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

Question Paper Code: U2206S

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.	What is the purpose of a Content Security Policy (CSP)?	CO1- U	
2.	What is the significance of recognizing web application security threats?	CO1- U	
3.	What are the key considerations for effective Security Incident Response Planning?	CO1- U	
4.	Why is security testing crucial in the development of web applications?	CO1- U	
5.	Which authorization framework is commonly used for securing APIs and granting access to resources?	CO1- U	
6.	What is OAuth2?	CO1- U	
7.	What is the Vulnerability Assessment Lifecycle?	CO1- U	
8.	Name a common type of penetration test used to assess the security of external network infrastructure.	CO1- U	
9.	What is Social Engineering in the context of hacking?	CO1- U	
10.	How does Comodo contribute to cyber security efforts?	CO1- U	

PART – B (5 x 16= 80 Marks)

11.	(a)	Discuss the evolution of web application security over the years, highlighting key milestones and challenges faced by developers.	CO1- U	(16)
		Or		
	(b)	Describe the components and processes involved in Secure Socket Layer (SSL) and Transport Layer Security (TLS), elucidating how they ensure secure communication over the internet.	CO1- U	(16)

12.	(a)	Evaluate the strengths and weaknesses of the OWASP Comprehensive Lightweight Application Security Process (CLASP) and its applicability in diverse software development environments. Provide recommendations for overcoming potential limitations.	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)	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)
		Or		
	(b)	Assess the role of audit logging in API security and compliance. Discuss the importance of maintaining detailed audit logs to track API activity, detect security incidents, and demonstrate regulatory compliance, and provide recommendations for designing and implementing effective audit logging mechanisms that meet the requirements of various security standards and regulations.	CO2- App	(16)
14.	(a)	Compare and contrast various types of vulnerability assessment tools, including cloud-based, host-based, network-based, and database-based scanners. Evaluate their strengths, weaknesses, and suitability for different environments and scenarios, considering factors such as scalability, accuracy, and ease of use.	CO1- U	(16)
		Or		
	(b)	Explore the importance of SSID or Wireless Testing in penetration testing and its role in assessing the security of wireless networks and their configurations. Discuss the methodology, tools, and techniques used in SSID or Wireless Testing, and provide recommendations for securing wireless networks against potential threats.	CO1- U	(16)

15.	(a)	Discuss the concept of Cross-Site Request Forgery (CSRF) attacks and their potential impact on web application security. Explore common CSRF attack scenarios, such as CSRF With GET requests, CSRF with POST requests, and CSRF with AJAX requests, and provide recommendations for preventing and mitigating CSRF vulnerabilities.	CO1- U	(16)
		Or		
	(b)	Discuss the risks associated with failure to restrict URL access in web applications and their potential impact on security. Explore common URL access control vulnerabilities, such as predictable resource locations, insecure direct object references(IDOR), and lack of access controls, and provide strategies for mitigating these risks.	CO1- U	(16)