Register Number:……………..

KUMARAGURU
college of technology
character is life

B.TECH DEGREE EXAMINATIONS: APRIL / MAY 2023

(Regulation 2018)

Seventh Semester

INFORMATION TECHNOLOGY

U18ITE0005: Web Application Security

COURSE OUTCOMES

CO1: Explain the architecture web application architecture
CO2: Demonstrate Core Defence Mechanisms
CO3: Explain the authenticated attacking mechanism
CO4: Explain various process of attacking user
CO5: Design attacking mechanism for Native Software Vulnerabilities

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

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

1. What is cross site request forgery? CO1 [K_2]
2. Differentiate Reject Known Bad and Accept Known Good. CO1 [K_2]
3. What is MS-SQL? CO2 [K_2]
4. What is HTTP parametrized injection? CO2 [K_2]
5. What is bypassing filters? CO3 [K_2]
6. What is Opaque data? Give an example. CO3 [K_2]
7. Differentiate Stack overflow and Heap overflow. CO4 [K_2]
8. Write a short note about WebDAV methods. CO4 [K_2]
9. What is OS Command injection? CO5 [K_2]
10. What is XPath injection? CO5 [K_2]

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

11. With an example list out the security measures CO1 [K_2]

1. Maintaining Audit Logs 8
2. Alerting administrators 8

that has been implemented to handle the Handling Attackers.

12.	What is insecure access control methods? How are the access control decisions made by the requested parameters? Explain the process and approaches in detail.	16	CO2	[K_2]
13.	A multistage login mechanism first requests the user’s username and then various other items across successive stages. If any supplied item is invalid, the user is immediately returned to the first stage. In this stage how the vulnerability can be identified and corrected. Explain the processing in detail using the multistage login mechanism.	16	CO2	[K_3]
14.	Explain the following terms in detail:		CO3	[K_2]
	1. E mail Header manipulation.	8		
	2. SMTP Command injection.	8		
15.	With a neat diagram explain the steps involved in the DOM based XSS attacks.	16	CO4	[K_2]
16.	List any two categories of common vulnerabilities that often have easily recognizable signatures within source code.	16	CO5	[K_2]

****