

WGU.Secure-Software-Design.v2024-09-28.q27

Exam Code:	Secure-Software-Design
Exam Name:	WGU Secure Software Design (KEO1) Exam
Certification Provider:	WGU
Free Question Number:	27
Version:	v2024-09-28
# of views:	1598
# of Questions views:	270
https://www.freepdfdumps.com/WGU.Secure-Software-Design.v2024-09-28.q27.html	

NEW QUESTION: 1

Which secure coding best practice says to require authentication before allowing any files to be uploaded and to limit the types of files to only those needed for the business purpose?

- A. File management
- B. Communication security
- C. Data protection
- D. Memory management

Answer: A (LEAVE A REPLY)

The secure coding best practice that requires authentication before allowing any files to be uploaded, and limits the types of files to only those needed for the business purpose, falls under the category of File Management. This practice is crucial for preventing unauthorized file uploads, which can be a common vector for attacks such as uploading malicious files or scripts. By enforcing authentication, the application ensures that only legitimate users can upload files. Additionally, restricting the file types to those necessary for business operations minimizes the risk of uploading potentially harmful files that could compromise the system.

References:

- * OWASP Secure Coding Practices¹
- * File Upload Security Best Practices | CodeHandbook²
- * File Upload Protection - 10 Best Practices for Preventing ... - OPSWAT³

NEW QUESTION: 2

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 (LEAVE A REPLY)

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.

References: 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.

NEW QUESTION: 3

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?

A. Fuzz testing

B. Dynamic code analysis

C. Binary fault injection

D. Binary code analysis

Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 4

The software security team is performing security testing on a new software product using a testing tool that scans the running application for known exploit signatures.

Which security testing technique is being used?

- A. Automated vulnerability scanning
- B. Penetration testing
- C. Properly-based testing
- D. Source-code analysis

Answer: (SHOW ANSWER)

The security testing technique that involves using a testing tool to scan a running application for known exploit signatures is known as Automated Vulnerability Scanning. This method is part of dynamic analysis, which assesses the software in its running state to identify vulnerabilities that could be exploited by attackers. Automated vulnerability scanning tools are designed to detect and report known vulnerabilities by comparing the behavior and outputs of the application against a database of known exploit signatures¹.

References: 1: Application Security Testing: Tools, Types and Best Practices | GitHub

NEW QUESTION: 5

A public library needs to implement security control on publicly used computers to prevent illegal downloads.

Which security control would prevent this threat?

- A. Nonrepudiation
- B. Authentication
- C. Integrity
- D. Availability

Answer: B (LEAVE A REPLY)

Authentication is the most effective control for the scenario because it directly addresses who is using the public computers:

- * User Identification: Authentication requires users to identify themselves (e.g., library card, login credentials) before accessing the computers. This links actions to specific individuals, making it easier to control unauthorized activity.
- * Policy Enforcement: Combined with other controls (e.g., content filtering), authentication enables the library to implement policies restricting downloads. If users violate the policy, their identities can be used for consequences.
- * Deterrent: Knowing they can be identified discourages users from attempting illegal downloads.

NEW QUESTION: 6

Which SDL security goal is defined as ensuring timely and reliable access to and use of information?

- A. Information security
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: C (LEAVE A REPLY)

The term 'availability' in the context of Secure Software Development Lifecycle (SDL) refers to ensuring that systems, applications, and data are accessible to authorized users when needed. This means that the information must be timely and reliable, without undue delays or interruptions. Availability is a critical aspect of security, as it ensures that the software functions correctly and efficiently, providing users with the information they need to perform their tasks.

References:

- * The definition of availability as per the National Institute of Standards and Technology (NIST) Glossary¹.
- * The Microsoft Security Development Lifecycle (SDL) which emphasizes the importance of availability in secure software design².
- * General principles of Secure Software Development Life Cycle (SSDLC) that include availability as a key security goal³.

NEW QUESTION: 7

Which design and development deliverable contains the results of each type of evaluation that was performed and the type and number of vulnerabilities discovered?

- A. Security test execution report
- B. Security testing reports
- C. Privacy compliance report
- D. Remediation report

Answer: B (LEAVE A REPLY)

Security testing reports are the deliverables that typically contain detailed results of the security evaluations performed. These reports include the types of tests conducted, such as static and dynamic analysis, penetration testing, and code reviews, as well as the number and types of vulnerabilities discovered. The purpose of these reports is to document the security posture of the software at the time of testing and to provide a basis for remediation efforts.

References: The information aligns with best practices in secure software development, which emphasize the importance of documenting security requirements and conducting risk analysis during the design phase to identify and mitigate vulnerabilities early in the SDLC¹².

NEW QUESTION: 8

Which security assessment deliverable identifies possible security vulnerabilities in the product?

- A. SDL project outline
- B. Metrics template
- C. Threat profile
- D. List of third-party software

Answer: C ([LEAVE A REPLY](#))

A threat profile is a security assessment deliverable that identifies possible security vulnerabilities in a product. It involves a systematic examination of the product to uncover any weaknesses that could potentially be exploited by threats. The process typically includes identifying the assets that need protection, assessing the threats to those assets, and evaluating the vulnerabilities that could be exploited by those threats. This deliverable is crucial for understanding the security posture of a product and for prioritizing remediation efforts.

References: The importance of a threat profile in identifying security vulnerabilities is supported by various security resources. For instance, Future Processing's blog on vulnerability assessments outlines the steps involved in identifying security vulnerabilities, which align with the creation of a threat profile¹. Additionally, UpGuard's article on conducting vulnerability assessments further emphasizes the role of identifying vulnerabilities as part of the security assessment process².

NEW QUESTION: 9

In which step of the PASTA threat modeling methodology will the team capture infrastructure, application, and software dependencies?

- A. Attack modeling
- B. Define technical scope
- C. Define objectives
- D. Risk and impact analysis

Answer: ([SHOW ANSWER](#))

The step of the PASTA threat modeling methodology where the team will capture infrastructure, application, and software dependencies is the Define technical scope step. This step involves detailing the technical elements of the project, which includes understanding and documenting the infrastructure, applications, and software dependencies that are critical to the system's operation and security.

References: The PASTA (Process for Attack Simulation and Threat Analysis) threat modeling methodology is a seven-step process that includes defining the technical scope as a critical step for capturing the necessary technical details of the system being analyzed¹²³.

NEW QUESTION: 10

Features have been developed and fully tested, the production environment has been created, and leadership has approved the release of the new product. Technicians have scheduled a time and date to make the product available to customers.

Which phase of the software development lifecycle (SDLC) is being described?

- A. Maintenance
- B. Deployment
- C. End of life
- D. Testing

Answer: ([SHOW ANSWER](#))

The phase being described is the Deployment phase of the SDLC. This phase involves making the software available for use by customers after it has been developed, tested, and approved for release. It includes the installation of the software in the production environment, ensuring that all features are operational as intended, and obtaining formal approval from leadership to proceed with making the product available to end-users. The deployment phase is critical as it transitions the software from a development setting to a real-world operational environment.

References:

- * SDLC Deployment Phase - A Step by Step Guide¹
- * Understanding the SDLC: Software Development Lifecycle Explained²

NEW QUESTION: 11

What is a countermeasure to the web application security frame (ASF) authentication threat category?

- A. Role-based access controls restrict access
- B. Credentials and tokens are encrypted.
- C. Cookies have expiration timestamps.
- D. Sensitive information is scrubbed from error messages

Answer: A ([LEAVE A REPLY](#))

* ASF Authentication Threats: The Web Application Security Frame (ASF) authentication category encompasses threats related to how users and systems prove their identity to the application. This includes issues like weak passwords, compromised credentials, and inadequate access controls.

* Role-Based Access Control (RBAC): RBAC is a well-established security principle that aligns closely with addressing authentication threats. It involves assigning users to roles and granting those roles specific permissions based on the principle of least privilege. This limits the attack surface and reduces the impact of a compromised user account.

Let's analyze the other options:

* B. Credentials and tokens are encrypted: While vital for security, encryption primarily protects data at rest or in transit. It doesn't directly address authentication risks like brute-force attacks or weak password management.

* C. Cookies have expiration timestamps: Expiring cookies are a good practice, but their primary benefit is session management rather than directly mitigating authentication-specific threats.

* D. Sensitive information is scrubbed from error messages: While essential for preventing information leakage, this practice doesn't address the core threats within the ASF authentication category.

References:

* NIST Special Publication 800-53 Revision 4, Access Control (AC)

Family: (<https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>) Details the importance of RBAC as a cornerstone of access control.

* The Web Application Security Frame (ASF):

(<https://patents.google.com/patent/US7818788B2/en>) Outlines the ASF categories, with authentication being one of the primary areas.

NEW QUESTION: 12

Which secure coding practice involves clearing all local storage as soon as a user logs off for the night and will automatically log a user out after an hour of inactivity?

- A. Access control
- B. System configuration
- C. Communication security
- D. Session management

Answer: D (LEAVE A REPLY)

The practice of clearing all local storage when a user logs off and automatically logging a user out after an hour of inactivity falls under the category of Session Management. This is a security measure designed to prevent unauthorized access to a user's session and to protect sensitive data that might be stored in the local storage. By clearing the local storage, any tokens, session identifiers, or other sensitive information are removed, reducing the risk of session hijacking or other attacks. The automatic logout feature ensures that inactive sessions do not remain open indefinitely, which could otherwise be exploited by attackers.

References: The information aligns with the secure coding practices outlined by the OWASP Foundation¹, and is supported by common practices in web development for managing sessions and local storage².

NEW QUESTION: 13

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

Answer: C (LEAVE A REPLY)

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: 14

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.** Data protection
- C.** Input validation
- D.** Authentication

Answer: A (LEAVE A REPLY)

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.

References:

- * 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: 15

The scrum team decided that before any change can be merged and tested, it must be looked at by the team's lead developer, who will ensure accepted coding patterns are being followed and that the code meets the team's quality standards.

Which category of secure software best practices is the team performing?

- A.** Architecture analysis
- B.** Penetration testing
- C.** Code review
- D.** Training

Answer: C (LEAVE A REPLY)

The practice described is Code review, which is a part of secure software development best practices. Code reviews are conducted to ensure that the code adheres to accepted coding patterns and meets the team's quality standards. This process involves the examination of source code by a person or a group other than the author to identify bugs, security vulnerabilities, and ensure compliance with coding standards.

References:

- * Fundamental Practices for Secure Software Development - SAFECode1.
- * Secure Software Development Framework | CSRC2.
- * Secure Software Development Best Practices - Hyperproof3.

NEW QUESTION: 16

The software security group is conducting a maturity assessment using the Building Security in Maturity Model (BSIMM). They are currently focused on reviewing attack models created during recently completed initiatives.

Which BSIMM domain is being assessed?

- A. Governance
- B. Software security development life cycle (SSDL) touchpoints
- C. Intelligence
- D. Deployment

Answer: C (LEAVE A REPLY)

The Intelligence domain in the Building Security in Maturity Model (BSIMM) focuses on gathering and using information about software security. This includes understanding the types of attacks that are possible against the software being developed, which is why reviewing attack models falls under this domain. The BSIMM domain of Intelligence involves creating models of potential attacks on software (attack models), analyzing actual attacks that have occurred (attack intelligence), and sharing this information to improve security measures. By reviewing attack models, the software security group is essentially assessing the organization's ability to anticipate and understand potential security threats, which is a key aspect of the Intelligence domain.

References: The references used to verify this answer include the official BSIMM documentation and related resources that describe the various domains and their activities within the BSIMM framework¹²³⁴⁵.

Valid Secure-Software-Design Dumps shared by Actual4test.com for Helping Passing Secure-Software-Design Exam! Actual4test.com now offer the **newest Secure-Software-Design exam dumps**, the Actual4test.com Secure-Software-Design exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com Secure-Software-Design dumps with Test Engine here:

NEW QUESTION: 17

The security team is reviewing all noncommercial software libraries used in the new product to ensure they are being used according to the legal specifications defined by the authors.

What activity of the Ship SDL phase is being performed?

- A. Policy compliance analysis
- B. Open-source licensing review
- C. Penetration testing
- D. Final security review

Answer: (SHOW ANSWER)

The activity described pertains to the review of noncommercial software libraries to ensure compliance with the legal specifications set by the authors. This is part of the open-source licensing review, which is a critical activity in the Ship phase of the Security Development Lifecycle (SDL). This review ensures that all open-source components are used in accordance with their licenses, which is essential for legal and security compliance.

References: The Ship phase of the SDL includes various activities such as policy compliance review, vulnerability scanning, penetration testing, open-source licensing review, and final security and privacy reviews¹². The open-source licensing review specifically addresses the legal aspects of using third-party software components².

NEW QUESTION: 18

Which privacy impact statement requirement type defines how personal information will be protected when authorized or independent external entities are involved?

- A. Personal information retention requirements
- B. User controls requirements
- C. Third party requirements
- D. Data integrity requirements

Answer: (SHOW ANSWER)

The privacy impact statement requirement that defines how personal information will be protected when authorized or independent external entities are involved is best categorized under Third party requirements.

This aspect of privacy impact assessments ensures that personal data is safeguarded even when it is necessary to involve third parties, which could be service providers, partners, or other entities that might handle personal information on behalf of the primary organization. These requirements typically include stipulations for data handling agreements, security measures, and compliance checks to ensure that third parties maintain the confidentiality and integrity of the personal information they process.

References:

- * Guide to undertaking privacy impact assessments | OAIC¹
- * A guide to Privacy Impact Assessments - Information and Privacy²
- * Personal Information Protection Law of China: Key Compliance Considerations³
- * Privacy Impact Assessment - General Data Protection Regulation (GDPR)⁴
- * Privacy impact assessment (PIA) - TechTarget⁵

NEW QUESTION: 19

Which mitigation technique can be used to fight against a threat where a user may gain access to administrator level functionality?

- A. Encryption
- B. Quality of service
- C. Hashes
- D. Run with least privilege

Answer: D (LEAVE A REPLY)

The principle of running with the least privilege is a fundamental security concept that involves granting users only the permissions they need to perform their tasks and no more. This minimizes the risk of a user gaining access to administrator-level functionality that they are not authorized to use. By limiting the privileges of user accounts to the bare minimum necessary, the potential damage from various attacks, such as privilege escalation, is significantly reduced.

References: The concept of least privilege is widely recognized as a critical security measure. Resources like Exabeam's article on preventing privilege escalation and TechTarget's guide on privilege escalation attacks provide insights into how enforcing least privilege can mitigate such threats¹². These sources verify that running with the least privilege is an effective mitigation technique against the threat of unauthorized access to elevated privileges.

NEW QUESTION: 20

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 (LEAVE A REPLY)

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.

References:

- * Understanding of HTTP and HTTPS protocols¹².
- * Definition and role of proxy servers³.

NEW QUESTION: 21

A recent vulnerability scan uncovered an XML external entity (XXE) flaw that could allow attackers to return the contents of a system file by including a specific payload in an XML request.

How should the organization remediate this vulnerability?

- A. Ensure audit trails exist for all sensitive transactions
- B. Disable resolution of external entities in the parsing library
- C. Enforce role-based authorization in all application layers
- D. Ensure authentication cookies are encrypted

Answer: ([SHOW ANSWER](#))

Security change management within the change management process involves ensuring that any changes, including updates or modifications to software, do not introduce new vulnerabilities and are in line with security policies. The question about securing remote administration directly reflects this component because it addresses the security considerations that must be managed when changes are made to how software is accessed and controlled remotely. This includes implementing secure protocols, authentication methods, and monitoring to prevent unauthorized access or breaches, which are crucial when managing changes in a secure manner.

References:

- * Change management in cybersecurity emphasizes the structured approach to implementing alterations in security protocols, technologies, and processes, ensuring systematic assessment and monitoring¹.
- * The role of change management in cybersecurity includes decisions about network access and ensuring the right person can access the right information at the right time, which aligns with securing remote administration².
- * Seminal change management models in cybersecurity, like PROSCI's ADKAR model, guide individuals through the change process, managing resistance and identifying training needs, which is relevant to securing remote administration³.

NEW QUESTION: 22

Senior IT staff has determined that a new product will be hosted in the cloud and will support web and mobile users. Developers will need to deliver secure REST services. Android and iOS mobile apps. and a web application. Developers are currently determining how to deliver each part of the overall product.

Which phase of the software development lifecycle (SDLC) is being described?

- A. Maintenance
- B. End of life
- C. Deployment

D. Design

Answer: D (LEAVE A REPLY)

The phase being described is the Design phase of the SDLC. During this phase, developers and IT staff determine the architectural and operational details of the product, which includes decisions on how to deliver various components such as secure REST services, mobile apps, and web applications. The Design phase is crucial for setting the foundation for the development work that will follow, ensuring that the product will be secure, scalable, and maintainable.

References: The information aligns with the descriptions of the SDLC phases provided in resources such as GitHub's explanation of the SDLC¹ and other industry-standard software development lifecycle resources²³⁴.

NEW QUESTION: 23

What is a best practice of secure coding?

- A. Planning**
- B. Session management**
- C. User acceptance testing**
- D. Microservices**

Answer: B (LEAVE A REPLY)

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.

References: 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.

NEW QUESTION: 24

What is the privacy impact rating of an application that stores personally identifiable information, monitors users with ongoing transfers of anonymous data, and changes settings without notifying the user?

- A. P1 high privacy risk**
- B. P2 moderate privacy risk**
- C. P3 low privacy risk**
- D. P4 no privacy risk**

Answer: A (LEAVE A REPLY)

The privacy impact rating for an application that stores personally identifiable information (PII), monitors users with ongoing transfers of anonymous data, and changes settings without notifying the user would be P1 high privacy risk. Storing PII already poses a significant risk due to the potential for data breaches and misuse. Monitoring users and transferring data, even if anonymous, increases the risk as it involves ongoing data collection. Changing settings without user notification is a serious privacy concern because it can lead to unauthorized data processing or sharing, further elevating the risk level.

References:

- * Practical Data Security and Privacy for GDPR and CCPA - ISACA¹.
- * Privacy risk assessment and privacy-preserving data monitoring².
- * How To Effectively Monitor Your Privacy Program: A New Series³.

NEW QUESTION: 25

The software security team has been tasked with assessing a document management application that has been in use for many years and developing a plan to ensure it complies with organizational policies.

Which post-release deliverable is being described?

- A. Security strategy for M&A products
- B. Security strategy for legacy code
- C. Post-release certifications
- D. External vulnerability disclosure response process

Answer: (SHOW ANSWER)

The task described involves assessing a document management application that has been in use for many years. This scenario typically requires a security strategy that addresses the unique challenges of legacy code.

Legacy code refers to software that has been around for a long time and may not have been developed with current security standards in mind. A security strategy for legacy code would include measures to ensure that the application complies with current organizational policies, which may involve code reviews, updates, and the implementation of modern security practices to mitigate any potential vulnerabilities inherent in older code¹².

References:

- * Remotebase, "Best Practices for Managing Legacy Code"
- * Medium, "The Engineer's Complete Guide to Legacy Code"
- * Parasoft, "Testing Legacy Code & 3 Steps to Update"

NEW QUESTION: 26

Credit card numbers are encrypted when stored in the database but are automatically decrypted when data is fetched. The testing tool intercepted the GET response, and testers were able to view credit card numbers as clear text.

How should the organization remediate this vulnerability?

- A. Never cache sensitive data
- B. Ensure there is an audit trail for all sensitive transactions
- C. Ensure all data in transit is encrypted
- D. Enforce role-based authorization controls in all application layers

Answer: C (LEAVE A REPLY)

The core issue here is cleartext transmission of sensitive data, and option C directly addresses this:

* Addressing the Problem: The scenario reveals the vulnerability is the lack of encryption during data transmission (the GET response). Ensuring encryption in transit fixes this specific exploit.

* Transport Layer Security: Encryption during transit is typically achieved through protocols like TLS (HTTPS), preventing the interception of sensitive information.

NEW QUESTION: 27

The security team has a library of recorded presentations that are required viewing for all new developers in the organization. The video series details organizational security policies and demonstrates how to define, test for, and code for possible threats.

Which category of secure software best practices does this represent?

- A. Attack models
- B. Training
- C. Architecture analysis
- D. Code review

Answer: B (LEAVE A REPLY)

The category of secure software best practices being described is Training. This is because the focus is on educating new developers about organizational security policies and coding practices to mitigate potential threats. Training is a proactive approach to ensure that developers are aware of security concerns and are equipped with the knowledge to address them in their coding practices.

References: The importance of training in secure software best practices is supported by industry resources such as the SAFECode's "Fundamental Practices for Secure Software Development" which emphasizes the need for application security control definition and management¹, and the NIST's Secure Software Development Framework (SSDF) which recommends integrating secure development practices throughout the software development lifecycle². Additional support for this category can be found in resources detailing effective secure development practices^{3,4,5}.

Valid Secure-Software-Design Dumps shared by Actual4test.com for Helping Passing Secure-Software-Design Exam! Actual4test.com now offer the **newest Secure-Software-Design exam dumps**, the Actual4test.com Secure-Software-Design exam

questions have been updated and **answers have been corrected** get the **newest**
Actual4test.com Secure-Software-Design dumps with Test Engine here:
https://www.actual4test.com/Secure-Software-Design_examcollection.html (**118** Q&As
Dumps, **30%OFF** Special Discount: **Freepdfdumps**)