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

Question Paper Code: U2206

B.E./B.Tech. DEGREE EXAMINATION, NOV 2024

Professional Elective

21CSV206 - WEB APPLICATION SECURITY

(Régulations 2021)

(Common to All Questions)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

1.	What is the purpose of a Content Security Policy (CSP)?	CO1 U
2.	Name four common web application security threat.	CO1 U
3.	What is Microsoft Security Development Life cycle (SDL)?	CO1 U
4.	How does Microsoft SDL contribute to secure software development?	CO1 U
5.	How are incoming requests secured in API development?	CO1 U
6.	What measures can be implemented to secure incoming requests in API development?	CO1 U
7.	Name a common type of penetration test used to assess the security of external network infrastructure.	CO1 U
8.	What is the primary objective of Mobile Application Testing in penetration testing?	CO1 U
9.	What vulnerability does Cross-Site Scripting (XSS) exploit?	CO1 U
10.	What vulnerability is exploited w hen sensitive data is stored in an insecure manner?	CO1 U

PART – B (5 x 16= 80 Marks)

11.	(a)	Discuss the evolution of web application security over the years, high lighting key milestones and challenges faced by developers.	CO1 - U	(16)
		Or		
	(b)	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.	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) Assess the effectiveness of the Software Assurance Maturity Model (SAMM) in improving software security across different stages of the development lifecycle. Discuss its impact on organizationalsecuritypracticesanditsalignmentwithindustrystandardsandbe stpractices. 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) Explore the challenges and benefits of securing micro service APIs using a service mesh architecture. Discuss how service mesh technologies facilitate secure communication, traffic management, and observability in distributed micro service environments, and assess their impact on overall system reliability and security posture. CO2 - App (16)

14. (a) 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. CO2 - App (16)

Or

(b) Analyze the challenges and considerations involved in conducting Internal Penetration Testing to assess the security of an organization's internal network infrastructure. Discuss the methodology, scope, and limitations of Internal Penetration Testing, and provide strategies for overcoming common obstacles and ensuring comprehensive coverage. CO2 - App (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. Evaluate the severity of injection attacks in terms of potential damage and provide recommendations for mitigating these risks. CO1 - U (16)

Or

(b) 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)