Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

B.E/B.TECH DEGREE END SEMESTER THEORY EXAMINATIONS, APRIL-MAY 2025

Sixth Semester

Artificial Intelligence and Data Science

CCS374 - Web Application Security

(Common to Information technology and Computer Science and Engineering)

Regulations – 2021

Duration : 3 Hrs ***Maximum: 100 Marks***

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

Q.No	*Questions*	*BLT*	*CO*	*Marks*
1.	Differentiate Authentication and Authorization.	L2	1	2
2.	How does Cross-Site Request Forgery (CSRF) work?	L2	1	2
3.	Why is security testing crucial in the development of web applications?	L2	2	2
4.	Outline the steps involved in Security Incident Response Planning.	L1	2	2
5.	Interpret the purpose of API keys in securing service-to-service APIs.	L2	3	2
6.	Define the concept of token-based authentication in API security.	L1	3	2
7.	List the stages involved in the Vulnerability Assessment Lifecycle.	L1	4	2
8.	What is the need for penetration testing?	L1	4	2
9.	Define Social Engineering and its significance in cybersecurity.	L1	5	2
10.	How do broken authentication and session management vulnerabilities compromise the security of web applications?	L2	5	2

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

Q.No		*Questions*	*BLT*	*CO*	*Marks*
11.	a	Explain the various authentication mechanisms commonly employed in web applications, along with their strengths and weaknesses. Compare and contrast session-based and token-based authentication methods.	L2	1	16
		Or			
	b	Illustrate 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.	L2	1	16
12.	a	Discover the challenges and benefits associated with integrating security into the software development life cycle through the Microsoft Security Development Lifecycle (SDL). Provide strategies	L4	2	16

		for overcoming barriers to implementation and maximizing its effectiveness.			
		Or			
	b	Critically analyze the Software Assurance Maturity Model (SAMM) as a framework for improving software security practices. Assess its scalability, flexibility, and adaptability to different organizational contexts, along with its potential impact on risk management and compliance efforts.	L4	2	16
13.	a	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.	L2	3	16
		Or			
	b	Extend the challenges and benefits of securing microservice APIs using a service mesh architecture. Discuss how service mesh technologies facilitate secure communication, traffic management, and observability in distributed microservice environments, and assess their impact on overall system reliability and security posture.	L2	3	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.	L5	4	16
		Or			
	b	Evaluate the effectiveness of External Testing as a penetration testing technique for assessing the security of an organization's external network infrastructure. Discuss the methodology, tools, and best practices involved in conducting External Testing, and provide recommendations for addressing common challenges and limitations.	L5	4	16
15.	a	Given your understanding of Cross-Site Request Forgery (CSRF), consider a web application scenario where a user is authenticated in an online banking system. Demonstrate how an attacker might exploit CSRF vulnerabilities using GET, POST, or AJAX requests to initiate unauthorized transactions. Based on your analysis, apply best practices to design and implement appropriate CSRF prevention mechanisms to secure the application.	L4	5	16
		Or			
	b	Identify the role of penetration testing tools such as Burp Suite in identifying security vulnerabilities and weaknesses in web applications. Discuss the features and functionalities of Burp Suite, including its proxy, scanner, and intruder modules, and provide	L4	5	16

recommendations for leveraging its capabilities to conduct comprehensive penetration tests effectively.