Nada mohamed abd elsatar

2205173

Note: I was unable to upload the database or the entire project folder to GitHub directly.

1. Introduction

This report outlines the steps taken to complete the Information Security Management task, which involved designing a database, developing a RESTful API, and implementing authentication and CRUD operations. The project was developed using PHP, MySQL (phpMyAdmin), and JWT authentication.

2. Database Design

A database named security_mgmt was created using phpMyAdmin. Two tables were designed:

Users Table

id (Primary Key, Auto-increment)

name (String, Required)

username (String, Unique, Required)

password (Hashed, Required)

Products Table

pid (Primary Key, Auto-increment)

pname (String, Required)

description (Text)

price (Decimal, Required)

stock (Integer, Required)

created_at (Timestamp, Default Current Time)

3. API Development

A RESTful API was developed with the following functionalities:

Authentication

Implemented JWT-based authentication.

Created a SignUp endpoint to register users.

Implemented a Login endpoint that generates a JWT token valid for 10 minutes.

Secured protected routes by requiring a valid token.

User Operations

POST /signup → Registers a new user.

POST /login → Authenticates user and returns JWT token.

PUT /users/{id} → Updates user details (Only authorized users with valid tokens).

Product Operations (Require JWT Token)

POST /products → Adds a new product.

GET /products → Retrieves all products.

GET /products/{pid} → Retrieves a single product by ID.

PUT /products/{pid} → Updates product details.

DELETE /products/{pid} → Deletes a product.

4. Security Measures

Password Hashing: User passwords are securely hashed before storing.

JWT Middleware: Implemented middleware to validate JWT tokens before accessing protected routes.

Environment Variables: Used environment variables for storing sensitive data such as database credentials and JWT secret keys.