Register Number:……..

B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC 2024

(Regulation 2018)

Seventh Semester

INFORMATION SCIENCE AND ENGINEERING

U18ISE0012: Software Security

COURSE OUTCOMES

CO1: Understand the need for software security by survey of current vulnerabilities and attacks.

CO2: Differentiate between traditional and secure software requirements and design.

CO3: Understand secure coding best practices and methods of analyzing.

CO4: Understand the importance of security testing and how it impacts the quality of software.

CO5: Understand the importance of secure installation, deployment and manage security incidents.

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

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1.	Define confidentiality, integrity, and availability in the context of software security.	CO1	[K_2]
2.	Explain the difference between authentication and authorization in software security.	CO1	[K_2]
3.	Identify two common software vulnerabilities and give an example of each.	CO1	[K_2]
4.	What is the purpose of input validation in software security? Provide an example.	CO2	[K_2]
5.	Briefly analyze how threat modeling contributes to secure software design	CO2	[K_4]
6.	List two secure coding best practices and explain their importance.	CO3	[K_2]
7.	What is the role of security testing in quality assurance?	CO4	[K_2]
8.	Describe penetration testing and its purpose in security testing.	CO4	[K_2]
9.	What is configuration management in the context of secure software deployment?	CO5	[K_2]
10.	Explain the concept of vulnerability tracking in software maintenance.	CO5	[K_2]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.	a)	Describe the types of low-level security attacks and explain one in detail.	8	CO1	[K_2]
	b)	Discuss memory safety mechanisms and their role in defending against low-level attacks.	8	CO1	[K_2]

12.	a)	Differentiate between functional and operational security requirements in software design.	8	CO2	[K_4]
	b)	Explain the principle of "defense in depth" and provide an example of how it can be applied in software security.	8	CO2	[K_3]
13.	a)	Identify the main differences between declarative and imperative security in secure coding.	8	CO3	[K_2]
	b)	Explain static analysis as a method for secure code analysis and its advantages in software security.	8	CO3	[K_2]
14.	a)	Outline the different types of testing (functional, non-functional, security testing) and describe how each contributes to software security.	8	CO4	[K_2]
	b)	Discuss the importance of bug tracking and attack surface validation in security testing.	8	CO4	[K_2]
15.	a)	Describe the process of secure installation and deployment, focusing on configuration management and elevated privileges.	8	CO5	[K_2]
	b)	Explain the role of audits and metrics in the operations and maintenance phase of software deployment.	8	CO5	[K_2]
16.		Case Scenario: A small e-commerce website has a login form that directly inserts user input into an SQL query without validation. An attacker tries to enter the following into the username field: ' OR '1'='1' – a. Analyze the security vulnerability in this scenario, explaining how an attacker could exploit it. b. Propose two secure design practices that could prevent this type of attack and briefly explain their effectiveness.	16	CO2	[K_4]

****