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 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