Reg. No. : | | | | | | | | | | | | |

Question Paper Code:U2206

B.E./B.Tech. DEGREE EXAMINATION, NOV 2025

Professional Elective

21CSV206 - WEB APPLICATION SECURITY

(Régulations 2021)

(Common to CSE,ECE,EEE,MECH,IT,BME,AI&DS,AGRI & CSE(AIML) Engineering branches)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Define Web Application Security.	CO1- U	
2.	Explain Transport Layer Security (TLS).	CO1- U	
3.	What is Microsoft Security Development Lifecycle (SDL)?	CO1- U	
4.	Outline the steps involved in Security Incident Response Planning.	CO1- U	
5.	What is the purpose of session cookies in API security?	CO1- U	
6.	What role does encryption play in securing data transmitted between clients and APIs?	CO1- U	
7.	Name a type of vulnerability assessment tool used for scanning vulnerabilities in cloud environments.	CO1- U	
8.	What is the primary objective of Mobile Application Testing in penetration testing?	CO1- U	
9.	Define Social Engineering and its significance in cyber security.	CO1- U	
10.	How does Comodo contribute to cyber security efforts?	CO1- U	

PART – B (5 x 16= 80 Marks)

11.	(a)	Critically analyze the importance of input validation in web application security, discussing common techniques and best practices for implementing robust input validation mechanisms. Provide examples of vulnerabilities that can be mitigated through effective input validation.	CO2- App	(16)

Or

	(b)	Evaluate the significance of session management in web applications, out lining potential security risks associated with poor session handling practices. Discuss strategies for implementing secure session management mechanisms, including session tokens and session expiration policies.	CO2- App	(16)
12.	(a)	Assess the effectiveness of the Software Assurance Maturity Model (SAMM) in improving software security across different stages of the development lifecycle.	CO2- App	(16)
		Or		
	(b)	Explore the challenges and benefits associated with integrating security into the software development lifecycle through the Microsoft Security Development Lifecycle (SDL). Provide strategies for overcoming barriers to implementation and maximizing its effectiveness.	CO2- App	(16)
13.	(a)	Evaluate the effectiveness of different authentication mechanisms, including API keys and OAuth2, in securing service-to-service APIs. Discuss their strengths, weaknesses, and suitability for various deployment scenarios, considering factors such as scalability, manageability, and security requirements.	CO2- App	(16)
		Or		
	(b)	Compare and contrast token-based authentication with other authentication mechanisms, such as HTTP basic authentication and API keys. Discuss the advantages and disadvantages of each approach in terms of security, scalability, and ease of implementation, and provide recommendations for selecting the most appropriate authentication method based on specific use case requirements.	CO2- App	(16)
14.	(a)	Discuss the role of audit logging and reporting in vulnerability assessment and penetration testing. Explore the importance of documenting findings, vulnerabilities, and remediation efforts, and provide recommendations for effectively communicating assessment results to stakeholders and decision-makers.	CO1- U	(16)
		Or		
	(b)	Discuss the significance of Web Application Testing in penetration testing and its role in identifying security vulnerabilities in web applications and their underlying infrastructure.	CO1- U	(16)

15.	(a)	Discuss the various types of injection attacks, including SQL injection, LDAP injection, and XML injection, and explain how they exploit vulnerabilities in web applications.	CO1- U	(16)
		Or		
	(b)	Discuss the concept of Cross-Site Request Forgery (CSRF) attacks and their potential impact on web application security.	CO1- U	(16)