REG.NO.: 23BCE2043

SLOT: B2+TB2

# VIT
Vellore Institute of Technology

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
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 | :28.01.2026, 14:00PM – 15:30PM |
| Exam Duration | : 90 minutes Maximum Marks: 50 |

**General instruction(s):**

- 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 | Module | Marks | CO | BL |
|---|---|---|---|---|---|
| 1. | Identify the types of brute force attack for the real world scenario and explain .<br>(i) A local bakery has an old employee Wi-Fi router that only accepts a 6-digit PIN for access. There are no security measures to block repeated attempts. If an attacker uses a script to systematically try every number from 000000 to 999999, what type of attack are they performing?<br>(ii) An attacker wants to break into a specific user's email account. Instead of trying random strings of letters, they load a text file containing 100,000 of the most commonly used English words and names into their hacking tool. Why is this more effective than a simple brute-force attack, and what is this method called? | 2 | 10 | 2 | 1 |
| 2. | How will the front-end fetch, filter, and display available hotels and room details (like price, amenities) from the back-end's JSON-based API , and how will booking requests with user/room/date data be structured in JSON for the API to handle real-time availability checks and create a reservation record? | 1 | 10 | 1 | 1 |
| 3. | a) Sarah is a Project Manager who uses the Gmail or Outlook app on her smartphone. She has "Swipe Actions" enabled, where swiping right on an email automatically archives it. For this real world scenario identify the attack and describe. | 2 | 5 | 2 | 1 |

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

REG.NO.:

SLOT: B2+TB2

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

| | | | | | |
|---|---|---|---|---|---|
| | b) Marcus just started a new job as a Senior Accountant at a mid-sized tech firm. To celebrate, he updates his LinkedIn profile and posts a photo on Instagram of his new office desk, which includes a "Welcome" balloon and a branded company mug. Two hours later, Marcus receives a text message or a DM:<br>"Hey Marcus! Welcome to the team! I'm Sarah from HR. Loved your desk photo—that mug is a classic. I noticed your onboarding paperwork is missing one digital signature for your first paycheck. Can you quickly verify it here so we don't miss the Friday cutoff? [Malicious Link]". Identify the attack and provide a solution. | 2 | 5 | | |
| 4. | a) Stage 1: In a professional web application like a corporate news portal, the security process begins with an identity check at the login screen, where a user provides credentials like a password or a Single Sign-On (SSO) token to prove they are a legitimate employee. This initial stage is focused entirely on the question, "Is this person who they claim to be?" and once verified, the system allows them entry into the platform.<br>Stage 2: Once the user is inside, the system shifts to an access control phase to determine their specific boundaries based on their assigned role.<br>For this scenario identify which stage is authentication and which stage is authorization. Distinguish them. | 1 | 5 | 1 | 1 |
| | b) Describe about Browser DOM with real world example. | 1 | 5 | | |
| 5. | Imagine an online bookstore called "BookCloud." It allows users to search for books, leave reviews, manage their profiles, and purchase items. However, the developers rushed the launch and missed several security checks. Discuss in detail about the different types of security checks. | 3 | 10 | 3 | 1 |

**********