# 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

* The areas of security relevant to the current project are Input Validation, Code Error, and Code Quality.
* I chose Input Validation due to the project focusing around user inputs and to ensure that malicious commands can not be used. Code Error was chosen in correspondence to Input Validation to deal with incorrect or blocked inputs, as well as ensuring that error codes and program crashes are dealt with properly. Since the application is a web app, error codes can be used to gain information about the application that could be used for malicious purposes.. Code Quality compliments the previous two by helping ensure each of the areas of security are dealt with correctly. Code Quality also helps to ensure known CVE’s are taken into account and that bugs, small and large are patched.

## Code Review Summary

* I started by taking a look at the POM to inspect what versions are being used. Springframework boot should be updated to 2.6.7, per their GItHub latest release. Spring Data REST WebMVC could also be updated, however I was unable to determine which of the recent updates was considered stable and not alpha or beta.
* One other potential issue is that the values used within the code such as “myArray” and “name” are public. Modifiable variables, unless needed by the end user, should be restricted to private or protected.

## Mitigation Plan

* I would start by updating all the dependencies to the most recent versions, as well as updating any code that may no longer be supported within the Spring Framework and potentially Java.
* I would then adjust the access permissions for variables to ensure that they are only modified by the intended target.