# 

# 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.

While others are against the exposure of computer weakness because they believe the vulnerability will be utilized. Supporters of restricted disclosure believe that restricting information to specific groups minimizes the possibility of exploitation. Vulnerability is a weakness that cybercriminals exploit to gain unauthorized access to computer systems (Joshi et al., 2015). Afterward, the cybercriminals install viruses into the computer system, steal sensitive data, and run malicious codes to harm computer systems. Numerous vulnerabilities influence popular software, leaving many computer users using the software at increased risk of data cracking.

## Areas of Security

* A complex web application that uses the spring framework: is an area where security is needed mostly because here is where the user is exposed; thus, there is a need to implement an expressive command input unction for the application.
* **Input validation:** This happens when an individual wants to log in. due to the implementation of a command input function, we must authenticate all inputs into the function strictly. By doing this, it will influence a safe system and prevent any injection attacks.
* **APIs:** The uses of the system are away and need to access the system in another place; thus, a RESTFUL API needs to be put in place that allows the user to gain access to the function even when one is far from the main system. Due to the vulnerabilities, there is a need to create an API that does not allow unauthorized access into the system. We could use the input validation at the API level.
* **Cryptography:** is also an area of security, and here, there is a need to consider appropriate cryptography is used to protect and encrypt data.
* **Client/server:** The communication period between the server and client can pose a sector of weakness; thus, there is necessary to ensure data safety during the transfer according to the HTTPS requests.
* **Code Error:** During the coding, there can be errors made, thus making the system vulnerable and solving the issue, reviews of all command input functions and any API access layer code.
* **Encapsulation:** Lastly, during encapsulation, we need to ensure appropriate usage and that there is no messing with the designed data structures.

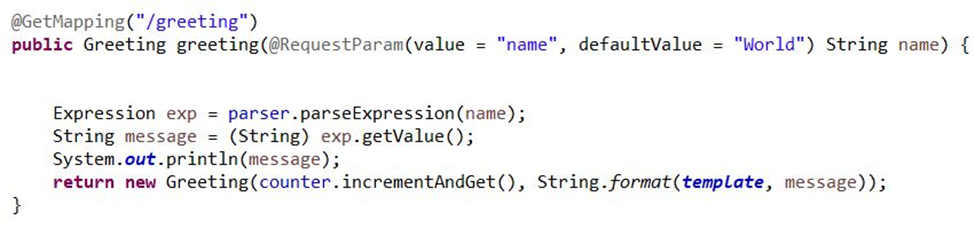
## Code Review Summary

* The Spring framework from the project uses an older version. When importing the file into the Eclipse platform, an error occurred referring to the dependency version in the pom.xml file. Therefore, eclipse provides a warning in the description, stating:

*“Overriding managed version 3.2.4. RELEASE for spring-data-rest-webmvc”.*

In contrast, the most recent version is 3.2.4

* The current version is outdated, and at the rate at which the technology advances, new versions need to be adopted. We will upgrade the current version 2.6.5 to latest version, which has numerous security updates.
* Within class GreetinController.java, the length of the string to be taken in will be limited in size to avoid any risk.



## Mitigation Plan

Mitigation planning reduces loss of information and data, ensures the safety of information by reducing the impact of vulnerabilities and disasters. By noting the risks, we will be able to develop long-lasting strategies for safeguarding systems. Furthermore, mitigation plans are fundamentals to ensuring safety.

* In our case, we will ensure the upgrade of the spring-data-rest-web MVC version to the latest 3.2.4.
* We will input validation and look for the length of data to avoid large data sizes that are being passed in. In addition, we will look for any problematic string patterns.

**Reference**

Joshi, C., Singh, U. K., & Tarey, K. (2015). A review on taxonomies of attacks and vulnerability in computer and network system. International Journal, 5(1).