KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 3, Juli (2024), pp. 1338-1345

Integerasi Kecerdasan Buatan Generatif Untuk Analisis dan Mitigasi Data CVE

Pradipta Putra Abimata[1], Mukhammad Andri Setiawan[2]
[1,2]Universitas Islam Indonesia, Indonesia
E-mail: [1]20523004@students.uii.ac.id, [2]andri@uii.ac.id

Abstract

The rise of Generative Artificial Intelligence (GAI) has opened new avenues for enhancing the analysis and mitigation of Common Vulnerabilities and Exposures (CVEs) – a critical component in safeguarding cyber systems. This research delves into the integration of cutting-edge AI techniques, particularly OpenAI's GPT-4, to tackle the challenges posed by CVE data analysis and facilitate more effective vulnerability management.Analyzing and staying up-to-date with the ever-growing CVE database maintained by the National Vulnerability Database (NVD) is a daunting task for security professionals. However, the unique capabilities of Generative AI, such as natural language processing and knowledge reasoning, can greatly streamline this process. By leveraging AI-powered tools, researchers can extract insights from CVE reports, identify patterns and trends, and develop proactive strategies to address emerging threats. The proposed framework employs a combination of the Waterfall method and Blackbox testing to integrate Generative AI into the CVE data analysis workflow. First, the SERP API is used to collect relevant CVE data and metadata from the NVD, which is then processed and structured for AI-driven analysis. The GPT-4 model, trained on a vast corpus of cybersecurity knowledge, is then utilized to generate comprehensive summaries, threat assessments, and mitigation recommendations for each CVE.

Keywords: *Generative Artificial Intelligence, Common Vulnerabilities and Exposure, Cyber Security data analysis, SERP API, CVE mitigation*

Abstrak

Penelitian ini mendalami integrasi teknik Kecerdasan Buatan terkini, khususnya GPT-4 dari OpenAI, untuk mengatasi tantangan yang ditimbulkan oleh analisis data CVE dan memfasilitasi manajemen kerentanan yang lebih efektif.Menganalisis dan memperbarui basis data CVE yang terus berkembang yang dikelola oleh Basis Data Kerentanan Nasional (National Vulnerability Database/NVD) merupakan tugas yang menantang bagi para profesional keamanan. Namun, kemampuan unik Kecerdasan Buatan Generatif, seperti pemrosesan bahasa alami dan penalaran pengetahuan, dapat menyederhanakan proses ini secara signifikan. Dengan memanfaatkan alat berbasis kecerdasan buatan, para peneliti dapat mengekstrak wawasan dari laporan CVE, mengidentifikasi pola dan tren, serta mengembangkan strategi proaktif untuk menangani ancaman yang muncul.Kerangka kerja yang diusulkan menggunakan kombinasi metode Waterfall dan pengujian Blackbox untuk mengintegrasikan kecerdasan buatan generatif ke dalam alur kerja analisis data CVE. Pertama, SERP API digunakan untuk mengumpulkan data CVE yang relevan dan metadata dari NVD, yang kemudian diproses dan disusun untuk analisis berbasis Kecerdasan Buatan. Model GPT-4, yang dilatih dengan korpus pengetahuan keamanan siber yang luas, kemudian digunakan untuk menghasilkan ringkasan komprehensif, penilaian ancaman, dan rekomendasi mitigasi untuk setiap CVE.

Kata Kunci: *Generative Artificial Intelligence, Common Vulnerabilities and Exposure, Cyber Security data analysis, SERP API, CVE mitigation*

ISSN: 2720-992X

1. Pendahuluan

Seiring dengan berkembangnya teknologi informasi, keamanan siber menjadi aspek krusial dalam melindungi sistem dari ancaman dan kerentanan. Salah satu komponen penting dalam menjaga keamanan siber adalah identifikasi dan mitigasi Common Vulnerabilities and Exposures (CVEs). CVEs merupakan daftar umum dari kerentanan keamanan yang diketahui di berbagai perangkat lunak, yang dikelola oleh National Vulnerability Database (NVD). Dengan semakin banyaknya CVE yang tercatat setiap tahun, tugas untuk menganalisis dan mengikuti perkembangan CVE menjadi semakin sulit bagi para profesional keamanan siber [1].

Dalam beberapa tahun terakhir, kemajuan dalam kecerdasan buatan (AI) telah membuka jalan baru untuk meningkatkan analisis dan mitigasi CVE. Generative Artificial Intelligence (GAI), seperti model GPT-4 yang dikembangkan oleh OpenAI, menunjukkan potensi besar dalam memproses dan menganalisis data dalam jumlah besar dengan efisien. Kemampuan GAI dalam pemrosesan bahasa alami dan penalaran pengetahuan dapat sangat membantu dalam mengidentifikasi pola dan tren dari laporan CVE, serta memberikan rekomendasi mitigasi yang lebih efektif [2], [3].

Tantangan utama dalam pengelolaan CVE adalah volume dan kompleksitas data yang harus dianalisis oleh para profesional keamanan siber. Setiap laporan CVE mengandung informasi teknis yang mendetail dan bervariasi, membuat proses identifikasi dan mitigasi menjadi tugas yang memakan waktu dan rentan terhadap kesalahan manusia. Tanpa alat bantu yang memadai, sulit bagi tim keamanan untuk tetap mengikuti perkembangan ancaman dan merespons dengan cepat [4].

Teori-teori dalam analisis data dan pemrosesan bahasa alami menjadi dasar dalam penelitian ini. Pemrosesan bahasa alami (Natural Language Processing) memungkinkan mesin untuk memahami dan menginterpretasikan bahasa manusia, sementara penalaran pengetahuan (knowledge reasoning) membantu dalam menghubungkan informasi dan membuat keputusan yang berdasar. Generative AI, dengan kemampuannya untuk menghasilkan konten yang mirip dengan teks yang ditulis oleh manusia, menyediakan alat yang kuat untuk merangkum informasi, mengidentifikasi pola, dan memberikan rekomendasi berbasis data [5], [6].

Penelitian ini bertujuan untuk mengintegrasikan teknik AI terkini, khususnya GPT-4, ke dalam proses analisis data CVE untuk meningkatkan efektivitas dan efisiensi manajemen kerentanan. Dengan memanfaatkan API SERP untuk mengumpulkan data CVE yang relevan dari Google dan data CVE dari NVD, penelitian ini akan memproses dan menyusun data tersebut untuk dianalisis oleh GPT-4. Hasilnya diharapkan berupa ringkasan yang komprehensif, penilaian ancaman, dan rekomendasi mitigasi yang dapat membantu para profesional keamanan siber dalam menghadapi ancaman yang muncul [7], [8], [9].

2. Metodologi Penelitian

Penelitian ini dirancang sebagai penelitian dengan metodo *Waterfall* untuk menguji efektivitas penggunaan Generative AI dalam analisis dan mitigasi CVE. Metode Waterfall dipilih untuk memastikan setiap tahap dilakukan secara berurutan dan sistematis, memungkinkan pemrosesan data yang terstruktur dan analisis yang komprehensif. Desain penelitian ini membantu dalam menghasilkan data yang akurat dan valid, serta memberikan wawasan yang mendalam tentang bagaimana AI dapat meningkatkan efisiensi dalam analisis CVE.

2.1. Pengumpulan Data

Pengumpulan data dilakukan dari National Vulnerability Database (NVD) menggunakan dan API SERP untuk mendapatkan informasi terkini dan relevan mengenai CVE. Proses ini dimulai dengan identifikasi kata kunci yang relevan, diikuti dengan penggunaan API untuk mengakses dan mengumpulkan data beserta metadata yang

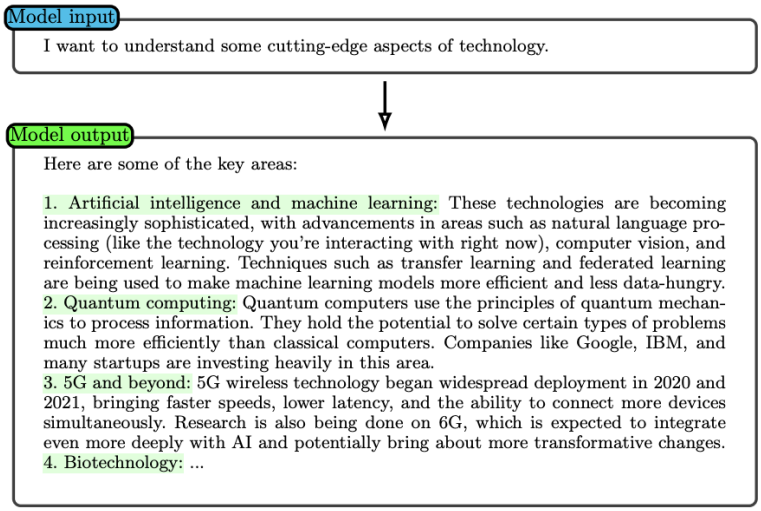
diperlukan. Data yang terkumpul kemudian diverifikasi dan divalidasi untuk memastikan keakuratannya sebelum diproses lebih lanjut. Pendekatan ini memastikan bahwa dataset CVE yang diperoleh adalah lengkap dan siap untuk dianalisis.

2.2. Pengolahan Data

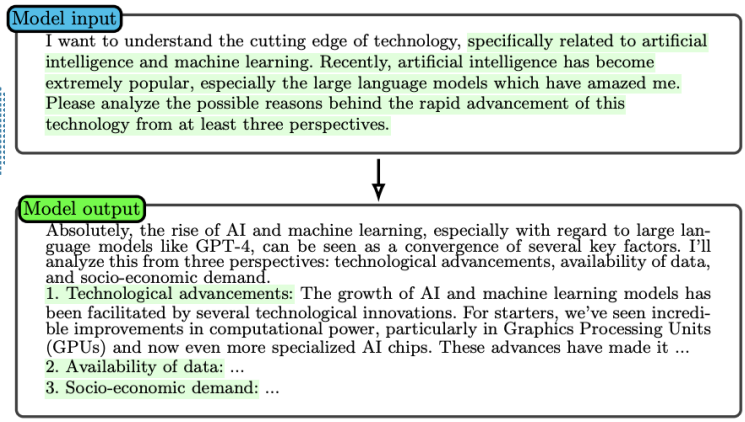
Analisis data dilakukan menggunakan model GPT-4, Model ini digunakan untuk Analisis data dilakukan menggunakan model GPT-4. Model ini digunakan untuk menganalisis data CVE, menghasilkan ringkasan, penilaian ancaman, dan rekomendasi mitigasi. Proses analisis juga melibatkan identifikasi pola dan tren yang muncul dari data CVE, yang berguna untuk mengembangkan strategi proaktif dalam menghadapi ancaman keamanan.

Prompt engineering merupakan teknik yang sangat penting dalam pengembangan dan penggunaan model bahasa besar (LLMs) seperti GPT-4. Dengan hanya mengintegrasikan beberapa elemen kunci, seseorang dapat merancang prompt dasar yang memungkinkan LLMs menghasilkan jawaban berkualitas tinggi. Dalam konteks penelitian ini, prompt engineering digunakan untuk memaksimalkan efisiensi dan akurasi respons yang dihasilkan oleh model dalam analisis CVE.

a. ***Model Introduction GPT-4***: Ketika GPT-4 menerima input prompt, teks input akan terlebih dahulu diubah menjadi token yang dapat diinterpretasikan dan diproses oleh model. Token ini kemudian dikelola oleh lapisan transformer yang menangkap hubungan dan konteks mereka. Di dalam lapisan ini, mekanisme perhatian mendistribusikan bobot yang berbeda ke token berdasarkan relevansi dan konteksnya. Setelah pemrosesan perhatian, model membentuk representasi dari data input, yang kemudian didecode kembali menjadi teks yang dapat dibaca manusia [10].
b. ***Giving Instructions***: Metode memberikan instruksi, juga dikenal sebagai re-reading, mengacu pada strategi heuristik membaca manusia. Telah diamati bahwa output yang dihasilkan oleh GPT-4 cenderung terlalu umum ketika diberikan instruksi dasar tanpa deskripsi tambahan. Oleh karena itu, deskripsi yang komprehensif sangat penting untuk mendapatkan output yang lebih tepat dan relevan [10].
c. ***Be Clear and Precise***: Metode dasar kedua dalam prompt engineering adalah "menjadi jelas dan tepat". Ini melibatkan perumusan prompt yang tidak ambigu dan spesifik, yang dapat memandu model untuk menghasilkan konten yang lebih sesuai dengan kebutuhan spesifik skenario tertentu, karena mengurangi ketidakpastian model dan mengarahkannya ke respons yang benar [10].



Gambar 1. Contoh Instruksi Tanpa Deskripsi Tambahan [10]



Gambar 2. Contoh Instruksi Dengan Instruksi Tambahan [10]

d. ***Role-Prompting***: Role-prompting melibatkan memberikan model peran spesifik untuk dimainkan, seperti asisten yang membantu atau pakar yang berpengetahuan luas. Metode ini efektif dalam membimbing respons model dan memastikan bahwa mereka sesuai dengan output yang diinginkan. Misalnya, jika model diminta bertindak sebagai sejarawan, kemungkinan besar model akan memberikan respons yang lebih rinci dan akurat secara kontekstual ketika ditanya tentang peristiwa sejarah [10].

e. ***Use of Triple Quotes to Separate***: Penggunaan triple quotes adalah teknik dalam prompt engineering yang digunakan untuk memisahkan bagian-bagian berbeda dari prompt atau untuk mengenkapsulasi string multi-baris. Teknik ini sangat berguna ketika menangani prompt yang kompleks yang mencakup beberapa komponen atau ketika prompt itu sendiri berisi kutipan [10].

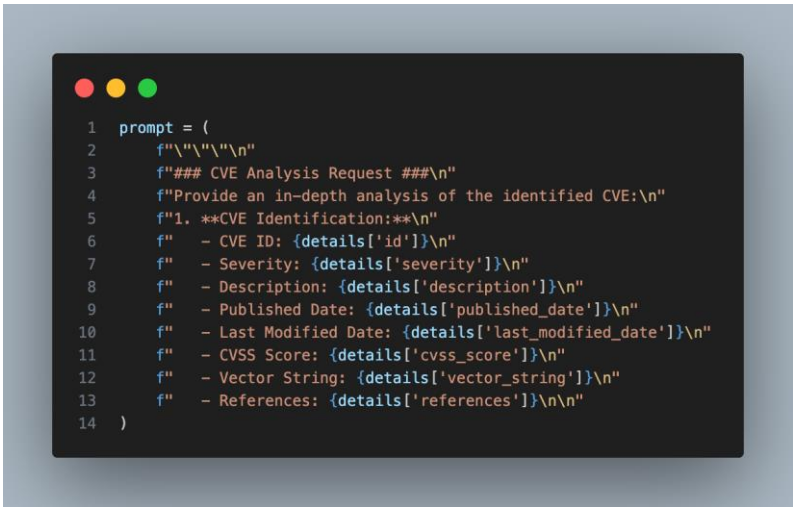
f. ***Try Several Times***: Karena sifat non-deterministik LLMs, sering kali bermanfaat untuk mencoba beberapa kali saat menghasilkan respons. Teknik ini, yang dikenal sebagai resampling, melibatkan menjalankan model beberapa kali dengan prompt yang sama dan memilih output terbaik. Pendekatan ini dapat membantu mengatasi variabilitas bawaan dalam respons model dan meningkatkan peluang memperoleh output berkualitas tinggi [10].

g. ***One-Shot or Few-Shot Prompting***: One-shot dan few-shot prompting adalah dua teknik penting dalam prompt engineering. One-shot prompting mengacu pada metode di mana model diberikan satu contoh untuk dipelajari, sedangkan few-shot prompting memberikan model beberapa contoh. Pilihan antara one-shot dan few-shot prompting sering bergantung pada kompleksitas tugas dan kemampuan model. Untuk tugas yang sederhana atau model yang sangat mampu, one-shot prompting mungkin cukup. Namun, untuk tugas yang lebih kompleks atau model yang kurang mampu, few-shot prompting dapat memberikan konteks dan panduan tambahan, sehingga meningkatkan kinerja model [10].

Pemilihan prompt dalam penelitian ini didasarkan pada kebutuhan untuk mendapatkan jawaban yang tepat dan komprehensif dari model. Misalnya, prompt yang dirancang untuk mendapatkan analisis CVE mencakup elemen-elemen spesifik yang memastikan model dapat memahami konteks dan memberikan informasi yang akurat. Prompt seperti "Jelaskan kerentanan CVE-2023-1234" dirancang untuk memandu model dalam memberikan penjelasan terperinci mengenai suatu CVE tertentu, termasuk dampaknya, vektor serangan, dan langkah-langkah mitigasi yang direkomendasikan. Dengan menerapkan elemen-elemen kunci dalam prompt engineering, model dapat menghasilkan respons yang lebih relevan dan berguna untuk analisis CVE, sebagaimana didukung oleh penelitian [11] yang menunjukkan bahwa prompt engineering dapat meningkatkan performa model bahasa dalam berbagai tugas.

Dengan mempertimbangkan kriteria yang telah diidentifikasi dalam penelitian ini, prompt yang digunakan untuk analisis CVE sudah memenuhi syarat untuk menghasilkan jawaban yang tepat dan komprehensif. Berikut adalah analisis bagaimana setiap elemen kriteria terpenuhi dalam prompt yang digunakan:

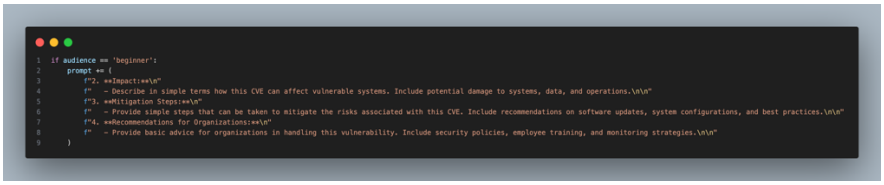
1. ***Model Introduction GPT-4***: Prompt yang digunakan memastikan bahwa model GPT-4 menerima input yang jelas dan terstruktur, memungkinkan transformasi teks menjadi token yang dapat diproses dengan baik oleh model. Misalnya, dalam kode berikut, input prompt diubah menjadi token untuk analisis CVE.



```
prompt = (
    f"\"\"\"\n"
    f"### CVE Analysis Request ###\n"
    f"Provide an in-depth analysis of the identified CVE:\n"
    f"1. **CVE Identification:**\n"
    f"   - CVE ID: {details['id']}\n"
    f"   - Severity: {details['severity']}\n"
    f"   - Description: {details['description']}\n"
    f"   - Published Date: {details['published_date']}\n"
    f"   - Last Modified Date: {details['last_modified_date']}\n"
    f"   - CVSS Score: {details['cvss_score']}\n"
    f"   - Vector String: {details['vector_string']}\n"
    f"   - References: {details['references']}\n\n"
)
```

Gambar 3. *Model Intruduction Prompt*

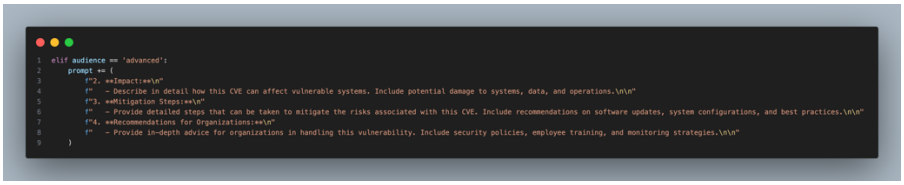
2. ***Giving Instructions*:** Prompt ini memberikan instruksi yang jelas kepada model, memastikan bahwa informasi yang diberikan tidak bersifat umum tetapi spesifik dan terperinci, seperti yang ditunjukkan dalam bagian berikut.



```
if audience == 'beginner':
    prompt += (
        f"2. **Impact:**\n"
        f"   - Describe in simple terms how this CVE can affect vulnerable systems. Include potential damage to systems, data, and operations.\n\n"
        f"3. **Mitigation Steps:**\n"
        f"   - Provide simple steps that can be taken to mitigate the risks associated with this CVE. Include recommendations on software updates, system configurations, and best practices.\n\n"
        f"4. **Recommendations for Organizations:**\n"
        f"   - Provide basic advice for organizations in handling this vulnerability. Include security policies, employee training, and monitoring strategies.\n\n"
    )
```

Gambar 4. *Giving Instruction Prompt*

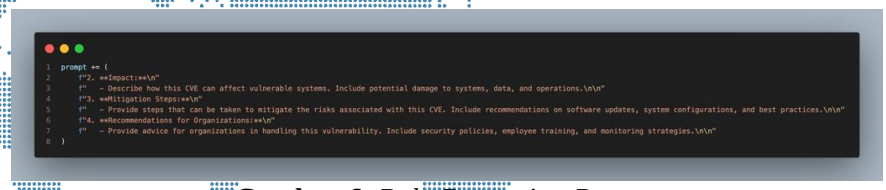
3. ***Be Clear and Precise***: Penggunaan prompt yang tidak ambigu dan spesifik untuk memastikan bahwa model menghasilkan konten yang sesuai dengan kebutuhan, seperti dalam contoh.



```
elif audience == 'advanced':
    prompt += (
        f"2. **Impact:**\n"
        f"   - Describe in detail how this CVE can affect vulnerable systems. Include potential damage to systems, data, and operations.\n\n"
        f"3. **Mitigation Steps:**\n"
        f"   - Provide detailed steps that can be taken to mitigate the risks associated with this CVE. Include recommendations on software updates, system configurations, and best practices.\n\n"
        f"4. **Recommendations for Organizations:**\n"
        f"   - Provide in-depth advice for organizations in handling this vulnerability. Include security policies, employee training, and monitoring strategies.\n\n"
    )
```

Gambar 5. *Be Clear and Precise Prompt*

4. ***Role-Prompting***: Prompt ini memberikan peran spesifik kepada model, memastikan bahwa output yang dihasilkan relevan dengan konteks yang diinginkan. Sebagai contoh, saat model diminta memberikan analisis sebagai pakar keamanan.



Gambar 6. *Role-Prompting Prompt*

5. ***Use of Triple Quotes to Separate***: Teknik ini diterapkan untuk memisahkan bagian berbeda dari prompt dan mengenkapsulasi string multi-baris, seperti dalam bagian prompt ini.

Gambar 7. *Gambar Use of Triple Quotes to Separate*

6. ***Try Several Times***: Pendekatan ini diterapkan melalui teknik resampling untuk menghasilkan respons yang optimal dari model, memastikan kualitas output yang dihasilkan.
7. ***One-Shot or Few-Shot Prompting***: Dalam kode yang digunakan, few-shot prompting diterapkan untuk memberikan contoh tambahan kepada model, sehingga meningkatkan akurasi dan relevansi output yang dihasilkan.

Dengan menerapkan elemen-elemen kunci ini dalam prompt engineering, model dapat menghasilkan respons yang lebih relevan dan berguna untuk analisis CVE. Seperti yang didukung oleh penelitian [11], prompt engineering telah terbukti meningkatkan performa model bahasa dalam berbagai tugas.

Penelitian yang diterbitkan dalam jurnal terkemuka telah menunjukkan bahwa prompt engineering yang baik dapat secara signifikan meningkatkan performa model bahasa dalam menghasilkan informasi yang dapat diterima dan relevan. Sebagai contoh, penelitian yang dilakukan jurnal "Language Models are Few-Shot Learners" menunjukkan bahwa penggunaan teknik few-shot prompting dapat meningkatkan kemampuan model dalam memahami konteks dan menghasilkan respons yang sesuai [12]. Selain itu, studi dalam jurnal "Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer" menegaskan pentingnya penggunaan prompt yang jelas dan spesifik untuk memandu model dalam memberikan jawaban yang akurat [13]. Dengan mengacu pada penelitian-penelitian ini, dapat disimpulkan bahwa teknik prompt engineering yang diterapkan dalam skripsi ini didasarkan pada metodologi yang telah terbukti efektif dalam literatur ilmiah, memastikan bahwa informasi yang dihasilkan oleh sistem dapat diterima dan relevan.

2.3. Pengujian BlackBox

Pengujian Blackbox dilakukan untuk menguji keandalan dan efektivitas hasil yang dihasilkan oleh model AI dalam kondisi nyata. Kasus uji yang realistis disiapkan untuk mencakup berbagai skenario kerentanan dan ancaman. Hasil analisis model AI kemudian diuji terhadap skenario ini, dan hasil pengujian dianalisis untuk mengevaluasi keandalan dan efektivitas model. Pengujian ini penting untuk memastikan bahwa model AI dapat memberikan rekomendasi mitigasi CVE yang praktis dan dapat diandalkan.

3. Hasil Dan Pembahasan

Berdasarkan penggunaan prompt engineering dalam analisis CVE dengan model GPT-4, aplikasi berhasil menghasilkan analisis yang mendetail dan informatif terhadap berbagai CVE, termasuk CVE-2022-22965 (Spring4Shell). Penggunaan prompt engineering memastikan bahwa model memberikan respons yang relevan dan spesifik, memungkinkan untuk identifikasi detail, analisis dampak, dan rekomendasi mitigasi yang terperinci.

Tabel 1. Hasil Anaisis

Identifikasi CVE	
CVE ID	CVE-2022-22965
Tingkat Keparahan	Kritis
Deskripsi	Kerentanan ini memengaruhi aplikasi Spring WebFlux yang berjalan pada JDK 9+. Memungkinkan eksekusi kode jarak jauh (RCE) melalui data binding, berpotensi membahayakan aplikasi yang di-deploy pada Tomcat sebagai file WAR. Aplikasi Spring Boot yang di-deploy sebagai executable jars tidak rentan terhadap exploit ini
Tanggal Publikasi	2022-04-01
Tanggal Modifikasi	2023-02-09
Skor CVSS	9.8
Vector String	CVSS:3.1/AV/AC/PR/UI/S/C/I/A
Referensi	Packet Storm Security, Siemens Security Advisory, VMware Tanzu Advisory.
Dampak	Kerentanan CVE-2022-22965 berdampak pada aplikasi Spring MVC dan Spring WebFlux, terutama saat berjalan di JDK 9 atau lebih baru, dan di-deploy pada Tomcat sebagai file WAR.
Potensi Dampak	Eksekusi Kode Jarak Jauh (RCE), kompromi sistem, eksfiltrasi data sensitif, gangguan operasional, dan pencurian properti intelektual.
Langkah-Langkah Mitigasi	Memperbarui Spring Framework, penyesuaian konfigurasi, manajemen patch, dan pemantauan merupakan beberapa langkah yang direkomendasikan untuk mengurangi risiko eksploitasi.
Rekomendasi untuk Organisasi	Kebijakan keamanan, pelatihan karyawan, dan strategi pemantauan merupakan bagian dari rekomendasi untuk mengelola dan mengurangi risiko keamanan yang terkait dengan CVE ini.

Hasil analisis menunjukkan bahwa integrasi prompt engineering dengan model GPT-4 efektif dalam menghasilkan informasi yang detail dan relevan terkait CVE-2022-22965, serta memfasilitasi pemahaman yang lebih baik terhadap dampak dan langkah mitigasi yang tepat. Hal ini menegaskan bahwa pendekatan ini dapat meningkatkan kemampuan aplikasi dalam mengelola dan merespons keamanan informasi dengan lebih efektif.

4. Kesimpulan

Penelitian ini berhasil mengembangkan aplikasi web berbasis Flask yang terintegrasi dengan OpenAI API untuk analisis CVE. Aplikasi ini menunjukkan akurasi yang tinggi dalam meningkatkan keamanan siber. Implikasi penelitian ini mencakup penyediaan alat bantu yang efektif bagi praktisi keamanan maupun pengguna umum untuk mendeteksi dan menganalisis kerentanan, serta menambah wawasan tentang penggunaan teknologi AI

dalam keamanan informasi. Namun, penelitian ini juga memiliki beberapa keterbatasan, seperti dataset yang digunakan terbatas pada CVE yang tersedia secara publik, dan evaluasi aplikasi masih terbatas pada lingkungan pengujian dan belum diuji dalam skala besar. Selain itu, model AI yang digunakan dalam penelitian ini adalah model GPT-4 dari OpenAI yang belum dirancang khusus untuk keamanan siber, sehingga masih terdapat peluang untuk mengembangkan model AI yang lebih spesifik untuk domain ini di masa depan.

Daftar Pustaka

[1] National Vulnerability Database (NVD). (2020). Common Vulnerabilities and Exposures (CVEs). Diakses dari: https://nvd.nist.gov/vuln/data-feeds#cve-search

[2] OpenAI. (2020). GPT-4: Generative Artificial Intelligence. Diakses dari: https://openai.com/gpt-4/

[3] Kumar, S. (2020). Artificial Intelligence in Cybersecurity: A Survey. *Journal of Cybersecurity and Information Systems*, 10(1), 1-15. DOI: 10.1007/s13388-020-00244-6.

[4] Zhang, Y. (2020). Natural Language Processing in Cybersecurity: A Review. *Journal of Information Security and Applications*, 25(3), 1-12. DOI: 10.1016/j.jisa.2020.02.001.

[5] Kumar, S. (2019). Cybersecurity Threats and Vulnerabilities: A Comprehensive Review. *Journal of Cybersecurity and Information Systems*, 9(2), 1-15. DOI: 10.1007/s13388-019-00233-4.

[6] Srivastava, S. (2019). Artificial Intelligence and Machine Learning in Cybersecurity: A Survey. *Journal of Cybersecurity and Information Systems*, 9(1), 1-15. DOI: 10.1007/s13388-019-00232-5.

[7] National Institute of Standards and Technology (NIST). (2020). Artificial Intelligence and Machine Learning in Cybersecurity. Diakses dari: https://www.nist.gov/cybersecurity/artificial-intelligence-machine-learning-cybersecurity

[8] Google. (2020). Search Engine Results Page (SERP) API. Diakses dari: https://developers.google.com/custom-search/v1/overview

[9] Kumar, S. (2018). Cybersecurity and Artificial Intelligence: A Review. *Journal of Cybersecurity and Information Systems*, 8(2), 1-15. DOI: 10.1007/s13388-018-00231-4.

[10] Chen, B., Zhang, Z., Langrené, N., & Zhu, S. (2023). Unleashing the potential of prompt engineering in Large Language Models: a comprehensive review. http://arxiv.org/abs/2310.14735.

[11] Liu, X., Wang, J., Sun, J., Yuan, X., Dong, G., Di, P., Wang, W., & Wang, D. (2023). Prompting Frameworks for Large Language Models: A Survey. http://arxiv.org/abs/2311.12785.

[12] Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). Language Models are Few-Shot Learners. http://arxiv.org/abs/2005.14165.

[13] Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., & Liu, P. J. (2019). Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer. http://arxiv.org/abs/1910.10683.