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

**Work Integrated Learning Programmes Division**

**First Semester 2022-2023**

**Comprehensive Examination**

**(EC-3 Regular)**

Course No. : SE ZG566

Course Title : Secure Software Engineering

Nature of Exam : Open Book

Weightage : 50%

No. of Pages = 2

# No. of Questions = 9

Duration : 2 Hours

Date of Exam : 26/11/2022 (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 crisp responses (in 100 words) [2X6 = 12 Marks]
   1. Does the pesticide paradox apply to security testing?
   2. Briefly explain the Java security architecture.
   3. Do you think NoSQL databases are more secure than SQL databases?
   4. What are relative strengths of symmetric and asymmetric encryption?
   5. What are the challenges in finding a good dataset to develop a robust IDS?
   6. How will you estimate the cost of a breach?
5. List features of a penetration testing tool with help of an example. Do you recommend a development team member to carry out penetration testing? [4 Marks]
6. How does SQUARE augment conventional requirements engineering? [4 Marks]
7. List significant components of the attack surface of a Web Application. [5 marks]
8. List concerns, if any, with the program segment given below. [5 marks]

#include <stdio.h>

#include <string.h>

void hello\_func(char \*name)

{

char buf[20];

strcpy(buf, name);

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

}

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

{

hello\_func(argv[1]);

return 0;

}

1. List concerns, if any, with the program segment given below. [5 marks]

int concatStrs(char \*buf1, char \*buf2, unsigned len1, unsigned len2)

{

char tempBuf[256];

if ((len1 + len2) > 256)

return FAILURE;

memcpy(tempBuf, buf1, len1);

memcpy(tempBuf + len1, buf2, len2);

processStr(tempBuf);

return SUCCESS;

}

1. You are the Security expert for an ecommerce provider. They maintain their data in an RDBMS. They plan to offer self-service feature for product queries. Customers can search for products using a variety of criteria. The software assembles appropriate SQL query, executes it, and shows results to customers. Prepare a set of guidelines for developers building the functionality based on your knowledge of software vulnerabilities. [5 marks]
2. You are a product development organization which needs to regularly release patches for your customers distributed across the globe. List (and justify) the steps taken by you to ensure that your customers receive genuine software.   [5 marks]
3. 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]

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