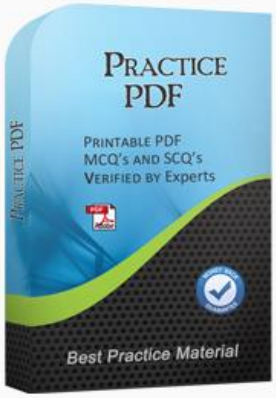
BraindumpQuiz

BraindumpQuiz

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Exam : **CT-GenAI**

Title : ISTQB Certified Tester Testing with Generative AI (CT-GenAI) v1.0

Vendor : iSQI

Version : DEMO

NO.1 A tester uploads crafted images that steer the LLM into validating non-existent acceptance criteria. Which attack vector is this?

A. Data exfiltration

B. Request manipulation

C. Malicious code generation

D. Data poisoning

Answer: B

Explanation:

This scenario describes a form ofRequest Manipulation, specifically a type of "Prompt Injection" or "Adversarial Prompting." In this attack vector, the user (or an external attacker) provides malicious or deceptive input-in this case, via an image in a multimodal LLM-to bypass the model's intended constraints or to steer its logic toward an unintended outcome. By crafting an image that tricks the LLM into seeing

"acceptance criteria" that aren't actually there, the attacker manipulates the model's request processing to generate false validation results. This is different fromData Poisoning(Option A), which involves corrupting the training data before the model is even built. It is also distinct fromData Exfiltration(Option B), which aims to steal data from the model. In a testing environment, request manipulation is a significant risk because it can lead to "Silent Failures," where the AI reports that tests have passed or requirements are met based on deceptive input, thereby compromising the integrity of the entire Quality Assurance process.

NO.2 Which concept refers to breaking text into smaller units for processing by LLMs?

A. Transformer

B. Tokenization

C. Embeddings

D. Context Window

Answer: B

Explanation:

Tokenizationis the foundational process by which an LLM breaks down raw text into smaller, manageable units called "tokens." These tokens can represent individual words, parts of words (sub-words), or even punctuation marks. This is a critical step because LLMs do not "read" words like humans do; they process numerical representations of these tokens. The way text is tokenized directly impacts the model's efficiency and its ability to understand complex technical terminology used in software testing. For example, a rare technical term might be broken into several sub-word tokens. This process is closely linked to theContext Window(Option C), which is the maximum number of tokens a model can "remember" or process at one time. WhileEmbeddings(Option B) are the numerical vectors that represent the meaning of these tokens, and theTransformer(Option A) is the underlying architecture that processes them, tokenization is the specific mechanism for initial text decomposition. Understanding tokenization is vital for testers when managing long requirement documents to ensure they do not exceed the model's limits.

NO.3 Which technique MOST directly reduces hallucinations by grounding the model in project realities?

A. Use longer temperature settings

B. Randomize prompts each run

C. Rely on generic examples only

D. Provide detailed context

Answer: D

Explanation:

Hallucinations-where an LLM generates factually incorrect or nonsensical information-occur primarily when the model lacks sufficient specific information and "fills in the gaps" using probabilistic patterns from its training data. The most effective mitigation strategy is "grounding," which involves providing the model with detailed, project-specific context. By including technical specifications, existing API schemas, business rules, and identified constraints within the prompt, the tester restricts the model's operational space to the

"project realities." This ensures the model does not have to guess or improvise details about the System Under Test (SUT). In contrast, randomizing prompts (Option B) or relying on generic examples (Option C) increases the likelihood of inconsistent and inaccurate outputs. Furthermore, using "longer" or higher temperature settings (Option D) actually encourages creativity and randomness, which is the opposite of the precision required for testing and significantly increases the risk of hallucinations. Therefore, rich contextual grounding is the technical foundation for reliable AI-assisted test analysis.

NO.4 You are tasked with applying structured prompting to perform impact analysis on recent code changes. Which of the following improvements would BEST align the prompt with structured prompt engineering best practices for comprehensive impact analysis?

A. Include references to version control systems like Git in the constraints.

B. Specify that the role is a test architect specializing in CI/CD pipelines.

C. Add a step to review the change log for syntax errors before analysis.

D. Include mapping code changes to affected modules, identifying test cases, prioritizing by risk level and change complexity

Answer: D