# 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

* Input Validation
* APIs
* Cryptography
* Client/Server
* Code Error
* Encapsulation

## Areas of Security Justification

* Input Validation – Many of the vulnerabilities were subjected to injection. Validating the input can help prevent SQL injections.
* APIs – Considering that requests and retrievals will be across a network, secure API interactions are a must. A RESTful API would be preferred, working with input validation.
* Cryptography – When working with information moving across a network, it is best to encrypt all information, at least on the client side.
* Client/Server – Since an API will be in use, secure distributed composing must be implemented.
* Code Error – Safety measures in the code should be addressed, as well as a record of code errors to keep track of attempts at denial of services.
* Encapsulation – Secure data structures are a must. If the request needs to access stored data on the server, alterations and deletions must be prohibited.

## Code Review Summary

The product Apache Tomcat seems to have critical vulnerabilities, although many seem to be resolved in an updated version. Another critical vulnerability is with the spring webmvc which has injection issues that could cause infinite loops, denial of service, and exposure of sensitive information to an unauthorized actor. This is also due to a lack of up-to-date versions.

## Mitigation Plan

The first step is to update all available dependencies to the latest versions, if possible. Next would be to introduce input validations for all requests. This should at least secure the inputs and fight against injections, thus limiting the risk of denial of service. Another approach would be to use encryption on sensitive user information which may lower the risk of exposure of sensitive information to an unauthorized user.