K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June : 2025-2026
(B. Tech.) Program: Computer Engineering Scheme: III
Regular: TY Semester: V
Course Code: CEDLC5043 and Course Name: web security
Date of Exam: 28/11/2025 Duration: 02.5 Hours Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

Q. No.	Question	Max. Marks	CO	BT level
Q 1	Solve any **two** questions out of three: (05 marks each)	10		
a)	Explain how a social engineering attack works and demonstrate its execution with an example scenario.		CO2	Ap
b)	Apply vulnerability assessment and penetration testing (VAPT) methodology to identify weaknesses in an organization.		CO3	Ap
c)	Define ethical hacking and discuss the importance of understanding enemy tactics.		CO1	U
Q 2	Solve any **two** questions out of three: (05 marks each)	10		
a)	Demonstrate the process of conducting a physical penetration test and suggest defenses against it.		CO4	Ap
b)	Explain insider attacks and describe how organizations can defend against them.		CO6	U
c)	Apply Metasploit to perform a client-side exploit and describe the steps involved.		CO5	Ap
Q.3	Solve any **two** questions out of three. (10 marks each)	20		
a)	Plan and execute a full penetration test, including structure, execution, reporting, and information sharing.		CO6	Ap
b)	Explain buffer overflow attacks in Linux with stack operations and exploit development steps.		CO2	U

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June : 2025-2026
(B. Tech.) Program: Computer Engineering Scheme: III
Regular: TY Semester: V
Course Code: CEDLC5043 and Course Name: web security
Date of Exam: 28/11/2025 Duration: 02.5 Hours Max. Marks: 60

c)	Apply Windows exploit development concepts (SEH, memory protections) to craft a basic exploit scenario.		CO6	Ap
Q.4	Solve any **two** questions out of three. (10 marks each)	20		
a)	Analyze SQL Injection and Cross-Site Scripting (XSS) vulnerabilities in web applications and propose mitigation strategies.		CO3	An
b)	Apply client-side browser exploitation concepts to demonstrate how a heap spray attack is executed.		CO5	Ap
c)	Explain the OWASP Mobile Top 10 and discuss common mobile security vulnerabilities with examples.		CO4	U

****