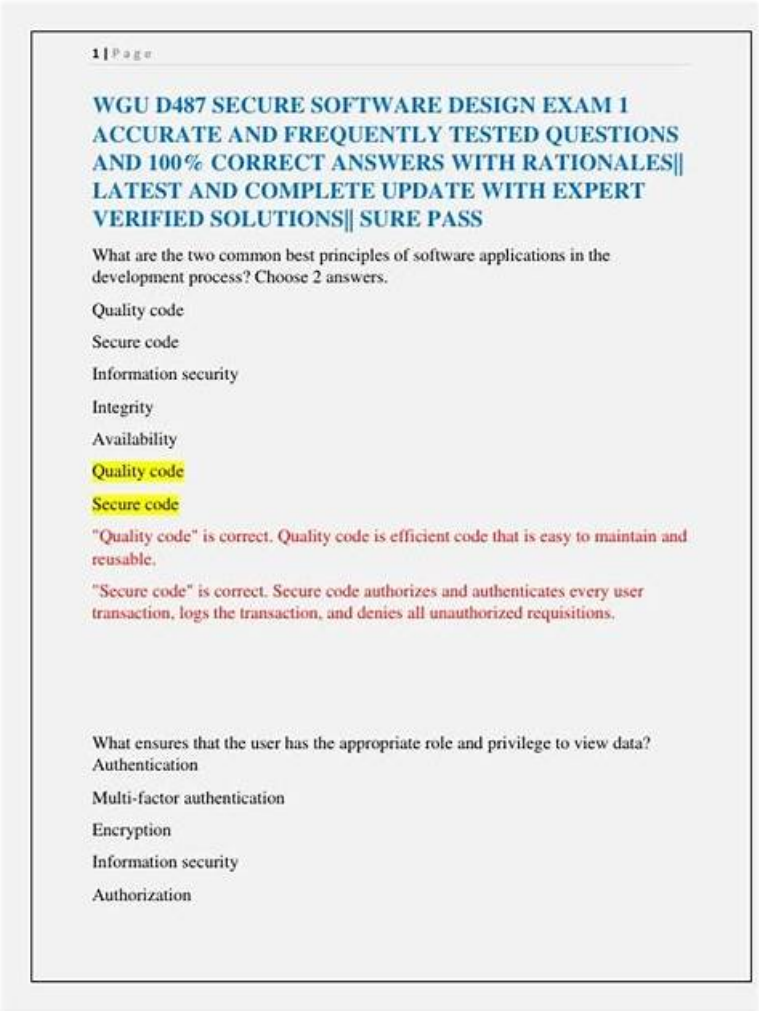
WGU Secure-Software-Design Vce Free, Latest Secure-Software-Design Real Test


1 | Page

WGU D487 SECURE SOFTWARE DESIGN EXAM 1 ACCURATE AND FREQUENTLY TESTED QUESTIONS AND 100% CORRECT ANSWERS WITH RATIONALES|| LATEST AND COMPLETE UPDATE WITH EXPERT VERIFIED SOLUTIONS|| SURE PASS

What are the two common best principles of software applications in the development process? Choose 2 answers.

Quality code

Secure code

Information security

Integrity

Availability

Quality code

Secure code

"Quality code" is correct. Quality code is efficient code that is easy to maintain and reusable.

"Secure code" is correct. Secure code authorizes and authenticates every user transaction, logs the transaction, and denies all unauthorized requisitions.

What ensures that the user has the appropriate role and privilege to view data?
Authentication

Multi-factor authentication

Encryption

Information security

Authorization

BTW, DOWNLOAD part of BraindumpsIT Secure-Software-Design dumps from Cloud Storage: https://drive.google.com/open?id=1sT5JWUeDsXqvqXxThh0FGH-x-EYJ2llu

Compared with the book version, our Secure-Software-Design exam dumps is famous for instant access to download, and if you receive your downloading link within ten minutes, and therefore you don't need to spend extra time on waiting the arriving of the exam materials. Furthermore, Secure-Software-Design training materials are edited and verified by professional experts, therefore the quality can be guaranteed. We offer you free update for one year for Secure-Software-Design Study Materials, and the update version will be sent to your email automatically. If you choose us, you just choose to pass your exam just one time!

For some difficult points of the Secure-Software-Design exam questions which you may feel hard to understand or easy to confuse for too similar with the others. In order to help you memorize the Secure-Software-Design guide materials better, we have detailed explanations of the difficult questions such as illustration, charts and referring website. Every year some knowledge of the Secure-Software-Design Practice Braindumps is reoccurring over and over. You must ensure that you master them completely.

>> WGU Secure-Software-Design Vce Free <<

Latest Secure-Software-Design Real Test | Secure-Software-Design Dumps Questions

In order to meet the needs of all customers, our company employed a lot of leading experts and professors in the field. These experts and professors have designed our Secure-Software-Design exam questions with a high quality for our customers. We can promise that our Secure-Software-Design training guide will be suitable for all people, including students and workers and so on. You can use our Secure-Software-Design study materials whichever level you are in right now. And we can promise you will get success by our products.

WGU Secure-Software-Design Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Reliable and Secure Software Systems: This section of the exam measures skills of Software Engineers and Security Architects and covers building well structured, reliable, and secure software systems. Learners explore principles for creating software that performs consistently and protects against security threats. The content addresses methods for implementing reliability measures and security controls throughout the software development lifecycle.
Topic 3	• 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 4	• Software System Management: This section of the exam measures skills of Software Project Managers and covers the management of large scale software systems. Learners study approaches for overseeing software projects from conception through deployment. The material focuses on coordination strategies and management techniques that ensure successful delivery of complex software solutions.
Topic 5	• 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.

WGUSecure Software Design (KEO1) Exam Sample Questions (Q33-Q38):

NEW QUESTION # 33
Recent vulnerability scans discovered that the organization's production web servers were responding to ping requests with server type, version, and operating system, which hackers could leverage to plan attacks.
How should the organization remediate this vulnerability?

- A. Access to configuration files is limited to administrators
- B. Always uninstall or disable features that are not required
- C. Ensure servers are configured to return as little information as possible to network requests
- D. Ensure servers are regularly updated with the latest security patches

Answer: C

Explanation:
To remediate the vulnerability of servers responding to ping requests with sensitive information, the organization should configure the servers to return as little information as possible to network requests. This practice is known as reducing the attack surface. By limiting the amount of information disclosed, potential attackers have less data to use when attempting to exploit vulnerabilities.
Regular updates and patching (Option B) are also important, but they do not address the specific issue of information disclosure.
Uninstalling or disabling unnecessary features (Option C) and restricting access to configuration files (Option D) are good security practices, but they do not directly prevent the leakage of server information through ping responses.
References: The remediation steps are aligned with best practices in vulnerability management, which include finding, prioritizing, and

fixing vulnerabilities, as well as configuring servers to minimize the exposure of sensitive information123.

NEW QUESTION # 34
While performing functional testing of the ordering feature in the new product, a tester noticed that the order object was transmitted to the POST endpoint of the API as a human-readable JSON object.
How should existing security controls be adjusted to prevent this in the future?

- A. Ensure passwords and private information are not logged
- B. Ensure the contents of authentication cookies are encrypted
- C. Ensure sensitive transactions can be traced through an audit log
- D. Ensure all requests and responses are encrypted

Answer: D

Explanation:
Comprehensive and Detailed In-Depth Explanation:
Transmitting data in a human-readable format, such as JSON, over an API can expose sensitive information if the communication channel is not secure. To protect the confidentiality and integrity of the data, it's essential to encrypt all requests and responses between clients and servers.
Implementing encryption, typically through protocols like HTTPS (which utilizes TLS/SSL), ensures that data transmitted over the network is not readable by unauthorized parties. This prevents potential attackers from intercepting and understanding the data, thereby safeguarding sensitive information contained within the API communications.
This practice is a fundamental aspect of secure software development and aligns with the Implementation business function of the OWASP SAMM. Within this function, the Secure Build practice emphasizes the importance of configuring the software to operate securely in its intended environment, which includes enforcing encryption for data in transit.
References:
* OWASP SAMM: Implementation - Secure Build

NEW QUESTION # 35
Which secure software design principle assumes attackers have the source code and specifications of the product?

- A. Separation of Privileges
- B. Total Mediation
- C. Psychological Acceptability
- D. Open Design

Answer: D

NEW QUESTION # 36
Using a web-based common vulnerability scoring system (CVSS) calculator, a security response team member performed an assessment on a reported vulnerability in the company's customer portal. The base score of the vulnerability was 9.9 and changed to 8.0 after adjusting temporal and environmental metrics.
Which rating would CVSS assign this vulnerability?

- A. High severity
- B. Medium severity
- C. Critical severity
- D. Low severity

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
CVSS scores are classified into severity levels based on numeric ranges. A base score of 9.9 falls within the Critical range (9.0-10.0), but after adjustment for temporal and environmental metrics, the score is 8.0, which falls into the High severity category (7.0-8.9). Therefore, the final rating assigned is High severity.
Medium severity corresponds to scores between 4.0 and 6.9, and low severity is below 4.0. This scoring methodology is defined by the FIRST Common Vulnerability Scoring System v3.1 Specification which guides how scores are adjusted to reflect real-world risk

contexts.
References:
FIRST CVSS v3.1 Specification
OWASP Vulnerability Severity Classification
NIST National Vulnerability Database (NVD)

NEW QUESTION # 37
Recent vulnerability scans discovered that the organization's production web servers were responding to ping requests with server type, version, and operating system, which hackers could leverage to plan attacks.
How should the organization remediate this vulnerability?

- A. Access to configuration files is limited to administrators
- B. Always uninstall or disable features that are not required
- C. Ensure servers are configured to return as little information as possible to network requests
- D. Ensure servers are regularly updated with the latest security patches

Answer: C

Explanation:
To remediate the vulnerability of servers responding to ping requests with sensitive information, the organization should configure the servers to return as little information as possible to network requests. This practice is known as reducing the attack surface. By limiting the amount of information disclosed, potential attackers have less data to use when attempting to exploit vulnerabilities.
Regular updates and patching (Option B) are also important, but they do not address the specific issue of information disclosure.
Uninstalling or disabling unnecessary features (Option C) and restricting access to configuration files (Option D) are good security practices, but they do not directly prevent the leakage of server information through ping responses.
: The remediation steps are aligned with best practices in vulnerability management, which include finding, prioritizing, and fixing vulnerabilities, as well as configuring servers to minimize the exposure of sensitive information123.

NEW QUESTION # 38
.....