KUMARAGURU
college of technology
character is life

Register Number:…………….

MCA DEGREE EXAMINATIONS: NOV/DEC 2024

(Regulation 2020)

Third Semester

MASTER OF COMPUTER APPLICATIONS

P20CAE0232**:** Secure Software Development

COURSE OUTCOMES

CO1: Demonstrate various vulnerabilities related to memory attacks.

CO2: Apply security principles in software development.

CO3: Evaluate the extent of risks.

CO4: Apply security principles in the testing phase of software development.

CO5: Use tools for securing software.

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 2 = 20 Marks)

1. Define common software vulnerabilities that threaten security. CO1 $[K_2]$
2. Differentiate between threat, vulnerability, and risk. CO1 $[K_2]$
3. Describe the potential risks associated with executing untrusted content in software systems. CO2 $[K_2]$
4. Explain the process of session hijacking in the context of secure software design. CO2 $[K_2]$
5. Describe the purpose of risk assessment in the life cycle. CO3 $[K_2]$
6. Explain the role of asset identification in the risk profiling process. CO3 $[K_2]$
7. Identify the key components of a risk-based testing strategy. CO4 $[K_2]$
8. List the typical goals of post-exploitation activities. CO4 $[K_1]$
9. Define governance in the context of secure project management. CO5 $[K_1]$
10. Explain the significance of monitoring and reporting in security governance. CO5 $[K_2]$

Answer all the Questions:-

PART B (6 x 5 = 30 Marks)

11. Apply encryption methods to secure sensitive data during transmission and at rest. 5 CO1 $[K_3]$

12.	Utilize runtime analysis tools to identify and mitigate vulnerabilities related to stack and heap memory.	5	CO1	[K_3]
13.	Identify the key steps in the SQUARE process.	5	CO2	[K_3]
14.	Apply risk evaluation techniques to assess the impact of a potential data breach on an organization's reputation and finances.	5	CO3	[K_3]
15.	Apply common web application exploitation techniques to identify vulnerabilities in a sample web application.	5	CO4	[K_3]
16.	Develop a set of security policies derived from an enterprise software security framework, explaining how each policy supports project goals and risk management.	5	CO5	[K_3]

Answer any FIVE Questions

PART C (5 x 10 = 50 Marks)

17.	Demonstrate how to configure a firewall to protect against common network-based attacks.	10	CO1	[K_3]
18.	Compare buffer overflow and code injection vulnerabilities in terms of their exploitation techniques and effects.	10	CO2	[K_3]
19.	Implement a continuous monitoring process for threats and vulnerabilities in an organization's infrastructure, detailing the tools and methodologies used.	10	CO3	[K_3]
20.	Develop a quantitative risk assessment model for an organization's critical assets, including the calculations used to determine risk levels.	10	CO3	[K_3]
21.	Apply the steps of the penetration testing process to evaluate a corporate network’s security posture, detailing the tools used in each phase.	10	CO4	[K_3]
22.	Illustrate the integration of security metrics into project performance reporting, explaining how these metrics reflect the maturity of security practices.	10	CO5	[K_3]

****