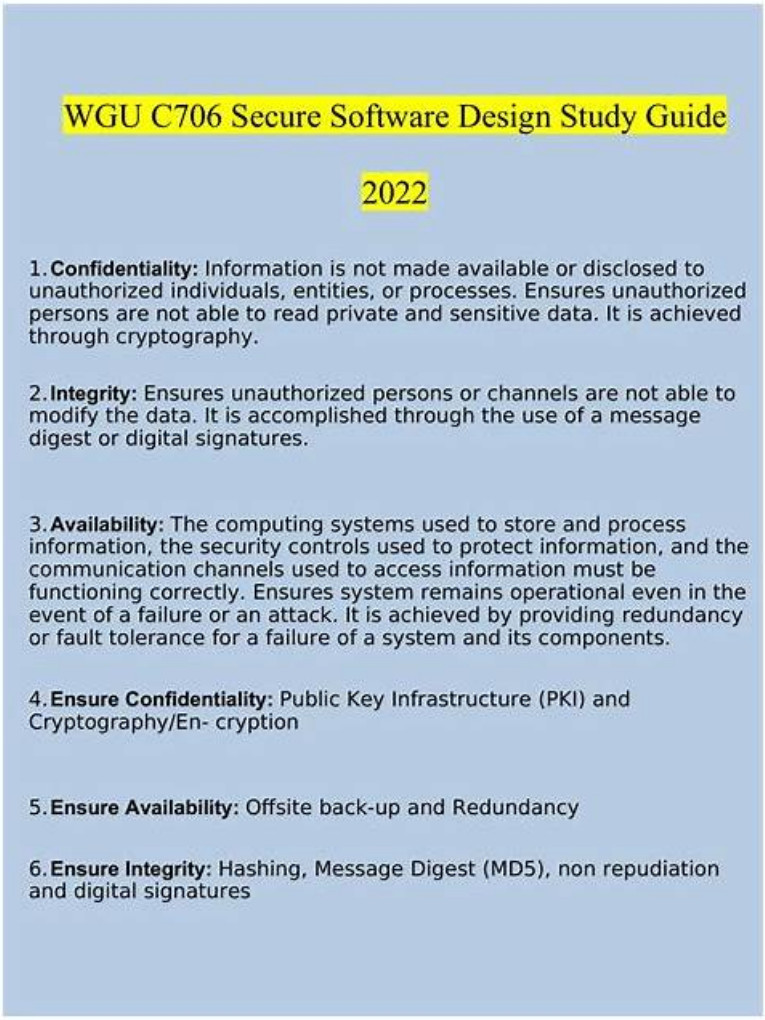
Reliable Secure-Software-Design Study Materials - Certified Secure-Software-Design Questions



BTW, DOWNLOAD part of Prep4sureExam Secure-Software-Design dumps from Cloud Storage: https://drive.google.com/open?id=1Q4XAfNHnN7bhOZpzpDRkk4wOr_Y6b0Z7

WGU Secure-Software-Design Exam Questions just focus on what is important and help you achieve your goal. With high-quality Secure-Software-Design guide materials and flexible choices of learning mode, they would bring about the convenience and easiness for you. Every page is carefully arranged by our experts with clear layout and helpful knowledge to remember.

WGU Secure-Software-Design Exam Syllabus Topics:

Topic	Details
Topic 1	• Large Scale Software System Design: This section of the exam measures skills of Software Architects and covers the design and analysis of large scale software systems. Learners investigate methods for planning complex software architectures that can scale and adapt to changing requirements. The content addresses techniques for creating system designs that accommodate growth and handle increased workload demands.

Topic 2	• Design Pattern Selection and Implementation: This section of the exam measures skills of Software Developers and Software Architects and covers the selection and implementation of appropriate design patterns. Learners examine common design patterns and their applications in software development. The material focuses on understanding when and how to apply specific patterns to solve recurring design problems and improve code organization.
Topic 3	• Software Architecture and Design: This module covers topics in designing, analyzing, and managing large scale software systems. Students will learn various architecture types, how to select and implement appropriate design patterns, and how to build well structured, reliable, and secure software systems.
Topic 4	• Software Architecture Types: This section of the exam measures skills of Software Architects and covers various architecture types used in large scale software systems. Learners explore different architectural models and frameworks that guide system design decisions. The content addresses how to identify and evaluate architectural patterns that best fit specific project requirements and organizational needs.

WGU certification Secure-Software-Design exam questions and answers come out

Up to now, there are three versions of Secure-Software-Design exam materials for your choice. So high-quality contents and flexible choices of Secure-Software-Design learning mode will bring about the excellent learning experience for you. Though the content of these three versions of our Secure-Software-Design study questions is the same, their displays are totally different. And you can be surprised to find that our Secure-Software-Design learning quiz is developed with the latest technologies as well.

WGUSecure Software Design (KEO1) Exam Sample Questions (Q16-Q21):

NEW QUESTION # 16
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. Fault injection
- B. Manual peer review
- C. User acceptance testing
- 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.
References:
* 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

NEW QUESTION # 17
Which DKEAD category has a risk rating based on the threat exploit's potential level of harm?

- A. Affected users
- B. Exploitability
- C. Reproducibility

- D. Damage potential

Answer: D

Explanation:
The DKEAD category that has a risk rating based on the threat exploit's potential level of harm is Damage potential. This category assesses the total damage or impact that a threat could cause if it is exploited by an attacker. The risk rating in this category is determined by evaluating the severity of the potential damage, which could range from information disclosure to complete system destruction or loss of system availability.
:
DREAD Threat Modeling1
OWASP Risk Rating Methodology2
DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis3

NEW QUESTION # 18
Which type of security analysis is performed by injecting malformed data into open interfaces of an executable or running application and is most commonly executed during the testing or deployment phases of the SDLC?

- A. Static Analysis
- B. Dynamic Analysis
- C. Manual Code Review
- D. Fuzz Testing

Answer: D

NEW QUESTION # 19
A new product does not display personally identifiable information, will not let private documents be printed, and requires elevation of privilege to retrieve archive documents. Which secure coding practice is this describing?

- A. Access control
- B. Input validation
- C. Authentication
- D. Data protection

Answer: A

Explanation:
The secure coding practice being described is Access Control. This practice ensures that access to data and features within a system is restricted and controlled. The description given indicates that the product has mechanisms to prevent the display of personally identifiable information (PII), restrict the printing of private documents, and require elevated privileges to access archived documents. These are all measures to control who has access to what data and under what circumstances, which is the essence of access control.
:
ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud1.
NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)2.
ISO/IEC 29151:2017, Code of practice for personally identifiable information protection3.

NEW QUESTION # 20
Which type of threat exists when an attacker can intercept and manipulate form data after the user clicks the save button but before the request is posted to the API?

- A. Tampering
- B. Elevation of privilege
- C. Spoofing
- D. Information disclosure

Answer: A

Explanation:
The type of threat described is Tampering. This threat occurs when an attacker intercepts and manipulates data being sent from the client to the server, such as formdata being submitted to an API. The attacker may alter the data to change the intended operation, inject malicious content, or compromise the integrity of the system. Tampering attacks are a significant concern in secure software design because they can lead to unauthorized changes and potentially harmful actions within the application.
References:
* Understanding the different types of API attacks and their prevention1.
* Comprehensive guide on API security and threat mitigation2.
* Detailed analysis of Man-in-the-Middle (MitM) attacks and their impact on API security3.

NEW QUESTION # 21
.....

Our Secure-Software-Design practice materials comprise of a number of academic questions for your practice, which are interlinked and helpful for your exam. So their perfection is unquestionable. As a result, Secure-Software-Design real exam win worldwide praise and acceptance. Our Secure-Software-Design practice materials are determinant factors giving you assurance of smooth exam. The sooner you make up your mind, the more efficient you will win.