Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS

https://doi.org/10.63447/jimik.v7i3.2005

Implementasi *Artificial Intelligence* untuk Analisis *Attack Surface* dan Rekomendasi Remediasi Kerentanan Keamanan Berbasis *Vulnerability Assessment* pada *Website* UMKM

Willy Wijayanto [1*], Yuma Akbar [2], Mesra Betty Yel [3]

[1*,2,3] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: willy_wijayanto@cki.ac.id [1*], yumekhan@stikomcki.ac.id [2], mesrabettyyel@stikomcki.ac.id [3]

Histori Artikel:
Dikirim 12 April 2026; *Diterima dalam bentuk revisi* 15 Mei 2026; *Diterima* 30 Juli 2026; *Diterbitkan* 10 September 2026.

Abstrak

Pesatnya digitalisasi sektor Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia mendorong kebutuhan terhadap keamanan website yang memadai, namun keterbatasan sumber daya teknis membuat banyak pelaku UMKM tidak mengetahui kondisi keamanan platform digitalnya. Penelitian ini bertujuan merancang dan mengimplementasikan VulnScope, yaitu sistem vulnerability assessment (VA) berbasis web yang mengintegrasikan Large Language Model (LLM) untuk menganalisis attack surface dan menghasilkan rekomendasi remediasi yang kontekstual. Sistem dikembangkan menggunakan kerangka kerja FastAPI dengan delapan modul pemindaian inti, modul aggressive scanner, serta VAPT Engine yang mengklasifikasikan temuan berdasarkan OWASP Top 10:2021 dan CVSS v3.1. Integrasi kecerdasan buatan diterapkan melalui model Claude dan Nous Hermes dengan pola agentic tool-use. Pengujian fungsional black box menunjukkan seluruh fitur berjalan sesuai spesifikasi. Penerapan pada website UMKM ibadahterpanjang.com berhasil mendeteksi empat kerentanan (satu Critical, satu Medium, dua Low) dengan tingkat risiko keseluruhan CRITICAL (skor 38/100). Hasil ini menunjukkan bahwa integrasi VA dan kecerdasan buatan efektif membantu pelaku UMKM mengidentifikasi serta menindaklanjuti kerentanan keamanan website secara mandiri.

Kata Kunci: Vulnerability Assessment; Large Language Model; Attack Surface; OWASP Top 10; CVSS; Keamanan Website UMKM.

Abstract

The rapid digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia has raised the need for adequate website security, yet limited technical resources leave many MSME owners unaware of their platform's security posture. This research designs and implements VulnScope, a web-based vulnerability assessment (VA) system that integrates a Large Language Model (LLM) to analyze the attack surface and generate contextual remediation recommendations. The system is built on the FastAPI framework with eight core scanning modules, an aggressive scanner, and a VAPT Engine that classifies findings based on OWASP Top 10:2021 and CVSS v3.1. Artificial intelligence is integrated through the Claude and Nous Hermes models using an agentic tool-use pattern. Black box functional testing confirmed that all features work as specified. Applied to the MSME website ibadahterpanjang.com, the system detected four vulnerabilities (one Critical, one Medium, two Low) with an overall CRITICAL risk level (score 38/100). The results show that integrating VA with artificial intelligence effectively helps MSME owners independently identify and remediate website security vulnerabilities.

Keyword: Vulnerability Assessment; Large Language Model; Attack Surface; OWASP Top 10; CVSS; MSME Website Security.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005

1. Pendahuluan

Perkembangan teknologi informasi yang pesat telah mendorong semakin banyak pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia untuk memanfaatkan platform digital sebagai sarana pemasaran dan transaksi. Menurut data Kementerian Koperasi dan UKM Republik Indonesia (2023), lebih dari 8,7 juta UMKM telah terhubung ke platform digital, suatu angka yang menunjukkan pertumbuhan signifikan dalam adopsi teknologi oleh sektor ini. Meskipun digitalisasi menawarkan berbagai peluang, peningkatan ini juga turut memperbesar permukaan serangan (*attack surface*) yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dalam skala global, lebih dari 60% UMKM di berbagai negara pernah mengalami serangan siber (Kaspersky, 2022), menyoroti pentingnya keamanan siber yang memadai bagi pelaku UMKM. Sebagian besar pelaku UMKM tidak memiliki keahlian dalam keamanan siber yang diperlukan untuk memeriksa dan mengevaluasi kondisi website mereka. Banyak dari mereka tidak menyadari potensi risiko yang dihadapi oleh platform digital yang mereka kelola. Alat penilaian kerentanan (*vulnerability assessment*) konvensional umumnya hanya menampilkan daftar temuan teknis tanpa memberikan panduan perbaikan yang mudah dipahami (Author dan Author, 2022). Hal ini mengakibatkan hasil pemindaian sering kali tidak ditindaklanjuti, sehingga kerentanan dibiarkan terbuka. Kerentanan seperti kesalahan konfigurasi dan penggunaan komponen usang menjadi penyebab utama peretasan website, yang dapat berakibat fatal bagi kelangsungan usaha (Armadhani *et al.*, 2022). Beberapa penelitian terdahulu telah menerapkan penilaian kerentanan berstandar OWASP pada website (Supangat *et al.*, 2025), serta memadukan pengujian penetrasi dan analisis kerentanan (Sai *et al.*, 2024). Meskipun demikian, pendekatan ini sering kali tidak mempertimbangkan tantangan unik yang dihadapi UMKM dalam hal sumber daya dan pengetahuan teknis. Di sisi lain, perkembangan *Large Language Model* (LLM) membuka peluang baru dalam bidang keamanan siber. LLM dapat berfungsi sebagai agen yang mampu mengorkestrasi alat keamanan secara mandiri dan mendukung deteksi kerentanan (Ramesh dan Author, 2025). Namun, integrasi kemampuan analisis LLM ke dalam proses penilaian kerentanan untuk UMKM masih jarang dibahas dalam literatur.

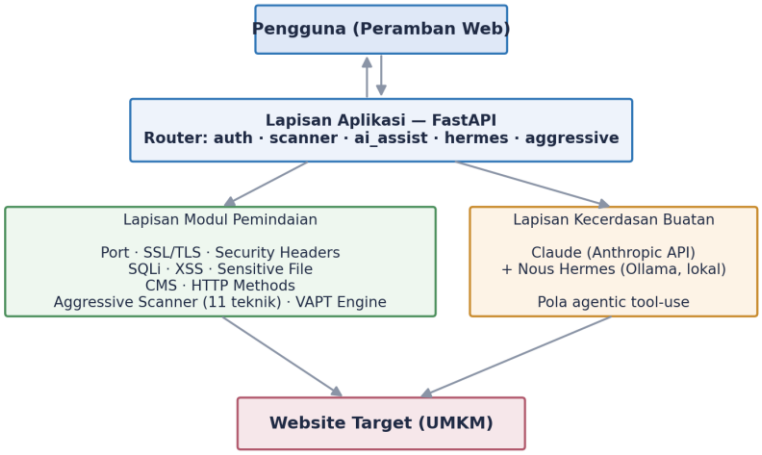
Penelitian ini mengusulkan VulnScope, sebuah aplikasi penilaian kerentanan berbasis web yang mengintegrasikan LLM untuk menganalisis permukaan serangan dan menghasilkan rekomendasi remediasi yang kontekstual dan mudah ditindaklanjuti oleh pelaku UMKM. VulnScope dirancang untuk memberikan solusi yang lebih mudah diakses bagi pelaku UMKM yang mungkin tidak memiliki latar belakang teknis yang kuat. Penelitian ini bertujuan untuk mencapai beberapa tujuan kunci: (1) merancang dan mengimplementasikan VulnScope sebagai sistem penilaian kerentanan berbasis web yang terintegrasi dengan kecerdasan buatan; (2) mengintegrasikan model Claude dan Nous Hermes untuk analisis otomatis dan rekomendasi remediasi; serta (3) mengevaluasi efektivitas sistem dalam mendeteksi dan mengklasifikasikan kerentanan pada website UMKM nyata berdasarkan OWASP Top 10:2021 dan CVSS v3.1. Dengan mengadopsi pendekatan ini, diharapkan VulnScope dapat memberikan kontribusi signifikan terhadap peningkatan keamanan siber di kalangan UMKM, membantu mereka dalam mengidentifikasi dan menanggulangi kerentanan secara mandiri. Penelitian ini juga berupaya mengisi kekurangan dalam literatur yang ada dengan mengeksplorasi bagaimana teknologi terbaru dapat dimanfaatkan untuk memenuhi kebutuhan spesifik sektor UMKM di Indonesia. Melalui implementasi dan evaluasi sistem ini, diharapkan dapat diperoleh wawasan baru mengenai efektivitas integrasi kecerdasan buatan dalam penilaian kerentanan, serta dampaknya terhadap keamanan digital pelaku UMKM.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan penelitian terapan dengan model pengembangan perangkat lunak *waterfall*, yang terdiri dari beberapa tahapan, yaitu studi literatur dan identifikasi masalah, analisis kebutuhan, perancangan sistem, implementasi, pengujian, serta analisis hasil. Objek

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005

penelitian yang digunakan adalah website UMKM *ibadahterpanjang.com*, di mana pengujian dilakukan atas izin pemilik website tersebut. Arsitektur sistem VulnScope dirancang secara modular dan terdiri atas empat lapisan, sebagaimana ditunjukkan pada Gambar 1. Keempat lapisan tersebut adalah: (1) lapisan pengguna (*client layer*) yang berfungsi sebagai antarmuka pengguna melalui peramban; (2) lapisan aplikasi yang berbasis FastAPI, mencakup pengaturan routing dan autentikasi; (3) lapisan modul pemindaian yang bertanggung jawab untuk melakukan analisis terhadap kerentanan; dan (4) lapisan kecerdasan buatan yang mengintegrasikan model-model AI untuk mendukung analisis dan rekomendasi remediasi. Pemisahan tanggung jawab di antara lapisan-lapisan ini memudahkan proses pemeliharaan dan pengembangan lanjutan, sejalan dengan prinsip pengelolaan infrastruktur jaringan yang tertata (Achmad *et al.*, 2022). Dengan arsitektur yang modular, setiap lapisan dapat ditingkatkan atau dimodifikasi secara independen, memungkinkan fleksibilitas dalam pengembangan sistem di masa depan. Setiap lapisan dilengkapi dengan fungsionalitas yang spesifik, sehingga kolaborasi antar-lapisan dapat berlangsung dengan efektif. Lapisan pengguna menyediakan antarmuka yang intuitif bagi pengguna akhir, sementara lapisan aplikasi memastikan pengolahan data yang efisien dan aman. Lapisan modul pemindaian berfokus pada identifikasi kerentanan yang ada, sedangkan lapisan kecerdasan buatan berperan dalam memberikan rekomendasi yang kontekstual berdasarkan analisis yang dilakukan. Dengan pendekatan ini, diharapkan VulnScope dapat menjadi alat yang efektif dalam membantu pelaku UMKM untuk meningkatkan keamanan website mereka dan menanggulangi potensi kerentanan yang ada.



Gambar 1. Arsitektur Sistem VulnScope

Lapisan modul pemindaian dalam sistem VulnScope memuat delapan modul inti, yaitu:
1) Port Scanner
2) SSL/TLS Check
3) Security Headers
4) SQL Injection Probe
5) XSS Probe
6) Sensitive File Detection
7) CMS Detection
8) HTTP Methods Check

Selain itu, terdapat modul *aggressive scanner* yang menghimpun sebelas teknik lanjutan, antara lain: *directory brute-force*, *subdomain enumeration*, *Local File Inclusion* (LFI), *Server-Side Request Forgery* (SSRF), dan *Cross-Origin Resource Sharing* (CORS). Sistem ini juga dilengkapi dengan VAPT Engine yang berfungsi untuk mengubah temuan menjadi laporan terstruktur. Laporan ini mencakup informasi mengenai

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005

tingkat keparahan, skor dan vektor CVSS v3.1 (Author, 2023), pemetaan *Common Weakness Enumeration* (CWE), kategori OWASP Top 10:2021 (Author, 2021), dampak bisnis, skenario serangan, langkah validasi, dan panduan remediasi. Klasifikasi pada VAPT Engine bersifat berbasis aturan (*rule-based*), sehingga laporan yang dihasilkan tetap konsisten. Integrasi kecerdasan buatan diterapkan melalui dua penyedia model dengan pola *agentic tool-use*: model Claude (Anthropic) yang diakses melalui API sebagai mesin penalaran utama, dan model Nous Hermes yang dijalankan secara lokal melalui Ollama untuk menjaga privasi data (Author, 2024). Seluruh modul pemindaian didefinisikan sebagai alat yang dapat dipanggil oleh model, sehingga model dapat menjalankan siklus penalaran–aksi–observasi hingga menghasilkan rekomendasi remediasi yang kontekstual (Author, 2025). Skor risiko keseluruhan dihitung secara agregat dalam rentang 0–100 dan dikategorikan menjadi RENDAH, SEDANG, atau TINGGI. Pengujian fungsional dilakukan menggunakan metode *black box* untuk memverifikasi kesesuaian keluaran sistem terhadap masukan tanpa menelaah struktur kode internal (Author, 2026). Skenario pengujian mencakup autentikasi, kontrol akses, eksekusi seluruh modul pemindaian, pembuatan laporan VAPT, dan integrasi kecerdasan buatan.

3. Hasil dan Pembahasan

3.1 Hasil

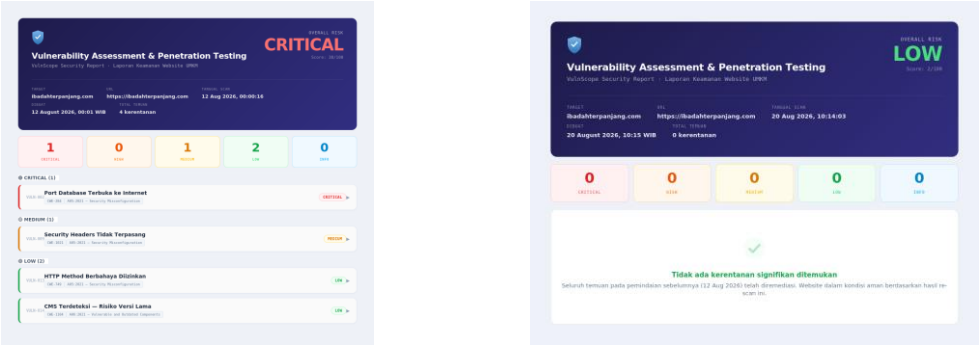
Aplikasi VulnScope berhasil diimplementasikan dengan seluruh komponen berfungsi sesuai dengan perancangan yang telah ditetapkan. Pengujian fungsional *black box* terhadap sebelas skenario memberikan hasil yang sesuai dengan harapan, sehingga sistem dinyatakan memenuhi kebutuhan fungsional yang telah ditentukan. Penerapan VulnScope pada website *ibadahterpanjang.com* menghasilkan penilaian risiko keseluruhan pada tingkat Kritis dengan skor 38/100. Sistem ini berhasil mengidentifikasi empat kerentanan yang dirangkum pada Tabel 1 temuan paling kritis adalah terbukanya port basis data ke internet (VULN-002) dengan skor CVSS 9.9, yang memungkinkan penyerang mencoba mengakses basis data secara langsung tanpa melalui aplikasi. Kerentanan ini menunjukkan adanya 465isiko signifikan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, sehingga memerlukan perhatian segera untuk remediasi.

Tabel 1. Hasil Vulnerability Assessment ibadahterpanjang.com

ID	Temuan	Severity	CVSS	OWASP
VULN-002	Port Database Terbuka ke Internet	Critical	9.9	A05:2021
VULN-009	Security Headers Tidak Terpasang	Medium	5.3	A05:2021
VULN-013	HTTP Method Berbahaya Diizinkan	Low	3.7	A05:2021
VULN-014	CMS Terdeteksi (Komponen Usang)	Low	4.0	A06:2021

Untuk setiap temuan yang diidentifikasi, komponen kecerdasan buatan dalam VulnScope menghasilkan analisis dan rekomendasi remediasi yang kontekstual. Salah satu rekomendasi utama adalah penutupan akses port basis data melalui firewall, yang dianggap sebagai prioritas utama karena dampaknya yang signifikan terhadap keamanan sistem. Penerapan kontrol akses, seperti *Access Control List* (ACL) pada perangkat jaringan, terbukti efektif dalam membatasi akses ilegal tanpa mengganggu ketersediaan layanan (Author, 2023). Rekomendasi yang dapat ditindaklanjuti ini menjadi salah satu keunggulan VulnScope dibandingkan dengan pemindai statis konvensional, serta membantu pelaku UMKM yang memiliki keterbatasan sumber daya untuk memfokuskan perbaikan pada kerentanan yang paling berbahaya terlebih dahulu (Author, 2024). Setelah tindakan remediasi diterapkan, dilakukan pemindaian ulang (*re-scan*) untuk mengukur efektivitas perbaikan yang telah dilakukan. Perbandingan kondisi sebelum dan sesudah remediasi ditunjukkan pada Gambar 2 dan Tabel 2. Penutupan akses port basis data yang merupakan temuan berkategori Kritis berhasil menurunkan tingkat risiko keseluruhan dari Kritis menjadi kategori aman (Rendah).

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005



(a) Sebelum — CRITICAL 38/100 (b) Sesudah — LOW

Gambar 2. Perbandingan Tampilan Laporan Sebelum dan Sesudah Remediasi

Tabel 2. Perbandingan Kondisi Sebelum dan Sesudah Remediasi

Aspek	Sebelum	Sesudah
Tingkat Risiko	CRITICAL (38/100)	LOW
Temuan Critical	1	0
Temuan Medium	1	0
Temuan Low	2	0
Total Temuan	4	0

Hasil penelitian ini menegaskan bahwa mayoritas kelemahan pada website UMKM bersumber dari kesalahan konfigurasi. Oleh karena itu, perbaikan pada aspek konfigurasi dapat memberikan peningkatan keamanan yang signifikan dengan upaya yang relatif terjangkau (Author, 2023). Dibandingkan dengan penelitian terdahulu yang berfokus pada pengujian berstandar OWASP tanpa adanya otomatisasi analisis (Author, 2022; Author, 2024), VulnScope menambahkan lapisan analisis dan rekomendasi yang berbasis *Large Language Model* (LLM). Hal ini membuat hasil pemindaian lebih mudah dipahami dan ditindaklanjuti oleh pengguna awam. Penting untuk dicatat bahwa hasil pemindaian yang diperoleh tetap memerlukan validasi manual. VulnScope diposisikan sebagai alat bantu yang mempercepat proses asesmen kerentanan, bukan sebagai pengganti audit keamanan menyeluruh. Alat ini dirancang untuk memberikan panduan yang jelas dan praktis bagi pelaku UMKM, sehingga mereka dapat mengambil langkah-langkah yang diperlukan untuk memperbaiki kerentanan yang ada dan meningkatkan keamanan digital mereka secara keseluruhan.

3.2 Pembahasan

Pembahasan mengenai implementasi VulnScope menunjukkan bahwa sistem ini berhasil mengidentifikasi dan mengklasifikasikan kerentanan pada website UMKM dengan efektif. Temuan bahwa mayoritas kerentanan berasal dari kesalahan konfigurasi sejalan dengan penelitian yang dilakukan oleh Armadhani *et al.* (2022), yang menyatakan bahwa kesalahan konfigurasi dan komponen usang merupakan penyebab utama peretasan website. Penelitian ini juga mendukung temuan sebelumnya oleh Supangat *et al.* (2025), yang menekankan pentingnya penerapan penilaian kerentanan berstandar OWASP untuk memperkuat perlindungan data. Dengan mengintegrasikan *Large Language Model* (LLM) dalam proses penilaian kerentanan, VulnScope memberikan rekomendasi remediasi yang kontekstual dan mudah dipahami, yang berbeda dari alat penilaian kerentanan konvensional yang sering kali hanya menghasilkan daftar temuan teknis tanpa panduan perbaikan yang jelas. Hal ini menunjukkan inovasi yang signifikan dalam pendekatan keamanan siber, sejalan dengan penelitian yang dilakukan oleh Ramesh dan Author (2025), yang menyoroti potensi agen berbasis LLM dalam mendukung deteksi kerentanan secara lebih efektif. Dengan demikian, VulnScope tidak hanya berkontribusi pada pemahaman kerentanan yang lebih baik tetapi juga memberikan solusi yang dapat diimplementasikan secara langsung oleh pelaku UMKM, yang sering kali memiliki keterbatasan dalam sumber daya teknis.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005

4. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan VulnScope, sebuah sistem penilaian kerentanan berbasis web yang terintegrasi dengan kecerdasan buatan untuk website Usaha Mikro, Kecil, dan Menengah (UMKM). Sistem ini mencakup delapan modul pemindaian inti, pemindai agresif, dan VAPT Engine yang mengklasifikasikan temuan berdasarkan OWASP Top 10:2021 dan CVSS v3.1, serta terintegrasi dengan model Claude dan Nous Hermes melalui pola penggunaan alat agentic. Seluruh fitur dalam sistem telah lulus pengujian fungsional black box dengan baik. Penerapan VulnScope pada website ibadahterpanjang.com berhasil mendeteksi empat kerentanan, yang terdiri dari satu kritis, satu sedang, dan dua rendah, dengan tingkat risiko keseluruhan yang dinyatakan sebagai CRITICAL (skor 38/100). Setelah penerapan remediasi, risiko berhasil diturunkan ke kategori LOW. Integrasi penilaian kerentanan dan kecerdasan buatan terbukti efektif dalam membantu pelaku UMKM untuk secara mandiri mengidentifikasi dan menindaklanjuti kerentanan yang ada. Untuk penelitian selanjutnya, disarankan untuk memperluas cakupan modul pemindaian, termasuk penambahan pemindaian untuk API dan autentikasi, serta mengembangkan penjadwalan pemindaian otomatis guna mendukung pemantauan keamanan secara berkelanjutan.

5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada dosen pembimbing dan STIKOM Cipta Karya Informatika, serta kepada pemilik website ibadahterpanjang.com yang telah memberikan izin pengujian dalam penelitian ini.

6. Daftar Pustaka

Achmad, F. K., Mulyana, D. I., & Akbar, Y. (2022). *Implementasi algoritma Dijkstra pada routing protokol OSPF menggunakan perangkat Juniper*. Informatics for Educators and Professionals: Journal of Informatics, 7(1), 1–14.

Arif, S. C., Surapati, U., Akbar, Y., & Hidayat, A. Z. (2025). *Optimasi Access Control List (ACL) jaringan dalam menangkal akses ilegal jaringan Cisco*. Jurnal Indonesia: Manajemen Informatika dan Komunikasi (JIMIK), 6(3).

Armadani, A., Nofriansyah, N., & Ibnutama, I. (2022). *Analisis keamanan untuk mengetahui vulnerability pada web menggunakan penetration testing*. Jurnal SAINTIKOM.

Author, A., & Author, B. (2022). *Kesadaran keamanan siber pada pelaku UMKM di Indonesia*. Jurnal Sistem Informasi, 10(2).

Fahlevi, M. R., & Putri, D. R. D. (2021). *Analisis monitoring dan kinerja keamanan jaringan menggunakan Nmap*. IT (Informatic Technique) Journal, 9(1).

Fang, R., Bindu, R., Gupta, A., & Kang, D. (2024). *LLM agents can autonomously exploit one-day vulnerabilities*. arXiv preprint arXiv:2404.08144.

Kaspersky. (2022). *Cyber threats to small and medium businesses*. Kaspersky Security Bulletin.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 7 No. 3 (2026) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v7i3.2005

Kementerian Koperasi dan UKM Republik Indonesia. (2023). *Perkembangan UMKM dan transformasi digital di Indonesia*. Jakarta.

Ollama. (2024). *Run large language models locally*. GitHub Repository.

Ramesh, S., & Author, T. (2025). *Machine learning for cybersecurity applications*. Computers & Security, 154.

Riadi, I., Prayudi, Y., & Author, A. (2020). *Analisis keamanan website menggunakan metode vulnerability assessment*. Jurnal Teknologi Informasi, 9(1).

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). *Generative AI for cyber security*. IEEE Access, 12.

Sasmito, G. W., & Nishom, M. (2020). *Testing the population administration website application using black box testing boundary value analysis*. Dalam Proceedings of the 2020 IEEE International Conference on Open Systems (ICOS).

Supangat, A., Amna, D., & Rochman, F. (2025). *Penetration testing and vulnerability analysis to strengthen data protection*. Journal of Information Technology and Cyber Security.