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

**Work Integrated Learning Programmes Division**

**Second Semester 2021-2022**

**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 30 Minutes

Date of Exam : 20/05/2022 (FN)

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) [2X5 = 10 Marks]
   1. Differentiate security testing from functional testing.
   2. What is the importance of Secure Logger implementation pattern?
   3. Why an attacker may choose Arc Injection?
   4. Differentiate Symmetric and Asymmetric Encryption.
   5. Differentiate anomaly detection and signature detection approaches to detect intrusions.
5. A news headline says “Suspected Chinese APT Group Targets Power Grid in Northern India”. Elaborate the statement using your knowledge of Threat Modelling. [5 marks]
6. Compare security concerns of cloud-resident software system with that of a system based in office premises. [5 Marks]
7. Compare Security concerns in C/C++, Java, and Python programming languages. [5 Marks]

1. Do you see any concerns with the code segment given below? [5 Marks]

Function makeNewUserDir(username) {

if invalidUsername(username) {

print('Usernames cannot contain invalid characters')

return False

}

raisePrivileges()

int flag = mkdir('/home/' + username)

if (!flag)

printf("Directory created\n");

else {

printf("Unable to create directory\n");

exit(1);

}

lowerPrivileges()

return True

}

1. Find vulnerabilities, if any, in the code snippet given below: [5 Marks]

int main(int argc, char \*argv[])  
{  
char user\_input[100];  
... ...   
scanf("%s", user\_input);   
printf(user\_input);   
return 0;  
}

1. A state agency maintains taxpayers’ data. The data includes demographic information (age, gender, education, income, race, etc.) of taxpayers. The agency would like to help researchers understand income distribution. At the same time, they are bound by the citizens’ privacy rights on their financial records. Prepare a set of rules that should govern access to the data. [5 Marks]
2. You are appointing one of your colleagues as CISO (Chief Information Security Officer) for your organization. Prepare an assignment letter with responsibilities (at least 10) and a brief explanation of each one. [5 Marks]
3. Provide crisp answers to the following: [2+3 Marks]
4. Differentiate Threat, Vulnerability, and Risk with help of examples.
5. Differentiate Technical, Operational, and Management controls for IT Security with help of examples.

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