24MCPE661

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Third Semester MCA Degree Examination, 2025-26

SECURE SOFTWARE DEVELOPMENT

Time: 3 Hours **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	C
Q1	a.	A startup company has developed a mobile app for online payments. The app works correctly and passes all functional tests. However, after deployment, some users report unauthorized transactions. As a security consultant: Identify whether this problem is related to software assurance or software security and how both concepts should have been addressed during development to avoid this issue.	10	L3	CO1
	b.	Two teams develop the same application: • Team A uses secure coding standards, code reviews, and penetration testing. • Team B focuses only on functionality and speed of development. After deployment, Team B's software gets attacked. • Justify how development practices influence security properties of software. • Compare both teams' approaches.	10	L3	CO1
		OR			
Q2	a.	The government portal handles citizen data such as Aadhaar number, address, and bank details. The software works correctly but later suffers from data leakage. As a security analyst: • Identify the possible sources of insecurity • Discuss the missing security properties • Explain how secure software development management and early security detection could have prevented this problem.	10	L3	CO1
	b.	A development team rushes a hospital management system to meet a deadline and skips input validation and code review. Later, the system gets compromised. • Identify the sources of software insecurity in this scenario. • Explain how development practices contributed to the vulnerability.	10	L3	CO1
		Module- 2			
Q3	a.	A college portal allows students to upload assignments. • Create two misuse/abuse cases related to this system. • How these misuse cases help in identifying security requirements.	10	L3	CO2
	b.	A software team wants to adopt SQUARE for a railway reservation system. • What tools or techniques can be used in the SQUARE process? • What documents or outputs should be produced after applying SQUARE?	10	L3	CO2

		OR			
Q4	a.	A company is building a mobile banking app. Identify and write at least five security requirements that must be captured during the requirements phase. Explain how security requirements engineering helps prevent future attacks.	10	L3	CO2
	b.	A company has identified the following requirements for an e-commerce site: • User login security • Product search speed • Data encryption • UI improvements • Admin access control How would you prioritize these requirements from a security point of view ? Justify your prioritization.	10	L3	CO2
		Module- 3			
Q5	a.	A developer stores passwords in plain text and gives all users the same access privileges. • Identify which security principles are violated. • Explain how applying proper security principles would improve the system design.	10	L3	CO3
	b.	While designing an online voting system: Identify three possible attack patterns. Explain how the architecture can be designed to defend against them.	10	L3	CO3
		OR			
Q6	a.	Two designs are proposed for a railway reservation system: • Design A: Single-tier architecture where UI, logic, and database are tightly coupled. • Design B: Multi-tier architecture with authentication, validation, and access control layers. Which design is more secure and why? Explain using security principles and architectural risk analysis.	10	L3	CO3
	b.	An attacker repeatedly tries different passwords until one works. Identify the attack pattern used. Explain how knowing attack patterns helps architects design more secure systems.	10	L3	CO3
		Module – 4			
Q7	a.	A company performs security testing only after deployment. Do you think this approach is risky? Describe how security testing should be integrated throughout the SDLC.	10	L3	CO4
	b.	A developer is writing a user registration module. Write the secure coding steps he should follow. How this module should be tested from security point of view.	10	L3	CO4
		OR			
Q8	a.	Consider a file upload feature in a web application. Illustrate how you would use this feature from a functional perspective and an attacker's perspective. Identify possible security risks.	10	L3	CO4
	b.	A software system correctly implements an account lockout feature after three failed login attempts, yet it is compromised by an attacker. Examine this situation from the functional tester's point of view and the attacker's point of view. List down the limitations of functional testing and justify why both perspectives are essential in security analysis.	10	L3	CO4

MODULE 5					
Q9	a.	A fintech company wants maximum security, but the project budget and time are limited. Propose a risk-based approach to decide how much security is enough for this system. Is it practical to build a "100% secure" system? Analyze this statement and justify your answer using cost, usability, and risk trade-offs.	10	L3	CO5
	b.	An organization performs security testing only after development is complete. Evaluate the maturity level of this practice and suggest improvements to move to a higher maturity level. Compare a low-maturity security organization and a high-maturity security organization in terms of process, people, and technology.	10	L3	CO5
OR					
Q10	a.	A startup is developing a healthcare application that handles sensitive patient data. Analyze the security risks involved and propose a security strategy to be followed from the early stages of development.	10	L3	CO5
	b.	A university is developing an online examination system. Identify the major security concerns and design a security approach to address them. An organization believes functional correctness is enough and security can be handled later. Critically analyze this mindset and justify the need for early security engineering.	10	L3	CO5