# CS 305 Module Two Written Assignment

## Areas of Security

Based on the provided scenario, the areas of security I feel should be looked at most are input validation, APIs, and code quality to ensure that major security concerns are addressed.

## Areas of Security Justification

**Input Validation –** Input validation is very important to address as validating inputs from the user can ensure that any areas where an injection attack could happen are safe. This helps provide some defense to the outside in of the application making sure that input from the user is valid.

**Application Programming Interfaces (APIs) –** APIs should be addressed as it will be crucial that any data to and from related APIs that will be working with the spring framework such as the REST API are not introducing any new vulnerabilities into the system from the inside.

**Code Quality –** Code quality should also be looked at very tightly during the development of the application and future development as making sure that all developers are following best practices, this helps to ensure known vulnerabilities of the practices used are the only thing that would need to be addressed versus introducing more vulnerabilities by using other practices.

## Code Review Summary

When looking at the code base, some areas to note that should be addressed are that in the pom.xml file, the version being used of the spring-data-rest-webmvc in Spring Framework is an older version, notably 2.6.5, whereas the latest version is 4.1.5 ([spring-data-rest-webmvc](https://mvnrepository.com/artifact/org.springframework.data/spring-data-rest-webmvc)). Also noted is that in the GreetingController.java file, when sending a parameter request, the value is hard-coded for the value. Also in the same file, an @PathVariable parameter is used to get an id value but for each of these, no input validation is used to prevent injection attacks.

## Mitigation Plan

For these findings, it is recommended in the pom.xml file that an updated version of spring-data-rest-webmvc for the Spring Framework be used as newer versions could have fixes for vulnerabilities that are unbeknownst to us. In the GreetingController.java file, a proper parameter request should be used to get the specified value as well as using proper input validation for this parameter request as well as the @PathVariable parameter used thereafter to ensure that inputs can not be used to inject special commands that could infiltrate the system.