REG.NO.:

VIT

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: D1+TD1

Programme Name & Branch	: B.Tech. CSE - IS
Course Code and Course Name	: BCSE320L - Web Application Security
Faculty Name(s)	: Dr.Arulkumar V, Dr.Natarajan P
Class Number(s)	: VL2024250101451 / VL2024250101449
Date of Examination	: 16-10-2024
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level
- Course Outcomes
  - CO3: Learn the web application hacking techniques and prevention solutions.
  - CO4: Apply the best practices of Secure Credentials, session management, and Security Automation in web applications.

Q. No	Question	M	CO	BL

1.	You are sending an application to a foreign university for a Master's program. Your recommender has submitted their recommendation, but you have not received any information for three months about whether you have been selected. When you checked online, you found a feedback page where you can leave a comment. You are providing your comment in the following format:
	
	`I applied for the MS in Computer Science at your esteemed university.`
	`I submitted my application on 22-6-2024.`
	`My application number is 58923 and my name is "xxxxxxx".`
	`<strong> But I have not received any information from you for the last three months. </strong>`
	`I am requesting you to send a reply as soon as possible.`
	
	Identify the type of attack. Identify the vulnerability of this attack. Does it affect your machine or the foreign university's machine? Explain this attack with a suitable diagram.
		10	3	3

2.	You submit a data-filling form to a target server that is not accessible to the creator of the form, but it is accessible to you, the submitter. Identify the type of attack you are attempting. Explain the identified attack with a suitable example.	10	3	4
3.	Which attack could potentially give us write permissions to critical files in addition to read permissions? Explain it with a suitable example.	10	3	4

REG.NO.:

VIT

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: D1+TD1

4.	Consider the regular expression `/^((nnm)*)+$/`. The user is allowed to provide the regular expression as input. The user gives the following input pattern. (a) nnmnnmnnmnnmnnm (b) nnmnnmnnmnnmnnmnnm (c) nnmnnmnnmnnmnnmnnmnnmh (d) nnmnnmnnmnnmnnmnnmnnmnnmnnm Check the above four user inputs and determine which are valid and which are not. Provide reasons for your answers. What will the regular expression parser do with the above inputs? Estimate the time taken to validate the inputs. Identify the type of attack this could be used in. How would an attacker exploit this attack?	10	3	5
5.	Our VIT management has decided to create a network between the four campuses and conduct the placement test simultaneously using VITplaceApp. No one should be able to copy or exchange any questions or answers on the web application. Assume that you are responsible for writing the application code. You need to write the application code in a fully secure manner without any vulnerabilities. Describe the various techniques you will use to write the web app to ensure it is secure and error-free.	10	4	4