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

May-June 2024
(B.Tech)Program: Computer Engineering(Honors) Scheme I
Regular Examination: LY Semester: VIII
Course Code: HCSC801 and Course Name: Application Security
Date of Exam: 24/5/2024 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.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight:	12		
i)	Explain the types of cross site scripting attack?	2	CO1	U
ii)	Describe two techniques for testing API's and web services	2	CO5	U
iii)	Differentiate between Authentication and Authorization.	2	CO3	U
iv)	Outline some key application security activities that should be part of SSDLC.	2	CO4	AP
v)	Explain the significance of input validation in web security.	2	CO2	U
vi)	Determine the methods for improving application security and its impact on the overall quality and reliability of software products.	2	CO6	AP
vii)	Compare and Contrast between design flaw and a security bug in software development.	2	CO4	U
viii)	Explain the importance of dynamic web application profiling in testing.	2	CO5	U
Q.2	Solve any four questions out of six.	16		
i)	Describe the integration of security practices within the various stages of the software development lifecycle.	4	CO4	U
ii)	Determine the methodology for identifying weak points in the architecture of web application during reconnaissance.	4	CO1	AP

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

May-June 2024 I
(B.Tech)Program: Computer Engineering(Honors) Scheme
Regular Examination: LY Semester: VIII
Course Code: HCSC801 and Course Name: Application Security Security
Date of Exam: Duration: 02.5 Hours Max. Marks: 60

iii)	Describe the concept of integration testing and discuss why it is crucial for ensuring the reliability of complex software systems.	4	CO5	U
iv)	Explain the key objectives of threat modeling and how it helps improve the overall security of an application.	4	CO6	U
v)	Illustrate the various methods for defending against injection attacks such as SQL injection and NoSQL injection.	4	CO2	AP
vi)	Explain the importance of encryption in ensuring security requirements for web applications. Provide example.	4	CO3	U
Q.3	Solve any two questions out of three.	16		
i)	Describe the role of configuration management tools in infrastructure testing and deployment, highlighting their benefits in maintaining consistency and reliability.	8	CO5	U
ii)	Analyze the challenges associated with implementing security measures in agile software development environments.	8	CO4	U
iii)	Explain API analysis in web application reconnaissance. How can analyzing APIs help in understanding the overall security of web application .Provide real world example to support your answer	8	CO1	U
Q.4	Solve any two questions out of three.	16		
i)	Discuss the role of security headers in enhancing the protection of web applications against various attacks, give example of commonly used security header and explain how they mitigate specific security threats	8	CO3	U
ii)	Compare and contrast various existing threat modeling approaches in terms of their effectiveness and applicability.	8	CO6	U
iii)	Interpret on the measures implemented to safeguard against DDOS (Distributed denial of Service) attacks in the context of modern web application security.	8	CO2	U

****