Air University
Department of Cyber Security
(Mid-Term Examination: Spring 2025)

Student ID: ....

Subjective Part

Subject: Secure Software Design & Development
Class: BS-Cyber Security
Code: CY-256
Section: A & B
FM Name: Ms. Maryam Malik
FM Signature: ....

Total Marks: 35
Time Allowed: _1hr 40 min_______
Date:
Max Duration: 2 Hours

HoD Signature: ....

Instructions:

- You are required to attempt **ALL Questions.**
- This is a closed book/notes exam.
- **Return question paper with the answer sheet**

Q. No	Questions	CLO	Marks
2	a) Define Attack Surface and list the three types of attack surfaces with examples. **(3 Marks)** b) How does the Principle of Open Design improve security? **(3 Marks)** c) Why is Complete Mediation necessary for access control? **(3 Marks)** d) A web application allows users to reset passwords by answering security questions. Attackers guess common answers (e.g., "What is your pet's name?"). Which OWASP risk is being exploited? **(3 Marks)** e) Differentiate between Secure Functional Requirements and Non-Secure Functional Requirements with examples. **(3 Marks)**	2	15
3	a) A large e-commerce company is facing an increasing number of cyber threats, including phishing attacks, data breaches, and DDoS attacks. The company's management wants to improve its cybersecurity posture using the **NIST CSF**. Based on the CSF Core Functions, discuss how the company should approach this problem. **(5 Marks)** **b) A malicious actor intends to take over a user's social media account. Develop an attack tree** illustrating different attack strategies. Also, define different cut sets and discuss the parameters used to choose the best path. (Draw a table). **(5 Marks)** **c) A university's online student portal allows students, faculty, and administrators to perform various actions. Students can log in, view grades, enroll in courses, and update personal information. Faculty can**	3	20

	upload grades and send announcements, while administrators manage user accounts. The system consists of a web interface, an authentication system, a database server, and an email notification system for password resets and course updates. **(10 Marks)** I. Draw a Level 1 Data Flow Diagram (DFD) representing the system's data flow. II. Identify security threat using **STRIDE** model and For each threat, Vulnerable component and Mitigation strategy		

*********************End of Paper *********************