# CS 305 Module Two Written Assignment Template

Winnie Kwong

Southern New Hampshire University

CS-305 Software Security

Professor Foultz

September 9th, 2023

## 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

Based on the Vulnerability Assessment Process Flow Diagram (VAPFD), the security areas most relevant to the scenario are input validation, APIs, and Code Quality.

## Areas of Security Justification

Input validation is important because it helps to prevent bad actors from entering and harming the system, damaging data, and mitigating the risk of cross-site scripting (XSS) or SQL injection attacks. In this case, the input validation would ensure data matches and returns what is needed. Application programming interface (API) is essential because it helps to prevent attacks by using the backend framework to protect sensitive data as it is transferred. Without API, there would not be a connection between the code and Spring Framework. Lastly, code quality determines the overall quality of the software. Without the code quality, the comprehensive system would lack a safe, secure, and reliable codebase that would hinder the consistency of handling bugs and complexity.

## Code Review Summary

Looking over Version 2.6.5 of the spring-data-rest-webmvc in Spring Framework, there are a few signals that should not be overlooked. The first concern is that the current version of the latest Spring Framework is 6.0.11. Having a difference between versions is a big concern because the latest version would have more security updates that have fixed possible bugs and security holes as well as other improved features and speed enhancements for the back-end developer.

## Mitigation Plan

For best practices, potential techniques to resolve these problems is to update to the most current version as well as setting a limitation on the length of strings that are acceptable. When updating software to its latest version, issues from previous versions are addressed and improves the overall functionality and efficiency of the software. Furthermore, having the latest version protects means less time for cybercriminals to exploit security or find vulnerabilities within the system when comparing to other software that has been on the market without change.