Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, NOV/DEC 2025

Sixth Semester

Computer Science and Engineering

CCS374 - Web Application Security

(Common to Information Technology)

Regulations - 2021

Duration : 3 Hrs *Maximum : 100 Marks*

*PART – A (ANSWER ALL QUESTIONS) (Marks 10*2=20)*

Q.No	*Questions*	*BLT*	*CO*	*Marks*
1.	Compare Authentication and Authorization.	L2	1	2
2.	Why is it essential to update software regularly in the context of web application security?	L2	1	2
3.	Recall the steps involved in Security Incident Response.	L1	2	2
4.	Summarize the benefits of SAMM.	L2	2	2
5.	Infer the measures can be implemented to secure incoming requests in API development.	L2	3	2
6.	What is the role of encryption in API security?	L1	3	2
7.	List the stages involved in the Vulnerability Assessment Lifecycle.	L1	4	2
8.	In penetration testing, what does SSID or Wireless Testing focus on?	L2	4	2
9.	Relate the risk associated with failure to restrict URL access.	L2	5	2
10.	Outline the concept of Cross-Site Request Forgery attacks and their potential consequences.	L2	5	2

*PART – B (ANSWER ALL QUESTIONS) (Marks 5*16 = 80)*

Q.No		*Questions*	*BLT*	*CO*	*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.	L4	1	16
		Or			
	b	Analyze the impact of common web application security threats such as Cross-Site Scripting (XSS), SQL Injection, and Cross-Site Request Forgery (CSRF) on the security posture of web applications. Propose mitigation strategies to address these threats effectively.	L4	1	16
12.	a	Outline the key components of a comprehensive Security Incident Response Plan (SIRP), detailing the steps involved in incident detection, analysis, containment, eradication, recovery, and post- incident review.	L2	2	16
		Or			
	b	Explain how OWASP CLASP addresses the security concerns of web applications and enhances the overall security posture of an organization. Illustrate its implementation process and key considerations for successful adoption.	L2	2	16

13.	a	Analyze the effectiveness of different authentication mechanisms, including API keys and OAuth2, in securing service-to-service APIs.	L4	3	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.	L4	3	16
14.	a	Explain 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.	L2	4	16
		Or			
	b	Explain the Vulnerability Assessment Lifecycle in detail, outlining each stage's significance and activities involved. Provide examples of tools and techniques commonly used in each stage to effectively identify, remediate, and verify vulnerabilities within an organization's infrastructure.	L2	4	16
15.	a	Analyze the various types of injection attacks, including SQL injection, LDAP injection, and XML injection, and explain how they exploit vulnerabilities in web applications.	L4	5	16
		Or			
	b	Analyze the strengths and weakness of OpenVAS and Burp Suite.	L4	5	16