# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **1/19/2025** | **Ryan Schermerhorn** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In this report, identify your security vulnerability findings and recommend the next steps to remedy the issues you have found.

* Respond to the five steps outlined below and include your findings.
* Respond using your own words. You may also include images or supporting materials. If you include them, make certain to insert them in the relevant locations in the document.
* Refer to the Project One Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Ryan Schermerhorn

**1. Interpreting Client Needs**

Determine your client’s needs and potential threats and attacks associated with the company’s application and software security requirements. Consider the following questions regarding how companies protect against external threats based on the scenario information:

* What is the value of secure communications to the company?
* Are there any international transactions that the company produces?
* Are there governmental restrictions on secure communications to consider?
* What external threats might be present now and in the immediate future?
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?

1. **Importance of Secure Communications:**

* Secure communication is crucial for the company because it protects sensitive data shared in the software application. By using strong encryption and secure channels, the company can lower the risk of unauthorized access, data tampering, and interception. This ensures the privacy and security of important information.

1. **International Transactions:**

* If the company deals with international transactions, it must pay attention to certain security issues. It is important to follow international data protection rules and use encryption standards to keep data safe while it is being transferred, especially when it crosses borders.

1. **Governmental Restrictions and Secure Communications:**

* Government rules may require certain steps for secure communication, especially in industries like finance and healthcare. Following these rules is important to avoid legal troubles, protect customer data, and keep the trust of stakeholders.

1. **Identifying External Threats:**

* To plan security effectively, it's important to identify possible external threats. These threats may include unauthorized access attempts, data breaches, injection attacks, social engineering attacks, and new risks like zero-day vulnerabilities. By understanding and addressing these risks, the company can strengthen its defenses and reduce potential weaknesses.

1. **Modernization Requirements and Emerging Technologies:**

* When assessing security, it is important to consider modernization needs and keep up with new technologies. This means regularly updating and patching open-source libraries, using secure frameworks, and staying informed about new web application technologies. By following industry best practices, the company can improve the security of its software and address new threats proactively.

Developer

1. Romario Gustave
2. 1. Interpreting Client Needs
3. a) Importance of Secure Communications:
4. Secure communications are vital for the company as they safeguard the confidentiality, integrity, and
5. authenticity of sensitive data transmitted within the software application. By implementing robust
6. encryption protocols and secure communication channels, the company can mitigate the risk of
7. unauthorized access, data tampering, and interception, ensuring the privacy and security of critical
8. information.
9. b) International Transactions:
10. If the company engages in international transactions, specific security considerations must be
11. considered. Compliance with international data protection regulations and adherence to encryption
12. standards are crucial to protect the confidentiality of data during transit, particularly when crossing
13. geographical boundaries.
14. c)

**2. Areas of Security**

Refer to the vulnerability assessment process flow diagram. Identify which areas of security apply to Artemis Financials’ software application. Justify your reasoning for why each area is relevant to the software application.

**Architecture Review:**

Conducting an architecture review is essential for assessing the design and structure of the software application. This evaluation aids in identifying potential security vulnerabilities that may arise from architectural flaws or weaknesses. By meticulously examining the architecture, we can ascertain whether secure distributed computing, client/server interactions, and the secure composition of components have been properly implemented.

**Code Review:**

A thorough code review is critical for pinpointing vulnerabilities within the software application. This review should encompass various code components, including models, controllers, data access layers, services, plug-ins, and APIs. By closely analyzing the codebase, we can uncover potential security weaknesses associated with error handling, secure coding practices, data structures, encryption utilization, and overall vulnerabilities.

**Secure API Interactions:**

Given that Artemis Financials’ web application likely interacts with multiple APIs, it is vital to evaluate the security aspects of these interactions. The assessment should include an analysis of authentication mechanisms, data encryption, and the validation of API responses to mitigate potential security risks and vulnerabilities. Ensuring secure API usage is crucial for maintaining the integrity and confidentiality of the data exchanged between the application and external systems.

**Summary of Findings with Mitigation Plan:**

A thorough vulnerability assessment should conclude with a concise summary of findings and a well-defined mitigation plan. This summary will provide an overview of identified vulnerabilities, categorize them by severity, and outline specific steps for effective mitigation. Prioritizing these vulnerabilities based on their potential impact on the application's security is essential for efficient risk management.

**3. Manual Review**

Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

* **Potential Connection Security Issue:**

In the DocData class, during the establishment of a database connection using

DriverManager.getConnection, there is a potential security issue related to the lack of specifying a secure connection. The code does not enforce the use of SSL/TLS protocols or other secure communication mechanisms when interacting with the database server. This omission can leave the communication channel vulnerable to eavesdropping or tampering, compromising the confidentiality and integrity of the transmitted data.

* **Potential SQL Injection Vulnerability:**

In the DocData class, specifically within the readDocument method, there is a potential SQL injection vulnerability. This method accepts user-provided values for the key and value parameters, but it does not implement adequate input sanitization or parameterization before including these values in the SQL query. As a result, the application could be exposed to SQL injection attacks, where malicious input might manipulate the query, potentially leading to unauthorized access or data manipulation.

**4. Static Testing**

Run a dependency check on Artemis Financials’ software application to identify all security vulnerabilities in the code. Record the output from the dependency-check report. Include the following items:

* The names or vulnerability codes of the known vulnerabilities
* A brief description and recommended solutions provided by the dependency-check report
* Any attribution that documents how this vulnerability has been identified or documented previously

Log4j-api-2.12.2.jar = This has one vulnerability, and the solution would be to update it

to the most recent update 2.13.2

•Bcprov-jdk15on-1.46.jar= A LOT of vulnerabilities, the solution would be to update to

1.60

•Snakeyaml-1.25.jar = one vulnerability, solution is to update to latest system.

•Tomcat-embed-core-9.0.30.jar = Three vulnerabilities, update to Apache Tomcat 10.0.6

•Jackson-databind-2.10.2.jar= One vulnerability, solution is to update to current version.

•Hibernate-validator-6.0.18.final.jar= One vulnerability, solution is to update to 6.0.20

**5. Mitigation Plan**

Interpret the results from the manual review and static testing report. Then identify the steps to mitigate the identified security vulnerabilities for Artemis Financials’ software application.

Upon reviewing the results from the manual assessment and static testing, it is essential to outline the steps needed to address the identified security vulnerabilities in Artemis Financials’ software application. First, all systems should be updated to their latest versions to mitigate known issues. Next, implementing HTTPS is crucial for securing online access. Following that, establishing a robust authentication system will ensure that customers can only access their own information. Once these initial measures are in place, we can evaluate further actions required to safeguard sensitive information while ensuring it remains easily accessible to authorized individuals.

Insert

Retry