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

**Work Integrated Learning Programmes Division**

**First Semester 2022-2023**

**Mid-Semester Test**

**(EC-2 Regular)**

Course No. : SE ZG566

Course Title : Secure Software Engineering

Nature of Exam : Open Book

Weightage : 30%

No. of Pages = 1

# No. of Questions = 4

Duration : 2 Hours

Date of Exam : 24/09/2022 (EVENING)

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. What is the risk of depending on Open-Source components?
   2. What are considerations in choosing a Software Composition Analysis tool?
   3. Differentiate Firewall from SWG(Secure Web Gateway).
   4. How does CIA triad apply to an eCommerce company?
   5. What is a malware? How do bots differ from viruses?
   6. Differentiate an entry in CVE from CWE.
5. What do you understand by Software Supply Chain? Why should Security Professional be concerned with supply chain? Provide point-wise exemplified response. [4 Marks]
6. Why do we use DFD for threat modeling? Draw a DFD to represent modern bank’s operations highlighting trust boundaries. List attack surface of the bank, briefly describing each part of the attack surface. [8 Marks]
7. Answer the following: [2 + 2 + 2 = 6 Marks]
   1. Differentiate attack resistance and attack resilience.
   2. List approaches to software architecture for enhancing security.
   3. How are attack resistance/resilience impacted by approaches listed above?

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