# 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

Relevant areas of security that are applicable for a software application, in my opinion, are input validation, API, cryptography, client/server, code error, and code quality.

## Areas of Security Justification

Input Validation: Since we are taking user commands (like text inputs), strict checks are needed to block hackers from injecting malicious codes.

API: We can validate the inputs at the API level. It may be necessary to implement a RESTful API if our command input function needs to be accessible outside of our system, such as by front end.

Cryptography: If the app stores passwords or secrets, weak encryption = stolen data. Even if not now, better safe than sorry.

Client / Server: Data travels over the internet (HTTP). Unsecured requests will easily let attackers spy on or alter user commands.

Code Error: If the app crashes when parsing input, hackers might see stack traces, which are roadmaps to vulnerabilities.

Code Quality: Hard-to-read code = hidden bugs.

## Code Review Summary

Outdated dependencies: we are using an outdated version of spring-data-rest-webmvc, which is still on version 2.6.5. The spring boot dependency also has wavy lines beneath it, which indicates there are vulnerabilities found in this dependency. It could be outdated too.

On line 27-30 of GreetingController.java, User input (name) is directly executed as code (Spring Expression Language). The code parses user input (name) as SpEL expressions, letting attackers run system commands, which can be devastating.

## Mitigation Plan

Update all dependencies to the latest version.

Use whitelist safe characters for user input:  
// Only allow safe characters in input

if (!name.matches("[a-zA-Z0-9\\s]+")) {

throw new InvalidInputException();

}