Competency

In this project, you will demonstrate your mastery of the following competency:

- Analyze how advanced security concepts are applied to develop secure code

Scenario

You work as a developer for a software engineering company, Global Rain, that specializes in custom software design and development. The software is for entrepreneurs, businesses, and government agencies around the world. Part of the company's mission is that "Security is everyone's responsibility." Global Rain has promoted you to their new agile scrum team.

At Global Rain, you work with a client, Artemis Financial, a consulting company that develops individualized financial plans for their customers. The financial plans include savings, retirement, investments, and insurance.

Artemis Financial wants to modernize their operations. As a crucial part of the success of their custom software, they also want to use the most current and effective software security. Artemis Financial has a RESTful web application programming interface (API). They are seeking Global Rain's expertise about how to protect the organization from external threats.

As part of the team, you must examine Artemis Financial's web-based software application to identify any security vulnerabilities. You'll document what you learn in a vulnerability assessment report that will be used for mitigating the security vulnerabilities that you find.

Directions

You must conduct a vulnerability assessment. In it, you'll examine Artemis Financial's web-based software application. Use what you have learned so far and the resources provided in the Supporting Materials section to help you. Review and analyze the security vulnerabilities specific to Artemis Financial's web-based software application. Use the Project One Template, linked in What to Submit, to document the following for your vulnerability assessment report:

1. **Interpreting Client Needs**: Review the scenario to determine your client's needs and potential threats and attacks associated with their application and software security requirements. Document your findings in your vulnerability assessment report. Consider the scenario information and the following questions regarding how companies protect against external threats:
    a. What is the value of secure communications to the company?
    b. Does the company make any international transactions?
    c. Are there governmental restrictions about secure communications to consider?
    d. What external threats might be present now and in the immediate future?
    e. What are the modernization requirements that you must consider? For example:
        i. The role of open-source libraries
        ii. Evolving web application technologies

2. **Areas of Security**: Use what you've learned in step 1 and refer to the Vulnerability Assessment Process Flow Diagram provided. Think about the functionality of the software application to identify which areas of security apply to Artemis Financial's web application. Document your findings in your vulnerability assessment report and justify why each area is relevant to the software application.

Please note: Not all seven areas of security in the Vulnerability Assessment Process Flow Diagram apply to the company's software application.

3. **Manual Review**: Refer to the seven security areas outlined in the Vulnerability Assessment Process Flow Diagram. Use what you've learned in steps 1 and 2 to guide your manual review. Identify all vulnerabilities in the Project One Code Base, linked in Supporting

Materials, by manually inspecting the code. Document your findings in your vulnerability assessment report. Be sure to include a description that identifies where the vulnerabilities are found (specific class file, if applicable).

4. **Static Testing:** Integrate the dependency-check plug-in into Maven by following the instructions outlined in the Integrating the Maven Dependency-Check Plug-in tutorial provided in Supporting Materials. Run a dependency check on Artemis Financial's software application to identify all security vulnerabilities in the code. Specifically, identify all vulnerabilities in the code base by analyzing results from running the code through a static test. Include these items from the dependency-check report in your vulnerability assessment report:
    a. The names or vulnerability codes of the known vulnerabilities
    b. A brief description and recommended solutions that are found in the dependency-check report
    c. Attribution (if any) that documents how this vulnerability has been identified or how it was documented in the past

5. **Mitigation Plan:** Interpret the results from the manual review and static testing report. Identify steps to mitigate the identified security vulnerabilities by creating an action list that documents how to fix each vulnerability in your vulnerability assessment report.

Please note: You do not need to fix these vulnerabilities in this project.