KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Secure Software Design**

Title : WGU Secure Software Design (D487) Exam

Version : DEMO

1.What are the three primary goals of the secure software development process?
A. Performance, reliability, and maintainability
B. Cost, speed to market, and profitability
C. Redundancy, scalability, and portability
D. Confidentiality, integrity, and availability
Answer: D
Explanation:
The three primary goals of the secure software development process, often referred to as the CIA triad, are confidentiality, integrity, and availability. These principles form the cornerstone of security considerations in the software development life cycle (SDLC).
Confidentiality ensures that sensitive information is accessed only by authorized individuals and systems. This involves implementing access controls and encryption to protect data from unauthorized access.
Integrity refers to maintaining the accuracy and consistency of data across its lifecycle. This means that the data is not altered or tampered with by unauthorized entities. Techniques like checksums and digital signatures help ensure data integrity.
Availability ensures that information and resources are accessible to authorized users when needed. This involves creating resilient systems that can withstand attacks and recover quickly from any disruptions.
By integrating these security goals into each phase of the SDLC, from planning and design to development, testing, and maintenance, organizations can create more secure software systems that are resilient to cyber threats.
Reference: The information provided here is verified as per the Secure Software Design documents and best practices in the field, as outlined by sources such as Snyk1, GeeksforGeeks2, and SAFECode3.

2.What refers to the review of software source code by developers other than the original coders to try to identify oversights, mistakes, assumptions, a lack of knowledge, or even experience?
A. User acceptance testing
B. Manual peer review
C. Fault injection
D. Dynamic code review
Answer: B
Explanation:
Manual peer review refers to the systematic examination of software source code by developers other than the original author. This practice is recognized as a valuable tool for reducing software defects and improving the quality of software projects. It involves developers inspecting the code to find and fix mistakes overlooked in the initial development phase, which enhances both the overall quality of software and the developers' skills. Peer code review is less formal and more "lightweight" than the code inspections performed in the past, and it provides benefits such as knowledge transfer, increased team awareness, and creation of alternative solutions to problems.
Reference: Expectations, Outcomes, and Challenges Of Modern Code Review1 Introduction to Software Engineering/Quality/Code Review2
Software Security during Modern Code Review: The Developer's Perspective3

3.Which software-testing technique can be automated or semi-automated and provides invalid, unexpected, or random data to the inputs of a computer software program?
A. Fuzzing
B. Static analysis
C. Dynamic analysis
D. Bugtraq
Answer: A
Explanation:
Fuzzing is an automated or semi-automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program1. This process is designed to uncover coding errors, security vulnerabilities, and other potential issues within the software by observing how it behaves under unexpected or malformed inputs. Fuzzing is particularly effective because it can expose corner cases that have not been properly dealt with and can be used to test programs that take structured inputs, such as file formats or protocols2.
Reference: 1: Wikipedia - Fuzzing 2: DZone - Fuzzing in Software Engineering

4.What sits between a browser and an internet connection and alters requests and responses in a way the developer did not intend?
A. Load testing
B. Input validation
C. Intercept proxy
D. Reverse engineering
Answer: C
Explanation:
An intercept proxy, also known as a proxy server, sits between a web client (such as a browser) and an external server to filter, monitor, or manipulate the requests and responses passing through it.
This can be used for legitimate purposes, such as security testing and user privacy, but it can also be exploited by attackers to alter web traffic in a way that the developer did not intend, potentially leading to security vulnerabilities.
Reference: Understanding of HTTP and HTTPS protocols12.
Definition and role of proxy servers3.

5.What is a best practice of secure coding?
A. Planning
B. Session management
C. User acceptance testing
D. Microservices
Answer: B
Explanation:
Session management is a core component of secure coding, which involves maintaining the state of a user’s interaction with a system. Proper session management can help protect against various security vulnerabilities, such as session hijacking and session fixation attacks. It is essential for ensuring that user data is handled securely throughout an application’s workflow.
Reference: The OWASP Secure Coding Practices guide emphasizes the importance of implementing

secure coding standards, which include robust session management1. Additionally, Snyk’s secure coding practices highlight the significance of access control, including authentication and authorization, as fundamental to protecting a system2. These resources align with the concept that effective session management is a best practice in secure coding.