Reg. No.																

Question Paper Code	13622

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Fifth Semester

Computer Science and 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. State the purpose of a code review in secure coding *1 K1 CO1*
   (a) To identify bugs and potential security issues
   (b) To reduce code length
   (c) To improve the application’s visual appearance
   (d) To improve the user interface
2. Show the acronym XSS stand for in web security *1 K1 CO1*
   (a) Cross-Script System (b) Cross-Site Scripting
   (c) Cross-Script Style (d) Cross-Site Security
3. To protect against Insecure Deserialization attacks, you should __________. *1 K1 CO2*
   (a) Disable all serialization mechanisms (b) Validate deserialized objects
   (c) Use plain text for serialization (d) Avoid using SSL for deserialized data
4. Which of the following best describes a man-in-the-middle (MITM) attack? *1 K1 CO2*
   (a) A type of attack where the attacker directly modifies the server
   (b) An attacker secretly relays and possibly alters communication between two parties
   (c) An attacker gains control of a machine via a backdoor
   (d) A phishing attack targeting financial information
5. OAuth 2.0 is a protocol used for ______. *1 K1 CO3*
   (a) Authentication only (b) Authorization only
   (c) Both authentication and authorization (d) Token-based encryption
6. Which of the following ensures that a user’s session ends after a period of inactivity? *1 K1 CO3*
   (a) Token revocation (b) Session timeout (c) MFA (d) CAPTCHA
7. What is the primary function of a session cookie? *1 K1 CO4*
   (a) To store user credentials securely
   (b) To remember user actions across multiple requests
   (c) To track user activity on the server
   (d) To encrypt user data
8. What is the purpose of a session identifier? *1 K1 CO4*
   (a) To track user preferences (b) To uniquely identify a user's session
   (c) To store user credentials (d) To log user activity
9. What is the function of the SameSite cookie attribute? *1 K1 CO5*
   (a) To restrict cookie access to same-origin requests (b) To encrypt cookie data
   (c) To make cookies accessible via JavaScript (d) To store user preferences
10. Quote the acronym "OWASP" stand for *1 K1 CO6*
    (a) Open Web Application Security Protocol
    (b) Open Web Application Security Project
    (c) Online Web Application Security Project
    (d) Open Worldwide Application Security Program

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11. Explain the concept of data encryption at rest and in transit. *2 K1 CO1*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

12. Explain threat modeling in the context of secure coding. *2 K1 CO1*

13. Define buffer overflow. *2 K2 CO2*

14. Why is input validation important in secure coding? *2 K2 CO2*

15. Differentiate between authentication and authorization. *2 K2 CO3*

16. Define Role-Based Access Control (RBAC)? *2 K2 CO3*

17. Discuss about session hijacking attack. *2 K2 CO4*

18. State the important to use HTTPS for session management. *2 K1 CO4*

19. Identify the significance of using parameterized queries in database interactions. *2 K2 CO5*

20. Mention the purpose of using HTTPS in web applications. *2 K1 CO5*

21. Explain the purpose of a Web Application Firewall (WAF). *2 K2 CO6*

22. Define Dynamic Application Security Testing (DAST). *2 K2 CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23. a) Define Cross-Site Scripting (XSS) and explain how it can be prevented. *11 K2 CO1*

OR

b) Explain the principle of "Least Privilege" and its role in secure coding. *11 K2 CO1*

24. a) Explain in detail about input validation and sanitation. *11 K2 CO2*

OR

b) Explain in detail about types of vulnerabilities with suitable examples. *11 K2 CO2*

25. a) Describe the difference between Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). *11 K2 CO3*

OR

b) Explain Multi-Factor Authentication (MFA) and its importance. *11 K2 CO3*

26. a) Describe the role of tokens in session management and their advantages over traditional session IDs. *11 K3 CO4*

OR

b) Illustrate the Cross-Site Request Forgery (CSRF) affect session management, and what measures can be taken to prevent it. *11 K3 CO4*

27. a) Explain the concept of the principle of least privilege and its importance in web applications. *11 K2 CO5*

OR

b) Describe the Cross-Site Request Forgery (CSRF) attacks and how can they is prevented? *11 K2 CO5*

28. a) Explain the Dynamic Application Security Testing (DAST), and how is it different from SAST in secure coding? *11 K3 CO6*

OR

b) Explain the importance of cryptographic key management in secure coding and the potential risks of poor key management practices. *11 K3 CO6*