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

**Work Integrated Learning Programmes Division**

**First Semester 2024-2025**

**Comprehensive Examination**

**(EC-3 Regular)**

Course No. : SS ZG566

Course Title : Secure Software Engineering

Nature of Exam : Open Book

Weightage : 45%

No. of Pages = 2

# No. of Questions = 8

Duration : 2 Hours 30 Minutes

Date of Exam : 30/11/2024 (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 answers (within 100 words): [5 X 2 = 10]
   1. What are the concerns with penetrate-and-patch approach?
   2. What is meant by zero trust? Does it offer attack resistance or attack resilience?
   3. Differentiate temporal and spatial memory safety with help of examples.
   4. What are relative strengths of symmetric and asymmetric encryption?
   5. Do you think NoSQL databases are more secure than SQL databases?
5. Do you think security testing has to be performed manually or can we automate it? [5 Marks]
6. List significant aspects of the attack surface of a Web Application. [5 Marks]
7. Briefly explain process memory organization for Unix or Windows machine. Identify parts of process memory that can potentially be exploited by an attacker. Justify your answer. [5 Marks]

1. Compare security concerns in Python with that of C language. [5 Marks]
2. List concerns, if any, with the program given below. Justify. [5 Marks]

#include <stdio.h>

#include <string.h>

void welcome\_func(char \*name)

{

char buf[30];

strcpy(buf, name);

printf("Welcome %s\n", buf);

}

int main(int argc, char \*argv[])

{

welcome\_func(argv[1]);

return 0;

}

1. An ecommerce site stores product details in an RDBMS. It allows user to enter product group, captures into a variable named prodGroup and lists name and manufacturer (both are of type varchar) for the available products in the product group. They generate the SQL statement by appending prodGroup to the string “SELECT name, manufacturer FROM Products WHERE group =”. Further prodGroup is validated for absence of special characters.
   1. Do you notice any flaws/weaknesses in the software design? What can we do about it?
   2. Is it possible for an attacker to obtain usernames and passwords stored in another table Users by crafting input for the product group? [5 Marks]
2. You are the CISO (Chief Information Security Officer) of an organization. List the events (in software environment) that you would like to be alerted promptly. Provide a brief justification for each event. [5 Marks]

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