# 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

The dependency check and code review identified these critical security areas:

1. **Input Validation** - Confirmed critical risk from unfiltered SpEL expressions.
2. **APIs** - Found 3 high-risk vulnerabilities in spring-data-rest-webmvc.
3. **Cryptography** - No sensitive data encryption detected (added to mitigation plan).
4. **Client/Server** - TLS not enforced (added to mitigations).
5. **Code Error** - Array index bounds errors identified.
6. **Code Quality** - 33 vulnerabilities from outdated dependencies.
7. **Encapsulation** - No direct exposure found (confirmed secure).

## Areas of Security Justification

1. **Input Validation**:
   * *Found*: SpEL injection via parser.parseExpression(name) in GreetingController.
   * *Fix*: Replaced with regex sanitization ([^a-zA-Z0-9 ]).
2. **APIs**:
   * *Found*: CVE-2021-22119 in spring-data-rest-webmvc 2.6.5.
   * *Fix*: Upgraded to 3.7.1 via Spring Boot 2.7.18 parent POM.
3. **Cryptography**:
   * *Action*: Added spring-boot-starter-security for future credential encryption.
4. **Client/Server**:
   * *Action*: Will enforce HTTPS in application.properties.
5. **Code Error**:
   * *Found*: Unchecked array access in /number/{id} endpoint.
   * *Fix*: Added bounds validation (if (id < 0 || id >= myArray.length)).
6. **Code Quality**:
   * *Found*: 11 vulnerable dependencies (33 CVEs total).
   * *Fix*: Upgraded Spring Boot and removed unused libraries.
7. **Encapsulation**:
   * *Confirmed*: Greeting class fields properly encapsulated (private final).

## Code Review Summary

* **Critical Issues Fixed**:
  + SpEL injection removed (was exploitable via name=#{7\*7}).
  + Array index bounds check added (prevented DoS via /number/100).
* **Dependency Upgrades**:
  + Spring Boot: 2.2.4 → 2.7.18 (patched 12 CVEs).
  + spring-data-rest-webmvc: 2.6.5 → 3.7.1.

## Mitigation Plan

**Input Validation** *(Completed)*

* Replaced SpEL evaluation with regex sanitization.
* Added @Size and @Pattern validations to parameters.

**2. API Security** *(Completed)*

* Upgraded spring-data-rest-webmvc to 3.7.1.
* Added @PreAuthorize to endpoints.

**3. Cryptography** *(Pending)*

* Will implement Jasypt for secrets encryption (next sprint).

**4. Error Handling** *(Completed)*

* Added @ControllerAdvice with generic error messages.

**5. CSRF Protection** *(Pending)*

* Requires Spring Security setup (planned for Module 3).

**Priority Order**:

1. Input validation
2. Dependency upgrades
3. Error handling
4. CSRF/cryptography (next phase).

A screenshot of a computer

AI-generated content may be incorrect.