WGU Secure-Software-Design D487 Practice Questions

Shared by Walton on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- User acceptance testing
B- Manual peer review
C- Fault injection
D- Dynamic code review

P2P exams

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.

P2P exams

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

Question 2

Question Type: MultipleChoice

Company leadership has contracted with a security firm to evaluate the vulnerability of all externally lacing enterprise applications via automated and manual system interactions. Which

security testing technique is being used?

Options:

A- Properly-based-testing
B- Source-code analysis
C- Penetration testing
D- Source-code fault injection

Answer:

C

Explanation:

The security testing technique that involves evaluating the vulnerability of all externally facing enterprise applications through both automated and manual system interactions is known as Penetration Testing. This method simulates real-world attacks on systems to identify potential vulnerabilities that could be exploited by attackers. It is a proactive approach to discover security weaknesses before they can be exploited in a real attack scenario. Penetration testing can include a variety of methods such as network scanning, application testing, and social engineering tactics to ensure a comprehensive security evaluation.

Question 3

Question Type: MultipleChoice

What is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or distribution to provide confidentiality, integrity, and availability?

Options:

A- Availability
B- Integrity
C- Confidentiality
D- Information Security

Answer:

D

Question 4

Question Type: MultipleChoice

Which concept is demonstrated when every module in a particular abstraction layer of a computing environment can only access the information and resources that are necessary for its legitimate purpose?

Options:

A- Privacy
B- Principle of Least Privilege
C- Elevation of Privilege
D- Confidentiality

Answer:

B

Question 5

Question Type: MultipleChoice

Which type of security analysis is limited by the fact that a significant time investment of a highly skilled team member is required?

Options:

A- Fuzz testing
B- Dynamic code analysis
C- Manual code review
D- Static code analysis

Answer:

C

Explanation:

Manual code review is a type of security analysis that requires a significant time investment from a highly skilled team member. This process involves a detailed and thorough examination of the source code to identify security vulnerabilities that automated tools might miss. It is labor-intensive because it relies on the expertise of the reviewer to understand the context, logic, and potential security implications of the code. Unlike automated methods like static or dynamic code analysis, manual code review demands a deep understanding of the codebase, which can be time-consuming and requires a high level of skill and experience.

Question 6

Question Type: MultipleChoice

Which security assessment deliverable identities unmanaged code that must be kept up to date throughout the life of the product?

Options:

A- Threat profile
B- Metrics template
C- Product risk profile
D- List of third-party software

Answer:

D

Explanation:

The security assessment deliverable that identifies unmanaged code that must be kept up to date throughout the life of the product is the List of third-party software. Unmanaged code refers to code that does not run under the garbage-collected environment of the .NET Common Language Runtime, and it often includes legacy code, system libraries, or code written in languages that do not support automatic memory management. Keeping a list of third-party software is crucial because it helps organizations track dependencies and ensure they are updated, patched, and compliant with security standards. This is essential for maintaining the security posture of the software over time, as outdated components can introduce vulnerabilities.

Question 7

Question Type: MultipleChoice

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?

Options:

A- User acceptance testing
B- Manual peer review
C- Fault injection
D- Dynamic code review

P2P exams

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.

P2P exams

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

Question 8

Question Type: MultipleChoice

The software security team is performing security testing for a new software product that is close to production release. They are concentrating on integrations between the new product

and database servers, web servers, and web services.

Which security testing technique is being used?

Options:

A- Fuzz testing
B- Dynamic code analysis
C- Binary fault injection
D- Binary code analysis

Answer:

A

Explanation:

Fuzz testing is the ideal technique in this scenario. Here's why:

Focus on Integrations: The scenario emphasizes testing links between the software, databases, web servers, and web services. Fuzz testing is specifically designed to find vulnerabilities in how software handles data and communication between components.

Pre-release Testing: The product being close to release indicates a critical need to identify security flaws before public deployment. Fuzz testing is effective in uncovering unexpected behavior and potential vulnerabilities.

Fuzz Testing Targets: Fuzz testing works by injecting invalid or unexpected data into interfaces (like those between databases, web components, etc.) to observe how the software reacts. This helps expose potential security gaps and weaknesses.

Question 9

Question Type: MultipleChoice

Which secure coding practice requires users to log in to their accounts using an email address and a password they choose?

Options:

A- Access Control
B- Data Protection

C- Input Validation
D- Authentication

Answer:

D

Question 10

Question Type: MultipleChoice

Which threat modeling step identifies the assets that need to be protected?

Options:

A- Set the Scope
B- Analyze the Target
C- Rate Threats
D- Identify and Document Threats

Answer:

A

Question 11

Question Type: MultipleChoice

Which DREAD category is based on how easily a threat exploit can be found?

Options:

A- Damage Potential
B- Affected Users
C- Discoverability
D- Reproducibility

Answer:

C

Question 12

Question Type: MultipleChoice

A potential threat was discovered during vulnerability testing when an environment configuration file was found that contained the database username and password stored in plain text.

How should existing security controls be adjusted to prevent this in the future?

Options:

A- Enforce Role-Based Authorization
B- Encrypt Secrets in Storage and Transit
C- Ensure Strong Password Policies are in Effect
D- Validate All User Input

Answer:

B

To Get Premium Files for Secure-Software-Design Visit

https://www.p2pexams.com/products/secure-software-design

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/secure-software-design

