Air University
(Mid-Term Examination: Spring 2025)

Subject: **Secure Software Design And Development Lab**
Course Code: **CY-256L**
Class: **BS-CYS**
Semester: **VI**
Section: **A/B**
HoD Signatures:_____

Total Marks: **50**
Date:
Time:
Duration: **1 Hours**
FM Name: Mahaz Khan
FM Signatures:_____

Note:

- **All questions must be attempted.**
- **This examination carries 15% weight towards the final grade.**
- **Close book and Internet.**
- **Submit Docx file(.docx) .**

	Q. No. 1 (CLO 1)	30 Marks
A	**E-Commerce Data Breach** **Background:** ShopMaster is a popular e-commerce platform that enables users to shop for various products online, track their orders, and make secure payments through integrated payment gateways. Customers create accounts, add items to their cart, and complete transactions using secure payment methods. To improve user experience, the platform stores users' payment information and order history for faster checkouts in future purchases. **Challenge:** A hacker exploited a vulnerability in ShopMaster's payment gateway integration, gaining unauthorized access to users' payment details, including credit card numbers, billing addresses, and transaction history. This data was used for fraudulent purchases, and customers were unaware of the breach until it was reported by several victims. The breach not only led to financial losses but also severely damaged the platform's reputation, raising concerns about its security measures. **Features:** 1. **User Registration and Login:** Customers create accounts, log in, and manage personal information. 2. **Shopping Cart:** Users can add and remove items, proceed to checkout, and make payments. 3. **Payment Gateway Integration:** Secure payment options such as credit cards and digital wallets. 4. **Order Tracking:** Customers can track their orders from purchase to delivery. 5. **Security Measures:** SSL encryption for secure transactions and data protection. 6. **Transaction History:** Platform stores payment information for future use, increasing convenience for customers.	15

Instructions:
Your task is to create a **misuse case diagram** to model potential misuse scenarios related to ShopMaster's e-commerce platform. Focus on unauthorized access to user payment details, fraudulent transactions, and exploitation of vulnerabilities in the payment gateway. Highlight possible attacks like SQL injection, session hijacking, man-in-the-middle attacks, and improper data handling.

5.

B

ATM Withdrawal Process

Background:
Automated Teller Machines (ATMs) are essential banking services that allow customers to access their bank accounts without needing to visit a branch. The ATM withdrawal process needs to be user-friendly, secure, and efficient to provide quick access to cash, check balances, and offer other banking services while maintaining high levels of security.

Challenge:
Designing an ATM withdrawal process that balances security, user convenience, and operational efficiency. The challenge is ensuring that the ATM system verifies the user's identity securely (through PIN authentication), handles transaction requests (like withdrawals), and manages state transitions like insufficient funds, invalid PIN entries, and other errors without compromising the user experience.

Features:

1. **Card Insertion:**
   - **Description:** The ATM starts a session when the user inserts their card into the machine. The card is read to verify account information and initiate communication with the bank's server.
   - **Details:** The system checks if the card is valid, active, and not expired. If invalid, the ATM prompts the user to reinsert the card.
2. **PIN Authentication:**
   - **Description:** Users enter their Personal Identification Number (PIN) to authenticate their identity and access their account.
   - **Details:** The ATM system checks if the entered PIN matches the one stored in the bank's database. After multiple failed attempts, the ATM locks the user out or asks for revalidation.
3. **Account Verification:**
   - **Description:** The ATM system verifies if the user's account is active and has sufficient balance to process the requested withdrawal.
   - **Details:** The system communicates with the bank's database to check for sufficient funds and account status (active or frozen). If sufficient funds are available, the ATM proceeds; otherwise, it prompts an error message.
4. **Transaction Selection:**
   - **Description:** After PIN authentication, the user can select the type of transaction they wish to perform, such as withdrawal, balance inquiry, or transfer.
   - **Details:** The system presents the user with options and records the selected transaction type. For withdrawal, the user is prompted to select an amount.

Cash Dispensing:

- **Description:** After the withdrawal amount is confirmed, the ATM dispenses the requested cash.
- **Details:** The machine checks its cash dispenser for the requested denominations and ensures the correct amount is provided. It also ensures that the user collects the cash before the session ends.

6. **Error Handling:**
   - **Description:** The system detects errors like insufficient funds, invalid PIN, or incorrect transaction requests and displays appropriate error messages.
   - **Details:** Error messages may include "Insufficient Funds," "Invalid PIN," or "Machine Out of Service." In cases like invalid PINs, the ATM may lock the card after a certain number of failed attempts.
7. **Session Timeout:**
   - **Description:** The ATM session automatically ends after a certain period of inactivity to protect against unauthorized access.
   - **Details:** The system logs the user out and returns to the Idle state if the user does not interact with the ATM within a predefined time (e.g., 30 seconds).

Your task is to create a State Chart Diagram that models the behavior of an ATM withdrawal process. Consider states like idle, card insertion, authentication, transaction type selection, funds availability check, cash dispensing, and session end. Include transitions based on user inputs, successful transactions, and error handling for incorrect PIN, insufficient funds, and system malfunctions.

	Q. No. 2 (CLO 2)	20 Marks
1	**Unauthorized Access to Company Database** A tech company stores sensitive customer information, including credit card details and personal identification numbers (PINs), in a cloud-based database. The database is accessed by employees through an internal application, which uses basic authentication methods. Recently, external hackers have attempted to access the system, targeting weaknesses in the company's cloud infrastructure and the internal application's security. **Instructions:** • Assume the attacker targets the cloud infrastructure or internal application to gain access to sensitive customer data. • **Draw an attack tree** where the goal of the attacker is to gain access to the **investment plan document** stored in the company's database. • The attack tree should include at least three levels (including the root) and use **both "AND"** and **"OR"** nodes.	20