Air University

Department of Cyber Security

(Final-Term Examination: Spring 2025)

Student ID: _____

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

Total Marks: 100
Time Allowed: _3hr_____
Date:
Max Duration: 3 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
1		2	30

a) A user submits the following comment:

Nice post %3Cscript%3Ealert(1)%3C/script%3E

The developer only validates against raw characters like < and > but doesn't decode inputs before validation. Will this attack be detected? Why or why not? What secure coding principle is being violated?

b) You are asked to deploy a multi-container application using Docker Compose. List the main components required in a docker-compose.yml file.

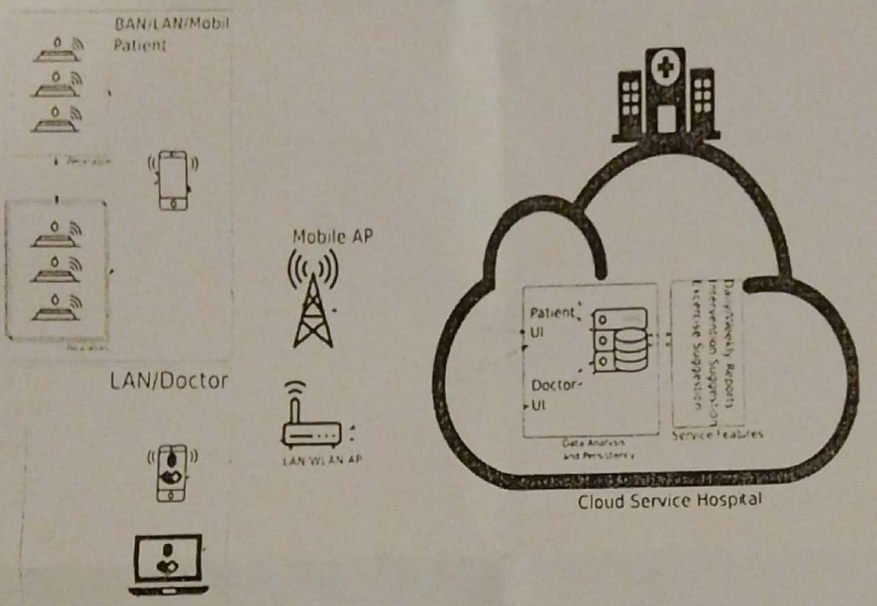
c) Explain why not specifying a character set, such as UTF-8, in a web application could lead to security vulnerabilities. Describe a potential attack scenario where an attacker could exploit this oversight to introduce an XSS attack.

d) A developer pushes code directly to the production branch on GitHub. As a DevOps engineer, what measures would you take to prevent this?

e) Explain the concept of Infrastructure as Code (IaC). What tool would you use for IaC?

f) Describe the difference between a **virtual machine** and a **container**.

2	Mobile Health (mHealth) is on the rise and it is likely to reduce costs and improve the quality of healthcare. It tightly intersects with the Internet of Things (IoT) and comes with special challenges in terms of interoperability and security. We need to focus on security challenges and offers a mitigation solution especially with a focus on authentication and encryption for resource constrained devices. We need to identify assets in a prototyped mHealth ecosystem and classifies threats with the STRIDE methodology. Furthermore, identifies associated risk levels using DREAD and possible mitigation strategies to provide a reasonable trustworthy environment. Terminology – Body Area Network(BAN)	3	30



a) Provide the connection between STRIDE and mHealth Security Perspective, address all STRIDE threat categories? **[10 marks]**

b) Draw possible EDFD in an mHealth environment (scenario given above), covering sensors controller, smartphone application, mHealth platform, storage, doctor/physician app and any AI model attached with application? **[10 marks].**

c) Complete threat modeling tables for "Authentication" threats of the above system? **[10 marks].**

Description	STRIDE	DREAD
Patient identity sharing or loss		
Personal Identity sharing or loss		
Patient and personal identity theft		
Sensor spoofing		
Smartphone spoofing		

3

a) **With reference to the OWASP secure coding guidelines "All validation failures should result in input rejection" answer the following questions: [15 marks]**

Consider the following code:

```
import re

def reject_invalid_input(data):
 if not re.match("^[a-zA-Z0-9_]+$", data):
    return {"error": "Invalid input"}, 400
 return {"message": "Input is valid"}, 200

input_data = "invalid_data!"
response = reject_invalid_input(input_data)
print(response)
```

I. Explain how the principle of "All validation failures should result in input rejection" is demonstrated in this code. Identify potential security risks if this principle is not enforced. What could go wrong if invalid inputs are not rejected?

II. Refactor the above code to centralize the validation process. This should ensure that all inputs across the application are validated through a single, centralized routine, minimizing the risk of missed validations or inconsistent error handling.

III. Implement additional validation to handle other input types, such as email addresses or passwords, ensuring that different inputs are validated securely while maintaining a centralized validation function.

b) **Review the following code, Identify the security and suggest how to fix it. Rewrite code to fix.(15 marks)**

I.

```
import mysql.connector

conn = mysql.connector.connect(
  host="localhost",
  user="admin",
  password="my_db_password",
  database="student_db"
)
```

II.

```
def save_upload(file_name, content):
  path = "/uploads/" + file_name
  with open(path, "wb") as f:
   f.write(content)
```

III.

```
def compress_file(name):
  command = f"zip backup.zip {name}"
  run_command(command)

def run_command(cmd):
  import os
```

4 40

os.system(cmd)

c) **Analyze the scenario and answer the questions below.(10 marks)**

I. Your organization has discovered a recent attack where attackers used file upload to execute a malicious script.
Based on secure file management practices, what precautions could have prevented this attack?

II. A web application logs all user activity, including session identifiers and partial password data, for debugging purposes. Identify and explain at least three security issues with this logging approach and suggest corrective actions.

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