REG.NO.:21BCI0046

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
WINTER SEMESTER 2024-2025

SLOT: A2 + TA2

Programme Name & Branch	: B.Tech. CSE & CSE with Information Security
Course Code and Course Name	: BCSE320L Web Application Security
Faculty Name(s)	: Dr. P.Natarajan
Class Number(s)	: VL2024250501659
Date of Examination	: 16-3-2025
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)
  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.	Assume that you are the database in charge for the web application software. Without knowing to you, your friend had stored some malicious code on the database. When the database accessed and the data is retrieved from the database by the user, the malicious code is run on the data retrieved user machine. This is not happened for him only, many more users who all are retrieved the data they had the same experience. As a database in charge you are in the position to identify the type of attack. Describe the attack with suitable diagram and state in which way it is dangerous. How will you rectify it or avoid like this attack?	10	3	4
2.	You are planning to get money from the unknown persons account as a hacker. You are going to target the person who has the highest chance of being logged in and having correct amount of fund? How can you hit as many people with this in a short period of time before it is detected? Note that in this attack you are not going to request money from the account holder, on behalf of you some other person is going to request. Identify the attack which you have to exploit? Give the step by step approach how you are going to attack and get the money to your account?	10	3	3
3.	Due to lack of sanitization an API endpoint is provided with additional unexpected command when it is called by a command-line interface (CLI). Provided unexpected commands are executed against the CLI. Identify the type of attack and explain the attack with suitable examples.	10	3	5
4.	You are using the VIT University web server. Your VIT University web server resources are drained by your competitors. As a result you are experiencing the performance degradation or loss of service.	10	3	4

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

REG.NO.:

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

SLOT: A2 + TA2

	Identify the type of attack. List out in which all are the way this attack can be performed. How will you overcome from this attack? Illustrate the attack with suitable example.			
5.	Assume that you are working in a web application programming organization. In your organization you are assigned to develop and check the Engineering College web application program. At the time of development you had evaluated the security before writing the code in the architecture level. You had also evaluated the security during the development process. Identify the next step which you have to do. Explicate the identified step in terms of Discovery, Analysis, Management, Testing and Mitigation.	10	4	5

****