



Notifications

[Messages](#)

Search S.



My courses



S2-24_MERGEDSSE



General



Quiz 2

**Status** Finished**Started** Saturday, 10 May 2025, 7:32 PM**Completed** Saturday, 10 May 2025, 8:09 PM**Duration** 37 mins 26 secs**Grade** 4.50 out of 5.00 (90%)**Question 1**

Complete

Mark 0.25 out of 0.25

Which of the following can be considered as a possible solutions for SQL injection vulnerability?

- ☐ a. Secure cookies
- ☒ b. Data Validation
- ☐ c. Exception handling
- ☐ d. Encryption

**Question 2**

Complete

Mark 0.25 out of 0.25

Which of the following is not a compile-time defense against buffer overflow?

- ☐ a. Use of safe libraries
- ☐ b. Safe coding standards
- ☐ c. None of these
- ☒ d. Randomize address space

Question 3

Complete

Mark 0.25 out of 0.25

What is the common cause of buffer over flows, cross-site scripting, SQL injection and format string attacks?

- ☒ a. Unvalidated input
- ☐ b. Improper error handling
- ☐ c. Lack of authentication
- ☐ d. Insecure configuration management

Question 4

Complete

Mark 0.25 out of 0.25

Which of the following is an example of asymmetric encryption?

- ☐ a. AES
- ☐ b. TripleDES
- ☒ c. RSA
- ☐ d. RC4



Question 5

Complete

Mark 0.25 out of 0.25

What does "White List" data validation means?

- ☐ a. Parsing input for special characters
- ☐ b. Data is validated against a list of values that are known to be invalid
- ☐ c. None of these
- ☒ d. Data is validated against a list of values that are known to be valid

Question 6

Complete

Mark 0.25 out of 0.25

Which of the following enables access bypassing all security mechanisms?

- ☐ a. Phishing
- ☐ b. Trojan Horse
- ☐ c. Spam
- ☒ d. Backdoor

Question 7

Complete

Mark 0.00 out of 0.25

Which of the following is not included in documenting an Attack Pattern?

- ☐ a. Vector of attack
- ☐ b. Asset at risk
- ☐ c. Attack prerequisite
- ☒ d. Attacker Skill

Question 8

Complete

Mark 0.25 out of 0.25

Which of the following is an example of black box testing?

- ☐ a. Code-based fault injection
- ☐ b. Trust boundary mapping
- ☒ c. Network security testing
- ☐ d. Data flow analysis

Question 9

Complete

Mark 0.25 out of 0.25

SQL injection consists of

- ☒ a. Entering SQL statements instead of legitimate data
- ☐ b. Attempting an elevation of privilege
- ☐ c. Fuzzing inputs to application
- ☐ d. Entering invalid data through SQL queries

Question 10

Complete

Mark 0.25 out of 0.25

What will be output from the following C code?

...

```
int i=7,j=4;
printf("%d %d %d", i, j);
```

...

- ☐ a. 7 4 4
- ☐ b. 4 7 7
- ☐ c. Compile-time error
- ☒ d. 7 4 memory contents

Question 11

Complete

Mark 0.25 out of 0.25

Which of the following is not among design principles for software security?

- ☐ a. Separation of Privileges
- ☒ b. Focus on Assets
- ☐ c. Defense in Depth
- ☐ d. Complete Mediation

Question 12

Complete

Mark 0.25 out of 0.25

Applications developed in which programming languages are likely to have buffer-overflow vulnerability?

- ☒ a. C, C++
- ☐ b. C, Ruby
- ☐ c. C++, C#
- ☐ d. Python, Ruby

Question 13

Complete

Mark 0.25 out of 0.25

In what way Buffer Overflow is more troublesome compared to Arc Injection?

- ☐ a. Memory based protection schemes do not work
- ☐ b. A small overflow is adequate
- ☒ c. Attacker can use any payload
- ☐ d. Can avoid detection

Question 14

Complete

Mark 0.25 out of 0.25

Which of the following roles provides assurance of CSP capabilities?

- ☐ a. Cloud Carrier
- ☐ b. Cloud Consumer
- ☒ c. Cloud Auditor
- ☐ d. Cloud Broker

Question 15

Complete

Mark 0.25 out of 0.25

Which of the following is not a type of fuzz testing?

- ☐ a. Protocol-based fuzzing
- ☐ b. State-based fuzzing
- ☒ c. Logic-based fuzzing
- ☐ d. Format-based fuzzing

Question 16

Complete

Mark 0.25 out of 0.25

Buffer-overflow attack can take place if machine can execute code that resides in the _____ segment.

- ☐ a. None of these
- ☒ b. Stack
- ☐ c. Text
- ☐ d. Kernel

Question 17

Complete

Mark 0.25 out of 0.25

Which of the following is not an implication of the design principle - Reluctance to Trust

- ☐ a. Environment is expected to be insecure
- ☒ b. Coding standards are inadequate
- ☐ c. Users are susceptible to social engineering attacks
- ☐ d. Input may be malformed

Question 18

Complete

Mark 0.00 out of 0.25

Which of the following is a safe conversion?

- ☐ a. long to char
- ☒ b. unsigned short to short
- ☐ c. typecasting a pointer
- ☐ d. unsigned short to long

Question 19

Complete

Mark 0.25 out of
0.25

Which of the following browser components is a part of rendering engine in the Chromium architecture?

- ☒ a. JavaScript interpreter
- ☐ b. Safe Browsing blacklist
- ☐ c. Cookie database
- ☐ d. Download manager

Question 20

Complete

Mark 0.25 out of
0.25

Which of the following is a way to build dynamic SQL statements?

- ☐ a. Writing a query with parameters
- ☒ b. All of these
- ☐ c. Using stored procedure with parameters
- ☐ d. Executing SQL inside programs using EXEC

[← Previous](#)[Quiz 1](#)[Next →](#)[SSE Assignment](#)Contact for support : support@wilp.bits-pilani.ac.in

@2025 Copyright BITS Pilani WILP

