RANCANG BANGUN *SMART DOOR LOCK* BERBASIS PENGENALAN WAJAH

Sub Judul:

EVALUASI KEAMANAN *ROLE-BASED ACCESS CONTROL (RBAC)* DAN MITIGASI *BROKEN ACCESS CONTROL* MENGGUNAKAN METODE *IP WHITELISTING* DAN PENGUATAN *SESSION MANAGEMENT* PADA APLIKASI WEB MONITORING SMART DOOR LOCK

SKRIPSI

Maria Intan Prety Stefani

2207421044

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

EVALUASI KEAMANAN *ROLE-BASED ACCESS CONTROL (RBAC)* DAN MITIGASI *BROKEN ACCESS CONTROL* MENGGUNAKAN METODE *IP WHITELISTING* DAN PENGUATAN *SESSION MANAGEMENT* PADA APLIKASI WEB MONITORING SMART DOOR LOCK

SKRIPSI

Dibuat untuk Melengkapi Syarat – Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

Maria Intan Prety Stefani

2207421044

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama	:	Maria Intan Prety Stefani
Nim	:	2207421044
Jurusan	:	Teknik Informatika dan Komputer
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Evaluasi Keamanan *Role-Based Access Control (RBAC)* dan Mitigasi *Broken Access Control* Menggunakan Metode *IP Whitelisting* dan Penguatan *Session Management* pada Aplikasi Web Monitoring *Smart Door Lock*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjukan sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila dikemudian hari terbukti atau dapat dibuktikan dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 29 Juni 2026

Yang membuat pernyataan,

(Maria Intan Prety Stefani)

Nim. 2207421044

LEMBAR PENGESAHAAN

Skripsi diajukan oleh :

Nama	:	Maria Intan Prety Stefani
NIM	:	2207421022
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Evaluasi Keamanan *Role-Based Access Control (RBAC)* dan Mitigasi *Broken Access Control* Menggunakan Metode *IP Whitelisting* dan Penguatan *Session Management* pada Aplikasi Web Monitoring *Smart Door Lock*

Telah diuji oleh tim dalam Sidang Skripsi pada hari Kamis, Tanggal 2, Bulan Juli Tahun 2026, dan dinyatakan LULUS.

Disahkan Oleh:

Pembimbing I	Dr. Indra Hermawan, S.Kom., M.Kom.	( )
Penguji I	Maria Agustin, S.Kom., M.Kom	( )
Penguji II	Susana Dwi Yulianti, S.Kom, M.Kom.	( )
Penguji III	Asep Kurniawan, S.Pd., M.Kom.	( )

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa. Atas berkat, rahmat, dan karunia-Nya, penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Evaluasi Keamanan Role-Based Access Control (RBAC) dan Mitigasi Broken Access Control Menggunakan Metode IP Whitelisting dan Penguatan Session Management pada Aplikasi Web Monitoring Smart Door Lock".

Dalam proses penyusunan skripsi ini, penulis memperoleh banyak dukungan, bimbingan, dan bantuan dari berbagai pihak. Oleh karena itu penulis ingin menyampaikan ucapan terima kasih kepada:

1. Tuhan Yang Maha Esa atas segala kekuatan dan kemudahan yang diberikan kepada penulis.
2. Kedua orang tua yang tidak pernah putus memberikan doa dan dukungan yang senantiasa menjadi motivasi penulis dalam menyelesaikan pendidikan ini.
3. Priscilla Agnes Wijayanti, selaku kakak penulis, atas segala pengorbanan dan dukungan moral yang luar biasa, yang telah menjadi pendorong semangat terbesar selama masa perkuliahan.
4. Bapak Dr. Indra Hermawan, S.Kom., M.Kom., selaku Dosen Pembimbing atas bimbingan, arahan, dan masukan selama penyusunan skripsi.
5. M. Haikal Fadhillah dan M. Berryl Muchtada selaku rekan kelompok penulis yang bersedia bekerja sama dalam menyelesaikan skripsi ini.
6. Seluruh dosen, tenaga kependidikan, dan teman-teman di Politeknik Negeri Jakarta atas ilmu, pengalaman, dan dukungan yang diberikan. Serta seluruh pihak lain yang telah membantu dan mendukung proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan, sehingga kritik dan saran yang membangun sangat diharapkan. Semoga skripsi ini dapat memberikan manfaat dan kontribusi bagi pengembangan teknologi Internet of Things, khususnya pada sistem kontrol akses Smart Door Lock.

Depok, 29 Juni 2026

Maria Intan Prety Stefani

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama : Maria Intan Prety Stefani

Nim : 2207421044

Jurusan : Teknik Informatika dan Komputer

Program Studi : Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Evaluasi Keamanan *Role-Based Access Control (RBAC)* dan Mitigasi *Broken Access Control* Menggunakan Metode *IP Whitelisting* dan Penguatan *Session Management* pada Aplikasi Web Monitoring *Smart Door Lock*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsisaya tanpa meminta izin darisaya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 29 Juni 2026

Yang Menyatakan,

(Maria Intan Prety Stefani)

NIM. 2207421044

Evaluasi Keamanan *Role-Based Access Control (RBAC)* dan Mitigasi *Broken Access Control* Menggunakan Metode *IP Whitelisting* dan Penguatan *Session Management* pada Aplikasi Web Monitoring *Smart Door Lock*

ABSTRAK

Aplikasi web monitoring smart door lock berbasis Internet of Things (IoT) berfungsi sebagai antarmuka pengguna sekaligus pusat kendali administratif yang rentan terhadap eksploitasi Broken Access Control (BAC). Pengujian awal menunjukkan adanya inkonsistensi penerapan Role-Based Access Control (RBAC) pada antarmuka pengguna, JSON Web Token (JWT) yang tetap aktif setelah logout, tidak adanya batas waktu sesi (idle dan absolute timeout), serta belum diterapkannya pembatasan akses berbasis jaringan. Penelitian ini bertujuan mengevaluasi dan memitigasi kerentanan tersebut melalui penyelarasan RBAC pada frontend, penguatan session management, dan implementasi IP Whitelisting. Evaluasi dilakukan menggunakan metode one-group pretest-posttest berdasarkan standar OWASP ASVS versi 4.0.3 Level 2 dan pemindaian OWASP ZAP. Hasil penelitian menunjukkan peningkatan keberhasilan skenario keamanan dari 65,4% (17 dari 26 skenario) pada pretest menjadi 100% (26 dari 26 skenario) pada posttest. Pemindaian OWASP ZAP pascaimplementasi juga menunjukkan mitigasi kerentanan terkait sesi (cookie). Dengan demikian, penyelarasan RBAC, penguatan session management, dan IP Whitelisting terbukti efektif memitigasi celah Broken Access Control serta meningkatkan keamanan aplikasi web monitoring IoT tanpa mengganggu mekanisme otorisasi sistem.

Kata Kunci: *Broken Access Control, IP Whitelisting, OWASP ASVS, Role-Based Access Control, Session Management.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada sistem *smart door lock* berbasis IoT, aplikasi web tidak hanya berfungsi sebagai antarmuka pengguna, tetapi juga berperan sebagai pusat kendali (*control plane*) untuk pengelolaan sistem. Melalui aplikasi ini, pengguna dapat memantau status perangkat, melacak riwayat akses, dan mengatur konfigurasi sistem sesuai kebutuhan. Selain itu, berbagai fitur administratif dan operasional yang tersedia pada aplikasi web memungkinkan proses pengelolaan sistem menjadi jauh lebih efektif (Al-Adhim & Dewi, 2024). Karena aplikasi web memiliki kendali terhadap fungsi administratif dan data sensitif, maka aspek keamanan akses pada aplikasi web menjadi sangat krusial.

Salah satu akar permasalahan dalam keamanan aplikasi web adalah lemahnya otorisasi akses, di mana sistem tidak mampu secara akurat membedakan batasan akses antara pengguna yang sah dengan pihak yang tidak berwenang (Kusnana et al., 2025). Jika pihak yang tidak berwenang berhasil mengeksploitasi aplikasi tersebut, dampak nyatanya tidak terbatas pada kebocoran data pengguna saja, tetapi meluas hingga ancaman keamanan fisik. Secara teknis, peretas dapat mengakses fungsi administratif untuk memanipulasi konfigurasi *gateway*, mendaftarkan Face ID ilegal, atau membuka kunci pintu secara paksa melalui *dashboard* web. Kondisi ini merupakan bentuk nyata dari kerentanan *Broken Access Control* (BAC), yaitu kegagalan sistem dalam membatasi akses pengguna sesuai dengan hak yang dimilikinya (Purba, 2024).

Mengingat besarnya dampak yang dapat ditimbulkan, penerapan mekanisme keamanan yang memadai pada aplikasi web monitoring menjadi aspek yang sangat penting. Oleh karena itu, diperlukan pengujian keamanan seperti *penetration testing* untuk mengidentifikasi tingkat kerentanan sistem dan melindungi aplikasi dari potensi penyalahgunaan oleh pihak yang tidak berwenang (Muhammad et al., 2025). Selain melakukan *penetration testing*, proses evaluasi keamanan juga perlu mengacu pada standar yang terstruktur agar hasil pengujian dapat dilakukan secara

sistematis. Salah satu standar yang banyak digunakan adalah OWASP Application Security Verification Standard (ASVS). ASVS merupakan kerangka kerja untuk memverifikasi keamanan aplikasi web berdasarkan tingkat risiko melalui serangkaian kategori verifikasi yang mencakup aspek autentikasi, manajemen sesi, kontrol akses, validasi masukan, dan konfigurasi keamanan sistem. Penerapan ASVS membantu mengevaluasi apakah kontrol keamanan pada aplikasi telah diterapkan sesuai dengan tingkat keamanan yang dibutuhkan sehingga proses identifikasi kerentanan dapat dilakukan secara lebih sistematis (Kurniawan et al., 2025).

Aplikasi web *monitoring smart door lock* yang digunakan dalam penelitian ini merupakan hasil pengembangan dari penelitian sebelumnya. Secara operasional, aplikasi tersebut memang telah mampu berfungsi dengan baik sebagai pusat kendali untuk mengintegrasikan perangkat keras dan lunak. Namun, terdapat celah signifikan pada pengembangan terdahulu, yaitu fokus yang hanya terbatas pada pemenuhan kebutuhan fungsional alat. Aspek keamanan aplikasi web, khususnya pada manajemen hak akses, belum pernah dievaluasi secara mendalam. Dampak dari tidak adanya evaluasi ini akhirnya terbukti secara nyata melalui hasil pengujian awal terhadap sistem, di mana ditemukan indikasi kerentanan pada manajemen otorisasi akses.

Berdasarkan hasil pengujian, implementasi kontrol akses pada sistem belum mampu menjamin penerapan prinsip *least privilege* secara konsisten pada seluruh lapisan sistem, sehingga memunculkan kerentanan *Broken Access Control*. Selain itu, pengujian pada aspek *session management* menunjukkan bahwa token autentikasi JSON Web Token (JWT) yang telah diterbitkan tetap valid meskipun pengguna telah melakukan proses *logout*. Kondisi ini menyebabkan sesi tidak langsung berakhir, sehingga token yang seharusnya tidak lagi digunakan masih dapat dimanfaatkan selama belum mencapai masa kedaluwarsa. Hal tersebut membuka peluang terjadinya penyalahgunaan token oleh pihak yang tidak berwenang, termasuk penggunaan token milik administrator untuk mengakses sistem tanpa izin.

Aplikasi web monitoring tersebut sebenarnya telah mengimplementasikan pembagian hak akses menggunakan Role-Based Access Control (RBAC). Namun, mekanisme RBAC pada dasarnya hanya mempertimbangkan identitas pengguna dan peran yang dimiliki, sehingga kurang fleksibel dalam menerapkan kebijakan akses yang berbasis lokasi atau jaringan (Zahra & Nasution, 2025). Kondisi ini memungkinkan pihak yang tidak berwenang untuk tetap mengakses sistem apabila mereka berhasil menyalahgunakan token sesi dari jaringan luar.

Oleh karena itu, penelitian ini menerapkan mekanisme keamanan berlapis untuk memperkuat pengendalian akses pada aplikasi web monitoring Smart Door Lock. Selain melakukan evaluasi terhadap implementasi Role-Based Access Control (RBAC), penelitian ini juga menambahkan mekanisme IP Whitelisting pada aplikasi web. IP Whitelisting merupakan mekanisme pengendalian akses berbasis alamat Internet Protocol (IP-based access control) yang membatasi akses hanya pada alamat atau rentang IP tertentu yang telah diotorisasi sebelumnya (Prasetyo & Zulkarnain, 2025). Penggabungan mekanisme ini memastikan bahwa hak akses administratif tidak hanya divalidasi berdasarkan peran, tetapi juga dibatasi hanya untuk perangkat yang terhubung dari jaringan yang telah diotorisasi.

Selain itu, penelitian ini juga melakukan penguatan pada aspek session management melalui implementasi token invalidation pada JWT sehingga token yang telah digunakan tidak lagi dapat dimanfaatkan setelah pengguna melakukan proses logout. Mekanisme ini bertujuan untuk mencegah penyalahgunaan token yang masih aktif serta meningkatkan keamanan sesi dengan memastikan bahwa akses ke sistem hanya dapat dilakukan melalui sesi yang valid dan masih berlaku.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana penerapan penguatan *Session Management* serta metode *IP Whitelisting* dalam meningkatkan keamanan akses pada aplikasi web monitoring Smart Door Lock?

2. Bagaimana hasil evaluasi dan penyelarasan implementasi *Role-Based Access Control (RBAC)* antara sisi backend dan frontend dalam mendukung penerapan prinsip *least privilege?*
3. Bagaimana perbandingan hasil pengujian keamanan sebelum dan sesudah penerapan penguatan keamanan menggunakan metode *one-group pretest-posttest?*

1.3 Batasan Masalah

Agar pembahasan penelitian lebih terarah, maka batasan masalah yang diterapkan adalah:

1. Penelitian difokuskan pada penguatan keamanan aplikasi web monitoring Smart Door Lock melalui penyelarasan Role-Based Access Control (RBAC), penerapan Session Management, dan IP Whitelisting.
2. Penguatan Session Management yang diterapkan meliputi mekanisme JWT invalidation, idle timeout, dan absolute timeout.
3. Analisis dan pengujian keamanan difokuskan pada aspek Authentication, Session Management, dan Access Control berdasarkan OWASP ASVS 4.0.3 Level 2 menggunakan metode *one-group pretest-posttest*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah:

1. Menerapkan mekanisme Session Management berupa JWT invalidation, idle timeout, dan absolute timeout serta IP Whitelisting untuk meningkatkan keamanan akses administratif aplikasi web monitoring Smart Door Lock.
2. Mengevaluasi dan menyelaraskan implementasi Role-Based Access Control (RBAC) antara sisi backend dan antarmuka pengguna (frontend) untuk mendukung penerapan prinsip *least privilege.*
3. Mengukur efektivitas penerapan mekanisme keamanan melalui perbandingan hasil pengujian pretest dan posttest.

1.4.2 Manfaat

Manfaat yang diharapkan dari penelitian ini adalah:

1. Meningkatkan keamanan akses administratif aplikasi web melalui evaluasi RBAC dan kombinasi mitigasi *Session Management* serta *IP whitelisting* sebagai pendekatan *defense in depth*.
2. Terwujudnya keselarasan akses pengguna antara sisi *backend* dan *frontend* berdasarkan hasil evaluasi *Role-Based Access Control* (RBAC), sehingga meminimalisir *Broken Access Control* dan memastikan prinsip *least privilege* telah diterapkan dengan tepat.
3. Menghasilkan data hasil pengujian pretest dan posttest yang menunjukkan efektivitas mekanisme keamanan yang diterapkan. Hasil tersebut dapat digunakan sebagai dasar dalam evaluasi maupun pengembangan keamanan aplikasi web monitoring Smart Door Lock pada tahap selanjutnya.

1.5 Sistematika Penulisan

Sistematika penulisan pada penelitian ini disusun untuk memberikan gambaran mengenai alur pembahasan yang dilakukan pada setiap bab. Adapun sistematika penulisan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan yang digunakan dalam penyusunan skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini memuat landasan teori dan penelitian terdahulu yang berkaitan dengan keamanan aplikasi web, Smart Door Lock berbasis Internet of Things (IoT), Broken Access Control, Role-Based Access Control (RBAC), Session Management, IP Whitelisting, JSON Web Token (JWT), serta konsep dan teknologi lain yang mendukung penelitian.

BAB III METODE PENELITIAN

Bab ini menguraikan metode penelitian yang digunakan, meliputi rancangan penelitian, tahapan penelitian, objek penelitian, skenario pengujian, teknik pengumpulan data, serta metode analisis data yang digunakan untuk mengevaluasi efektivitas mekanisme keamanan yang diterapkan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil pengujian awal (pretest), perancangan dan implementasi mekanisme keamanan, hasil pengujian akhir (posttest), serta analisis terhadap efektivitas penerapan Role-Based Access Control (RBAC), Session Management, dan IP Whitelisting dalam memitigasi risiko Broken Access Control pada aplikasi web monitoring Smart Door Lock.

BAB V PENUTUP

Bab ini berisi simpulan yang diperoleh berdasarkan hasil penelitian serta saran yang dapat digunakan sebagai pengembangan penelitian maupun implementasi keamanan pada penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Kajian pustaka merupakan landasan teoritis yang digunakan untuk mendukung pelaksanaan penelitian serta memberikan pemahaman mengenai konsep, metode, dan teknologi yang berkaitan dengan objek penelitian. Pada penelitian ini, kajian pustaka memuat teori dan penelitian terdahulu yang relevan dengan pengembangan dan pengamanan sistem monitoring Smart Door Lock berbasis web, meliputi konsep Smart Door Lock berbasis Internet of Things (IoT), keamanan aplikasi web, autentikasi dan manajemen sesi, pembatasan akses berdasarkan alamat IP, serta standar keamanan OWASP Application Security Verification Standard (ASVS). Kajian tersebut digunakan sebagai dasar dalam menentukan kebutuhan sistem, merancang mekanisme pengamanan, serta mengevaluasi efektivitas implementasi keamanan yang diterapkan pada penelitian ini.

2.1.1 Smart Door Lock Berbasis Internet of Things (IoT)

Penggunaan kunci konvensional pada pintu dapat ditingkatkan keamanannya melalui penerapan sistem smart door lock berbasis Internet of Things (IoT) (Adidrana et al., 2022). Sistem ini memungkinkan proses seleksi terhadap pengguna yang memiliki hak akses serta mencatat setiap aktivitas akses yang terjadi pada pintu. Dalam sistem smart door lock berbasis IoT, perangkat berfungsi sebagai pengendali fisik pintu yang bertugas melakukan proses penguncian dan pembukaan berdasarkan hasil autentikasi. Data yang dihasilkan oleh perangkat, seperti status pintu dan hasil autentikasi akses, dikirimkan ke server untuk diproses dan disimpan. Selanjutnya, data tersebut dapat ditampilkan melalui aplikasi monitoring sehingga pengguna dapat memantau kondisi sistem secara real-time. Konsep ini menjadi dasar dalam pengembangan sistem monitoring smart door lock berbasis web pada penelitian ini.

2.1.2 Aplikasi Web sebagai Sistem Monitoring IoT

Aplikasi web merupakan aplikasi yang berjalan pada server dan dapat diakses melalui browser tanpa memerlukan instalasi khusus pada perangkat pengguna.

Dalam sistem smart door lock berbasis IoT, aplikasi web digunakan sebagai dashboard monitoring yang menampilkan informasi kondisi sistem secara terpusat. Melalui aplikasi web, administrator dapat memantau status pintu, melihat riwayat aktivitas akses berdasarkan hasil autentikasi, serta melakukan pengelolaan data sistem. Selain berfungsi sebagai media pemantauan, dashboard yang terintegrasi juga memungkinkan pengelolaan sistem dilakukan secara lebih efektif melalui penyediaan berbagai fitur yang mendukung operasional dan administrasi sistem (Al-Adhim & Dewi, 2024). Aplikasi web juga berfungsi sebagai antarmuka utama dalam penerapan mekanisme keamanan server, seperti autentikasi pengguna dan pembatasan akses ke halaman pengelolaan sistem. Oleh karena itu, aplikasi web menjadi komponen penting dalam mendukung pengawasan dan manajemen smart door lock secara efektif.

2.1.3 OWASP Top 10

Open Web Application Security Project (OWASP) merupakan organisasi nirlaba global yang berfokus pada peningkatan postur keamanan perangkat lunak. Kontribusi utama dari organisasi ini adalah publikasi OWASP Top 10, yaitu daftar yang diperbarui secara berkala dan memuat sepuluh kategori kerentanan keamanan aplikasi web yang paling umum terjadi (Sugara & Sriyasa, 2024). Dalam penelitian ini, kerangka kerja OWASP *Top 10* digunakan sebagai acuan dasar (kriteria kerentanan) untuk mengidentifikasi ancaman, mengevaluasi risiko, dan memprioritaskan perbaikan pada aplikasi web *monitoring smart door lock*, guna memastikan sistem terlindungi dari vektor serangan siber yang umum.

2.1.4 Broken Access Control (BAC)

Broken Access Control (BAC) saat ini menempati posisi teratas sebagai kerentanan aplikasi web paling kritis dalam daftar OWASP *Top 10*. Kerentanan ini terjadi ketika sistem gagal membatasi hak dan kewenangan pengguna secara ketat, sehingga memungkinkan pengguna biasa mengakses, mengubah, atau menghapus data yang berada di luar batas otorisasi mereka (Hamdallah, 2025). Dalam konteks aplikasi *monitoring smart door lock*, kerentanan BAC sangat berbahaya karena dapat memungkinkan *user* biasa untuk mem- *bypass* validasi guna mengakses

endpoint administratif, seperti mendaftarkan kartu RFID baru atau menghapus data pengguna lain, yang secara langsung mengancam keamanan pintu fisik. Mitigasi celah BAC inilah yang menjadi fokus utama dalam penelitian ini.

2.1.5 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) adalah model otorisasi yang memberikan izin akses berdasarkan peran (*role*) yang melekat pada akun pengguna. Metode ini menegakkan prinsip *least privilege*, di mana pengguna hanya diberikan kewenangan minimum yang diperlukan untuk menjalankan tugas fungsionalnya (Purba & Hidayasari, 2026). Pada sistem yang digunakan dalam penelitian ini, RBAC telah diterapkan untuk mengatur hak akses berdasarkan peran pengguna. Penelitian ini berfokus pada evaluasi dan penyelarasan implementasi RBAC pada sisi backend dan frontend untuk memastikan bahwa prinsip least privilege diterapkan secara konsisten serta meminimalkan risiko terjadinya *Broken Access Control.*

2.1.6 IP Whitelisting

IP Whitelisting merupakan mekanisme pengendalian akses berbasis alamat Internet Protocol (IP-based access control) yang membatasi akses hanya pada alamat atau rentang IP tertentu yang telah diotorisasi sebelumnya (Prasetyo & Zulkarnain, 2025). Dalam penelitian ini, mekanisme *IP Whitelisting* diintegrasikan ke dalam sistem *monitoring* sebagai lapisan mitigasi kedua setelah RBAC. Pengguna dengan hak akses tinggi (Super Admin, Admin, dan Operator) tidak hanya diwajibkan memberikan kredensial login yang valid, tetapi juga harus terhubung melalui jaringan (IP) yang telah didaftarkan untuk dapat mengakses fungsi-fungsi vital.akses hanya dari alamat IP tertentu yang telah terdaftar dalam daftar izin. Penerapan IP whitelisting bertujuan untuk memperkecil kemungkinan akses dari pihak tidak berwenang. Dengan membatasi akses berdasarkan alamat IP, risiko serangan dari jaringan luar dapat dikurangi. Namun, penerapan metode ini perlu disesuaikan dengan lingkungan jaringan karena perubahan alamat IP dapat mempengaruhi akses sistem. IP whitelisting diterapkan pada endpoint administratif

dengan memvalidasi alamat IP client terhadap daftar IP yang tersimpan di server sebelum request diproses.

2.1.7 Session Management dan JSON Web Token (JWT)

Session Management merupakan mekanisme untuk mengelola dan mengamankan siklus hidup interaksi pengguna dengan aplikasi web pasca-autentikasi (Kurnia & Huizen, 2026). Dalam sistem terdistribusi modern, manajemen sesi sering kali mengandalkan JSON *Web Token* (JWT) sebagai representasi otorisasi yang disematkan pada setiap *request*. Untuk memitigasi risiko pembajakan sesi (*session hijacking*) atau penggunaan ulang token (*replay attack*), penelitian ini mengimplementasikan parameter *Session Management* secara ketat. Hal ini mencakup penerapan *absolute timeout* (batas kedaluwarsa token JWT), *idle timeout* (penghentian sesi saat pengguna pasif), dan *token revocation* (invalidasi token setelah proses *logout*).

2.1.8 OWASP Application Security Verification Standard (ASVS)

OWASP *Application Security Verification Standard* (ASVS) merupakan kerangka kerja komprehensif yang berisi daftar periksa (*checklist*) kontrol keamanan untuk merancang, mengembangkan, dan memverifikasi aplikasi web yang aman (OWASP Foundation, 2025). ASVS membagi tingkat keamanan menjadi tiga level verifikasi sesuai dengan tingkat kebutuhan keamanan aplikasi (OWASP Foundation, 2025). Penelitian ini mengacu pada ASVS Level 2—yang dirancang untuk aplikasi yang menangani data sensitif atau transaksi *Business-to-Business* (B2B) (OWASP Foundation, 2025). Dalam penelitian ini, OWASP ASVS Level 2 digunakan sebagai acuan dalam penyusunan skenario pengujian serta evaluasi efektivitas penguatan keamanan yang diterapkan pada sistem.

2.1.9 OWASP Zed Attack Proxy (ZAP)

OWASP Zed Attack Proxy (ZAP) merupakan perangkat lunak *open-source* yang digunakan untuk mengidentifikasi dan mengatasi kerentanan dalam aplikasi web (Mu'min et al., 2024). ZAP bekerja dengan memposisikan dirinya sebagai *proxy* antara *browser* pengguna dan aplikasi web untuk mencegat, menganalisis, dan memodifikasi lalu lintas data. Pengujian keamanan menggunakan OWASP

ZAP bertujuan untuk menemukan kerentanan umum seperti miskonfigurasi *header HTTP*, kelemahan pada *cookie* sesi, serta celah kontrol akses secara otomatis yang dapat melengkapi proses pengujian manual.

2.1.10 Pengujian Keamanan Aplikasi Web

Septian et al. (2024) menyatakan bahwa keamanan website merupakan salah satu komponen penting yang tidak dapat diabaikan karena berkaitan dengan perlindungan data serta pencegahan akses yang tidak sah terhadap sistem. Oleh karena itu, pengujian keamanan aplikasi web bertujuan untuk mengevaluasi efektivitas mekanisme pengamanan yang diterapkan dalam sistem. Pengujian dapat dilakukan dengan pendekatan black box, di mana penguji melakukan pengujian akses tanpa mengetahui struktur internal aplikasi. Dalam penelitian ini, pengujian dilakukan menggunakan pendekatan black box melalui skenario pretest dan posttest untuk mengevaluasi efektivitas penguatan keamanan berupa penyelarasan Role-Based Access Control (RBAC), penerapan Session Management, dan IP Whitelisting dalam memitigasi risiko Broken Access Control.

2.2 Penelitian Terdahulu

Penelitian - penelitian terdahulu ini menjadi landasan teoritis sekaligus pembanding untuk mengetahui posisi dan kebaruan penelitian ini. Oleh karena itu, beberapa karya ilmiah yang relevan mengenai keamanan aplikasi web, penerapan Role-Based Access Control (RBAC), IP Whitelisting, serta evaluasi keamanan menggunakan standar OWASP Application Security Verification Standard (ASVS) dikaji sebagai acuan dalam perancangan, implementasi, dan evaluasi mekanisme keamanan yang diusulkan. Ringkasan penelitian-penelitian tersebut disajikan pada tabel berikut.

Tabel 2. 1 Penelitian Terkait

No	Penelitian	Hasil	Perbedaan
1	(Fachrudin, 2023)	Pengembangan sistem smart door lock berbasis IoT dengan fokus pada arsitektur jaringan dan sinkronisasi data antar perangkat Penelitian tidak membahas keamanan aplikasi web monitoring.	Penelitian ini menggunakan sistem smart door lock sebagai objek, tetapi berfokus mengevaluasi keamanan aplikasi, serta mengimplementasikan mitigasi *Broken Access Control*.
2	(Zahra & Nasution, 2025)	Menyimpulkan bahwa RBAC efektif dalam membatasi hak akses pengguna sesuai dengan perannya pada tingkat dasar. Namun, mekanisme tersebut memiliki kelemahan karena hanya bergantung pada validasi peran tanpa melakukan verifikasi terhadap asal jaringan koneksi pengguna.	Penelitian ini menyempurnakan pendekatan tersebut dengan menerapkan keamanan berlapis. Selain menggunakan RBAC, penelitian ini mengintegrasikan mekanisme *IP Whitelisting* untuk memblokir permintaan akses dari alamat IP yang tidak terdaftar, sehingga secara efektif menambal celah kerentanan dari jaringan luar.
3	(Kurniawan et al., 2025	Penelitian ini berfokus pada evaluasi keamanan aplikasi untuk mengidentifikasi celah kerentanan akses ilegal. Sistem yang diuji mampu menolak token JWT yang telah kedaluwarsa (*expired*). Selain	Penelitian ini tidak hanya melakukan evaluasi kerentanan (*pretest*, *posttest*, dan pemindaian OWASP ZAP), tetapi juga menerapkan perbaikan langsung pada *source code* (*IP Whitelisting*

No	Penelitian	Hasil	Perbedaan
		itu, sistem belum mendukung pembatalan sesi saat *logout* dan hanya merekomendasikan perpendekan masa aktif token (*token lifetime*) sebagai solusi mitigasi di masa depan.	dan penguatan *middleware*). Selain itu, penelitian ini menambal celah kerentanan JWT yang belum terselesaikan pada penelitian sebelumnya dengan mengimplementasikan mekanisme *JWT Invalidation* untuk mencabut hak akses token secara instan tepat saat pengguna melakukan *logout*.
4	(Prasetyo & Zulkarnain, 2025)	Penelitian berfokus pada pembatasan akses aplikasi web menggunakan IP Whitelisting untuk meningkatkan keamanan sistem. tidak menganalisis kontrol akses berbasis peran (RBAC).	Penelitian ini Mengembangkan konsep tersebut menjadi pertahanan berlapis (*defense-in-depth*). *IP Whitelisting* dikombinasikan dengan validasi RBAC, khusus untuk mengamankan fungsi administrati.

BAB III
METODE PENELITIAN

3.1 Rancangan Penelitian

Rancangan penelitian disusun sebagai pedoman dalam pelaksanaan penelitian agar proses pengumpulan, pengolahan, dan analisis data dapat dilakukan secara sistematis dan terarah sesuai dengan tujuan penelitian yang telah ditetapkan. Pada penelitian ini, rancangan penelitian mencakup pendekatan dan jenis penelitian yang digunakan, teknik pengumpulan data, serta metode analisis data yang digunakan untuk mengevaluasi efektivitas mekanisme keamanan yang diterapkan pada aplikasi web monitoring Smart Door Lock.

3.1.1 Pendekatan dan Jenis Penelitian

Penelitian ini merupakan penelitian terapan (*applied research*) dengan pendekatan kuantitatif deskriptif. Menurut Sugiyono (2024), berdasarkan tujuannya penelitian dapat diklasifikasikan menjadi penelitian dasar (*basic research*), penelitian terapan (*applied research*), dan penelitian pengembangan (*research and development*). Penelitian ini termasuk ke dalam penelitian terapan karena berfokus pada penerapan dan evaluasi mekanisme keamanan untuk menyelesaikan permasalahan praktis pada aplikasi web monitoring Smart Door Lock.

Pendekatan kuantitatif deskriptif digunakan karena penelitian ini berfokus pada pengumpulan, pengukuran, dan analisis data numerik untuk menggambarkan kondisi keamanan sistem sebelum dan sesudah penerapan mekanisme keamanan. Pendekatan ini memungkinkan data disajikan secara sistematis melalui representasi statistik sehingga pola dan perubahan kondisi keamanan sistem dapat diidentifikasi dengan lebih jelas (Andriana & Satwika, 2025).

Desain penelitian yang digunakan adalah *pre-experimental design* dengan bentuk *one-group pretest-posttest design*. Sutanto et al. (2023) menyatakan bahwa desain *one-group pretest-posttest* digunakan untuk membandingkan keadaan sebelum dan sesudah diberikan perlakuan secara lebih akurat.

$$O_1 - X - O_2$$

Keterangan:

- O_1 (Nilai *Pretest*): Observasi awal terhadap tingkat kerentanan sistem *Smart Door Lock* (yang masih menggunakan kontrol akses konvensional) sebelum diberikan perbaikan keamanan.
- X (*Treatment*): Perlakuan berupa penyelarasan *Role-Based Access Control* (RBAC), penguatan session management yang meliputi *JWT invalidation*, idle timeout, dan absolute timeout, serta penerapan *IP Whitelisting* pada aplikasi web monitoring Smart Door Lock.
- O_2 (Nilai *Posttest*): Observasi akhir untuk mengukur ulang tingkat ketahanan sistem terhadap serangan setelah mekanisme mitigasi (*treatment*) tersebut diterapkan.

3.1.2 Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini difokuskan pada perolehan data kuantitatif terkait kondisi keamanan aplikasi sebelum dan sesudah penerapan mekanisme keamanan. Data dikumpulkan melalui dua metode utama, yaitu pengujian keamanan sistem (*security testing*) dan penilaian kerentanan (*vulnerability assessment*).

Pengumpulan data dilakukan pada tahap *pretest* dan *posttest* menggunakan skenario pengujian yang sama agar hasil pengukuran dapat dibandingkan secara konsisten. Skenario pengujian disusun berdasarkan kontrol keamanan pada OWASP ASVS versi 4.0.3 Level 2 yang menjadi ruang lingkup penelitian, yaitu kategori V2 Authentication, V3 Session Management, dan V4 Access Control.

Pada tahap *pretest*, dilakukan pengujian terhadap Dashboard Smart Door Lock sebelum penerapan mekanisme keamanan untuk mengidentifikasi kerentanan yang masih terdapat pada sistem. Setelah itu, diterapkan mekanisme penguatan keamanan berupa penyelarasan Role-Based Access Control (RBAC), penerapan *session management* yang meliputi *JWT invalidation*, *idle timeout*, dan *absolute*

timeout, serta pembatasan akses administratif menggunakan IP Whitelisting sebagai perlakuan (*treatment*) dalam penelitian. Selanjutnya, dilakukan pengujian ulang (*posttest*) menggunakan skenario yang sama untuk mengevaluasi perubahan kondisi keamanan sistem setelah perlakuan diterapkan.

Pengujian manual dilakukan menggunakan Postman dan antarmuka aplikasi berdasarkan skenario pengujian yang telah disusun. Peneliti menjalankan berbagai skenario akses yang sah maupun tidak sah menggunakan akun dengan peran yang berbeda untuk mengevaluasi mekanisme autentikasi, manajemen sesi, dan kontrol akses yang diterapkan pada sistem.

Hasil pengujian dicatat berdasarkan respons yang diberikan sistem, seperti keberhasilan atau penolakan akses serta kode status HTTP yang dihasilkan, antara lain 200 OK, 401 Unauthorized, dan 403 Forbidden. Data tersebut digunakan untuk mengevaluasi kemampuan sistem dalam memberikan akses sesuai hak pengguna dan menolak akses yang tidak memiliki autentikasi maupun otorisasi yang sesuai.

Selain pengujian manual, penelitian ini juga memanfaatkan OWASP ZAP untuk melakukan *vulnerability assessment* terhadap aplikasi. Hasil pemindaian menghasilkan data kuantitatif berupa jumlah temuan kerentanan, tingkat risiko kerentanan, serta perubahan kondisi keamanan sistem sebelum dan sesudah penerapan mekanisme keamanan.

3.1.3 Teknik Analisis Data

Data yang diperoleh kemudian dianalisis dengan membandingkan hasil pengujian pada tahap *pretest* (O_1) dan *posttest* (O_2). Perbandingan dilakukan terhadap hasil *security testing* dan *vulnerability assessment* untuk mengevaluasi efektivitas mekanisme keamanan yang diterapkan pada aplikasi web monitoring Smart Door Lock.

Pada pengujian autentikasi, manajemen sesi, dan kontrol akses, analisis dilakukan berdasarkan respons yang diberikan sistem pada setiap skenario pengujian. Respons tersebut meliputi keberhasilan atau penolakan akses serta kode status HTTP yang dihasilkan, seperti 200 OK, 401 Unauthorized, dan 403 Forbidden. Hasil pengujian

digunakan untuk menentukan apakah sistem telah mampu memberikan akses sesuai dengan hak akses pengguna serta menolak akses yang tidak memiliki autentikasi maupun otorisasi yang sesuai.

Efektivitas penerapan mekanisme keamanan dianalisis berdasarkan jumlah skenario akses tidak sah yang berhasil dicegah setelah implementasi dilakukan. Tingkat keberhasilan mitigasi dihitung menggunakan persamaan berikut.

$$Persentase\ Keberhasilan = \frac{Jumlah\ skenario\ yang\ berhasil}{Jumlah\ seluruh\ skenario}\ x\ 100\%$$

Semakin tinggi persentase keberhasilan yang diperoleh pada tahap *posttest*, maka semakin efektif mekanisme keamanan yang diterapkan dalam meningkatkan keamanan akses pada aplikasi web monitoring Smart Door Lock.

Selain itu, dilakukan analisis terhadap hasil *vulnerability assessment* menggunakan OWASP ZAP dengan membandingkan jumlah *alert* dan tingkat risiko kerentanan yang ditemukan pada tahap *pretest* dan *posttest*. Penurunan jumlah kerentanan dengan tingkat risiko *High* dan *Medium* menunjukkan adanya peningkatan kondisi keamanan sistem setelah mekanisme penguatan keamanan diterapkan.

Hasil analisis keseluruhan disajikan dalam bentuk tabel rekapitulasi dan uraian deskriptif untuk memberikan gambaran mengenai efektivitas mekanisme keamanan yang diterapkan. Parameter analisis data yang digunakan dalam penelitian ini ditunjukkan pada Tabel 3.1

Tabel 3. 1 Parameter Analisis Data

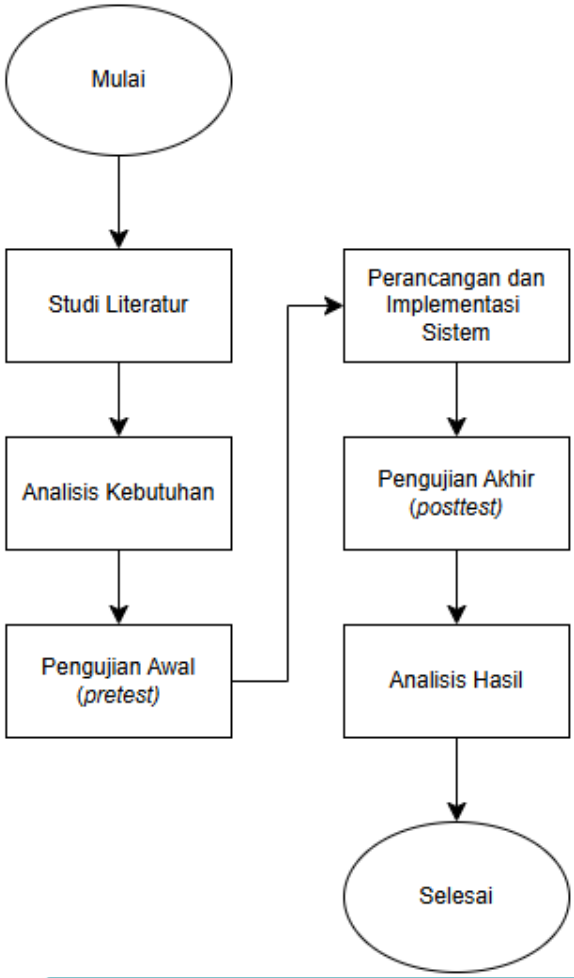
No	Aspek	Parameter	Indikator
1	Authentication	Mekanisme autentikasi dan validasi token kredensial.	Upaya akses tanpa kredensian ataupun token JWT yang valid otomatis ditolak oleh sistem.
2	Access control	Hak akses pengguna terhadap fitur dan endpoint	Akses yang tidak sesuai dengan peran (*role*) berhasil ditolak oleh sistem
3	Session Management	Logout invalidation,	Sesi pengguna berakhir

No	Aspek	Parameter	Indikator
		absolute timeout, dan idle timeout	sesuai kebijakan yang ditetapkan
4	IP Whitelisting	Pembatasan akses berdasarkan alamat IP	Akses dari IP yang tidak terdaftar berhasil ditolak
5	Vulnerability Assessment	Kerentanan keamanan aplikasi	Jumlah dan tingkat risiko kerentanan berkurang secara signifikan pada pemindaian *posttest*
6	Efektivitas pengujian	Perbandingan hasil *pretest* dan *posttest*	Persentase keberhasilan skenario pengujian pada tahap posttest lebih tinggi dibandingkan tahap pretest

Pada tabel 3.1 Analisis data pada penelitian ini mengacu pada kontrol keamanan OWASP ASVS versi 4.0.3 Level 2 yang menjadi ruang lingkup penelitian, yaitu kategori V2 Authentication, V3 Session Management, dan V4 Access Control. Selain itu, hasil *vulnerability assessment* menggunakan OWASP ZAP digunakan sebagai pendukung evaluasi keamanan melalui perbandingan jumlah dan tingkat risiko kerentanan yang ditemukan pada tahap *pretest* dan *posttest*. Efektivitas penerapan mekanisme keamanan dievaluasi berdasarkan kemampuan sistem dalam mencegah skenario akses tidak sah serta menurunkan jumlah kerentanan yang ditemukan setelah implementasi dilakukan.

3.2 Tahapan Penelitian

Tahapan penelitian dilakukan secara bertahap agar proses pengembangan sistem berjalan terstruktur.



Gambar 3. 1 Tahapan Penelitian

Pada gambar 3.1 ditunjukan tahapan penelitian yang digunakan dalam penelitian ini. Tahap pertama adalah studi literatur. Pada tahap ini dilakukan pengumpulan dan kajian berbagai referensi yang berkaitan dengan keamanan aplikasi web, khususnya mengenai Broken Access Control, Role-Based Access Control (RBAC), Session Management, IP Whitelisting, OWASP Application Security Verification Standard (ASVS), serta penelitian terdahulu yang relevan. Selain itu, dilakukan pula kajian terhadap dokumentasi dan teknologi yang digunakan pada website monitoring IoT Smart Door Lock. Hasil dari tahap ini berupa landasan teori dan pemahaman mengenai mekanisme keamanan yang akan diterapkan serta metode evaluasi yang digunakan dalam penelitian.

Tahap kedua adalah analisis kebutuhan. Pada tahap ini dilakukan identifikasi terhadap kondisi awal website monitoring IoT Smart Door Lock untuk mengetahui

mekanisme autentikasi, kontrol akses, serta pengelolaan sesi yang telah diterapkan pada sistem. Analisis dilakukan dengan mempelajari arsitektur aplikasi, fitur yang tersedia, endpoint API yang digunakan, serta hak akses yang dimiliki oleh masing-masing pengguna. Selain itu, dilakukan identifikasi terhadap potensi kelemahan yang berkaitan dengan risiko Broken Access Control, seperti kemungkinan akses terhadap fitur administratif oleh pengguna yang tidak berwenang, pengelolaan sesi yang belum optimal, serta tidak adanya pembatasan akses berdasarkan alamat IP. Hasil dari tahap ini digunakan sebagai dasar dalam menentukan mekanisme keamanan yang akan diterapkan pada sistem.

Tahap ketiga adalah pengujian awal (pretest). Pengujian dilakukan untuk memperoleh kondisi awal keamanan sistem sebelum penerapan mekanisme keamanan. Pada tahap ini dilakukan pengujian terhadap fitur dan endpoint yang berkaitan dengan kontrol akses dan pengelolaan sesi pengguna. Pengujian dilakukan berdasarkan kategori V2 Authentication, V3 Session Management, dan V4 Access Control pada OWASP ASVS versi 4.0.3 Level 2. Selain itu, dilakukan vulnerability assessment menggunakan OWASP ZAP untuk mengidentifikasi kerentanan yang terdapat pada aplikasi sebelum dilakukan implementasi mekanisme keamanan. Hasil pengujian pada tahap ini digunakan sebagai acuan untuk membandingkan kondisi sistem setelah dilakukan perbaikan.

Tahap keempat adalah perancangan dan implementasi mekanisme keamanan. Pada tahap ini dilakukan perancangan solusi mitigasi berdasarkan hasil analisis kebutuhan dan temuan kerentanan pada tahap sebelumnya. Selanjutnya, mekanisme keamanan tersebut diimplementasikan pada website monitoring IoT Smart Door Lock untuk mengurangi risiko Broken Access Control dan meningkatkan keamanan pengelolaan sesi pengguna. Mekanisme keamanan yang diterapkan meliputi penyelarasan Role-Based Access Control (RBAC), penerapan Session Management, dan IP Whitelisting. Penyelarasan RBAC dilakukan untuk memastikan bahwa pembatasan hak akses pada backend telah diterapkan secara konsisten pada seluruh lapisan sistem, termasuk antarmuka pengguna (frontend), sehingga setiap pengguna hanya dapat mengakses sumber daya sesuai dengan kewenangannya. Session Management diterapkan untuk meningkatkan keamanan

pengelolaan sesi pengguna melalui mekanisme *JWT invalidation*, *absolute timeout*, dan *idle timeout* sehingga sesi pengguna dapat dihentikan secara otomatis sesuai kebijakan yang ditentukan serta tidak dapat digunakan kembali setelah proses logout dilakukan. Sementara itu, IP Whitelisting diterapkan untuk membatasi akses terhadap akun dengan hak akses administratif sehingga hanya dapat diakses dari alamat IP yang telah terdaftar dan diotorisasi oleh sistem.

Tahap kelima adalah pengujian akhir (posttest). Pengujian dilakukan setelah seluruh mekanisme keamanan berhasil diterapkan pada sistem. Skenario pengujian yang digunakan pada tahap ini sama dengan skenario yang digunakan pada tahap pretest untuk menjaga konsistensi pengukuran. Pengujian dilakukan untuk mengevaluasi kemampuan sistem dalam membatasi akses sesuai dengan hak akses pengguna, mengelola sesi pengguna secara aman, serta mencegah akses dari sumber jaringan yang tidak terdaftar. Selain itu, dilakukan kembali vulnerability assessment menggunakan OWASP ZAP untuk mengetahui perubahan tingkat risiko kerentanan setelah implementasi mekanisme keamanan.

Tahap terakhir adalah analisis hasil pengujian. Analisis dilakukan dengan membandingkan hasil pengujian pada tahap pretest dan posttest berdasarkan indikator keberhasilan yang telah ditentukan. Analisis difokuskan pada perubahan respons sistem terhadap permintaan akses, kode status HTTP yang dihasilkan, kemampuan mekanisme keamanan dalam mencegah akses yang tidak sah, serta perubahan tingkat risiko kerentanan yang diperoleh dari hasil vulnerability assessment menggunakan OWASP ZAP. Hasil analisis tersebut digunakan untuk mengevaluasi efektivitas penerapan Role-Based Access Control (RBAC), Session Management, dan IP Whitelisting dalam memitigasi risiko Broken Access Control pada website monitoring IoT Smart Door Lock.

3.3 Objek Penelitian

Objek penelitian pada penelitian ini adalah aplikasi web monitoring Smart Door Lock berbasis Internet of Things (IoT) yang berfungsi sebagai media pengelolaan dan pemantauan sistem. Aplikasi web digunakan sebagai pusat kendali (*control plane*) yang memungkinkan pengguna melakukan autentikasi, memantau status

perangkat, mengelola data pengguna, melihat riwayat aktivitas akses, serta melakukan konfigurasi sistem sesuai dengan hak akses yang dimiliki.

Perangkat keras Smart Door Lock digunakan sebagai objek pendukung yang menghasilkan data aktivitas untuk ditampilkan dan dikelola melalui aplikasi web. Sistem ini dirancang untuk mendukung pengelolaan akses pada ruang Dosen yang berlokasi di Gedung AA, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta.

Fokus penelitian ini dibatasi secara spesifik pada aspek keamanan aplikasi web monitoring, khususnya pada mekanisme autentikasi, kontrol akses, dan pengelolaan sesi pengguna baik pada sisi server (*backend*) maupun antarmuka pengguna (*frontend*).

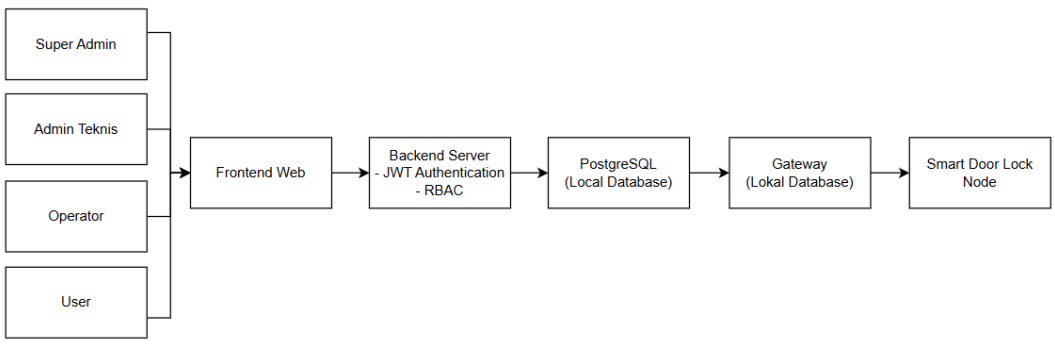
BAB IV
HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk memahami kondisi awal website monitoring IoT Smart Door Lock serta mengidentifikasi kebutuhan keamanan yang diperlukan untuk memitigasi risiko Broken Access Control. Analisis dilakukan melalui observasi terhadap arsitektur sistem, mekanisme autentikasi, kontrol akses, serta pengelolaan sesi pengguna yang telah diterapkan pada sistem. Selain itu, dilakukan identifikasi terhadap potensi kelemahan keamanan yang kemudian dipetakan berdasarkan kategori pada OWASP Application Security Verification Standard (ASVS) versi 4.0.3 Level 2 sebagai dasar dalam menentukan mekanisme keamanan yang akan diterapkan.

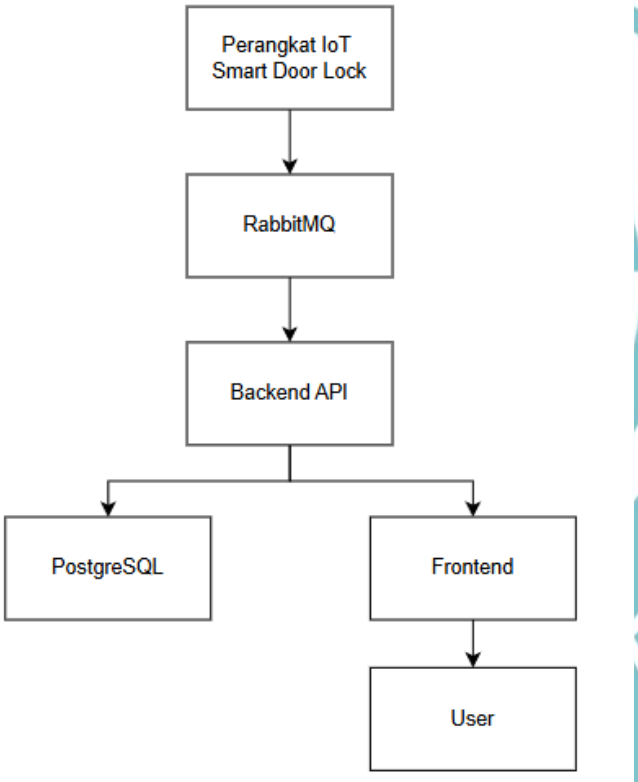
4.1.1 Analisis Sistem Berjalan

Berdasarkan hasil observasi terhadap *website* monitoring IoT Smart Door Lock, sistem ini digunakan untuk melakukan pemantauan perangkat Smart Door Lock secara *real-time* serta pengelolaan perangkat, pengguna, dan konfigurasi sistem melalui antarmuka berbasis web. Arsitektur sistem terdiri atas beberapa komponen utama, yaitu *frontend* berbasis web, *backend* API, *database* PostgreSQL, serta perangkat IoT yang berkomunikasi melalui *message broker* RabbitMQ. *Backend* berperan sebagai pusat pemrosesan data yang menangani autentikasi, otorisasi, serta logika bisnis sistem, sedangkan *database* digunakan untuk menyimpan data pengguna, perangkat, serta aktivitas sistem.



Gambar 4. 1 Arsitektur Sistem IoT Smart Door Lock

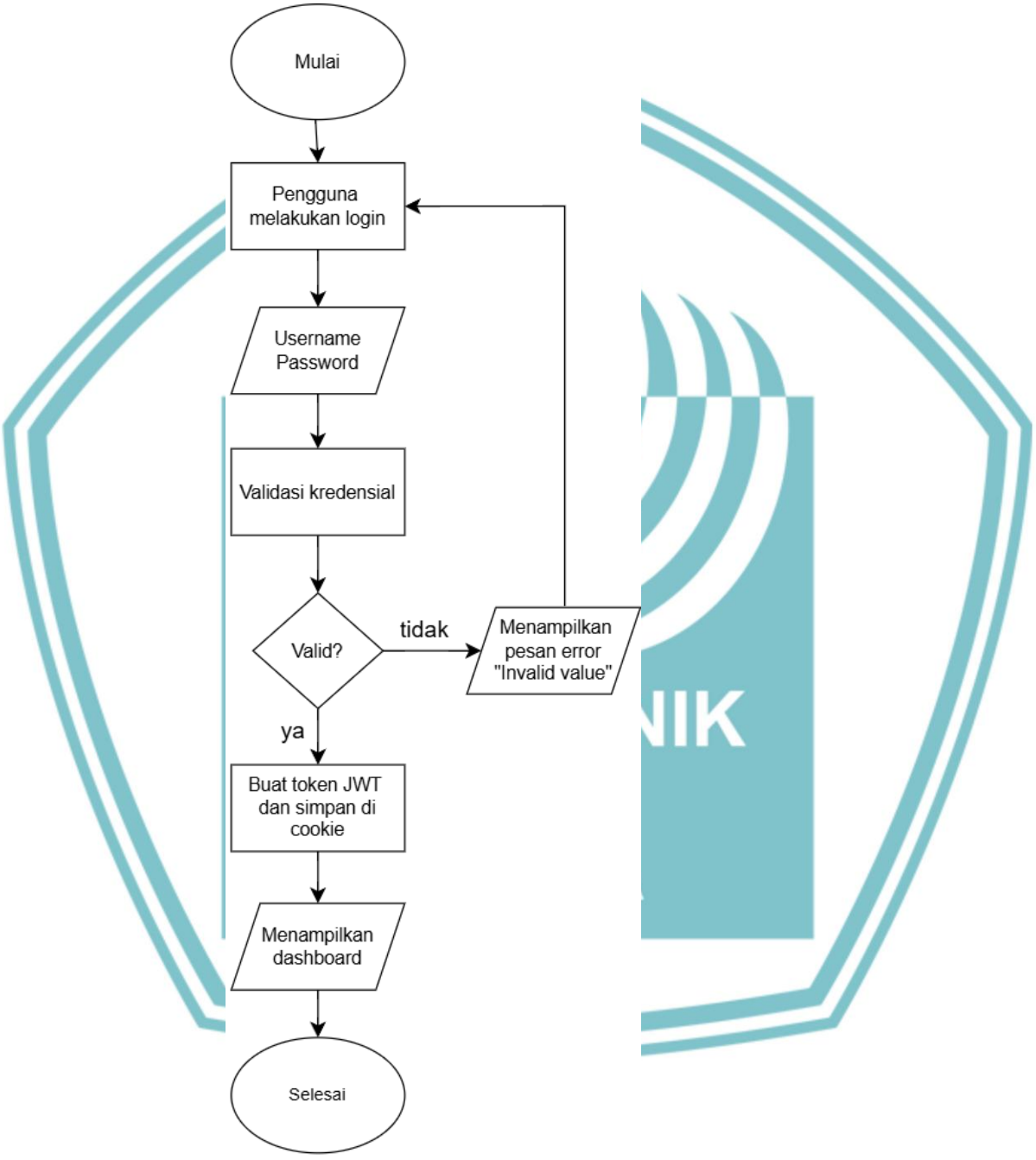
Gambar 4.1 Arsitektur Sistem IoT Smart Door Lock menunjukkan arsitektur website monitoring IoT Smart Door Lock yang digunakan pada penelitian ini. Perangkat IoT mengirimkan data status dan event melalui RabbitMQ menuju backend. Selanjutnya backend melakukan pemrosesan, validasi, serta penyimpanan data ke database PostgreSQL sebelum informasi tersebut ditampilkan pada frontend sesuai dengan hak akses pengguna.



Gambar 4. 2 Alur Komunikasi Data

Untuk memperjelas aliran komunikasi antar komponen, Gambar 4.2 menunjukkan alur komunikasi data pada sistem. Data yang dihasilkan oleh perangkat Smart Door Lock dikirimkan melalui RabbitMQ menuju *backend* API. *Backend* kemudian melakukan pemrosesan data dan menyimpannya ke dalam *database* PostgreSQL. Data yang telah tersimpan selanjutnya ditampilkan pada *frontend* sehingga dapat dipantau oleh pengguna sesuai dengan kebutuhan operasional.

Untuk dapat mengakses sistem, pengguna diwajibkan melakukan proses autentikasi menggunakan *username* dan *password*. Berdasarkan hasil analisis *source code*, sistem menerapkan mekanisme autentikasi berbasis *JSON Web Token* (JWT).



Gambar 4. 3 Alur Mekanisme Login

Gambar 4.3 menunjukkan mekanisme autentikasi yang diterapkan pada sistem. Proses dimulai ketika pengguna memasukkan username dan password melalui

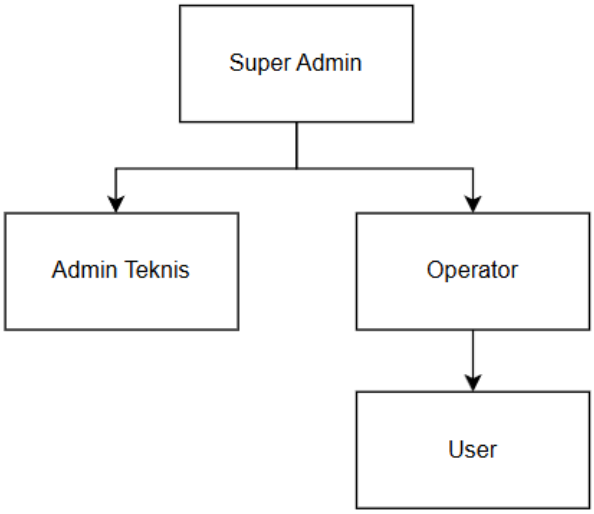
halaman login. Backend kemudian melakukan validasi kredensial terhadap database. Apabila proses autentikasi berhasil, sistem menghasilkan JSON Web Token (JWT) yang berisi identitas dan role pengguna. Token tersebut disimpan pada browser melalui cookie dan digunakan sebagai identitas pengguna pada setiap request menuju backend.

Selain autentikasi, sistem juga menerapkan Role-Based Access Control (RBAC) sebagai mekanisme otorisasi untuk membatasi akses ke endpoint yang dilindungi berdasarkan peran pengguna.

Gambar 4. 4 Mekanisme RBAC

Gambar 4.4 menunjukkan mekanisme otorisasi RBAC yang dijalankan pada sisi backend setelah pengguna berhasil melakukan autentikasi. Proses dimulai ketika pengguna mengirimkan request menuju endpoint atau fitur yang dilindungi, baik melalui antarmuka web maupun alat pengujian seperti Postman. Middleware otorisasi kemudian mengekstrak identitas pengguna dari token JWT, mengambil informasi role pengguna dari basis data, dan membandingkannya dengan role yang dipersyaratkan oleh endpoint yang diakses. Apabila role sesuai, sistem memberikan akses ke endpoint tersebut. Sebaliknya, apabila role tidak sesuai, sistem mengembalikan respons penolakan akses (*Forbidden*).

Sistem menerapkan empat jenis role pengguna, yaitu Super Admin, Admin Teknis, Operator, dan User. Masing-masing role memiliki fungsi dan hak akses yang berbeda sesuai dengan kebutuhan operasional sistem.



Gambar 4. 5 Struktur Role

Gambar 4.5 menunjukkan struktur role yang diterapkan pada sistem. Super Admin memiliki hak akses penuh terhadap seluruh fitur yang tersedia. Admin Teknis bertanggung jawab terhadap pengelolaan konfigurasi serta perangkat tertentu. Operator memiliki hak akses yang lebih terbatas untuk mendukung aktivitas operasional, sedangkan User merupakan pengguna umum yang hanya dapat

mengakses data yang berkaitan dengan dirinya sendiri. Pembagian hak akses masing-masing role ditunjukkan pada Tabel 4.1.

Tabel 4. 1 Hak Akses Berdasarkan Role

Fitur	Super Admin	Admin Teknis	Operator	User
Dashboard	Allow	Allow	Allow	Deny
Card List	Allow	Deny	Allow	Deny
User List	Allow	Deny	Allow	Deny
Room	Allow	Allow	Allow	Deny
Building	Allow	Deny	Deny	Deny
Hardware	Allow	Allow	Deny	Deny
Api Key	Allow	Allow	Deny	Deny
Gateway Device	Allow	Allow	Deny	Deny
Gateway Spot	Allow	Allow	Deny	Deny
User card	Allow	Deny	Allow	Allow

Tabel 4.1 menunjukkan pembagian hak akses yang diterapkan pada setiap role dalam sistem. Super Admin memiliki akses penuh terhadap seluruh fitur yang tersedia, sedangkan Administrator Teknis dan Operator hanya diberikan akses terhadap fitur tertentu sesuai kebutuhan operasional. Pembagian hak akses ini menjadi dasar implementasi RBAC yang digunakan untuk membatasi akses terhadap sumber daya sistem.

Berdasarkan hasil analisis sistem, website monitoring IoT Smart Door Lock telah menerapkan mekanisme autentikasi berbasis JSON Web Token (JWT) dan mekanisme otorisasi menggunakan Role-Based Access Control (RBAC) sebagai kontrol keamanan dasar. Selain itu, akses pengguna pada sistem masih bergantung pada validitas token autentikasi dan hak akses berdasarkan role yang dimiliki. Sistem belum menerapkan mekanisme pembatasan akses berdasarkan alamat IP pengguna sebagai lapisan keamanan tambahan.

Oleh karena itu, diperlukan identifikasi dan evaluasi lebih lanjut terhadap implementasi kontrol keamanan yang diterapkan untuk mengetahui potensi kerentanan yang masih terdapat pada sistem.

4.1.2 Identifikasi Kelemahan Keamanan

Berdasarkan hasil observasi dan analisis terhadap implementasi website monitoring IoT Smart Door Lock, diketahui bahwa sistem telah menerapkan mekanisme autentikasi menggunakan JSON Web Token (JWT) dan mekanisme otorisasi berbasis Role-Based Access Control (RBAC). Meskipun demikian, beberapa aspek keamanan masih memerlukan evaluasi lebih lanjut untuk memastikan efektivitas pengendalian akses yang diterapkan.

Dari aspek pengelolaan sesi pengguna, sistem masih mengandalkan validitas access token sebagai dasar autentikasi. Konfigurasi masa berlaku token serta mekanisme penghentian sesi secara otomatis perlu dievaluasi untuk memastikan bahwa sesi pengguna dikelola secara aman dan mampu meminimalkan risiko penyalahgunaan sesi.

Dari aspek kontrol akses, diperlukan evaluasi terhadap konsistensi penerapan hak akses pada seluruh lapisan sistem, baik pada backend maupun antarmuka pengguna. Selain itu, pembatasan akses berdasarkan sumber koneksi pengguna juga belum diterapkan sebagai lapisan keamanan tambahan bagi akun dengan hak akses administratif.

Berdasarkan hasil identifikasi tersebut, terdapat beberapa aspek keamanan yang perlu dilakukan pengujian lebih lanjut sebagaimana ditunjukkan pada Tabel 4.2

Tabel 4. 2 Aspek Keamanan yang Perlu Dievaluasi

No	Aspek	Tujuan
1	Authentication	Memastikan hanya pengguna yang valid yang dapat mengakses website
2	Session Management	Memastikan pengelolaan sesi pengguna dilakukan secara aman
3	Access Control	Memastikan hak akses pengguna diterapkan

No	Aspek	Tujuan
		secara konsisten

Tabel 4.2 menunjukkan bahwa aspek yang memerlukan evaluasi lebih lanjut terutama berkaitan dengan Authentication, Session Management, dan Access Control yang memiliki hubungan dengan risiko Broken Access Control. Oleh karena itu, aspek-aspek tersebut selanjutnya dipetakan ke dalam kontrol keamanan OWASP Application Security Verification Standard (ASVS) versi 4.0.3 Level 2 sebagai dasar dalam penyusunan skenario pengujian keamanan dan implementasi penguatan keamanan pada tahap berikutnya.

4.1.3 Pemetaan Aspek Keamanan terhadap OWASP ASVS

Pada penelitian ini digunakan standar keamanan OWASP Application Security Verification Standard (ASVS) versi 4.0.3 sebagai acuan dalam melakukan evaluasi dan pengujian keamanan sistem. OWASP ASVS merupakan kerangka kerja yang menyediakan sekumpulan kontrol keamanan yang dapat digunakan untuk memverifikasi tingkat keamanan aplikasi secara sistematis.

Penelitian ini menerapkan OWASP ASVS Level 2 karena Dashboard Smart Door Lock merupakan aplikasi berbasis web yang mengelola data autentikasi pengguna, data perangkat, serta fungsi administrasi yang memiliki tingkat risiko menengah. Level 2 dipilih karena ditujukan untuk aplikasi yang memproses data sensitif dan memerlukan penerapan mekanisme keamanan yang lebih kuat dibandingkan aplikasi dengan risiko rendah.

Berdasarkan karakteristik sistem dan hasil identifikasi aspek keamanan yang memerlukan evaluasi lebih lanjut pada website monitoring IoT Smart Door Lock, dilakukan pemetaan terhadap kategori verifikasi pada OWASP Application Security Verification Standard (ASVS) versi 4.0.3 Level 2.

Tabel 4. 3 Pemetaan Temuan Keamanan terhadap OWASP ASVS

ASVS	Kategori	Relevansi terhadap Sistem
V2	Authentication	Memastikan proses autentikasi pengguna

ASVS	Kategori	Relevansi terhadap Sistem
		dilakukan secara aman sehingga hanya pengguna yang memiliki kredensial yang valid yang dapat memperoleh akses ke sistem.
V3	Session Management	Memastikan pengelolaan sesi pengguna dilakukan secara aman untuk mencegah penyalahgunaan sesi dan risiko session hijacking.
V4	Access Control	Memastikan pengguna hanya dapat mengakses fitur dan layanan sesuai dengan hak akses yang dimiliki, termasuk pembatasan akses berbasis role maupun pembatasan akses berbasis jaringan melalui IP Whitelisting.

Berdasarkan hasil pemetaan pada Tabel 4.3, pengujian pada penelitian ini difokuskan pada kategori V2 Authentication, V3 Session Management, V4 Access Control. Ketiga kategori tersebut dipilih karena memiliki keterkaitan langsung dengan mekanisme keamanan yang diterapkan pada website monitoring IoT Smart Door Lock, yaitu mekanisme autentikasi berbasis JSON Web Token (JWT), Session Management, Role-Based Access Control (RBAC), serta IP Whitelisting. Hasil pemetaan ini selanjutnya digunakan sebagai dasar dalam penyusunan skenario pengujian keamanan pada tahap *pretest* dan *posttest*.

4.2 Pengujian Awal (Pretest)

Pada tahap ini dilakukan pengujian awal (pretest) untuk mengetahui kondisi keamanan website monitoring IoT Smart Door Lock sebelum diterapkannya mekanisme penguatan keamanan. Pengujian ini bertujuan untuk memperoleh baseline keamanan sistem yang kemudian digunakan sebagai pembanding terhadap hasil setelah implementasi perbaikan.

Pengujian dilakukan menggunakan beberapa metode, yaitu pengujian antarmuka pengguna, pengujian Role-Based Access Control (RBAC) pada backend menggunakan Postman, pengujian Session Management, serta vulnerability assessment menggunakan OWASP ZAP.

4.2.1 Pretest Authentication

Pengujian authentication dilakukan untuk mengevaluasi mekanisme autentikasi yang diterapkan pada website monitoring IoT Smart Door Lock. Pengujian ini mengacu pada kategori OWASP ASVS V2 – Authentication yang berfokus pada verifikasi identitas pengguna serta memastikan bahwa hanya pengguna yang memiliki kredensial yang valid yang dapat memperoleh akses ke sistem.

Tujuan pengujian ini adalah untuk memastikan bahwa proses autentikasi berjalan dengan benar, pengguna dengan kredensial yang valid dapat berhasil melakukan login, sedangkan pengguna yang memberikan kredensial tidak valid atau menggunakan token yang telah dimodifikasi akan ditolak oleh sistem.

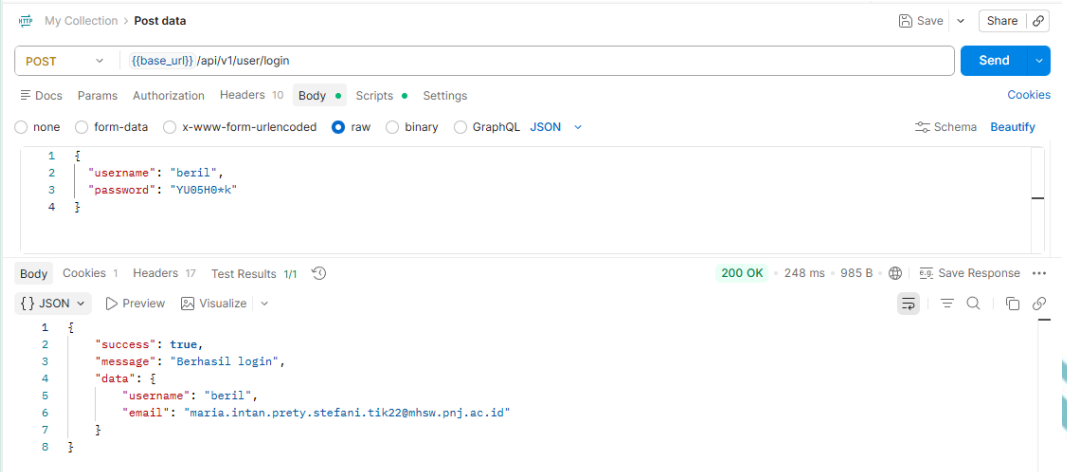
Hasil pengujian authentication disajikan pada Tabel 4.4

Tabel 4. 4 Hasil Pretest Authentication

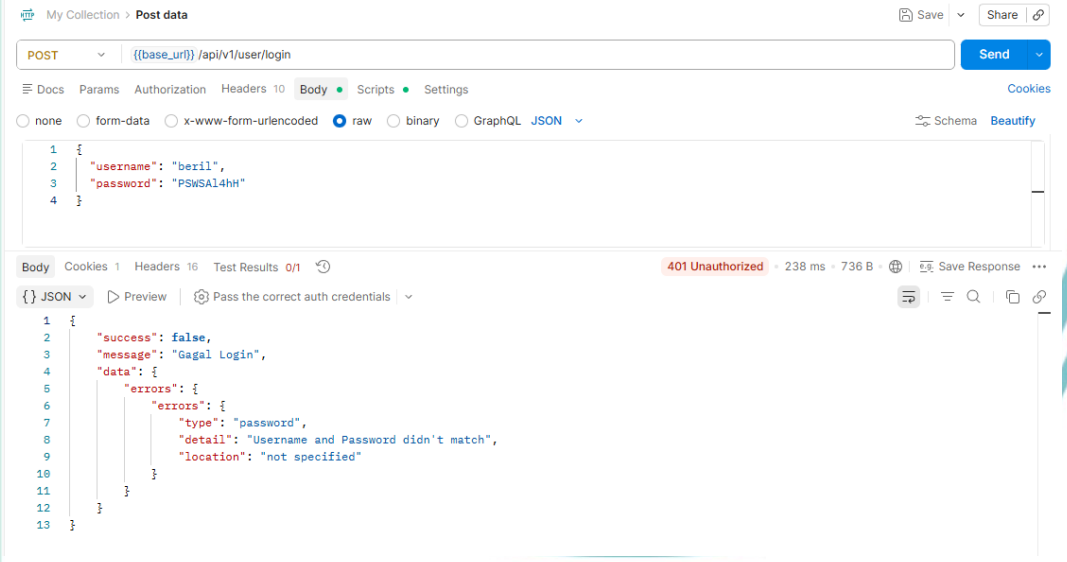
No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Melakukan login dengan username dan password benar	Login berhasil	Sistem menerima akses (200 OK)	Sesuai
2	Melakukan login dengan password salah	Login gagal	Ditolak (401 Unauthorized)	Sesuai
3	Melakukan login dengan username tidak terdaftar	Login gagal	Ditolak (401 Unauthorized)	Sesuai
4	Mengakses endpoint menggunakan JWT yang telah dimodifikasi	Sistem menolak akses	Ditolak (401 Unauthorized)	Sesuai

Berdasarkan Tabel 4.4, seluruh skenario pengujian menunjukkan hasil yang sesuai dengan mekanisme autentikasi yang diterapkan pada sistem. Pengguna yang memasukkan username dan password yang benar berhasil memperoleh akses ke sistem, sedangkan percobaan login menggunakan password yang salah, username yang tidak terdaftar, maupun penggunaan JSON Web Token (JWT) yang telah dimodifikasi berhasil ditolak oleh sistem dengan respons 401 Unauthorized.

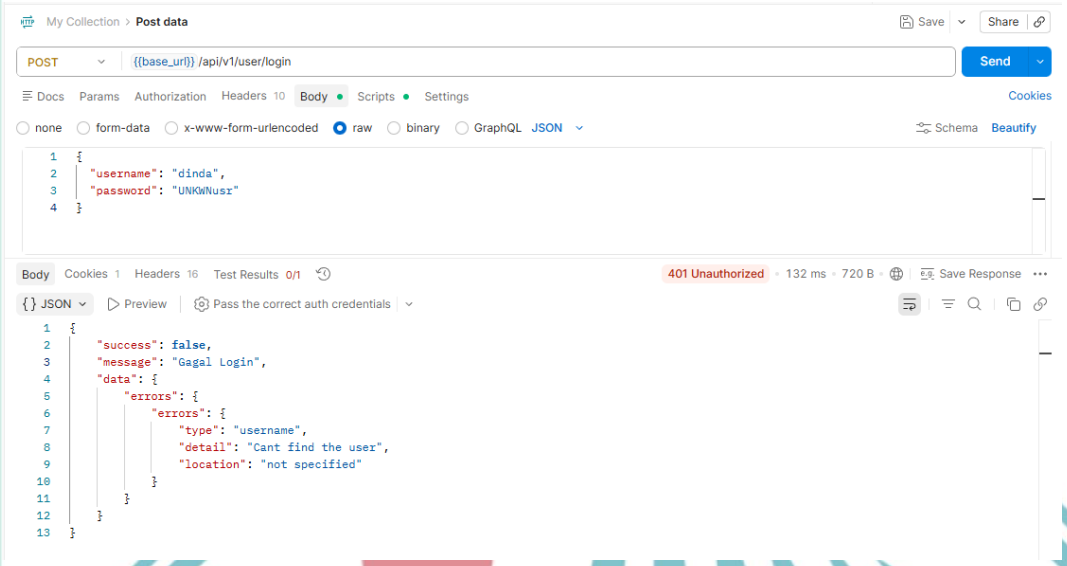
Untuk memperjelas pelaksanaan pengujian, dokumentasi pengujian ditunjukkan pada Gambar 4.6 hingga Gambar 4.9



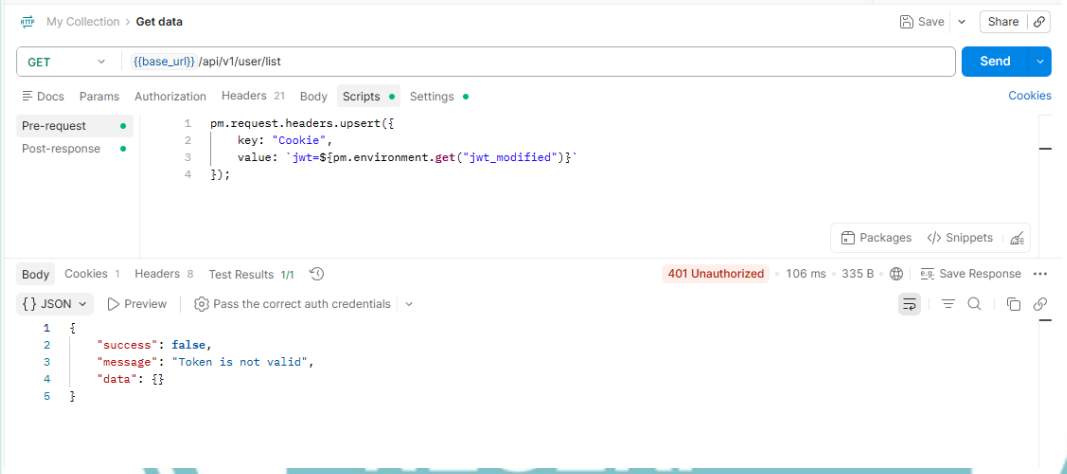
Gambar 4. 6 Login dengan username dan password benar



Gambar 4. 7 Login dengan password salah



Gambar 4. 8 Login dengan username tidak terdaftar



Gambar 4. 9 Akses Endpoint dengan JWT Modifikasi

Gambar 4.7 hingga Gambar 4.10 menunjukkan hasil pengujian mekanisme autentikasi pada website monitoring IoT Smart Door Lock. Pengujian dilakukan menggunakan beberapa skenario, yaitu login menggunakan kredensial yang valid, login dengan password yang salah, login dengan username yang tidak terdaftar, serta akses ke endpoint menggunakan JSON Web Token (JWT) yang telah dimodifikasi. Hasil pengujian menunjukkan bahwa sistem berhasil memberikan akses kepada pengguna dengan kredensial yang sah melalui respons **200 OK**, sedangkan percobaan autentikasi yang tidak valid dan penggunaan token yang telah dimodifikasi berhasil ditolak dengan respons **401 Unauthorized**. Hasil tersebut

menunjukkan bahwa mekanisme autentikasi pada sistem telah berjalan sesuai dengan yang diharapkan dan mampu mencegah akses dari pengguna yang tidak terotorisasi.

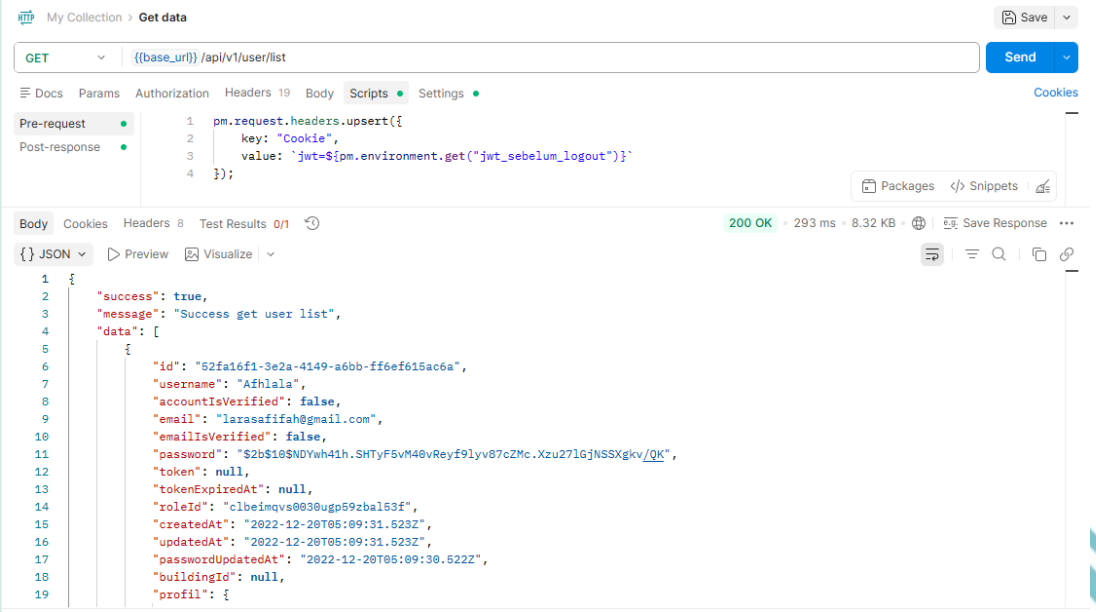
4.2.2 Pretest Session Management

Tujuan pengujian ini adalah untuk memastikan bahwa token autentikasi tidak dapat digunakan kembali setelah logout, token yang telah kedaluwarsa tidak dapat digunakan kembali, serta sistem memiliki mekanisme pengendalian masa aktif sesi yang memadai untuk mengurangi risiko penyalahgunaan akun. Selain itu, pengujian juga dilakukan untuk mengevaluasi keberadaan mekanisme penghentian sesi otomatis ketika pengguna tidak melakukan aktivitas dalam jangka waktu tertentu. Hasil pengujian menunjukkan bahwa sistem belum memiliki mekanisme idle timeout, sehingga sesi pengguna tetap aktif meskipun tidak terdapat aktivitas dalam periode waktu yang lama.

Tabel 4. 5 Hasil Pretest Session Management

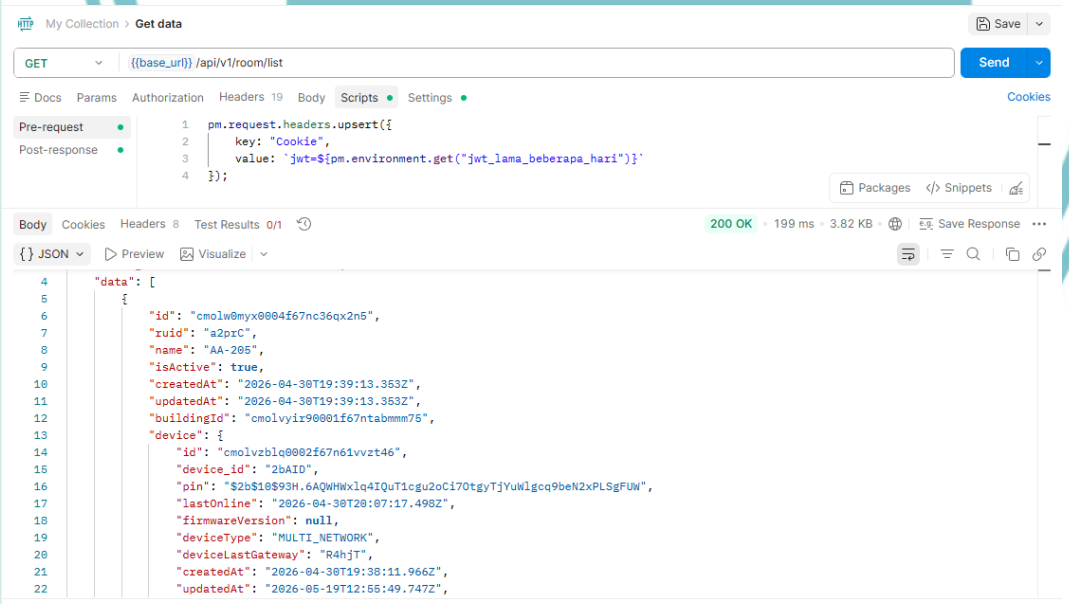
No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Mengakses sistem menggunakan token lama setelah logout	Sistem menolak akses	Sistem menerima akses (200 OK)	Tidak Sesuai
2	Menggunakan token setelah periode penggunaan yang lama	Token telah expired	Token masih valid (200 OK)	Tidak Sesuai
3	Membiarkan sesi tanpa aktivitas dalam periode tertentu	Sistem melakukan logout otomatis	Sesi tetap aktif dan tidak terjadi logout otomatis	Tidak Sesuai

Berdasarkan Tabel 4.5 hasil pengujian session management. Dari hasil tersebut ditemukan bahwa sebagian mekanisme pengelolaan sesi belum berjalan secara optimal.



Gambar 4. 10 Penggunaan Token Lama Setelah Logout

Gambar 4.11 menunjukkan bahwa token yang diperoleh sebelum proses logout masih dapat digunakan untuk mengakses endpoint yang dilindungi, meskipun sesi pengguna telah diakhiri. Hal ini menunjukkan bahwa sistem belum melakukan invalidasi token setelah logout.



Gambar 4. 11 Penggunaan Token Setelah Periode Penggunaan yang Lama

Gambar 4.12 berikutnya menunjukkan bahwa token masih dapat digunakan setelah periode penggunaan yang lama, yang mengindikasikan bahwa masa berlaku token

cukup panjang dan belum didukung mekanisme pengendalian sesi tambahan seperti idle timeout atau absolute timeout.

Berdasarkan hasil pengujian, ditemukan dua kelemahan utama pada mekanisme session management, yaitu tidak adanya invalidasi token setelah logout serta masa berlaku token yang relatif panjang tanpa mekanisme pembatasan sesi tambahan.

Kondisi ini berpotensi meningkatkan risiko penyalahgunaan token apabila token berhasil diperoleh oleh pihak yang tidak berwenang. Meskipun demikian, sistem telah berhasil menerapkan validasi signature JWT dengan baik, sehingga token yang dimodifikasi tidak dapat digunakan untuk mengakses sistem.

Dengan demikian, permasalahan yang ditemukan bukan berasal dari kelemahan validasi token, melainkan dari pengelolaan siklus hidup sesi setelah token diterbitkan.

4.2.3 Pretest Access Control

Pengujian access control dilakukan untuk mengevaluasi penerapan pembatasan akses pada website monitoring IoT Smart Door Lock berdasarkan role pengguna yang telah ditetapkan. Pengujian ini mengacu pada OWASP Application Security Verification Standard (ASVS) V4 – Access Control yang menekankan penerapan prinsip least privilege, sehingga setiap pengguna hanya dapat mengakses fitur dan sumber daya sesuai dengan hak akses yang dimilikinya.

Pengujian dilakukan pada dua lapisan sistem, yaitu antarmuka pengguna (frontend) dan backend. Pengujian pada frontend bertujuan untuk mengevaluasi kesesuaian tampilan menu dan fitur berdasarkan role pengguna, sedangkan pengujian pada backend dilakukan untuk memastikan bahwa setiap endpoint hanya dapat diakses oleh pengguna yang memiliki hak akses yang sesuai.

4.2.3.1 Pretest Access Control pada Antarmuka Pengguna

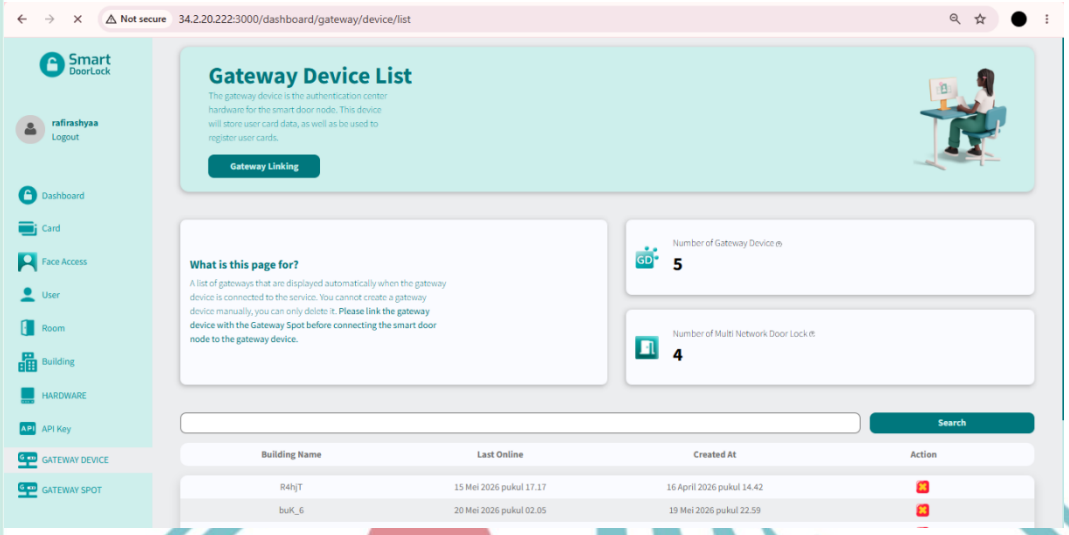
Pengujian ini dilakukan untuk mengevaluasi implementasi role-based rendering pada antarmuka pengguna. Hasil pengujian access control pada antarmuka pengguna disajikan pada Tabel 4.6.

Tabel 4. 6 Hasil Pretest Access Control pada Antarmuka Pengguna

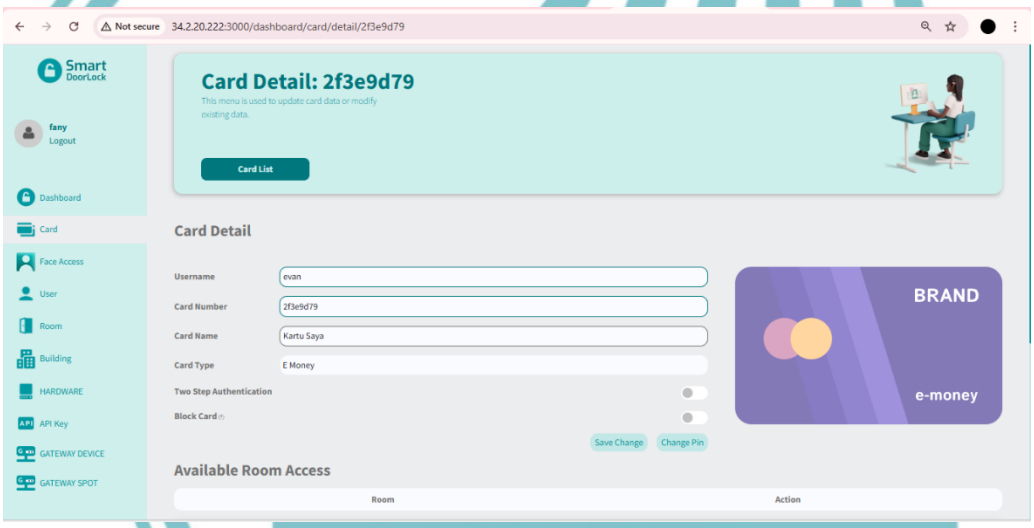
No	Role	Skenario	Hasil yang diharapkan	Hasil aktual	Status
1	Guest	Mengakses dashboard tanpa login	Redirect ke halaman login	Redirect ke halaman login	Sesuai
2	User	Akses kartu milik sendiri	Data kartu tampil	Data kartu tampil	Sesuai
3	Super admin	Mengakses seluruh menu administratif	Seluruh menu dapat ditampilkan	Seluruh menu dapat ditampilkan	Sesuai
4	Admin Teknis	Mengakses menu sesuai hak akses	Hanya menu Admin Teknis yang ditampilkan	Menu sesuai hak akses dapat diakses, namun terdapat menu Super Admin pada sidebar	Tidak sesuai
5	Operator	Mengakses menu sesuai hak akses	Hanya menu Operator yang ditampilkan	Menu sesuai hak akses dapat diakses, namun terdapat menu Super Admin pada sidebar	Tidak sesuai

Berdasarkan Tabel 4.6, sebagian besar fitur pada antarmuka pengguna telah ditampilkan sesuai dengan hak akses masing-masing role. Namun demikian, masih ditemukan ketidaksesuaian pada implementasi role-based rendering, yaitu munculnya menu yang seharusnya hanya dapat diakses oleh Super Admin pada akun Admin Teknis dan Operator. Kondisi tersebut menunjukkan bahwa prinsip least privilege pada sisi antarmuka pengguna belum diterapkan secara konsisten.

Untuk memperjelas temuan yang diperoleh, dokumentasi hasil pengujian ditunjukkan pada Gambar 4.13 dan Gambar 4.14



Gambar 4. 12 Menu Super Admin Tampil pada Role Admin Teknis



Gambar 4. 13 Menu Super Admin Tampil pada Role Operator

Gambar 4.13 hingga 4.14 menunjukkan adanya kebocoran menu administratif pada antarmuka pengguna, di mana menu Super Admin masih ditampilkan pada role Administrator Teknis dan Operator meskipun tidak memiliki hak akses terhadap fitur tersebut. Kondisi ini menunjukkan bahwa implementasi role-based rendering pada sisi frontend belum sepenuhnya konsisten

Meskipun demikian, temuan tersebut tidak secara langsung menyebabkan akses tidak sah terhadap endpoint backend karena mekanisme RBAC pada sisi server masih diterapkan dengan baik. Namun, kondisi tersebut berpotensi memberikan informasi mengenai fitur administratif yang tersedia pada sistem serta dapat

memengaruhi pengalaman pengguna. Oleh karena itu, diperlukan penyelarasan implementasi kontrol akses antara frontend dan backend agar kebijakan access control dapat diterapkan secara konsisten pada seluruh lapisan sistem.

4.2.3.2 Pretest Role-Based Access Control (RBAC)

Pengujian Role-Based Access Control (RBAC) dilakukan untuk mengevaluasi mekanisme pembatasan akses pada sisi backend berdasarkan role pengguna. Pengujian dilakukan menggunakan Postman untuk memastikan bahwa setiap endpoint hanya dapat diakses oleh pengguna yang memiliki hak akses yang sesuai.

Pengujian RBAC dilakukan menggunakan beberapa endpoint yang dipilih secara representatif berdasarkan matriks hak akses yang diterapkan pada sistem. Pemilihan endpoint dilakukan untuk mewakili berbagai kombinasi role dan sumber daya yang memiliki tingkat hak akses berbeda, sehingga mekanisme pembatasan akses dapat dievaluasi tanpa harus menguji seluruh endpoint yang tersedia

Hasil pengujian RBAC pada backend menggunakan Postman disajikan pada Tabel 4.7.

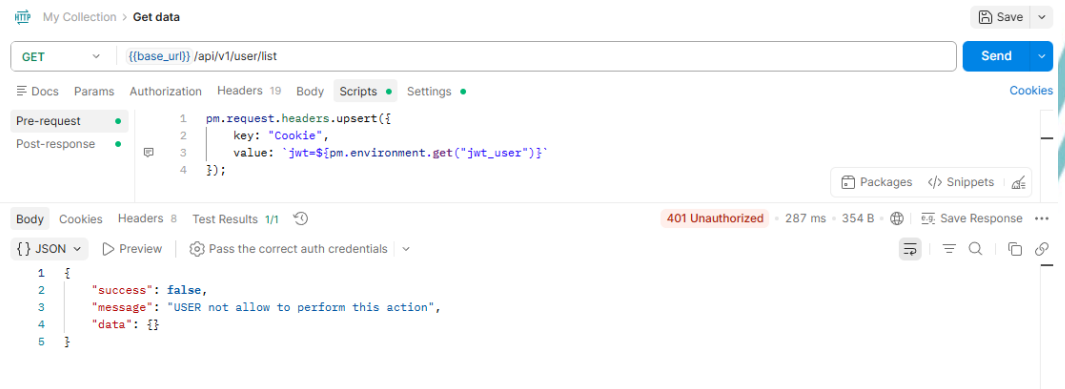
Tabel 4. 7 Hasil Pretest Role-Based Access Control

No	Skenario Pengujian	Endpoint	Hasil yang diharapkan	Hasil aktual	Status
1	User mengakses User List	/api/v1/user/list	Ditolak	Ditolak (401 Unauthorized)	Sesuai
2	User biasa mencoba membuka card list	/api/v1/card/unavailable	Ditolak	Ditolak (401 Unauthorized)	Sesuai
3	User biasa mencoba membuka room list	/api/v1/room/list	Ditolak	Ditolak (401 Unauthorized)	Sesuai
4	Operator mengakses Gateway Device	/api/v1/gateway/device/general-information	Ditolak	Ditolak (401 Unauthorized)	Sesuai
5	Operator mencoba membuka gateway spot	/api/v1/gateway/general-information	Ditolak	Ditolak (401 Unauthorized)	Sesuai

No	Skenario Pengujian	Endpoint	Hasil yang diharapkan	Hasil aktual	Status
6	Operator mencoba membuka Building List	/api/v1/building/general-information	Ditolak	Ditolak (401 Unauthorized)	Sesuai
7	Admin Teknis mengakses User List	/api/v1/user/list	Ditolak	Ditolak (401 Unauthorized)	Sesuai
8	Admin Teknis mencoba membuka Building List	/api/v1/building/general-information	Ditolak	Ditolak (401 Unauthorized)	Sesuai
9	Admin Teknis mencoba membuka card list	/api/v1/card/unavailable	Ditolak	Ditolak (401 Unauthorized)	Sesuai

Berdasarkan Tabel 4.7, seluruh skenario pengujian menunjukkan hasil yang sesuai dengan kebijakan akses yang telah ditetapkan. Seluruh percobaan akses terhadap endpoint administratif oleh pengguna yang tidak memiliki hak akses berhasil ditolak oleh sistem.

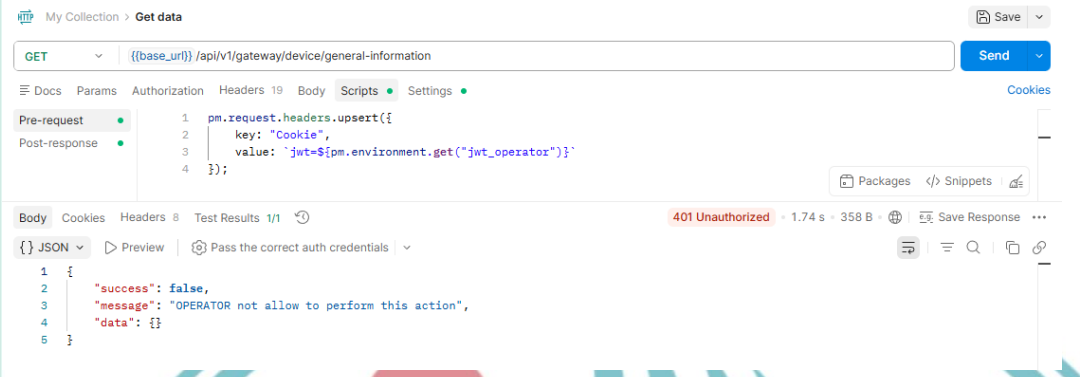
Untuk memperjelas pelaksanaan pengujian, dokumentasi beberapa skenario pengujian representatif ditunjukkan pada Gambar 4.14 hingga Gambar 4.18.



Gambar 4. 14 User Mengakses User List

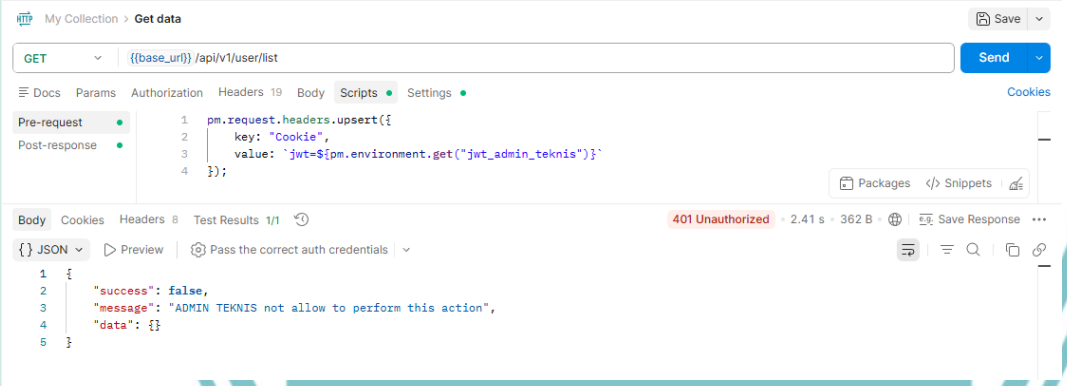
Gambar 4.15 menunjukkan bahwa pengguna dengan role User mencoba mengakses endpoint /api/v1/user/list. Sistem melakukan validasi token dan role sebelum memproses permintaan, dan hasilnya akses ditolak dengan respons HTTP 401

Unauthorized. Hal ini menunjukkan bahwa mekanisme RBAC berhasil mencegah akses tidak sah terhadap data pengguna.



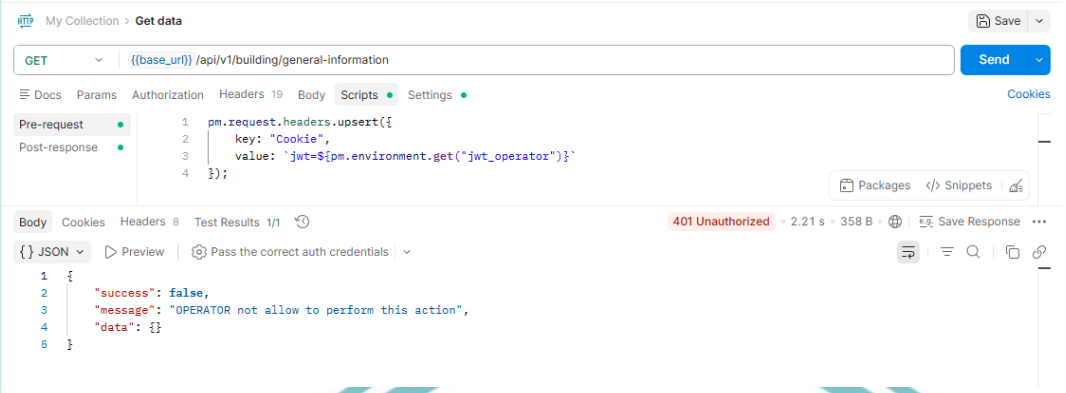
Gambar 4. 15 Operator Mengakses Gateway Device

Gambar 4.16 menunjukkan pengujian pada role Operator yang mencoba mengakses endpoint /api/v1/gateway/device/general-information. Sistem menolak permintaan tersebut karena endpoint hanya diperuntukkan bagi role tertentu yang memiliki hak administratif.



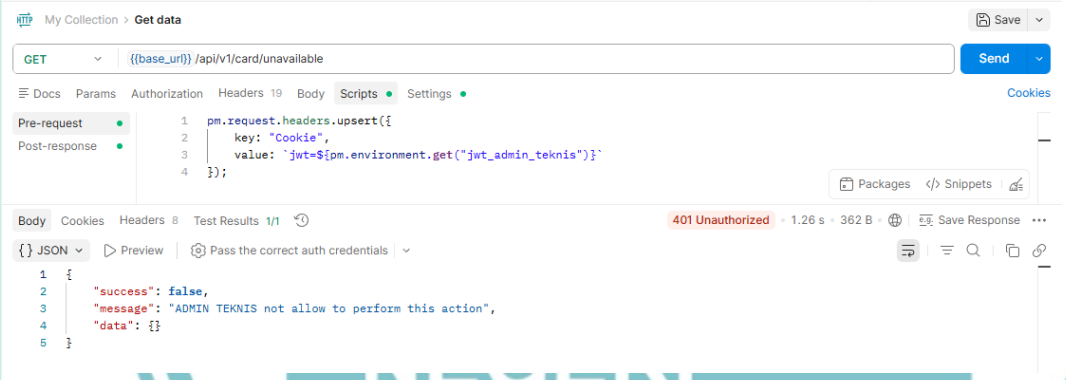
Gambar 4. 16 Admin Teknis Mengakses User List

Gambar 4.17 menunjukkan bahwa pengguna dengan role Admin Teknis mencoba mengakses endpoint /api/v1/user/list. Sistem berhasil melakukan validasi role dan menolak akses, sehingga tidak terjadi privilege escalation.



Gambar 4. 17 Operator Mengakses Building Information

Gambar 4.18 menunjukkan pengujian akses langsung ke endpoint /api/v1/building/general-information oleh role Operator melalui Postman. Meskipun tidak tersedia pada antarmuka pengguna, backend tetap menolak akses dengan respons 401 Unauthorized.



Gambar 4. 18 Admin Teknis Mengakses Card List

Gambar 4.19 menunjukkan bahwa role Admin Teknis mencoba mengakses endpoint /api/v1/card/unavailable. Sistem kembali menolak akses karena endpoint berada di luar cakupan hak akses role tersebut.

Berdasarkan seluruh skenario pengujian yang dilakukan, tidak ditemukan endpoint yang dapat diakses oleh pengguna di luar hak akses yang dimilikinya. Seluruh percobaan akses tidak sah berhasil ditolak oleh backend melalui mekanisme validasi role pada middleware otorisasi.

Hasil ini menunjukkan bahwa implementasi Role-Based Access Control (RBAC) pada sisi backend telah berjalan sesuai dengan kebijakan keamanan yang

ditetapkan. Dengan demikian, tidak ditemukan kerentanan Broken Access Control yang disebabkan oleh kegagalan mekanisme otorisasi backend pada tahap pengujian awal (pretest).

4.2.3.3 Pretest Pembatasan Akses Berdasarkan Alamat IP

Pengujian pembatasan akses berdasarkan alamat IP dilakukan untuk mengevaluasi kondisi keamanan sistem sebelum penerapan mekanisme IP Whitelisting. Pengujian dilakukan dengan mencoba melakukan autentikasi dan mengakses sistem menggunakan jaringan yang berbeda serta melakukan perubahan jaringan selama sesi berlangsung.

Tabel 4. 8 Pretest Sebelum Implementasi IP Whitelist

No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Login menggunakan Super Administrator dari IP berbeda	Login ditolak	Login berhasil (200 OK)	Tidak sesuai
2	Login menggunakan akun Administrator Teknis dari IP berbeda	Login ditolak	Login berhasil (200 OK)	Tidak sesuai
3	Login menggunakan akun Operator dari IP berbeda	Login ditolak	Login berhasil (200 OK)	Tidak sesuai
4	Mengakses endpoint dilindungi setelah login dari IP mana pun	Akses ditolak	Akses berhasil (200 OK)	Tidak sesuai
5	Perubahan jaringan saat sesi berlangsung	Sesi diakhiri	Sesi tetap aktif	Tidak sesuai

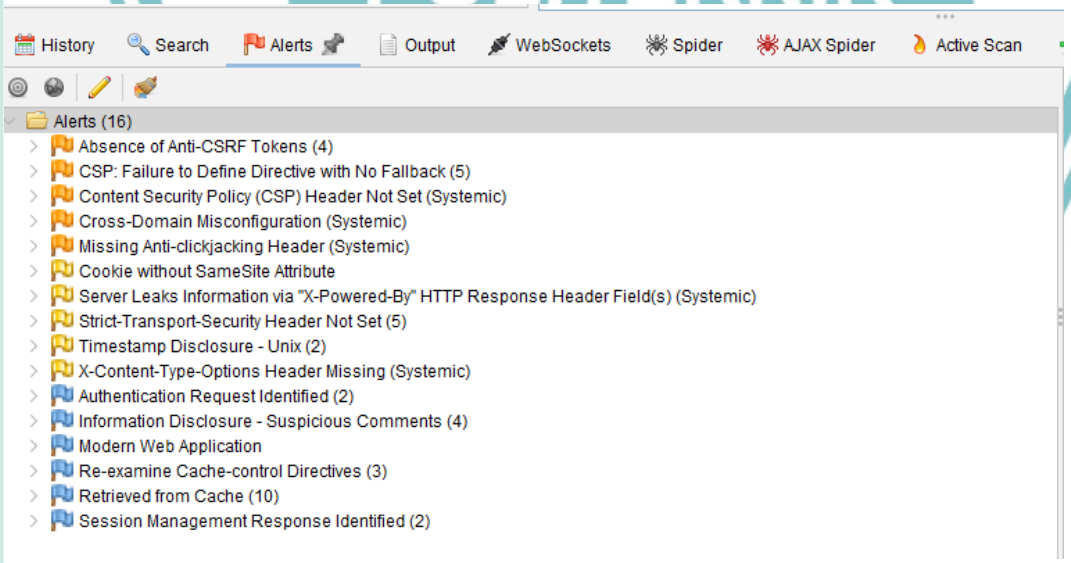
Berdasarkan Tabel 4.8, seluruh skenario pengujian menunjukkan bahwa sistem masih mengizinkan pengguna administratif untuk melakukan login dan mengakses sistem dari alamat IP yang berbeda. Selain itu, perubahan jaringan selama sesi berlangsung tidak menyebabkan sesi pengguna diakhiri maupun akses ditolak oleh sistem. Hasil tersebut menunjukkan bahwa pada tahap pretest belum terdapat mekanisme pembatasan akses berdasarkan alamat IP, sehingga proses autentikasi dan akses terhadap endpoint yang dilindungi masih sepenuhnya bergantung pada

kredensial pengguna, token autentikasi, serta mekanisme Role-Based Access Control (RBAC) yang diterapkan.

Kondisi tersebut meningkatkan risiko penyalahgunaan akses apabila kredensial atau token autentikasi berhasil diperoleh oleh pihak yang tidak berwenang. Akun dengan hak akses administratif masih dapat digunakan dari jaringan mana pun selama kredensial dan token yang digunakan masih valid. Oleh karena itu, diperlukan mekanisme keamanan tambahan berupa IP Whitelisting untuk membatasi akses hanya dari alamat IP yang telah terdaftar sehingga dapat memberikan lapisan perlindungan tambahan terhadap akun dengan hak akses tinggi.

4.2.4 Pretest Kerentanan Menggunakan OWASP ZAP

Pengujian kerentanan dilakukan menggunakan OWASP Zed Attack Proxy (ZAP) untuk mengidentifikasi potensi kerentanan keamanan pada aplikasi web secara otomatis sebelum dilakukan implementasi penguatan keamanan. Pengujian ini bertujuan untuk memperoleh gambaran awal mengenai kondisi keamanan sistem serta memverifikasi hasil pengujian manual yang telah dilakukan pada subbab sebelumnya.



Gambar 4. 19 Hasil Pretest OWASP ZAP

Berdasarakan Gambar 4.20 hasil pemindaian OWASP ZAP ditemukan sebanyak 16 alert dengan tingkat risiko Medium, Low, dan Informational. Namun, tidak seluruh temuan memiliki keterkaitan langsung dengan ruang lingkup penelitian. Oleh karena itu, pembahasan difokuskan pada temuan yang berkaitan dengan kategori OWASP ASVS V3 Session Management, sedangkan temuan lainnya dicatat sebagai informasi tambahan.

Tabel 4. 9 Hasil Pretest OWASPZAP

No	Temuan	Risk	ASVS	Dampak
1	Cookie without SameSite Attribute	Medium	V3 Session Management	Risiko penyalahgunaan cookie lintas situs
2	Session Management Response Identified	Informational	V3 Session Management	Mengindikasikan mekanisme sesi perlu evaluasi
3	Re-examine Cache-Control Directives	Low	V3 Session Management	Data sensitif berpotensi tersimpan di cache browser
4	Absence of Anti-CSRF Tokens	Medium	Temuan di luar ruang lingkup penelitian	Potensi request tidak sah dari browser pengguna
5	Strict-Transport-Security Header Not Set	Medium	Temuan di luar ruang lingkup penelitian	Komunikasi HTTPS berpotensi diturunkan ke HTTP
6	X-Content-Type-Options Header Missing	Low	Temuan di luar ruang lingkup penelitian	Risiko MIME sniffing oleh browser

Tabel 4.9 menunjukkan hasil pemetaan temuan OWASP ZAP berdasarkan kategori OWASP ASVS yang menjadi ruang lingkup penelitian. Temuan yang berkaitan dengan aspek session management digunakan sebagai informasi pendukung dalam proses implementasi penguatan keamanan pada tahap selanjutnya, sedangkan temuan lain yang berada di luar ruang lingkup penelitian dicatat sebagai informasi tambahan.

Berdasarkan hasil pemindaian OWASP ZAP, tidak ditemukan kerentanan kritis yang secara langsung memungkinkan terjadinya bypass autentikasi maupun bypass mekanisme Role-Based Access Control (RBAC) pada sisi backend. Hal ini sejalan dengan hasil pengujian manual pada subbab sebelumnya yang menunjukkan bahwa endpoint backend telah menerapkan pembatasan akses sesuai dengan role pengguna yang dimiliki.

Meskipun demikian, masih ditemukan beberapa temuan yang berkaitan dengan aspek session management, seperti konfigurasi cookie dan pengelolaan cache pada browser. Temuan tersebut melengkapi hasil pengujian manual pada Subbab 4.2.2 yang menunjukkan bahwa token autentikasi masih dapat digunakan setelah proses logout dan belum terdapat mekanisme pengelolaan sesi yang memadai. Oleh karena itu, aspek session management menjadi salah satu fokus utama dalam implementasi penguatan keamanan pada tahap berikutnya.

Dengan demikian, hasil pemindaian menggunakan OWASP ZAP menunjukkan bahwa sebagian besar temuan yang ditemukan berkaitan dengan konfigurasi keamanan aplikasi dan tidak memiliki keterkaitan langsung dengan ruang lingkup penelitian. Selain itu, tidak ditemukan kerentanan kritis yang secara langsung memungkinkan bypass autentikasi maupun bypass mekanisme Role-Based Access Control (RBAC). Temuan yang berkaitan dengan aspek session management digunakan sebagai pendukung hasil pengujian manual, sedangkan temuan lainnya dicatat sebagai informasi tambahan. Oleh karena itu, implementasi penguatan keamanan pada tahap selanjutnya difokuskan pada peningkatan mekanisme session management, penyempurnaan Role-Based Access Control (RBAC), serta penerapan IP Whitelisting sesuai dengan ruang lingkup penelitian.

4.2.5 Rekapitulasi Temuan Keamanan

Rekapitulasi temuan keamanan dilakukan untuk merangkum seluruh hasil pengujian yang telah dilakukan pada tahap *pretest* dan menjadi dasar implementasi perbaikan pada bab berikutnya.

Tabel 4. 10 Rekapitulasi Temuan Keamanan

No	Temuan	ASVS	Status
1	Menu Super Admin tampil pada Admin Teknis	V4 Access Control	Tidak Sesuai
2	Menu Super Admin tampil pada Operator	V4 Access Control	Tidak Sesuai
3	Token autentikasi masih aktif setelah proses logout	V3 Session Management	Tidak Sesuai
4	Token memiliki masa aktif yang terlalu panjang tanpa batas *idle*	V3 Session Management	Tidak Sesuai
5	Akses tidak dibatasi berdasarkan alamat IP	V4 Access Control	Tidak Sesuai
6	Perubahan alamat IP tidak menyebabkan sesi diakhiri	V4 Access Control	Tidak Sesuai
7	Cookie sesi tidak memiliki atribut *SameSite*	V3 Session Management	Tidak Sesuai

Berdasarkan Tabel 4.10, diperoleh tujuh temuan keamanan utama yang terdistribusi pada kategori OWASP ASVS V3 Session Management dan V4 Access Control. Kelemahan yang paling dominan ditemukan pada aspek session management dan implementasi access control pada antarmuka pengguna. Pada sisi access control, ditemukan ketidaksesuaian antara matriks hak akses dengan implementasi role-based rendering sehingga menyebabkan kebocoran visibilitas menu administratif pada role Administrator Teknis dan Operator. Selain itu, sistem belum menerapkan pembatasan akses berdasarkan alamat IP secara efektif.

Pada aspek session management, ditemukan bahwa token autentikasi masih dapat digunakan setelah proses logout, masa berlaku token relatif panjang tanpa mekanisme idle timeout, serta cookie sesi belum menerapkan atribut SameSite. Kondisi tersebut meningkatkan risiko penyalahgunaan sesi oleh pihak yang tidak berwenang.

Berdasarkan hasil rekapitulasi tersebut, ketujuh temuan keamanan selanjutnya menjadi dasar dalam implementasi penguatan keamanan pada tahap berikutnya melalui perbaikan role-based rendering pada frontend, penerapan IP Whitelisting, serta penguatan mekanisme session management.

4.3 Perancangan dan Implementasi Sistem

Berdasarkan hasil pengujian awal (*pretest*) yang telah dilakukan pada Subbab 4.2, ditemukan beberapa kelemahan keamanan yang berkaitan dengan mekanisme autentikasi, kontrol akses, dan pengelolaan sesi pengguna pada aplikasi web monitoring Smart Door Lock. Temuan tersebut menunjukkan bahwa sistem masih memiliki risiko terhadap penyalahgunaan akses, penggunaan token yang tidak semestinya, serta akses administratif dari sumber jaringan yang tidak terotorisasi. Oleh karena itu, dilakukan perancangan dan implementasi mekanisme penguatan keamanan yang difokuskan pada penyelarasan kontrol akses, penguatan pengelolaan sesi pengguna, serta pembatasan akses berdasarkan alamat IP. Seluruh mekanisme yang diterapkan mengacu pada kontrol keamanan OWASP ASVS versi 4.0.3 Level 2 yang menjadi ruang lingkup penelitian.

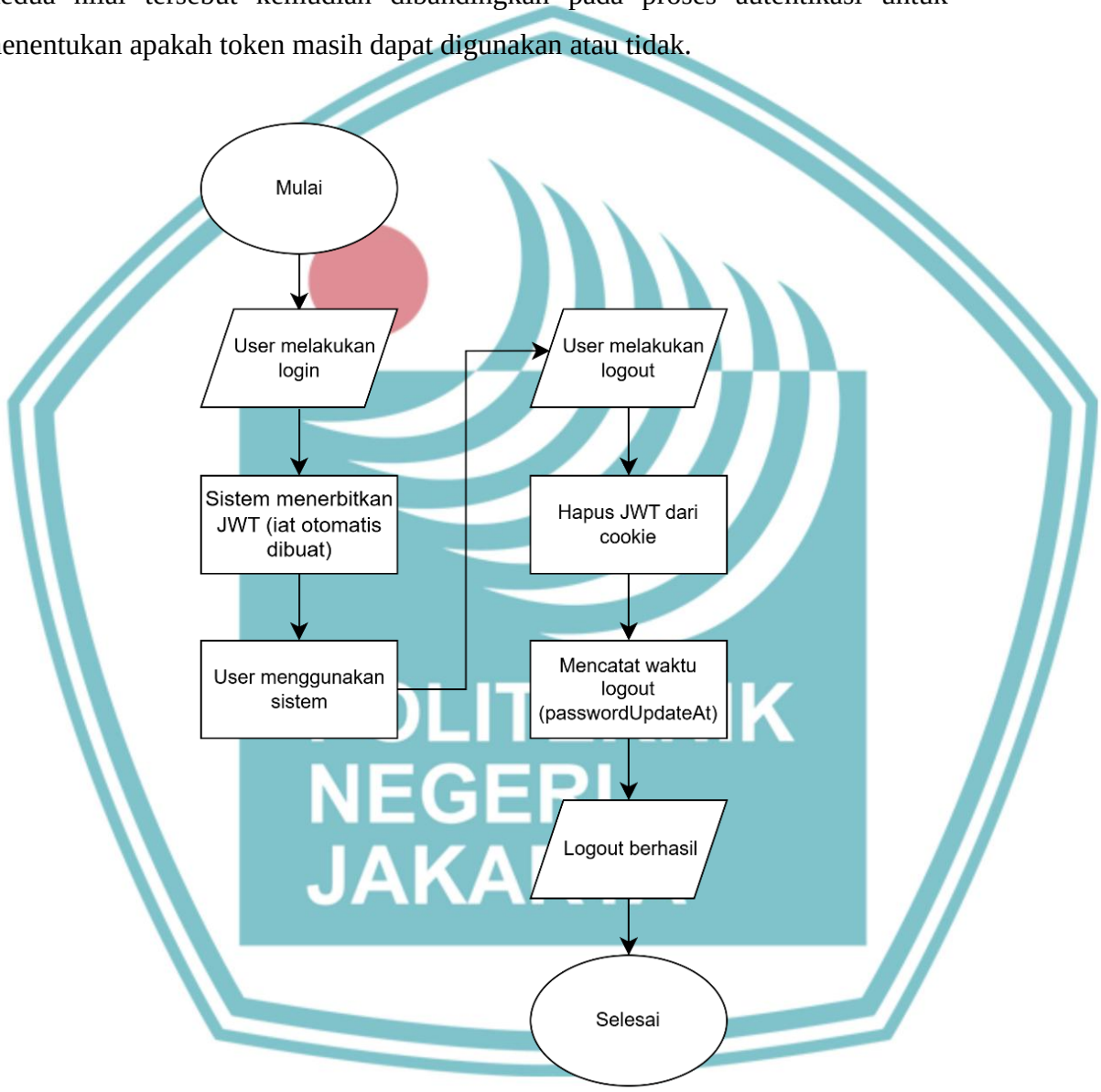
4.3.1 Perancangan Sistem

Tahap perancangan dilakukan untuk menentukan mekanisme mitigasi yang sesuai dengan kerentanan yang ditemukan pada tahap pengujian awal. Perancangan difokuskan pada penguatan keamanan akses melalui penerapan mekanisme *session management*, penyelarasan kontrol akses pada antarmuka pengguna, serta pembatasan akses administratif berbasis jaringan. Hasil perancangan ini selanjutnya digunakan sebagai acuan dalam proses implementasi mekanisme keamanan pada sistem.

4.3.1.1 Perancangan JWT Invalidation

Berdasarkan hasil analisis dan pengujian yang dilakukan pada sistem, proses logout sebelumnya hanya dilakukan dengan menghapus token autentikasi pada sisi klien tanpa adanya mekanisme invalidasi token pada sisi server. Kondisi tersebut menyebabkan token yang telah diterbitkan tetap valid hingga mencapai masa kedaluwarsanya apabila token berhasil diperoleh oleh pihak yang tidak berwenang.

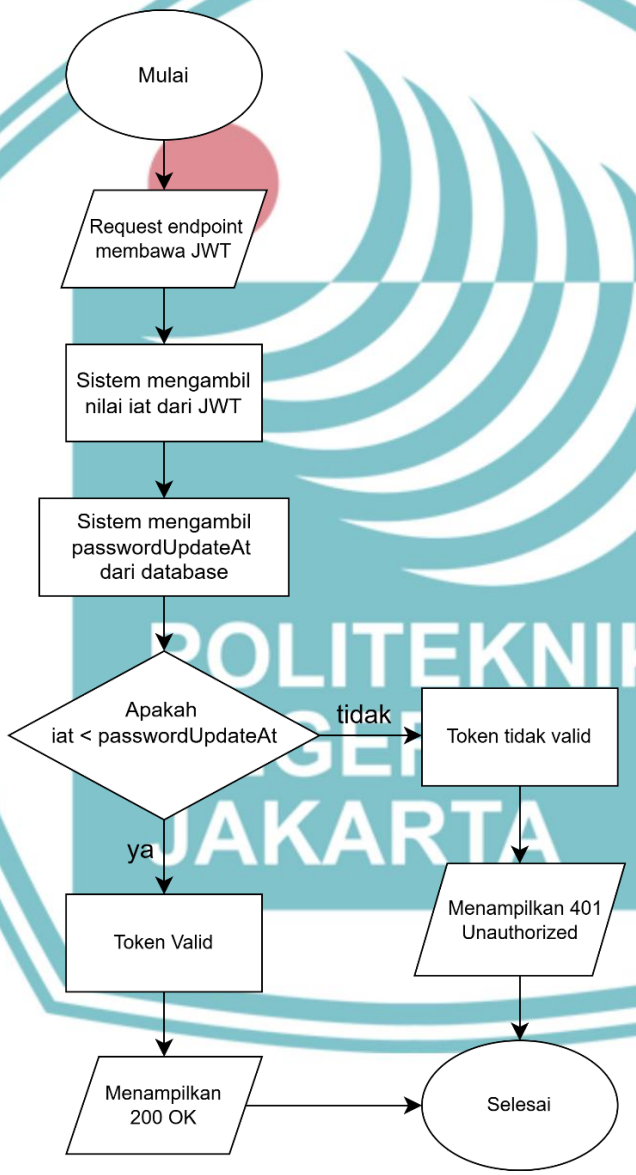
Untuk mengatasi permasalahan tersebut, dirancang mekanisme JWT Invalidation menggunakan pendekatan pencatatan waktu logout terakhir pengguna. Mekanisme ini memanfaatkan dua informasi utama, yaitu Issued At (iat) yang terdapat pada token JWT dan passwordUpdatedAt yang disimpan pada basis data pengguna. Kedua nilai tersebut kemudian dibandingkan pada proses autentikasi untuk menentukan apakah token masih dapat digunakan atau tidak.



Gambar 4. 20 Flowchart Proses Login dan Logout

Gambar 4.21 menunjukkan proses pembentukan nilai iat dan passwordUpdatedAt yang digunakan pada mekanisme JWT Invalidation. Proses dimulai ketika pengguna melakukan login. Setelah kredensial berhasil divalidasi, sistem menerbitkan token JWT yang secara otomatis memuat *claim* Issued At (iat) sebagai

penanda waktu penerbitan token. Token tersebut kemudian disimpan pada cookie sehingga dapat digunakan pengguna untuk mengakses sumber daya yang memerlukan autentikasi. Ketika pengguna melakukan logout, sistem menghapus token JWT dari cookie pada sisi klien dan mencatat waktu logout ke dalam atribut passwordUpdatedAt pada basis data. Nilai iat dan passwordUpdatedAt inilah yang selanjutnya digunakan pada proses validasi token.



Gambar 4. 21 Flowchart Mekanisme JWT Invalidation

Gambar 4.22 menunjukkan mekanisme JWT Invalidation yang dilakukan pada middleware autentikasi setiap kali pengguna mengirimkan permintaan ke server

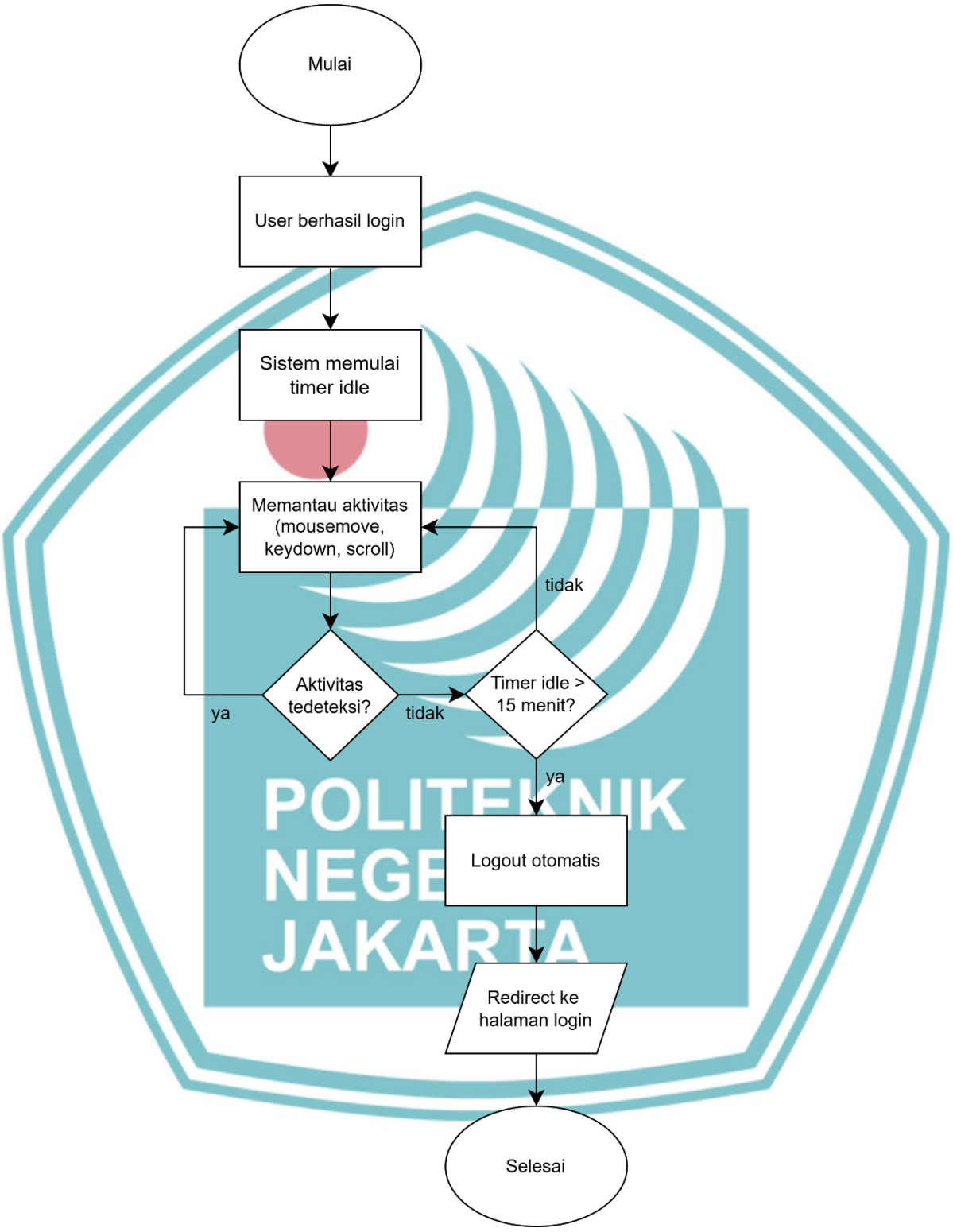
menggunakan token JWT. Middleware terlebih dahulu mengambil nilai **iat** dari payload JWT, kemudian mengambil nilai passwordUpdatedAt milik pengguna dari basis data. Selanjutnya sistem membandingkan kedua nilai tersebut. Apabila nilai iat lebih kecil daripada passwordUpdatedAt, berarti token diterbitkan sebelum pengguna melakukan logout sehingga token dinyatakan tidak valid. Dalam kondisi tersebut sistem menolak permintaan pengguna dan mengembalikan respons HTTP 401 Unauthorized. Sebaliknya, apabila nilai iat lebih besar atau sama dengan passwordUpdatedAt, token dinyatakan masih valid sehingga permintaan pengguna diteruskan ke proses berikutnya dan server mengembalikan respons sesuai hasil pemrosesan.

4.3.1.2 Perancangan Idle Timeout

Berdasarkan hasil pengujian awal pada Subbab 4.2.3, ditemukan bahwa sistem belum memiliki mekanisme penghentian sesi secara otomatis ketika pengguna tidak melakukan aktivitas dalam jangka waktu tertentu. Kondisi tersebut meningkatkan risiko penyalahgunaan akun apabila perangkat ditinggalkan dalam keadaan masih login sehingga pihak lain masih dapat memanfaatkan sesi yang masih aktif untuk mengakses sistem.

Pada penelitian ini, mekanisme *idle timeout* dirancang untuk mengakhiri sesi pengguna secara otomatis apabila tidak terdapat aktivitas dalam periode waktu tertentu. Mekanisme ini bertujuan untuk mengurangi risiko penyalahgunaan akun akibat perangkat yang ditinggalkan dalam keadaan login maupun penggunaan sesi oleh pihak yang tidak berwenang.

Karena sistem menggunakan *JSON Web Token* (JWT) yang bersifat *stateless*, server tidak menyimpan informasi aktivitas pengguna secara persisten setelah token diterbitkan. Akibatnya, server tidak dapat secara langsung menentukan apakah pengguna masih aktif menggunakan aplikasi atau telah meninggalkan sesi dalam keadaan login. Sebagai solusi, mekanisme *idle timeout* dirancang untuk diimplementasikan pada sisi *frontend* menggunakan JavaScript yang bertugas memantau aktivitas pengguna selama menggunakan aplikasi.



Gambar 4. 22 Flowchart Mekanisme Idle Timeout

Berdasarkan Gambar 4.23, mekanisme *idle timeout* dimulai setelah pengguna berhasil melakukan proses login ke dalam sistem. Setelah autentikasi berhasil,

sistem akan mengaktifkan penghitung waktu ketidakaktifan (*idle timer*) yang berfungsi untuk memantau aktivitas pengguna selama sesi berlangsung. Aktivitas seperti *mousemove*, *keydown*, dan *scroll* digunakan sebagai indikator bahwa pengguna masih aktif menggunakan aplikasi.

Setiap aktivitas yang terdeteksi akan menyebabkan sistem melakukan *reset timer* sehingga waktu ketidakaktifan dihitung kembali dari awal dan sesi pengguna tetap aktif. Sebaliknya, apabila tidak terdapat aktivitas yang terdeteksi, sistem akan melakukan pemeriksaan terhadap durasi ketidakaktifan pengguna. Jika durasi tersebut belum melebihi batas waktu yang ditentukan, maka sistem akan terus melanjutkan proses pemantauan aktivitas pengguna.

Namun, apabila tidak terdapat aktivitas hingga melebihi batas waktu yang telah ditentukan, sistem akan menganggap pengguna berada dalam kondisi *idle* dan secara otomatis menjalankan proses *logout*. Setelah proses *logout* selesai dilakukan, pengguna akan diarahkan kembali ke halaman login untuk melakukan autentikasi ulang sebelum dapat mengakses sistem kembali.

Pada penelitian ini, batas waktu ketidakaktifan ditetapkan selama 15 menit. Pemilihan durasi tersebut mempertimbangkan keseimbangan antara aspek keamanan dan kenyamanan pengguna sehingga risiko penyalahgunaan akun akibat sesi yang ditinggalkan dalam keadaan aktif dapat diminimalkan.

4.3.1.3 Perancangan IP Whitelisting

Berdasarkan hasil pengujian awal dan analisis keamanan yang telah dilakukan, mekanisme autentikasi dan Role-Based Access Control (RBAC) pada sistem telah mampu membatasi akses berdasarkan identitas pengguna dan hak akses yang dimiliki. Namun demikian, sistem belum menerapkan pembatasan akses berdasarkan lokasi jaringan (*network-based restriction*) pengguna yang melakukan akses.

Kondisi tersebut menyebabkan akun dengan hak akses tinggi, seperti Super Admin, Administrator Teknis, dan Operator, tetap dapat digunakan dari jaringan mana pun selama kredensial login dan token autentikasi masih valid. Apabila kredensial atau

token autentikasi tersebut berhasil diperoleh oleh pihak yang tidak berwenang, maka tidak terdapat mekanisme tambahan yang dapat memverifikasi apakah akses tersebut berasal dari jaringan yang sah atau tidak.

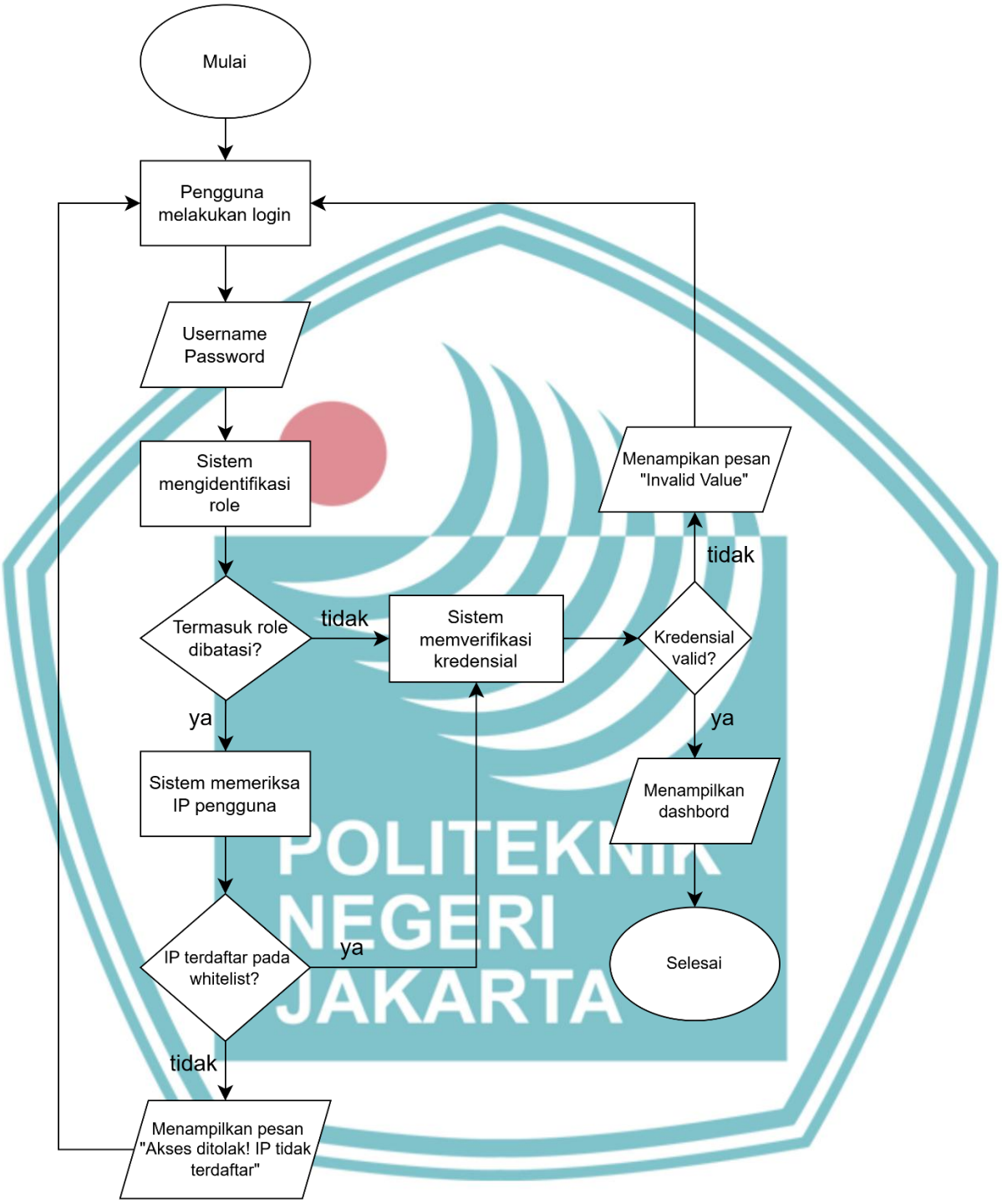
Untuk mengurangi risiko tersebut, pada penelitian ini dirancang mekanisme IP Whitelisting sebagai lapisan keamanan tambahan (*defense in depth*) yang melengkapi mekanisme autentikasi dan RBAC yang telah diterapkan sebelumnya. Melalui mekanisme ini, akses terhadap akun tertentu dibatasi sehingga hanya dapat dilakukan dari alamat IP yang telah didaftarkan dan diotorisasi oleh sistem.

Mekanisme ini dirancang untuk mendukung skenario implementasi Smart Door Lock pada ruang Embedded di lingkungan Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta. Oleh karena itu, akses administratif dibatasi agar hanya dapat dilakukan melalui jaringan internal atau jaringan terpercaya yang telah ditentukan sebelumnya.

Pada rancangan ini, sistem terlebih dahulu melakukan identifikasi terhadap role pengguna pada saat proses autentikasi berlangsung. Apabila pengguna termasuk ke dalam kelompok role yang dikenakan kebijakan IP Whitelisting, sistem akan melakukan validasi alamat IP pengguna terhadap daftar alamat IP yang diizinkan.

Jika alamat IP pengguna ditemukan pada daftar *whitelist*, proses autentikasi akan dilanjutkan hingga token berhasil diterbitkan. Sebaliknya, apabila alamat IP tidak ditemukan pada daftar tersebut, sistem akan menghentikan proses autentikasi dan mengembalikan respons HTTP 403 Forbidden meskipun pengguna memiliki kredensial yang valid.

Selain diterapkan pada proses login, mekanisme ini juga dirancang untuk melakukan pemantauan alamat IP selama sesi berlangsung. Apabila terdeteksi perubahan jaringan yang menyebabkan alamat IP pengguna tidak lagi sesuai dengan kebijakan yang telah ditentukan, sistem dapat mengakhiri sesi pengguna secara otomatis untuk mencegah penyalahgunaan akses.



Gambar 4. 23 Flowchart Mekanisme IP Whitelisting

Gambar 4.24 mmenunjukkan alur kerja mekanisme IP Whitelisting yang diterapkan pada proses autentikasi pengguna. Proses dimulai dengan identifikasi role pengguna, kemudian dilanjutkan dengan validasi alamat IP terhadap daftar whitelist bagi role yang dikenakan pembatasan akses berbasis jaringan. Hanya pengguna

yang memenuhi kedua syarat tersebut yang diizinkan melanjutkan proses autentikasi hingga token diterbitkan, sedangkan permintaan dari alamat IP yang tidak terdaftar akan ditolak oleh sistem dengan respons HTTP 403 Forbidden.

4.3.2 Implementasi Sistem

Tahap implementasi sistem dilakukan berdasarkan rancangan mekanisme keamanan yang telah disusun pada tahap sebelumnya. Implementasi difokuskan pada penguatan keamanan aplikasi web monitoring Smart Door Lock melalui penerapan mekanisme *session management*, penyelarasan kontrol akses pada antarmuka pengguna, serta pembatasan akses administratif berbasis alamat IP.

Setiap mekanisme keamanan diimplementasikan untuk mengatasi kelemahan yang ditemukan pada tahap pengujian awal (*pretest*), sehingga sistem diharapkan mampu mengelola sesi pengguna secara lebih aman, menerapkan prinsip *least privilege* secara lebih konsisten, serta membatasi akses administratif hanya dari sumber jaringan yang telah diotorisasi.

4.3.2.1 Implementasi Absolute Timeout

Berdasarkan hasil pengujian awal pada Subbab 4.2.3, ditemukan bahwa token autentikasi memiliki masa berlaku yang relatif panjang sehingga tetap dapat digunakan dalam jangka waktu yang lama setelah diterbitkan. Kondisi tersebut meningkatkan risiko penyalahgunaan token apabila token berhasil diperoleh oleh pihak yang tidak berwenang. Oleh karena itu, dilakukan implementasi mekanisme *absolute timeout* untuk membatasi masa aktif token autentikasi sesuai dengan rancangan yang telah disusun pada tahap sebelumnya.

Implementasi *absolute timeout* dilakukan dengan mengubah konfigurasi masa berlaku (*expiration time*) pada token JSON Web Token (JWT). Sebelum dilakukan perbaikan, token memiliki masa berlaku selama tiga hari. Setelah implementasi, masa aktif token dibatasi menjadi delapan jam sehingga setiap token yang diterbitkan akan dinyatakan tidak berlaku secara otomatis setelah melewati batas waktu tersebut.

Dengan pembatasan masa berlaku token, sistem dapat mengurangi kemungkinan penyalahgunaan token autentikasi yang masih aktif. Meskipun token berhasil diperoleh oleh pihak yang tidak berwenang, token tersebut hanya dapat digunakan selama periode validitas yang telah ditentukan. Setelah masa berlaku berakhir, pengguna diwajibkan melakukan proses autentikasi kembali untuk memperoleh token baru.

4.3.2.2 Implementasi JWT Invalidation

Berdasarkan hasil pengujian awal pada Subbab 4.2.3, ditemukan bahwa token autentikasi masih dapat digunakan kembali setelah pengguna melakukan proses *logout*. Kondisi tersebut terjadi karena proses *logout* hanya menghapus autentikasi pada sisi *client*, sedangkan token yang telah diterbitkan masih dianggap valid hingga mencapai masa kedaluwarsanya. Akibatnya, sesi pengguna belum sepenuhnya berakhir setelah proses *logout* dilakukan.

Untuk meningkatkan keamanan pengelolaan sesi, diimplementasikan mekanisme JWT Invalidation dengan memanfaatkan atribut *passwordUpdatedAt* pada data pengguna. Atribut tersebut digunakan sebagai penanda waktu terakhir sesi dinyatakan tidak berlaku. Setiap kali pengguna melakukan *logout*, sistem memperbarui nilai *passwordUpdatedAt* sehingga seluruh token yang diterbitkan sebelum waktu tersebut tidak lagi dapat digunakan.

Selanjutnya, setiap permintaan yang membawa token autentikasi akan melalui proses validasi pada middleware autentikasi. Sistem membandingkan waktu penerbitan token (*issued at*) dengan nilai *passwordUpdatedAt* yang tersimpan pada basis data. Apabila token diterbitkan sebelum waktu *logout* terakhir, maka token dinyatakan tidak valid dan permintaan akan ditolak. Sebaliknya, apabila token diterbitkan setelah waktu tersebut, maka token dianggap masih valid sehingga pengguna diizinkan untuk mengakses sumber daya yang diminta.

Dengan mekanisme tersebut, sesi pengguna dapat dihentikan secara efektif setelah proses *logout* dilakukan. Implementasi ini mencegah penggunaan kembali token yang sebelumnya masih aktif sehingga risiko penyalahgunaan sesi akibat token yang masih berlaku dapat diminimalkan.

4.3.2.3 Implementasi Idle Timeout

Berdasarkan rancangan yang telah disusun pada tahap sebelumnya, mekanisme *idle timeout* diimplementasikan pada sisi *frontend* untuk memantau aktivitas pengguna selama menggunakan aplikasi. Implementasi ini bertujuan untuk mengakhiri sesi secara otomatis apabila pengguna tidak melakukan aktivitas dalam jangka waktu tertentu, sehingga dapat mengurangi risiko penyalahgunaan akun ketika perangkat ditinggalkan dalam keadaan masih login.

Sistem melakukan pemantauan terhadap berbagai aktivitas pengguna yang merepresentasikan interaksi dengan aplikasi, seperti pergerakan kursor (*mousemove*), penekanan tombol (*keydown*), dan pengguliran halaman (*scroll*). Setiap aktivitas yang terdeteksi akan mengatur ulang waktu ketidakaktifan sehingga sesi pengguna tetap dianggap aktif.

Apabila tidak terdapat aktivitas pengguna hingga melebihi batas waktu yang telah ditentukan, sistem akan mengakhiri sesi secara otomatis dengan menghapus autentikasi yang masih aktif dan mengarahkan pengguna kembali ke halaman login. Dengan mekanisme tersebut, sesi pengguna tidak dapat terus digunakan ketika aplikasi ditinggalkan tanpa pengawasan, sehingga keamanan pengelolaan sesi dapat ditingkatkan.

4.3.2.4 Implementasi Role-based Rendering pada Frontend

Implementasi role-based rendering pada frontend dilakukan dengan menyesuaikan mekanisme pembentukan tampilan antarmuka berdasarkan role pengguna yang sedang login. Pada implementasi ini, sistem mengidentifikasi role pengguna sebelum halaman ditampilkan, kemudian menentukan komponen antarmuka yang sesuai dengan hak akses masing-masing role. Dengan mekanisme tersebut, setiap pengguna hanya memperoleh menu dan fitur yang relevan dengan kewenangannya.

Penyesuaian ini dilakukan pada proses rendering halaman sehingga tampilan antarmuka tidak lagi menggunakan layout yang sama untuk seluruh pengguna. Akibatnya, menu administratif hanya ditampilkan kepada pengguna yang memiliki hak akses, sedangkan menu yang tidak sesuai dengan kewenangan pengguna tidak

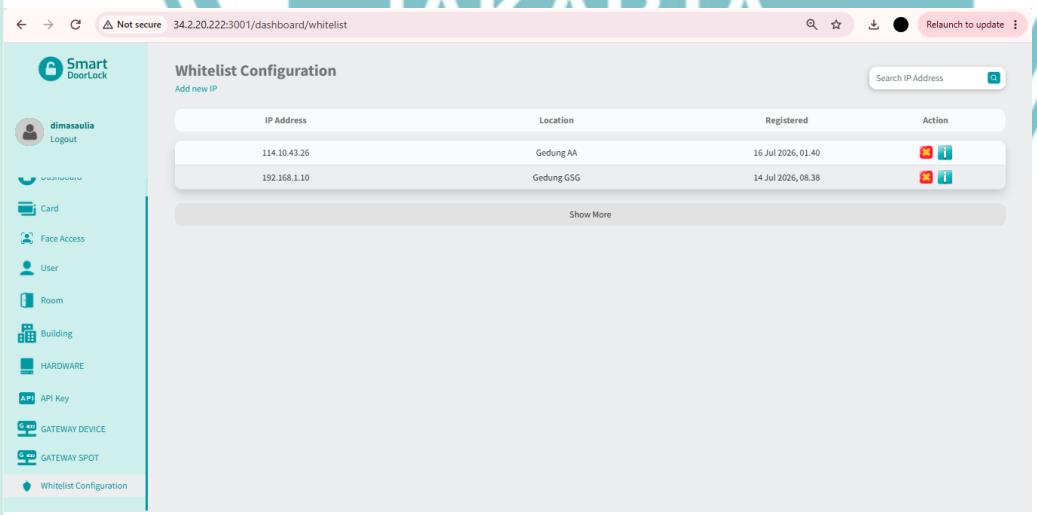
ditampilkan pada antarmuka. Implementasi ini mendukung penerapan prinsip *least privilege* pada sisi frontend serta mengurangi kemungkinan terjadinya kebocoran informasi mengenai struktur fitur administratif.

Efektivitas implementasi role-based rendering terhadap kesesuaian tampilan antarmuka berdasarkan hak akses pengguna dibahas lebih lanjut pada Subbab 4.4 melalui hasil pengujian pretest dan posttest.

4.3.2.5 Implementasi IP Whitelisting

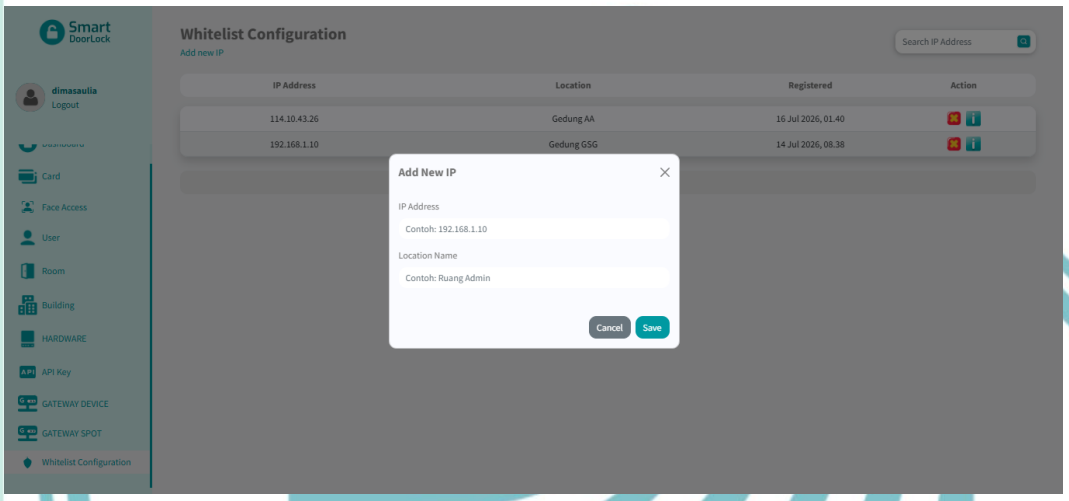
Implementasi IP Whitelisting dilakukan dengan menambahkan fitur pengelolaan daftar alamat IP pada aplikasi web monitoring Smart Door Lock. Fitur ini digunakan untuk mengelola alamat IP yang diizinkan mengakses sistem, sehingga hanya perangkat yang berasal dari alamat IP yang telah terdaftar yang dapat melewati proses validasi pada saat autentikasi. Pengelolaan whitelist hanya dapat dilakukan oleh pengguna dengan role Super Admin, karena berkaitan dengan konfigurasi keamanan sistem.

Halaman pengelolaan whitelist menyediakan informasi berupa alamat IP yang terdaftar, lokasi IP (IP Location), waktu pendaftaran (Registered At), serta aksi untuk mengubah (Edit) atau menghapus (Delete) data whitelist. Melalui halaman ini, Super Admin dapat melakukan pengelolaan daftar whitelist secara terpusat sesuai dengan kebutuhan operasional sistem.



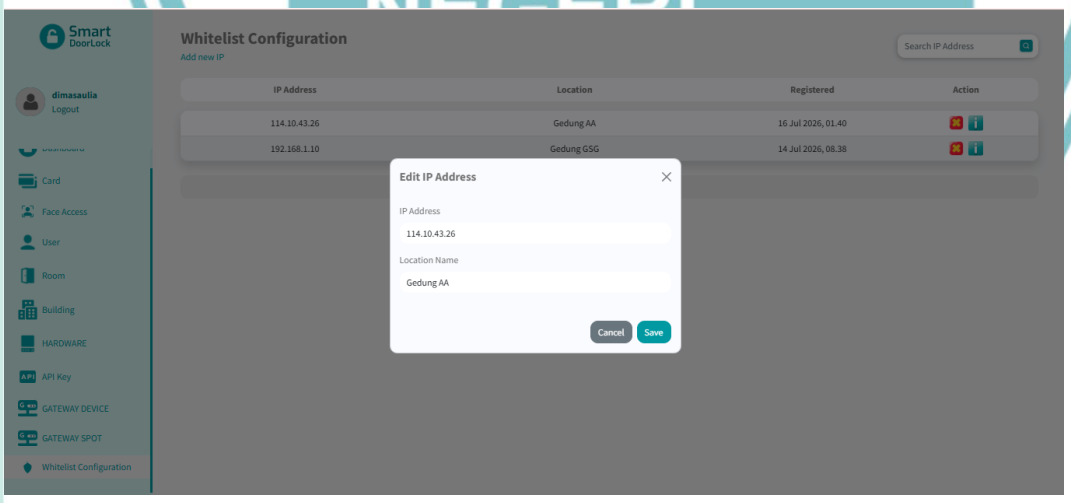
Gambar 4. 24 Fitur Konfigurasi Whitelist

Gambar 4.25 menunjukkan halaman pengelolaan whitelist yang digunakan oleh Super Admin untuk melihat daftar alamat IP yang diizinkan mengakses sistem. Halaman ini menampilkan informasi alamat IP, lokasi IP, waktu pendaftaran, serta menyediakan aksi Edit dan Delete untuk mengelola data whitelist.



Gambar 4. 25 Form Penambahan Whitelist

Gambar 4.26 menunjukkan formulir Add New Whitelist yang digunakan untuk menambahkan alamat IP baru ke dalam daftar whitelist. Super Admin mengisi alamat IP beserta informasi lokasi IP sebagai identitas jaringan yang akan diberikan izin akses ke sistem.



Gambar 4. 26 Form Edit Whitelist

Gambar 4.27 menunjukkan formulir Edit Whitelist yang digunakan untuk memperbarui data whitelist yang telah tersimpan. Melalui formulir ini, Super Admin dapat mengubah alamat IP maupun informasi lokasi sesuai dengan perubahan konfigurasi jaringan tanpa perlu menghapus data yang sudah ada.

4.3.2.6 Implementasi IP Whitelisting Selama Sesi Berlangsung

Selain diterapkan pada tahap autentikasi, mekanisme IP Whitelisting juga diimplementasikan selama sesi pengguna berlangsung. Mekanisme ini bertujuan untuk memastikan bahwa sesi yang telah berhasil dibuat tetap digunakan dari alamat IP yang sama dengan saat proses login. Dengan demikian, apabila terjadi perubahan jaringan atau upaya penggunaan sesi dari alamat IP yang berbeda, sistem dapat mendeteksi kondisi tersebut sebelum permintaan diproses lebih lanjut.

Implementasi dilakukan dengan menambahkan proses validasi alamat IP pada setiap request yang dikirimkan oleh pengguna ke endpoint yang dilindungi. Sistem akan membandingkan alamat IP saat ini dengan daftar whitelist yang telah terdaftar. Proses validasi hanya diterapkan pada pengguna dengan role yang dikenakan kebijakan IP Whitelisting, sedangkan pengguna dengan role lain tetap diproses sesuai mekanisme autentikasi yang berlaku.

Apabila alamat IP yang digunakan tidak sesuai dengan daftar whitelist, sistem akan menghentikan sesi pengguna secara otomatis dengan menghapus token autentikasi dan menolak permintaan menggunakan respons HTTP 403 Forbidden. Dengan mekanisme tersebut, sesi yang masih aktif tidak dapat digunakan kembali apabila terjadi perpindahan jaringan atau akses dari alamat IP yang tidak sah. Implementasi ini memperkuat mekanisme IP Whitelisting karena pengendalian akses tidak hanya dilakukan pada saat login, tetapi juga selama sesi pengguna masih berlangsung.

4.4 Pengujian Akhir (Posttest)

Pengujian akhir (posttest) dilakukan untuk memverifikasi efektivitas implementasi penguatan keamanan yang telah diterapkan pada sistem. Pengujian difokuskan pada aspek yang mengalami perubahan selama tahap implementasi, yaitu access control, session management, dan hasil pemindaian menggunakan OWASP ZAP. Pengujian

authentication tidak dilakukan kembali karena pada tahap pretest mekanisme autentikasi telah menunjukkan hasil yang sesuai dan tidak dilakukan perubahan terhadap mekanisme tersebut.

4.4.1 Posttest Authentication

Pengujian authentication pada tahap posttest dilakukan untuk memverifikasi bahwa implementasi penguatan keamanan yang diterapkan pada sistem tidak memengaruhi mekanisme autentikasi yang telah berjalan dengan baik sebelumnya. Pengujian ini mengacu pada kategori OWASP ASVS V2 – Authentication dengan menggunakan skenario yang sama seperti pada tahap pretest.

Tujuan pengujian ini adalah untuk memastikan bahwa pengguna dengan kredensial yang valid tetap dapat memperoleh akses ke sistem, sedangkan pengguna yang menggunakan kredensial tidak valid maupun token JWT yang telah dimodifikasi tetap ditolak oleh sistem.

Hasil pengujian authentication setelah implementasi penguatan keamanan ditunjukkan pada Tabel 4.11.

Tabel 4. 11 Hasil Posttest Authentication

No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Melakukan login dengan username dan password benar	Login berhasil	Sistem menerima akses (200 OK)	Sesuai
2	Melakukan login dengan password salah	Login gagal	Ditolak (401 Unauthorized)	Sesuai
3	Melakukan login dengan username tidak terdaftar	Login gagal	Ditolak (401 Unauthorized)	Sesuai
4	Mengakses endpoint menggunakan JWT yang telah dimodifikasi	Sistem menolak akses	Ditolak (401 Unauthorized)	Sesuai

Berdasarkan Tabel 4.11, seluruh skenario pengujian pada tahap posttest menunjukkan hasil yang sesuai dengan mekanisme autentikasi yang diterapkan pada sistem. Pengguna yang memasukkan username dan password yang benar

berhasil memperoleh akses ke sistem, sedangkan percobaan login menggunakan password yang salah, username yang tidak terdaftar, maupun penggunaan JSON Web Token (JWT) yang telah dimodifikasi tetap ditolak oleh sistem dengan respons 401 Unauthorized.

Hasil tersebut menunjukkan bahwa implementasi penguatan keamanan yang dilakukan tidak memengaruhi mekanisme autentikasi yang telah berjalan dengan baik sebelumnya. Dengan demikian, kontrol keamanan pada kategori OWASP ASVS V2 – Authentication tetap dapat dipertahankan setelah proses implementasi dilakukan.

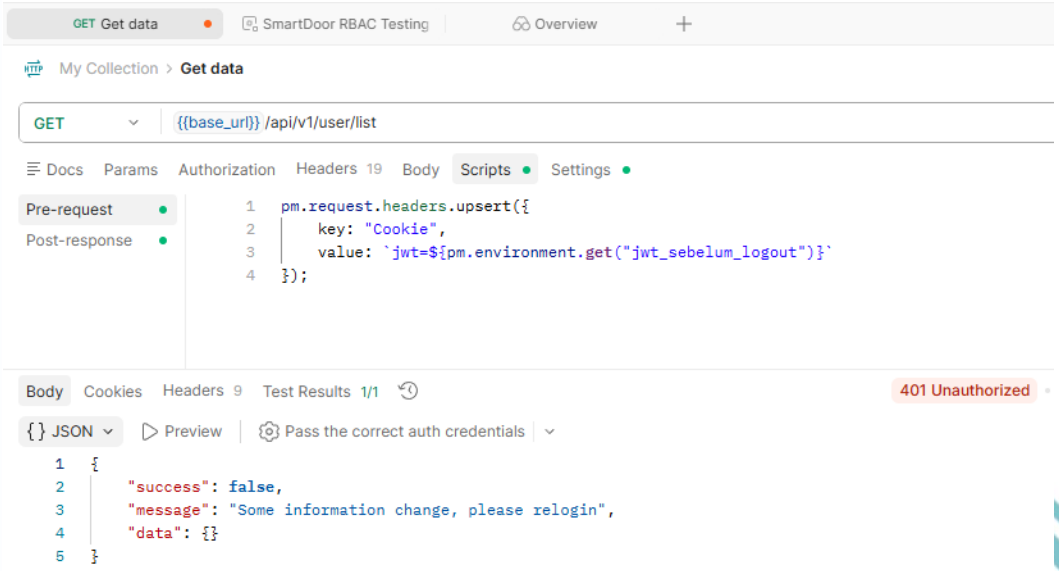
4.4.2 Posttest Session Management

Pengujian *session management* dilakukan kembali untuk memverifikasi efektivitas mekanisme pengelolaan sesi yang telah diterapkan. Fokus pengujian adalah memastikan bahwa seluruh celah keamanan yang ditemukan pada tahap *pretest*—seperti token yang tetap aktif pasca-*logout* dan tidak adanya batasan durasi sesi—telah berhasil dimitigasi.

Tabel 4. 12 Hasil Posttest Session Management

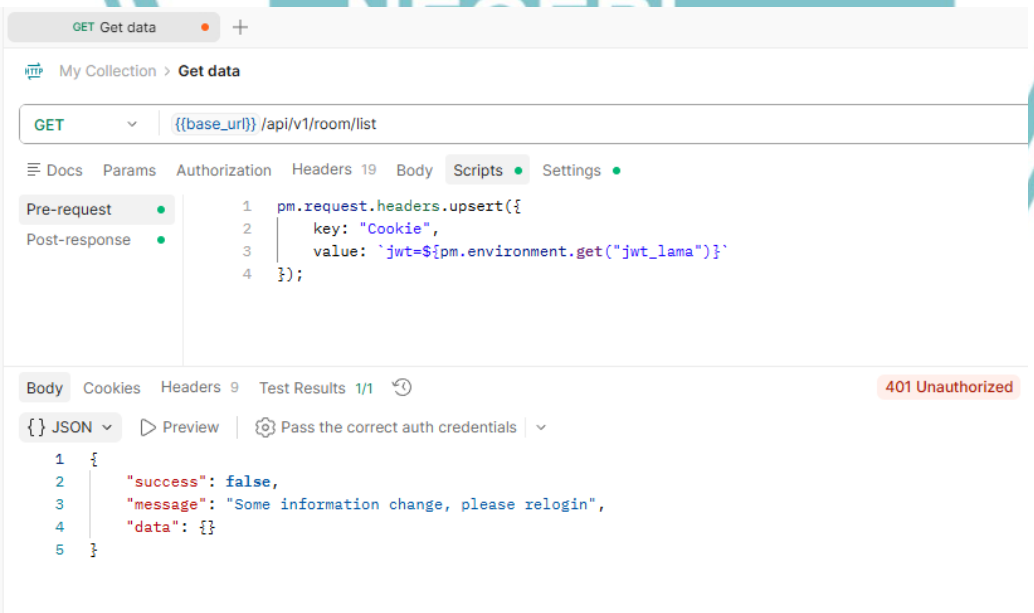
No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Mengakses sistem menggunakan token lama setelah logout	Sistem menolak akses	401 Unauthorized	Sesuai
2	Menggunakan token setelah melewati masa berlaku delapan jam	Token telah expired	401 Unauthorized	Sesuai
3	Tidak terdapat aktivitas pengguna selama 15 menit	Logout otomatis	Logout berhasil dilakukan	Sesuai

Tabel 4.12 menunjukkan bahwa seluruh skenario pengujian berhasil dijalankan sesuai dengan mekanisme session management yang telah diterapkan. Tidak ditemukan lagi token yang tetap aktif setelah logout maupun token yang dapat digunakan melebihi masa berlaku yang telah ditentukan.



Gambar 4. 27 Token Invalid Setelah Proses Logout

Gambar 4.28 menunjukkan bahwa token yang diperoleh sebelum proses logout tidak lagi dapat digunakan untuk mengakses endpoint yang dilindungi. Sistem melakukan validasi waktu penerbitan token terhadap informasi sesi yang tersimpan pada database dan mengembalikan respons HTTP 401 Unauthorized. Hasil ini menunjukkan bahwa mekanisme invalidasi token setelah logout telah berjalan dengan baik.



Gambar 4. 28 Token Invalid Karena Telah Melewati Masa Berlaku

Gambar 4.29 menunjukkan bahwa token autentikasi yang telah melewati batas waktu delapan jam tidak lagi dapat digunakan untuk mengakses endpoint yang dilindungi. Sistem mendeteksi bahwa token telah mencapai masa kedaluwarsa dan mengembalikan respons HTTP 401 Unauthorized. Hasil ini menunjukkan bahwa mekanisme Absolute Timeout telah berhasil diterapkan.

Berdasarkan seluruh hasil pengujian yang dilakukan, mekanisme session management yang diterapkan pada sistem telah berhasil mengatasi kelemahan yang ditemukan pada tahap pretest. Token yang diterbitkan sebelum proses logout tidak lagi dapat digunakan kembali, masa aktif token berhasil dibatasi melalui mekanisme Absolute Timeout, dan sesi pengguna dapat dihentikan secara otomatis ketika tidak terdapat aktivitas dalam periode tertentu. Dengan demikian, pengelolaan siklus hidup sesi pengguna menjadi lebih aman dan risiko penyalahgunaan akun akibat penggunaan token yang tidak sah dapat diminimalkan.

4.4.3 Posttest Access Control

Pengujian access control dilakukan untuk mengevaluasi penerapan pembatasan akses pada website monitoring IoT Smart Door Lock berdasarkan role pengguna yang telah ditetapkan. Pengujian ini mengacu pada OWASP Application Security Verification Standard (ASVS) V4 – Access Control yang menekankan penerapan prinsip least privilege, sehingga setiap pengguna hanya dapat mengakses fitur dan sumber daya sesuai dengan hak akses yang dimilikinya.

Pengujian dilakukan pada dua lapisan sistem, yaitu antarmuka pengguna (frontend) dan backend. Pengujian pada frontend bertujuan untuk mengevaluasi kesesuaian tampilan menu dan fitur berdasarkan role pengguna, sedangkan pengujian pada backend dilakukan untuk memastikan bahwa setiap endpoint hanya dapat diakses oleh pengguna yang memiliki hak akses yang sesuai.

4.4.3.1 Posttest Access Control pada Antarmuka Pengguna

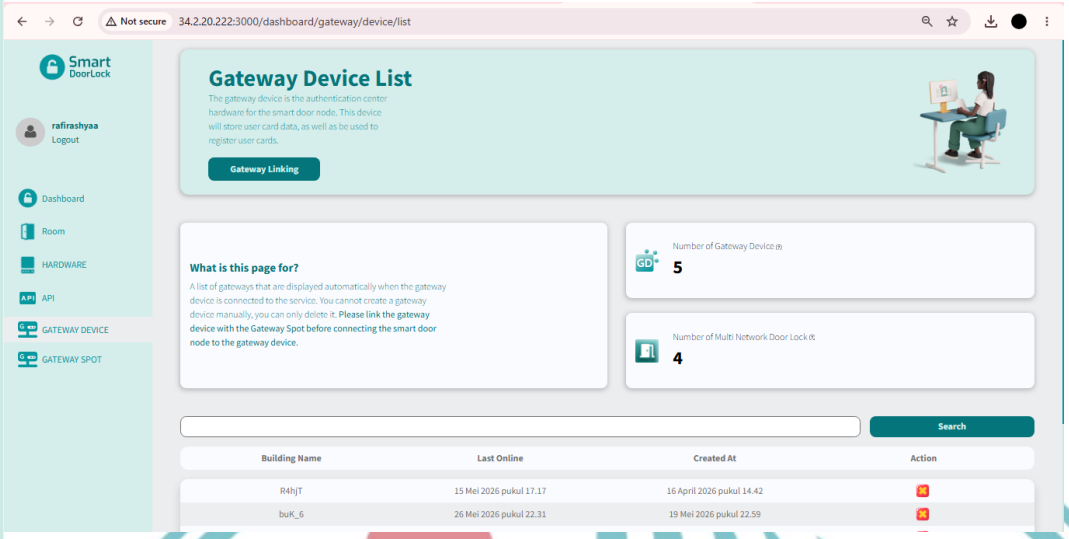
Pengujian ini dilakukan untuk memverifikasi efektivitas perbaikan mekanisme *role-based rendering* pada sisi *frontend*. Fokus pengujian adalah memastikan bahwa setiap pengguna hanya dapat melihat menu dan fitur yang sesuai dengan hak

aksesnya, serta menghilangkan kebocoran fitur administratif yang ditemukan pada tahap *pretest*.

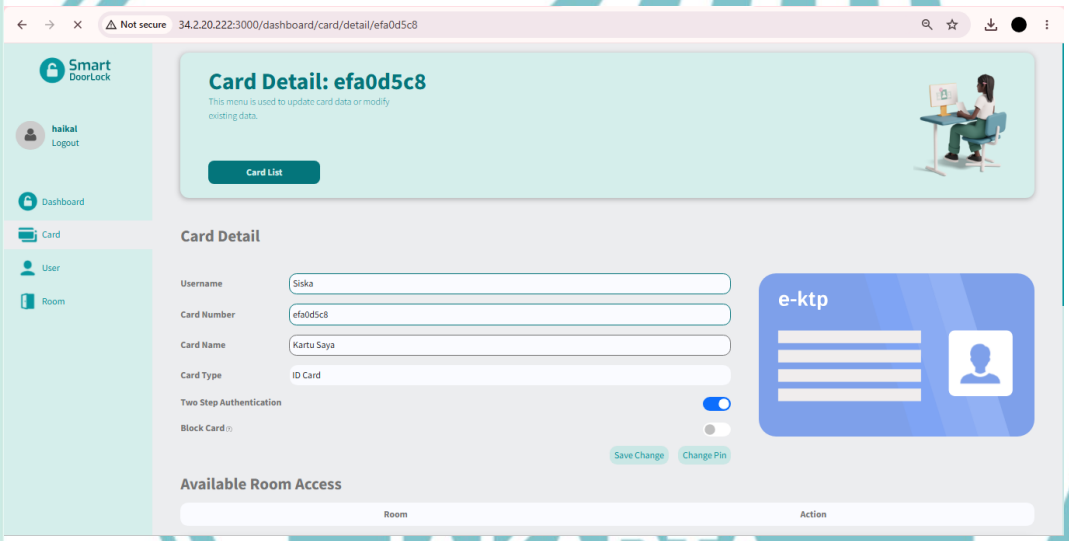
Tabel 4. 13 Hasil Posttest Access Control pada Antarmuka Pengguna

No	Role	Skenario	Hasil yang diharapkan	Hasil aktual	Status
1	Guest	Mengakses dashboard tanpa login	Redirect ke halaman login	Redirect ke halaman login	Sesuai
2	User	Akses kartu milik sendiri	Data kartu tampil	Data kartu tampil	Sesuai
3	Super admin	Mengakses seluruh menu administratif	Seluruh menu dapat ditampilkan	Seluruh menu dapat ditampilkan	Sesuai
4	Admin Teknis	Mengakses menu sesuai hak akses	Hanya menu Admin Teknis yang ditampilkan	Hanya menu Admin Teknis yang ditampilkan	Sesuai
5	Operator	Mengakses menu sesuai hak akses	Hanya menu Operator yang ditampilkan	Hanya menu Operator yang ditampilkan	Sesuai

Berdasarkan Tabel 4.13, seluruh skenario pengujian telah berjalan sesuai dengan kebijakan *access control* yang ditetapkan. Tidak ditemukan lagi ketidaksesuaian tampilan menu maupun kegagalan *rendering* fitur yang sebelumnya ditemukan pada tahap *pretest*.



Gambar 4. 29 Menu Super Admin Tidak Tampil pada Role Admin Teknis



Gambar 4. 30 Menu Super Admin Tidak Tampil pada Role Operator

Gambar 4.30 hingga Gambar 4.31 menunjukkan bahwa menu Super Admin tidak lagi ditampilkan pada akun Administrator Teknis maupun Operator. Hal ini mengonfirmasi bahwa mekanisme *role-based rendering* pada sisi *frontend* kini telah berjalan konsisten dan selaras dengan kebijakan *access control* di sisi *backend*. Dengan demikian, informasi mengenai fitur administratif yang sebelumnya terekspos pada tahap *pretest* telah berhasil disembunyikan bagi pengguna yang tidak memiliki hak akses, sehingga prinsip *least privilege* telah diterapkan secara konsisten pada seluruh lapisan sistem.

Berdasarkan seluruh hasil pengujian yang dilakukan, tidak ditemukan lagi ketidaksesuaian implementasi access control pada antarmuka pengguna. Seluruh menu dan fitur telah ditampilkan sesuai dengan hak akses masing-masing role, sehingga prinsip least privilege dapat diterapkan secara lebih konsisten pada sisi frontend. Dengan demikian, kelemahan berupa kebocoran menu administratif telah berhasil diperbaiki setelah dilakukan implementasi penguatan keamanan.

4.4.3.2 Posttest Role-Based Access Control (RBAC)

Pengujian RBAC pada *backend* dilakukan kembali untuk memastikan bahwa implementasi mekanisme keamanan tambahan (*Session Management* dan *IP Whitelisting*) tidak menyebabkan regresi atau kerusakan pada logika otorisasi yang telah ada. Pengujian dilakukan menggunakan skenario yang sama seperti pada tahap pretest melalui *Postman* untuk memverifikasi konsistensi hak akses pada *endpoint* administratif.

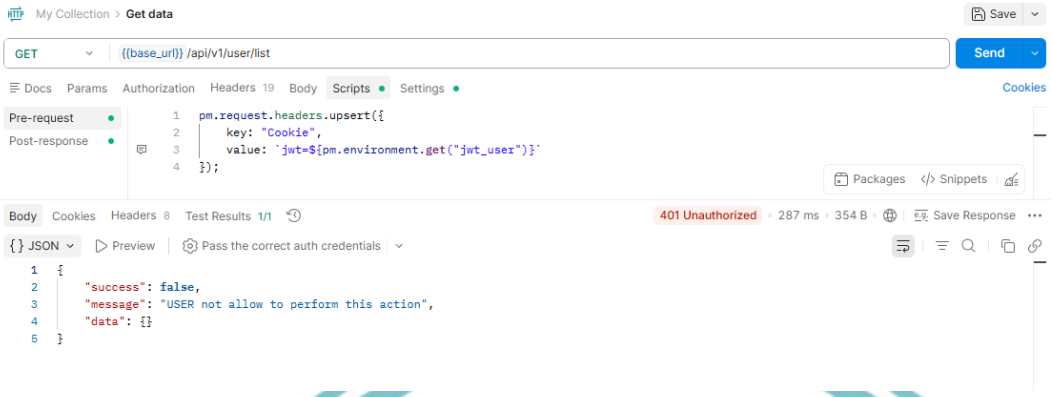
Tabel 4.14 Ringkasan Hasil Pengujian RBAC Backend Setelah Implementasi

Tabel 4. 14 Ringkasan Hasil Posttest RBAC Backend

Kategori	Jumlah skenario	Sesuai	Tidak sesuai
Endpoint administratif	9	9	0

Berdasarkan hasil pengujian yang dirangkum pada Tabel 4.14, seluruh skenario pengujian berhasil dijalankan sesuai dengan kebijakan akses yang ditetapkan. Tidak ditemukan adanya *endpoint* yang dapat diakses oleh pengguna di luar hak akses yang dimilikinya.

Implementasi mekanisme keamanan tambahan terbukti tidak mengganggu alur validasi pada *middleware* otorisasi. Sebagai contoh, percobaan akses *user* terhadap *endpoint* /api/v1/user/list tetap konsisten memberikan respons *401 Unauthorized* (atau *403 Forbidden*) sebagaimana ditunjukkan pada Gambar 4.43.



Gambar 4. 31 User Mengakses User List

Gambar 4.32 menunjukkan bukti bahwa sistem tetap menolak akses tidak sah dengan tepat. Berdasarkan seluruh hasil pengujian ini, dapat disimpulkan bahwa penerapan lapisan keamanan tambahan pada penelitian ini berjalan secara berlapis (*defense-in-depth*) tanpa menimbulkan konflik pada mekanisme otorisasi yang telah ada sebelumnya.

4.4.3.3 Posttest IP Whitelist

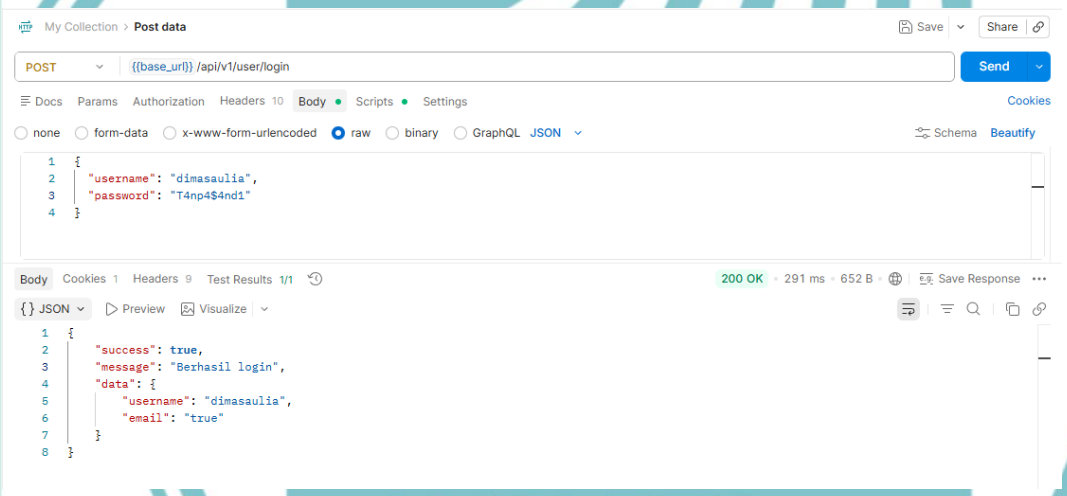
Pengujian *IP Whitelisting* dilakukan untuk mengevaluasi efektivitas mekanisme pembatasan akses berbasis jaringan yang telah diterapkan. Pengujian ini bertujuan untuk memastikan bahwa hanya pengguna administratif yang berasal dari alamat IP terdaftar yang dapat mengakses sistem, serta memverifikasi bahwa perubahan alamat IP selama sesi berlangsung akan memicu penghentian sesi otomatis.

Tabel 4. 15 Hasil Posttest IP Whitelisting

No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
1	Login akun admin menggunakan IP yang terdaftar pada whitelist	Login berhasil	200 OK. Login berhasil	Sesuai
2	Login akun admin menggunakan IP yang tidak terdaftar	Akses ditolak	403 Forbidden	Sesuai
3	Pengguna dengan role biasa mengakses sistem dari IP mana pun	Akses berhasil	200 OK. Login berhasil	Sesuai

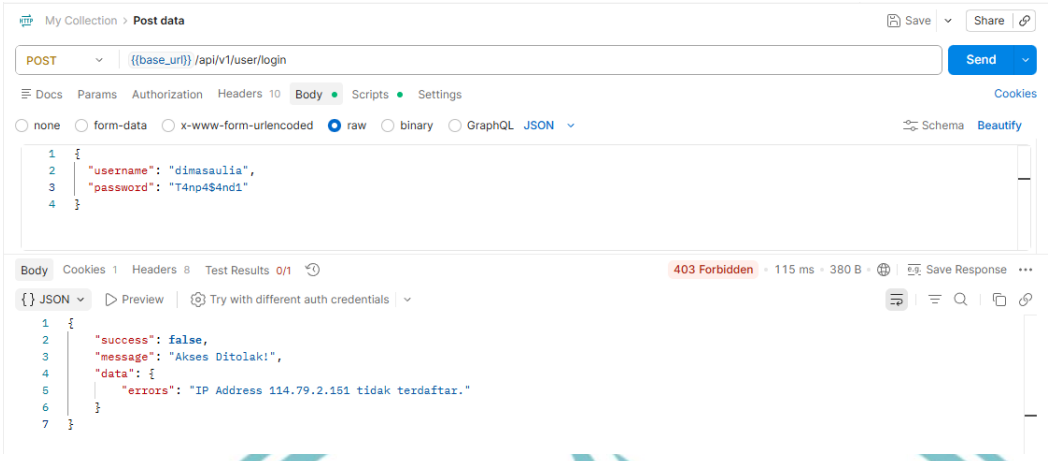
No	Skenario Pengujian	Hasil yang diharapkan	Hasil aktual	Status
4	Mengakses endpoint yang dilindungi dari alamat IP yang berbeda setelah berhasil login menggunakan alamat IP yang terdaftar.	Akses ditolak	403 Forbidden	Sesuai
5	Perubahan jaringan saat sesi berlangsung	Sesi dihentikan	401 Unauthorized	Sesuai

Berdasarkan Tabel 4.15, seluruh skenario pengujian berhasil dijalankan sesuai dengan kebijakan yang ditetapkan. Hasil pengujian menunjukkan bahwa sistem berhasil membatasi akses pengguna administratif secara ketat serta mampu mendeteksi penggunaan token dari jaringan yang tidak sah.



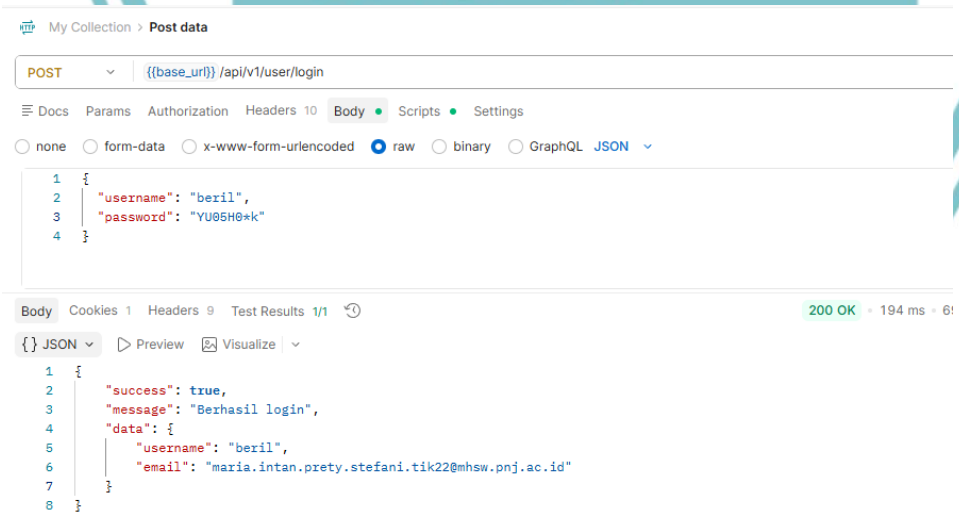
Gambar 4. 32 Login Berhasil dari Alamat IP yang Terdaftar

Gambar 4.33 menunjukkan hasil pengujian ketika pengguna dengan role yang dikenakan kebijakan IP Whitelist melakukan proses login menggunakan perangkat yang terhubung ke jaringan yang telah terdaftar pada whitelist. Pada skenario ini, pengguna mengakses halaman login menggunakan browser dan memasukkan kredensial yang valid. Sistem kemudian melakukan identifikasi role pengguna dan memverifikasi alamat IP yang digunakan. Karena alamat IP tersebut sesuai dengan daftar whitelist, proses autentikasi dilanjutkan dan sistem berhasil menerbitkan token autentikasi. Hasil pengujian menunjukkan bahwa sistem memberikan respons HTTP 200 OK sehingga pengguna dapat mengakses aplikasi secara normal.



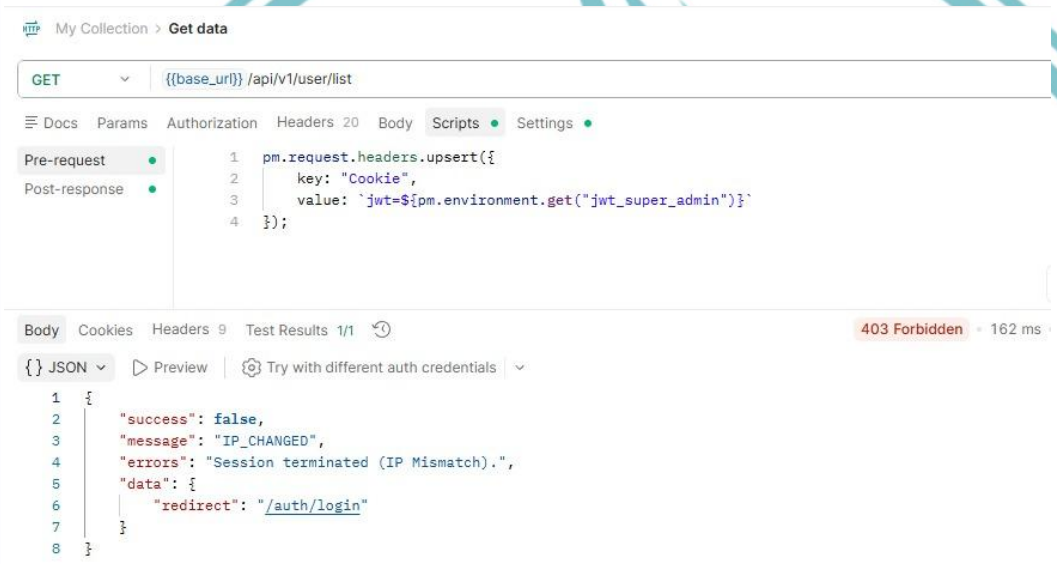
Gambar 4. 33 Login Ditolak dari Alamat IP yang Tidak Terdaftar

Gambar 4.34 menunjukkan hasil pengujian ketika pengguna dengan role administratif mencoba melakukan login menggunakan perangkat yang terhubung ke jaringan yang tidak terdaftar pada whitelist. Pada skenario ini, kredensial login yang digunakan tetap valid, namun alamat IP yang digunakan tidak terdapat pada daftar IP yang diizinkan. Sistem mendeteksi ketidaksesuaian tersebut pada middleware loginIpWhitelistCheck dan menghentikan proses autentikasi sebelum token diterbitkan. Akibatnya, sistem mengembalikan respons HTTP 403 Forbidden disertai pesan bahwa alamat IP tidak terdaftar. Hasil ini menunjukkan bahwa mekanisme IP Whitelist berhasil mencegah akses dari jaringan yang tidak sah meskipun pengguna mengetahui username dan password yang benar.



Gambar 4. 34 Role Pengguna Biasa Tidak Dikenakan Kebijakan IP Whitelist

Gambar 4.35 menunjukkan hasil pengujian terhadap pengguna dengan role biasa yang tidak termasuk ke dalam kategori pembatasan IP. Pengujian dilakukan dengan menggunakan alamat IP yang tidak terdapat pada whitelist. Meskipun demikian, proses autentikasi tetap berhasil dilakukan karena pengguna tersebut tidak termasuk ke dalam kelompok role yang diawasi oleh mekanisme IP Whitelist. Hasil ini menunjukkan bahwa implementasi pembatasan IP hanya diterapkan pada akun dengan tingkat privilese tinggi, yaitu Super Admin, Administrator Teknis, dan Operator, sehingga tidak mengurangi fleksibilitas akses bagi pengguna biasa.



Gambar 4. 35 Token dari Jaringan Berbeda Berhasil Dideteksi Sistem

Gambar 4.36 menunjukkan hasil pengujian terhadap mekanisme pemantauan alamat IP selama sesi berlangsung. Pengujian dilakukan menggunakan dua perangkat dengan jaringan yang berbeda. Pada perangkat pertama (Device A), pengguna melakukan login menggunakan jaringan yang telah terdaftar pada whitelist sehingga proses autentikasi berhasil dan token JWT berhasil diperoleh. Selanjutnya, token tersebut disalin dan digunakan pada perangkat kedua (Device B) yang terhubung ke jaringan yang tidak terdaftar. Pengujian dilakukan menggunakan Postman dengan menambahkan token JWT hasil login sebelumnya pada header Authorization untuk mengakses endpoint yang dilindungi.

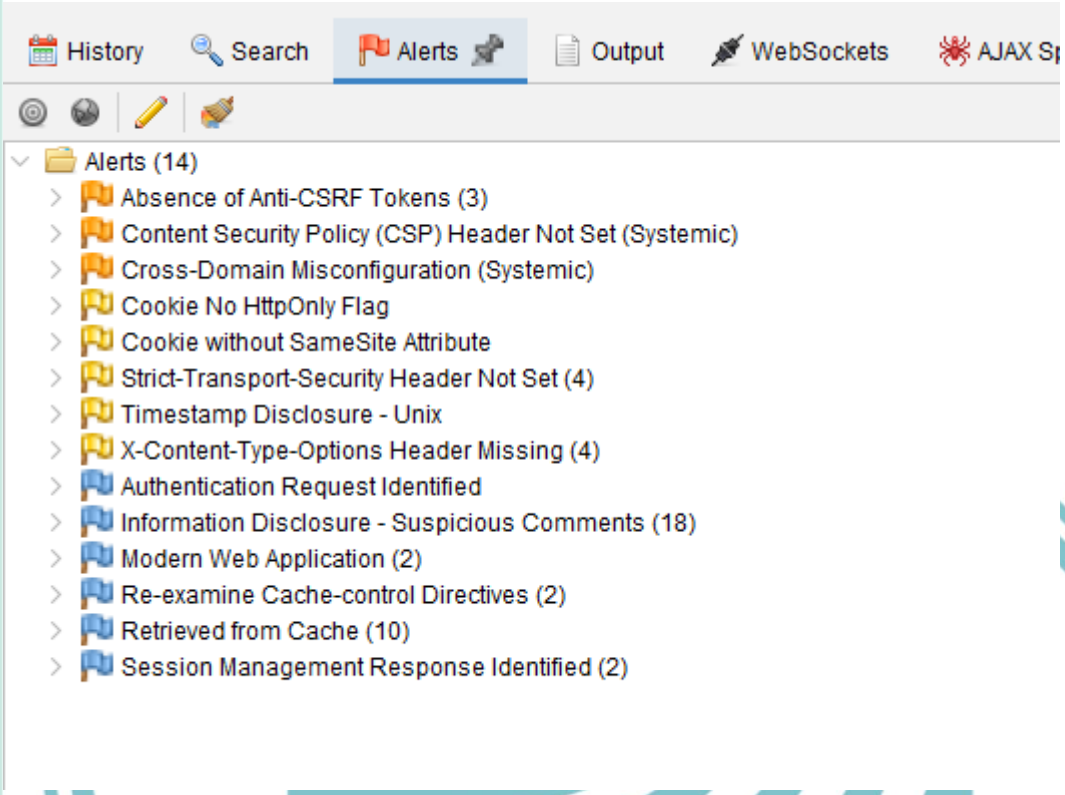
Ketika request dikirimkan, middleware ipWhitelistCheck melakukan identifikasi pengguna dan memeriksa alamat IP yang digunakan pada perangkat kedua. Karena alamat IP tersebut tidak sesuai dengan daftar whitelist, sistem mendeteksi adanya ketidaksesuaian jaringan dan menganggap sesi tidak lagi berasal dari sumber yang sah. Akibatnya, sistem menghentikan sesi aktif dan menolak permintaan dengan mengembalikan respons HTTP 401 Unauthorized atau HTTP 403 Forbidden sesuai dengan konfigurasi yang diterapkan.

Hasil pengujian ini menunjukkan bahwa token autentikasi yang berhasil diperoleh dari jaringan yang sah tidak dapat digunakan kembali dari jaringan yang berbeda. Dengan demikian, implementasi IP Whitelist tidak hanya mampu membatasi proses login, tetapi juga memberikan perlindungan tambahan terhadap risiko pencurian dan penyalahgunaan token autentikasi oleh pihak yang tidak berwenang.

Berdasarkan seluruh skenario pengujian yang dilakukan, mekanisme IP Whitelist berhasil diterapkan sesuai dengan rancangan yang telah dibuat. Sistem mampu membatasi akses pengguna administratif hanya dari alamat IP yang telah terdaftar serta melakukan penghentian sesi apabila terjadi perubahan alamat IP selama sesi berlangsung. Dengan demikian, implementasi IP Whitelist berhasil menambahkan lapisan keamanan tambahan pada sistem dan membantu meminimalkan risiko penyalahgunaan akun maupun token autentikasi dari jaringan yang tidak sah.

4.4.4 Posttest Kerentanan Menggunakan OWASP ZAP

Setelah dilakukan implementasi penguatan keamanan pada aspek Session Management dan Access Control, dilakukan pengujian ulang (posttest) menggunakan OWASP Zed Attack Proxy (ZAP). Pengujian ini bertujuan untuk memverifikasi efektivitas mekanisme keamanan yang telah diterapkan serta memastikan bahwa kerentanan yang ditemukan pada tahap pretest telah berhasil diminimalkan.



Gambar 4. 36 Hasil Posttest Pemindaian OWASP ZAP

Gambar 4.37 menunjukkan hasil pemindaian keamanan menggunakan OWASP ZAP setelah dilakukan implementasi penguatan keamanan. Berdasarkan hasil pemindaian, beberapa temuan yang berkaitan dengan kategori Session Management berhasil diminimalkan melalui penerapan atribut keamanan pada cookie autentikasi dan penguatan konfigurasi pengelolaan sesi.

Tabel 4. 16 Hasil Posttest OWASP ZAP

No	Temuan	Risk	ASVS	Keterangan
1	Cookie without SameSite Attribute	Medium	V3 Session Management	Berhasil dimitigasi melalui konfigurasi SameSite pada cookie autentikasi
2	Session Management Response Identified	Informational	V3 Session Management	Mekanisme pengelolaan sesi telah diperkuat melalui implementasi logout dan timeout sesi
3	Re-examine Cache-Control	Low	V3 Session Management	Konfigurasi cache telah diperkuat melalui

No	Temuan	Risk	ASVS	Keterangan
	Directives			middleware Helmet
4	Absence of Anti-CSRF Tokens	Medium	-	Temuan di luar ruang lingkup penelitian
5	Strict-Transport-Security Header Not Set	Medium	-	Temuan di luar ruang lingkup penelitian
6	X-Content-Type-Options Header Missing	Low	-	Temuan di luar ruang lingkup penelitian

Berdasarkan Tabel 4.16, terlihat adanya peningkatan kondisi keamanan dibandingkan dengan hasil pengujian pada tahap pretest. Penguatan pada aspek Session Management melalui implementasi token blacklist, mekanisme timeout sesi, serta konfigurasi atribut SameSite pada cookie autentikasi berhasil mengurangi risiko penyalahgunaan sesi pengguna.

Meskipun masih ditemukan beberapa alert dengan tingkat risiko Medium dan Low, sebagian temuan tersebut berada di luar ruang lingkup penelitian dan tidak berkaitan secara langsung dengan kategori OWASP ASVS yang menjadi fokus penelitian. Secara keseluruhan, hasil pemindaian OWASP ZAP menunjukkan bahwa implementasi penguatan keamanan yang dilakukan telah meningkatkan keamanan aplikasi, khususnya pada aspek Session Management dan Access Control, serta mendukung hasil pengujian manual yang telah dilakukan pada tahap posttest.

4.5 Analisis Hasil Pengujian

Analisis hasil pengujian dilakukan untuk mengevaluasi efektivitas implementasi penguatan keamanan yang telah diterapkan pada website monitoring IoT Smart Door Lock. Evaluasi dilakukan dengan membandingkan hasil pengujian pada tahap pretest dan posttest berdasarkan skenario pengujian yang telah disusun pada Bab III. Pengujian dilakukan terhadap aspek Authentication, Session Management, Access Control, dan IP Whitelisting yang mengacu pada kategori OWASP ASVS versi 4.0.3 Level 2.

Pada tahap pretest, dilakukan pengujian terhadap 26 skenario yang terdiri atas 4 skenario authentication, 3 skenario session management, 5 skenario access control pada antarmuka pengguna, 9 skenario access control pada backend, dan 5 skenario IP whitelisting. Dari keseluruhan skenario tersebut, sebanyak 17 skenario menunjukkan hasil yang sesuai dengan kondisi yang diharapkan, sedangkan 9 skenario lainnya belum memenuhi mekanisme keamanan yang seharusnya diterapkan.

Persentase keberhasilan pengujian pada tahap pretest dihitung menggunakan Persamaan sebagai berikut:

$$Persentase\ Keberhasilan\ Pretest = \frac{17}{26}\ x\ 100\% = 65.4\%$$

Setelah dilakukan implementasi penguatan keamanan berupa penyempurnaan mekanisme Role-Based Access Control (RBAC), penerapan session management, serta IP Whitelisting, dilakukan pengujian kembali menggunakan skenario yang sama. Hasil pengujian pada tahap posttest menunjukkan bahwa seluruh skenario pengujian berhasil memenuhi kondisi yang diharapkan sehingga diperoleh persentase keberhasilan sebagai berikut:

$$Persentase\ Keberhasilan\ Posttest = \frac{26}{26}\ x\ 100\% = 100\%$$

Ringkasan hasil pengujian pada tahap pretest dan posttest ditunjukkan pada Tabel 4.17.

Tabel 4. 17 Perbandingan Pretest Posttest

Tahap pengujian	Skenario Berhasil	Jumlah Skenario	Presentase
Pretest	17	26	65.4%
Posttest	26	26	100%

Berdasarkan Tabel 4.17, terjadi peningkatan persentase keberhasilan pengujian dari 65.4% pada tahap pretest menjadi 100% pada tahap posttest. Peningkatan tersebut menunjukkan bahwa mekanisme penguatan keamanan yang diterapkan berhasil

meningkatkan efektivitas kontrol akses pada website monitoring IoT Smart Door Lock.

Sebelum dilakukan implementasi penguatan keamanan, masih ditemukan beberapa skenario yang belum memenuhi kondisi yang diharapkan, terutama pada aspek session management, implementasi role-based rendering pada antarmuka pengguna, serta belum diterapkannya mekanisme pembatasan akses berdasarkan alamat IP. Setelah dilakukan implementasi perbaikan, seluruh skenario pengujian berhasil dipenuhi sehingga mekanisme authentication, session management, access control, dan IP whitelisting telah berjalan sesuai dengan yang diharapkan.

Dengan demikian, implementasi penguatan keamanan yang diterapkan mampu meningkatkan efektivitas kontrol akses serta meminimalkan risiko terjadinya Broken Access Control pada website monitoring IoT Smart Door Lock.

Tabel 4. 18 Rekapitulasi Hasil Pretest dan Posttest

No	Skenario Pengujian	Pretest	Postest	ASVS
1	Menu Super Admin muncul pada Admin Teknis	Tidak sesuai	Sesuai	V4 Access Control
2	Menu Super Admin muncul pada Operator	Tidak sesuai	Sesuai	V4 Access Control
3	Token masih dapat digunakan setelah logout	Tidak sesuai	Sesuai	V3 Session Management
4	Masa berlaku token terlalu panjang tanpa idle timeout	Tidak sesuai	Sesuai	V3 Session Management
5	Akses tidak dibatasi berdasarkan alamat IP	Tidak sesuai	Sesuai	V4 Access Control
6	Penggunaan token dari IP yang berbeda	Tidak sesuai	Sesuai	V4 Access Control
7	Cookie belum memiliki atribut SameSite	Tidak sesuai	Sesuai	V3 Session Management

Berdasarkan Tabel 4.18, seluruh kelemahan yang ditemukan pada tahap *pretest* berhasil diperbaiki. Hasil pengujian *posttest* membuktikan bahwa setiap kontrol keamanan yang diterapkan mampu bekerja sesuai dengan tujuan mitigasi. Berikut

adalah analisis mendalam terhadap aspek keamanan berdasarkan kategori OWASP ASVS Level 2.

4.5.1 Analisis Berdasarkan Kategori OWASP ASVS

1. Analisis *Access Control* (ASVS V4): Perbaikan pada mekanisme *role-based rendering* di sisi *frontend* telah menghilangkan kebocoran visibilitas menu administratif bagi pengguna yang tidak berwenang. Integrasi *IP Whitelisting* sebagai lapisan keamanan tambahan berhasil memastikan bahwa akun administratif tidak dapat disalahgunakan dari jaringan luar yang tidak terdaftar. Hal ini mengonfirmasi terpenuhinya prinsip *least privilege* dan pembatasan akses berbasis jaringan.

2. Analisis *Session Management* (ASVS V3): Kelemahan berupa token yang tetap aktif pasca-*logout* telah dimitigasi melalui mekanisme *token invalidation* berbasis passwordUpdatedAt. Penambahan *Absolute Timeout* (8 jam) dan *Idle Timeout* (15 menit) telah memperpendek siklus hidup sesi yang sebelumnya terlalu panjang dan rentan terhadap *session hijacking*.

BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil evaluasi keamanan dan implementasi penguatan keamanan pada aplikasi web monitoring Smart Door Lock, maka dapat disimpulkan sebagai berikut:

1. Hasil evaluasi awal menunjukkan bahwa aplikasi web monitoring Smart Door Lock masih memiliki beberapa kelemahan keamanan, terutama pada aspek access control dan session management. Kerentanan yang ditemukan meliputi tampilan menu yang tidak sesuai dengan hak akses pengguna, akses langsung terhadap endpoint tanpa pembatasan yang memadai, token autentikasi yang masih dapat digunakan setelah proses logout, serta tidak adanya pembatasan akses berdasarkan alamat IP pada akun dengan hak akses tinggi.

2. Implementasi penguatan keamanan menggunakan penyelarasan Role-Based Access Control (RBAC), mekanisme invalidasi token setelah logout, idle timeout, absolute timeout, dan IP whitelisting berhasil diterapkan pada sistem. Mekanisme tersebut mampu membatasi akses sesuai hak akses pengguna, menghentikan sesi yang tidak aktif secara otomatis, mencegah penggunaan kembali token yang telah logout, serta membatasi akses akun administratif hanya dari alamat IP yang telah terdaftar.

3. Berdasarkan hasil pengujian setelah implementasi, tingkat keberhasilan mitigasi meningkat dari 65,4% (17 dari 26 skenario) pada tahap pretest menjadi 100% (26 dari 26 skenario) pada tahap posttest. Implementasi penyelarasan RBAC, penguatan session management, dan IP whitelisting berhasil memastikan akses sesuai role, mencegah penggunaan kembali token setelah logout, mengakhiri sesi secara otomatis sesuai batas waktu yang ditentukan, serta menolak akses dari alamat IP yang tidak terdaftar. Selain itu, hasil vulnerability assessment menggunakan OWASP ZAP menunjukkan penurunan jumlah temuan kerentanan dari 16 alert menjadi

14 alert, yang menunjukkan adanya peningkatan keamanan pada aplikasi web monitoring Smart Door Lock.

5.2 Saran

Berdasarkan hasil penelitian, implementasi, dan evaluasi yang telah dilakukan pada aplikasi web monitoring Smart Door Lock, terdapat beberapa saran yang dapat digunakan sebagai acuan pengembangan sistem selanjutnya, yaitu sebagai berikut:

1. Pengujian keamanan dapat diperluas dengan menggunakan standar dan skenario pengujian yang lebih komprehensif, seperti penetration testing pada lingkungan produksi, sehingga tingkat keamanan sistem dapat dievaluasi secara lebih menyeluruh.
2. Pengembangan berikutnya dapat mempertimbangkan penambahan mekanisme keamanan pada sisi autentikasi, seperti Multi-Factor Authentication (MFA) guna meningkatkan perlindungan terhadap penyalahgunaan akun tanpa mengubah struktur utama sistem yang sudah ada.
3. Sistem dapat dikembangkan dengan menambahkan fitur audit logging untuk mencatat aktivitas pengguna secara lebih detail, sehingga dapat mendukung proses monitoring dan investigasi apabila terjadi aktivitas yang tidak sesuai dengan kebijakan keamanan.

DAFTAR PUSTAKA

Adidrana, D., Suryoprayogo, H., & Hakim, A. R. (2022). Perancangan sistem *smart door lock* menggunakan *Internet of Things* (Studi kasus: Institut Teknologi Telkom Jakarta). *Journal of Informatics and Communications Technology (JICT), 4*(2), 102–108.

Al-Adhim, M. F., & Dewi, G. S. (2024). Sistem monitoring IoT smart farm berbasis web dengan integrasi template dashboard Bootstrap dan Laravel 10 (*Web-based smart farm IoT monitoring system with Bootstrap and Laravel 10 dashboard template integration*). *Comserva: Jurnal Penelitian dan Pengabdian Masyarakat, 4*(7), 1973–1981. https://doi.org/10.59141/comserva.v4i7.2595

Andriana, E. A., & Satwika, Y. W. (2025). Analisis kuantitatif deskriptif tingkat keterikatan kerja pada guru SMK (*Descriptive quantitative analysis of the level of work engagement in vocational school teachers*). *Character: Jurnal Penelitian Psikologi, 12*(1), 143–152. https://doi.org/10.26740/cjpp.v12n1.p143-152

Fachrudin, D. A. (2023). *Rancang bangun sistem pintu cerdas dengan arsitektur multi network dan event driven data synchronization* [Skripsi sarjana terapan, Politeknik Negeri Jakarta]. Politeknik Negeri Jakarta.

Hamdallah, F. (2025). Analisis kerentanan *broken access control*, *cryptographic failures* dan *injection* pada aplikasi bimbingan konseling menggunakan *white-box testing*. *MJ: Jurnal Multidisiplin, 3*(3), 528–535.

Kurnia, R., & Huizen, L. M. (2026). Implementasi Node.js dan keamanan JWT untuk sistem informasi manajemen sekolah dasar berbasis web. *Jurnal TRANSFORMATIKA, 23*(2), 213–219.

Kurniawan, M. C., Gamayanto, I., Sanyoto, G. K., & Widjajanto, B. (2025). Security evaluation of Keycloak-based role-based access control in microservice architectures using the OWASP ASVS framework. *Journal of Applied Informatics and Computing (JAIC), 9*(6), 3964–3973.

Kusnana, Gymnastiar, P., & Riswanto, B. (2025). Analisis kerentanan *Insecure Direct Object Reference* (IDOR) dan *Broken Access Control* pada aplikasi invoice berbasis web. *Digital Transformation Technology (Digitech), 5*(2). https://doi.org/10.47709/digitech.v5i2.6948

Mu'min, M. A., Tristanti, N., & Fanani, G. P. I. (2024). Analisis dan pengujian kerentanan website menggunakan OWASP ZAP. *Jurnal Riset Sistem dan Teknologi Informasi (RESTIA), 3*(1), 36–50.

Muhammad, A., Hadiana, A. I., & Ilyas, R. (2025). Eksploitasi *Broken Access Control* untuk eskalasi hak akses pada LMS Universitas XYZ. *Jurnal Algoritma*. https://doi.org/10.33364/algoritma/v.1-1.2287

Prasetyo, A., & Zulkarnain, A. (2025). Perancangan sistem absensi berbasis web yang aman dengan validasi lokasi menggunakan QR code dan pengendalian akses berbasis IP. *INSERT: Information System and Emerging Technology Journal, 6*(1).

Purba, A. D. (2024). *Analisis dan mitigasi broken access control dan broken authentication pada OWASP Juice Shop. Seminar Nasional Informatika Bela Negara (SANTIKA), 4*.

Purba, D. A., & Hidayasari, N. (2026). Implementasi *Role-Based Access Control* (RBAC) pada sistem informasi manajemen stok obat. *Sistemasi: Jurnal Sistem Informasi, 15*(2), 684–698.

Septian, F., Arfian, M. H., Asri, J. S., & Tjahjono, B. (2024). Pengujian keamanan website dengan metode penetration testing (Studi kasus: Universitas Esa Unggul). *Innovative: Journal of Social Science Research, 4*(5), 3629–3647. https://doi.org/10.31004/innovative.v4i5.15197

Sriyasa, I. W., & Sugara, V. I. (2024). Analisis keamanan website menggunakan *Open Web Application Security Project* (OWASP). *Indonesian Journal of Computer Science, 13*(2). https://doi.org/10.33022/ijcs.v13i2.3736

Sutanto, E. A. B., Tiurlina, & Fatihaturosyidah. (2023). Efektivitas model pembelajaran Polya terhadap kemampuan pemecahan masalah matematika

siswa dalam menyelesaikan soal cerita materi bangun ruang di kelas V SDN Cilegon IX. *Didaktika, 3*(4), 388–397.

Zahra, F. A., & Nasution, M. I. P. (2025). Analisis implementasi model kontrol akses berbasis peran dan enkripsi untuk keamanan data pada sistem basis data relasional. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, 2*(12), 561–567. https://doi.org/10.5281/zenodo.15683326

DAFTAR RIWAYAT HIDUP

Maria Intan Prety Stefani

Lahir di Bogor pada tahun 2003, Merupakan anak ketiga dari tiga bersaudara, berdomisili di Kota Depok. Lulus pendidikan dasar pada tahun 2016. Kemudian melanjutkan pendidikan menengah pertama dan lulus pada tahun 2019. Kemudian melanjutkan pendidikan menengah atas dan lulus pada tahun 2022. Kemudian melanjutkan pendidikan sebagai mahasiswa Diploma Empat (D4) Politeknik Negeri Jakarta (PNJ) dengan jurusan Teknik Informatika dan Komputer dengan prodi Teknik Multimedia dan Jaringan.

.

LAMPIRAN

Lampiran 1. Link Source Code

https://github.com/fanymaria/smartdoor-server.git