# CS 305 Module Two Code Review and Mitigation Plan Assignment

## Instructions

Replace the bracketed text with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Areas of Security

* Input Validation
  + Since the team has been tasked with creating an input function for the application, implementing input validation methods is an absolute must in order to ensure the security of user entries. It is also important that the team takes into account how to properly handle accidental mis-inputs versus attempted attacks.
* APIs
  + The Spring Framework relies on many APIs in order to function properly. The team has been instructed to use Version 2.6.5 of the spring-data-rest-webmvc API, so it is essential that this resource is validated and that safe and secure practices be followed with all APIs in the Spring Framework.
* Client/Server
  + Since this is going to be a web-based application, ensuring that all data sent and received by both the client and server is secured from attacks is vital. This will help to keep the system safer from injection or interception based attacks.
* Code Quality
  + As with any project, following best coding practices is very important for maximizing both the quality and security of the final system. While building this system we will be using the Spring Expression Language so it is essential that the team adjusts accordingly and follows all proper conventions.

## Code Review Summary

* One vulnerability of this system is its use of Version 2.6.5 of the spring-data-rest-webmvc API. This is a very outdated version of the API and having outdated dependencies like this will likely cause the system to be more susceptible to attacks.
* As is the case with the spring-data-rest-webmvc dependency, the version of Spring Boot that is being used is outdated. This could cause vulnerabilities in the expressive command input function as it utilizes this dependency.
* Another vulnerability in this code is that in the Greeting.java file, the constructor and accessor methods for the

## Mitigation Plan

* The first step in the mitigation plan for the vulnerabilities in this software would be to update the outdated dependencies. The newest versions of both spring-data-rest-webmvc and Spring Boot should be implemented into the system.
* Best practices regarding encapsulation and code error must be followed in order to ensure code quality. Also, extra attention should be paid to proper use of the Spring Expression Language.
* We must address the issue in this java application of the public constructor and accessor methods. These methods must be made private in order to protect them from being exploited by outside attacks.