Reg. No.																

Question Paper Code	13923

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Fifth Semester

Computer Science Engineering (Cyber Security)

20SCPC501 - SECURE CODING

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	What is the primary goal of secure coding? (a) Faster execution (b) Maintainability (c) Prevention of security vulnerabilities (d) Better GUI	1	K1	CO1
2.	Least privilege principle ensures: (a) All users get admin access (b) Users only have necessary permissions (c) Maximum feature access (d) Limited login attempts	1	K1	CO1
3.	Which vulnerability allows attackers to inject malicious SQL statements? (a) CSRF (b) XSS (c) SQL Injection (d) Buffer Overflow	1	K1	CO2
4.	Which the type of attack involves executing scripts in the victim's browser. (a) SQL Injection (b) CSRF (c) XSS (d) Buffer Overflow	1	K1	CO2
5.	Which of the following best describes a strong password policy? (a) Short and easy to remember (b) Use of dictionary words (c) Combination of letters, numbers, and special symbols (d) Same password across accounts	1	K1	CO3
6.	Which encryption method is most commonly used to store passwords securely? (a) Base64 encoding (b) Hashing with salt (c) Plain text storage (d) Symmetric encryption only	1	K1	CO3
7.	Select the best way for a developer wants to prevent reflected XSS in a search form (a) Encode user input before rendering it in HTML (b) Store input in database directly (c) Disable HTTPS (d) Hide form using CSS	1	K1	CO4
8.	How can a developer mitigate CSRF? (a) Use Captcha only (b) Use CSRF tokens in every request (c) Store passwords in cookies (d) Disable JavaScript	1	K1	CO4
9.	Static analysis tools are primarily used to (a) Detect runtime errors (b) Find vulnerabilities in source code without execution (c) Test user interface designs (d) Encrypt source code	1	K1	CO5
10.	Select the type of security testing that executes the application to detect vulnerabilities? (a) Static Analysis (b) Dynamic Application Security Testing (DAST) (c) Code Review (d) Unit Testing	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Define Secure coding.	2	K1	CO1
12.	List any two common software vulnerabilities.	2	K1	CO1
13.	Differentiate between input validation and input sanitization.	2	K2	CO2
14.	State SQL Injection with an example.	2	K1	CO2
15.	Explain the concept of multi-factor authentication with example.	2	K2	CO3
16.	Differentiate between authentication and authorization.	2	K2	CO3
17.	Explain how CSRF tokens can be applied in a login form.	2	K2	CO4

18.	Demonstrate prevention of XSS using input validation.	*2*	*K2*	*CO4*
19.	Summarize how static analysis tools help detect vulnerabilities.	*2*	*K2*	*CO5*
20.	Explain why DevOps requires continuous security testing.	*2*	*K2*	*CO5*
21.	Illustrate the integration of vulnerability scanning in CI/CD pipelines.	*2*	*K2*	*CO6*
22.	Demonstrate the principle of "Shift Left Security" in CI/CD pipelines.	*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a) (i)	Explain in detail Principles of Secure Coding in detail.	*6*	*K2*	*CO1*
	(ii)	Outline buffer over flow attack.	*5*	*K2*	*CO1*
		OR			
	b) (i)	Explain different phases of Secure Software Development Life Cycle (SDLC).	*6*	*K2*	*CO1*
	(ii)	Summarize in detail about scrum model with a neat diagram.	*5*	*K2*	*CO1*
24.	a)	Demonstrate about the different types of injection vulnerabilities: SQL, XSS, and CSRF with examples and neat diagrams.	*11*	*K2*	*CO2*
		OR			
	b)	Interpret common mistakes in file handling that lead to vulnerabilities. How can they be prevented?	*11*	*K2*	*CO2*
25.	a)	Summarize the Role-Based Access Control (RBAC) with examples from enterprise systems.	*11*	*K2*	*CO3*
		OR			
	b)	Infer the principle of least privilege and its importance in reducing attack surfaces.	*11*	*K2*	*CO3*
26.	a)	Identify how CSRF tokens work in securing online banking applications?	*11*	*K3*	*CO4*
		OR			
	b)	Apply suitable coding practices to prevent XSS in modern web applications.	*11*	*K3*	*CO4*
27.	a)	Outline the process of code review and its importance in secure software development.	*11*	*K2*	*CO5*
		OR			
	b)	Explain the role of DevOps in modern software development and the need for security integration.	*11*	*K2*	*CO5*
28.	a)	Apply penetration testing techniques to evaluate application security.	*11*	*K3*	*CO6*
		OR			
	b)	Develop how CI/CD pipelines can be included in automated vulnerability scanning?	*11*	*K3*	*CO6*