

Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/6/2022 7:33:37 pm • Time spent: 02:44

Score: 100%

Passing Score: 80%



▼ Question 1: ✓ Correct

Which application development model approaches software development as a continuous, changing process with never-ending versions, bug fixes, and enhancements?

- Agile
- Waterfall
- Code signing
- Fuzz testing

EXPLANATION

The Agile development model approaches software development as a continuous, changing process with never-ending versions, bug fixes, and enhancements.

The Waterfall development model is the most widely used model. It is called this because each step is completed before the next step is begun. This way, each step flows to the next.

Fuzz testing is software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application.

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

REFERENCES

- 10.4.3 SDLC and Development Facts

q_sdlc_agile_secp7.question.fex

▼ Question 2: Correct

You are performing a security test from the outside on a new application that has been deployed.

Which secure testing method are you MOST likely using?

- Interactive
- Static
-  Dynamic
- Runtime

EXPLANATION

Dynamic application security testing scans applications after they have been deployed. These tests are performed from the outside.

Static application security testing focuses on analyzing source code, binaries, and byte code early in the development process.

Interactive application security testing is built into static testing and uses source code scanners.

Runtime is a type of coding error that occurs while software is running.

REFERENCES

-  10.4.3 SDLC and Development Facts

q_sdlc_dynamic_secp7.question.fex

▼ Question 3: Correct

Which of the following enters random data to the inputs of an application?

- Application hardening
- Routines
-  Fuzzing
- Validation rules

EXPLANATION

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Fuzzing programs come in two types:

- Mutation-based programs, which mutate existing data samples to create test data.
- Generation-based programs, which define new test data based on models of the input.

Input validation is the process of ensuring that a program operates on clean, correct, and useful data. Input validation uses routines (also called validation rules or check routines) that check for correctness, meaningfulness, and secureness in data input to the system. Application hardening is the process of preventing vulnerability exploitation in software applications.

REFERENCES

-  [10.4.3 SDLC and Development Facts](#)

[q_sdlc_fuzzing_secp7.question.fex](#)

▼ Question 4:

✓ Correct

Which of the following is the first step in the Waterfall application development model?

 Requirements

Design

Implementation

Maintenance

EXPLANATION

The Waterfall development life cycle model steps are:

- Requirements
- Design
- Implementation
- Testing
- Development
- Maintenance

REFERENCES

 10.4.3 SDLC and Development Facts

q_sdlc_require_secp7.question.fex

▼ Question 5: Correct

Which of the following are the two main causes of software vulnerabilities? (Select two.)

 Coding errors Design flaws Normalization Obfuscation Fuzzing**EXPLANATION**

Coding errors and design flaws are the main causes of software vulnerabilities.

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy. This is done by having all related data stored in one place. This is not one of the main causes of software vulnerabilities.

Obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand. This is not one of the main causes of software vulnerabilities.

REFERENCES 10.4.3 SDLC and Development Facts

q_sdlc_software_secp7.question.fex

▼ Question 6: Correct

Which of the following is considered a drawback of the Waterfall application development life cycle?

- Each step in the life cycle only needs to be completed once before moving on to the next one.
-  Requirements are determined at the beginning and are carried through to the end product.
- Development is broken into Sprints.
- Testing is performed throughout development.

EXPLANATION

The Waterfall development life cycle is a slow process and may take months or years to complete. It also lacks flexibility since the requirements determined in the beginning are carried through to the end product.

Development is broken into Sprints when using the Agile development model.

The Agile development model performs testing throughout development.

When using the Waterfall development model, an application likely goes through some of these steps multiple times before moving on to the next step.

REFERENCES

-  10.4.3 SDLC and Development Facts

q_sdlc_waterfall_secp7.question.fex

▼ Question 7: Correct

You have just finished developing a new application. Before putting it on the website for users to download, you want to provide a checksum to verify that the object has not been modified.

Which of the following would you implement?

- Memory management
- Code obfuscation
-  Code signing
- Normalization

EXPLANATION

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. The process employs the use of a cryptographic hash to validate authenticity and integrity.

Code signing:

- Provides security when deployed.
 - Helps prevent namespace conflicts in some programming languages.
 - Provides a digital signature mechanism to verify the identity of the author or build system.
 - Provides a checksum to verify that the object has not been modified.
 - Provides versioning information about an object as well as storing other metadata about the object.
- Memory management is a resource-management process applied to computer memory.

Code obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy by having all related data stored in one place.

REFERENCES

-  10.4.7 Application Development Security Facts

q_app_devsec_code_secp7.question.fex

▼ Question 8: Correct

Which fuzz testing program type defines new test data based on models of the input?

- Memory management
-  Generation-based
- Code signing
- Mutation-based

EXPLANATION

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Fuzzing program types are:

- Mutation-based programs
 - Mutate existing data samples to create data
- Generation-based programs
 - Define new test data based on models of the input

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

Memory management is a resource-management process applied to computer memory.

REFERENCES

-  [10.4.7 Application Development Security Facts](#)

q_app_devsec_fuzz_secp7.question.fex

▼ Question 9: Correct

What is the storage location called that holds all the development source files that version control systems use?

- Memory management
-  **Repository**
- Stored procedures
- Normalization

EXPLANATION

A version control system uses a repository, which is a storage location that holds all the source files used during development.

Stored procedures are one or more database statements stored as a group in a database's data dictionary.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy by having all related data stored in one place.

Memory management is a resource-management process applied to computer memory.

REFERENCES

-  10.4.7 Application Development Security Facts

q_app_devsec_repo_secp7.question.fex

▼ Question 10: Correct

What is a set of software development tools called that can be installed as one unit and provides code frameworks or code snippets to help development go faster?

- Code signing
-  **SDK**
- Memory management
- Repository

EXPLANATION

A software development kit (SDK) is a set of software development tools that can be installed as one unit. These tools can provide code frameworks or code snippets to help development go faster.

A version control system uses a repository, which is a storage location that holds all the source files used during development.

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

Memory management is a resource-management process applied to computer memory.

REFERENCES

-  10.4.7 Application Development Security Facts

q_app_devsec_sdk_secp7.question.fex

Copyright © 2022 TestOut Corporation All rights reserved.