HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under Section 2(f) of UGC Act, 1956

Term Evaluation (Odd) Semester Examination September 2025

Roll no.............................

Name of the Course: B.Tech CSE
Semester: V
Name of the Paper: Computer System Security
Paper Code: TCS-597
Time: 1.5 hour **Maximum Marks: 50**

Note:

(i) Answer all the questions by choosing any one of the sub-questions
(ii) Each question carries 10 marks.

Q1. (10 Marks)

a. What is fuzzing, and how is it used in security testing? Provide examples of how fuzzing has been effective in discovering vulnerabilities. CO1

OR

b. Compare static, concolic, and dynamic analysis as techniques for detecting security vulnerabilities in software. What are the advantages and disadvantages of each approach? CO1

Q2. (10 Marks)

a. Define integer overflow in the context of software security. Provide an example of how integer overflow can lead to a security vulnerability. CO1

OR

b. What are the primary goals of system security? Discuss the importance of confidentiality, integrity, and availability in securing systems. CO1

Q3. (10 Marks)

a. Explain the concept of the return-to-libc attack. How does it differ from traditional buffer overflow attacks, and what defenses can be implemented to prevent it? CO2

OR

b. What is Race condition? Also provide an programming example of race condition vulnerability. CO2

Q4. (10 Marks)

a. Write a short note on:
 i) Heartbleed attack
 ii) Shellshock attack CO2

OR

b. Demonstrate a Buffer Overflow vulnerability using C/Cpp Program. CO2

Q5. (10 Marks)

a. How can %x and %n format specifiers be used by attackers? Provide a programming example. CO2

OR

b. Differentiate between stack overflow and heap overflow vulnerabilities. CO2