistem, aplikasi, atau layanan yang belum disesuaikan dengan kebutuhan keamanan.
12	Layanan	Program atau fungsi yang berjalan pada server untuk menyediakan akses tertentu, seperti layanan web, basis data, email, atau administrasi jarak jauh.
13	Lingkungan Produksi	Lingkungan sistem yang digunakan secara aktif oleh pengguna dan terhubung dengan layanan operasional.

No	Istilah	Keterangan
14	Mail Server	Server yang digunakan untuk mengelola pengiriman, penerimaan, dan penyimpanan email.
15	Mitigasi	Upaya untuk mengurangi, memperbaiki, atau mengendalikan risiko keamanan yang ditemukan pada sistem.
16	*Non-Destruktif*	Pendekatan pengujian yang dilakukan tanpa merusak, menghapus, mengubah atau mengganggu data dan layanan yang sedang berjalan.
17	OWASP	Singkatan dari *Open Web Application Security Project,* yaitu organisasi yang menyediakan panduan, standar, dan referensi terkait keamanan aplikasi web.
18	OWASP Top 10	Daftar 10 risiko keamanan aplikasi web yang umum digunakan sebagai acuan dalam mengidentifikasi dan mengklasifikasikan kerentanan.
19	*Penetration Testing*	Metode pengujian keamanan dengan mensimulasikan serangan terhadap sistem untuk mengetahui apakah kerentanan dapat dimanfaatkan oleh pihak yang tidak berwenang.
20	Port	Jalur komunikasi pada jaringan yang digunakan oleh layanan tertentu untuk menerima atau mengirim data.
21	Port Terbuka	Kondisi ketika port pada server dapat diakses melalui jaringan, baik secara internal maupun publik.
22	*Post-Exploitation*	Tahap setelah eksploitasi yang bertujuan untuk menganalisis dampak lanjutan dari kerentanan yang berhasil diverifikasi.
23	*Pre-engagement Interaction*	Tahap awal dalam PTES yang berisi penentuan tujuan, ruang lingkup, batasan, aturan, serta izin pelaksanaan pengujian.
24	PTES	Singkatan dari *Penetration Testing Execution Standard,* yaitu kerangka kerja yang digunakan untuk menjalankan *penetration testing* secara sistematis mulai dari persiapan hingga pelaporan.
25	*Reporting*	Tahap penyusunan laporan hasil pengujian yang berisi temuan, bukti, dampak, tingkat risiko, dan rekomendasi perbaikan.
26	Rekomendasi Perbaikan	Saran teknis yang diberikan berdasarkan hasil pengujian untuk meningkatkan keamanan sistem.
27	Risiko Keamanan	Potensi terjadinya kerugian atau gangguan akibat adanya ancaman yang memanfaatkan kerentanan pada sistem.

No	Istilah	Keterangan
28	*Security Headers*	Konfigurasi pada HTTP header yang digunakan untuk membantu meningkatkan perlindungan aplikasi web dari serangan berbasis peramban.
29	*Security Misconfiguration*	Kesalahan konfigurasi keamanan pada server, layanan, aplikasi, atau komponen pendukung yang dapat menyebabkan celah keamanan.
30	*Security Testing*	Proses pengujian keamanan sistem untuk menemukan kelemahan, kerentanan, atau celah keamanan yang dapat menimbulkan risiko terhadap sistem.
31	Server	Komputer atau sistem yang menyediakan layanan, data, atau sumber daya kepada pengguna atau sistem melalui jaringan.
32	*Server Hardening*	Proses penguatan keamanan server dengan membatasi layanan yang tidak diperlukan, memperbarui sistem, mengatur hak akses, dan menyesuaikan konfigurasi agar lebih aman.
33	SSL/TLS	Protokol keamanan yang digunakan untuk mengenk ripsi komunikasi antara pengguna dan server agar data tidak mudah disadap.
34	Subdomain	Bagian tambahan dari domain utama yang digunakan untuk memisahkan atau mengelola layanan tertentu.
35	*Threat Modeling*	Tahap pemetaan ancaman berdasarkan informasi yang telah dikumpulkan untuk menentukan potensi risiko terhadap sistem.
36	unpas.dev	Domain yang menjadi objek penelitian dalam laporan tugas akhir ini, khususnya pada aspek keamanan konfigurasi server dan layanan.
37	*Vulnerability Analysis*	Tahap analisis terhadap kelemahan atau kerentanan yang ditemukan untuk mengetahui potensi risiko keamanan.
38	*Vulnerability Assessment*	Proses identifikasi dan analisis kerentanan pada sistem tanpa melakukan eksploitasi secara langsung.
39	Web Server	Server yang menyediakan layanan web agar halaman atau aplikasi web dapat diakses melalui browser.
40	*White-box Testing*	Pendekatan pengujian keamanan yang dilakukan dengan pengetahuan penuh terhadap sistem, termasuk konfigurasi, kode, dan arsitektur internal.

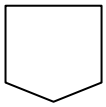
DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SIMBOL

1. *Flow Direction*

Nama	Simbol	Deskripsi
Proses		Melambangkan suatu langkah, tindakan, atau proses yang dilakukan dalam suatu alur
Flow Line		Menunjukkan arah aliran atau urutan proses dari satu simbol menuju simbol berikutnya
Off-Page Connector		Menghubungkan alur proses yang berlanjut dari satu halaman ke halaman yang lain
Decision		Menunjukkan suatu titik pengambilan keputusan dalam alur proses, dimana terdapat dua atau lebih kemungkinan yang menentukan arah alur selanjutnya.

2. *Fishbone Diagram*

Nama	Simbol	Deskripsi
Head		Menggambarkan penyebab / akibat dari permasalahan
Spine		Memetakan arah penyebab permasalahan

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi menjadi salah satu tantangan krusial bagi institusi pendidikan tinggi di Indonesia. Seiring dengan meningkatnya penggunaan sistem informasi berbasis web untuk mendukung layanan akademik, risiko serangan siber terhadap sistem tersebut juga semakin meningkat. Sistem akademik menyimpan berbagai data sensitif seperti identitas mahasiswa, nilai akademik, serta informasi administratif yang jika tidak dikelola dengan baik dapat menjadi target serangan siber. Oleh karena itu, pengelolaan keamanan sistem informasi menjadi aspek yang sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data [WHI22].

Dalam beberapa tahun terakhir, sektor pendidikan juga mulai menjadi sasaran kebocoran data dan serangan siber. Dugaan kebocoran data mahasiswa dari sejumlah perguruan tinggi di Indonesia pernah terungkap setelah data pribadi mahasiswa dilaporkan diperjualbelikan di forum *dark web*. Data yang diduga bocor mencakup informasi sensitif seperti nama, email, nomor telepon, hingga riwayat akademik yang berpotensi disalahgunakan untuk berbagai tindakan kriminal, seperti phishing dan pencurian identitas. Kejadian tersebut kemudian menjadi perhatian publik dan pemerintah karena menunjukkan adanya risiko serius terhadap keamanan data pribadi mahasiswa [DEW26].

Salah satu penyebab umum terjadinya insiden keamanan pada sistem informasi berbasis web adalah kesalahan konfigurasi sistem atau *Security Misconfiguration*. Berdasarkan laporan OWASP Top 10 tahun 2025, *Security Misconfiguration* merupakan salah satu kerentanan paling umum yang terjadi pada aplikasi web dan infrastruktur server. Kesalahan konfigurasi dapat berupa port layanan yang terbuka secara publik, penggunaan konfigurasi *default*, atau pengaturan keamanan server yang tidak optimal sehingga dapat dimanfaatkan oleh penyerang untuk mendapatkan akses tidak sah ke dalam sistem [OWA25].

Fakultas Teknik Universitas Pasundan melalui domain unpas.dev menyediakan layanan akademik penting seperti remedial, penilaian dosen sejawat, *whistleblowing system*, serta manajemen Kerja Praktik dan Tugas Akhir (KPTA). Layanan-layanan tersebut beroperasi pada lingkungan produksi yang terhubung langsung dengan jaringan internet publik. Infrastruktur sistem sebelumnya pernah mengalami insiden keamanan seperti serangan *ransomware* dan *deface*, yang salah satunya disebabkan oleh kesalahan konfigurasi server, seperti terbukanya port database (3306) ke jaringan publik serta pengaturan keamanan sistem yang kurang optimal. Namun hingga saat ini belum pernah dilakukan pengujian keamanan secara formal terhadap konfigurasi server sejak domain tersebut diaktifkan. Kondisi ini menimbulkan potensi risiko keamanan apabila terdapat kesalahan konfigurasi yang belum teridentifikasi.

Berdasarkan permasalahan tersebut, diperlukan pengujian keamanan sistem secara preventif menggunakan metode *Vulnerability Assessment* berbasis *Penetration Testing Execution Standard* (PTES) yang menyediakan kerangka kerja secara sistematis dalam melakukan pengujian keamanan mulai dari tahap pengumpulan informasi, analisis kerentanan hingga pelaporan hasil pengujian [PTE14]. Oleh karena itu, penelitian ini dilakukan untuk menguji tingkat keamanan konfigurasi server dan layanan pada domain unpas.dev serta memberikan perbaikan guna meningkatkan keamanan sistem.

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, masalah yang dapat diidentifikasi adalah sebagai berikut:

1. Infrastruktur domain unpas.dev pernah mengalami insiden keamanan yang berkaitan dengan kesalahan konfigurasi server, namun hingga saat ini belum pernah dilakukannya pengujian keamanan khusus pada konfigurasi server dan layanan pada domain unpas.dev sejak diaktifkan pada Maret 2024.
2. Belum diketahui kondisi keamanan dan tingkat risiko konfigurasi server serta layanan berdasarkan parameter *Security Misconfiguration.*
3. Belum tersedianya panduan atau rekomendasi teknis bagi pengelola sistem dalam melakukan evaluasi keamanan konfigurasi server sebagai langkah preventif.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana hasil pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev berdasarkan parameter *Security Misconfiguration* OWASP Top 10 Tahun 2025 menggunakan metode *Vulnerability Assessment* berbasis PTES?
2. Bagaimana tingkat risiko dari temuan *Security Misconfiguration* yang diperoleh pada konfigurasi server dan layanan domain unpas.dev?
3. Bagaimana rekomendasi perbaikan dan penguatan konfigurasi server serta layanan yang dapat diberikan kepada pengelola sistem berdasarkan hasil pengujian?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, maka tujuan penelitian ini adalah sebagai berikut:

1. Melakukan pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev berdasarkan parameter *Security Misconfiguration* OWASP Top 10 Tahun 2025 menggunakan metode *Vulnerability Assessment* berbasis PTES dengan pendekatan *black-box* dan non-destruktif.

2. Menilai tingkat risiko dari setiap temuan *Security Misconfiguration* yang diperoleh pada konfigurasi server dan layanan domain unpas.dev menggunakan CVSS v4.0.
3. Menyusun rekomendasi teknis perbaikan dan penguatan konfigurasi server serta layanan berdasarkan hasil pengujian yang telah divalidasi.

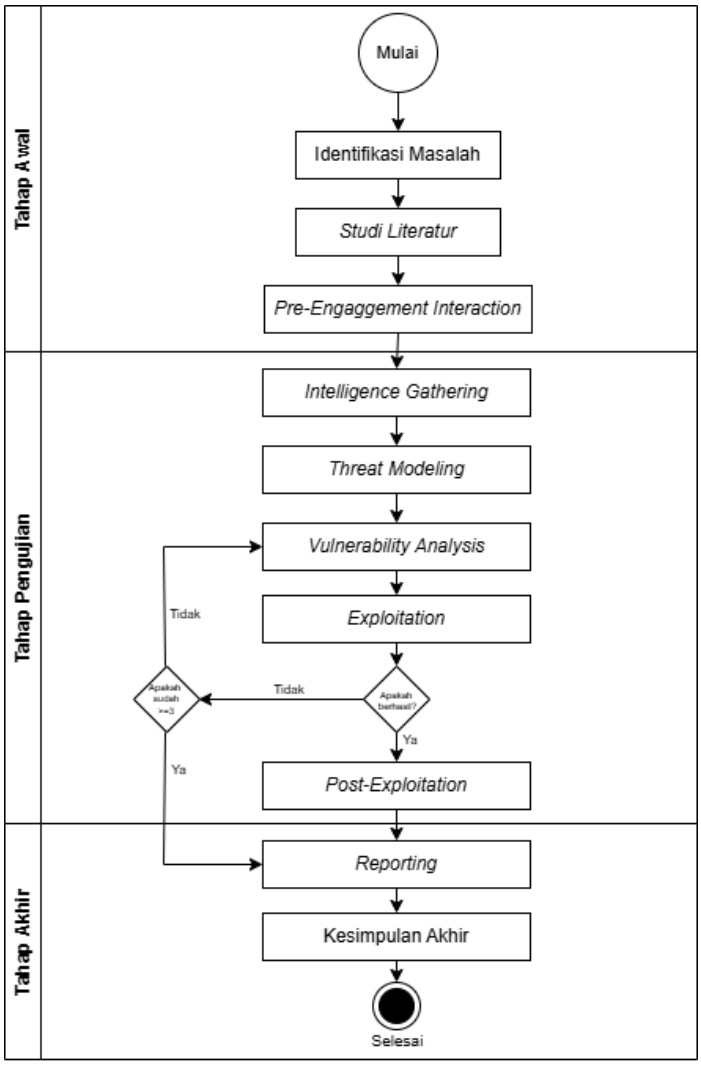
1.5 Lingkup dan Batasan Penelitian

Lingkup atau batasan dalam penelitian ini adalah sebagai berikut:

1. Objek penelitian difokuskan pada layanan akademik yang berjalan pada domain unpas.dev di lingkungan Fakultas Teknik Universitas Pasundan.
2. Pengujian keamanan pada penelitian ini mengacu pada kategori *Security Misconfiguration* berdasarkan OWASP Top 10 Tahun 2025.
3. Penelitian ini tidak mencakup pengujian terhadap kerentanan lain di luar kategori *Security Misconfiguration*, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), maupun kelemahan logika bisnis aplikasi.
4. Pengujian dilakukan secara non-destruktif, yaitu tanpa mengubah, merusak, maupun memanipulasi data serta mengganggu ketersediaan layanan yang sedang berjalan.
5. Pengujian dilakukan menggunakan pendekatan *black-box testing*, yaitu tanpa pengetahuan awal mengenai konfigurasi internal sistem.
6. Pengujian ini dilakukan pada domain, subdomain, port, dan layanan yang termasuk ruang lingkup pengujian. Apabila ditemukan aplikasi, subdomain, port, atau layanan lain di luar ruang lingkup, objek tersebut akan dicatat sebagai informasi pendukung dan tidak dilanjutkan ke tahap analisis kerentanan maupun validasi temuan.
7. Penggunaan AI dalam penelitian ini dibatasi sebagai alat bantu untuk menganalisis hasil awal tools pengujian dan untuk membantu penyuntingan bahasa. Setiap hasil dari AI diperiksa dan diverifikasi ulang sendiri oleh peneliti berdasarkan bukti teknis yang diperoleh. Pengujian, perhitungan CVSS, dan kesimpulan akhir sepenuhnya dilakukan sendiri oleh peneliti.
8. Penelitian ini dilaksanakan hingga tahap *Vulnerability Analysis*. Fase *Exploitation* dan *Post-Exploitation* pada kerangka PTES tidak dilaksanakan. Verifikasi manual terhadap indikasi temuan dilakukan sebagai bagian dari tahap *Vulnerability Analysis* melalui observasi non-destruktif tanpa melakukan upaya pemanfaatan lebih lanjut terhadap temuan yang teridentifikasi.

1.6 Metodologi Penelitian

Metodologi dalam penelitian ini disusun secara sistematis untuk memastikan setiap proses berjalan secara terstruktur. Gambaran umum mengenai tahapan tersebut dapat dilihat pada gambar di bawah ini:



Gambar 1. 1 Metodologi Tugas Akhir

1. Tahap Awal

   Pada tahap awal, dilakukan identifikasi masalah terkait risiko keamanan pada layanan domain unpas.dev yang kemudian diselaraskan dengan studi literatur mengenai OWASP Top 10 Tahun 2025 dan metode PTES. Di sini juga dilakukan penetapan batasan pengujian agar prosesnya tetap aman dan tidak mengganggu layanan yang aktif.

2. Tahap Pengujian

   Tahap ini mencakup persiapan teknis dan pengumpulan informasi awal terhadap target yaitu unpas.dev. Selanjutnya, dilakukan analisis untuk mencari celah keamanan yang

dilanjutkan dengan verifikasi manual guna memastikan validitas indikasi kerentanan yang ditemukan pada server dan layanan.

3. Tahap Akhir

   Pada tahap akhir, dibuat laporan hasil pengujian yang memuat dokumentasi temuan. Laporan ini mencakup penilaian risiko menggunakan CVSS, penyusunan rekomendasi perbaikan, serta kesimpulan akhir dari seluruh rangkaian pengujian yang telah dilakukan.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun untuk memberikan gambaran umum mengenai isi dari setiap bab. Adapun sistematika penulisan dalam laporan tugas akhir ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang penelitian, identifikasi masalah, rumusan masalah, tujuan penelitian, lingkup dan batasan penelitian, metodologi penelitian, serta sistematika tugas akhir. Bab ini menjelaskan dasar permasalahan yang melatarbelakangi perlunya dilakukan pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev.

BAB 2 LANDASAN TEORI

Bab ini berisi teori-teori yang digunakan sebagai dasar dalam penelitian, meliputi pengujian keamanan, *Vulnerability Assessment, penetration testing execution standard* (PTES), OWASP Top 10 Tahun 2025, *Security Misconfiguration,* konfigurasi server dan layanan, *server hardening*, pengamanan port dan layanan, serta kerangka penilaian risiko menggunakan CVSS v4.0 beserta kajian penelitian terdahulu yang relevan dengan topik penelitian.

BAB 3 SKEMA PENELITIAN

Bab ini berisi penjelasan mengenai skema penelitian yang digunakan, meliputi pendahuluan skema penelitian, alur penelitian, perumusan masalah, analisis sebab akibat menggunakan diagram fishbone, solusi masalah, kerangka berpikir teoritis, gambaran produk tugas akhir, skema analisis teori, objek penelitian, dan profil tempat penelitian. Bab ini menjelaskan alur penelitian secara sistematis yang telah dijelaskan pada bab-bab sebelumnya.

BAB 4 ANALISIS DAN PERANCANGAN PENGUJIAN

Bab ini berisi analisis kebutuhan teknis dan perancangan skenario pengujian. Di dalamnya dijabarkan mengenai kebutuhan data, legalitas, perancangan tools terbuka (*open-source),* perancangan aktivitas teknis untuk setiap fase PTES, serta penyusunan *Test Case* dan *Test Scenario* berdasarkan 7 parameter *Security Misconfiguration*

BAB 5 HASIL DAN PEMBAHASAN

Bab ini berisi dokumentasi teknis dan pembahasan mendalam dari implementasi pengujian yang telah dilakukan. Pembahasan disajikan secara urut mengikuti fase operasional PTES, mencakup

hasil pengumpulan informasi aktif/pasif, pemetaan ancaman, analisis kerentanan otomatis dan manual, validasi celah keamanan, analisis dampak berbasis CIA triad terhadap sistem, hingga perhitungan tingkat keparahan risiko menggunakan CVSS v4.0 serta penyusunan daftar rekomendasi perbaikan.

BAB 6 KESIMPULAN DAN SARAN

Bab ini berisi bagian akhir laporan yang memuat kesimpulan menyeluruh yang menjawab seluruh rumusan masalah penelitian berdasarkan hasil temuan teknis yang diperoleh, serta pemberian saran teknis bagi pengelola sistem maupun arahan bagi peneliti selanjutnya.

DAFTAR PUSTAKA

Bagian ini berisi daftar referensi yang digunakan dalam penyusunan laporan tugas akhir, baik berupa buku, jurnal, standar, dokumen resmi, maupun sumber lain yang relevan dengan penelitian.

LAMPIRAN

Bagian ini berisi dokumen pendukung yang melengkapi isi laporan tugas akhir, seperti bukti wawancara, bukti persetujuan izin pengujian, serta dokumen lain yang berkaitan dengan pelaksanaan penelitian.

BAB 2
LANDASAN TEORI

2.1 Pengujian Keamanan (*Security Testing)*

Pengujian keamanan (*security testing)* merupakan proses pengujian yang dilakukan secara sistematis untuk mengevaluasi keamanan sistem informasi melalui perencanaan dan pelaksanaan pengujian teknis, serta analisis hasil guna mengidentifikasi kerentanan dan menentukan strategi mitigasi [SCA08b]. Aktivitas ini menjadi komponen penting dalam siklus hidup sistem karena membantu mengidentifikasi kerentanan, termasuk kesalahan konfigurasi yang dapat menimbulkan risiko keamanan pada sistem [OWA25].

Konsep dasar *security testing* berakar pada kebutuhan untuk melindungi tiga prinsip utama keamanan informasi, yaitu *confidentiality, integrity,* dan *availability* [ISO22a]. *Confidentiality* menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang, *integrity* menjamin keutuhan dan akurasi data dari modifikasi yang tidak sah, sedangkan *availability* menjamin ketersediaan sistem dan data ketika dibutuhkan oleh pengguna yang sah [NIS17]. Ketiga prinsip tersebut menjadi acuan utama dalam merancang skenario pengujian yang komprehensif agar seluruh aspek keamanan dapat dievaluasi secara seimbang. Apabila salah satu dari ketiga prinsip tersebut tidak terpenuhi, maka sistem dianggap memiliki risiko keamanan yang harus segera ditangani melalui mekanisme mitigasi yang sesuai dengan konteks operasional organisasi [NIS12].

2.1.1 Jenis-jenis *Security Testing*

Security testing terdiri dari berbagai jenis pengujian yang diklasifikasikan berdasarkan tujuan, pendekatan dan kedalaman analisis terhadap sistem [SCA08b]. Setiap jenis pengujian memiliki karakteristik dan keluaran yang berbeda sehingga metode yang digunakan harus disesuaikan dengan kebutuhan pengujian. Pemahaman terhadap variasi metode ini menjadi penting, khususnya dalam pengujian server yang rentan terhadap kesalahan konfigurasi [OWA25].

2.1.1.1 *Vulnerability Assessment*

Vulnerability Assessment merupakan proses sistematis untuk mengidentifikasi dan menganalisis kerentanan tanpa melakukan eksploitasi terhadap sistem [SCA08b]. Melalui proses ini, penguji dapat memperoleh daftar kerentanan beserta tingkat keparahannya sebagai dasar dalam menentukan langkah mitigasi. Dalam praktiknya, metode ini efektif digunakan untuk mendeteksi kesalahan konfigurasi seperti layanan usang, *patch* yang belum diperbarui, dan port terbuka yang tidak terlindungi [OWA25].

2.1.1.2 *Penetration Testing*

Penetration Testing merupakan metode pengujian keamanan yang dilakukan dengan mensimulasikan serangan nyata untuk mengeksploitasi kerentanan yang ada pada sistem [SCA08b]. Pendekatan ini memberikan gambaran konkret mengenai dampak yang dapat ditimbulkan dari celah

keamanan yang ditemukan. Metode ini sangat relevan untuk memverifikasi apakah kesalahan konfigurasi dapat benar-benar dieksploitasi dalam kondisi nyata [PTE14]. Berdasarkan pendekatan, *penetration testing* dapat dilakukan dalam bentuk *black-box, white-box,* dan *gray-box* sesuai dengan tingkat informasi yang dimiliki oleh penguji [OWA25].

2.1.1.3 *Security Auditing*

Security auditing merupakan proses evaluasi terhadap konfigurasi sistem untuk memastikan kesesuaian dengan standar keamanan yang telah ditetapkan [ISO22a].

2.1.1.4 *Risk Assessment*

Risk Assessment merupakan proses identifikasi dan analisis risiko keamanan yang mempertimbangkan ancaman serta kerentanan pada sistem [NIS12]. Hasil dari proses ini digunakan untuk menentukan prioritas penanganan berdasarkan tingkat dampak dan kemungkinan terjadinya risiko [ISO22a].

2.1.1.5 *Compliance Testing*

Compliance Testing merupakan proses pengujian yang bertujuan untuk memastikan sistem telah memenuhi standar dan regulasi yang berlaku. Pengujian ini mencakup verifikasi konfigurasi sistem, kontrol akses, serta penerapan kebijakan keamanan yang sesuai dengan pendekatan yang berlaku [ISO22a]. Pendekatan ini bertujuan untuk memastikan bahwa sistem telah memenuhi kontrol keamanan yang ditetapkan dan meminimalkan potensi kerentanan akibat kesalahan konfigurasi [NIS12].

Teori ini digunakan sebagai landasan konseptual utama dalam penelitian ini karena secara langsung berkaitan dengan aktivitas yang dilakukan, yaitu melakukan pengujian keamanan terhadap server dan layanan untuk mengidentifikasi kesalahan konfigurasi (*misconfiguration).*

2.1.2 Prinsip CIA Triad

Confidentiality, Integrity, dan *Availability* (CIA) merupakan tiga prinsip dasar yang menjadi fondasi dalam pengelolaan keamanan informasi [HAR23]. *Confidentiality* merujuk pada upaya menjaga agar informasi hanya dapat diakses oleh pihak yang memiliki wewenang, sehingga mencegah terjadinya pengungkapan informasi kepada pihak yang tidak berhak [HAR23]. *Integrity* menjamin bahwa data tetap akurat, lengkap, dan tidak mengalami perubahan yang tidak sah selama proses penyimpanan [HAR23]. *Availability* memastikan bahwa informasi dan layanan dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan, tanpa mengalami gangguan yang tidak semestinya [HAR23]. Ketiga prinsip tersebut saling berkaitan, sehingga apabila salah satu prinsip terganggu, tingkat keamanan sistem secara keseluruhan akan menurun [ISO22a]. Dalam konteks *Security Misconfiguration*, pelanggaran terhadap prinsip CIA dapat terjadi akibat kesalahan pengaturan yang membuka celah bagi pihak tidak berwenang untuk mengakses, mengubah, atau mengganggu ketersediaan layanan [HAR23].

Teori ini digunakan dalam penelitian ini karena prinsip CIA triad menjadi kerangka acuan pada tahap Analisis Dampak untuk menganalisis dampak setiap temuan *Security Misconfiguration* terhadap aspek kerahasiaan, integritas, dan ketersediaan layanan pada domain unpas.dev.

2.2 *Vulnerability Assessment*

Vulnerability Assessment merupakan proses identifikasi dan analisis kerentanan pada sistem secara sistematis tanpa melakukan eksploitasi secara langsung, dengan tujuan untuk mengetahui potensi risiko keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang [SCA08b]. Berbeda dengan *Penetration Testing* yang mencakup upaya aktif untuk membuktikan dampak suatu kerentanan melalui simulasi serangan nyata [PTE14], *Vulnerability Assessment* berfokus pada identifikasi, verifikasi, dan analisis kerentanan tanpa melakukan eksploitasi lebih lanjut terhadap sistem target [OWA25]. Dalam pelaksanaannya, *Vulnerability Assessment* tetap perlu mengikuti pendekatan yang sistematis agar hasil pengujian dapat dipertanggungjawabkan [SCA08b]. *OWASP Web Security Testing* menekankan pentingnya proses pengujian yang terstruktur sehingga evaluasi keamanan dapat menghasilkan temuan yang jelas dan dapat ditindaklanjuti [OWAc]. Teori ini digunakan dalam penelitian ini karena *Vulnerability Assessment* digunakan sebagai metode utama untuk mengidentifikasi dan memverifikasi kerentanan pada server dan layanan melalui observasi dan verifikasi non-destruktif, tanpa melakukan eksploitasi terhadap sistem target.

2.2.1 Pendekatan *Vulnerability Assessment*

Pendekatan *Vulnerability Assessment* dapat diklasifikasikan berdasarkan tingkat informasi yang dimiliki terhadap target pengujian. IBM menjelaskan bahwa ada 3 jenis pendekatan, yaitu:

1. *Black-box testing,* dilakukan tanpa pengetahuan awal mengenai sistem target, sehingga penguji bertindak seperti penyerang eksternal yang hanya mengandalkan informasi yang tersedia dari luar.
2. *White-box testing,* dilakukan ketika penguji memiliki akses penuh terhadap informasi internal sistem, termasuk arsitektur, konfigurasi, dan detail teknis lainnya.
3. *Grey-box testing,* yaitu pengujian dengan sebagian informasi yang diberikan kepada penguji, sehingga pendekatannya berada di antara pengujian eksternal dan internal.

Klasifikasi tersebut penting karena mempengaruhi kedalaman pengujian, strategi identifikasi target, serta bentuk temuan yang diperoleh [IBM26]. Penelitian ini menggunakan pendekatan *black-box testing* karena pendekatan tersebut merepresentasikan sudut pandang penyerang dari luar sistem tanpa pengetahuan awal mengenai konfigurasi dan informasi apapun, sehingga sesuai dengan skenario ancaman yang realistis terhadap domain unpas.dev sebagai layanan yang terhubung langsung dengan jaringan internet publik.

2.3 *Penetration Testing Execution Standard* (PTES)

Penetration Testing Execution Standard (PTES) merupakan kerangka kerja yang digunakan untuk mendukung pelaksanaan *Penetration Testing* secara terstruktur dan sistematis. PTES disusun sebagai panduan yang menjelaskan tahapan pengujian, mulai dari persiapan hingga pelaporan hasil, sehingga proses pengujian tidak dilakukan secara acak dan dapat dipertanggungjawabkan secara metodologis [PTE14]. Dibandingkan dengan metodologi pengujian keamanan lain, seperti OSSTMM yang mencakup ranah keamanan fisik dan manusia di luar kebutuhan penelitian ini [ISE10], serta NIST SP 800-115 yang bersifat umum tanpa alur kerja baku dari perencanaan hingga pelaporan [SCA08b], PTES dipilih karena menyediakan alur kerja yang lebih ringkas, terfokus, dan terstruktur dari *Pre-Engagement* sampai *Reporting,* sehingga sesuai dengan kebutuhan dokumentasi proses penelitian secara sistematis. Dengan adanya kerangka ini, pengujian keamanan dapat dilaksanakan melalui alur yang jelas dan terdokumentasi.

2.3.1 Fase-Fase dalam PTES

PTES membagi proses *penetration testing* ke dalam beberapa fase utama, yaitu *Pre-Engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, dan Reporting* [PTE14]. Setiap fase memiliki fungsi yang berbeda, tetapi saling berkaitan dalam membentuk alur pengujian yang utuh. Dalam penelitian ini, fase-fase tersebut digunakan sebagai acuan untuk mengarahkan proses pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev.

Fase-fase dalam PTES dijelaskan sebagai berikut:

1. ***Pre-engagement Interactions***

   Fase ini merupakan tahap awal yang mencakup penentuan tujuan, ruang lingkup, batasan, dan aturan pelaksanaan pengujian. Dalam penelitian ini, fase tersebut penting untuk memastikan bahwa pengujian hanya dilakukan pada target yang telah ditetapkan, yaitu domain unpas.dev, serta tetap berada dalam batas etis dan teknis yang diizinkan.

2. ***Intelligence Gathering***

   Fase ini dilakukan untuk mengumpulkan informasi mengenai target pengujian, seperti domain, subdomain, port terbuka, layanan aktif, teknologi yang digunakan, dan informasi teknis lain yang dapat diamati dari luar. Dalam konteks penelitian ini, tahap ini sangat penting untuk mengidentifikasi komponen server dan layanan yang berpotensi mengalami *Security Misconfiguration.*

3. ***Threat Modeling***

   Fase ini bertujuan untuk memetakan kemungkinan ancaman berdasarkan informasi yang telah diperoleh pada fase *Intelligence Gathering*. Pemetaan ancaman dilakukan dengan mengidentifikasi potensi risiko yang relevan, mengelompokkannya berdasarkan kategori

kerentanan yang menjadi fokus pengujian, serta menentukan prioritas pengujian berdasarkan estimasi tingkat dampak.

4. ***Vulnerability Analysis***

Fase ini merupakan tahap analisis terhadap kelemahan yang telah teridentifikasi berdasarkan hasil *Threat Modeling* dan *Intelligence Gathering*. Pada fase ini, penulis melakukan pemeriksaan teknis menggunakan *tools* yang telah ditentukan untuk mengidentifikasi indikasi *Security Misconfiguration* pada setiap parameter pengujian.

5. ***Exploitation***

Fase ini dilakukan untuk memverifikasi apakah kelemahan yang ditemukan benar-benar dapat dimanfaatkan dalam skenario pengujian yang sah dan terkontrol. Fase ini tidak dilaksanakan dalam penelitian ini dan verifikasi indikasi kerentanan cukup dilakukan pada tahap *Vulnerability Analysis.*

6. ***Post-Exploitation***

Fase ini umumnya mencakup aktivitas seperti mempertahankan akses dan pengumpulan data sensitif setelah eksploitasi berhasil dilakukan. Fase ini tidak dilaksanakan dalam penelitian ini, karena penelitian ini berhenti pada tahap *Vulnerability Analysis.* Sebagai gantinya, analisis dampak tetap disusun secara terpisah sebagai bagian dari proses penilaian risiko, yaitu menilai potensi konsekuensi dari setiap temuan terhadap tiga aspek utama keamanan informasi (CIA Triad).

7. ***Reporting***

Fase terakhir adalah penyusunan laporan hasil pengujian yang memuat temuan, analisis, tingkat risiko, dan rekomendasi perbaikan.

Berdasarkan fase-fase tersebut, dapat dipahami bahwa PTES menyediakan alur kerja yang jelas dan runtut dalam pelaksanaan *Penetration Testing.*

2.4 OWASP Top 10 Tahun 2025

OWASP Top 10 Tahun 2025 merupakan daftar sepuluh risiko keamanan aplikasi web yang dipublikasikan oleh OWASP Foundation dan digunakan secara luas sebagai acuan dalam mengidentifikasi kategori kerentanan yang paling penting untuk diperhatikan. Daftar ini disusun berdasarkan tren ancaman, temuan pengujian keamanan, serta perkembangan praktik pengamanan aplikasi web modern [OWA25]. Karena dipublikasikan oleh organisasi yang berfokus pada keamanan aplikasi, OWASP Top 10 menjadi salah satu referensi yang paling sering digunakan dalam pengembangan aplikasi, audit keamanan, dan penelitian di bidang keamanan siber.

Dalam penelitian ini, OWASP Top 10 Tahun 2025 digunakan sebagai landasan klasifikasi untuk menentukan fokus pengujian keamanan pada domain *unpas.dev*. Penggunaan versi 2025 dipilih karena merupakan acuan yang terbaru dalam menggambarkan kategori risiko keamanan

aplikasi web saat ini. Hal ini relevan dengan objek penelitian yang berupa layanan akademik berbasis web yang berjalan pada server publik, sehingga berpotensi terpapar berbagai risiko keamanan, khususnya yang berkaitan dengan kesalahan konfigurasi server dan layanan.

Berikut adalah kategori risiko OWASP Top 10 Tahun 2025 yang menjadi kerangka klasifikasi dalam penelitian ini:

Tabel 2. 1 Kategori OWASP Top 10 Tahun 2025

Kode & Tahun	Kategori
A01:2025	*Broken Access Control*
A02:2025	*Security Misconfiguration*
A03:2025	*Software Supply Chain Failures*
A04:2025	*Cryptographic Failures*
A05:2025	*Injection*
A06:2025	*Insecure Design*
A07:2025	*Authentication Failures*
A08:2025	*Software or Data Integrity Failures*
A09:2025	*Security Logging and Alerting Failures*
A10:2025	*Mishandling of Exceptional Conditions*

Daftar kategori ini menggarisbawahi beragam aspek yang dapat berdampak pada keamanan aplikasi web, mulai dari kontrol akses, kegagalan autentikasi, hingga desain sistem dan pengelolaan rantai pasokan perangkat lunak. Dalam penelitian ini, kategori *Security Misconfiguration* (A02:2025) dipilih sebagai fokus utama dikarenakan kerentanannya yang terkait erat dengan konfigurasi server dan layanan yang mendukung domain *unpas.dev,* sesuai dengan riwayat insiden keamanan yang pernah dialami.

2.5 *Security Misconfiguration*

Security Misconfiguration adalah salah satu kategori risiko keamanan yang termasuk dalam daftar OWASP Top 10 Tahun 2025. Kerentanan ini terjadi akibat pengaturan yang tidak tepat, tidak lengkap, atau masih menggunakan konfigurasi default pada server, layanan, aplikasi, *framework*, atau komponen pendukung lainnya yang memungkinkan terjadinya akses tidak sah, kebocoran data, atau gangguan operasional [OWA25]. Kesalahan konfigurasi ini merupakan salah satu kategori risiko utama dalam keamanan aplikasi web terbaru dan menjadi fokus penting dalam pengujian keamanan infrastruktur TI, termasuk pada domain *unpas.dev* yang menyediakan layanan akademik berbasis web.

Security Misconfiguration dapat terjadi pada berbagai lapisan infrastruktur, seperti pengaturan port dan *firewall,* konfigurasi hak akses file, pengelolaan sertifikat SSL/TLS, hingga pengamanan fitur layanan administratif. Faktor penyebab umumnya ditemukan meliputi penggunaan konfigurasi default, tidak dilakukannya *hardening* pada server, terekspos nya informasi sensitif

melalui pesan kesalahan, serta tidak diperbaruinya komponen perangkat lunak pendukung [OWA25]. Oleh karena itu, mitigasi risiko *Security Misconfiguration* harus mencakup pemeriksaan dan perbaikan pengaturan keamanan pada seluruh komponen sistem yang terlibat.

Teori ini digunakan dalam penelitian ini karena menjadi fokus utama dalam pengujian keamanan yang dilakukan, yaitu mengidentifikasi kesalahan konfigurasi pada server dan layanan yang berpotensi menimbulkan risiko keamanan pada sistem.

2.5.1 Jenis-jenis *Security Misconfiguration*

Berbagai bentuk *security misconfiguration* yang umum ditemukan di lingkungan server dan aplikasi web meliputi:

1. **Port dan layanan yang tidak diperlukan terbuka secara publik**

   Kondisi ini terjadi ketika layanan yang seharusnya hanya dapat diakses secara internal tetap terbuka ke jaringan publik tanpa mekanisme pembatasan yang memadai [OWA25]. Contohnya adalah port basis data MySQL (3306) yang seharusnya hanya dapat diakses secara internal, tetapi terbuka ke internet. Kondisi tersebut dapat membuka peluang eksploitasi oleh pihak yang tidak berwenang [SCA08a].

2. **Penggunaan pengaturan bawaan (konfigurasi default)**

   Konfigurasi default merupakan pengaturan bawaan dari perangkat lunak, sistem operasi, web server, *framework*, atau layanan tertentu yang belum disesuaikan dengan kebutuhan keamanan. Penggunaan akun bawaan, kata sandi default, halaman default, file contoh, atau konfigurasi awal yang masih aktif termasuk ke dalam *Security Misconfiguration* karena dapat memberikan peluang akses atau informasi teknis kepada pihak yang tidak berwenang [OWA25]. Dalam pengamanan server, akun bawaan, file contoh, dan komponen yang tidak diperlukan sebaiknya dinonaktifkan atau dihapus agar tidak memperluas risiko keamanan [SCA08a].

3. **Aktifnya *directory listing* pada *web server***

   Directory listing adalah kondisi ketika web server menampilkan daftar file dan direktori kepada pengguna ketika tidak terdapat halaman indeks atau ketika konfigurasi direktori mengizinkan penelusuran. Jika fitur aktif pada direktori yang tidak seharusnya terbuka, pihak luar dapat melihat struktur direktori, nama file, atau dokumen tertentu yang berpotensi berisi informasi sensitif [OWA25]. Informasi tersebut bisa digunakan sebagai dasar untuk serangan lanjutan.

4. **Pesan kesalahan atau *debugging* yang terlalu informatif**

   Kondisi ini terjadi ketika sistem menampilkan informasi internal pada pesan kesalahan, seperti *stack* trace jalur direktori, versi perangkat lunak, struktur aplikasi, konfigurasi server,

atau detail basis data [OWA25]. Informasi tersebut dapat membantu pihak yang tidak berwenang memahami lingkungan sistem dan menentukan teknik serangan yang lebih tepat.

Kondisi ini dikategorikan sebagai CWE-209 (*Generation of Error Message Containing Sensitive Information)*, yang mendefinisikan kelemahan tersebut sebagai kondisi ketika suatu produk perangkat lunak menghasilkan pesan kesalahan yang memuat informasi sensitif mengenai lingkungan, pengguna, atau data yang berkaitan dengannya [MIT26]. Informasi yang terungkap melalui pesan kesalahan tersebut dapat bernilai secara langsung, misalnya berupa kredensial, atau dimanfaatkan sebagai bahan pengintaian (*reconnaissance)* untuk merencanakan serangan lanjutan yang lebih terarah [MIT26].

5. Tidak diterapkannya HTTP *security headers*

HTTP *security headers* merupakan konfigurasi pada respon HTTP yang membantu browser menerapkan kontrol keamanan tambahan. Contohnya adalah *Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer* dan *Strict-Transport-Security* [OWA25]. Jika header tersebut tidak diterapkan, aplikasi web dapat lebih rentan terhadap serangan berbasis peramban seperti *clickjacking, content sniffing,* atau penyalahgunaan pemuatan konten dari sumber yang tidak dipercaya.

Header X-Frame-Options berfungsi mengendalikan apakah suatu halaman web diperbolehkan ditampilkan di dalam elemen <frame> atau <iframe> milik situs lain, sehingga penerapannya dapat mencegah serangan *clickjacking* [OWAb]. Efectivitas *header* ini bergantung pada penerapannya sebagai HTTP response header, karena penerapan melalui tag <meta> tidak akan dikenali oleh peramban [OWAa]. *Header X-Content-Type-Options* dengan nilai *nosniff* memerintahkan peramban untuk mengikuti tipe MIME yang dinyatakan pada *header Content-Type* tanpa melakukan penebakan (*MIME-sniffing)*, sehingga mencegah berkas yang semula tidak dapat dieksekusi berubah menjadi dapat dieksekusi akibat kesalahan interpretasi tipe konten [OWAb]. *Header Permission-Policy* digunakan untuk mengatur fitur peramban tertentu, seperti kamera, mikrofon, dan lokasi, yang boleh diakses oleh suatu halaman maupun elemen pihak ketiga yang dimuat di dalamnya [OWAb].

6. Konfigurasi SSL/TLS kurang aman

SSL/TLS digunakan untuk mengamankan komunikasi antara pengguna dan server, khususnya pada koneksi HTTPS. Konfigurasi SSL/TLS yang kurang aman dapat berupa penggunaan protokol TLS versi lama, penggunaan *cipher suite* yang lemah, sertifikat digital yang kedaluwarsa, sertifikat yang tidak sesuai dengan domain, atau konfigurasi rantai sertifikat yang tidak valid [MCK19]. Kondisi tersebut dapat menurunkan perlindungan terhadap kerahasiaan dan integritas data yang dikirimkan antara pengguna dan server.

Ketentuan mengenai usangnya TLS versi lama dituangkan secara resmi dalam RFC 8996 yang diterbitkan oleh *Internet Engineering Task Force* (IETF), yang menyatakan TLS 1.0 dan TLS 1.1 sebagai *deprecated* (usang), sehingga dokumen spesifikasi asli keduanya yaitu RFC 2246 dan RFC 4346, dipindahkan ke status *historic* [IET21]. Alasan teknis yang mendasari keputusan tersebut antara lain ketergantungan proses jabat tangan (*handhsake)* dan otentikasi pada fungsi hash SHA-1 yang telah dinyatakan rentan, serta tidak didukungnya *cipher suite Authenticated Encryptions with Associated Data* (AEAD) yang baru tersedia mulai TLS 1.2 [IET21].

7. Informasi versi layanan yang terekspos

Kondisi ini terjadi ketika server atau aplikasi menampilkan informasi web server, *framework*, sistem, database atau layanan tertentu melalui *banner, response header,* halaman default, maupun pesan kesalahan. Informasi versi layanan yang terekspos termasuk ke dalam *Security Misconfiguration* karena dapat membantu pihak yang tidak berwenang mengidentifikasi teknologi yang digunakan dan mencari kerentanan yang sesuai dengan versi perangkat lunak tersebut [OWA25]. Dalam pengamanan server, informasi yang tidak diperlukan sebaiknya dibatasi agar tidak memberikan petunjuk tambahan kepada pihak luar [SCA08a].

Berbagai bentuk *Security Misconfiguration* tersebut menunjukkan bahwa kesalahan konfigurasi dapat terjadi pada banyak lapisan sistem, mulai dari jaringan, web server, layanan basis data, mekanisme enkripsi, hingga akses administratif. Oleh karena itu, diperlukan parameter pengujian yang jelas agar proses identifikasi *Security Misconfiguration* dapat dilakukan secara terarah dan sesuai dengan ruang lingkup penelitian.

2.6 Konfigurasi Server dan Layanan

Konfigurasi server dan layanan merupakan aspek penting dalam keamanan sistem karena server berperan sebagai komponen utama yang menyediakan layanan, jaringan, mengelola proses, serta menangani akses terhadap sumber daya yang dibutuhkan pengguna. Dalam lingkungan yang terhubung ke jaringan publik, konfigurasi server tidak hanya memengaruhi kinerja layanan, tetapi juga menentukan tingkat paparan sistem terhadap ancaman keamanan. Keamanan server sangat dipengaruhi oleh cara sistem dikonfigurasi, dikelola, dan dipelihara selama masa operasionalnya, termasuk dalam pengelolaan layanan, akses, dan komponen pendukung yang berjalan pada server [SCA08a].

Konfigurasi dan layanan yang tidak tepat dapat membuka peluang terjadinya akses tidak sah, paparan informasi sensitif, maupun eksploitasi terhadap komponen yang seharusnya dibatasi. Dalam konteks keamanan sistem, pengelolaan konfigurasi yang baik bertujuan memastikan bahwa hanya layanan yang diperlukan yang dijalankan, akses ke sistem dibatasi sesuai kebutuhan, dan perubahan konfigurasi tetap berada dalam kendali. NIST menegaskan bahwa *configuration management*

merupakan bagian penting dari kontrol keamanan karena perubahan konfigurasi yang tidak terkontrol dapat meningkatkan risiko terhadap sistem informasi [JOI20].

Teori ini digunakan dalam penelitian ini karena berkaitan langsung dengan objek yang akan diuji, yaitu server dan layanan, sehingga menjadi dasar dalam mengidentifikasi potensi kesalahan konfigurasi yang dapat menimbulkan risiko keamanan pada sistem.

2.6.1 *Server Hardening*

Server Hardening merupakan upaya pengamanan server yang dilakukan dengan memperkuat konfigurasi, membatasi fungsi server sesuai kebutuhan operasional, menonaktifkan atau menghapus layanan yang tidak diperlukan, serta menghindari penggunaan pengaturan bawaan yang berisiko [SCA08b]. Upaya ini bertujuan untuk memperkecil *attack surface* sehingga server tidak memiliki lebih banyak titik akses daripada yang benar-benar dibutuhkan.

Secara umum, penerapan *server hardening* mencakup pembaruan sistem dan perangkat lunak secara berkala, penonaktifan akun maupun layanan bawaan yang tidak digunakan, pembatasan hak akses administratif, pengamanan layanan manajemen jarak jauh, serta penyesuaian konfigurasi keamanan pada layanan yang berjalan [SCA08a]. Selain itu, pengaturan terhadap file, direktori, dan mekanisme autentikasi juga perlu dilakukan secara tepat agar akses terhadap sumber daya tertentu hanya diberikan kepada pihak yang berwenang. Pendekatan ini sejalan dengan prinsip *configuration management* yang menekankan pentingnya pengelolaan konfigurasi sistem secara hati-hati agar tetap berada dalam kondisi aman [JOI20].

2.6.2 Pengamanan Port dan Layanan

Pengamanan port dan layanan merupakan bagian penting dalam keamanan server karena setiap port yang terbuka dan layanan yang aktif dapat menjadi titik masuk potensial bagi pihak luar. Port berfungsi sebagai jalur komunikasi antar sistem dan jaringan, sedangkan layanan dijalankan untuk menyediakan fungsi tertentu, seperti akses web, administrasi jarak jauh, pertukaran file, atau koneksi basis data. Pembatasan lalu lintas jaringan dan pengendalian akses terhadap layanan menjadi langkah yang penting untuk menurunkan risiko serangan pada sistem yang terhubung ke jaringan [SCA09].

Salah satu prinsip utama dalam pengamanan port dan layanan adalah hanya membuka port yang benar-benar diperlukan untuk operasional sistem. Layanan yang tidak dibutuhkan sebaiknya dinonaktifkan, sedangkan layanan sensitif perlu diamankan melalui pembatasan akses, *filtering,* atau pembatasan berdasarkan sumber koneksi [SCA09]. Apabila layanan atau port sensitif terbuka ke publik tanpa perlindungan yang memadai, kondisi tersebut dapat termasuk ke dalam *Security Misconfiguration* yang meningkatkan peluang terjadinya pemindaian, *enumerasi*, percobaan autentikasi, maupun serangan lanjutan oleh pihak yang tidak berwenang [OWA25].

2.6.3 Arsitektur CDN dan Reverse Proxy

Content Delivery Network (CDN) merupakan jaringan server yang tersebar secara geografis dan berfungsi untuk mendistribusikan konten melalui titik akses (*edge server)* terdekat dengan pengguna, sehingga kecepatan akses dan mengurangi bebas server asal (*origin server)* [CLOa]. Selain sebagai penyedia konten, layanan CDN modern seperti *Cloudflare* umumnya juga berperan sebagai *reverse proxy*, yaitu perantara yang menerima seluruh permintaan dari pengguna kemudian meneruskannya ke server asal, sehingga alamat IP asli server tidak terekspos langsung kepada publik [CLOb]. Dengan mekanisme tersebut, permintaan yang diterima penguji keamanan dari sisi publik pada dasarnya telah di filter oleh lapisan CDN, bukan permintaan yang langsung mencapai server asal [CLOb]. Kondisi ini mempengaruhi hasil pengujian keamanan dari sisi eksternal, karena sejumlah informasi teknis seperti versi web server maupun sistem operasi asli dapat disembunyikan otomatis oleh lapisan CDN, sehingga tidak seluruh port maupun layanan pada server asal dapat teramati langsung melalui *black-box testing* [CLOa].

Teori ini digunakan dalam penelitian ini karena landasan teori ini diperlukan untuk menjelaskan mengapa sejumlah informasi teknis tidak dapat teramati langsung.

2.7 *Risk Assessment*

Risk assessment merupakan proses untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko terhadap sistem informasi dan organisasi [NIS12]. NIST menjelaskan bahwa *Risk Assessment* digunakan untuk memberikan informasi yang dibutuhkan dalam menentukan tindakan yang tepat terhadap risiko yang telah diidentifikasi [NIS12]. Proses ini menjadi bagian penting dalam keamanan informasi karena membantu memahami ancaman, kerentanan, kemungkinan terjadinya risiko, serta dampak yang dapat ditimbulkan terhadap sistem.

Dalam konteks pengujian keamanan, *Risk Assessment* digunakan untuk menilai tingkat risiko dari temuan berdasarkan potensi dampaknya terhadap sistem [NIS12]. Penilaian risiko diperlukan agar temuan keamanan tidak hanya dicatat sebagai kelemahan teknis, tetapi juga dapat diprioritaskan berdasarkan tingkat keparahan dan dampaknya terhadap aspek kerahasiaan, integritas, dan ketersediaan sistem [NIS12].

Dalam penelitian ini, *Risk Assessment* digunakan untuk menilai tingkat risiko dari temuan *Security Misconfiguration* yang diperoleh selama proses pengujian konfigurasi server dan layanan pada domain unpas. Hasil penilaian risiko tersebut digunakan sebagai dasar dalam menentukan prioritas rekomendasi perbaikan dan penguatan konfigurasi server serta layanan. Dengan demikian, temuan yang memiliki tingkat risiko yang lebih tinggi dapat diprioritaskan untuk segera ditangani oleh pengelola sistem.

2.8 *Common Vulnerability Scoring System* (CVSS)

Common Vulnerability Scoring System (CVSS) merupakan standar industri yang digunakan secara luas untuk menilai tingkat keparahan kerentanan keamanan pada sistem informasi secara objektif dan terukur [FIR23]. CVSS dikembangkan dan dikelola oleh *Forum of Incident Response and Security Teams* (FIRST) sebagai kerangka penilaian yang memungkinkan organisasi untuk memahami karakteristik dan dampak dari suatu kerentanan secara terstandarisasi [FIR23]. FIRST merilis versi 4.0 sebagai versi terbaru yang menyempurnakan versi sebelumnya dengan memberikan penilaian yang lebih tinggi, metrik yang lebih lengkap, serta kemampuan yang lebih baik dalam merepresentasikan dampak kerentanan pada sistem [FIR23].

CVSS v4.0 menghasilkan nilai numerik dalam rentang 0.0 hingga 10.0 yang merepresentasikan tingkat keparahan suatu kerentanan [FIR23]. Skor tersebut dihitung berdasarkan serangkaian metrik yang mencerminkan karakteristik teknis kerentanan serta dampaknya terhadap sistem yang terdampak [FIR23].

Teori ini digunakan dalam penelitian ini karena CVSS v4.0 menyediakan kerangka penilaian risiko yang objektif, terstandarisasi dan merupakan versi terbaru yang selaras dengan keamanan terkini, sehingga setiap kerentanan yang ditemukan selama proses pengujian keamanan pada domain unpas.dev dapat dinilai tingkat keparahannya secara jelas.

2.8.1 Komponen Penilaian CVSS v4.0

CVSS versi 4.0 memperkenalkan struktur metrik yang lebih komprehensif dibandingkan versi sebelumnya dengan membagi penilaian ke dalam empat kelompok metrik utama [FIR23]. Setiap kelompok metrik memiliki peran yang berbeda dalam menghasilkan skor akhir yang merepresentasikan tingkat keparahan suatu kerentanan. Keempat kelompok metrik tersebut adalah sebagai berikut:

1. **Base Metrics**

   Base Metrics merupakan kelompok metrik yang menggambarkan karakteristik dasar suatu kerentanan yang bersifat tetap dan tidak bergantung pada lingkungan maupun waktu [FIR23]. Kelompok ini metrik ini menghasilkan *Base Score* yang menjadi dasar utama dalam penilaian CVSS v4.0. *Base Metrics* terdiri dari dua sub kelompok, yaitu:

   a. ***Exploitability Metrics***

      Exploitability Metrics mengukur kemudahan eksploitasi suatu kerentanan dari sudut pandang penyerang [FIR23]. Sub kelompok ini mencakup lima komponen, yaitu *Attack Vector* (AV) yang menggambarkan konteks dimana eksploitasi dapat dilakukan, *Attack Complexity* (AC) yang menggambarkan kondisi teknis yang diperlukan untuk melakukan eksploitasi, *Attack Requirements* (AT) yang merupakan metrik baru dalam CVSS v4.0 untuk menggambarkan prasyarat serangan, *Privileges Required* (PR) yang

menggambarkan tingkat hak akses yang dibutuhkan oleh penyerang, serta *User Interaction* (UI) yang digambarkan apakah eksploitasi memerlukan interaksi dari pengguna lain [FIR23].

b. *Impact Metrics*

Impact Metrics mengukur dampak yang ditimbulkan apabila kerentanan berhasil dieksploitasi [FIR23]. Dalam CVSS v4.0, *Impact Metrics* dibagi menjadi dua bagian, yaitu dampak pada *Vulnerable System* yang mencakup *Confidentiality* (VC), *Integrity* (VI), *Availability* (VA), serta dampak pada *Subsequent System* yang mencakup *Confidentiality* (SC), *Integrity* (SI), dan *Availability* (SA) sebagai bentuk penyempurnaan dari versi sebelumnya [FIR23].

2. Threat Metrics

Threat Metrics merupakan kelompok metrik baru yang diperkenalkan dalam CVSS v4.0 sebagai pengganti dari *Temporal Metrics* pada versi sebelumnya [FIR23]. Kelompok metrik ini berfokus pada informasi ancaman yang relevan dengan kerentanan yang dinilai, khususnya terkait dengan ketersediaan dan kematangan eksploit yang dapat digunakan oleh penyerang di dunia maya [FIR23].

3. Environmental Metrics

Environmental Metrics merupakan kelompok metrik yang mempertimbangkan karakteristik lingkungan spesifik dari organisasi yang terdampak oleh suatu kerentanan [FIR23]. Kelompok metrik ini bersifat opsional dan memungkinkan pengelola sistem untuk menyesuaikan skor CVSS berdasarkan konteks operasional sistem yang di uji [FIR23].

4. Supplemental Metrics

Supplemental Metrics merupakan kelompok metrik tambahan yang sepenuhnya baru dalam CVSS v4.0 dan tidak terdapat pada versi sebelumnya [FIR23]. Kelompok metrik ini tidak mempengaruhi skor akhir CVSS, melainkan berfungsi untuk memberikan konteks tambahan mengenai karakteristik kerentanan yang tidak mencakup dalam metrik utama. *Supplemental Matrics* mencakup aspek *Safeti, Automatable, Recovery, Value Density, Vulnerability Response Effort,* dan *Provider Urgency* yang dapat digunakan untuk memperkaya informasi dalam laporan kerentanan.

2.8.2 Skala Penilaian CVSS v4.0

Berdasarkan skor yang dihasilkan dari perhitungan metrik-metrik di atas, CVSS v4.0 mengklasifikasikan tingkat keparahan kerentanan ke dalam lima kategori sebagai berikut:

Tabel 2. 2 Skala Penilaian CVSS v4.0

Skor CVSS	Tingkat Keparahan
0.0	*None*
0.1 – 3.9	*Low*
4.0 – 6.9	*Medium*
7.0 – 8.9	*High*
9.0 – 10.0	*Critical*

Sumber: FIRST.org (2023)

Klasifikasi tingkat keparahan tersebut memberikan gambaran yang jelas mengenai urgensi penanganan setiap kerentanan yang ditemukan [FIR23]. Kerentanan dengan tingkat keparahan *Critical* dan *High* memerlukan penanganan segera karena berpotensi menimbulkan dampak yang signifikan terhadap keamanan sistem, termasuk terhadap aspek kerahasiaan, integritas, dan ketersediaan data [FIR23]. Sedangkan kerentanan dengan tingkat keparahan *Medium* dan *Low* dapat dijadikan sebagai rekomendasi perbaikan dalam jangka menengah dengan tetap mempertimbangkan konteks lingkungan sistem yang bersangkutan [NAT24].

Dalam penelitian ini, skala penilaian CVSS v4.0 digunakan sebagai acuan untuk menentukan prioritas penanganan kerentanan yang ditemukan selama proses pengujian keamanan pada domain unpas.dev. Setiap kerentanan yang berhasil diidentifikasi akan dinilai menggunakan CVSS versi 4.0 sehingga pengelola sistem dapat memahami tingkat risiko dari masing-masing temuan secara terukur dan dapat segera mengambil langkah mitigasi yang sesuai berdasarkan tingkat keparahan yang telah ditetapkan.

2.9 Penelitian Terdahulu

Sejumlah penelitian terdahulu telah membahas pengujian keamanan sistem dengan menggunakan metode *Penetration Testing* dan kerangka kerja PTES pada website, sistem informasi akademik, maupun perangkat jaringan. Hasil penelitian-penelitian tersebut menunjukkan bahwa PTES dapat diterapkan secara sistematis untuk mengidentifikasi berbagai kerentanan, termasuk kelemahan yang berkaitan dengan *Security Misconfiguration*. Meskipun demikian, penelitian yang secara khusus memfokuskan pengujian pada konfigurasi server dan layanan pada domain akademik yang terhubung ke jaringan publik masih relatif terbatas. Oleh karena itu, penelitian ini diarahkan untuk mengkaji aspek tersebut pada domain unpas.dev. Berikut beberapa penelitian terdahulu, antara lain:

Tabel 2. 3 Peneliti Terdahulu

No	Peneliti dan Tahun	Judul Penelitian	Hasil Penelitian	Metode Penelitian	Alasan Digunakan
1	[YUW26]	Analisis Keamanan Website Universitas Pasundan Menggunakan Metode *Penetration Testing* Berbasis Kerangka Kerja PTES	Menemukan kerentanan *Local File Inclusion, Insecure Direct Object References* (IDOR) dan *Broken access Control* pada website institusi	*Penetration Testing* berbasis PTES	Relevan karena menerapkan metode PTES dalam lingkungan universitas yang sama dan menunjukkan adanya kelemahan pada sistem berbasis web yang mendukung penelitian ini.
2	(Syarifudin, Widyawati, & Asroni, 2025)	*Web Security Vulnerability Analysis and Mitigation Based on OWASP Top 10*	Menemukan kerentanan seperti *Security Misconfiguration, vulnerable components,* dan *authentication failure berdasarkan OWASP Top 10*	*Penetration Testing* berbasis OWASP Top 10	Digunakan karena mengacu pada OWASP Top 10 sebagai standar klasifikasi kerentanan yang juga digunakan dalam penelitian ini.
3	[LIS24]	*Security Testing with Penetration Testing Execution Standards (PTES) Methods to Find Misconfiguration Vulnerabilities in Network Devices*	Menemukan kerentanan *Misconfiguration* pada perangkat jaringan, termasuk layanan SSH dan FTP.	*Penetration Testing* berbasis PTES	Mendukung penerapan PTES dalam mengidentifikasi *Misconfiguration* pada infrastruktur jaringan dan server.
4	[SAF23]	*Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website*	Menemukan 42 kerentanan dengan berbagai tingkat risiko (*high, medium, low*) pada website pemerintah menggunakan PTES	*Penetration Testing* berbasis PTES	Dipilih sebagai referensi metodologi karena memaparkan implementasi tahapan PTES secara sistematis serta hasil pengujian yang terukur.
5	[UTA24]	*Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method*	Menemukan kerentanan seperti *SQL Injection, broken access control*, dan *weak encryption* pada sistem informasi akademik	*Penetration Testing* dengan kombinasi PTES dan OWASP Top 10	Relevan karena berfokus pada sistem akademik sebagai objek kajian dengan menggunakan kombinasi metodologi PTES dan OWASP

Berdasarkan kajian terhadap penelitian-penelitian sebelumnya, metode *Penetration Testing* berbasis PTES telah banyak diterapkan untuk mendeteksi kerentanan pada website, sistem informasi akademik, maupun infrastruktur jaringan. Di samping itu, OWASP Top 10 sering digunakan menjadi acuan dalam mengklasifikasikan jenis kerentanan yang berhasil ditemukan.

Namun, sebagian besar penelitian tersebut masih terpusat pada pengujian kerentanan aplikasi web secara umum, seperti *SQL Injection, Broken Access Control, dan* kegagalan autentikasi.

Penelitian yang secara khusus berfokus pada kerentanan *Security Misconfiguration* pada konfigurasi server dan layanan, khususnya pada domain akademik yang terhubung ke jaringan publik, masih relatif terbatas.

Oleh karena itu, penelitian ini dilakukan untuk mengisi celah tersebut dengan melakukan pengujian keamanan yang berfokus pada *Security Misconfiguration* pada konfigurasi server dan layanan menggunakan metode *Vulnerability Assessment* berbasis PTES.

BAB 3
SKEMA PENELITIAN

3.1 Pendahuluan Skema Penelitian

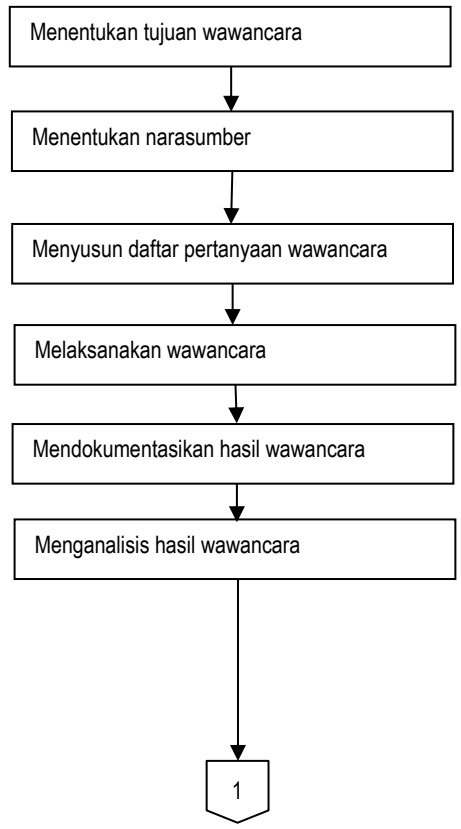
Skema penelitian ini dirancang untuk memastikan proses pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev dapat dilaksanakan secara terukur, terarah, dan dapat dipertanggungjawabkan secara metodologis. Penelitian ini menggunakan metode *Vulnerability Assessment* berbasis *Penetration Testing Execution Standard (PTES)* dengan mengacu pada kategori *Security Misconfiguration* (A02:2025) dalam standar OWASP Top 10 Tahun 2025.

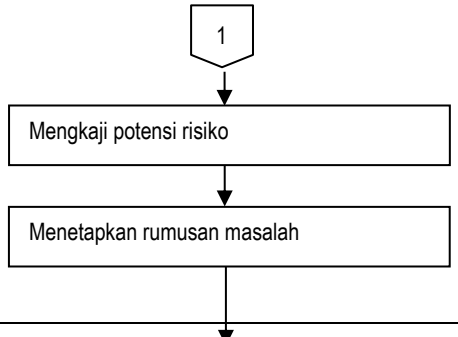
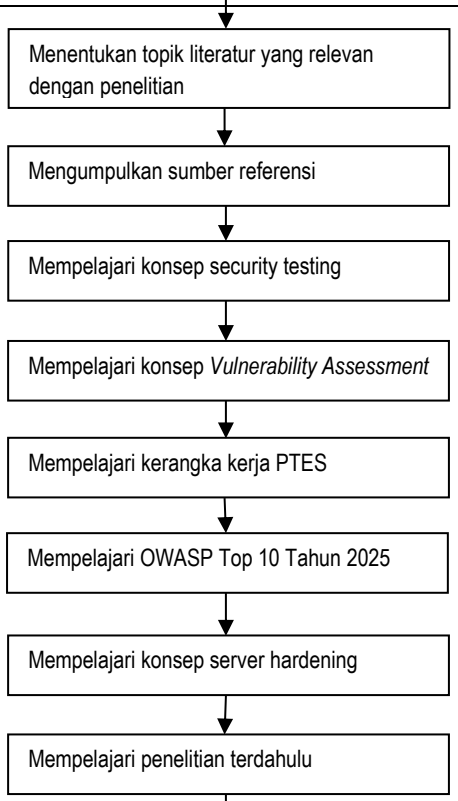
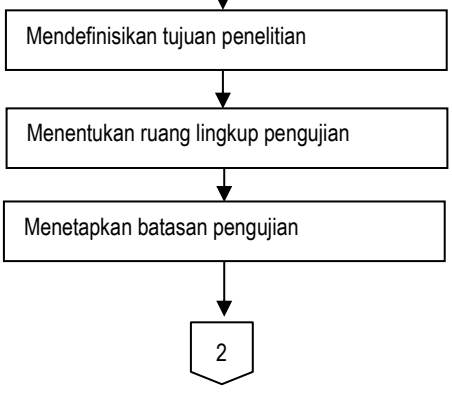
Secara keseluruhan, alur penelitian ini terbagi menjadi tiga tahap utama, yaitu Tahap Awal, Tahap Pengujian, dan Tahap Akhir. Setiap tahap memiliki aktivitasnya yang saling berkaitan dan mendukung satu sama lain dalam membentuk alur penelitian yang utuh.

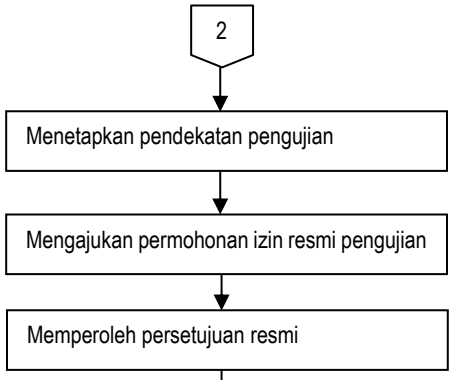
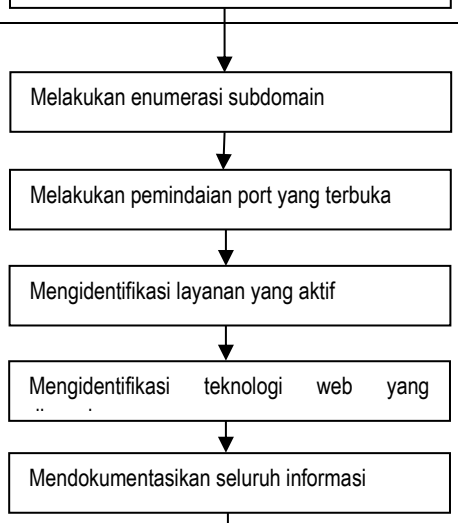
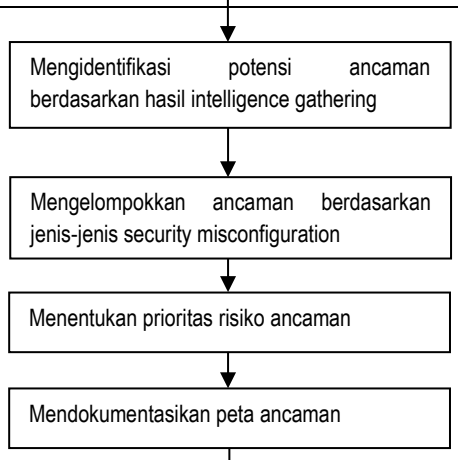
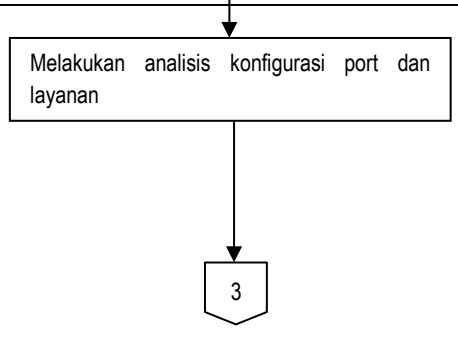
3.2 Alur Penelitian

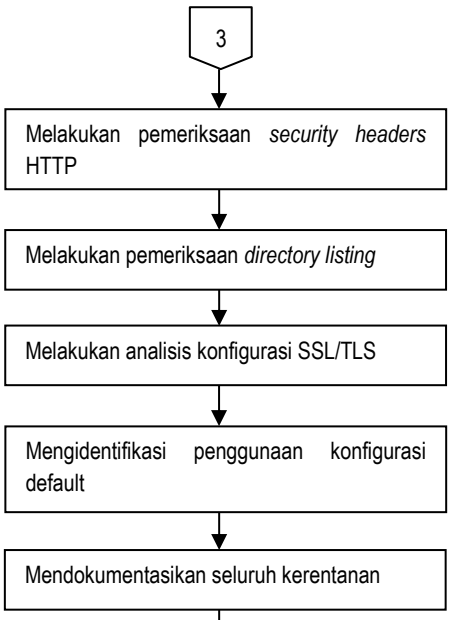
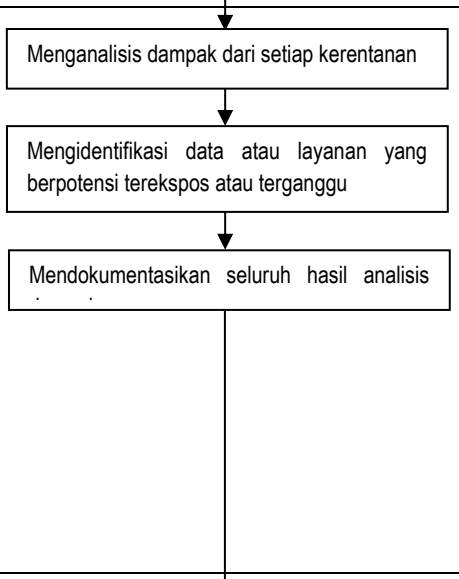
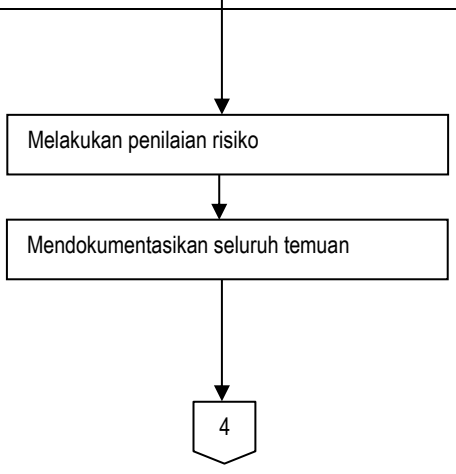
Berikut adalah alur penelitian yang dilakukan:

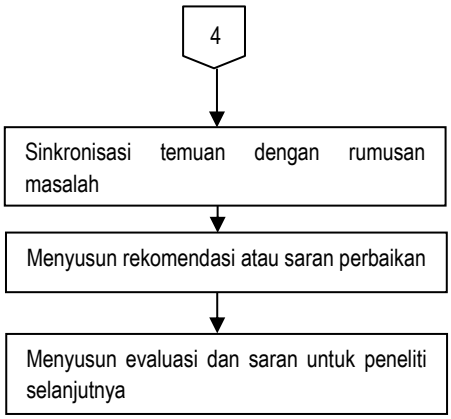
Tabel 3. 1 Alur Penelitian

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
Tahap 1: Identifikasi masalah **Deskripsi:** Mencari permasalahan keamanan konfigurasi server dan layanan pada domain unpas.dev. **Hasil:** Mengetahui informasi tentang masalah keamanan konfigurasi. **Kontribusi:** Sebagai acuan awal pengerjaan tugas akhir		- Teknik Wawancara [SUG13]

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
		
Tahap 2: Studi Literatur **Deskripsi:** mempelajari teori dan konsep yang berkaitan dengan pengujian keamanan sistem sebagai dasar penelitian. **Hasil:** Diperoleh landasan teori yang mendukung pengujian ini. **Kontribusi:** Sebagai landasan teoritis dalam pelaksanaan penelitian.		- *Security Testing* [SCA08b] - *Vulnerability Assessment* - *Penetration Testing Execution Standard* [PTE14] - OWASP Top 10 Tahun 2025 [OWA25]. - *Server Hardening* [SCA08a]
Tahap 3: *Pre-engagement Interaction* **Deskripsi:** Menentukan ruang lingkup dan aturan pengujian. **Hasil**: Diperoleh izin resmi, ruang lingkup dan batasan pengujian. **Kontribusi:** Sebagai dasar legalitas dan batasan dalam proses pengujian.		- *Pre-engagement Interaction* [PTE14]

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
		
Tahap 4: *Intelligence Gathering* **Deskripsi:** Mengumpulkan informasi target. **Hasil:** Memperoleh informasi sistem mengenai fitur, subdomain, layanan, dan teknologi yang digunakan. **Kontribusi:** sebagai dasar dalam proses *threat modeling.*		- *Intelligence Gathering* [PTE14]
Tahap 5: *Threat Modeling* **Deskripsi:** Menganalisis potensi ancaman berdasarkan informasi yang telah dikumpulkan pada tahap sebelumnya. **Hasil:** Peta ancaman dan prioritas risiko. **Kontribusi:** Sebagai acuan dalam proses analisis kerentanan.		- *Threat Modeling* [PTE14]
Tahap 6: *Vulnerability Analysis* **Deskripsi:** Mengidentifikasi dan menganalisis kerentanan keamanan pada sistem berdasarkan informasi pada tahap sebelumnya **Hasil:** Diperoleh daftar kerentanan yang termasuk		- *Vulnerability Analysis* [PTE14] - *Security Misconfiguration* [OWA25]

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
dalam kategori *Security Misconfiguration.* **Kontribusi:** sebagai dasar dalam proses verifikasi manual dan analisis dampak		
Tahap 7: Analisis Dampak **Deskripsi:** Menganalisis dampak dari kerentanan terhadap keamanan sistem. **Hasil:** Diperoleh informasi mengenai dampak kerentanan terhadap keamanan sistem. **Kontribusi:** Sebagai dasar dalam penilaian risiko dan penyusunan rekomendasi.		- Analisis dampak [NIS12]
Tahap 8: *Reporting* **Deskripsi:** Menyusun laporan hasil pengujian keamanan berdasarkan seluruh temuan yang diperoleh. **Hasil:** Laporan pengujian yang berisi kerentanan, bukti, dampak, dan rekomendasi perbaikan **Kontribusi:** Sebagai dasar dalam penarikan kesimpulan dan rekomendasi perbaikan		- *Reporting* [PTE14]

Tahap dan Hasil	Langkah Penelitian	Literatur dan Referensi
Tahap 9: Kesimpulan akhir **Deskripsi:** Menyimpulkan hasil penelitian berdasarkan seluruh proses pengujian yang telah dilakukan **Hasil:** Kesimpulan serta saran perbaikan keamanan sistem. **Kontribusi:** Menjawab rumusan masalah penelitian		- Teknik penarikan kesimpulan dan saran [SUG13]

3.3 Perumusan Masalah

Perumusan masalah pada penelitian tugas akhir ini dilakukan untuk mengidentifikasi dan memahami permasalahan yang terjadi terkait keamanan konfigurasi server dan layanan pada domain unpas.dev milik Fakultas Teknik Universitas Pasundan. Secara umum perumusan masalah dalam penelitian ini dibagi ke dalam dua bagian, yaitu:

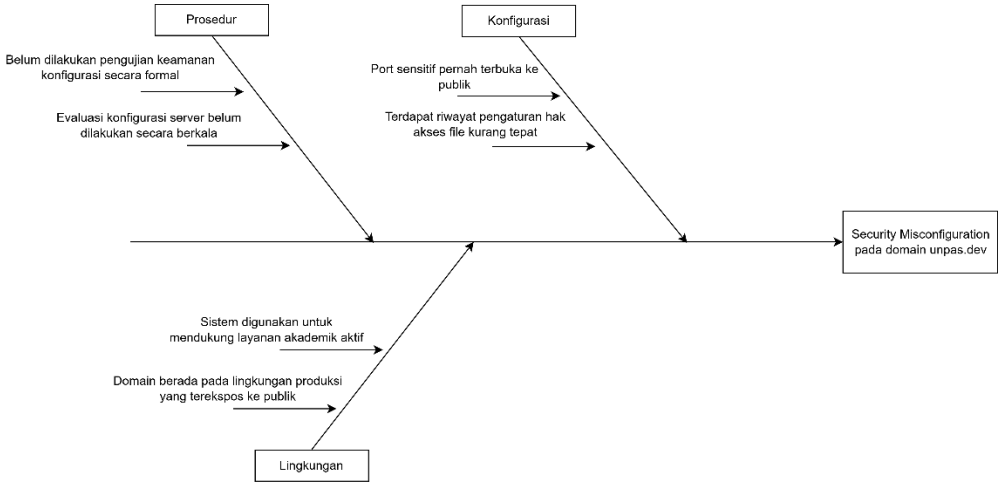
1. Identifikasi penyebab masalah yang digambarkan menggunakan diagram *Fishbone* (*Ishikawa*) untuk memetakan akar permasalahan keamanan konfigurasi server dan layanan pada domain unpas.dev.
2. Solusi masalah yang dimungkinkan berdasarkan penyebab-penyebab yang telah berhasil dipetakan pada bagian pertama sebagai dasar pemberian rekomendasi perbaikan konfigurasi server domain unpas.dev.

Pada subbab perumusan masalah ini akan dibahas mengenai identifikasi sebab-akibat menggunakan *Fishbone Diagram* sebagai upaya untuk memahami akar permasalahan keamanan konfigurasi server dan layanan yang terjadi pada domain unpas.dev secara mendalam.

3.3.1 Analisis Sebab Akibat

Analisis sebab akibat dilakukan untuk mengidentifikasi faktor-faktor yang menjadi penyebab terjadinya *Security Misconfiguration* pada domain unpas.dev. Analisis ini dipetakan menggunakan Diagram *Fishbone* dengan tujuan untuk mengetahui akar permasalahan berdasarkan beberapa aspek yang berpengaruh terhadap kondisi keamanan sistem.

Berdasarkan diagram *fishbone* yang telah disusun, faktor penyebab dikelompokkan ke dalam tiga kategori utama, yaitu prosedur, konfigurasi, dan lingkungan, sebagaimana ditunjukkan pada Gambar 3.1.



Gambar 3. 1 Diagram Analisis Sebab Akibat

Berdasarkan Diagram *Fishbone* pada Gambar 3.1, berikut penjelasan dari setiap kategori:

1. **Prosedur**

   Pada aspek prosedur, diketahui bahwa proses pengujian seperti *Vulnerability Assessment/Penetration Testing* (VA/PT) belum dilakukan. Selain itu, belum terdapat evaluasi rutin terhadap konfigurasi server. Kondisi ini menyebabkan potensi celah keamanan dan kesalahan konfigurasi tidak dapat teridentifikasi secara terukur.

2. **Konfigurasi**

   Pada aspek konfigurasi, terdapat beberapa kondisi yang dapat memicu terjadinya kesalahan konfigurasi keamanan, yaitu adanya layanan sensitif yang pernah terbuka ke publik serta pengaturan hak akses file kurang tepat. Layanan sensitif yang pernah terekspos ke publik dapat memperbesar peluang terjadinya akses tidak sah, terutama apabila layanan tersebut tidak dilindungi dengan mekanisme pembatasan akses yang memadai.

3. **Lingkungan**

   Pada aspek lingkungan, domain unpas.dev berada pada lingkungan produksi yang terekspos ke publik dan digunakan untuk mendukung layanan aktif. Kondisi ini membuat sistem memiliki tingkat risiko yang lebih tinggi karena dapat diakses melalui internet dan berhubungan langsung dengan layanan yang digunakan oleh pengguna.

3.3.2 Solusi Masalah

Berdasarkan hasil analisis menggunakan diagram *fishbone*, permasalahan utama yang diidentifikasi adalah *Security Misconfiguration* pada domain unpas.dev yang dipengaruhi oleh tiga faktor utama, yaitu prosedur, konfigurasi, dan lingkungan. Solusi yang diusulkan dalam penelitian ini adalah melakukan pengujian keamanan terhadap konfigurasi dan layanan untuk mengidentifikasi potensi *Security Misconfiguration.* Pengujian ini dilakukan secara sistematis menggunakan metodologi *Penetration Testing Execution Standard* (PTES) dengan *black-box testing*. Pendekatan

ini dipilih karena pengujian dilakukan dari sudut pandang eksternal tanpa akses langsung terhadap konfigurasi internal sistem, sehingga dapat menggambarkan kondisi sistem sebagaimana terlihat dari sisi publik.

Adapun solusi yang diusulkan berdasarkan masing-masing faktor penyebab ditunjukkan pada Tabel 3.2.

Tabel 3. 2 Solusi Masalah

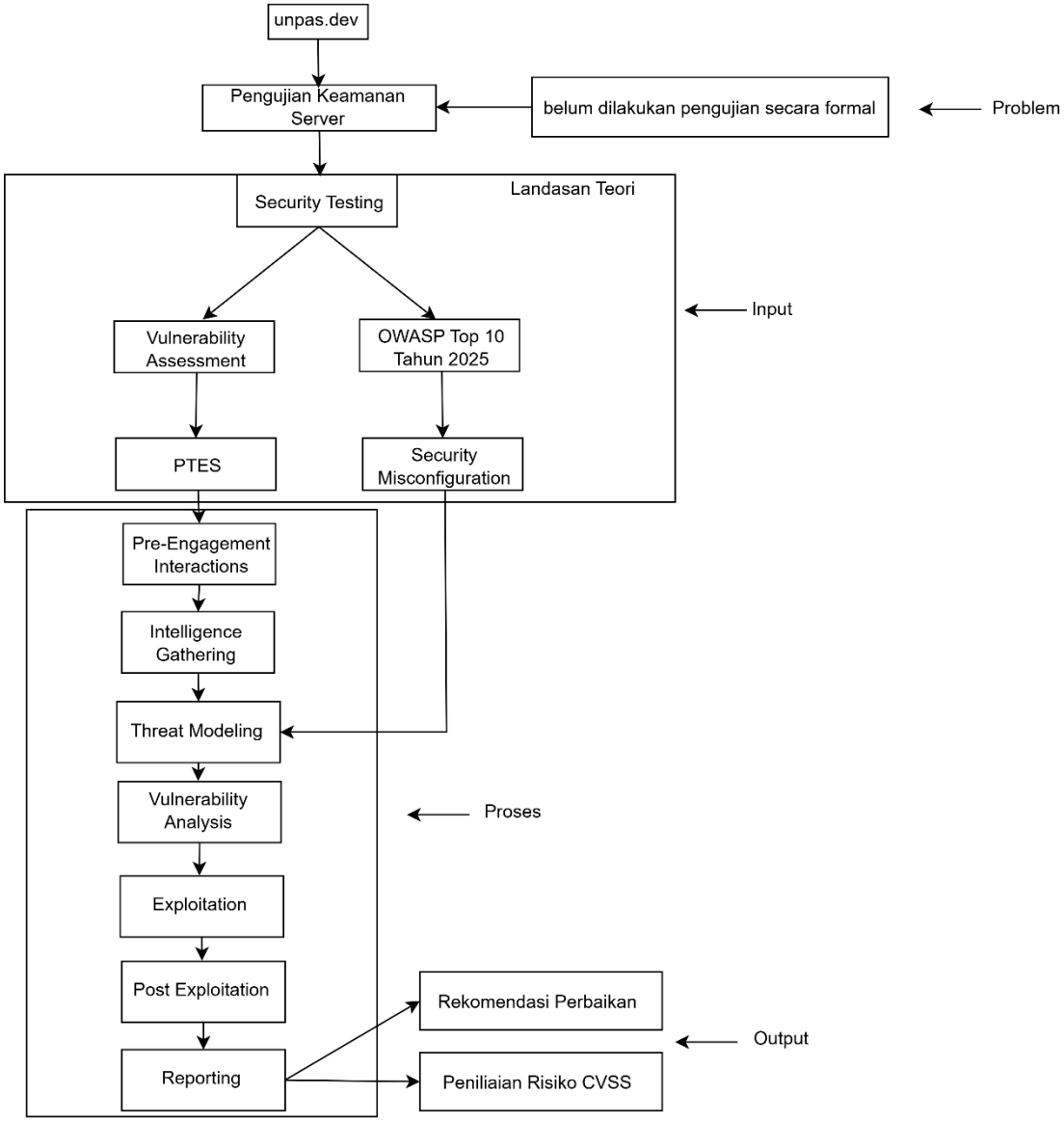
Masalah Utama	Penyebab	Solusi
Security Misconfiguration pada domain unpas.dev	Prosedur: 1. Belum dilakukan pengujian keamanan konfigurasi secara formal. 2. Evaluasi konfigurasi server belum dilakukan	Melakukan pengujian keamanan secara sistematis menggunakan metodologi PTES untuk mengidentifikasi potensi kesalahan konfigurasi pada server dan layanan.
	Konfigurasi: 1. Port sensitif pernah terbuka ke publik. 2. Terdapat riwayat pengaturan hak akses file kurang tepat.	Melakukan pemeriksaan terhadap konfigurasi layanan, port yang terbuka, serta hak akses file dan direktori. Pengujian ini bertujuan untuk memastikan bahwa layanan sensitif dan hak akses file tidak dapat diakses secara bebas dari publik.
	Lingkungan: 1. Sistem digunakan untuk mendukung layanan akademik aktif. 2. Domain berada pada lingkungan produksi yang terekspos ke publik.	Melakukan pengujian keamanan dari sisi eksternal dengan *black-box testing* untuk menilai risiko pada sistem yang berada di lingkungan produksi. Pengujian ini bertujuan untuk mengetahui potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

Berdasarkan solusi yang diusulkan, penelitian ini berfokus pada penerapan pengujian keamanan secara sistematis untuk mengidentifikasi potensi *Security Misconfiguration* pada domain unpas.dev. Hasil dari pengujian tersebut selanjutnya akan digunakan sebagai dasar dalam proses analisis temuan serta penyusunan rekomendasi perbaikan keamanan pada tahap berikutnya.

3.4 Kerangka Berpikir Teoritis

Pada subbab ini dibahas mengenai gambaran tugas akhir dan skema analisis teori yang digunakan dalam penelitian. Kerangka berpikir teoritis bertujuan untuk menggambarkan hubungan antara permasalahan, teori, metode, serta tahapan pengujian keamanan yang digunakan dalam penelitian ini. Selain itu, skema analisis teori digunakan untuk memperlihatkan alur analisis penelitian mulai dari input, proses analisis, hingga output yang dihasilkan.

Berikut merupakan kerangka berpikir teoritis yang digunakan dalam penelitian tugas akhir ini:



Gambar 3. 2 Kerangka Berpikir Teoritis

Gambar di atas menunjukkan kerangka berpikir teoritis yang dibagi menjadi 4 tahapan utama, yaitu:

1. **Tahap identifikasi masalah (*problem)***

   Fokus penelitian berawal dari domain target unpas.dev yang memiliki permasalahan utama berupa belum dilakukannya pengujian keamanan secara formal pada domain tersebut. Kondisi ini mendasari perlunya dilakukan pengujian keamanan server untuk mengidentifikasi potensi kerentanan yang ada.

2. Tahap *Input*

Landasan teori yang digunakan sebagai masukan penelitian mencakup konsep *Security Testing* yang diimplementasikan melalui metode *Vulnerability Assessment* dengan merujuk pada standar *Penetration Testing Execution Standard* (PTES). Selain itu, standar OWASP Top 10 Tahun 2025 digunakan sebagai acuan parameter kerentanan, dengan fokus spesifik pada kategori *Security Misconfiguration.*

3. Tahap Proses

Tahap proses merupakan implementasi teknis yang mengikuti 7 fase metodologi PTES secara berurutan, mulai dari *Pre-Engagement Interaction, Intelligence Gathering,* hingga *Threat Modeling* yang mengintegrasikan teori *Security Misconfiguration*. Selanjutnya, dilakukan *Vulnerability Analysis* kemudian dilanjutkan dengan penyusunan Analisis Dampak, dan diakhiri dengan fase *Reporting.*

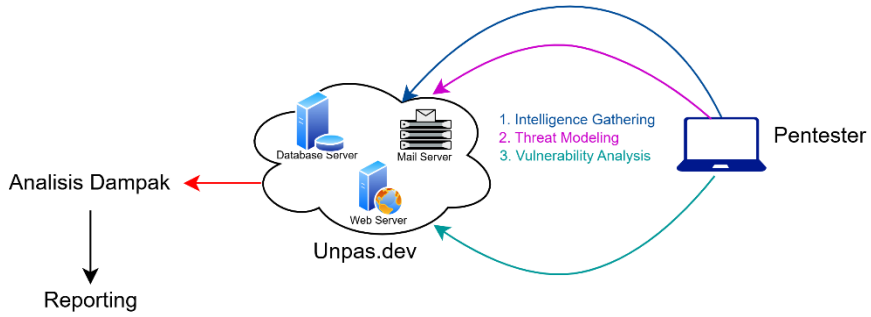
4. Tahap Output

Hasil akhir dari penelitian ini diperoleh melalui fase pelaporan yang menghasilkan dua luaran utama, yaitu penyusunan rekomendasi perbaikan untuk menutup celah keamanan yang ditemukan serta penilaian risiko menggunakan standar CVSS (*Common Vulnerability Scoring System*) untuk menentukan tingkat keparahan kerentanan.

3.4.1 Gambaran Produk Tugas Akhir

Gambaran produk tugas akhir pada penelitian ini berupa proses pengujian keamanan server dan layanan pada domain unpas.dev menggunakan metode *Vulnerability Assessment* berbasis PTES. Pengujian dilakukan untuk mengidentifikasi potensi *Security Misconfiguration* serta menghasilkan laporan hasil pengujian dan rekomendasi perbaikan.

Berikut merupakan gambaran produk tugas akhir yang digunakan dalam penelitian ini:



Gambar 3. 3 Gambaran Produk Tugas Akhir

Berdasarkan gambar di atas, penjelasan mengenai gambaran produk tugas akhir yang merepresentasikan alur kerja teknis penelitian ini adalah sebagai berikut:

1. Objek dan Subjek Pengujian

Diagram tersebut mengilustrasikan hubungan interaktif antara peneliti yang berperan sebagai *pentester* dengan infrastruktur domain unpas.dev sebagai objek target penelitian.

2. Sinkronisasi Aktivitas dan Warna

Terdapat 3 tahap utama pengujian yang dilakukan terhadap objek target, di mana setiap nomor aktivitas (1 hingga 3) memiliki warna yang selaras dengan garis panah alur pengujian. Hal ini menunjukkan urutan proses pengujian yang dimulai dari *Intelligence Gathering* (biru), *Threat Modeling* (ungu), hingga *Vulnerability Analysis* (hijau toska). Secara teknis, verifikasi manual terhadap validitas kerentanan yang ditemukan dilakukan pada tahap *Vulnerability Analysis* dengan batas maksimal tiga kali percobaan pemeriksaan per indikasi untuk meminimalkan risiko gangguan terhadap sistem target.

3. Representasi Server dan Layanan

Pengujian keamanan difokuskan pada tiga unit server utama, yaitu *web server*, *database server,* dan *mail server*. Masing-masing server merepresentasikan kumpulan layanan yang menjadi objek pengujian keamanan.

4. Pelaporan Hasil

Alur panah yang mengarah keluar dari objek penelitian menunjukkan tahapan pasca-pengujian, yaitu analisis dampak untuk menganalisis dampak dari kerentanan yang ditemukan. Seluruh proses pengujian kemudian diakhiri dengan tahap *reporting* yang berisi dokumentasi teknis, penilaian risiko, serta rekomendasi perbaikan.

3.4.2 Skema Analisis Teori

Skema analisis menjelaskan mengenai analisis yang dilakukan selama penelitian tugas akhir. Skema analisis ini memperlihatkan *input* yang diperlukan untuk kebutuhan analisis dan *output* dari hasil analisis yang dilakukan. Terdapat tiga komponen utama yang terdapat pada skema analisis yaitu sebagai berikut:

1. Input

Komponen pertama yang menjelaskan mengenai masukan yang digunakan sebagai acuan atau referensi untuk tahap analisis. *Input* bisa berupa data dan informasi yang dapat dijadikan dasar dalam analisis.

2. Analisis

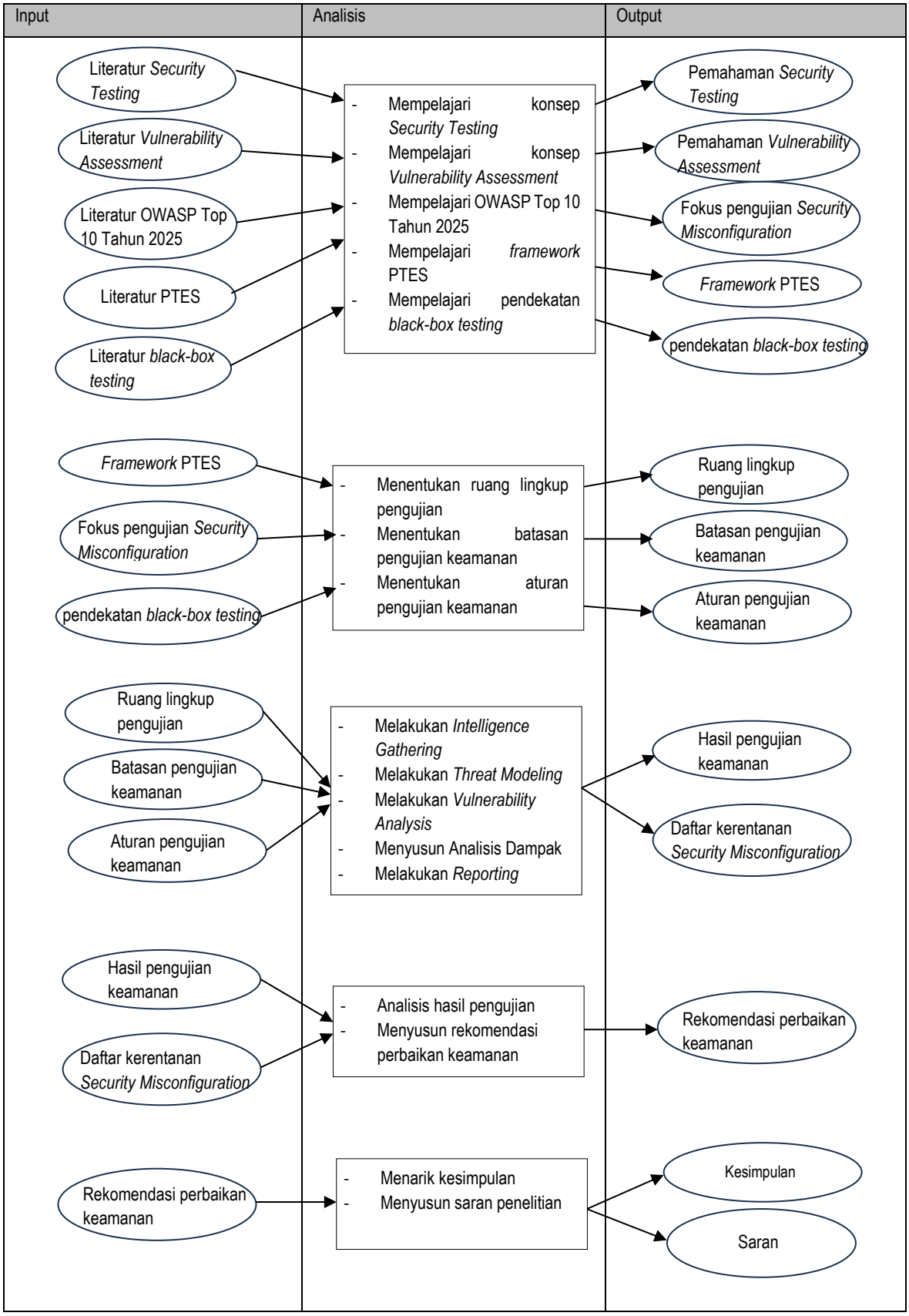
Komponen yang menjelaskan mengenai tahapan analisis yang dilakukan dalam penelitian tugas akhir. Tujuannya untuk mengetahui keadaan sebenarnya dalam pengerjaan tugas akhir terkait objek penelitian.

3. Output

Komponen terakhir yang menjelaskan mengenai keluaran yang dihasilkan dari tahap analisis.

Berikut merupakan gambar skema analisis dari penelitian tugas akhir yang dilakukan:

Tabel 3. 3 Skema Analisis Teori



Berdasarkan tabel di atas, berikut penjelasan detail skema analisis pengujian keamanan konfigurasi server dan layanan pada tugas akhir ini:

Tabel 3. 4 Penjelasan Skema Analisis Teori

No	Input	Analisis	Output	Penjelasan
1	- Literatur *Security Testing.* - Literatur *Vulnerability Assessment* - Literatur OWASP Top 10 Tahun 2025. - Literatur PTES. - Literatur *black-box testing.*	- Mempelajari konsep *Security Testing.* - Mempelajari konsep *Vulnerability Assessment.* - Mempelajari OWASP Top 10 Tahun 2025. - Mempelajari *framework* PTES. - Mempelajari pendekatan *black-box testing.*	- Pemahaman *Security Testing.* - Pemahaman *Vulnerability Assessment.* - Fokus pengujian *Security Misconfiguration.* - *Framework* PTES - Pendekatan *black-box testing.*	Tahap ini dilakukan untuk memahami konsep dasar pengujian keamanan, *Vulnerability Assessment*, *framework* PTES, serta pendekatan *black-box testing* yang digunakan sebagai dasar penelitian keamanan server dan layanan pada domain unpas.dev.
2	- *Framework* PTES. - Fokus pengujian *Security Misconfiguration.* - Pendekatan *black-box testing.*	- Menentukan ruang lingkup pengujian. - Menentukan batasan pengujian keamanan. - Menentukan aturan pengujian keamanan.	- Ruang lingkup pengujian. - Batasan pengujian keamanan. - Aturan pengujian keamanan.	Tahap ini dilakukan untuk menentukan ruang lingkup, batasan, dan aturan pengujian berdasarkan *framework* PTES dan *black-box testing* agar pengujian sesuai dengan fokus *Security Misconfiguration.*
3	- Ruang lingkup pengujian. - Batasan pengujian keamanan. - Aturan pengujian keamanan	- Melakukan *Intelligence Gathering* - Melakukan *Threat Modeling* - Melakukan *Vulnerability Analysis* - Menyusun Analisis Dampak - Melakukan *Reporting*	- Hasil pengujian keamanan - Daftar kerentanan *Security Misconfiguration*	Tahap ini dilakukan untuk melaksanakan *Vulnerability Assessment* pada domain unpas.dev menggunakan tahapan PTES guna memperoleh hasil pengujian dan mengidentifikasi kerentanan *Security Misconfiguration.*
4	- Hasil pengujian keamanan - Daftar kerentanan *Security Misconfiguration*	- Analisis hasil pengujian - Menyusun rekomendasi perbaikan keamanan	Rekomendasi perbaikan keamanan	Tahap ini dilakukan untuk menganalisis hasil *Vulnerability Assessment* dan menyusun rekomendasi

No	Input	Analisis	Output	Penjelasan
				perbaikan terhadap kerentanan *Security Misconfiguration* yang ditemukan pada domain unpas.dev
5	Rekomendasi perbaikan	- Menarik Kesimpulan - Menyusun saran penelitian	- Kesimpulan - Saran	Tahap ini dilakukan untuk menyusun Kesimpulan berdasarkan hasil *Vulnerability Assessment* serta memberikan saran untuk pengembangan penelitian selanjutnya.

3.5 Profil Penelitian

Pada penelitian ini, profil penelitian dibagi menjadi dua bagian yaitu objek penelitian dan tempat penilaian. Subbab ini bertujuan untuk menjelaskan objek yang diteliti serta Lokasi pelaksanaan penelitian.

3.5.1 Objek Penelitian

Objek penelitian dalam tugas akhir ini adalah domain unpas.dev milik Fakultas Teknik Universitas Pasundan. Domain unpas.dev merupakan domain yang digunakan sebagai lingkungan pengembangan dan pengujian layanan akademik di lingkungan Fakultas Teknik Universitas Pasundan. Domain ini mulai aktif digunakan sejak Maret 2024 dan beroperasi pada lingkungan produksi yang terhubung langsung dengan jaringan internet publik. Pengujian yang dilakukan pada domain unpas.dev difokuskan pada aspek keamanan konfigurasi server dan layanan yang berjalan pada domain tersebut.

3.5.2 Profil Tempat Penelitian

Penelitian tugas akhir ini dilaksanakan di Fakultas Teknik Universitas Pasundan yang beralamat di Jalan Dr. Setiabudhi No.193, Gegerkalong, Kec. Sukasari, Kota Bandung, Jawa Barat 40153. Fakultas Teknik yang awalnya bernama Fakultas Teknologi berdiri pada bulan Desember 1961 atas prakarsa seorang tokoh pendidikan yaitu Prof. Dr. Moestopo [FTU26].

Fakultas Teknik Universitas Pasundan saat ini menyelenggarakan enam program studi sarjana (S1) yang mayoritas telah berakreditasi Unggul, meliputi Teknik Industri, Teknologi Pangan, Teknik Mesin, Teknik Informatika, Teknik Lingkungan, dan Perencanaan Wilayah dan Kota (PWK/Planologi) [FTU26].

3.5.2.1 Visi

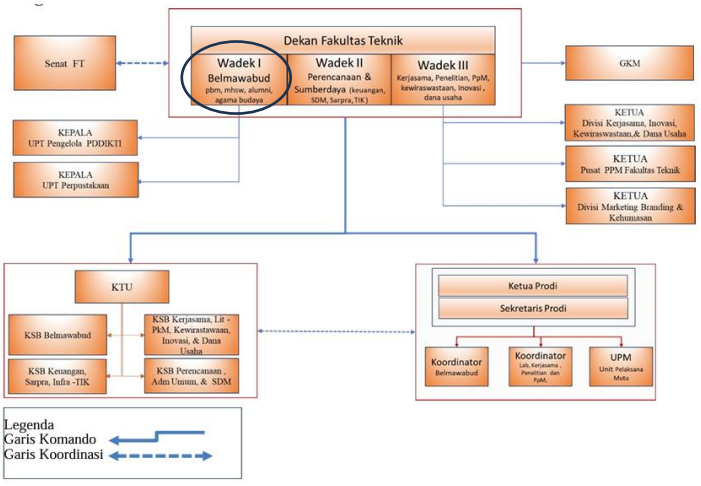
Menjadi Fakultas Teknik yang unggul dan diakui secara internasional dalam penyelenggaraan pendidikan, penelitian, dan pengabdian kepada masyarakat pada tahun 2037 [FTU26].

3.5.2.2 Misi

1. Menyelenggarakan pendidikan tinggi yang berkualitas berbasis *Outcome-Based Education* (OBE) dan Merdeka Belajar Kampus Merdeka (MBKM) guna menghasilkan lulusan yang kompeten, profesional, berkarakter, dan adaptif terhadap perkembangan teknologi.
2. Mengembangkan penelitian yang inovatif dan berdaya saing melalui peningkatan kualitas dan kuantitas publikasi ilmiah, penguatan riset unggulan, serta hilirisasi hasil penelitian yang memberikan nilai tambah bagi masyarakat dan industri.
3. Melaksanakan pengabdian kepada masyarakat yang berdampak nyata melalui penerapan teknologi tepat guna, pemberdayaan masyarakat, serta kontribusi dalam penyelesaian permasalahan sosial dan lingkungan.
4. Mewujudkan tata kelola fakultas yang unggul dan berkelanjutan melalui penerapan prinsip *Good Fakulty Governance,* sistem penjaminan mutu internal (SPMI), digitalisasi layanan, serta pengelolaan sumber daya yang transparan, akuntabel, dan efisien.

3.5.2.3 Struktur Organisasi

Secara struktural, penelitian ini berada di bawah koordinasi Program Studi Teknik Infomatika, Fakultas Teknik, Universitas Pasundan. Pelaksanaan pengujian pada penelitian ini memperoleh izin resmi dari Wakil Dekan Bidang I Fakultas Teknik Universitas Pasundan, yang membawahi bidang pembelajaran, kemahasiswaan, alumni, serta agama dan budaya (Belmawabud). Struktur Organisasi Fakultas Teknik Universitas Pasundan secara umum ditampilkan pada Gambar 3.4 berikut:



Gambar 3. 4 Struktur Organisasi

BAB 4
ANALISIS DAN PERANCANGAN PENGUJIAN

4.1 Kebutuhan Pengujian

4.1.1 Kebutuhan Data Pengujian

Sebelum melaksanakan pengujian, diperlukan beberapa data dan informasi awal sebagai dasar penentuan ruang lingkup, batasan, dan legalitas pengujian sesuai dengan fase *Pre-Engagement Interaction* pada PTES. kebutuhan data tersebut dijabarkan pada Tabel 4.1

Tabel 4. 1 Kebutuhan Data Pengujian

No	Kebutuhan Data	Keterangan
1	Target domain	Unpas.dev sebagai domain utama yang menjadi ruang lingkup pengujian sesuai izin resmi. Subdomain yang termasuk dalam ruang lingkup akan diidentifikasi secara teknis pada tahap *Intelligence Gathering*.
2	Ruang lingkup pengujian	*Security Misconfiguration*
3	Batasan pengujian	*black-box testing*, bersifat non-destruktif, validasi temuan maksimal 3x percobaan per indikasi.
4	Dokumentasi izin resmi	Surat izin penelitian No. 306/Unpas.FT.D1/Q/V/2026 dari Wakil Dekan Bidang I Fakultas Teknik Universitas Pasundan
6	Penanganan objek di luar ruang lingkup	Aplikasi, subdomain, port, atau layanan yang ditemukan di luar lingkup hanya dicatat sebagai informasi pendukung dan tidak dilanjutkan ke tahap analisis kerentanan

4.1.2 Kebutuhan Tools Pengujian

pengujian ini menggunakan beberapa tools berbasis open-source dan layanan daring yang dipilih berdasarkan kesesuaian dengan setiap parameter *Security Misconfiguration* yang diuji. Rincian tools tersebut dijabarkan pada Tabel 4.2.

Tabel 4. 2 Kebutuhan Tools Pengujian

No	Tools	Fase Penggunaan	Fungsi	Alasan Pemilihan
1	Dns Lookup, crt.sh	*Intelligence Gathering*	Enumerasi subdomain secara pasif melalui catatan DNS dan sertifikat SSL	Tidak mengirim permintaan langsung ke server target
2	Subfinder, theHarvester	*Intelligence Gathering*	Enumerasi subdomain dari berbagai sumber pasif (CT log, search engine, database publik)	Memperluas cakupan identifikasi subdomain tanpa menyentuh server target
3	Nmap	*Intelligence Gathering, Vulnerability Analysis*	Pemindaian port, deteksi layanan dan versi	Standar industri, mendukung service/version detection dan scripting engine
4	Netcat / curl	*Intelligence Gathering, Vulnerability Analysis*	Verifikasi status port, *banner grabbing*, pemeriksaan *response header HTTP*	Ringan, dapat dijalankan berulang dan validasi silang

No	Tools	Fase Penggunaan	Fungsi	Alasan Pemilihan
5	WhatWeb	*Intelligence Gathering*	Identifikasi teknologi web (CMS, *framework, web server*)	Mendukung *passive fingerprinting* tanpa membebani server
6	Browser Developer Tools	*Vulnerability Analysis*	Inspeksi header keamanan dan respon HTTP secara visual	Memudahkan verifikasi manual hasil curl/ZAP
7	OWASP ZAP	*Vulnerability Analysis*	Pemeriksaan *security headers, directory listing*, pesan error otomatis	Tools resmi OWASP, selaras dengan kerangka OWASP TOP 10:2025
8	Dirsearch	*Vulnerability Analysis*	Pencarian direktori dan file yang dapat diakses publik	Mendukung deteksi *directory listing* dan konfigruasi default
9	Testssl.sh	*Vulnerability Analysis*	Analisis konfigurasi SSL/TLS, versi protokol, dan cipher suite	*Command-line*, hasil terstruktur dan dapat disimpan sebagai file log
10	SSL Labs (web)	*Vulnerability Analysis*	Penilaian konfigurasi HTTPS secara daring dengan *grading* standar industri	Hasil mudah diinterpretasikan dan mengacu standar SSL Labs Rating Guide
11	Nmap ssl-enum-ciphers	*Vulnerability Analysis*	Enumerasi cipher suite yang didukung server	Validasi tambahan terhadap hasil testssl.sh
12	*AI Asistant*	*Intelligence Gathering, Vulnerability Analysis.*	Membantu memeriksa temuan dari berbagai tools, serta membantu memperkirakan tingkat risikonya	Mempercepat proses memeriksa data dari berbagai tools sebelum dicek ulang sendiri oleh penulis. AI tidak memiliki akses langsung terhadap target

4.2 Rancangan *Intelligence Gathering*

Tahap *Intelligence Gathering* merupakan tahap pengumpulan informasi awal terhadap target pengujian. Pada penelitian ini, tahap tersebut dilakukan untuk memperoleh informasi teknis mengenai domain unpas.dev dan layanan yang termasuk dalam ruang lingkup pengujian. Pengumpulan informasi dilakukan menggunakan *black-box testing*, sehingga informasi yang diperoleh berasal dari sisi eksternal atau publik. Rancangan tahap *Intelligence Gathering* dapat dilihat pada Tabel 4.3.

Tabel 4. 3 Rancangan *Intelligence Gathering*

No	Langkah Pengujian	Tools/Metode	Jenis Pengujian	Output
1	Melakukan identifikasi domain dan subdomain	DNS lookup, crt.sh, Search engine	Pasif	Daftar domain atau subdomain yang berkaitan dengan target pengujian.
2	Melakukan pemindaian port terbuka	Nmap, Netcat	Aktif	Daftar port terbuka pada target yang termasuk dalam ruang lingkup pengujian.
3	Mengidentifikasi layanan aktif	Nmap service detection, Banner grabbing (curl)	Aktif	Informasi layanan yang berjalan pada port terbuka

No	Langkah Pengujian	Tools/Metode	Jenis Pengujian	Output
4	Mengidentifikasi teknologi web	WhatWeb, curl, Browser developer tools	Pasif/aktif	Informasi teknologi web ,*Framework*, dan komponen pendukung yang digunakan
5	Mendokumentasikan informasi awal target	Screenshot, Log terminal	Pasif	Dokumentasi informasi awal target

4.3 Rancangan *Threat Modeling*

Tahap *Threat Modeling* merupakan tahap pemetaan potensi ancaman berdasarkan informasi awal yang diperoleh dari tahap *Intelligence Gathering*. Pada penelitian ini, tahap *Threat Modeling* difokuskan pada potensi ancaman yang berkaitan dengan konfigurasi server dan layanan pada domain unpas.dev. pemetaan ancaman dilakukan untuk mengelompokkan kemungkinan risiko berdasarkan parameter *Security Misconfiguration* sebelum dilakukan analisis kerentanan pada tahap berikutnya.

Rancangan tahap *Threat Modeling* dapat dilihat pada tabel 4.4.

Tabel 4. 4 Rancangan *Threat Modeling*

No	Langkah Pengujian	Output
1	Mengidentifikasi potensi ancaman berdasarkan hasil *Intelligence Gathering*	Daftar potensi ancaman terhadap konfigurasi server dan layanan
2	Mengelompokkan ancaman berdasarkan jenis *Security Misconfiguration*	Kelompok ancaman berdasarkan parameter *Security Misconfiguration*
3	Menentukan prioritas awal ancaman	Prioritas awal ancaman berdasarkan potensi dampak terhadap layanan
4	Mendokumentasikan peta ancaman	Dokumentasi peta ancaman sebagai dasar tahap Vulnerability Analysis

4.4 Rancangan *Vulnerability Analysis*

Tahap *Vulnerability Analysis* merupakan tahap analisis terhadap potensi kerentanan berdasarkan informasi yang telah diperoleh pada tahap sebelumnya. Pada penelitian ini, analisis diarahkan untuk menemukan indikasi awal *Security Misconfiguration* pada konfigurasi server dan layanan. Hasil dari tahap ini belum ditetapkan sebagai temuan akhir, tetapi menjadi dasar untuk proses validasi pada tahap berikutnya. Rancangan tahap *Vulnerability Analysis* dapat dilihat pada Tabel 4.5.

Tabel 4. 5 Rancangan *Vulnerability Analysis*

No	Langkah Pengujian	Tools/Metode	Output
1	Melakukan analisis konfigurasi port dan layanan	Nmap, Netcat/Telnet	Indikasi port dan layanan yang terbuka
2	Mengidentifikasi penggunaan konfigurasi default	Browser, curl, OWASP ZAP, Dirsearch	Indikasi halaman default, file contoh, atau konfigurasi bawaan

No	Langkah Pengujian	Tools/Metode	Output
3	Melakukan pemeriksaan *directory listing*	Browser, curl, OWASP ZAP	Indikasi direktori yang dapat ditelusuri publik
4	Melakukan pemeriksaan pesan error informatif	Browser, curl, OWASP ZAP	Indikasi pesan error yang menampilkan informasi teknis
5	Melakukan pemeriksaan HTTP security headers	Browser Developer Tools, curl, OWASP ZAP	Informasi header keamanan yang diterapkan atau belum diterapkan
6	Melakukan analisis konfigurasi SSL/TLS	SSL Labs, Testssl.sh, Nmap ssl-enum-ciphers	Informasi keamanan koneksi HTTPS
7	Melakukan pemeriksaan informasi versi layanan	Nmap service detection, curl, Whatweb	Indikasi informasi versi layanan yang terekspos
8	Mendokumentasikan seluruh indikasi kerentanan	Screenshot, Log terminal	Daftar indikasi potensi temuan

Sebagai bagian akhir dari tahap Vulnerability Analysis, dilakukan verifikasi manual terhadap indikasi kerentanan secara terbatas. Verifikasi dilakukan untuk memastikan apakah indikasi kerentanan yang diperoleh benar-benar valid. Rancangan verifikasi manual dapat dilihat pada Tabel 4.6.

Tabel 4. 6 Rancangan Verifikasi Manual Temuan

No	Langkah Pengujian	Keterangan	Output
1	Menentukan skenario validasi	Menentukan cara validasi untuk setiap indikasi temuan berdasarkan parameter *Security Misconfiguration.*	Skenario validasi temuan
2	Melakukan validasi menggunakan beberapa tools/metode	Melakukan pemeriksaan ulang menggunakan maksimal 3 tools atau metode pemeriksaan untuk mengurangi *false positive*	Bukti validasi
3	Membatasi aktivitas validasi	Membatasi validasi hanya pada pembuktian adanya indikasi kesalahan konfigurasi tanpa tindakan destruktif	Validasi yang aman dan terkontrol
4	Mendokumentasikan hasil validasi	Mencatat hasil validasi berupa temuan valid atau temuan yang dinyatakan tidak valid	Daftar temuan valid dan tidak valid

4.5 Rancangan Analisis Dampak

Tahap Analisis Dampak pada penelitian ini digunakan untuk menganalisis dampak dari temuan yang telah diverifikasi. Tahap ini tidak diarahkan untuk mempertahankan akses atau melakukan eksploitasi lanjutan terhadap sistem. Analisis dampak dilakukan untuk mengetahui

pengaruh temuan terhadap aspek kerahasiaan, integritas, dan ketersediaan layanan. Rancangan analisis dampak dapat dilihat pada Tabel 4.7.

Tabel 4. 7 Rancangan Analisis Dampak

No	Langkah Pengujian	Output
1	Menganalisis dampak dari setiap temuan yang telah divalidasi	Analisis dampak temuan terhadap keamanan sistem
2	Mengidentifikasi layanan yang berpotensi terdampak	Informasi potensi dampak terhadap layanan yang diuji
3	Menentukan dasar penilaian risiko berdasarkan dampak temuan	Dasar penilaian risiko menggunakan cvss
4	Mendokumentasikan hasil analisis dampak	Dokumentasi hasil analisis dampak sebagai dasar rekomendasi perbaikan

4.6 Rancangan Tahap *Reporting*

Tahap *Reporting* merupakan tahap penyusunan laporan hasil pengujian berdasarkan temuan yang divalidasi dan dianalisis dampaknya. Pada tahap ini, setiap temuan didokumentasikan secara sistematis agar dapat menjelaskan kondisi keamanan konfigurasi server dan layanan yang di uji. Hasil pelaporan juga mencakup penilaian risiko serta rekomendasi perbaikan yang sesuai dengan jenis temuan. Rancangan Tahap *Reporting* dapat dilihat pada Tabel 4.8.

Tabel 4. 8 Rancangan Tahap *Reporting*

No	Langkah Penelitian	Output
1	Mendokumentasikan seluruh temuan hasil pengujian	Daftar temuan valid beserta bukti pengujian
2	Melakukan penilaian risiko terhadap setiap temuan	Nilai dan tingkat risiko berdasarkan CVSS
3	Menyusun rekomendasi perbaikan	Rekomendasi teknis sesuai jenis temuan
4	Menyusun format laporan hasil pengujian	Rancangan laporan hasil pengujian keamanan

4.7 Rancangan *Test Case* dan *Test Scenario*

Rancangan *test case* dan *test scenario* digunakan sebagai acuan teknis dalam pelaksanaan pengujian *Security Misconfiguration. Test case* menjelaskan pemeriksaan yang dilakukan pada setiap parameter pengujian, sedangkan *test scenario* menjelaskan alur pelaksanaan pengujian secara lebih operasional. Rancangan ini disusun agar proses pengujian dilakukan secara terarah, terdokumentasi, dan sesuai dengan batasan penelitian. Rancangan test Case dapat dilihat pada Tabel 4.9.

Tabel 4. 9 Rancangan *Test Case*

Kode *Test Case*	Parameter Pengujian	*Test Case*	Kriteria Indikasi Temuan
TC-01	Port dan layanan terbuka	Memeriksa port dan layanan yang dapat diakses dari jaringan publik	Terdapat port sensitif atau layanan yang tidak diperlukan terbuka secara publik
TC-02	Konfigurasi default	Memeriksa kemungkinan adanya halaman default, file contoh, atau konfigurasi bawaan yang masih aktif	Terdapat halaman default, file contoh, atau konfigurasi bawaan yang masih dapat diakses

Kode *Test Case*	Parameter Pengujian	*Test Case*	Kriteria Indikasi Temuan
TC-03	*Directory listing*	Memeriksa apakah direktori pada web server dapat menampilkan daftar file atau folder secara publik	Direktori menampilkan daftar file atau folder secara publik tanpa pembatasan akses
TC-04	Pesan error informatif	Memeriksa pesan error yang ditampilkan oleh sistem	Pesan error menampilkan informasi teknis seperti path, versi layanan, *stack trace*, atau detail database
TC-05	HTTP *security headers*	Memeriksa penerapan header keamanan pada respons HTTP/HTTPS	Header keamanan tidak ada, tidak lengkap, atau belum dikonfigurasi dengan tepat
TC-06	Konfigurasi SSL/TLS	Memeriksa keamanan konfigurasi HTTPS pada target pengujian	Terdapat penggunaan protokol TLS lama. *Cipher* lemah, sertifikat bermasalah, atau konfigurasi HTTPS yang kurang aman
TC-07	Informasi versi layanan	Memeriksa informasi layanan yang terekspos melalui *banner, header*, atau respons layanan	Versi *web server, framework, database*, atau layanan tertentu dapat diketahui dari sisi publik

Rancangan *test scenario* dapat dilihat pada Tabel 4.10.

Tabel 4. 10 Rancangan *Test Scenario*

Kode *Test Sklenario*	*Test Skenario*	Kode *Test Case*	*Test Case*	*Test Step*	*Tools/Metode*	Output yang diharapkan
TS-01	Pengujian Port dan layanan terbuka	TC-01	Memeriksa port dan layanan yang dapat diakses dari jaringan publik	- Menentukan alamat IP atau domain target yang akan diuji - Melakukan pemindaian port terhadap target - Mengidentifikasi port yang statusnya terbuka - Mengidentifikasi layanan yang berjalan pada port terbuka - Mendokumentasikan hasil pemindaian untuk dianalisis lebih lanjut.	- Nmap - Netcat	Diperoleh daftar port dan layanan yang terbuka
TS-02	Pengujian Konfigurasi default	TC-02	Memeriksa kemungkinan adanya halaman default, file contoh, atau konfigurasi	- Mengakses halaman utama aplikasi atau server - Memeriksa keberadaan halaman default yang umum digunakan - Memeriksa kemungkinan adanya file contoh atau	- Browser - Dirsearch - OWASP ZAP	Diketahui apakah terdapat halaman default, file contoh atau konfigurasi bawaan yang masih dapat diakses

Kode *Test Sklenario*	*Test Skenario*	Kode *Test Case*	*Test Case*	*Test Step*	*Tools/Metode*	Output yang diharapkan
			bawaan yang masih aktif	dokumentasi bawaan yang dapat diakses publik - Mencatat setiap konfigurasi bawaan yang masih aktif - Mendokumentasikan hasil pemeriksaan		
TS-03	Pengujian Directory listing	TC-03	Memeriksa apakah direktori pada web server dapat menampilkan daftar file atau folder secara publik	- Mengidentifikasi direktori yang dapat diakses melalui web - Mengakses direktori yang teridentifikasi menggunakan browser atau alat bantu pemeriksaan - Mengamati apakah sistem menampilkan daftar file atau folder - Mencatat direktori yang memungkinkan penelusuran publik - Mendokumentasikan hasil pemeriksaan	- Browser - Curl - OWASP ZAP	Diketahui apakah terdapat direktori yang dapat ditelusuri publik
TS-04	Pengujian Pesan error informatif	TC-04	Memeriksa pesan error yang ditampilkan oleh sistem	- Mengakses halaman atau fungsi yang tersedia pada aplikasi - Mengamati respons sistem ketika terjadi kesalahan akses atau permintaan yang tidak valid - Memeriksa apakah pesan error menampilkan informasi teknis terekspos - Mendokumentasikan pesan error yang ditemukan	- Browser - Curl - OWASP ZAP	Diketahui apakah pesan error menampilkan informasi teknis atau informasi yang dapat membantu enumerasi
TS-05	Pengujian HTTP security headers	TC-05	Memeriksa penerapan header keamanan pada respons HTTP/HTTPS	- Mengambil respons header dari target menggunakan curl - Memeriksa header melalui Browser Developer Tools - Membandingkan hasil dengan OWASP ZAP - Mencatat header yang tersedia maupun yang tidak tersedia	- Curl - OWASP ZAP - Browser Developer Tools	Diketahui header keamanan yang sudah diterapkan atau belum diterapkan

Kode *Test Sklenario*	*Test Skenario*	Kode *Test Case*	*Test Case*	*Test Step*	*Tools/Metode*	Output yang diharapkan
TS-06	Pengujian Konfigurasi SSL/TLS	TC-06	Memeriksa keamanan konfigurasi HTTPS pada target pengujian	- Memeriksa layanan HTTPS - Mengidentifikasi versi TLS yang didukung - Memeriksa cipher suite - Memeriksa sertifikat digital - Mendokumentasikan hasil pemeriksaan konfigurasi SSL/TLS	- SSL Labs - Tetssl.sh - Nmap ssl-enum-ciphers	Diketahui kondisi keamanan konfigurasi SSL/TLS pada target
TS-07	Pengujian Informasi versi layanan	TC-07	Memeriksa informasi layanan yang terekspos melalui banner, header, atau respons layanan	- Mengidentifikasi teknologi web menggunakan WhatWeb - Memeriksa banner atau header menggunakan curl - Melakukan service detection menggunakan Nmap - Mencatat apakah terdapat informasi versi layanan yang terekspos	- WhatWeb - Nmap Service Detection - Curl	Diketahui apakah *versi web server, framework, database,* atau layanan tertentu terekspos dari sisi publik

BAB 5
HASIL DAN PEMBAHASAN

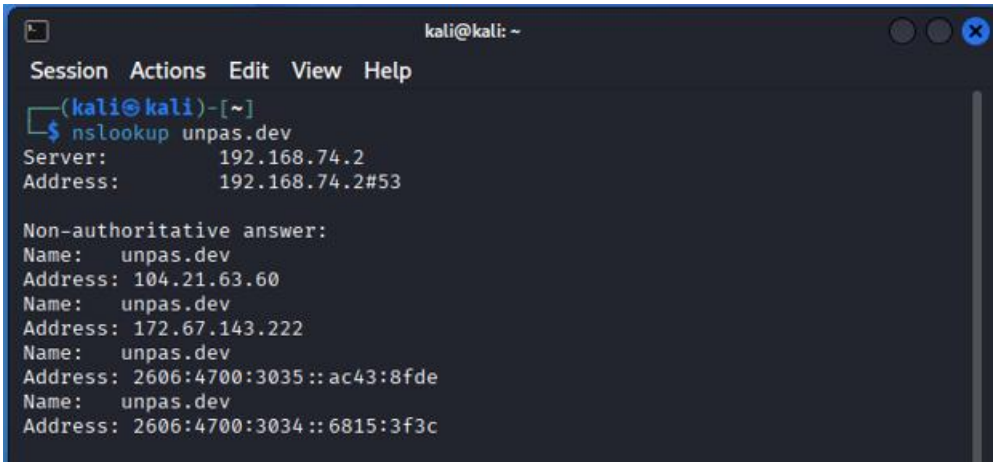
5.1 Hasil *Intelligence Gathering*

5.1.1 Hasil Identifikasi Domain dan Subdomain

Identifikasi domain dan subdomain dilakukan secara bertahap menggunakan beberapa teknik pasif, yaitu pencatatan DNS, *Certificate Transparency log,* enumerasi subdomain otomatis, *OSINT* gathering, dan Google dorking.

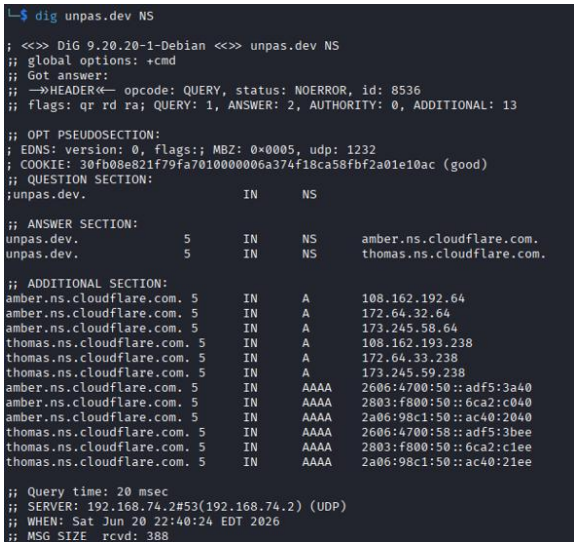
1. DNS Lookup

Pemeriksaan catatan DNS dilakukan menggunakan perintah nslookup dan dig untuk mengidentifikasi alamat IP, *name server*, serta MC, dan catatan TXT yang terkait dengan domain unpas.dev.



Gambar 5. 1 Hasil nslookup unpas.dev

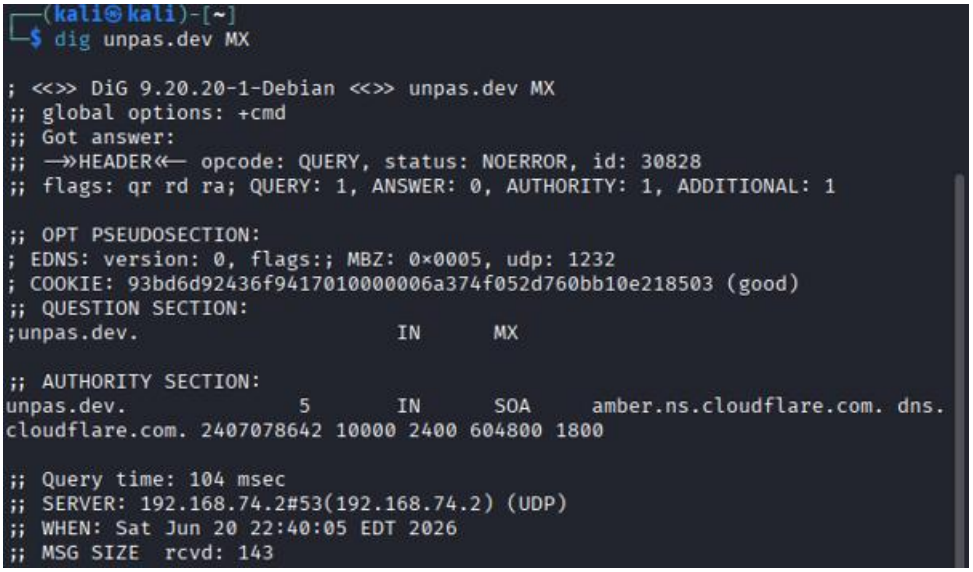
Berdasarkan gambar 5.1, domain unpas.dev me-*resolve* ke dua alamat IP publik yaitu 104.21.63.60 dan 172.67.143.222 beserta dua alamat Ipv6. Kedua IP tersebut merupakan alamat *edge* milik *Cloudflare*, bukan IP *origin* server asli dan mengindikasikan bahwa domain ini dilindungi oleh layanan *proxy*/CDN *Cloudflare*.



```
└─$ dig unpas.dev NS

; <<>> DiG 9.20.20-1-Debian <<>> unpas.dev NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8536
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
; COOKIE: 30fb08e821f79fa7010000006a374f18ca58fbf2a01e10ac (good)
;; QUESTION SECTION:
;unpas.dev.                     IN      NS

;; ANSWER SECTION:
unpas.dev.              5       IN      NS      amber.ns.cloudflare.com.
unpas.dev.              5       IN      NS      thomas.ns.cloudflare.com.

;; ADDITIONAL SECTION:
amber.ns.cloudflare.com. 5      IN      A       108.162.192.64
amber.ns.cloudflare.com. 5      IN      A       172.64.32.64
amber.ns.cloudflare.com. 5      IN      A       173.245.58.64
thomas.ns.cloudflare.com. 5     IN      A       108.162.193.238
thomas.ns.cloudflare.com. 5     IN      A       172.64.33.238
thomas.ns.cloudflare.com. 5     IN      A       173.245.59.238
amber.ns.cloudflare.com. 5      IN      AAAA    2606:4700:50::adf5:3a40
amber.ns.cloudflare.com. 5      IN      AAAA    2803:f800:50::6ca2:c040
amber.ns.cloudflare.com. 5      IN      AAAA    2a06:98c1:50::ac40:2040
thomas.ns.cloudflare.com. 5     IN      AAAA    2606:4700:58::adf5:3bee
thomas.ns.cloudflare.com. 5     IN      AAAA    2803:f800:50::6ca2:c1ee
thomas.ns.cloudflare.com. 5     IN      AAAA    2a06:98c1:50::ac40:21ee

;; Query time: 20 msec
;; SERVER: 192.168.74.2#53(192.168.74.2) (UDP)
;; WHEN: Sat Jun 20 22:40:24 EDT 2026
;; MSG SIZE  rcvd: 388
```

Gambar 5. 2 Hasil dig NS unpas.dev

Gambar 5.2 menunjukkan bahwa *name server* domain unpas.dev adalah amber.ns.cloudflare.com dan thomas.ns.cloudflare.com, yang mengonfirmasi bahwa pengelolaan DNS dilakukan sepenuhnya melalui layanan *Cloudflare*.



```
┌──(kali㉿kali)-[~]
└─$ dig unpas.dev MX

; <<>> DiG 9.20.20-1-Debian <<>> unpas.dev MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30828
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
; COOKIE: 93bd6d92436f9417010000006a374f052d760bb10e218503 (good)
;; QUESTION SECTION:
;unpas.dev.                     IN      MX

;; AUTHORITY SECTION:
unpas.dev.              5       IN      SOA     amber.ns.cloudflare.com. dns.
cloudflare.com. 2407078642 10000 2400 604800 1800

;; Query time: 104 msec
;; SERVER: 192.168.74.2#53(192.168.74.2) (UDP)
;; WHEN: Sat Jun 20 22:40:05 EDT 2026
;; MSG SIZE  rcvd: 143
```

Gambar 5. 3 Hasil dig MX unpas.dev

Gambar 5.3 menunjukkan bahwa tidak ditemukan catatan MX (*Mail Exchanger)* pada domain unpas.dev (ANSWER: 0), yang berarti tidak ada *mail server* yang terkonfigurasi pada domain ini saat pengujian dilaksanakan.

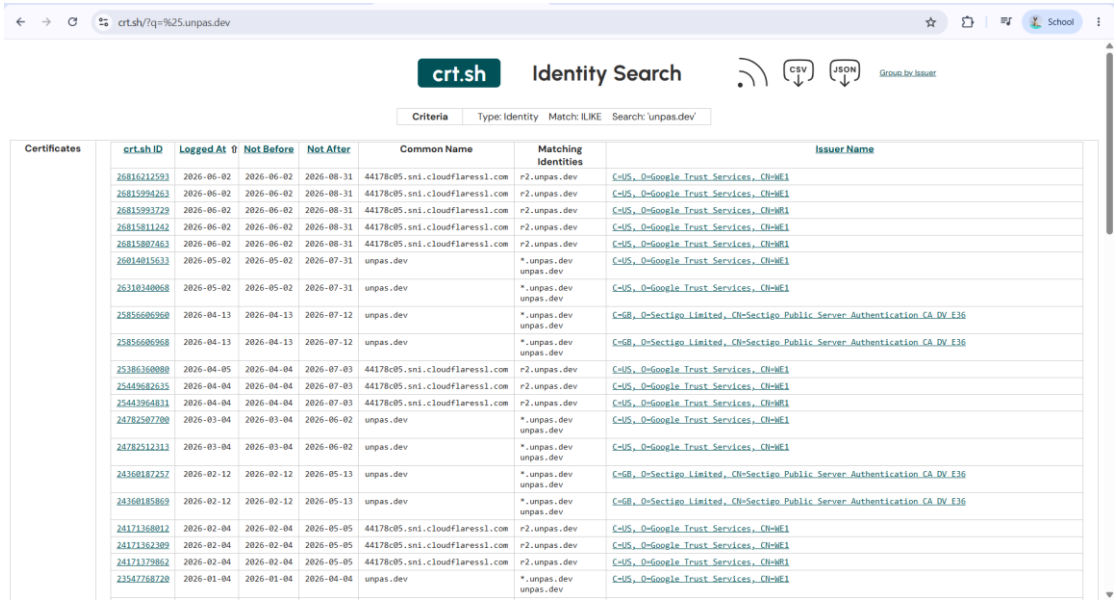
```
┌──(kali㉿kali)-[~]
└─$ dig unpas.dev TXT

; <<>> DiG 9.20.20-1-Debian <<>> unpas.dev TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63646
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
; COOKIE: ddf89d7b837b50e3010000006a374f2bd3cebcff2cc0bbfe (good)
;; QUESTION SECTION:
;unpas.dev.                     IN      TXT

;; ANSWER SECTION:
unpas.dev.              5       IN      TXT     "google-site-verification=On_
x0kZ1fPjzXjHXoLuQm-TznSV4ZBczNweNnhyaQ0E"

;; Query time: 28 msec
;; SERVER: 192.168.74.2#53(192.168.74.2) (UDP)
;; WHEN: Sat Jun 20 22:40:43 EDT 2026
;; MSG SIZE  rcvd: 147
```

Gambar 5. 4 Hasil dig TXT unpas.dev

Gambar 5.4 menampilkan catatan TXT yang berisi entri *google-site-verification*, yaitu token verifikasi kepemilikan domain pada *Google Search Console*. Tidak ditemukan catatan TXT lain yang berpotensi membocorkan informasi teknis sensitif.

2. *Certificate Transparency Log* (crt.sh)

Pencarian melalui *Certificate Trancsparency log* dilakukan menggunakan layanan crt.sh dengan kueri %25.unpas.dev untuk mengidentifikasi subdomain yang pernah menerbitkan sertifikat SSL/TLS



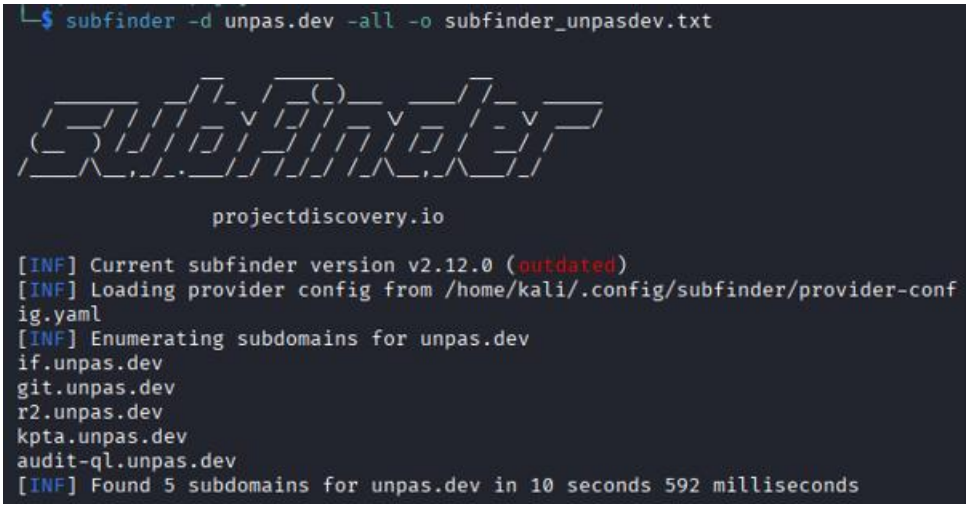
Gambar 5. 5 Hasil Pencarian Certificate Transparency Log (crt.sh)

Berdasarkan gambar 5.5, ditemukan dua informasi penting. Pertama, seluruh sertifikat yang ditemukan menggunakan *wildcard certificate* *.unpas.dev yang mengindikasikan bahwa

subdomain apa pun di bawah unpas.dev dilindungi oleh sertifikat yang sama sehingga tidak akan tercatat sebagai *Common Name* tersendiri di CT log. Kedua, subdomain r2.unpas.dev teridentifikasi melalui catatan SNI pada beberapa entri sertifikat. Tidak ditemukan subdomain lain secara eksplisit pada sumber ini karena penggunaan *wildcard certificate* tersebut.

3. Enumerasi Subdomain - Subfinder

Enumerasi subdomain otomatis dilakukan menggunakan tools Subfinder yang mengumpulkan data dari berbagai sumber pasif secara bersamaan.

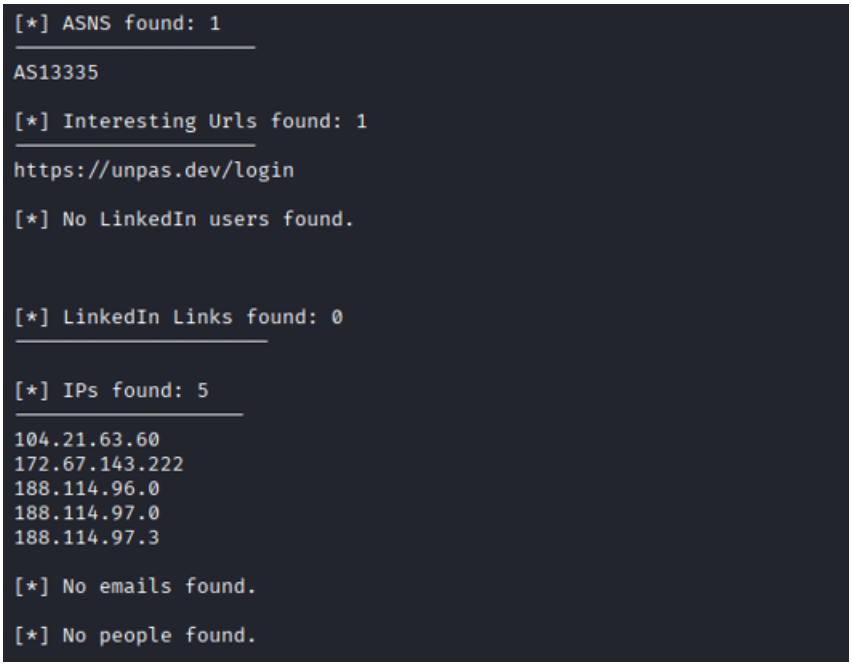


Gambar 5. 6 Hasil Enumerasi Subfinder

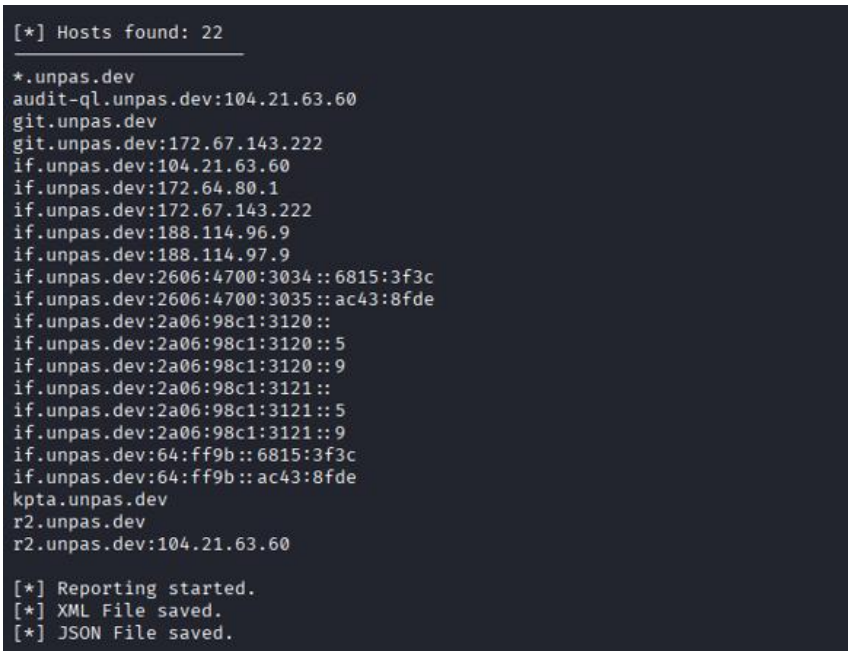
Gambar 5.6 menunjukkan hasil enumerasi pasif menggunakan Subfinder yang berhasil mengidentifikasi 5 subdomain dalam waktu kurang dari 11 detik. Subdomain yang ditemukan meliputi if.unpas.dev, git.unpas.dev, r2.unpas.dev, kpta.unpas.dev, dan audit-ql.unpas.dev. Temuan ini memperluas daftar kandidat subdomain yang sebelumnya hanya diketahui dari crt.sh.

4. OSINT *Gatheing* - theHarvester

Pengumpulan informasi *open-source intelligence* dilakukan menggunakan theHarvester yang menggabungkan berbagai sumber daring secara otomatis.



Gambar 5. 7 Hasil OSINT theHarvester – IP dan URL

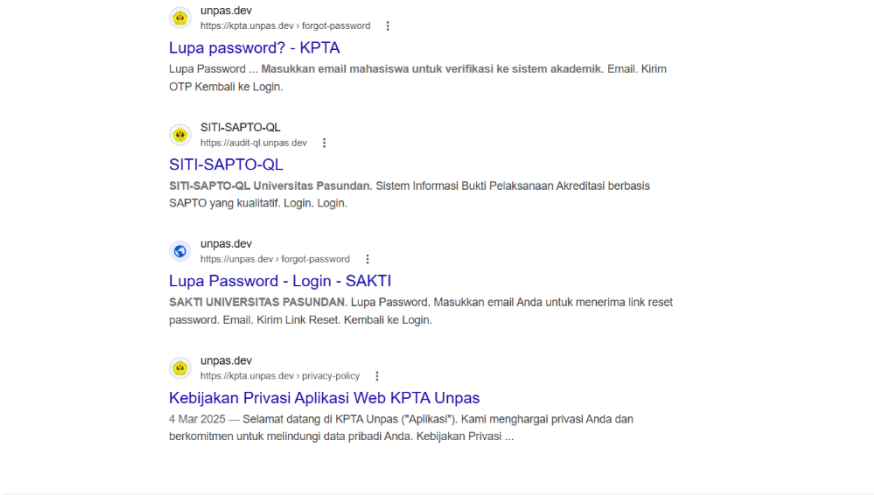


Gambar 5. 8 Hasil OSINT theHarvester - Daftar Host

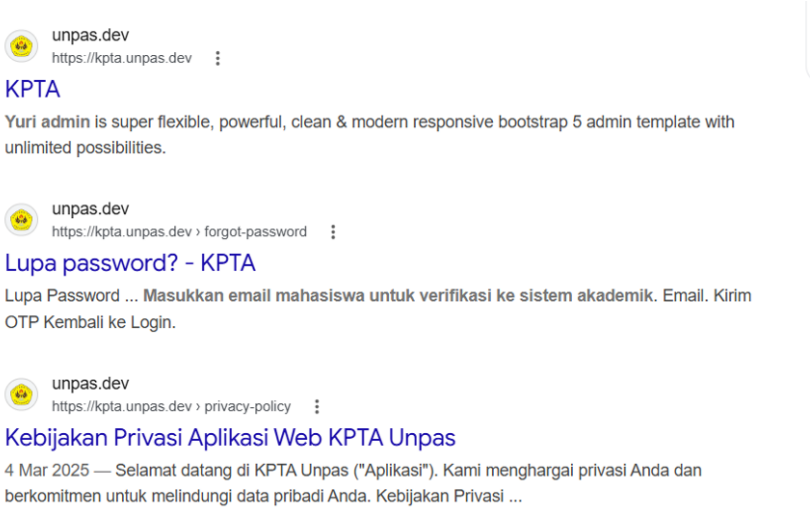
Gambar 5.7 dan 5.8 menunjukkan hasil theHarvester yang mengonfirmasi seluruh subdomain yang ditemukan sebelumnya oleh Subfinder, dengan tambahan informasi berupa pemetaan masing-masing subdomain. Seluruh IP yang ditemukan merupakan alamat milik *Cloudflare* (ASN AS13335), yang memperkuat konfirmasi bahwa seluruh infrastruktur domain unpas.dev berada di balik layanan *Cloudflare*. URL *https://unpas.dev/login* juga teridentifikasi sebagai URL publik yang dapat diindeks.

5. *Google Dorking*

Pencarian menggunakan operator *Google dork* dilakukan untuk mengidentifikasi halaman, subdomain, dan file yang terindeks oleh mesin pencari, serta memeriksa apakah terdapat file sensitif yang dapat diakses publik.



Gambar 5. 9 Hasil *Google Dork* site:unpas.dev



Gambar 5. 10 Hasil *Google Dork* site:kpta.unpas.dev

Berdasarkan Gambar 5.9 dan 5.10, *Google dorking* mengungkap subdomain baru yang tidak ditemukan oleh tools sebelumnya, yaitu monev-pbm,unpas.dev dengan judul “monev PBM” dan audit-ql.unpas.dev dengan judul “SITI-SAPTO-QL” (sistem informasi Bukti Pelaksanaan Akreditasi Berbasis SAPTO). Kedua subdomain ini dicatat sebagai informasi pendukung karena berada di luar lingkup pengujian. Pencarian dengan operator intitle:”index of” dan *filetype:pdf OR filetype:sql OR filetype:env* tidak menghasilkan temuan, mengindikasikan tidak ada file sensitif atau halaman *directory listing* yang terindeks oleh Google.

6. *Verifikasi Liveness* DNS Resolution Aktif

Untuk memastikan subdomain yang teridentifikasi benar benar aktif merespons, dilakukan verifikasi dengan DNS *resolution* aktif. Proses ini khususnya dilakukan terhadap kpta.unpas.dev yang teridentifikasi sebagai subdomain layanan KPTA yang secara eksplisit disebutkan dalam ruang lingkup pengujian.

Gambar 5. 11 Hasil Verifikasi DNS Resolution kpta.unpas.dev

Gambar 5.11 mengonfirmasi bahwa kpta.unpas.dev me-*resolve* ke alamat IP yang sama dengan domain utama unpas.dev (104.21.63.60 dan 172.67.143.222), yang berarti kedua host berbagi infrastruktur Cloudflare yang sama namun beroperasi sebagai entitas terpisah dengan kemungkinan konfigurasi server yang berbeda. Berasarkan verifikasi ini, kpta.unpas.dev ditetapkan sebagai host kedua yang masuk dalam ruang lingkup pengujian *Vulnerability Analysis.*

Tabel 5. 1 Hasil Identifikasi Domain dan Subdomain

No	Item	Hasil	Teknik	Status Lingkup
1	Domain Utama	unpas.dev	DNS lookup	Dalam lingkup
2	A Record	104.21.63.60, 172.67.143.222	DNS lookup	*IP edge Cloudflare*, bukan IP origin server asli
3	AAAA Record	2606:4700:3035::ac43:8fde, 2606:4700:3034::6815:3f3c	DNS lookup	*IP edge Cloudflare* (IPv6)
4	NS Record	amber.ns.cloudflare.com, thomas.ns.cloudflare.com	DNS lookup	DNS dikelola melalui layanan *Cloudflare*
5	MX Record	Tidak ditemukan (ANSWER:0)	DNS lookup	Tidak ada mail server aktif teridentifikasi
6	TXT Record	google-site-verification=On_x0kZ1f...	DNS lookup	Bukti verifikasi domain di *Google Search Console*

No	Item	Hasil	Teknik	Status Lingkup
7	Wildcard certificate	*.unpas.dev	crt.sh (CT log pasif)	Indikasi subdomain lain mungkin tidak tercatat di CT log
8	r2.unpas.dev	Teridentifikasi – http 404 (live)	Crt.sh, subfinder	Di luar lingkup (info pendukung)
9	git.unpas.dev	Teridentifikasi *resolve* ke 172.67.143.222	Subfinder, theHarvest	Di luar lingkup (info pendukung)
10	If.unpas.dev	Teridentifikasi multi-IP Cloudflare	Subfinder, theHarvest	Di luar lingkup (info pendukung)
11	audit-ql.unpas.dev	Teridentifikasi "SITI-SAPTO_QL" (sistem akreditasi)	Subfinder, Google dork	Di luar lingkup (info pendukung)
12	monev-pbm.unpas.dev	Teridentifikasi "monev PBM"	Google Dork (site:unpas.dev)	Di luar lingkup (info pendukung)
13	Kpta.unpas.dev	Terverifikasi aktif, resolve ke 104.21.63.60, 172.67.143.222	DNS lookup	Dalam lingkup

5.1.2 Hasil Pemindaian Port dan Layanan

Pemindaian port dilakukan untuk mengidentifikasi port yang terbuka dan layanan yang aktif pada kedua host dalam ruang lingkup pengujian.

1. Nmap (unpas.dev)

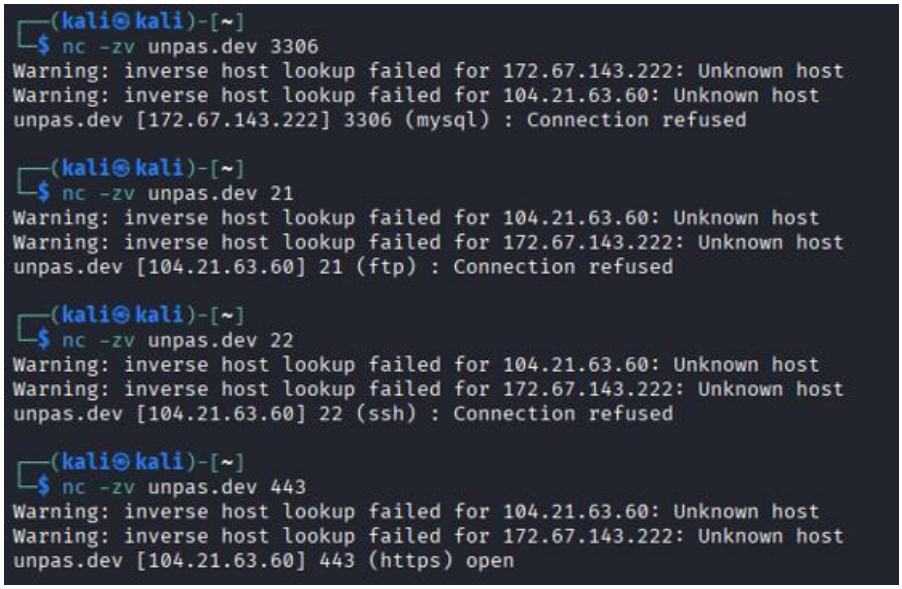
```
└─$ nmap -sV -T4 unpas.dev -oN log_nmap_basic.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-20 22:43 -0400
Nmap scan report for unpas.dev (172.67.143.222)
Host is up (0.0091s latency).
Other addresses for unpas.dev (not scanned): 104.21.63.60 2606:4700:3035::ac4
3:8fde 2606:4700:3034::6815:3f3c
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.39 seconds
```

Gambar 5. 12 Hasil Nmap unpas.dev

Gambar 5.12 menunjukkan hasil pemindaian Nmap terhadap unpas.dev. Ditemukan 4 port dalam status open yaitu port 80 (HTTP), 443 (HTTPS), 8080 (HTTP), dan 8443 (HTTPS), seluruhnya terdeteksi sebagai "Cloudflare http proxy". Sebanyak 996 port lainnya berstatus *filtered* (tidak merespons) yang mengindikasikan mekanisme *firewall* atau *WAF Cloudflare* yang secara aktif menyaring lalu lintas jaringan.

2. Netcat

Netcat digunakan untuk memverifikasi terhadap port-port sensitif yang memiliki riwayat insiden keamanan.



Gambar 5. 13 Hasil Verifikasi Port Spesifik via Netcat

Gambar 5.13 mengonfirmasi bahwa port 3306 (MySQL), 21 (FTP), dan 22 (SSH) tidak dapat diakses dari jaringan publik (*Connection refused*). Hasil ini merupakan perbaikan signifikan dibandingkan kondisi sebelumnya disebutkan dalam latar belakang penelitian, dimana port 3306 pernah terbuka ke publik dan menjadi salah satu penyebab insiden keamanan. Port 44 terkonfirmasi open sesuai hasil Nmap sebelumnya.

Tabel 5. 2 Hasil Pemindaian Port dan Layanan

No	Port	Status	Layanan Terdeteksi	Keterangan
1	80/tcp	*Open*	*Cloudflare http proxy*	Melakukan *redirect* ke HTTPS (302)
2	443/tcp	*Open*	*Cloudflare http proxy*	HTTPS aktif
3	8080/tcp	*Open*	*Cloudflare http proxy*	Tidak ada layanan origin yang nyata
4	8443/tcp	*Open*	*Cloudflare http proxy*	DNS dikelola melalui layanan *Cloudflare*
5	3306/tcp	*Closed (refused)*	MySql	Tidak dapat diakses
6	21/tcp	*Closed (refused)*	FTP	Tidak dapat diakses
7	22/tcp	*Closed (refused)*	SSH	Tidak dapat diakses
8	996 port lain	*Filtered*	-	Paket di drop yang mengindikasikan *WAF/firewall Cloudflare* aktif

5.1.3 Identifikasi Layanan Aktif

Identifikasi layanan aktif dilakukan menggunakan Nmap *service detection* dan curl untuk memperoleh informasi banner dan respons HTTP dari kedua host.

1. ***Nmap Service Detection***

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC unpas.dev -oN log_nmap_service.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-20 22:49 -0400
Nmap scan report for unpas.dev (104.21.63.60)
Host is up (0.011s latency).
Other addresses for unpas.dev (not scanned): 172.67.143.222 2606:4700:3035::a
c43:8fde 2606:4700:3034::6815:3f3c
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
53/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped
8443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.84 seconds
```

Gambar 5. 14 Hasil Nmap *Service Detection* unpas.dev

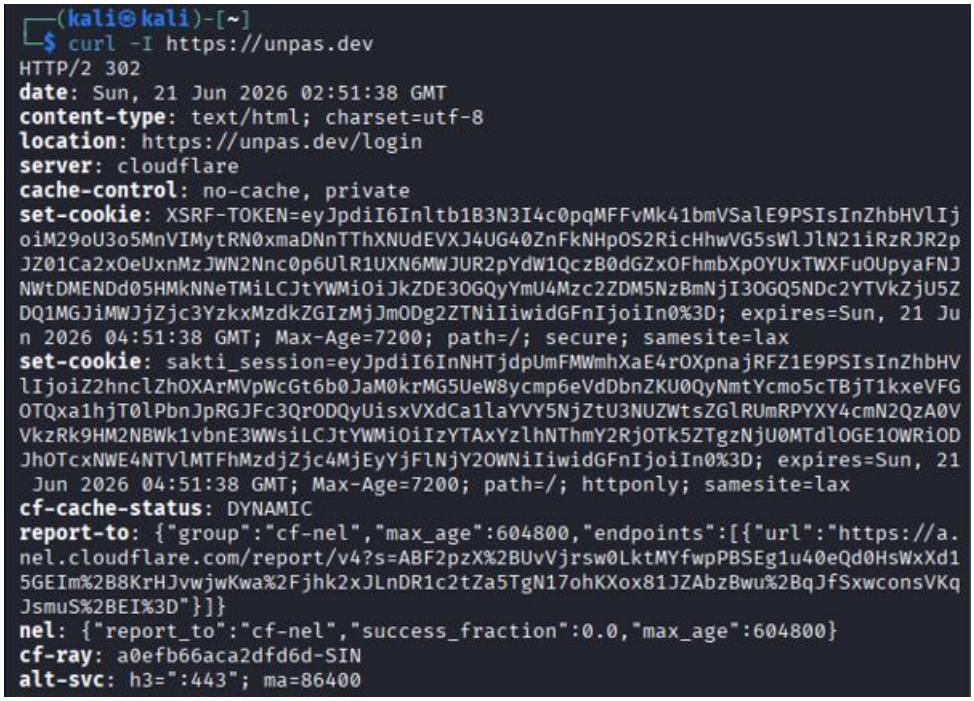
Gambar 5.14 menunjukkan bahwa seluruh port yang terbuka terdeteksi sebagai "tcpwrapped", *Cloudflare* memutus koneksi sebelum Nmap sempat memperoleh banner layanan origin asli. Kondisi ini merupakan bentuk perlindungan *information disclosure* pada lapisan infrastruktur yang diterapkan oleh *Cloudflare*.

2. **Curl - Pemeriksaan Respons *Header HTTP***

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://unpas.dev
HTTP/1.1 302 Found
Date: Sun, 21 Jun 2026 02:51:16 GMT
Content-Type: text/html
Connection: keep-alive
Server: cloudflare
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Location: https://unpas.dev/
Cf-Cache-Status: DYNAMIC
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.
nel.cloudflare.com/report/v4?s=%2BGqYyimvE3gl9D0PWaxMcBtYkOOEcfjiGTGq86rcq9%2
BcbPUVF5vTiKXkYp0%2BzKdM7OVfHbJ1Y%2BQyuEnNNcN7ADVmkGMnnNci5qmYqWoeN%2Fnwta7lB
G7dOyILhkA%3D"}]}
CF-RAY: a0efb5e2abb83d86-SIN
alt-svc: h3=":443"; ma=86400
```

Gambar 5. 15 Hasil curl HTTP unpas.dev

Gambar 5.15 menunjukkan bahwa permintaan HTTP pada port 80 secara otomatis diarahkan (*redirect* 302) ke HTTPS, membuktikan penerapan *HTTPS enforcement* pada domain ini.



Gambar 5. 16 Hasil Curl HTTPS unpas.dev

Gambar 5.16 menampilkan respons header HTTPS dari unpas.dev. Beberapa hal yang dapat diamati:

a. Redirect ke /login mengindikasikan seluruh akses diarahkan ke halaman autentikasi
b. Dua *cookie* ditemukan yaitu XSRF-TOKEN dan sakti_session, penamaan sakti_session mengindikasikan nama aplikasi, sedangkan XSRF-TOKEN mengindikasikan penggunaan *framework* Laravel.
c. Cookie sakti_session memiliki atribut httponly dan samesite=lax namun tidak memiliki atribut secure, ini merupakan indikasi awal yang akan divalidasi lebih lanjut pada tahap *Vulnerability Analysis*

Tabel 5. 3 Hasil Identifikasi Layanan Aktif

No	Pemeriksaan	Hasil	Keterangan
1	Nmap service detection	Seluruh port tcpwrapped	Cloudflare memblokir *banner grabbing* otomatis
2	Curl HTTP (port 80)	HTTP 302, redirect ke HTTPS	HTTPS *enforcement* aktif
3	Curl HTTPS (port 443)	HTTP 302, redirect ke /login, server: *cloudflare*	Header asli server tersembunyi
4	Cookie sakti_session	http only, samesite=lax, dan tidak memiliki atribut secure	Indikasi awal konfigurasi cookie belum lengkap
5	Cookie XSRF-TOKEN	Ditemukan	Indikasi penggunaan Laravel (CSRF *protection*)

5.1.4 Identifikasi Teknologi Web

Identifikasi teknologi web dilakukan menggunakan WhatWeb terhadap kedua host untuk memperoleh informasi *fingerprint* teknologi yang digunakan.

1. **WhatWeb - unpas.dev**

```
WhatWeb report for https://unpas.dev/login
Status    : 200 OK
Title     : Login - SAKTI
IP        : 104.21.63.60
Country   : UNITED STATES, US

Summary   : Bootstrap, Cookies[XSRF-TOKEN,sakti_session], HTML5, HTTPServer[c
loudflare], HttpOnly[sakti_session], PasswordField[password], Script, Uncommo
nHeaders[nel,cf-cache-status,report-to,cf-ray,alt-svc]
```

Gambar 5. 17 Hasil WhatWeb unpas.dev

Gambar 5.17 menampilkan hasil identifikasi teknologi WhatWeb pad unpas.dev. Aplikasi teridentifikasi dengan nama SAKTI (berdasarkan judul halaman "Login – SAKTI"), menggunakan *framework* Bootstrap, dan web server yang hanya menampilkan *cloudflare* pada *header* server sehingga versi web server dan sistem operasi origin tidak dapat diidentifikasi melalui teknik ini.

2. **WhatWeb (kpta.unpas.dev)**

```
└─$ whatweb -v https://kpta.unpas.dev
WhatWeb report for https://kpta.unpas.dev
Status    : 200 OK
Title     : KPTA
IP        : 172.67.143.222
Country   : RESERVED, ZZ

Summary   : Bootstrap, Cookies[XSRF-TOKEN,kpta_session], HTML5, HTTPServer[cl
oudflare], HttpOnly[kpta_session], JQuery, Meta-Author[pixelstrap], PasswordF
ield[password], Script, UncommonHeaders[report-to,cf-cache-status,nel,cf-ray,
alt-svc], X-UA-Compatible[IE=edge]
```

Gambar 5. 18 Hasil WhatWeb kpta.unpas.dev

Gambar 5.18 menampilkan hasil identifikasi teknologi pada kpta.unpas.dev. berbeda dari unpas.dev, pada host ini terdeteksi beberapa informasi tambahan yaitu *meta author pixelstrap, library jQuery* terdeteksi, dan *cookie* sesi menggunakan nama kpta_session. Seperti pada unpas.dev, *header* server hanya menampilkan *cloudflare*.

Tabel 5. 4 Hasil Identifikasi Teknologi Web

No	Item	Unpas.dev	Kpta.unpas.dev
1	Nama Aplikasi	SAKTI	KPTA
2	Indikasi *Framework Backend*	Laravel (*cookie* XSRF-TOKEN, sakti_session)	Laravel (*cookie* XSRF-TOKEN, kpta_session)
3	*Framework Frontend*	Bootstrap	Bootstrap
4	Library JS	-	jQuery
5	*Header server*	*Cloudflare*	*Cloudflare*
6	Versi asli Server/OS	Tidak terekspos	Tidak terekspos

No	Item	Unpas.dev	Kpta.unpas.dev
7	Integrasi Oauth	Google Oauth (/oauth/google)	Google Oauth (/oauth/google)
8	*Cookie httpOnly*	kpta_session	kpta_session
9	*Cookie secure*	Tidak ada	Tidak ada

5.2 Hasil *Threat Modeling*

Tahap *Threat Modeling* dilaksanakan setelah seluruh informasi awal berhasil dikumpulkan pada tahap *Intelligence Gathering*. Tujuan dari tahap ini adalah memetakan potensi ancaman yang dapat terjadi terhadap konfigurasi server dan layanan domain unpas.dev berdasarkan informasi yang diperoleh, kemudian mengelompokkannya sesuai kategori *Security Misconfiguration* untuk dijadikan acuan urutan prioritas pengujian pada tahap Vulnerability Analysis.

Pemetaan ancaman dilakukan secara kualitatif dengan mempertimbangkan dua acuan utama. Pertama, klasifikasi 7 jenis Security Misconfiguration sesuai dengan subbab 2.5.1. Kedua, estimasi tingkat keparahan awal berdasarkan karakteristik umum metrik CVSS v4.0 yaitu mempertimbangkan kemungkinan *Attack Vector, Attack Complexity, privilege, required*, serta potensi dampak terhadap aspek *confidentiality, integrity, dan availability*. Estimasi ini bersifat kualitatif dan belum merupakan penilaian CVSS final, perhitungan CVSS resmi dilakukan setelah temuan diverifikasi pada tahap *Vulnerability Analysis.*

5.2.1 Identifikasi Potensi Ancaman

Berdasarkan seluruh indikasi yang diperoleh pada tahap *Intelligence Gathering*, diidentifikasi sejumlah potensi ancaman terhadap konfigurasi server dan layanan pada kedua host dalam ruang lingkup pengujian. Hasil identifikasi dan pengelompokkan potensi ancaman tersebut disajikan pada Tabel 5.5 berikut.

Tabel 5. 5 Peta Ancaman Berdasarkan Hasil *Intelligence Gathering*

No	Indikasi temuan dari intelligence gathering	Kategori *Security Misconfiguration* (ref. 2.5.1)	Estimasi *Severity*	Prioritas
1	Respons HTTP tidak menampilkan *security header* apapun, dikonfirmasi dari hasil curl -I pada kedua host	HTTP *security headers* tidak diterapkan	*Low-medium*	Sedang
2	Aplikasi berbasis Laravel (cookie XSRF-TOKEN, sakti_session/kpta_session) berpotensi menampilkan *stack trace* atau konfigurasi sensitif jika mode debug aktif di lingkungan produksi	Pesan *error/debugging* terlalu informatif	*Medium-high*	Tinggi
3	Belum diverifikasi apakah direktori pada web server dapat ditelusuri publik	*Directory listing* aktif	*Low-medium*	sedang

No	Indikasi temuan dari intelligence gathering	Kategori *Security Misconfiguration* (ref. 2.5.1)	Estimasi *Severity*	Prioritas
4	Belum diverifikasi keberadaan halaman bawaan, file contoh, atau konfigurasi default yang masih aktif.	Penggunaan konfigurasi default	*Medium-critical*	Tinggi
5	Belum di verifikasi versi TSL dan *cipher suite* yang didukung. Namun, *cookie* sesi (sakti_session, kpta_session) tidak memiliki atribut secure	SSL/TLS kurang aman	*medium*	Sedang
6	Header server hanya menampilkan "cloudflare".Namun, versi asli web server dan sistem operasi tidak terekspos pada pemeriksaan awal	Informasi versi layanan terekspos	*None - low*	Rendah
7	Port 8080 dan 8443 terbuka selain 80/443, fungsi dan layanan yang dijalankan pada port tersebut belum diverifikasi	Port/layanan tidak diperlukan terbuka ke publik	*Low-medium*	sedang
8	Port 3306 (MySQL), 21 (FTP), 22 (SSH) dikonfirmasi tertutup dari publik	Kondisi positif	*none*	Temuan positif, tidak dilanjutkan ke VA
9	Kpta.unpas.dev merupakan host terpisah dengan potensi konfigurasi yang berbeda dari unpas.dev	Perlu di uji terpisah berdasarkan kategori yang sudah ditetapkan	-	TC-01 s.d TC-07 digunakan untuk kedua host

Tabel 5.5 menunjukkan bahwa dari 9 indikasi yang berhasil dipetakan, terdapat 2 ancaman dengan prioritas tinggi, 4 ancaman prioritas sedang, dan 1 ancaman dengan prioritas rendah. Satu indikasi (baris 8) merupakan temuan positif yang menunjukkan kondisi keamanan yang sudah baik sehingga tidak perlu dilanjutkan ke tahap *Vulnerability Analysis*. Satu baris terakhir (baris 9) bukan ancaman tersendiri, melainkan catatan cakupan yang menetapkan bahwa seluruh parameter diuji pada kedua host secara terpisah.

Prioritas tinggi pada jenis 4 (pesan *error* informatif) didasarkan pada estimasi karakteristik CVSS yang berpotensi menghasilkan *Attack Complexity:low* dan *privileges Required:none*, artinya jika mode debug Laravel benar-benar aktif, siapapun dari internet dapat memicu pesan error yang informatif tanpa memerlukan autentikasi atau kondisi khusus apapun. Prioritas tinggi pada konfigurasi default didasarkan pada rentang dampak yang sangat lebar dari sekedar informasi teknis (*low*) hingga potensi akses tidak sah melalui konfigurasi bawaan yang belum diubah (*critical*).

5.2.2 Urutan Prioritas Pengujian

Berdasarkan peta ancaman pada Tabel 5.5, disusun urutan prioritas pengujian untuk tahap *Vulnerability Analysis* sebagaima ditampilkan pada Tabel 5.6. Urutan ini memastikan bahwa parameter dengan potensi dampak tertinggi diuji terlebih dahulu.

Tabel 5. 6 Urutan Prioritas Pengujian *Vulnerability Analysis*

No	Kode	Parameter	Prioritas	Dasar Penetapan Prioritas
1	TC-02	Konfigurasi default	Tinggi	Rentang dampak lebar *(low-critical*), perlu diverifikasi aktif karena *Google Index* bersih tidak berarti file ada
2	TC-04	Pesan Error Informatif	Tinggi	Potensi *Attack Complexity:low, PR:None*, dampak langsung pada *confidentiality* jika debug aktif
3	TC-05	HTTP *Security Headers*	Sedang	Suda ada indikasi kuat dari hasil curl (tidak ada header keamanan terdeteksi)
4	TC-06	Konfigurasi SSL/TLS	Sedang	*Cookie* tanpa *secure* sudah teridentifikasi, namun versi TLS belum diverifikasi
5	TC-03	*Directory listing*	Sedang	Belum diverifikasi
6	TC-01	Port dan layanan terbuka	Sedang	Port 8080/8443 terbuka tapi belum diketahui layanannya
7	TC-07	Informasi versi layanan	Rendah	*Cloudflare* sudah menyembunyikan banner secara default

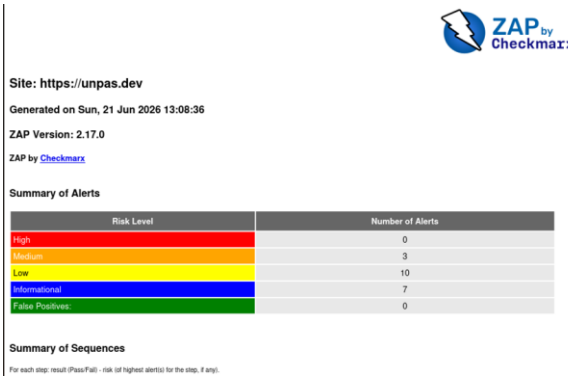
Tabel 5.6 ini menjadi acuan urutan pelaksanaan *Vulnerability Analysis* pada pada subbab berikutnya.

5.3 Hasil *Vulnerability Analysis*

Tahap *Vulnerability Analysis* dilaksanakan terhadap dua host dalam ruang lingkup pengujian sesuai urutan prioritas yang ditetapkan pada tabel 5.6. Pengujian menggunakan kombinasi tools sesuai Tabel 4.6, OWASP ZAP dijalankan terlebih dahulu sebagai *broad scan* awal, kemudian hasilnya divalidasi secara manual menggunakan curl, dirsearch, testssl.sh, dan Nmap per masing-masing TC. Hasil pada tahap ini masih berupa indikasi yang akan dikonfirmasi melalui verifikasi manual pada tahap yang sama.

5.3.1 OWASP ZAP - Baseline Scan

Sebelum pengujian per TC, OWASP ZAP Baseline Scan dijalankan terhadap kedua host menggunakan mode *spider* + *passive scan* (non-destruktif, tanpa *active scan*). Hasil *alerts* ZAP digunakan sebagai peta awal indikasi yang kemudian diverifikasi secara manual.



ZAP by Checkmarx ZAP Scanning Report

Site: https://unpas.dev

Generated on Sun, 21 Jun 2026 13:08:36

ZAP Version: 2.17.0

ZAP by Checkmarx

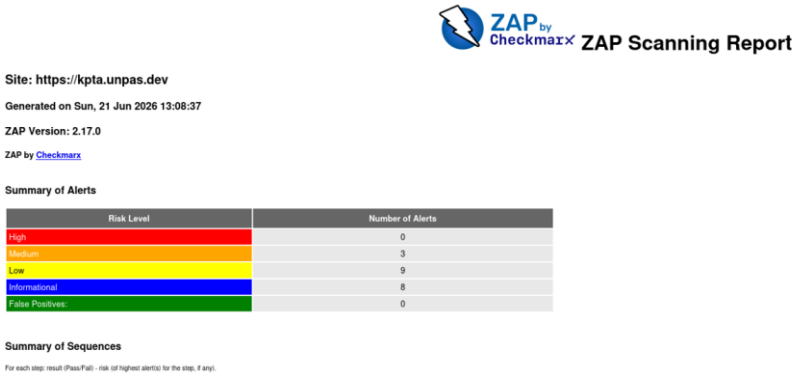
Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	10
Informational	7
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Gambar 5. 19 Ringkasan *Alert* OWASP ZAP unpas.dev



ZAP by Checkmarx ZAP Scanning Report

Site: https://kpta.unpas.dev

Generated on Sun, 21 Jun 2026 13:08:37

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	9
Informational	8
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Gambar 5. 20 Ringkasan *Alert* OWASP ZAP kpta.unpas.dev

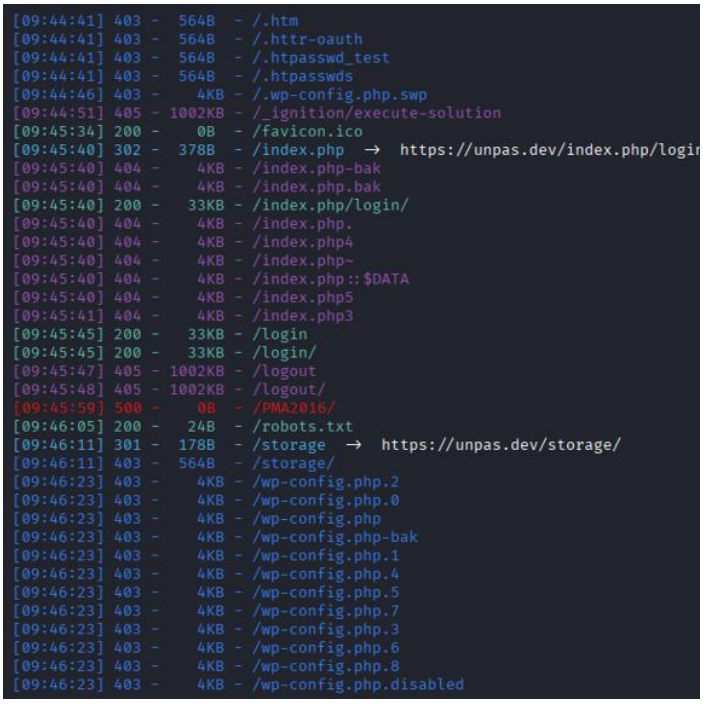
Gambar 5.19 dan 5.20 menampilkan ringkasan hasil *baseline scan* OWAP ZAP. Tidak ditemukan *alert* dengan tingkat risiko *HIGH* pada kedua host. Masing-masing host menghasilkan 3 *alert* tingkat *Medium* dan sejumlah *alert* tingkat *low* serta *informational*. Hasil *alert* ini selanjutnya dipetakan ke masing-masing TC sebagai bahan validasi silang dengan hasil pengujian manual.

5.3.2 TC-02 Konfigurasi Default

Pengujian TC-02 bertujuan untuk memeriksa apakah terdapat halaman default, file contoh, atau konfigurasi bawaan yang masih aktif dan dapat diakses dari sisi publik.

1. Dirsearch - Pemindaian File dan Konfigurasi Bawaan

Dirsearch dijalankan dengan ekstensi target yang mencakup file-file berpotensi sensitif (.php, .env, .sql, .git, .zip,.bak)



```
[09:44:41] 403 -  564B  - /.htm
[09:44:41] 403 -  564B  - /.httr-oauth
[09:44:41] 403 -  564B  - /.htpasswd_test
[09:44:41] 403 -  564B  - /.htpasswds
[09:44:46] 403 -    4KB - /.wp-config.php.swp
[09:44:51] 405 - 1002KB - /_ignition/execute-solution
[09:45:34] 200 -    0B  - /favicon.ico
[09:45:40] 302 -  378B  - /index.php  →  https://unpas.dev/index.php/logi
[09:45:40] 404 -    4KB - /index.php-bak
[09:45:40] 404 -    4KB - /index.php.bak
[09:45:40] 200 -   33KB - /index.php/login/
[09:45:40] 404 -    4KB - /index.php.
[09:45:40] 404 -    4KB - /index.php4
[09:45:40] 404 -    4KB - /index.php~
[09:45:40] 404 -    4KB - /index.php::$DATA
[09:45:40] 404 -    4KB - /index.php5
[09:45:41] 404 -    4KB - /index.php3
[09:45:45] 200 -   33KB - /login
[09:45:45] 200 -   33KB - /login/
[09:45:47] 405 - 1002KB - /logout
[09:45:48] 405 - 1002KB - /logout/
[09:45:59] 500 -    0B  - /PMA2016/
[09:46:05] 200 -   24B  - /robots.txt
[09:46:11] 301 -  178B  - /storage  →  https://unpas.dev/storage/
[09:46:11] 403 -  564B  - /storage/
[09:46:23] 403 -    4KB - /wp-config.php.2
[09:46:23] 403 -    4KB - /wp-config.php.0
[09:46:23] 403 -    4KB - /wp-config.php
[09:46:23] 403 -    4KB - /wp-config.php-bak
[09:46:23] 403 -    4KB - /wp-config.php.1
[09:46:23] 403 -    4KB - /wp-config.php.4
[09:46:23] 403 -    4KB - /wp-config.php.5
[09:46:23] 403 -    4KB - /wp-config.php.7
[09:46:23] 403 -    4KB - /wp-config.php.3
[09:46:23] 403 -    4KB - /wp-config.php.6
[09:46:23] 403 -    4KB - /wp-config.php.8
[09:46:23] 403 -    4KB - /wp-config.php.disabled
```

Gambar 5. 21 Hasil Dirsearch unpas.dev

Gambar 2.21 menampilkan hasil pemindaian dirsearch pada unpas.dev. dari seluruh path yang diperiksa, beberapa hasil penting yang perlu dicatat adalah sebagai berikut.

a. Seluruh varian file wp-config.php meresppons HTTP 403 terlindung dengan baik.
b. Direktori storage/ merespons 301 dan kemudian 403 tidak dapat ditelusuri publik
c. Path /PMA2016/ merespons HTTP 500 dengan ukuran 0 byte yang mengindikasikan *routing erros*, tidak menampilkan informasi sensitif dan dicatat sebagai anomali pendukung.
d. Dau endpoint /_ignition/execute-solution dan /logout merespons HTTP 405 dengan ukuran 1.002 KB, itu merupakan ukuran yang sangat tidak wajar untuk respons *Method Not Allowed* yang normalnya hanya beberapa KB. Temuan ini relevan dengan parameter TC-04 (Pesan *Error* Informatif) dan akan dibahas lebih lanjut pada subbab berikutnya.

```
└─$ dirsearch -u https://kpta.unpas.dev -e php,html,json,env,sql,git,zip,bak
-t 25 -o dirsearch_kpta.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
 pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/lat
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

                             v0.4.3
 (_|| | _) (/_(_|| (_| )

Extensions: php, html, json, env, sql, git, zip, bak | HTTP method: GET
Threads: 25 | Wordlist size: 13032

Output File: dirsearch_kpta.txt

Target: https://kpta.unpas.dev/

[09:46:55] Starting:
[09:47:01] 200 -  740B  - /.htaccess
[09:47:05] 403 -    4KB - /.wp-config.php.swp
[09:47:12] 200 -    5KB - /admin
[09:47:12] 200 -    5KB - /admin/
[09:47:13] 302 -  334B  - /admin/home  →  https://kpta.unpas.dev
[09:47:14] 405 -  252KB - /admin/login
[09:47:26] 403 -  548B  - /assets/
[09:47:26] 301 -  162B  - /assets  →  http://kpta.unpas.dev/assets/
[09:47:35] 500 -    6KB - /custom.zip
[09:47:35] 200 -    5KB - /dashboard
[09:47:36] 200 -    5KB - /dashboard/
[09:47:41] 200 -   67KB - /favicon.ico
[09:47:48] 200 -    6KB - /index.php
[09:48:14] 200 -   24B  - /robots.txt
[09:48:36] 403 -    4KB - /wp-config.php
[09:48:36] 403 -    4KB - /wp-config.php.0
[09:48:36] 403 -    4KB - /wp-config.php.9
```

Gambar 5. 22 Hasil Dirsearch kpta.unpas.dev

Gambar 5.22 menampilkan hasil dirsearch pada kpta.unpas.dev. Temuan yang perlu dicatat bahwa:

1. .htaccess merespons HTTP 200 dengan ukuran 740 byte, file ini dapat diakses secara publik, padahal seharusnya tidak.
2. /admin dan /dashboard merespons HTTP 200 kemungkinan halaman login panel admin, bukan direktory listing.

3. custom.zip merespons HTTP 500, ini anomali yang dicatat sebagai informasi pendukung.
4. Seluruh varian wp-config.php merespons HTTP 403 yang berarti terlindungi dengan baik.

Tabel 5. 7 Ringkasan Hasil Pemeriksaan TC-02

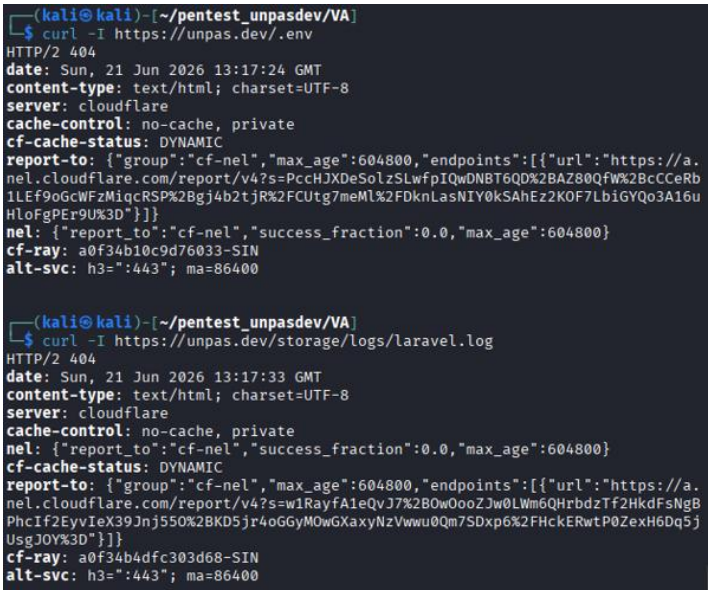
No	Path/Item	Host	Status HTTP	keterangan
1	.htaccess	unpas.dev	403	Terlindungi
2	.htaccess	Kpta.unpas.dev	200	Terbuka
3	Wp-config.php (semua)	keduanya	403	terlindungi
4	.env	keduanya	404	Tidak ditemukan
5	phpinfo.php, info.php	keduanya	404	Tidak ditemukan
6	.git/config	keduanya	404	Tidak ditemukan
7	Composer.json, package.json	keduanya	404	Tidak ditemukan
8	Install.php	keduanya	404	Tidak ditemukan
9	Storage/	unpas.dev	301, 403	Terlindungi
10	PMA2016	unpas.dev	500, 0 B	Anomali
11	custom.zip	Kpta.unpas.dev	500	Anomali
12	/_ignition/execute-solution	unpas.dev	405, 1.002 KB	Indikasi kuat
13	/logout	unpas.dev	405, 1.002 KB	Indikasi kuat

5.3.3 TC-04 Pesan Error Informatif

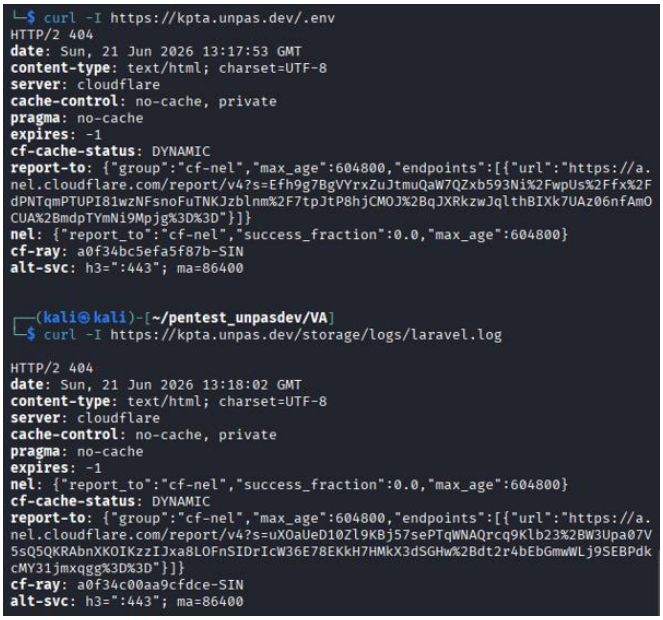
Pengujian TC-04 bertujuan untuk memeriksa apakah sistem menampilkan informasi teknis yang berlebihan melalu pesan error, termasuk *stack trace*, versi layanan, *path directory*, atau konfigurasi internal.

1. Curl - Pemeriksaan File Sensitif

Pemeriksaan dilakukan terhadap file-file yang umum berpotensi membocorkan informasi teknis jika dilindungi dengan benar.



Gambar 5. 23 Hasil Dirsearch unpas.dev

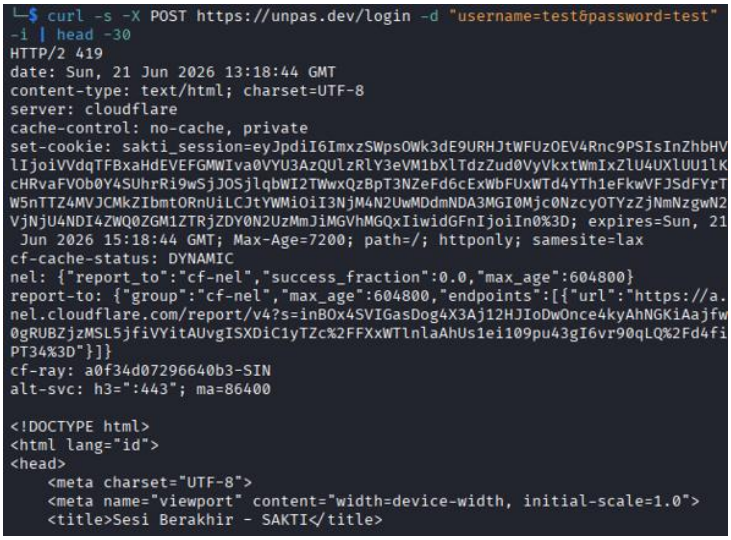


Gambar 5. 24 Hasil Pemeriksaan File Sensitif kpta.unpas.dev via curl

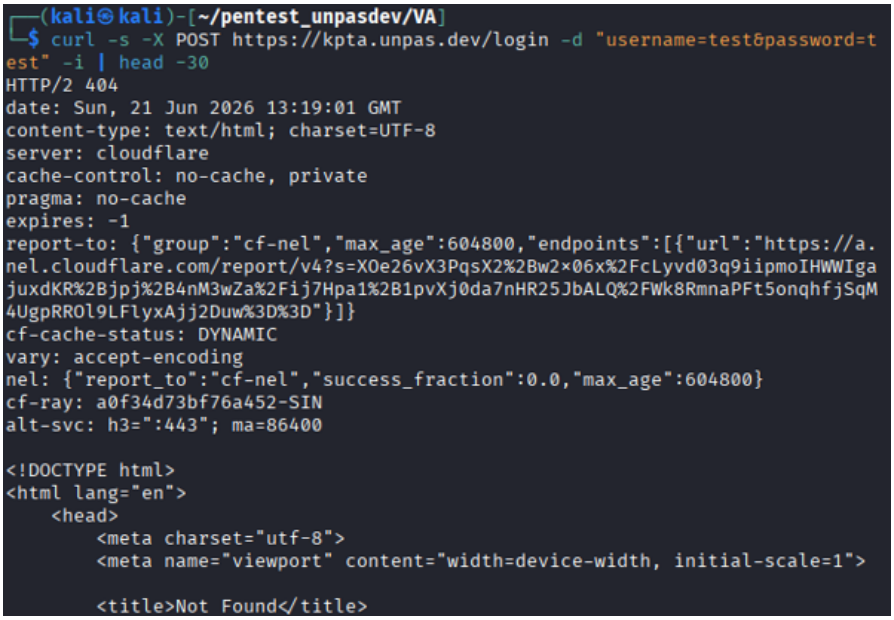
Gambar 5.23 dan 5.24 menunjukkan bahwa file .env dan storage/logs/laravel.log pada kedua host merespons dengan HTTP 404 yang berarti tidak dapat diakses dari sisi publik, kondisi ini merupakan hasil yang positif untuk parameter ini.

2. Curl - Pengujian Respons Error Form Login

Pengujian dilakukan dengan mengirimkan permintaan POST ke halaman login tanpa menyertakan SCRF token yang valid, untuk mengamati bagaimana sistem merespons kondisi error.



Gambar 5. 25 Hasil Pengujian Respons Error Form Login unpas.dev



Gambar 5. 26 Hasil Pengujian Respons Error Form Login kpta.unpas.dev

Gambar 5.23 menunjukkan bahwa unpas.dev merespons POST tanpa CSRF token dengan HTTP 419 (CSRF token *mismatch*) dan menampilkan halaman "sesi berakhir – SAKTI" tanpa menyertakan informasi teknis apapun. Ini menandakan perlindungan CSRF aktif dan berfungsi dengan baik. Pada Gambar 5.24, kpta.unpas.dev merespons HTTP 404 karena route loginnya berbeda (mahasiswa/login, bukan login)

3. Dirsearch - Pemindaian Direktori dan Endpoin

Berdasarkan hasil pemindaian dirsearch yang telah dilaksanakan pada TC-02 (gambar 5.21) ditemukan dua endpoint pada unpas.dev yang memberikan respons tidak wajar yaitu /_ignition/execute-solution dan /logout. Keduanya merespons HTTP 405 (method not allowed) dengan ukuran respons 1.002 KB, jauh melampaui ukuran normal respon 405 yang seharusnya hanya beberapa KB. Indikasi ini selanjutnya divalidasi pada tahap *vulnerability analysis*.

Tabel 5. 8 Ringkasan Hasil Pemeriksaan TC-04

No	Pengujian	Host	Hasil	Status
1	File .env	unpas.dev	HTTP 404	Tidak terekspos
2	File .env	Kpta.unpas.dev	HTTP 404	Tidak terekspos
3	Storage/logs/laravel.log	unpas.dev	HTTP 404	Tidak terekspos
4	Storage/logs/Laravel.log	Kpta.unpas.dev	HTTP 404	Tidak terekspos
5	POST tanpa CSRF token	unpas.dev	HTTP 419, halaman "sesi Berakhir" tetapi tidak membocorkan info teknis	CSRF protection aktif
6	POST tanpa CSRF token	Kpta.unpas.dev	HTTP 404 (route berbeda)	
7	/_ignition/execute-solution	unpas.dev	HTTP 405, ukuran 1.002 KB	Indikasi kuat dan akan dilanjutkan ke verifikasi manual

No	Pengujian	Host	Hasil	Status
8	/logout	unpas.dev	HTTP 405, ukuran 1.002 KB	Indikasi kuat dan akan dilanjutkan ke tahap verifikasi manual

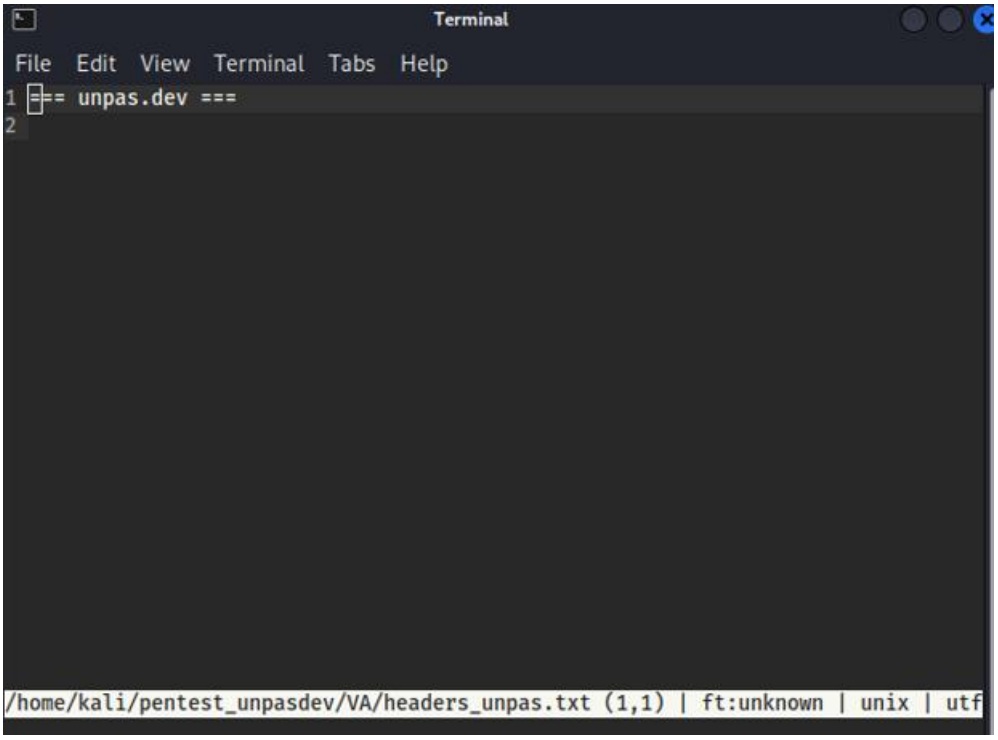
5.3.4 TC-05 HTTP Security Headers

Pengujian TC-05 bertujuan untuk memeriksa penerapan *header* keamanan HTTP pada respons dari kedua host.

1. Curl - Pemeriksaan Security Headers

```
┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ echo "== unpas.dev ==" | tee headers_unpas.txt
== unpas.dev ==

┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ curl -s -I https://unpas.dev | grep -iE "content-security-policy|x-frame-
options|x-content-type-options|strict-transport-security|referrer-policy|perm
issions-policy" | tee -a headers_unpas.txt
```

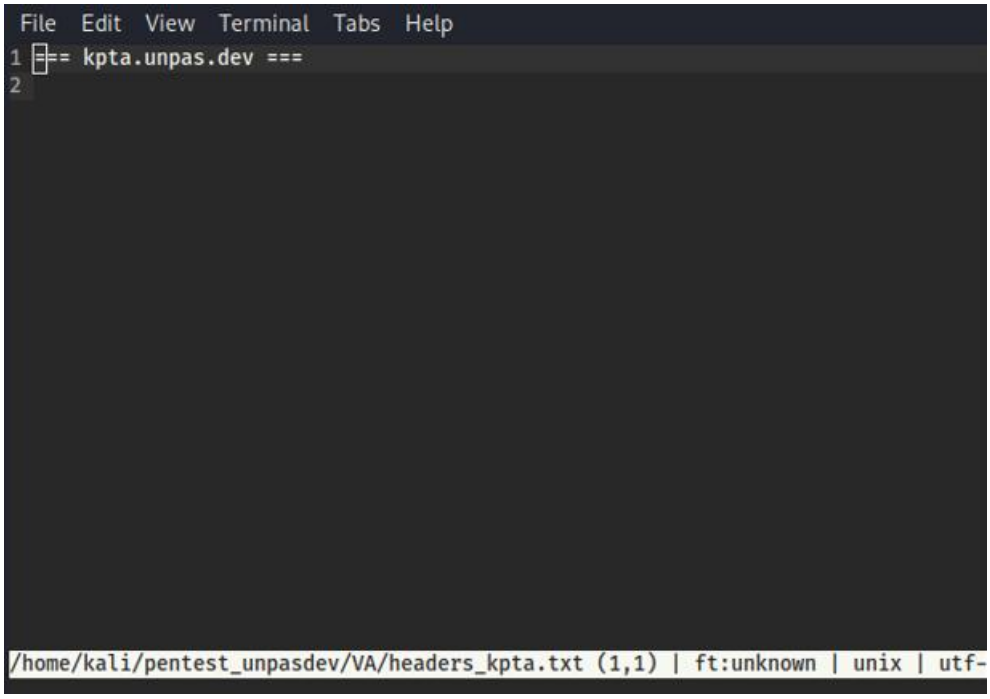
Gambar 5. 27 Kode Eksekusi curl unpas.dev



Gambar 5. 28 Hasil Pemeriksaan *Security Headers* unpas.dev via curl

```
┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ echo "== kpta.unpas.dev ==" | tee headers_kpta.txt
== kpta.unpas.dev ==

┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ curl -s -I https://kpta.unpas.dev | grep -iE "content-security-policy|x-f
rame-options|x-content-type-options|strict-transport-security|referrer-policy
|permissions-policy" | tee -a headers_kpta.txt
```

Gambar 5. 29 Kode Eksekusi curl kpta.unpas.dev



Gambar 5. 30 Hasil Pemeriksaan *Security Headers* kpta.unpas.dev via curl

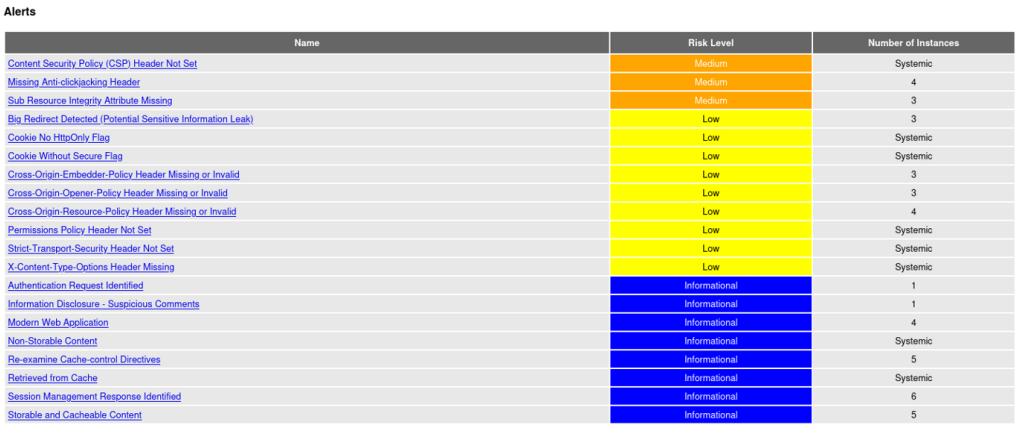
Gambar 5.28 dan 5.30 menampilkan hasil yang identik dari perintah grep, untuk seluruh *header* keamanan utama tidak menghasilkan output apapun pada kedua host. Hasil grep yang kosong mengindikasikan bahwa tidak satu pun dari *header conten-security-policy, x-frame-option, strict-transport-security, x-content-type-options, referrreer-policy*, maupun *permission-policy* diterapkan pada respons HTTP kedua host.

2. OWASP ZAP (Cross-check Security Headers)

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	5
Missing Anti-clickjacking Header	Medium	4
Sub Resource Integrity Attribute Missing	Medium	Systemic
Big Redirect Detected (Potential Sensitive Information Leak)	Low	5
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	Systemic
Cross-Origin-Embedder-Policy Header Missing or Invalid	Low	4
Cross-Origin-Opener-Policy Header Missing or Invalid	Low	4
Cross-Origin-Resource-Policy Header Missing or Invalid	Low	5
Permissions Policy Header Not Set	Low	5
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	5
Authentication Request Identified	Informational	2
Information Disclosure - Sensitive Information in URL	Informational	2
Non-Storable Content	Informational	Systemic
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	1
Session Management Response Identified	Informational	8
Storable and Cacheable Content	Informational	1

Gambar 5. 31 *Alert* ZAP unpas.dev



Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Missing Anti-clickjacking Header	Medium	4
Sub Resource Integrity Attribute Missing	Medium	3
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cross-Origin-Embedder-Policy Header Missing or Invalid	Low	3
Cross-Origin-Opener-Policy Header Missing or Invalid	Low	3
Cross-Origin-Resource-Policy Header Missing or Invalid	Low	4
Permissions Policy Header Not Set	Low	Systemic
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	4
Non-Storable Content	Informational	Systemic
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	Systemic
Session Management Response Identified	Informational	6
Storable and Cacheable Content	Informational	5

Gambar 5. 32 *Alert* ZAP unpas.dev

Gambar 5.31 dan 5.32 mengonfirmasi hasil pemeriksaan curl sebelumnya melalui laporan OWASP ZAP. ZAP menghasilkan alert yang konsisten untuk kedua host, mencakup ketiadaan *content-security-policy (medium), x-frame-options (medium), strict-transport-security (low), x-content-type-options (low), dan permission-policy (low).*

Tabel 5. 9 Ringkasan Hasil Pemeriksaan TC-05

No	Header Keamanan	unpas.dev	kpta.unpas.dev	Risiko (ref. ZAP)
1	*Content-Security-Policy*	Tidak Diterapkan	Tidak Diterapkan	*Medium*
2	*X-Frame-Options*	Tidak Diterapkan	Tidak Diterapkan	*Medium*
3	*Strict-Transport-Security*	Tidak Diterapkan	Tidak Diterapkan	*Low*
4	*X-Content-Type-Options*	Tidak Diterapkan	Tidak Diterapkan	*Low*
5	*Permissions-Policy*	Tidak Diterapkan	Tidak Diterapkan	*Low*
6	*Referrer-Policy*	Tidak Diterapkan	Tidak Diterapkan	*Low*

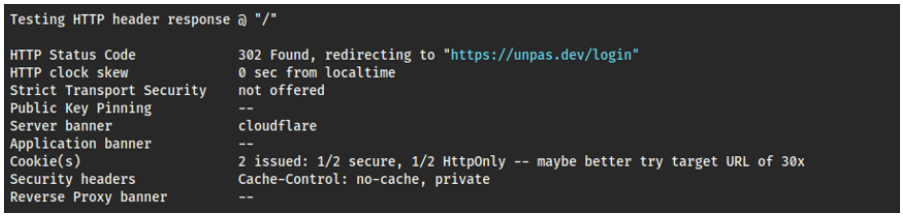
Seluruh *header* keamanan yang diperiksa tidak diterapkan pada kedua host. Indikasi ini dikonfirmasi secara konsisten oleh dua tools independen (curl dan OWASP ZAP) sehingga dinyatakan valid tanpa perlu verifikasi manual tambahan.

5.3.5 TC-06 Konfigurasi SSL/TLS

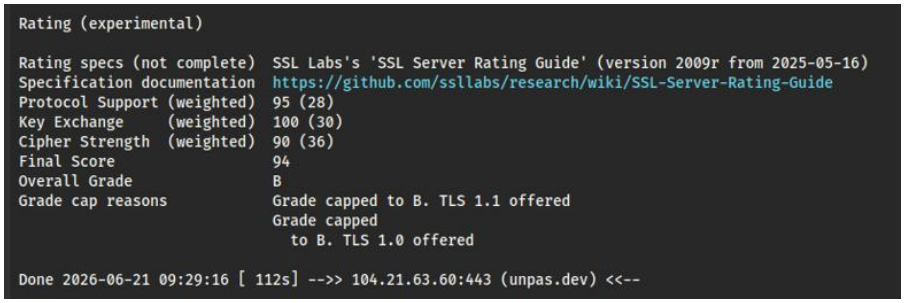
Pengujian TC-06 bertujuan untuk memeriksa keamanan konfigurasi HTTPS pada kedua host, mencakup versi protokol TLS yang didukung, *cipher suite*, validitas sertifikat, dan konfigurasi terkait keamanan sesi.

1. Testssl.sh - Analisis Konfigurasi TLS

Gambar 5. 33 Hasil testssl.sh Protokol TLS unpas.dev



Gambar 5. 34 Hasil testssl.sh HTTP Header Response dan Cookie unpas.dev



Gambar 5. 35 Hasil testssl.sh Grade unpas.dev

Gambar 5. 36 Hasil testssl.sh Protokol TLS kpta.unpas.dev

```
Rating (experimental)

Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009r from 2025-05-16)
Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)  95 (28)
Key Exchange     (weighted)  100 (30)
Cipher Strength  (weighted)  90 (36)
Final Score                  94
Overall Grade                B
Grade cap reasons            Grade capped to B. TLS 1.1 offered
                             Grade capped
                               to B. TLS 1.0 offered

Done 2026-06-21 09:33:37 [ 114s] -->> 172.67.143.222:443 (kpta.unpas.dev) <<--
```

Gambar 5. 37 Hasil testssl.sh Grade kpta.unpas.dev

Gambar 5.33 hingga 5.37 menampilkan hasil analisis testssl.sh terhadap kedua host. Hasil utama yang diperoleh yaitu:

a. TLS 1.0 dan TSL 1.1 masih diaktifkan pada kedua host dengan keterangan “deprecated”, itu menjadi penyebab utama grade keseluruhan diturunkan menjadi B.
b. HSTS (Strict-Transport-Security) tidak diterapkan pada kedua hosts, konsisten dengan hasil TC-05.
c. Cookie pada kedua host dikonfirmasi tidak memiliki attribut secure (“NONE secure”).
d. Sertifikat valid (*wildcard* *unpas.dev, *Google Trust Services*) dengan masa berlaku 40 hari tersisa per tanggal pengujian .

4. Nmap ssl-enum-cipers (Enumerasi Cipher Suite)

```
└─$ nmap --script ssl-enum-ciphers -p 443 unpas.dev -oN ssl_unpas_nmap.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-21 09:36 -0400
Nmap scan report for unpas.dev (172.67.143.222)
Host is up (0.0039s latency).
Other addresses for unpas.dev (not scanned): 104.21.63.60 2606:4700:3034::6815:3f3c 2606:4700:3035::ac43:8fde

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: client
```

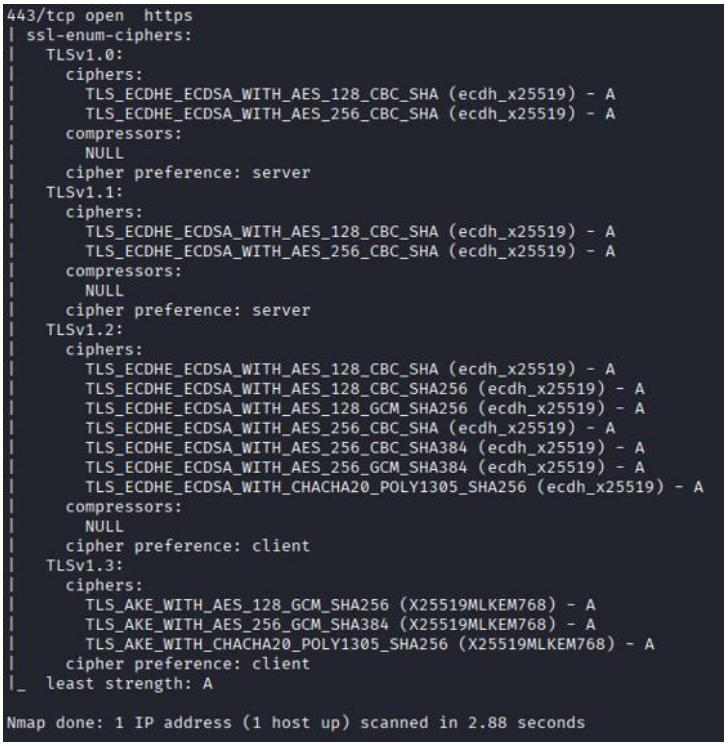
Gambar 5. 38 Hasil nmap ssl-enum-ciphers unpas.dev - Bagian 1

```
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: client
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (X25519MLKEM768) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (X25519MLKEM768) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (X25519MLKEM768) - A
|     cipher preference: client
|_  least strength: A

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

Gambar 5. 39 Hasil nmap ssl-enum-ciphers unpas.dev - Bagian 2

```
┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ nmap --script ssl-enum-ciphers -p 443 kpta.unpas.dev -oN ssl_kpta_nmap.tx
t

Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-21 09:36 -0400
Nmap scan report for kpta.unpas.dev (104.21.63.60)
Host is up (0.0039s latency).
Other addresses for kpta.unpas.dev (not scanned): 172.67.143.222 2606:4700:30
35::ac43:8fde 2606:4700:3034::6815:3f3c

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
```

Gambar 5. 40 Hasil nmap ssl-enum-ciphers kpta.unpas.dev - Bagian 1



Gambar 5. 41 Hasil nmap ssl-enum-ciphers kpta.unpas.dev - Bagian 2

Gambar 5.38 hingga 5.41 mengonfirmasi hasil testssl.sh bahwa TLS 1.0 dan TLS 1,1 memang diaktifkan pada kedua host. Meskipun kekuatan cipher individual dinilai A (baik) oleh Nmap, keberadaan TLS1.0/1.1 tetap menurunkan grade keseluruhan karena kedua protokol ini sudah usang dan tidak direkomendasikan.

Tabel 5. 10 Ringkasan Hasil Pemeriksaan TC-06

No	Item	unpas.dev	kpta.unpas.dev
1	SSLv2/SSLv3	Tidak ditawarkan	Tidak ditawarkan
2	TLS 1.0	Ditawarkan (deprecated)	Ditawarkan (deprecated)
3	TLS 1.1	Ditawarkan (deprecated)	Ditawarkan (deprecated)
4	TLS 1.2	Ditawarkan	Ditawarkan
5	TLS 1.3	Ditawarkan	Ditawarkan
6	Cipher NULL/Export	Tidak ditawarkan	Tidak ditawarkan
7	Forward Secrecy (AEAD)	ditawarkan	Ditawarkan
8	HSTS	Tidak diterapkan	Tidak diterapkan
9	Cookie secure flag	Tidak ada pada sakti_session	Tidak ada pada kpta_session
10	Cookie HttpOnly flag	Diterapkan	Diterapkan
11	Sertifikat	Valid, wildcard *unpas.dev	Wildcard sama
12	Sisa masa sertifikat	40 hari (per tanggal pengujian)	Sertifikat sama
13	Overall Grade	B	B

5.3.6 TC-03 *Directory Listing*

Pengujian TC-03 bertujuan untuk memeriksa apakah direktori pada web server menampilkan daftar file atau folder secara publik tanpa mekanisme pembatasan akses.

1. Curl - Pemeriksaan Direktory Listing

```
┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ for dir in uploads storage backup files images assets documents export; d
o
  echo "== unpas.dev/$dir/ =="
  curl -s https://unpas.dev/$dir/ | grep -i "index of"
  echo "== kpta.unpas.dev/$dir/ =="
  curl -s https://kpta.unpas.dev/$dir/ | grep -i "index of"
done
== unpas.dev/uploads/ ==
== kpta.unpas.dev/uploads/ ==
== unpas.dev/storage/ ==
== kpta.unpas.dev/storage/ ==
== unpas.dev/backup/ ==
== kpta.unpas.dev/backup/ ==
== unpas.dev/files/ ==
== kpta.unpas.dev/files/ ==
== unpas.dev/images/ ==
== kpta.unpas.dev/images/ ==
== unpas.dev/assets/ ==
== kpta.unpas.dev/assets/ ==
== unpas.dev/documents/ ==
== kpta.unpas.dev/documents/ ==
== unpas.dev/export/ ==
== kpta.unpas.dev/export/ ==
```

Gambar 5. 42 Hasil Pemeriksaan *Directory Listing* via curl

Gambar 5.42 menampilkan hasil pemeriksaan *directory listing* menggunakan curl pada 8 kategori umum yang diperiksa dari kedua host. Tidak satupun direktori yang memberikan respons dan mengindikasikan *directory listing* tidak aktif pada direktori-direktori tersebut.

2. OWASP ZAP (Cross-check Directory Listing)

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	5
Missing Anti-clickjacking Header	Medium	4
Sub Resource Integrity Attribute Missing	Medium	Systemic
Big Redirect Detected (Potential Sensitive Information Leak)	Low	5
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	Systemic
Cross-Origin-Embedder-Policy Header Missing or Invalid	Low	4
Cross-Origin-Opener-Policy Header Missing or Invalid	Low	4
Cross-Origin-Resource-Policy Header Missing or Invalid	Low	5
Permissions Policy Header Not Set	Low	5
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	5
Authentication Request Identified	Informational	2
Information Disclosure - Sensitive Information in URL	Informational	2
Non-Storable Content	Informational	Systemic
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	1
Session Management Response Identified	Informational	8
Storable and Cacheable Content	Informational	1

Gambar 5. 43 Hasil Konfirmasi ZAP - Tidak Ada *Alert Directory Browsing* unpas.dev

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Missing Anti-clickjacking Header	Medium	4
Sub Resource Integrity Attribute Missing	Medium	3
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cross-Origin-Embedder-Policy Header Missing or Invalid	Low	3
Cross-Origin-Opener-Policy Header Missing or Invalid	Low	3
Cross-Origin-Resource-Policy Header Missing or Invalid	Low	4
Permissions Policy Header Not Set	Low	Systemic
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	4
Non-Storable Content	Informational	Systemic
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	Systemic
Session Management Response Identified	Informational	6
Storable and Cacheable Content	Informational	5

Gambar 5. 44 Hasil Konfirmasi ZAP - Tidak Ada *Alert Directory Browsing* kpta.unpas.dev

Gambar 5.43 dan 5.44 mengonfirmasi bahwa OWASP ZAP tidak menghasilkan *alert* "*Directory Browsing*" pada pengujian *passive scan* terhadap kedua host. Kombinasi hasil curl dan ZAP menyimpulkan bahwa tidak ditemukan indikasi *directory listing* pada kedua host.

Tabel 5. 11 Ringkasan Hasil Pemeriksaan TC-03

No	Directory Diperiksa	unpas.dev	kpta.unpas.dev
1	/Upload, /storage/, /backup/. /files/. /images/, /assets/, /documents/. /export/	Tidak menampilkan "index of"	Tidak menampilkan "index of"
2	ZAP Alert "*directory browsing*"	Tidak ada	Tidak ada
Kesimpulan		**Tidak ada temuan**	**Tidak ada temuan**

5.3.7 TC-01 Port dan Layanan Terbuka

Pengujian TC-01 pada tahap ini difokuskan untuk memverifikasi fungsi aktual dari port 8080 dan 8443 yang sebelumnya terdeteksi open pada hasil Intelligence Gathering.

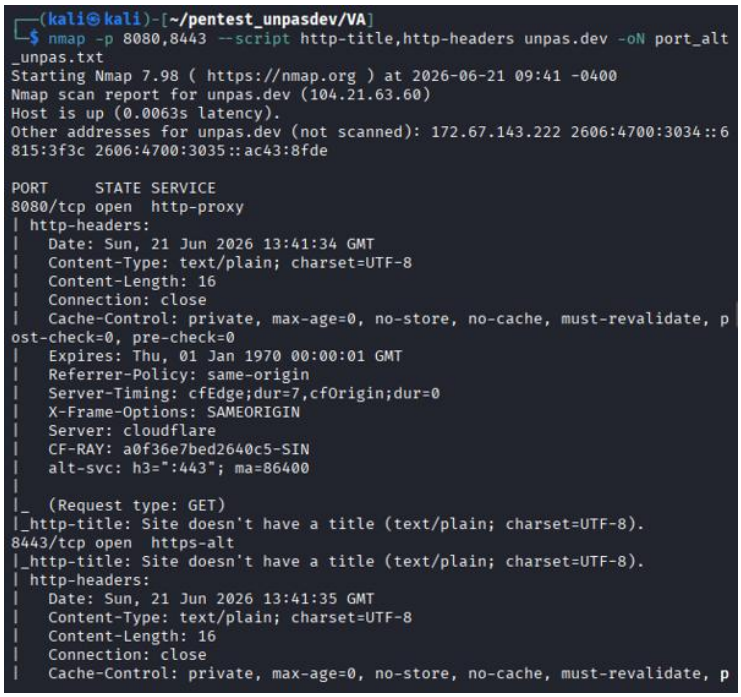
1. Curl - verifikasi Port 8080 dan 8443

```
┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ curl -I https://unpas.dev:8443 --max-time 5
HTTP/2 521
date: Sun, 21 Jun 2026 13:41:11 GMT
content-type: text/plain; charset=UTF-8
content-length: 16
cache-control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
expires: Thu, 01 Jan 1970 00:00:01 GMT
referrer-policy: same-origin
x-frame-options: SAMEORIGIN
server: cloudflare
cf-ray: a0f36de95ee68932-SIN
alt-svc: h3=":8443"; ma=86400


┌──(kali㉿kali)-[~/pentest_unpasdev/VA]
└─$ curl -I http://unpas.dev:8080 --max-time 5
HTTP/1.1 521 <none>
Date: Sun, 21 Jun 2026 13:41:24 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: keep-alive
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
X-Frame-Options: SAMEORIGIN
Server: cloudflare
CF-RAY: a0f36e38d80045da-SIN
alt-svc: h3=":443"; ma=86400
```

Gambar 5. 45 Hasil Verifikasi Port 8080 dan 8443 via curl

Gambar 5.45 menampilkan respons HTTP 521 (*Web server is down*) pada port 8080 dam 8443. Kode 521 merupakan kode error khusus *Cloudflare* yang berarti *Cloudflare* berhasil menerima koneksi di sisi *edge*nya, namun tidak ada server origin yang merespons di balik port tersebut. Ini mengindikasikan port tersebut terbuka di sisi *Cloudflare* sebagai bagian dari konfigurasi standar, tetapi tidak ada layanan atau aplikasi aktif yang berjalan di baliknya.

2. Nmap - Pemeriksaan Detail Port 8080 dan 8443



Gambar 5. 46 Hasil Nmap Detail Port 8080 dan 8443

Gambar 5.46 mengonfirmasi hasil curl dan nmap mendeteksi kedua port sebagai open namun kontennya hanya berupa teks kosong dengan *header Cloudflare* tanpa judul halaman. Tidak ada aplikasi atau layanan nyata yang teridentifikasi pada port ini.

Tabel 5. 12 Ringkasan Hasil Pemeriksaan TC-01

No	Port	Status (Nmap)	Respons (curl)	Layanan Aktif
1	8080	Open (http-proxy)	HTTP 521, tidak ada origin	Tidak ada layanan nyata
2	8443	Open (https-alt)	HTP 521 , tidak ada origin	Tidak ada layanan nyata
Kesimpulan		Port terbuka disisi *Cloudflare*, tidak ada layanan berbahaya	Tidak ada temuan	

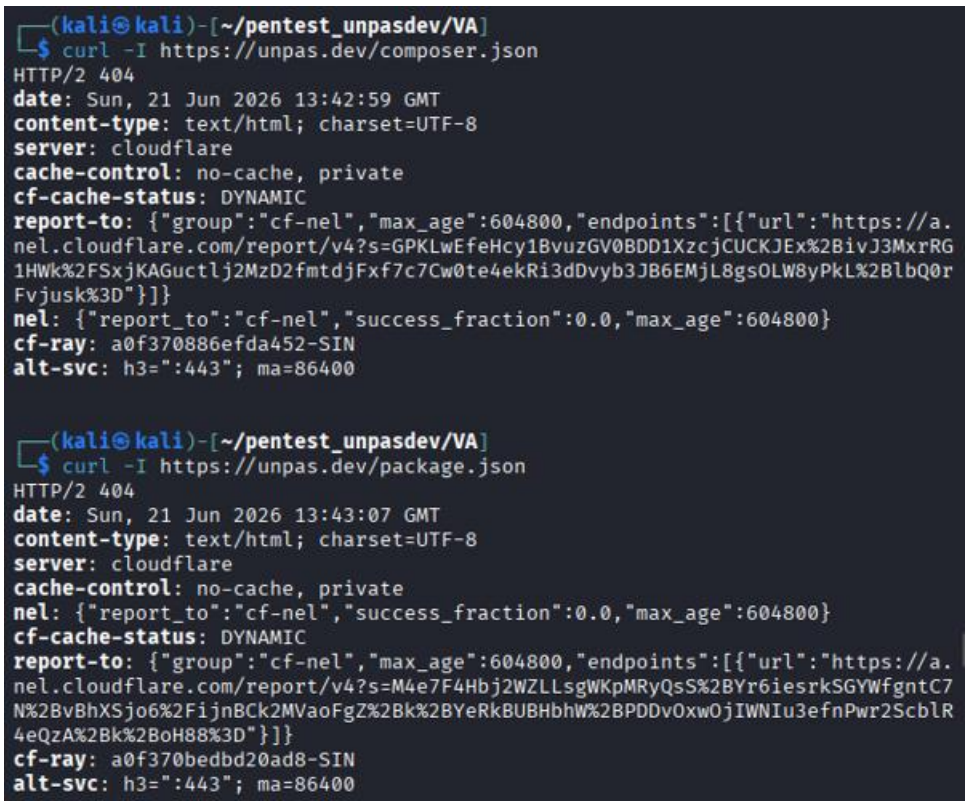
5.3.8 TC-07 Informasi Versi Layanan

Pengujian TC-07 bertujuan untuk memeriksa apakah informasi versi web server, *framework*, database, atau layanan lain dapat diidentifikasi dari sisi publik.

1. **WhatWeb (*Fingerprinting* Teknologi)**

   Merujuk pada gambar 5.17 (Whatweb unpas.dev) dan 5.18 (WhatWeb kpta.unpas.dev) header server pada kedua host hanya menampilkan "*cloudflare*" tanpa informasi versi web server asli, sistem operasi, atau versi framework yang digunakan.

2. **Curl - Pemeriksaan File Metadata Versi**

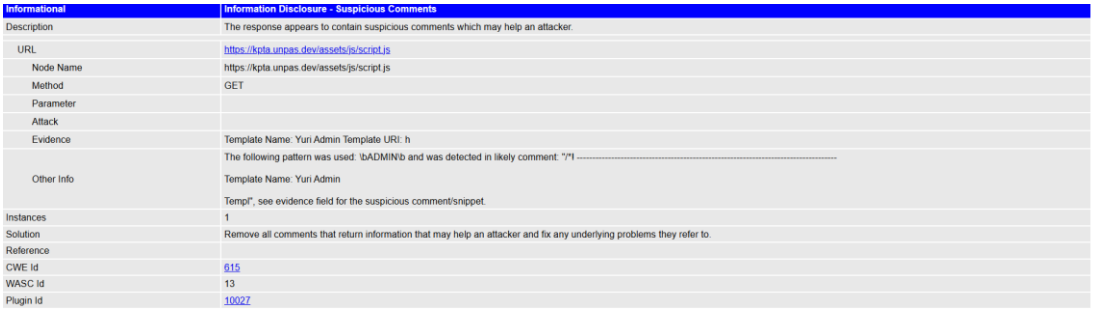


Gambar 5. 47 Hasil Pemeriksaan Meta Data unpas.dev

Gambar 5. 48 Hasil Pemeriksaan Meta Data kpta.unpas.dev

Gambar 5.47 dan 5.48 menunjukkan bahwa file comporser.json dan package.json yang biasanya berisi daftar *dependency* beserta versinya tidak dapat diakses dari sisi publik pada kedua host (HTTP 404).

3. Informasi Tambahan Komentar *Source Code* kpta.unpas.dev



Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://kpta.unpas.dev/assets/js/script.js
Node Name	https://kpta.unpas.dev/assets/js/script.js
Method	GET
Parameter	
Attack	
Evidence	Template Name: Yuri Admin Template URI: h
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "/*! ---------- Template Name: Yuri Admin Templ", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Gambar 5. 49 Komentar Source Code yang Mengungkapkan Nama Template kpta.unpas.dev

Gambar 5.49 menampilkan komentar pada file JavaScript kpta.unpas.dev/assets/js/script.js yang mengungkap nama template yang digunakan "Yuri Admin" karya pixelstrap. Informasi ini dikonfirmasi melalui alert ZAP "*Information Disclosure – Suspicious Comments*". Meskipun bukan versi aplikasi secara langsung, informasi nama template dapat digunakan oleh pihak yang tidak berwenang untuk mengidentifikasi teknologi yang digunakan dan mencari kerentanan terkait.

Tabel 5. 13 Ringkasan Hasil Pemeriksaan TC-07

No	Sumber	Unpas.dev	Kpta.unpas.dev
1	*Header Server*	*Cloudflare* (versi asli tersembunyi)	*Cloudflare* (versi asli tersembunyi)
2	*Header X-Powered-By*	Tidak ada	Tidak ada
3	Composer.json / package.json	HTTP 404	HTTP 404
4	WhatWeb	Tidak mendeteksi versi *Framework/OS*	Template "Yuri Admin" teridentifikasi
5	Komentar Source Code	Tidak ada	Template name: Yuri Admin pada script.jas
kesimpulan		Tidak ada informasi versi terekspos	Nama template teridentifikasi (risiko rendah)

5.3.9 Ringkasan Keseluruhan *Vulnerability Analysis*

Tabel 5. 14 Ringkasan Keseluruhan Hasil *Vulnerability Analysis*

Kode	Parameter	Unpas.dev	Kpta.unpas.dev	Status
TC-04	Pesan Error Informatif	Indikasi kuat (_ignition dan /logout 1MB)	Tidak ada indikasi	Lanjut ke verifikasi manual
TC-02	Konfigurasi Default	Anomali (PMA2016/ 500)	.htaccess HTTP 200	Lanjut ke verifikasi manual

Kode	Parameter	Unpas.dev	Kpta.unpas.dev	Status
TC-05	*HTTP Security Headers*	Semua header tidak ada	Semua header tidak ada	Valid dan tidak perlu verifikasi manual
TC-06	SSL/TLS	TLS 1.0/1.1 HSTS dan *cookie secure* tidak ada	Sama	Valid dan tidak perlu verifikasi manual
TC-03	Directory Listing	Tidak ditemukan	Tidak ditemukan	Tidak ada temuan
TC-01	Port dan layanan	Port 8080/8443 tidak aktif	-	Tidak ada temuan
TC-07	Versi layanan	Tidak terekspos	Nama Template	Dicatat (risiko rendah)

5.3.10 Verifikasi Manual Temuan

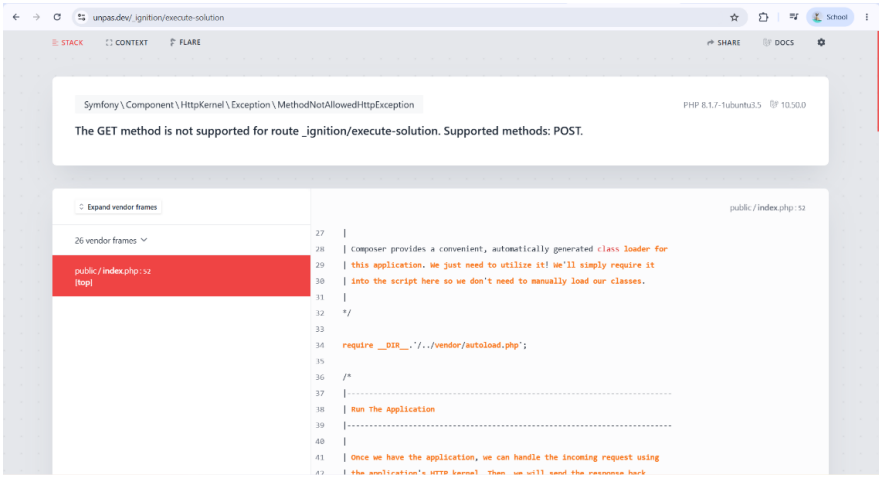
Sebagai bagian akhir dari tahap Vulnerability Analysis, dilakukan verifikasi manual secara terbatas. Verifikasi bertujuan untuk membuktikan apakah indikasi kerentanan yang diperoleh benar-benar valid, tanpa melakukan perubahan data maupun tindakan destruktif apapun terhadap sistem. Seluruh aktivitas pada tahap ini bersifat observasional dan dilaksanakan dalam batas maksimal 3 metode pemeriksaan per indikasi sesuai batasan penelitian.

Berdasarkan tabel 5.14 (ringkasan hasil VA, terdapat dua indikasi yang memerlukan validasi aktif lanjutan yaitu indikasi TC-04 dan indikasi TC-02. Temuan lainnya dinyatakan valid langsung berdasarkan bukti yang sudah dikonfirmasi silang oleh dua tools independen pada tahap *Vulnerability Analysis* sehingga tidak memerlukan validasi tambahan.

5.3.10.1 Validasi F-01 Laravel Debug mode Aktif

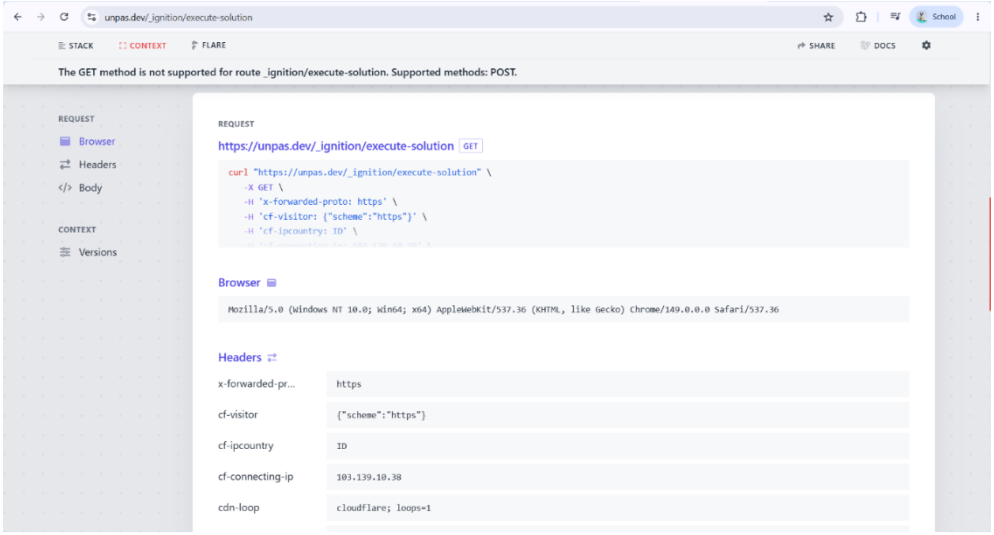
Validasi dilakukan dengan mengakses langsung kedua endpoint yang menunjukkan indikasi pada tahap VA menggunakan browser (*GET request* biasa tanpa *payload* atau parameter tambahan). Metode ini merupakan observasi langsung yang bersifat non-destruktif yang setara dengan membuka halaman web biasa.

1. Validasi via Browser - /_ignition/execute-solution



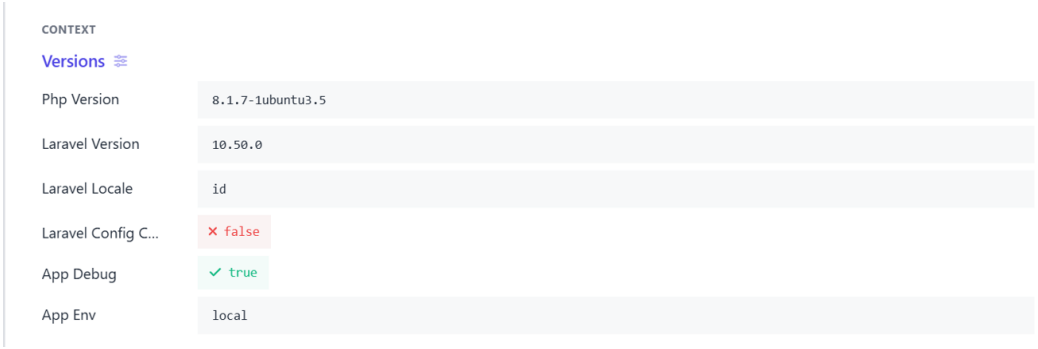
Gambar 5. 50 Halaman *Ignition Debug Page Stack Trace* dan *Source Code*

Gambar 5.50 menampilkan bagian stack trace pada halaman ignition yang mengekspos isi *source code* aplikasi secara langsung/ terlihat baris-baris kode dari file public/index.php beserta nomor barisnya, termasuk kode require_DIR_.'/..vendor/autoload.php, require_once_DIR_.'/.../bootstrap/app.php dan perintah inisialisasi kernel Laravel. Informasi ini memperlihatkan struktur internal aplikasi kepada siapa pun yang mengaksesnya dari internet publik.



Gambar 5. 51 Halaman *Ignition Debug Page - tab Context: Request* dan *header*

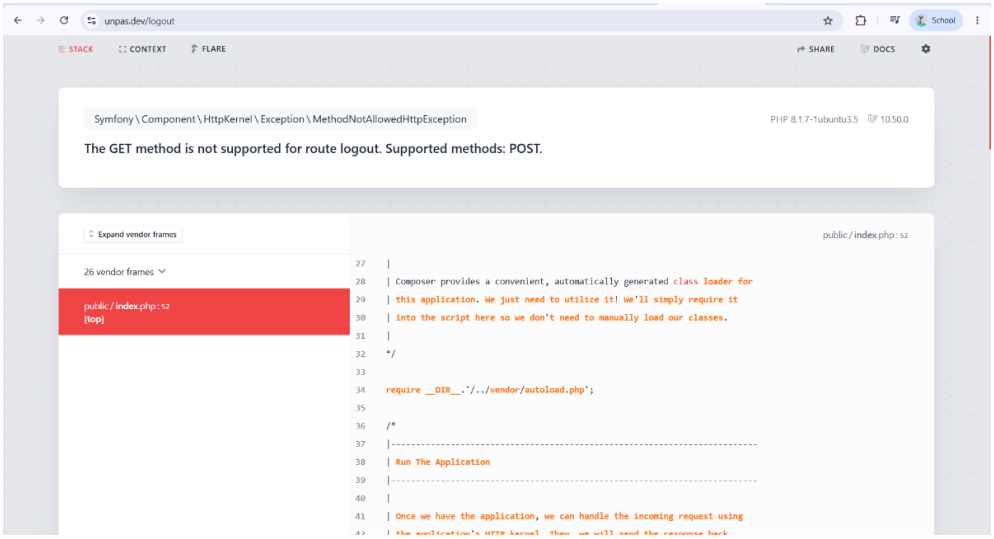
Gambar 5.51 menampilkan tab *CONTEXT* pada halaman ignition yang mengekspos seluruh detail *request* HTTP yang diterima server termasuk *header-header* internal *Cloudflare* (cf-connecting-ip, cf-ipcountry, cf-ray, cdn-loop) yang normalnya bersifat *backend-only* dan tidak seharusnya tampil ke sisi publik. Eksposur *header* internal ini dapat dimanfaatkan untuk memahami arsitektur infrastruktur di balik *Cloudflare*.



Gambar 5. 52 Halaman *Ignition Debug Page - tab Context: Versions*

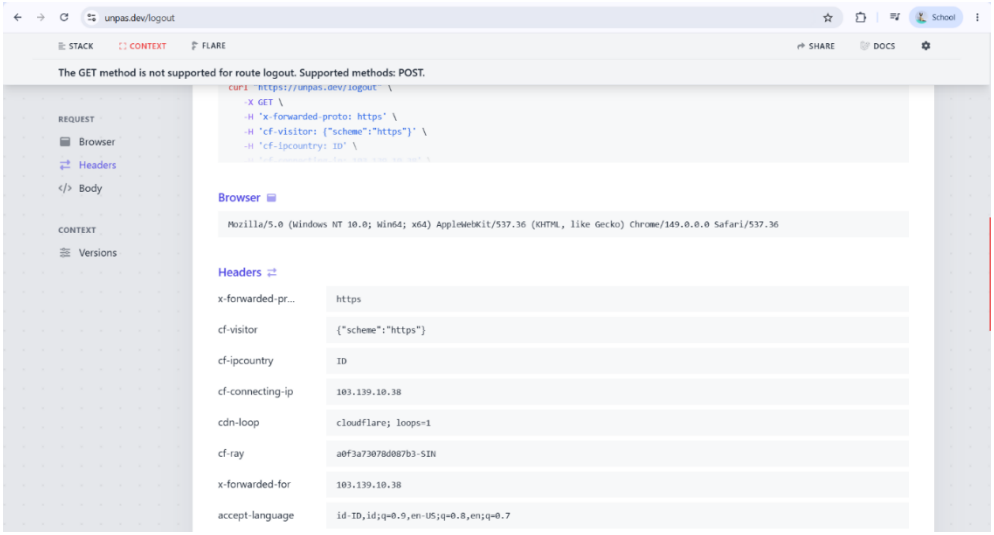
Gambar 5.52 merupakan bukti paling krusial dari seluruh rangkaian validasi TC-04. Tab CONTEXT dalam *version* pada halaman *Ignition* secara eksplisit menampilkan APP_DEBUG:true (ditandai *checklist* hijau) dan APP_ENV: local, itu merupakan dua konfigurasi yang seharusnya tidak pernah aktif di lingkungan produksi. Konfigurasi APP_ENV=local mengindikasikan bahwa aplikasi berjalan dalam mode pengembangan padahal domain unpas.dev merupakan layanan produksi aktif yang digunakan oleh civitas akademika Fakultas Teknik Universitas Pasundan.

2. Validasi via Browser - /logout

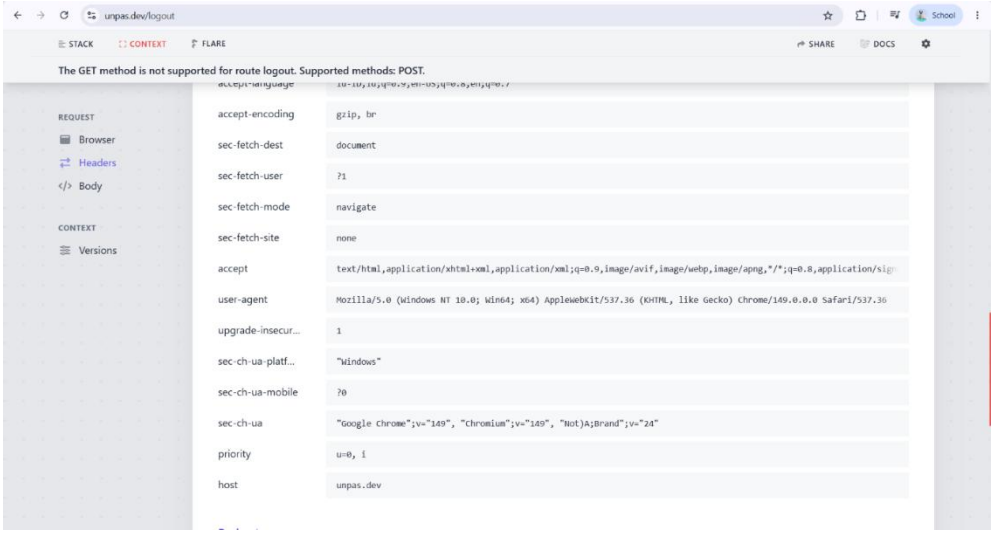


Gambar 5. 53 *Ignition Debug Page* pada *Route /logout*

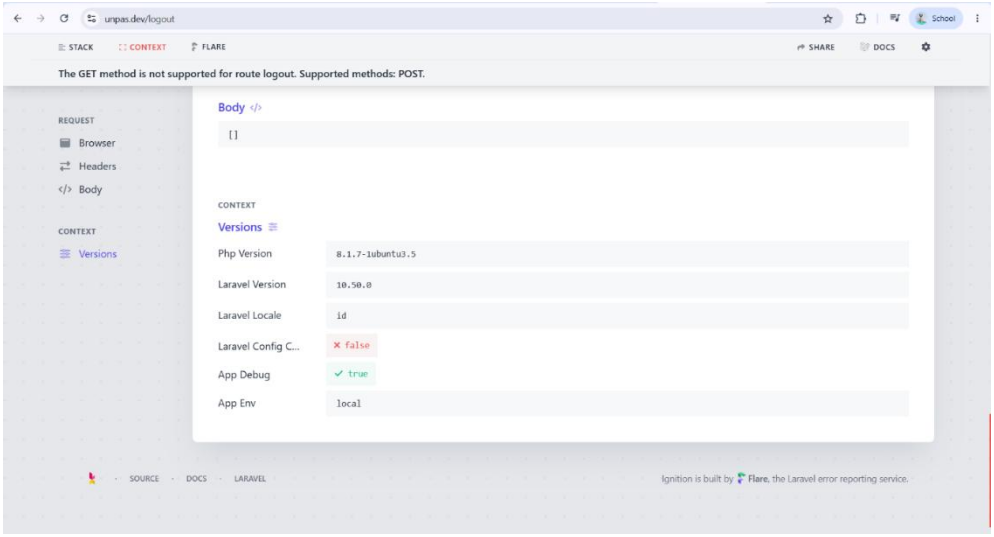
Gambar 5. 54 *Stack Trace Route* /logout



Gambar 5. 55 *Tab Context: Headers Route /logout*



Gambar 5. 56 *Tab Context: Headers Route /logout* - Lanjutan



Gambar 5. 57 *Tab Context versions Route /logout*

Gambar 5.53 hingga 5.57 menampilkan hasil akses terhadap *route* /logout yang menghasilkan tampilan identik dengan /_ignition/execute-solution. Kondisi ini membuktikan bahwa *debug mode* bukan hanya aktif pada satu *endpoint* tertentu, melainkan bersifat sistemik yang berarti seluruh route yang memicu *exception* akan menampilkan halaman ignition yang sama. Gambar 5.7 kembali mengonfirmasi APP_DEBUG: true dan APP_ENV: local pada route yang berbeda, memperkuat validitas temuan TC-04.

Batas validasi: Aktivitas dihentikan pada observasi GET, meskipun halaman Ignition menampilkan keterangan "*Supported methods:POST*" pada route /_ignition/execute-solution, tidak dilakukan percobaan POST maupun pengiriman payload apapun sesuai dengan batasan non-destruktif.

Tabel 5. 15 Ringkasan Hasil Validasi F-01

No	Item	Hasil Validasi
1	Endpoint yang divalidasi	/_ignition/execute-solution dan /logout
2	Metode akses	*GET request* via browser
3	Halaman yang ditampilkan	*Laravel Ignition Debug Page*
4	APP_DEBUG	*True*
5	APP_ENV	Local (seharusnya production)
6	Versi PHP	8.1.7-1ubuntu3.5
7	Versi Laravel	10.50.0
8	Stack trace terekspos	Ya, path internal public/index.php, vendor/autoload.php, bootstrap/app.php
9	Header internal Cloudflare terekspos	Ya, cf-connecting-ip, cf-ipcountry, cf-ray, cdn-loop
10	Status validasi	VALID
11	Tools yang digunakan	Browser dan Dirsearch

5.3.10.2 Validasi F-05 .htaccess Dapat Diakses Publik

Validasi dilakukan dengan mengakses langsung file .htaccess pada kpta.unpas.dev menggunakan curl untuk mengonfirmasi isi file dan memastikan bahwa file tersebut benar benar dapat diakses publik beserta kontennya.

1. Curl – Akses Langsung .htaccess

```
┌──(kali㉿kali)-[~]
└─$ curl -s https://kpta.unpas.dev/.htaccess
<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Handle X-XSRF-Token Header
    RewriteCond %{HTTP:x-xsrf-token} .
    RewriteRule .* - [E=HTTP_X_XSRF_TOKEN:%{HTTP:X-XSRF-Token}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```

Gambar 5. 58 Hasil Akses langsung .htaccess kpta.unpas.dev via curl

Gambar 5.58 mengonfirmasi bahwa file.htaccess pada kpta.unpas.dev dapat diakses dan dibaca secara penuh dari sisi publik. Isi file merupakan konfigurasi default bawaan *framework* Laravel, isi tersebut identik dengan template standar laravel/laravel yang tersedia secara publik di repositori resmi Laravel. Meskipun isi file tidak mengandung informasi sensitif (tidak ada kredensial, atau path spesifik), keberadaan akses publik ke file ini tetap merupakan *misconfiguration* karena file konfigurasi server seharusnya tidak dapat diakses dari jaringan publik sesuai praktik hardening standar.

Tabel 5. 16 Ringkasan Hasil Validasi F-05

No	Item	Hasil Validasi
1	File yang divalidasi	https://kpta.unpas.dev/.htaccess
2	Metode akses	*Curl GET request*
3	Status HTTP	200 OK
4	Isi file	*Konfigurasi default Laravel* (mod_rewrite, front controller)
5	Informasi sensitif ditemukan	Tidak
6	Status validasi	Valid (file dapat diakses publik)
7	Catatan	Konten tidak sensitif, namun akses publik tetap merupakan *misconfiguration*

5.3.10.3 Status Validasi Seluruh Temuan

Tabel 5. 17 Ringkasan Status Validasi Semua Temuan

Kode	Temuan	Metode validasi	Status
F-01	Laravel debug mode aktif (APP_DEBUG=true, APP_ENV=local)	Browser GET + dirsearch	Valid
F-02	HTTP security headers tidak diterapkan	Curl+ OWASP ZAP	Valid (langsung dari VA)
F-03	Cookie sesi tanpa atribut secure	Curl+ OWASP ZAP	Valid (langsung dari VA)
F-04	TLS 1.0 dan TLS 1.1 masih aktif	Curl+ OWASP ZAP	Valid (langsung dari VA)
F-05	.htaccess dapat diakses publik	Dirsearch + curl	Valid
F-06	SRI tidak diterapkan pada CDN eksternal	ZAP alert +source code (dari VA)	Valid (langsung dari VA) (informasi pendukung)
F-07	Referensi subdomain usang pada OAuth	ZAP passive observation (dari VA)	Dicatat (informasi pendukung)

5.4 Analisis Dampak

Analisis dampak dilaksanakan untuk menganalisis dampak dari seluruh temuan yang telah diverifikasi pada tahap *Vulnerability Analysis*. Analisis difokuskan pada penilaian dampak setiap temuan terhadap tiga aspek utama keamanan informasi yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), dan *Availability* (Ketersediaan).

5.4.1 Analisis Dampak per Temuan

1. F-01 Laravel Debug Mode Aktif (APP_DEBUG=true, APP_ENV=local)

Temuan F-01 merupakan temuan dengan dampak paling signifikan dari seluruh hasil pengujian. Halaman Laravel *Ignition Debug Page* yang aktif dan dapat diakses tanpa autentikasi mengekspos beberapa lapisan informasi teknis sekaligus dalam satu titik akses publik.

Dari aspek *Confidentiality* , temuan ini berdampak pada terekspos nya informasi berikut yang diperoleh langsung dari hasil validasi:

a. Versi PHP 8.1.7-1ubuntu3.5 dan versi Laravel 10.50.0 yang memungkinkan pihak luar mengidentifikasi teknologi spesifik yang digunakan dan mencari kerentanan yang diketahui pada versi tersebut (*version fingerprinting*).
b. Path struktur internal aplikasi (public/index.php, vendor/autoload.php, bootstrap/app.php) yang mengungkap arsitektur direktori server.
c. Seluruh header request termasuk header internal *Cloudflare* (cf-connecting-ip, cf-ipcountry, cf-ray) yang seharusnya bersifat *backend-only*.
d. Status konfigurasi APP_ENV=local yang mengonfirmasi sistem tidak dikonfigurasi untuk lingkungan produksi.

Dari aspek *integrity* dan *availability*, tidak ditemukan dampak langsung berdasarkan pengujian yang dilakukan. Validasi dibatasi pada observasi *GET* sehingga tidak ada bukti

kemampuan mengubah data atau mengganggu layanan yang dapat dikonfirmasi dalam batas pengujian ini.

Selain dampak langsung di atas, kondisi APP_DEBUG=true pada lingkungan produksi juga meningkatkan risiko tidak langsung secara signifikan. Endpoint /_ignition/execute-solution yang aktif memiliki riwayat terkait CVE-2021-3129 (*Remote Code Execution* melalui debug mode Laravel/Ignition) yaitu kerentanan Remote Code Execution tanpa autentikasi pada paket Ignition versi sebelum 2.5.2 yang digunakan bersama Laravel versi sebelum 8.4.2. CVE tersebut memperoleh skor CVSS 9.8 *CRITICAL* karena tereksploitasi tanpa autentikasi dan berdampak penuh pada *Confidentiality*, *Integrity*, dan *Availability*.

Meskipun demikian, skor CVSS pada temuan F-01 dalam penelitian ini tidak disamakan dengan skor CVE-2021-3129, dengan pertimbangan sebagai berikut:

1. Versi Laravel yang teridentifikasi pada target yaitu 10.50.0 berada jauh di atas versi yang diketahui rentan 8.4.2, sehingga rantai eksploitasi pada CVE tersebut kemungkinan besar telah mendapatkan perbaikan (*patched).*
2. Karena penelitian ini dibatasi hingga tahap *Vulnerability Analysis* dan tidak mencakup eksploitasi, dampak yang dapat dikonfirmasi secara langsung terbatas pada *information disclosure,* bukan pada pembuktian eksekusi jarak jauh.

2. F-02 HTTP *Security Headers* Tidak Diterapkan

Tidak adanya *security headers* pada kedua host menciptakan kondisi dimana browser pengguna tidak memiliki instruksi keamanan dari server mengenai cara menangani konten yang dimuat. Dampak terhadap *integrity* bersifat Low, ketiadaan *X-Frame-Options* dan *Content-Security-Policy* membuka peluang serangan *clickjacking* (memuat halaman dalam inframe tersembunyi untuk mengelabui pengguna melakukan aksi tertentu tanpa disadari). Dampak terhadap *confidentiality* bersifat Low, ketiadaan *Strict-Transport-Security* berarti browser tidak dipaksa menggunakan HTTPS pada kunjungan pertama, membuka celah *downgrade* HTTPS ke HTTP sebelum *redirect* terjadi. Dampak terhadap *availability None*, tidak ada layanan yang terganggu akibat ketiadaan header ini secara langsung. Perlu dicatat bahwa dampak F-02 umumnya baru signifikan jika dikombinasikan dengan kerentanan lain yang berada di luar lingkup penelitian ini.

3. F-03 Cookie Sesi Tanpa Atribut Secure

Cookie sakti_session (unpas.dev) dan kpta_session (kpta.unpas.dev) tidak memiliki atribut secure, yang berarti browser tidak diinstruksikan untuk membatasi pengiriman *cookie* hanya melalui koneksi HTTPS. Dampak terhadap *Confidentiality* bersifat Low, dalam skenario di mana terjadi downgrade HTTPS ke HTTP (misalnya pada jaringan yang tidak aman atau

melalui serangan MITM di jaringan lokal), *cookie* sesi berpotensi terkirim tanpa enkripsi dan dapat disadap, sehingga membuka peluang *session hijacking*. Dalam kondisi normal dengan HTTPS yang sudah dipaksakan (redirect 302), risiko ini termitigasi sebagian. Dampak terhadap *Integrity* dan *Availability None*. Perlu digarisbawahi bahwa *cookie* sesi sudah memiliki atribut *HttpOnly* yang artinya perlindungan terhadap pencurian cookie melalui XSS sudah ada, yang belum adalah perlindungan terhadap skenario jaringan tidak aman.

4. **F-04 TLS 1.0 dan TLS 1.1 Masih Aktif**

   Dukungan terhadap TLS 1.0 dan TLS 1.1 yang sudah usang (*deprecated*) pada kedua host menghasilkan penurunan *grade* keamanan TLS dari A menjadi B berdasarkan penilaian testssl.sh. Dampak terhadap *Confidentiality* dan *Integrity* bersifat *Low*, kedua protokol ini memiliki kerentanan yang diketahui (*BEAST* untuk TLS 1.0, *POODLE* untuk SSL 3.0 yang serupa secara konsep) meskipun browser modern sudah tidak menggunakannya secara default sehingga risiko aktual termitigasi. Risiko aktual lebih relevan pada klien lama atau sistem yang belum diperbarui yang masih menegosiasikan TLS 1.0/1.1. Dampak terhadap *Availability None*.

5. **F-05 .htaccess Dapat Diakses Publik**

   File .htaccess pada kpta.unpas.dev dapat diakses dan dibaca dari sisi publik. Berdasarkan hasil validasi, isi file merupakan konfigurasi default bawaan Laravel tanpa informasi sensitif tidak mengandung kredensial, path spesifik sistem, atau aturan keamanan kustom yang dapat dimanfaatkan langsung. Dampak terhadap *Confidentiality* bersifat *Negligible* (sangat rendah, hampir tidak ada) karena konten yang terekspos sudah tersedia secara publik di repositori *framework*. Meskipun demikian, file konfigurasi server seharusnya tidak dapat diakses dari jaringan publik sebagai dari praktik hardening standar. Dampak *Integrity* dan *Availability None*.

6. **F-06 Subresource Integrity Tidak Diterapkan pada CDN Eksternal**

   Tidak adanya atribut *integrity* pada tag <script> dan <link> yang memuat *resource* dari CDN eksternal (jsdelivr) pada unpas.dev berarti browser tidak melakukan verifikasi hash terhadap file yang dimuat. Dampak terhadap *Integrity* bersifat *Low*, jika CDN pihak ketiga mengalami kompromi (diretas atau terjadi *supply chain attack*), konten berbahaya berpotensi disisipkan dan dijalankan pada browser pengguna tanpa terdeteksi. Risiko ini bergantung pada keamanan pihak CDN itu sendiri sehingga dampak aktual dalam kondisi normal sangat rendah. Dampak terhadap *Confidentiality* dan *Availability None*. Temuan ini dicatat sebagai catatan karena hal ini di luar lingkup pengujian saat ini.

7. **F-07 Referensi Subdomain Usang pada Konfigurasi OAuth**

   Konfigurasi unpas.dev/auth/google yang masih merujuk ke redirect_uri=https://sadaya.unpas.dev/auth/google/callback menunjukkan adanya sisa konfigurasi dari sistem lama yang belum dibersihkan. Tidak ada dampak langsung teridentifikasi

terhadap aspek CIA karena subdomain sadaya.unpas.dev tidak ditemukan aktif pada saat pengujian dan temuan ini dicatat sebagai catatan karena hal ini di luar ruang lingkup pengujian saat ini.

5.4.2 Identifikasi Layanan yang Berpotensi Terdampak

Tabel 5. 18 Layanan yang Berpotensi Terdampak

No	Layanan	Host	Temuan Terkait	Potensi Dampak
1	SAKTI (termasuk modul Remedial, *Whistleblowing System,* penilaian dosen sejawat)	Unpas.dev	F-01, F-02, F-03,F-04, F-06, F-07	Risiko tertinggi F-01 hanya ditemukan di host ini dan berdampak pada seluruh layanan yang berjalan di bawahnya
2	KPTA	Kpta.unpas.dev	F-02, F-03, F-04, F-05	Risiko lebih rendah dibanding unpas.dev , tidak ditemukan F-01

5.4.3 Ringkasan Analisis Dampak

Tabel 5. 19 Ringkasan Analisis Dampak per Temuan

Kode	Temuan	Host	Dampak *Confidentiality*	Dampak *Integrity*	Dampak *Availability*	Catatan
F-01	*Laravel Debug* Mode Aktif	Unpas.dev	*Medium*	*None*	*None*	Versi PHP/Laravel, path internal, *header Cloudflare* internal terekspos tetapi tidak ada data pengguna/kredensial yang ditemukan dalam batas pengujian.
F-02	HTTP Security Headers tidak diterapkan	keduanya	*Low*	*Low*	*None*	Dampak nyata baru muncul jika dikombinasikan dengan kerentanan lain di luar lingkup.
F-03	Cookie sesi tanpa secure	Keduanya	*Low*	*None*	*None*	Dampak nyata baru muncul jika dikombinasikan dengan kerentanan lain di luar lingkup
F-04	TLS 1.0 dan TLS 1.1 aktif	Keduanya	*Low*	*Low*	*None*	Browser modern tidak menggunakan protokol ini.
F-05	.htaccess dapat diakses publik	Kpta.unpas.dev	*none*	*none*	*none*	Isi file adalah konfigurasi default tanpa informasi sensitif
F-06	SRI tidak diterapkan	Unpas.dev	*None*	*Low*	*None*	Bergantung pada keamanan CDN pihak ketiga
F-07	Referensi subdomain usang OAuth	Unpas.dev	*None*	*None*	*None*	Hanya dicatat dan tidak ada dampak langsung saat ini

5.4.4 Dasar Penilaian Risiko

Berdasrakan analisis dampak pada subbab 5.5.1 hingga 5.5.3, disusun estimasi *Base Metrics* CVSS v4.0 untuk setiap sebagai dasar perhitungan skor resmi pada tahap *Reporting*. Estimasi metrik dijabarkan pada Tabel 5.20.

Tabel 5. 20 Estimasi *Base Metrics* CVSS v4.0 per Temuan

Kode	AV	AC	AT	PR	UI	VC	VI	VA	Justifikasi Ringkas
F-01	N	L	N	N	N	L	N	N	Akses publik langsung (AV:N), tanpa autentukasi (PR:N), cukup GET request biasa (AC:L), dampak terbatas pada info teknis, bukan data pengguna (VC:L)
F-02	N	L	N	N	P	N	L	N	Meemrlukan interaksi korban (UI:P) untuk dieksploitasi, dampak integrity rendah (VI:L) melalui clickjacking
F-03	A	H	P	N	N	L	N	N	Membutuhkan posisi jaringan yang sama (AV:A) dan kondisi downgrade HTTP (AC:H, AT:P)
F-04	N	H	P	N	N	L	L	N	Memerlukan kondisi downgrade attack (AC:H, AT:P). Browser modern sudah memitigasi otomatis
F-05	N	L	N	N	N	N	N	N	Dapat akses tanpa hambatan (AV:N, AC:L) namun isi tidak sensitif sama sekali (AV:N, AC:L) namun isi tidak sensitif sama sekali (VC:N, VI:N, VA:N)
F-06	N	H	P	N	P	N	L	N	Bergantung pada komrpomi CDN pihak ketiga (AT:P) dan interaksi pengguna (UI:P)

Keterangan: *AV=Attack Vector, AC=Attack Complexity, AT=Attack Requirements, PR=Privileges Required, UI=User Interaction, VC=Confidentiality Impact (Vulnerable System, VI+Integrity Impact, VA=Availability Impact, N=None/Network, L=Low, H=High, A=Adjacent, P=Passive/Present*.

Seluruh estimasi *Base Metrics* pada tabel 5.20 menjadi dasar penyusunan vector string CVSS v4.0 dan penghitungan skor resmi menggunakan kalkulator FISRT pada tahap *Repoting*.

5.5 *Reporting*

Tahap reporting merupakan tahap akhir dari rangkaian pengujian menyajikan seluruh temuan secara sistematis, lengkap dengan penilaian risiko menggunakan CVSS v4.0 dan rekomendasi teknis perbaikan. Hasil pada tahap ini menjadi rujukan utama bagi pengelola sistem dalam menentukan prioritas dan langkah penanganan temuan *Security Misconfiguration* yang ditemukan pada domain unpas.dev dan kpta.unpas.dev.

5.5.1 Daftar Temuan

Berdasarkan seluruh proses pengujian yang telah dilaksanakan mulai dari *Intelligence Gathering* hingga *Reporting*, diperoleh 7 temuan *Security Misconfiguration* yang telah teridentifikasi. Dari ketujuh temuan yang teridentifikasi, empat di antaranya tergolong *Security*

Misconfiguration. Dua temuan lainnya, yaitu F-06 dan F-07, ditemukan secara insidental di luar lingkup pengujian.

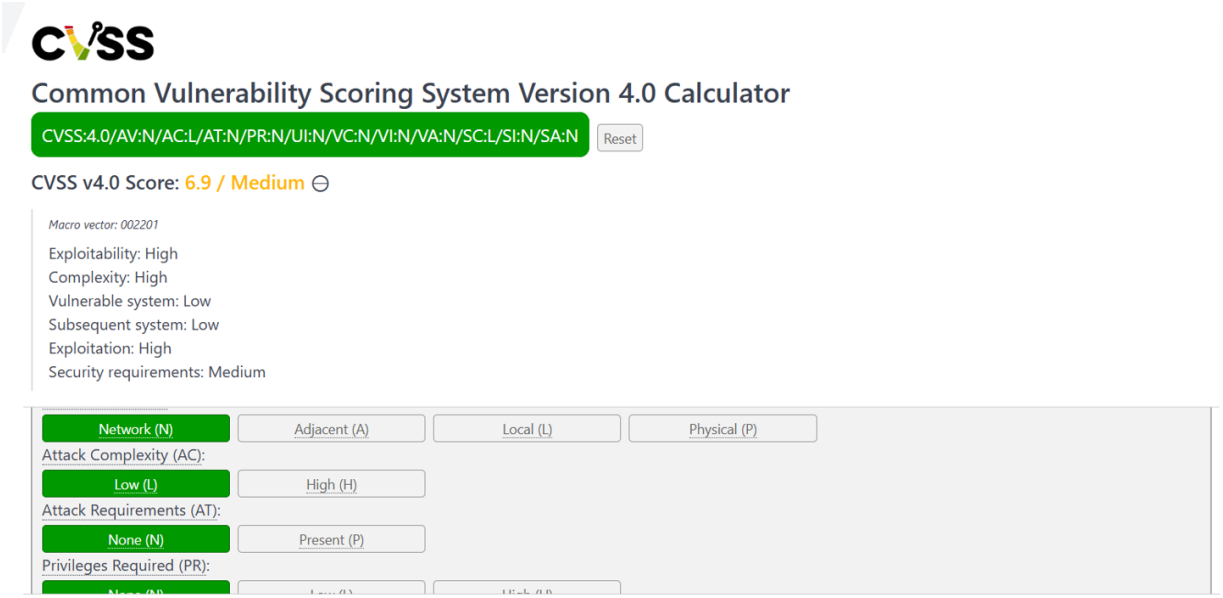
Kedua temuan tersebut tetap disajikan pada Tabel 5.21 dan dinilai dengan CVSS v4.0 sebagaimana temuan lain, sebagai bagian dari tanggung jawab pengungkapan atas kondisi yang ditemukan selama pengujian. Seluruh temuan dirangkum pada tabel 5.21 berikut.

Tabel 5. 21 Daftar Temuan *Security Misconfiguration* unpas.dev dan kpta.unpas.dev

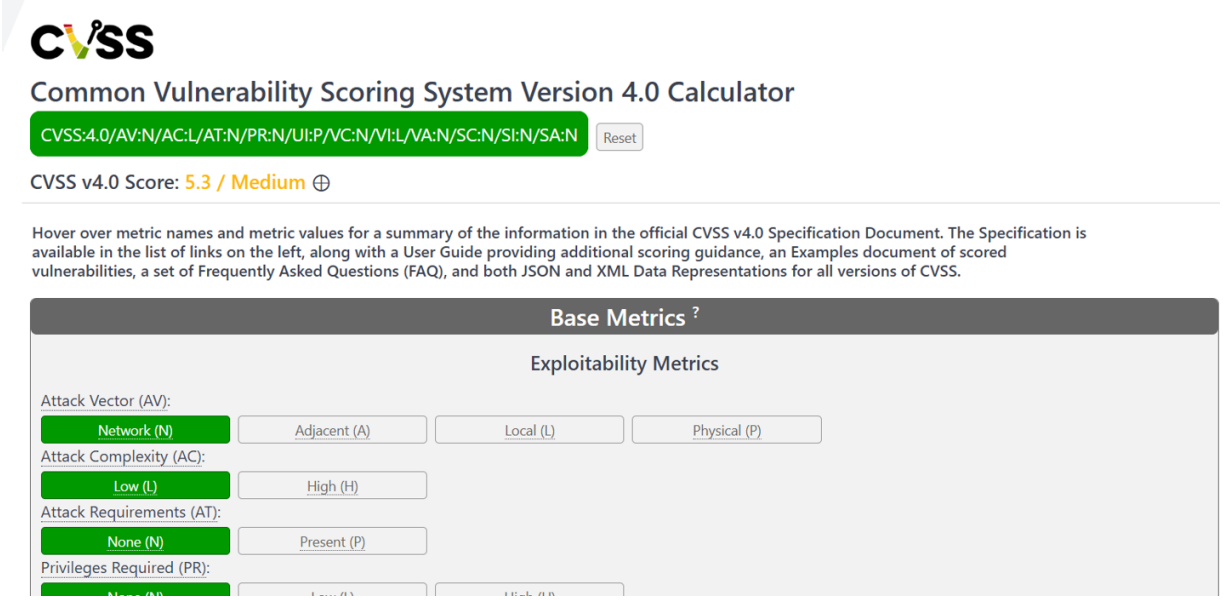
Kode	Temuan	Host	Kategori	Ruang Lingkup	Metode Validasi
F-01	Laravel Debug Mode aktif (APP_DEBUG=true, APP_ENV=local), ignition debug page dapat diakses publik tanpa autentikasi	unpas.dev	Pesan error terlalu informatif	Ya	Browser GET + dirsearch
F-02	HTTP Security Headers tidak diterapkan (CSP, X-Frame-Options, HSTS, X-Content-Type-Options, Permissions-Policy)	unpas.dev, kpta.unpas.dev	*Security headers* tidak diterapkan	Ya	Curl + OWASP ZAP
F-03	Cookie sesi tanpa atribut Secure (sakti_session, kpta_session)	unpas.dev, kpta.unpas.dev	SSL/TLS terkait konfigurasi sesi	Ya	Curl + OWASP ZAP
F-04	TLS 1.0 dan TLS 1.1 masih diaktifkan	unpas.dev, kpta.unpas.dev	SSL/TLS kurang aman	Ya	Testssl.sh+enum-ciphers
F-05	File .htaccess dapat diakses publik	kpta.unpas.dev	*Configuration File Exposure*	Di luar	Dirsearch+curl
F-06	*Subresource Integrity* (SRI) tidak diterapkan pada resources CDN eksternal	unpas.dev	*Software Supply Chain Failures*	Di luar	OWASP ZAP
F-07	Referensi subdomain usang sadaya.unpas.dev pada konfigurasi OAuth	unpas.dev	Auth/Subdomain Takeover	Di luar	OWASP ZAP (Passive Observation)

5.5.2 Penilaian Risiko CVSS v4.0

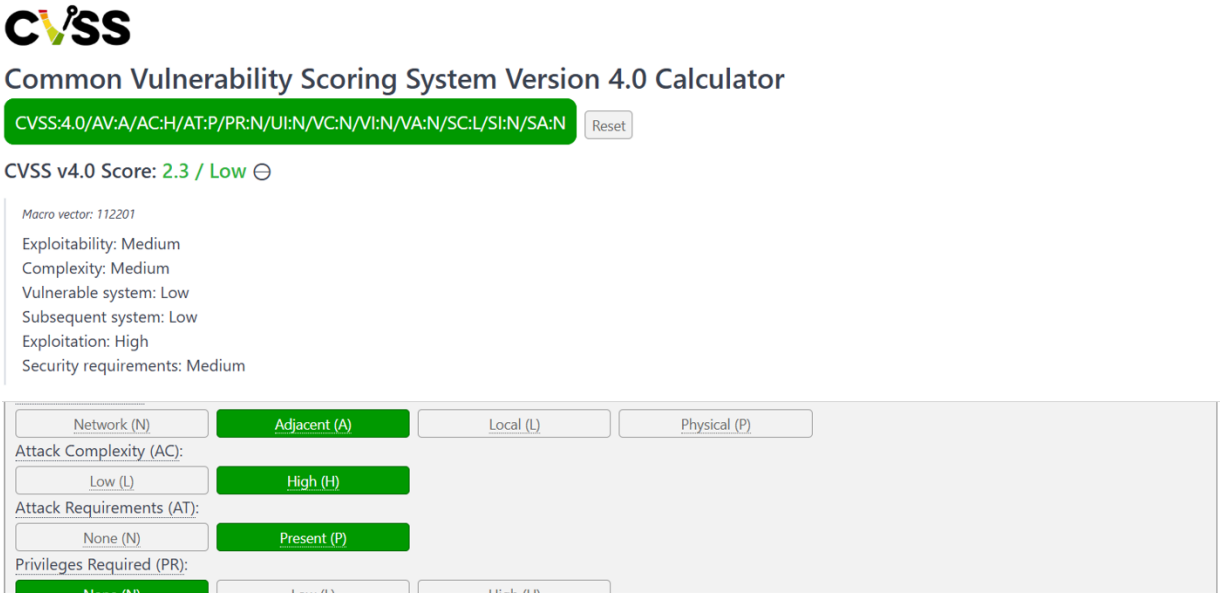
Penilaian risiko dilakukan menggunakan standar CVSS versi 4.0 berdasarkan estimasi *Base Metrics* yang telah disusun pada Tabel 5.20. *Vector string* untuk setiap temuan dimasukkan ke kalkulator resmi FIRST (http://www.first.org/cvss/calculator/4.0) untuk memperoleh skor akhir yang terstandarisasi.



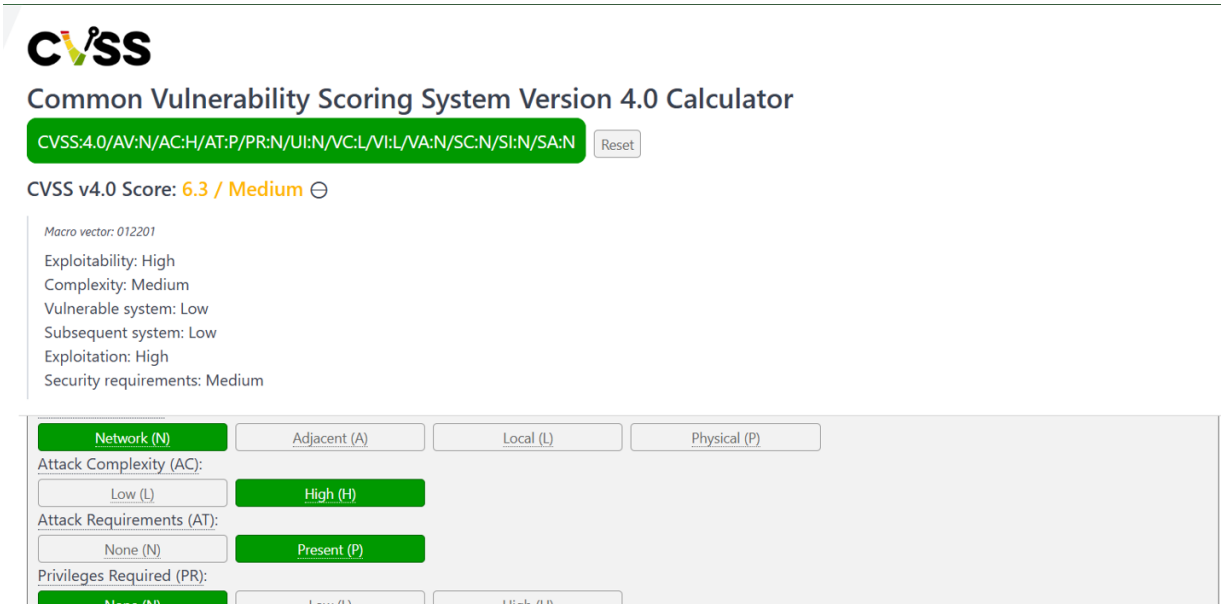
Gambar 5. 59 Kalkulasi CVSS v4.0 - F-01



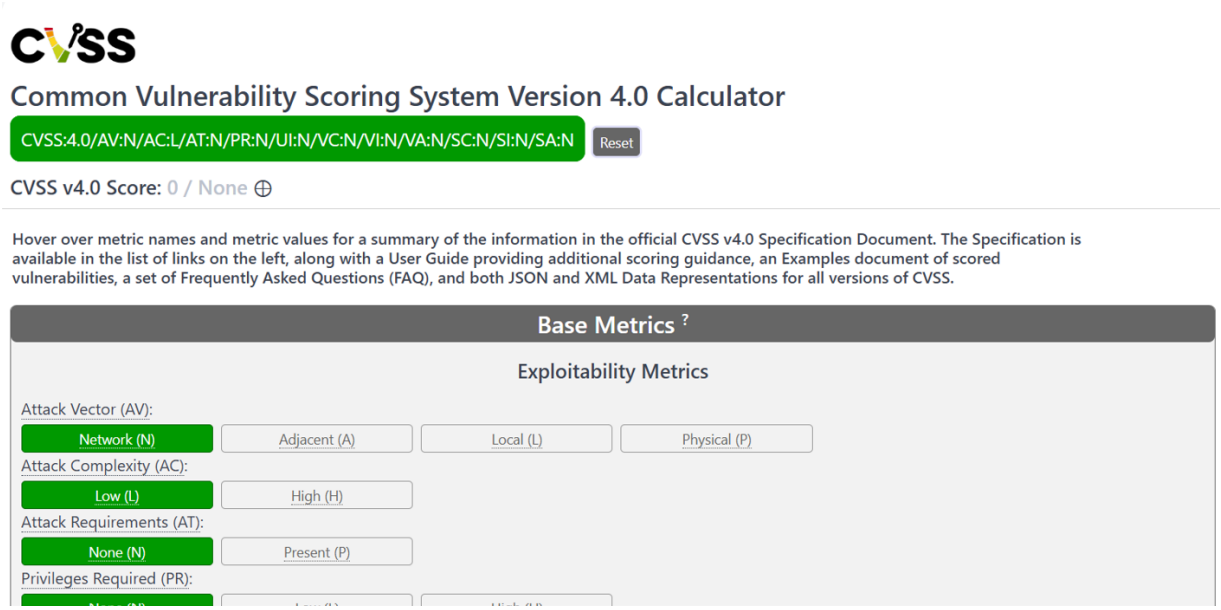
Gambar 5. 60 Kalkulasi CVSS v4.0 - F-02



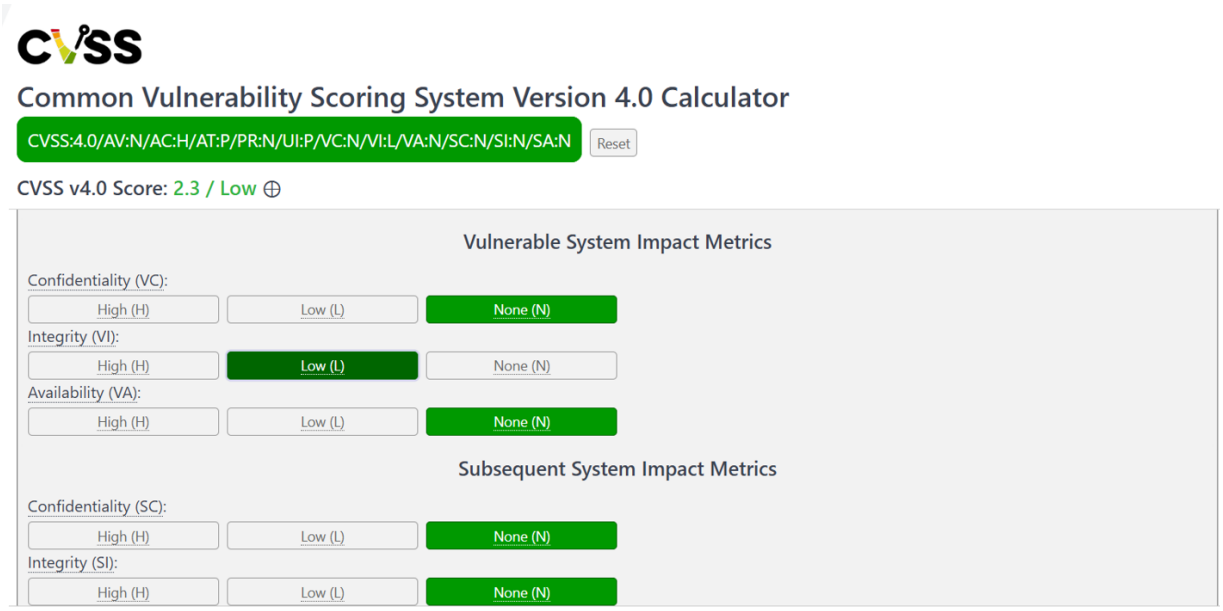
Gambar 5. 61 Kalkulasi CVSS v4.0 - F-03



Gambar 5. 62 Kalkulasi CVSS v4.0 - F-04



Gambar 5. 63 Kalkulasi CVSS v4.0 - F-05



Gambar 5. 64 Kalkulasi CVSS v4.0 - F-06

Gambar 5.59 hingga 5.64 menampilkan hasil kalkulasi CVSS v4.0 untuk masing-masing temuan menggunakan kalkulator resmi FIRST. Seluruh skor yang diperoleh dirangkum pada Tabel 5.22 berikut.

Tabel 5. 22 Penilaian Risiko CVSS v4.0 per Temuan

Kode	Vector String CVSS v4.0	Skor	Tingkat Keparahan	Ruang Lingkup
F-01	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/ SA:N	6.9	*Medium*	Ya
F-02	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/	5.3	*Medium*	Ya

Kode	Vector String CVSS v4.0	Skor	Tingkat Keparahan	Ruang Lingkup
	SA:N			
F-03	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/ SA:N	2.3	*Low*	Ya
F-04	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/ SA:N	6.3	*Medium*	Ya
F-05	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/ SA:N	0.0	*None*	Di luar
F-06	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/ SA:N	2.3	*Low*	Di luar
F-07	-	-	*Informational*	Di luar

5.5.3 Rekomendasi Perbaikan

Rekomendasi disusun berdasarkan seluruh temuan yang telah divalidasi dan dianalisis dampaknya, dengan mempertimbangkan karakteristik infrastruktur yang ditemukan selama pengujian khususnya penggunaan *Cloudflare* sebagai lapisan proxy/CDN.

5.5.3.1 Rekomendasi untuk Temuan dalam Ruang Lingkup

1. **F-01 Laravel mode Debug**

   Perbaikan utama yang harus dilakukan adalah menonaktifkan mode debug pada lingkungan produksi dengan mengubah nilai APP_DEBUG menjadi *false* dan nilai APP_ENV menjadi *production* pada konfigurasi aplikasi.

2. **F-02 HTTP *Security headers* tidak diterapkan**

   Pengelola sistem perlu menambahkan lima jenis header berikut pada respons kedua host: *Content-Security-Policy, X-Frame-options: SAMEORIGIN, X-Content-Options: nosniff, Strict-Transport-Security: max-age=31536000; includeSubdomain,* dan *Permissions-Policy*.

3. **F-03 Cookie sesi tanpa Atribut Secure**

   Pengelola sistem perlu mengaktifkan pengaturan *session secure cookie* pada konfigurasi *framework* Laravel di kedua aplikasi (unpas.dev dan kpta.unpas.dev) melalui berkas konfigurasi lingkungan aplikasi.

4. **F-04 TLS 1.0 dan TLS 1.1 Masih Aktif**

   Pengelola sistem perlu menonaktifkan dua versi protokol enkripsi lama (TLS 1.0 dan TLS 1.1) yang masih diizinkan pada koneksi HTTPS dan hanya mengizinkan versi yang lebih baru.

5.5.3.2 Rekomendasi untuk Temuan Tambahan

1. **F-05 .htaccess Dapat Diakses Publik**

   Pengelola sistem perlu memblokir akses publik terhadap berkas konfigurasi server (.htaccess) pada kpta.unpas.dev agar tidak dapat dibuka langsung melalui browser. Meskipun

berkas saat ini tidak mengandung informasi rahasia, konfigurasi seperti ini secara prinsip seharusnya tidak dapat diakses dari luar.

2. **F-06 SRI tidak diterapkan pada CDN Eksternal**

   Tambahan atribut *integrity* dan *cross origin=”anonymous” pada seluruh tag <script> dan <link> yang memuat* resource dari CDN eksternal.

3. **F-07 referensi Subdomain Usang pada Konfigurasi OAuth**

   Pengelola sistem disarankan meninjau ulang dan memperbarui pengaturan konfigurasi aplikasi ke domain aktif dan hapus URL lama yang merujuk ke sadaya.unpas.dev.

Tabel 5. 23 Ringkasan Rekomendasi Perbaikan

Kode	Rekomendasi Utama	Urgensi
F-01	Matikan mode debug	Segera
F-02	Tambahkan 5 header keamanan pada respons aplikasi	Tinggi
F-03	Aktifkan pengaturan agar cookie sesi hanya lewat HTTPS	Sedang
F-04	Matikan TLS lama, hanya izinkan versi terbaru	Sedang
F-05	Blokir akses publik ke berkas	Rendah
F-06	Tambahkan verifikasi keaslian file dari CDN eksternal	Rendah
F-07	Perbarui pengaturan login ke alamat aktif	Rendah

BAB 6
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil pengujian keamanan konfigurasi server dan layanan pada domain unpas.dev menggunakan metode *Vulnerability Assessment* berbasis PTES yang telah dilaksanakan, dapat ditarik kesimpulan sebagai berikut.

1. Pengujian terhadap dua host dalam ruang lingkup penelitian (unpas.dev dan kpta.unpas.dev) berhasil mengidentifikasi 4 temuan *Security Misconfiguration* yang tersebar pada 3 dari 7 parameter pengujian yang telah ditetapkan, yaitu pesan error informatif, *security headers*, konfigurasi SSL/TLS. Empat parameter lain, yaitu konfigurasi default, informasi layanan yang terekspos, *directory listing* dan port layanan tidak diperlukan, tidak menunjukkan adanya indikasi *Security Misconfiguration* berdasarkan ruang lingkup dan pendekatan pengujian yang digunakan. Selain itu, ditemukan 3 temuan tambahan (F-05, F-06 dan F-07) secara insidental di luar parameter *Security Misconfiguration,* yang tetap dilaporkan sebagai bagian dari tanggung jawab pengungkapan (*disclosure).*
2. Berdasarkan penilaian menggunakan CVSS v4.0, dari tujuh temuan yang diperoleh, tiga di antaranya berada pada tingkat *medium* (skor 5,3 hingga 6,9), dua pada tingkat *low*, satu dengan skor 0,0 (*none*), dan satu bersifat *informational*. Tidak ditemukan temuan dengan tingkat *HIGH* maupun *CRITICAL*, yang menunjukkan bahwa secara umum kondisi keamanan konfigurasi dari sisi publik tergolong relatif terkendali.
3. Telah disusun rekomendasi teknis perbaikan untuk seluruh temuan yang dikelompokkan berdasarkan tingkat urgensinya.

Dengan demikian, ketiga rumusan masalah yang ditetapkan pada subbab 1.3 telah terjawab melalui rangkaian pengujian yang dilaksanakan secara sistematis menggunakan kerangka kerja PTES dengan *black-box testing* dan non-destruktif hingga tahap Vulnerability Analysis.

6.2 Saran

Berdasarkan hasil penelitian yang telah dilaksanakan, terdapat beberapa saran yang dapat disampaikan baik bagi pengelola sistem domain unpas.dev maupun bagi penelitian selanjutnya.

Bagi pengelola sistem, disarankan untuk segera menindaklanjuti rekomendasi perbaikan yang telah disusun pada tabel 5.23, dengan prioritas utama pada penanganan temuan F-01 (Laravel mode debug) mengingat tingkat risikonya yang paling tinggi di antara temuan lainnya.

Bagi peneliti selanjutnya, mengingat penelitian ini dibatasi pada kategori *Security Misconfiguration* dengan *black-box testing* dan non-destruktif, beberapa subdomain yang teridentifikasi selama proses *Intelligence Gathering* namun berada di luar lingkup penelitian ini, khususnya git.unpas.dev yang berpotensi menjalankan layanan kontrol versi yang dapat menjadi

objek penelitian lanjutan untuk dianalisis lebih dalam. Penelitian selanjutnya juga dapat memperluas cakupan kategori pengujian di luar *Security Misconfiguration*, seperti *Broken Access Control* atau *Injection*, mengingat OWASP Top 10 Tahun 2025 mencakup seluruh kategori risiko yang lebih luas. Selain itu, penelitian dengan pendekatan *grey-box* atau *white-box* dapat dipertimbangkan untuk memperoleh gambaran kerentanan yang lebih menyeluruh khususnya pada area yang memerlukan autentikasi yang tidak tercakup dalam penelitian ini.

DAFTAR PUSTAKA

[CLOa] Cloudflare, "What is a CDN?", tersedia: 10 Juni 2026, https://www.cloudflare.com/learning/cdn/what-is-a-cdn/, 10 Juni 2026.

[CLOb] Cloudflare, "What is a Reverse Proxy? | Proxy Servers Explained", tersedia: 10 Juni 2026, https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/, 10 Juni 2026.

[DEW26] Dewi, I. R., "Komdigi Jawab Isu Data 13 Universitas di Indonesia Bocor", tersedia: Januari 2026, https://www.cnbcindonesia.com/tech/20260123101312-37-704671/komdigi-jawab-isu-data-13-universitas-di-indonesia-bocor, 23 Januari 2026.

[FTU26] Fakultas Teknik Universitas Pasundan, "Fakultas Teknik Universitas Pasundan", tersedia: Mei 2026, https://teknik.unpas.ac.id/, Mei 2026.

[FIR23] FIRST.Org, Inc., "Common Vulnerability Scoring System Version 4.0", FIRST.Org, Inc., Cary, North Carolina, 2023.

[HAR23] Harahap, A. H., Andani, C. D., Cristie, A., Nurhaliza, D., Fauzi, A., "Pentingnya Peranan CIA Triad dalam Keamanan Informasi dan Data untuk Pemangku Kepentingan atau Stakeholder", Jurnal Manajemen dan Pemasaran Digital, hal. 73-83, 2023.

[IBM26] IBM, "What is Penetration Testing?", tersedia: 20 April 2026, https://www.ibm.com/think/topics/penetration-testing, 20 April 2026.

[IET21] Internet Engineering Task Force (IETF), "RFC 8996: Deprecating TLS 1.0 and TLS 1.1", tersedia: Maret 2021, https://datatracker.ietf.org/doc/rfc8996/, Maret 2021.

[ISO22a] ISO/IEC, "Information Security, Cybersecurity and Privacy Protection — Information Security Controls", tersedia: 2022, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en, 2022.

[ISE10] Institute for Security and Open Methodologies (ISECOM), "Open Source Security Testing Methodology Manual (OSSTMM) 3.0", tersedia: 2010, https://www.isecom.org/OSSTMM.3.pdf, 2010.

[JOI20] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2020.

[LIS24] Listartha, I. E., Saskara, G. J., "Pengujian Keamanan dengan Metode Penetration Testing Execution Standard (PTES) untuk Menemukan Kerentanan Misconfigurations pada Perangkat Jaringan", Jurnal Elektro Lucea, hal. 1-9, November 2024.

[MCK19] McKay, K. A., Cooper, D. A., "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2019.

[MIT26] MITRE, "CWE-209: Generation of Error Message Containing Sensitive Information", tersedia: April 2026, https://cwe.mitre.org/data/definitions/209.html, 30 April 2026.

[NIS12] National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2012.

[NIS17] National Institute of Standards and Technology (NIST), "An Introduction to Information Security", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2017.

[NAT24] National Vulnerability Database, "Vulnerability Metrics", tersedia: Mei 2026, https://nvd.nist.gov/vuln-metrics/cvss, 27 Juni 2024.

[OWAa] OWASP Foundation, "Clickjacking Defense Cheat Sheet", tersedia: 10 Juni 2026, https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html, 10 Juni 2026.

[OWAb] OWASP Foundation, "HTTP Security Response Headers Cheat Sheet", tersedia: 20 April 2026, https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html, 20 April 2026.

[OWA25] OWASP Foundation, "OWASP Top 10:2025", tersedia: 2025, https://owasp.org/Top10/2025/, 2025.

[OWAc] OWASP Foundation, "Penetration Testing Methodologies", tersedia: 10 Juni 2026, https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies, 10 Juni 2026.

[PTE14] Penetration Testing Execution Standard (PTES), "Main Page", tersedia: Agustus 2014, http://www.pentest-standard.org/index.php/Main_Page, 16 Agustus 2014.

[SCA09] Scarfone, K., Hoffman, P., "Guidelines on Firewalls and Firewall Policy", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2009.

[SAF23] Safitra, M. F., Lubis, M., Widjajarto, A., "Security Vulnerability Analysis Using Penetration Testing Execution Standard (PTES): Case Study of Government's Website", Proceedings of the 6th International Conference on Electronics, Communications and Control Engineering (ICECC 2023), ACM, hal. 139-145, 2023.

[SCA08a] Scarfone, K., Jansen, W., Tracy, M., "Guide to General Server Security", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2008.

[SCA08b] Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A., "Technical Guide to Information Security Testing and Assessment (SP 800-115)", National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2008.

[SUG13] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif, dan R&D", Alfabeta, Bandung, 2013.

[UTA24] Utama, F. P., Nurhadi, R. M., "Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method", CommIT Journal, Jilid 18, Nomor 1, hal. 39-51, 2024.

[WHI22] Whitman, M. E., Mattord, H. J., "Principles of Information Technology", Edisi 7, Cengage Learning, Boston, 2022.

[YUW26] Yuwono, Y. Y., Ferdiansyah, D., Muttaqin, M. F., "Analisis Keamanan Website Universitas Pasundan Menggunakan Metode Penetration Testing Berbasis Kerangka Kerja PTES", Pasinformatik, Jilid 5, Nomor 1, Januari 2026, tersedia: https://journal.unpas.ac.id/index.php/pasinformatik/article/view/42058/22584

LAMPIRAN

LAMPIRAN A
BUKTI DOKUMEN WAWANCARA

A.1Bukti Wawancara

WAWANCARA PENELITIAN

Disusun oleh:

Nama Peneliti	Muhamad Rizki Maulana
NPM	223040167
Program Studi	Teknik Informatika
Fakultas	Teknik
Universitas	Universitas Pasundan
Tahun	2026

Identitas Narasumber:

Nama Narasumber	Wanda Gusdya P., S.T., M.T.
Jabatan/Posisi	Pengelola domain unpas.dev
Instansi	Fakultas Teknik, Universitas Pasundan
Waktu Wawancara	26 Februari 2026
Tempat Wawancara	Zoom Meeting

Saya yang bertanda tangan di bawah ini menyatakan bahwa informasi yang tercantum dalam dokumen ini benar dan telah sesuai dengan keterangan yang saya berikan pada saat sesi wawancara. Saya telah meninjau isi ringkasan hasil wawancara ini dan menyatakan bahwa data tersebut dapat digunakan sebagai lampiran untuk kepentingan akademik dan penyusunan Tugas Akhir.

Bandung, 11 Mei 2026

Narasumber	Peneliti
(Wanda Gusdya P., S.T., M.T.)	(Muhamad Rizki Maulana)
NIDN. 0430048803	NPM. 223040167

TANYA JAWAB WAWANCARA

Peneliti	Sejak kapan domain unpas.dev mulai digunakan sebagai layanan akademik aktif?
Narasumber	Domain unpas.dev mulai digunakan sekitar bulan Maret 2024.
Peneliti	Layanan apa saja yang dikelola melalui domain unpas.dev?
Narasumber	Domain unpas.dev digunakan untuk mendukung berbagai layanan akademik di Fakultas Teknik, seperti layanan remedial, semester sisipan, penilaian dosen oleh sejawat, *whistleblowing*, serta KPTA.
Peneliti	Apakah penggunaan layanan unpas.dev mencakup seluruh fakultas di Universitas Pasundan?
Narasumber	Penggunaan utama unpas.dev berada di lingkungan Fakultas Teknik, khususnya Program Studi Teknik Informatika. Namun, beberapa layanan seperti remedial dan semester sisipan juga ditawarkan untuk digunakan oleh fakultas lain.
Peneliti	Apakah domain unpas.dev berada pada lingkungan produksi?
Narasumber	Ya, domain unpas.dev berada pada lingkungan produksi.
Peneliti	Apakah selama penggunaan unpas.dev pernah terjadi gangguan layanan atau insiden keamanan?
Narasumber	Selama penggunaan unpas.dev belum pernah terjadi insiden keamanan maupun gangguan layanan. Namun, pada sistem sebelumnya pernah terjadi beberapa serangan, seperti database diretas hingga seluruh tabel terhapus akibat port MySQL 3306 terbuka ke publik. Selain itu pernah terjadi kasus deface website akibat lemahnya validasi upload file dan konfigurasi hak akses file pada server.
Peneliti	Menurut Bapak, seberapa penting aspek keamanan konfigurasi server dalam menjaga stabilitas layanan akademik?
Narasumber	Keamanan konfigurasi server sangat penting. Pengalaman sebelumnya menunjukkan bahwa konfigurasi yang kurang baik dapat menyebabkan berbagai serangan dan celah keamanan pada sistem.
Peneliti	Apakah sebelumnya pernah dilakukan pengujian terhadap konfigurasi server pada unpas.dev?
Narasumber	Hingga saat ini belum pernah dilakukan pengujian terhadap konfigurasi server pada unpas.dev.
Peneliti	Apakah terdapat tantangan dalam proses pembaruan sistem maupun pengamanan layanan pada unpas.dev?
Narasumber	Tantangan sebelumnya lebih banyak ditemukan pada sistem lama yang masih menggunakan CodeIgniter 3 dan PHP versi 5. Untuk mengatasi hal tersebut, sistem sempat dipindahkan menggunakan Docker agar beberapa versi aplikasi tetap dapat berjalan secara bersamaan. Namun, pada unpas.dev saat ini belum terdapat kendala yang berarti karena sistem masih relatif baru dan terus diperbarui.
Peneliti	Apakah terdapat kekhawatiran terkait potensi akses tidak sah maupun kebocoran data pada unpas.dev?
Narasumber	Kekhawatiran terhadap potensi akses tidak sah maupun kebocoran data tetap ada karena sistem terhubung langsung dengan internet publik dan berkaitan dengan layanan akademik.
Peneliti	Apakah evaluasi konfigurasi server perlu dilakukan secara berkala sebagai langkah preventif?
Narasumber	Evaluasi konfigurasi server penting dilakukan secara berkala karena berkaitan dengan keamanan layanan akademik.

Lampiran A. 1 Bukti Wawancara

LAMPIRAN B
BUKTI PERSETUJUAN IZIN PENGUJIAN

B.1 Bukti Persetujuan Izin Pengujian

UNIVERSITAS PASUNDAN
Fakultas Teknik

Teknik Industri 022 - 2019335
Teknologi Pangan 022 - 2019339
Teknik Mesin 022 - 2019352
Teknik Informatika 022 - 2019371
Teknik Lingkungan 022 - 2009574
Perencanaan Wilayah dan Kota 022 - 2006466

No : 306/Unpas.FT.D1/Q/V/2026
Lampiran : -
Perihal : Ijin Penelitian di Server Internal Fakultas Teknik

Kepada Yth
Pimpinan Prodi Teknik Informatika

Assalamualaikum Wr. Wb
Sampurasuun,

Alhamdulillahirabbil alamiin, kita semua di Fakultas Teknik senantiasa terlimpahi Rahmat dan karunia dariNya. Semoga kita diberi kemampuan untuk mensyukuri setiap aliran Rahman Rahim-Nya.

Terkait surat dari Prodi Teknik Informatika tentang permohonan ijin pelaksanaan skripsi tentang **" Testing tingkat keamanan konfigurasi server dan layanan di unpas.dev"** oleh :

Nama :Muhamad Rizki Maulana
Npm : 223040167

Maka bersama ini, kami dari Bidang Belmawabud mengijinkan kepada mahasiswa tersebut untuk melaksanakan aksi uji coba serangan ke server unpas.dev dengan tetap berpegang pada kaidah menjaga keamanan data dan layanan. Kami berharap, hasil ujicoba berupa temuan dan rekomendasi bisa disampaikan kepada Fakultas Teknik c.q Wadek Belmawabud

Demikian informasi ini kami sampaikan, semoga bisa menjadi perhatian dan ditindaklanjuti sebagaimana mestinya.

Waalaikumsalam Wr. Wb

Bandung, 13 Mei 2026
Wakil Dekan Bidang I Pembelajaran, Kemahasiswaan, Alumni, Riset, Agama dan Budaya,

Dr. Ririn Dwi Agustin, ST., MT
NUPTK. 1163749650230103

Tembusan
1. Pembimbing Tugas Akhir
2. Koordinator Belmawabud Teknik Informatika

Lampiran B. 1 Bukti Persetujuan Izin Pengujian