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

REG.NO.: 23BCE2093

SLOT: B2+TB2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2025-2026

Programme Name & Branch	:BCE, BCI
Course Code and Course Name	:BCSE320L and Web Application Security
Faculty Name(s)	:Ms.S.Anu Roopa Devi
Class Number(s)	: VL2025260506140
Date of Examination	:16.03.2026, 09:30AM – 11:00AM
Exam Duration	: 90 minutes Maximum Marks: 50

General instruction(s):

- Answer All Questions
- Course Outcomes
  1. Understand security challenges and the need for Authentication and Authorization in web based systems and applications.
  2. Familiarize the Application Programming Interface analysis and vulnerability management of securing a web-based system.
  3. Learn the web application hacking techniques and prevention solutions.
  4. Apply the best practices of Secure Credentials, session management, and Security Automation in web applications
  5. Develop the best strategies to prevent XSS, CSRF, XXE, Injection, DOS attacks and securing third party dependencies.

Q. No	Question	M	CO	BL
1.	During a class project, Olivia clicks a link sent by her classmate David, which takes her to a webpage displaying a message. The message contains a script that steals her session cookies. What type of XSS occurs when malicious code is delivered to the user in an HTTP response, often through a URL parameter or a form, without being stored permanently on the server? Explain what type of XSS is this with flowchart.	10	3	3
2.	In 2007, a 7-Eleven breach occurred: a group of attackers exploited an injection vulnerability to compromise the payment systems of several companies, including the 7-Eleven retail chain. This breach led to the theft of over 130 million credit card numbers. The attack was one of the largest data breaches of its time, demonstrating the immense financial. Identify the type of vulnerability and explain with flow chart	10	4	3
3.	a) The web server's CPU suddenly hits 100%, but network traffic is low. Logs show a single 50-character validation request for a "Promo Code" is hanging for 30 seconds. The code uses the regex ^([a-zA-Z]+)*$. What specific type of DoS attack is this? Explain briefly.	5	4	3
	b) Your "Network Utility" web page allows users to enter an IP to ping. An attacker submits 8.8.8.8 ; cat /etc/passwd. The server executes the ping, then displays your internal system files. Network traffic remains low, but sensitive data is leaked. Identify and explain the web attack with preventive measure.	5		
4.	a) An application's XML parser is configured to resolve external entities. An attacker uploads an XML file containing a system reference to file:///etc/passwd. The application processes the file and displays the server's local password file in the response. Identify the attack and explain it with a flowchart.	5	4	3
	b) A user visits a malicious site while logged into a web application. The malicious site triggers an unauthorized POST request to the application using the user's active session cookies. The application performs a sensitive action	5		

VIT

Vellore Institute of Technology

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

REG.NO.: 23BCE2093

SLOT: B2+TB2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - II

WINTER SEMESTER 2025-2026

	because it cannot distinguish between an intentional and a forged request. From the scenario, identify the web attack and explain briefly.			
5.	You are a security researcher who has just discovered a "Zero-Day" vulnerability in a widely used enterprise VPN software. You want to report this flaw so that it can be publicly tracked across all security tools, firewalls, and vulnerability scanners worldwide using a unique, standardized identifier. Explain the findings to be indexed in which global database?	10	4	3

****