# 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 areas of security that are relevant to assess are Input Validation, APIs, client/server, coding errors, code quality, and encapsulation.

## Areas of Security Justification

* Input Validation
  + Any application that takes input from users is vulnerable to attack. Users can use holes in input validation to gain access to tools and information they are not authorized to view. For this reason, we must validate and secure any input from users.
* APIs
  + APIs, or Application Programming Interfaces allow software components to communicate with each other. Care must be taken that any APIs are not vulnerable to excessive data exposure, broken authentication, or unrestricted resource consumption, among other vulnerabilities.
* Client/Server
  + Client server vulnerabilities may exist when server-side infrastructure allows attackers to gain access to or compromise the system. These vulnerabilities may include command injection, SQL injection, unvalidated redirects and forwards, or security misconfiguration.
* Coding errors/code quality
  + Errors or flaws in code can be exploited by attackers to gain access to the system.
* Encapsulation
  + Improperly encapsulated programs could give end users access to areas of the program that they are not authorized to view. Encapsulation, or hiding the inner workings of the code from end users protects the system from unauthorized requests.

## Code Review Summary

* Outdated version of Spring rest webmvc
  + The version of the Spring framework dependency specified in pom.xml lines 40-42, (spring-data-rest-webmvc 2.6.5.RELEASE) is outdated. As outdated versions of software are no longer maintained, this can lead to security vulnerabilities, compatibility issues, and performance issues.
* Raw data needs validation
  + On line 27 of GreetingController.java, raw data from the parser is put directly into a string value. This could pose a risk where an attacker could create unauthorized, or excessively long strings that could lead to vulnerabilities in our system.

## Mitigation Plan

Recommendations:

* Use most up to date version of Spring framework. As of writing this, the most up to date version is 4.29.0.
* Implementation of input verification, including length of string.