Applied Generative AI :
LLM Application Development

Dates: 12 & 19 September 2025

Lab 3: RAG with CVE Data (Streamlit GUI)

- **Learning Objectives**
  - LLMs are **pre-trained** → they can **reason**, but don't know **latest CVEs**.
  - We'll **ingest CVE data** (downloaded earlier from CVE.org), plus **system evidence Command Line (CLI)**
    - **Web Interface (Streamlit)**
  - We'll **retrieve relevant CVEs** and **ground** the model's answer with citations.

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 1: Activate Virtual Environment

Windows (PowerShell):

```
.\llm\Scripts\activate
```

macOS/Linux:

```
source llm/bin/activate
```

Step 2: Install Required Packages

- Download lab3_requirements.txt from bhattaraprot.com/lab3_requirements.txt
- Make sure the file is saved in your working directory.
- Install the required packages by running:

```
pip install -r lab3_requirements.txt
```

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 3: Source Installation

- Download lab3.zip from bhattaraprot.com/lab3.zip
- Extract the contents and place them into

```
llm/src/lab3
```

- Navigate into the lab3 folder
- Verify the structure by listing files

```
ls –R or dir
```

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 4: Run Streamlit

```
python -m streamlit run lab3/ui/streamlit_app_rag.py
```

Step 5: Upload files

- `Upload CVE-Example.json`
- `Upload System evidence files (logexam.txt, logexam2.txt)`

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 6: Prompt

- *“Summarize which CVEs mentioned in my logs are marked CRITICAL.”*
- *“Explain what CVE-2025-0171 and CVE-2025-0206 mean for my systems.”*
- *“Which of my uploaded system logs match vulnerabilities in the CVE dataset?”*
- *“Rank the top 3 vulnerabilities affecting my environment by CVSS score.”*
- *“Are there any SQL injection issues in my logs that map to known CVEs?”*
- *“Which issues in my logs are just warnings, and which are high severity CVEs?”*

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 6: Prompt

- *“For each CRITICAL CVE found in my logs, suggest an action plan or patch.”*
- *“Do my GitLab log errors correspond to CVE-2025-0206? What should I do?”*
- *“What remediation steps are recommended for CVE-2025-0197 (Struts RCE)?”*

Lab 3: RAG with CVE Data (Streamlit GUI)

Step 7: Reflection

- *“Show me examples where my log evidence mentions attacks but no matching CVE exists.”*
- *“Explain why top-k = 3 gives different answers than top-k = 8 for my query ‘SQL injection issues’.”*
- *“Compare results: What do I get if I ask with RAG vs without RAG for ‘Privilege escalation in kernel’?”*