Thilak - JO team

AUTOMATING VULNERABILITY TRIAGE FOR RAPID RESPONSE

Automating Vulnerability Triage for Rapid Response. Presented by Thilak (Jo-team) at the iHackMyPlace Hackathon Series.

thilakjo.com

Overcoming the Bottlenecks in Vulnerability Management

Addressing the Challenges of Unstructured Vulnerability Reports and Delayed Responses

Overwhelmed Security Teams

Constant influx of reports and advisories.

Time-Consuming Manual Analysis

Labor-intensive and prone to errors.

Delayed Critical Patching

Slow response increases potential risks.

Lack of Structured Insights

Immediate insights are not available.

Uncertainty in Prioritization

Difficulty in determining starting points.

Automating Vulnerability Triage with AI

Leveraging AI to enhance vulnerability management and decision-making efficiency in security operations.

AI Automation

Automates the initial analysis of raw vulnerability reports, streamlining the triage process significantly.

Insight Transformation

Transforms **unstructured text** into clear, actionable insights, enabling teams to quickly grasp the situation.

Informed Decisions

Enables **faster**, more informed decisions for security operations, helping organizations respond effectively to threats.

Intelligent Extraction

Leverages Google **Gemini LLM** for intelligent extraction and reasoning, enhancing the analytical capabilities of teams.

Operational Efficiency

Improves overall **operational efficiency** by reducing manual effort and accelerating the vulnerability management process.

Streamlined Workflow for Vulnerability Analysis

An intuitive process for rapid analysis of security reports using AI technology

User Interaction

The user pastes raw report information into the web app interface for processing.

Prompt Preparation

The `llm_handler.py` script structures the input into a coherent prompt for further analysis.

AI Processing

Google Gemini API analyzes the structured prompt and generates a JSON formatted analysis.

Results Display

The web app presents a clear and actionable summary of the analysis results to the user.

Key Features of Intelligent Patch Advisor

Explore powerful capabilities for vulnerability identification and actionable recommendations through AI-driven insights.

01

LLM-Powered Extraction

Utilizes **AI** technology to **accurately extract** critical information such as **Vulnerability ID**, **Products**, **Severity**, **Type**, and **Description** from security data, ensuring comprehensive analysis.

02

Contextual Impact Assessment

AI evaluates potential threats, offering a detailed description of **worst-case scenarios** to help organizations understand the implications of each vulnerability effectively.

03

Actionable Recommendations

Delivers clear **Primary/Secondary Mitigations**, prioritizing based on **Urgency Level** and providing detailed **Verification Steps** to streamline the remediation process for security teams.

04

Clean, Structured Output

Produces a **consistent JSON format** for the output, facilitating easy consumption and integration with existing security tools and workflows, enhancing efficiency in vulnerability management.

Working of Intelligent Patch Advisor

Explore the capabilities of the Intelligent Patch Advisor in real-time vulnerability analysis

01

Copy a sample vulnerability text.

Users will copy a sample vulnerability from a predefined file for analysis purposes.

02

Paste into the text area for analysis.

Users will paste the copied text into the designated area within the app to initiate the analysis.

03

Click on 'Analyze Vulnerability' button.

This action triggers the analysis process and generates structured output based on the input data.

04

Explore the structured output sections.

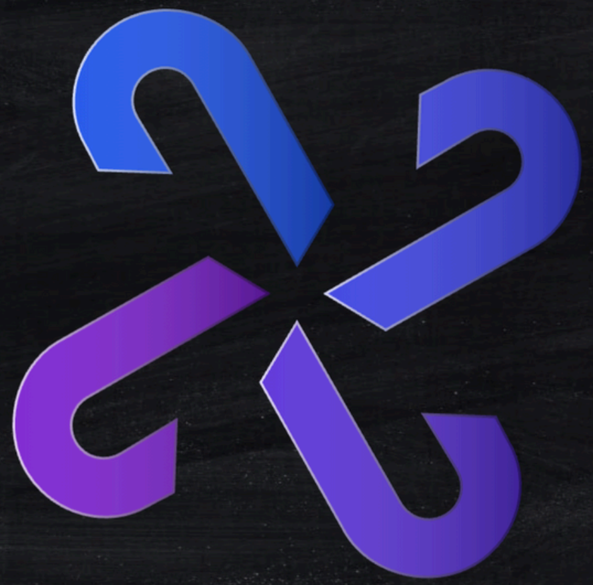
Walkthrough the output highlighting Key Details, Impact, and Recommendations for better understanding.

Exploring AI Robustness and Prompt Engineering

An overview of technical highlights in AI capabilities and robust prompt engineering practices for cybersecurity.

AI Capabilities Overview

Explains generative AI functions.



Prompt Engineering Strategy

Utilizes expert personas effectively.

Secure API Key Management

Utilizes .env for security.

Error Handling Mechanisms

Ensures model reliability and availability.

Overcoming Challenges in LLM Implementation

Key insights on addressing common issues in AI-driven processes

Addressing LLM Hallucination

Utilized structured prompts.

API Key Management Strategies

Adopted .env with python-dotenv.

Importance of Prompt Engineering

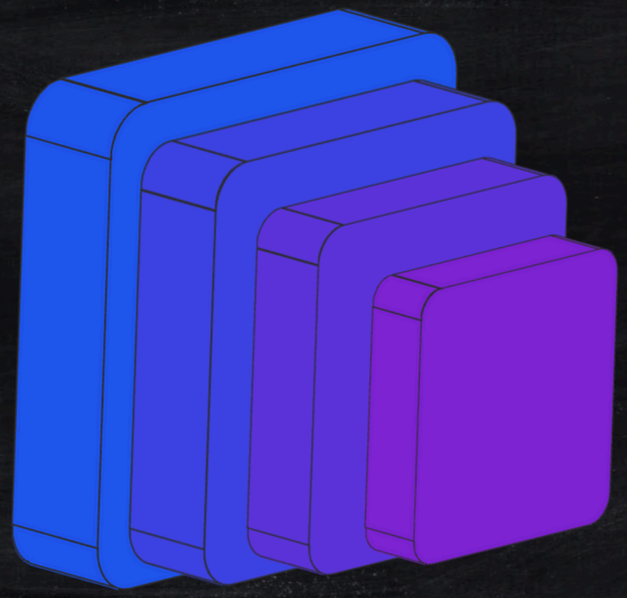
Ensures structured outputs.

Thank You for Your Attention

We appreciate your participation. Please feel free to ask any questions or reach out to us for more information.

Thank You

We sincerely appreciate your attention and engagement throughout this presentation. Your interest is what drives innovation and improvement in our field.



Questions?

We welcome any questions you may have. Please feel free to ask for clarification or further information on any topic we discussed today.

Try it yourself

We encourage you to explore the concepts discussed today by trying them out in your own projects. Hands-on experience is invaluable

Contact Info

For further inquiries or collaborations, please connect with us via GitHub, LinkedIn, or Email. We're excited to hear from you

Embrace the future of cybersecurity by trying out the Intelligent Patch Advisor now

Take the first step towards a more secure digital environment. With the Intelligent Patch Advisor, you can effectively manage vulnerabilities and enhance your cybersecurity posture. Experience the future of patch management and ensure your systems are always protected.