

INTISARI

PERANCANGAN DAN PENGEMBANGAN SISTEM OTOMATISASI LAPORAN *PENETRATION TESTING* BERBASIS CVE MENGGUNAKAN LLM *PROMPT ENGINEERING* PADA OPENAI DAN GEMINIAI

GABE ASRIEL WOLLY LIMBONG

21/480067/SV/19566

Penyusunan laporan *penetration testing* merupakan tahapan krusial dalam proses pengujian keamanan sistem, namun pada praktiknya masih banyak dilakukan secara manual sehingga membutuhkan waktu yang lama dan berpotensi menghasilkan laporan yang tidak konsisten. Penelitian ini bertujuan untuk merancang dan mengembangkan sistem otomatisasi pembuatan laporan *penetration testing* berbasis *Common Vulnerabilities and Exposures* (CVE) dengan memanfaatkan model kecerdasan buatan generatif OpenAI GPT-4.1-mini dan GeminiAI 2.5-flash. *Dataset* CVE yang digunakan dalam penelitian yaitu CVE-2012-2122 dan CVE-2018-10933 ini telah ditentukan sejak awal dan diperoleh dari mitra penelitian dalam bentuk hasil pemindaian kerentanan, sehingga merepresentasikan skenario pengujian nyata. Sistem yang dikembangkan mampu mengolah *dataset* tersebut, melakukan analisis otomatis, serta menghasilkan laporan *penetration testing* secara terstruktur dalam format Word dan PDF. Metodologi penelitian meliputi perancangan sistem, implementasi, serta evaluasi hasil. Evaluasi dilakukan dengan membandingkan keluaran kedua model AI berdasarkan struktur laporan, konsistensi format, jumlah *token*, dan waktu eksekusi. Hasil pengujian menunjukkan bahwa OpenAI GPT-4.1-mini menghasilkan laporan yang lebih ringkas dan memiliki waktu eksekusi yang lebih efisien, sedangkan GeminiAI 2.5-flash menghasilkan analisis yang lebih deskriptif dengan penggunaan *token* dan waktu pemrosesan yang lebih besar. Perbedaan tersebut dipengaruhi oleh arsitektur model dan karakteristik generasi teks masing-masing AI. Dengan demikian, sistem yang dikembangkan terbukti mampu mengotomatisasi proses penyusunan laporan *penetration testing* secara efektif.

Kata kunci : Pengujian Penetrasi, CVE, Otomatisasi Laporan, Rekayasa *Prompt*,
LLM

ABSTRACT

DESIGN AND DEVELOPMENT OF A CVE-BASED PENETRATION TESTING REPORT AUTOMATION SYSTEM USING LLM PROMPT ENGINEERING ON OPENAI AND GEMINIAI

GABE ASRIEL WOLLY LIMBONG

21/480067/SV/19566

The preparation of penetration testing reports is a critical phase in security assessments; however, manual reporting processes are time-consuming and may lead to inconsistent results. This study aims to design and develop an automated penetration testing reporting system based on Common Vulnerabilities and Exposures (CVE) by utilizing generative artificial intelligence models, namely OpenAI GPT-4.1-mini and GeminiAI 2.5-flash. The CVE dataset used in this research was predefined and obtained from a research partner in the form of vulnerability scanning results, specifically involving CVE-2012-2122 and CVE-2018-10933, ensuring that the data represent real-world testing scenarios. The proposed system processes the dataset, performs automated analysis, and generates structured penetration testing reports in Word and PDF formats. The research methodology includes system design, implementation, and result evaluation. The evaluation compares the outputs of both AI models in terms of report structure, format consistency, token usage, and execution time. The experimental results indicate that OpenAI GPT-4.1-mini produces more concise reports with faster execution time, while GeminiAI 2.5-flash provides more descriptive analyses with higher token consumption and longer processing time. These differences are influenced by the underlying model architectures and text generation characteristics. Overall, the developed system effectively automates the penetration testing reporting process and provides insights into selecting appropriate AI models based on system requirements.

Keyword : Penetration Testing, CVE, Report Automation, Prompt Engineering, LLM