



STRATHMORE UNIVERSITY
SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
Master of Science in Information Systems Security
Final Examination

MST 8104: SOFTWARE LABORATORY EXPERIENCE I

DATE: 27th April 2026

TIME: 2 ¼ hours

Instructions: Answer question one and any other two questions

The owner of a **Precision Tool & Equipment Rental Hub** requires you to develop software to facilitate the administration of the hub's daily operations.

The basic requirements specifications for the system to be developed include:

- **Borrowing and Returning:** The ability for **Contractors** (Patrons) and **Inventory Managers** (Librarians) to check out and check in specialized machinery and power tools.
- **Restocking:** A module for adding new inventory and replacing retired equipment.
- **Payment of Fines:** A system to calculate and process late fees or damage penalties incurred by the contractors.

Answer the following questions based on this write-up.

Question 1 (20 Marks)

- a) Write code to illustrate any inheritance scenario for such a software.
(3 Marks)
- b) Illustrate any form of Polymorphism that can result from this problem and state why it could enhance software security.
(3 Marks)
- c) From a security perspective, clearly describe two reasons why exception control would be mandatory for your program.
(4 Marks)
- d) An Inventory Manager receives an email that looks like it is from the Hub Owner, asking for the administrative password to "check the weekend's revenue."
 - i. What specific type of social engineering attack is this? **(2 Marks)**
 - ii. List one technical and one non-technical (procedural) defense against this.
(2 Marks)
- e) The system has two primary user roles: Contractors (who rent tools) and

Inventory Managers (who manage the database).

- i. Define the Principle of Least Privilege (PoLP). **(1 Mark)**
 - ii. How should PoLP be applied to a Contractor's access levels regarding the "Fines" and "Inventory Restocking" tables? **(2 Marks)**
- f) Describe any three types of software security threats that you need to address in developing the hub's software. **(3 Marks)**

Question 2 (15 Marks)

- a) With regards to computer security, describe two reasons why you would recommend using a Java framework for the development of the hub's software. **(4 Marks)**
- b) With regards to computer security, describe two reasons against the usage of frameworks for the development of the hub's software. **(4 Marks)**
- c) Explain any two ways that a loop (iteration) can be a concern in computer security. **(4 Marks)**
- d) Describe any three ways that you can validate input that is coming from a source. **(3 Marks)**

Question 3 (15 Marks)

- a) In your own words, describe the relationship between code complexity and security. **(4 Marks)**
- b) When a contractor signs up, the system asks for their "Job Site Address."
 - i. Define the difference between Validation and Sanitization. **(2 Marks)**
 - ii. Give an example of a "Sanitization" step for a text field to prevent a Cross-Site Scripting (XSS) attack. **(2 Marks)**
- c) An Inventory Manager wants to search for a contractor by their ID. The backend code is written as follows: query = "SELECT * FROM contractors WHERE id = " + user_input + ";"
 - i. Explain why this code is vulnerable if a user enters ' OR '1'='1 as their ID. **(2 Marks)**
 - ii. Rewrite or describe the secure alternative to this method. **(2 Marks)**

- d) In a nutshell, arrays can be used to implement buffers. Describe how this can be a problem and how it can be addressed. **(3 Marks)**

Question 4 (15 Marks)

- a) Assuming that during maintenance you notice that the hub's software has a backdoor, describe two potential problems that this may pose. **(4 Marks)**
- b) While reviewing the source code for the "Inventory Restocking" module, you find the following line:
`db_connect(user="admin", pass="YellowHammer2026!")`
- i. Why is "Hardcoding" credentials a severe security risk? **(2 Marks)**
 - ii. What is the industry-standard alternative for managing sensitive keys and passwords in a production environment? **(2 Marks)**
- c) An Iterator can be used to traverse a collection. Provide any possible alternative to an iterator. Support your response with an illustration. **(3 Marks)**
- d) Describe how a queue can be implemented using an array. **(4 Marks)**