**Birla Institute of Technology & Science, Pilani**

**Work Integrated Learning Programmes Division**

**First Semester 2024-2025**

**Mid-Semester Test**

**(EC-2 Regular)**

Course No. : SS ZG566

Course Title : Secure Software Engineering

Nature of Exam : Open Book

Weightage : 25%

No. of Pages = 1

# No. of Questions = 5

Duration : 2 Hours

Date of Exam : 21/09/2024 (EN)

Note to Students:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. Provide brief response (in 50 words) [2X6 = 12 Marks]
   1. How does CIA triad apply to a telecom service provider?
   2. How does taint analysis help uncover vulnerabilities?
   3. What is a malware? What is meant by zombie in context of malware?
   4. Why is software security considered an asymmetric problem?
   5. Differentiate interpretation of non-repudiation in contexts of security and privacy.
   6. Differentiate an entry in NIST CVE from MITRE CWE.
5. You are security consultant for a modern hospital, which has significant automated operations. Perform Threat Modelling with necessary artifacts, and propose recommendations for them. [4 Marks]

1. How does CMU SQUARE process differ from OWASP SAMM and Microsoft SDL w.r.t. Requirements Engineering? Explain (in 100 words). [3 Marks]
2. What are Secure Implementation Patterns? How do they enhance software quality? Explain with examples (in 100 words). [3 Marks]
3. You are a Security Professional. Your client, who is building an Information System, needs to choose between penetration and fuzz testing (choose only one). Prepare a questionnaire (with at least 3 questions) to the client to enable you to make recommendation. Justify the questionnaire. [3 Marks]

\*\*\*\*\*\*\*\*\*\*\*