JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2025

M.Tech-II Semester (CSE)

COURSE CODE (CREDITS): 18M1WCI115

COURSE NAME: Secure Software Design MAX. MARKS: 25

COURSE INSTRUCTORS: Dr. Nishant Sharma MAX. TIME: 1 Hour 30 Min

Note: *(a) All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

Q.No	Question	CO	Marks
Q1	a) Differentiate between Role-Based Access Control (RBAC) and Discretionary Access Control (DAC) with examples. b) Analyze a scenario where the lack of least privilege implementation leads to a privilege escalation attack. Explain how it could have been prevented.	2	[2+3]
Q2	a) Alice wants to send a message securely to Bob using asymmetric encryption. Explain the steps involved in the process using **RSA**. b) Explain the importance of **multi-factor authentication (MFA)** in authentication security. Compare **passwords, biometrics, and MFA** in terms of effectiveness and security.	3	[2+3]
Q3	a) Explain why server-side validation is more secure than client-side validation. b) Given an input form vulnerable to SQL injection, suggest validation and sanitization techniques to prevent exploitation.	3	[2+3]
Q4	Define **buffer overflow, use-after-free, and double-free vulnerabilities.** How do attackers exploit these issues, and what techniques can be used to mitigate them?	3	[5]
Q5	a) Identify the risks associated with third-party API integrations and file uploads. b) Describe how **steganography** and **traffic padding** contribute to data confidentiality. c) Propose a basic strategy for safely handling data from untrusted external sources in a web application.	4	[2+2+1]