1. Interpreting Client Needs: Review the scenario to determine your client's needs and potential threats and attacks associated with its 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?
        i. I think that there is great value within secure communications within a business or a in a company, because it is crucial when there is important information that must be protected, for example, in this case, Artemis Financial, is a company revolving around finance, which means that there is sensitive data, ensuring the maintenance of client confidentiality and making sure that secure communications are able to lead to substantial compliances to certain laws and regulations. This helps avoid any issues with unwanted breach and unwarranted access to data by external sources.
    b. Does the company make any international transactions?
        i. There is the possibility of Artemis Finance interacting with international transactions, financial companies usually partake in interactions with international firms, hence, it is imperative to have data protection laws and consider the different international regulations.
    c. Are there governmental restrictions about secure communications to consider?
        i. There are always many different regulations to consider, for example, the GDPR, which is the General Data Protection Regulation, which is meant to have certain protection requirements, though this is for EU citizens. This organization also has specific financial requirements which are meant to govern the communication and data transfers between different international agencies.
    d. What external threats might be present now and in the immediate future?
        i. From what I can imagine, I think that there can be data breaches and SQL injections. For data breaches, considering it is a finance company, there will be external sources that would like to obtain the information, which means that the data is very vulnerable. And an SQL injection is when there are certain codes implemented, so it attacks applications that are specifically data-driven.
    e. What are the modernization requirements that you must consider? For example:
        i. The role of open-source libraries
        ii. Evolving web application technologies
            1. I think the main sets of requirements to consider are to have very modern and up-to-date source libraries, to have data that is relevant to today's time, and to have certain application technologies to make sure that there are appropriate security practices that are implemented.

2. Areas of Security: Use what you have learned in step 1 and refer to the vulnerability assessment process flow diagram provided in the Supporting Materials section. 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.
    a. I think that there are several important key steps when it comes to maintaining the integrity and security of a company. For example, there should always be authentication and authorization to make sure that only the authorized personnel have access to the data, which relates to input validation within the vulnerability assessment process flow, to ensure that there is stable security input to make sure that the data is well protected, and can only be accessed through a set of validation. There should also always be some level of data protection, because it is important to encrypt data at different phases such as transit and at rest, to make sure that, even with authentication and authorization, the data can be protected.

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 the Supporting Materials section by manually inspecting the code. Document at least 7 to 10 findings in your vulnerability assessment report. Include a description that identifies where the vulnerabilities are found. Provide the specific class file, if applicable.
    a. There are some improper input handling, for example, the 'business_name' parameter can be exploited in a certain way if the data is used in a database query that has no sanitization available. Another inconsistency within the data could be the inconsistency within the class naming conventions, and it should follow Java's naming conventions. There is also a lack of exception handling which means that if any errors were to occur, then the application has a good possibility of crashing and/or returning not useful error messages which wouldn't help the process. There is also insufficient access control, meaning that the 'CRUD' method isn't able to implement any control methods to make sure that only the authorized personnel are able to access the application, which is an important part that was also mentioned in step two.

4. Static Testing: Integrate the dependency-check plug-in into Maven by following the instructions in the Integrating the Maven Dependency-Check Plug-in tutorial provided in the Supporting Materials section. 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 the following 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. Any attribution that documents how this vulnerability has been identified or how it was documented in the past
        i. The vulnerabilities were found in the dependencies, hence, it is important to update the identified libraries to make sure that the security is enhanced, hence there would be more updates to keep the maintenance process continuing.

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.
    a. The main vulnerabilities include: SQL injection, Direct Object References, Weak Validation and not sufficient enough of logging and monitoring. For the SQL injection, it would be important to make sure to implement certain systems to sanitize the user input before the system interacts with the data within the software. For the unstable object references, this refers to the fact that there should be stronger levels of authorization to make sure that only certain personnel are able to access the data given. The logging and monitoring ensures that the login data that is input into the data is monitored on a regular basis to ensure there are no problems.