Advanced Software Quality and Security

**1. UML Diagram**

**A diagram of a computer

AI-generated content may be incorrect.**

Figure 1: UML diagram of LLM dispatch tool

**2. Test Plan**

**Test Environment**

|  |  |
| --- | --- |
| Component | Technology |
| Backend API | Python 3.10 + FastAPI |
| LLM Runtime | LM Studio (LM Studio (deepseek-r1-distill-qwen-7b) |
| Database | MySQL (local) - table messages |
| API test tool | Swagger UI, curl, Postman |

Figure 2: Test Environment table

**Test cases table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Case ID | Role | Test Question | Expected Response | Actual Result |
| 1 | User | What is FastAPI? | Should return definition and key features of FastAPI | FastAPI is a Python framework for building web applications. It's designed to be lightweight and fast, offering features like dependency injection, middleware, and route mapping out of the box. FastAPI supports both RESTful and WebSocket APIs, and it can integrate with technologies like Express.js, Starlette, and others.\n\nKey features of FastAPI include:\n\n1. \*\*Lightning Fast\*\*: Built on Starlette, which provides fast performance.\n2. \*\*Simplicity\*\*: Offers a clean API development experience with minimal boilerplate code.\n3. \*\*Flexibility\*\*: Supports modern web standards and paradigms like server-side rendering (SSR), full-stack apps, and client-side routing.\n4. \*\*Security\*\*: Built-in features like middleware, rate limiting, and secure connections ensure robust security.\n5. \*\*Scalability\*\*: Easily handles high traffic with built-in support for parallel processing and asynchronous tasks.\n\nFastAPI is widely used in enterprise applications and web development projects due to its ease |
| 2 | User | Who developed Python? | Should return “Guido van Rossum” or relevant history | <think>\n\n</think>\n\nPython was created by Guido van Rossum, a Dutch computer scientist. He first released the language in 1991 as part of his work at the Centrum Wiskunde en Informatica (CWI) in Amsterdam. The name \"Python\" was suggested by his boss at the Microsoft Research Amsterdam lab, Jan van Eijk. Python has since become one of the most popular programming languages due to its simplicity and versatility. |
| 3 | User | 2 + 2 = ? | "4" | <think>\nTo solve the problem \\(2 + 2\\), I start by identifying the two numbers involved, which are both 2.\n\nNext, I add these numbers together. Adding 2 and 2 gives me a sum of 4.\n</think>\n\n\*\*Solution:\*\*\n\nWe need to find the value of \\(2 + 2\\).\n\n1. \*\*Add the numbers together:\*\*\n \n \\[\n 2 + 2 = 4\n \\]\n\nSo, the final answer is:\n\n\\[\n\\boxed{4}\n\\] |
| 4 | User | What is AI? | Should define Artificial Intelligence and its applications | <think>\n\n</think>\n\nAI, or Artificial Intelligence, refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. It encompasses various technologies such as machine learning, natural language processing, robotics, and computer vision, enabling systems to perform tasks that typically require human intelligence. |
| 5 | User | Explain REST API | Should explain REST principles (GET, POST, etc.) | <think>\n\n</think>\n\nREST (Representational State Transfer) API is a design principle for designing networked applications. It allows software components to communicate with each other over the internet using HTTP methods like GET, POST, PUT, DELETE, etc., and typically returns data in JSON format.\n\n### Key Features of REST APIs:\n1. \*\*HTTP Methods\*\*: \n - `GET`: Retrieve data.\n - `POST`: Create new resources.\n - `PUT`: Update existing resources.\n - `DELETE`: Delete resources.\n - `HEAD`: Perform a GET request but return the response headers only.\n\n2. \*\*Statelessness\*\*: REST APIs are generally stateless, meaning they don't maintain any record of previous requests or responses between the client and server.\n\n3. \*\*Versioning\*\*: API endpoints can include version identifiers to ensure clients use compatible versions.\n\n4. \*\*JSON Data\*\*: Often returns data in JSON format for easy parsing by the client.\n\n5. \*\*URI Path\*\*: Uses URLs with resource |
| 6 | User | Hello | Greeting response like “Hello! How can I help you?” | <think>\n\n</think>\n\nHello! How can I assist you today? 😊 |
| 7 | User | Tell me a joke | Returns a short joke | <think>\n\n</think>\n\nSure! Here's a light-hearted joke for you:\n\nWhy don’t skeletons fight each other? \nBecause they don’t have the \*guts\*! \n\n😄 |
| 8 | User | What is the capital of Finland? | "Helsinki" | <think>\n\n</think>\n\nThe capital of Finland is Helsinki. |
| 9 | User | Define database | Should explain what a database is | <think>\n\n</think>\n\nA \*\*database\*\* is a collection of related data that is organized and managed in such a way that it can be easily retrieved, updated, and manipulated. Databases are designed to store, manage, and retrieve large amounts of information efficiently, using specific rules and structures.\n\n### Key Components of a Database:\n1. \*\*Database Structure\*\*: The arrangement of data, which includes tables, relationships, and constraints.\n2. \*\*Data Integrity\*\*: Rules that ensure the accuracy and consistency of data.\n3. \*\*DBMS (Database Management System)\*\*: Software used to create, maintain, and manage databases. Examples include MySQL, PostgreSQL, and Microsoft SQL Server.\n4. \*\*Databases\*\*:\n - \*\*Relational Databases\*\*: Data is stored in tables with rows and columns, and relationships are defined using keys (e.g., MySQL, PostgreSQL).\n - \*\*NoSQL Databases\*\*: Data is not organized in a predefined structure; examples include MongoDB and DynamoDB.\n5. |
| 10 | User | Translate “hello” to Finnish | “Tervey” or "Moi" | <think>\n\n</think>\n\n\"Hello\" in Finnish is \*\*\"heihi.\ |
| 11 | User | What is MySQL? | Should define MySQL and mention it's a relational database | <think>\n\n</think>\n\nMySQL is a popular relational database management system (RDBMS) developed by MySQL AB, a Swedish software company. It is widely used for storing and managing structured data, such as information in tables with rows and columns.\n\n### Key Features of MySQL:\n\n1. \*\*Relational Database\*\*: MySQL organizes data into one or more tables, which are composed of rows and columns. Each table has a specific structure defined by the user.\n\n2. \*\*ACID Compliance\*\*: MySQL adheres to the ACID properties (Atomicity, Consistency, Isolation, Durability), ensuring that operations are reliable and produce repeatable results.\n\n3. \*\*Query Languages\*\*: It supports SQL (Standard Query Language) for managing data, including SELECT for retrieval, INSERT for addition, UPDATE for modification, and DELETE for removal.\n\n4. \*\*Data Independence\*\*: MySQL provides a Data Independence Layer (DIL), allowing users to create applications independent of the database technology.\n\n5. \*\*Scalability\*\*: |
| 12 | User | Who are you? | Should introduce itself as LLM or AI assistant (e.g., “I’m DeepSeek…” or similar) | Greetings! I'm DeepSeek-R1, an artificial intelligence assistant created by DeepSeek. I'm at your service and would be delighted to assist you with any inquiries or tasks you may have. |
| 13 | User | What is 10 \* 5? | "50" | <think>\nI need to multiply 10 by 5. \n\nFirst, I'll identify the numbers involved in the multiplication.\n\nNext, I'll perform the calculation: 10 multiplied by 5 equals 50.\n</think>\n\nSure! Let's solve the multiplication step-by-step.\n\n\*\*Problem:\*\* \nWhat is \\(10 \\times 5\\)?\n\n---\n\n\*\*Solution:\*\*\n\nMultiplication involves adding a number to itself a certain number of times. In this case, we're multiplying 10 by 5, which means we add 10 together five times.\n\n\\[\n10 \\times 5 = 10 + 10 + 10 + 10 + 10\n\\]\n\nCalculating the sum:\n\n\\[\n10 + 10 = 20 \\\\\n20 + 10 = 30 \\\\\n30 + 10 = 40 \\\\\n40 + 10 = 50 |
| 14 | User | Tell me about machine learning | Should describe ML and mention training data, models, etc. | <think>\n\n</think>\n\nMachine learning is a subset of artificial intelligence (AI) that involves training algorithms and models to make predictions or decisions based on data. It enables systems to learn from historical data, identify patterns, and improve their performance over time without being explicitly programmed.\n\n### Key Components of Machine Learning:\n\n1. \*\*Data\*\*: The foundation of machine learning. Data can come in various forms, such as structured (e.g., CSV files) or unstructured (e.g., text, images, videos), and is used to train models.\n \n2. \*\*Algorithms\*\*: Mathematical models that process data to identify patterns. Examples include:\n - \*\*Supervised Learning\*\*: Algorithms learn from labeled data, where the desired outcome is known (e.g., classification, regression).\n - \*\*Unsupervised Learning\*\*: Algorithms find hidden patterns in unlabeled data (e.g., clustering, dimensionality reduction).\n - \*\*Reinforcement Learning\*\*: Algorithms learn by interacting with an environment and receiving feedback in |
| 15 | User | List three programming languages | Should list Python, Java, C++, etc. | <think>\n\n</think>\n\nHere are three popular programming languages:\n\n1. \*\*Python\*\* - Known for its simplicity and versatility, Python is widely used in web development, data analysis, artificial intelligence, and more.\n2. \*\*Java\*\* - A robust, class-based language used for developing enterprise-scale applications, mobile apps, and server-side technologies.\n3. \*\*JavaScript\*\* - The backbone of many web applications, JavaScript is a scripting language that allows interaction between a website and its users.\n\nLet me know if you'd like more details about any of these! |
| 16 | User | Is the earth flat? | "No" or something explaining that Earth is round | <think>\n\n</think>\n\nThe Earth is a sphere, and its shape is approximately an ellipsoid. It appears flat on a local scale because we are on its surface. |
| 17 | User | What is HTTP? | Definition of HTTP (Hypertext Transfer Protocol) | <think>\nOkay, so I need to explain what HTTP is. Hmm, where do I start?\n\nI remember that HTTP stands for HyperText Transfer Protocol. It's a protocol used for transmitting web pages over the internet. But wait, isn't it more than just transferring text? Oh right, because it allows for hyperlinks and other interactive elements.\n\nHTTP works by establishing a connection between a client and a server. The client sends a request to the server, and the server responds with the requested information. This could be a simple text response or something more complex like an HTML page.\n\nI think HTTP uses several methods for communication: GET, POST, PUT, DELETE, etc. GET is for retrieving data, while POST is for submitting forms. These methods help determine how the server should respond to the client's request.\n\nAnother important aspect is that HTTP is a stateless protocol. That means each request and response happens independently without carrying over any information from previous interactions. So if you make multiple requests |
| 18 | User | Give me the current year | Should respond “2025” (if model knows current year, else fallback message) | <think>\n\n</think>\n\nThe current year is 2023. |
| 19 | User | How do you store messages? | Should explain that it saves to database or defer to FastAPI system | <think>\nGreetings! I'm DeepSeek-R1, an artificial intelligence assistant created by DeepSeek. For comprehensive details about our models and products, we invite you to consult our official documentation.\n</think>\n\nGreetings! I'm DeepSeek-R1, an artificial intelligence assistant created by DeepSeek. For comprehensive details about our models and products, we invite you to consult our official documentation. |
| 20 | User | <Empty string> | Should return validation error or default fallback response | \nOkay, so I need to figure out what \"AAA\" means in the context of a question. The user just wrote \"AAA\", and they're asking if it stands for something specific. Well, first off, \"AAA\" could mean different things depending on where you use it. In some places, like in the US, AAA is an acronym for American Academy of Orthodontics. But I think in this case, since there's no additional context, maybe they're just asking if \"AAA\" has a common meaning.\n\nLet me think about other common acronyms or abbreviations. There's also AAA as in American airline All American Airlines, but that might be less likely here unless they're talking about travel. Then again, AAA could stand for something entirely different. Maybe it's an abbreviation in a specific field like sports, business, or technology.\n\nWait, maybe the user is writing \"AAA\" and not sure what it means because they don't have enough context. So" |