PENGEMBANGAN ALAT BANTU BERBASIS AI AGENT UNTUK DETEKSI KERENTANAN BROKEN ACCESS CONTROL MELALUI OTOMATISASI PENGUJIAN ENDPOINT PADA APLIKASI BACK-END

SKRIPSI

CAROLINE SUSANTO
00000071280

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

PENGEMBANGAN ALAT BANTU BERBASIS AI AGENT UNTUK DETEKSI KERENTANAN BROKEN ACCESS CONTROL MELALUI OTOMATISASI PENGUJIAN ENDPOINT PADA APLIKASI BACK-END

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

CAROLINE SUSANTO
00000071280

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Caroline Susanto
Nomor Induk Mahasiswa	:	00000071280
Program Studi	:	Informatika

Skripsi dengan judul:

Pengembangan Alat Bantu Berbasis AI Agent untuk Deteksi Kerentanan Broken Access Control melalui Otomatisasi Pengujian Endpoint pada Aplikasi Back-End

merupakan hasil karya saya sendiri bukan plagiat dari laporan karya tulis ilmiah yang ditulis oleh orang lain, dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan maupun dalam penulisan laporan karya tulis ilmiah, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah yang telah saya tempuh.

Tangerang, 13 November 2025

(Caroline Susanto)

HALAMAN PENGESAHAN

Skripsi dengan judul

PENGEMBANGAN ALAT BANTU BERBASIS AI AGENT UNTUK DETEKSI KERENTANAN BROKEN ACCESS CONTROL MELALUI OTOMATISASI PENGUJIAN ENDPOINT PADA APLIKASI BACK-END

oleh

Nama	:	Caroline Susanto
NIM	:	00000071280
Program Studi	:	Informatika
Fakultas	:	Fakultas Teknik dan Informatika

Telah diujikan pada hari Jumat, 21 November 2025
Pukul 15.00 s/s 17.00 dan dinyatakan
LULUS
Dengan susunan penguji sebagai berikut

Ketua Sidang	Penguji
(Dr. Maria Irmina Prasetiyowati, S.Kom., M.T.)	(David Agustriawan, S.Kom., M.Sc., Ph.D.)
NIDN: 0725057201	NIDN: 0525088601

Pembimbing

(Moeljono Widjaja, B.Sc., M.Sc., Ph.D)
NIDN: 0311106903

Ketua Program Studi Informatika,

(Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH, CEI)
NIDN: 0315109103

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini:

Nama	:	Caroline Susanto
NIM	:	00000071280
Program Studi	:	Informatika
Jenjang	:	S1
Judul Karya Ilmiah	:	Pengembangan Alat Bantu Berbasis AI Agent untuk Deteksi Kerentanan Broken Access Control melalui Otomatisasi Pengujian Endpoint pada Aplikasi Back-End

Menyatakan dengan sesungguhnya bahwa saya bersedia:

☑ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya ke dalam repositori Knowledge Center sehingga dapat diakses oleh Sivitas Akademika UMN/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial.

☐ Saya tidak bersedia mempublikasikan hasil karya ilmiah ini ke dalam repositori Knowledge Center, dikarenakan: dalam proses pengajuan publikasi ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*) **.

☐ Lainnya, pilih salah satu:

- Hanya dapat diakses secara internal Universitas Multimedia Nusantara
- Embargo publikasi karya ilmiah dalam kurun waktu tiga tahun.

Tangerang, 13 November 2025

Yang menyatakan

Caroline Susanto

HALAMAN PERSEMBAHAN / MOTTO

”Hanya Kau tempatku berharap, berjalan bersama-Mu ’ku takkan goyah, sebab tangan kasih-Mu tersedia bagiku, s’lamanya Kau kucinta.”

Hanya Kau, Sari Simorangkir

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir berjudul "Pengembangan Alat Bantu Berbasis AI Agent untuk Deteksi Kerentanan Broken Access Control melalui Otomatisasi Pengujian Endpoint pada Aplikasi Back-End" dengan baik.

Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Universitas Multimedia Nusantara (UMN). Penelitian berfokus pada perancangan dan implementasi AI *Agent* untuk otomatisasi pengujian *endpoint back-end* pada aplikasi *Employee Self Service* (ESS), khususnya dalam mendeteksi kerentanan *Broken Access Control*. Ucapan terima kasih penulis sampaikan kepada:

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH, CEI, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Moeljono Widjaja, B.Sc., M.Sc., Ph.D, sebagai Pembimbing yang telah memberikan bimbingan, arahan, dan motivasi atas terselesainya tugas akhir ini.
5. Kepada Pembimbing di Perusahaan yang telah memberikan saran selama pelaksanaan tugas akhir.
6. Kepada Mentor pertama di Perusahaan yang telah memberikan bimbingan, saran, serta ilmu di bidang kecerdasan buatan dan keamanan.
7. Kepada Mentor kedua di Perusahaan yang telah memberikan bimbingan, saran, serta ilmu di bidang pengembangan *back-end*.
8. Kepada Ayah, Ibu, dan Adik penulis yang telah memberikan dukungan moral dan material sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki keterbatasan. Oleh karena itu, saran dan kritik yang membangun sangat diharapkan demi perbaikan

di masa mendatang. Besar harapan penulis agar karya ini memberikan manfaat praktis bagi organisasi dalam meningkatkan keamanan aplikasi *back-end*, sekaligus kontribusi teoretis bagi pengembangan keilmuan di bidang keamanan aplikasi dan pengujian keamanan perangkat lunak dengan bantuan *Artificial Intelligence*.

Tangerang, 13 November 2025

Caroline Susanto

PENGEMBANGAN ALAT BANTU BERBASIS AI AGENT UNTUK DETEKSI KERENTANAN BROKEN ACCESS CONTROL MELALUI OTOMATISASI PENGUJIAN ENDPOINT PADA APLIKASI BACK-END

Caroline Susanto

ABSTRAK

Proses pembaruan data pribadi karyawan di PT. XYZ dilakukan secara manual melalui *Human Resource* dan dinilai tidak efektif karena memiliki potensi keterlambatan, kesalahan, dan risiko kebocoran data. Untuk mengatasi hal tersebut, dibangun aplikasi internal *Employee Self Service* berbasis arsitektur *decoupled* dengan implementasi *Role-Based Access Control*. Namun, pengujian keamanan *endpoint back-end* masih dilakukan secara manual menggunakan *Postman* dengan keterbatasan *coverage* hanya 50% dari 56 *endpoint*, waktu bervariasi signifikan, dan dokumentasi tidak terstruktur. Aplikasi ESS memiliki 28 *endpoint* kritis yang rentan terhadap *Broken Access Control* seperti *Insecure Direct Object Reference* dan *Broken Object Level Authorization*. Penelitian ini mengembangkan BYEBAC, alat bantu berbasis AI *Agent* untuk otomatisasi pengujian *endpoint back-end* guna mendeteksi kerentanan BAC *horizontal* dan vertikal. BYEBAC mengintegrasikan *Large Language Model* Gemini 3.0 *Pro Preview* sebagai *reasoning engine* untuk menganalisis matriks RBAC, *OpenAPI Specification*, dan *policy rules*. Sistem terdiri dari enam komponen modular yang bekerja dalam siklus *plan-discover-execute-classify-report* untuk melakukan *automated test planning*, *resource ID discovery*, *multi-role testing*, dan *AI-powered security summary*. Hasil pengujian pada 28 *endpoint* kritis menunjukkan BYEBAC mencapai akurasi 97,3% dengan *precision* 91,4%, *recall* 100%, dan *F1-score* 95,5% dengan konsistensi 100% pada lima eksekusi independen. BYEBAC menguji 130 *test case* dalam waktu rata-rata dua menit dengan *coverage* 100%, 89 kali lebih cepat dibandingkan pengujian manual tiga jam yang hanya mencakup 50% *endpoint*. Sistem berhasil mendeteksi seluruh kerentanan BAC tanpa *false negative* dan menghasilkan dokumentasi terstruktur format JSON dan *Markdown* yang dapat diintegrasikan pada *CI/CD*, meningkatkan efektivitas pengujian keamanan aplikasi ESS secara signifikan.

Kata kunci: Agen AI, *Broken Access Control*, *OpenAPI Specification*, Pengujian Keamanan Otomatis, *RESTful API*

DEVELOPMENT OF AN AI AGENT-BASED TOOL FOR BROKEN ACCESS CONTROL VULNERABILITY DETECTION THROUGH ENDPOINT TESTING AUTOMATION IN BACK-END APPLICATIONS

Caroline Susanto

ABSTRACT

The employee personal data update process at PT. XYZ is conducted manually through Human Resources and is considered ineffective due to potential delays, errors, and risks of data breaches. To address this, an internal Employee Self Service application was built using a decoupled architecture with Role-Based Access Control implementation. However, back-end endpoint security testing is still performed manually using Postman with limited coverage of only 50% of 56 endpoints, significantly varying time, and unstructured documentation. The ESS application has 28 critical endpoints vulnerable to Broken Access Control, such as Insecure Direct Object Reference and Broken Object Level Authorization. This research develops BYEBAC, an AI Agent-based tool for automating back-end endpoint testing to detect horizontal and vertical BAC vulnerabilities. BYEBAC integrates Large Language Model Gemini 3.0 Pro Preview as a reasoning engine to analyze RBAC matrix, OpenAPI Specification, and policy rules. The system consists of six modular components working in a plan-discover-execute-classify-report cycle to perform automated test planning, resource ID discovery, multi-role testing, and AI-powered security summary. Testing results on 28 critical endpoints show BYEBAC achieves 97.3% accuracy with a precision 91.4%, recall 100%, and an F1-score 95.5% with 100% consistency across five independent executions. BYEBAC tests 130 test cases in average two minutes with 100% coverage, 89 times faster than manual testing, three hours covering only 50% endpoints. The system successfully detects all BAC vulnerabilities without false negatives and generates structured documentation in JSON and Markdown format ready for CI/CD integration, significantly improving ESS application security testing effectiveness.

***Keywords**: AI Agent, Automated Security Testing, Broken Access Control, OpenAPI Specification, RESTful API*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR KODE

DAFTAR RUMUS

DAFTAR LAMPIRAN