# CS 305 Module Two Written Assignment Template

## Instructions

Replace the bracketed text with the relevant information in your own words. If you choose to include images or supporting materials, make certain to insert them in all the relevant locations in the document.

## Areas of Security

The key areas of security that need consideration for this assessment are:

* **Authentication and Authorization:** Ensuring that users are properly authenticated and have the appropriate permissions to access various parts of the application.
* **Data Encryption:** Protecting sensitive data by encrypting it in transit and at rest, safeguarding it from unauthorized access.
* **Input Validation:** Validating all incoming data to prevent security vulnerabilities such as injection attacks.

## Areas of Security Justification

The choice of these areas for security assessment is justified as follows:

* **Authentication and Authorization:** Authentication ensures that only legitimate users gain access to the system, and authorization defines what actions each user can perform. This is essential for controlling access to sensitive data and functionalities.
* **Data Encryption:** Encryption is crucial to protect data confidentiality and integrity, especially when data is transmitted over networks or stored on servers. It prevents data breaches and leaks.
* **Input Validation:** Input validation is vital to prevent attacks like SQL injection, XSS (Cross-Site Scripting), and other security vulnerabilities that arise from unvalidated user inputs. It ensures data integrity and security.

## Code Review Summary

During the code review process, the following issues were identified:

* **Outdated Dependencies (POM.xml):** The project is currently using an outdated version (2.6.5.RELEASE) of the **spring-data-rest-webmvc** library. This version may not include the latest security enhancements and bug fixes.

## Mitigation Plan

To address the identified issue and enhance the security of the application, the following mitigation plan will be implemented:

* **Update Dependencies:**
  + In the "POM.xml" file, update the version of the **spring-data-rest-webmvc** dependency to the latest stable version compatible with the project. This ensures that the application benefits from the latest security patches and improvements.

By executing this mitigation measure, we aim to bolster the security and reliability of the application, diminishing the risk associated with outdated library dependencies.