Assessment Output

Assessment Output

Assessment Brief

Assignment 2: Secure RAG Implementation (30%)

Unit: LLM Security and Governance (Postgraduate Unit)

Learning Outcomes: 3, 4, and 5

Objective: Design and implement a secure RAG pipeline with structured output enforcement, g overnance strategies for AI deployment, and conduct prompt injection testing.

Instructions:

1. Develop a comprehensive report detailing the design of your secure RAG pipeline.
2. Implement a working prototype of your RAG pipeline using industry-standard tools and technol ogies.
3. Conduct a thorough analysis of your pipeline's security features and governance strategies.
4. Perform prompt injection testing on your pipeline, reporting:
   * Attack success rate
   * False block rate
   * JSON validity rate
   * Citation coverage
5. Include an ethics/compliance section addressing cyber law and regulatory considerations.

Submission Requirements:

* Report (max 10 pages): detailing the design of your secure RAG pipeline, governance strategie s, and prompt injection testing results.
* Working prototype code (zipped or linked repository).
* Ethics/Compliance document (max 2 pages): addressing cyber law and regulatory considerations.

Grading Criteria: Refer to the Marking Rubric below.

Marking Rubric

Secure RAG Pipeline Design (40%)

1. **Security Features (15%):**
   * Effectiveness of security measures
   * Adversarial risk analysis
2. **Governance Strategies (10%):**
   * Clarity and coherence of governance plan
   * Alignment with industry standards
3. **Prompt Injection Testing (10%):**
   * Thoroughness of testing
   * Accuracy of results

Implementation and Technical Merit (30%)

1. **Technical Soundness (15%):**
   * Correctness and efficiency of implementation
   * Use of industry-standard tools and technologies
2. **Code Quality (10%):**
   * Readability, maintainability, and scalability
   * Adherence to coding standards

Ethics/Compliance (20%)

1. **Cyber Law and Regulatory Considerations (15%):**
   * Depth and accuracy of analysis
   * Clarity and coherence of recommendations
2. **Compliance with Industry Standards (5%):**
   * Alignment with relevant regulations and guidelines

Student Submission Checklist

Please ensure you have included the following in your submission:

1. Report detailing secure RAG pipeline design, governance strategies, and prompt injection tes ting results.
2. Working prototype code (zipped or linked repository).
3. Ethics/Compliance document addressing cyber law and regulatory considerations.

Note: Late submissions will incur a penalty of 10% per day.