****

# CS 305 Project One

**Artemis Financial Vulnerability Assessment Report**

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **1/24/2021** | **Jovan Martinez-Saldana** |  |

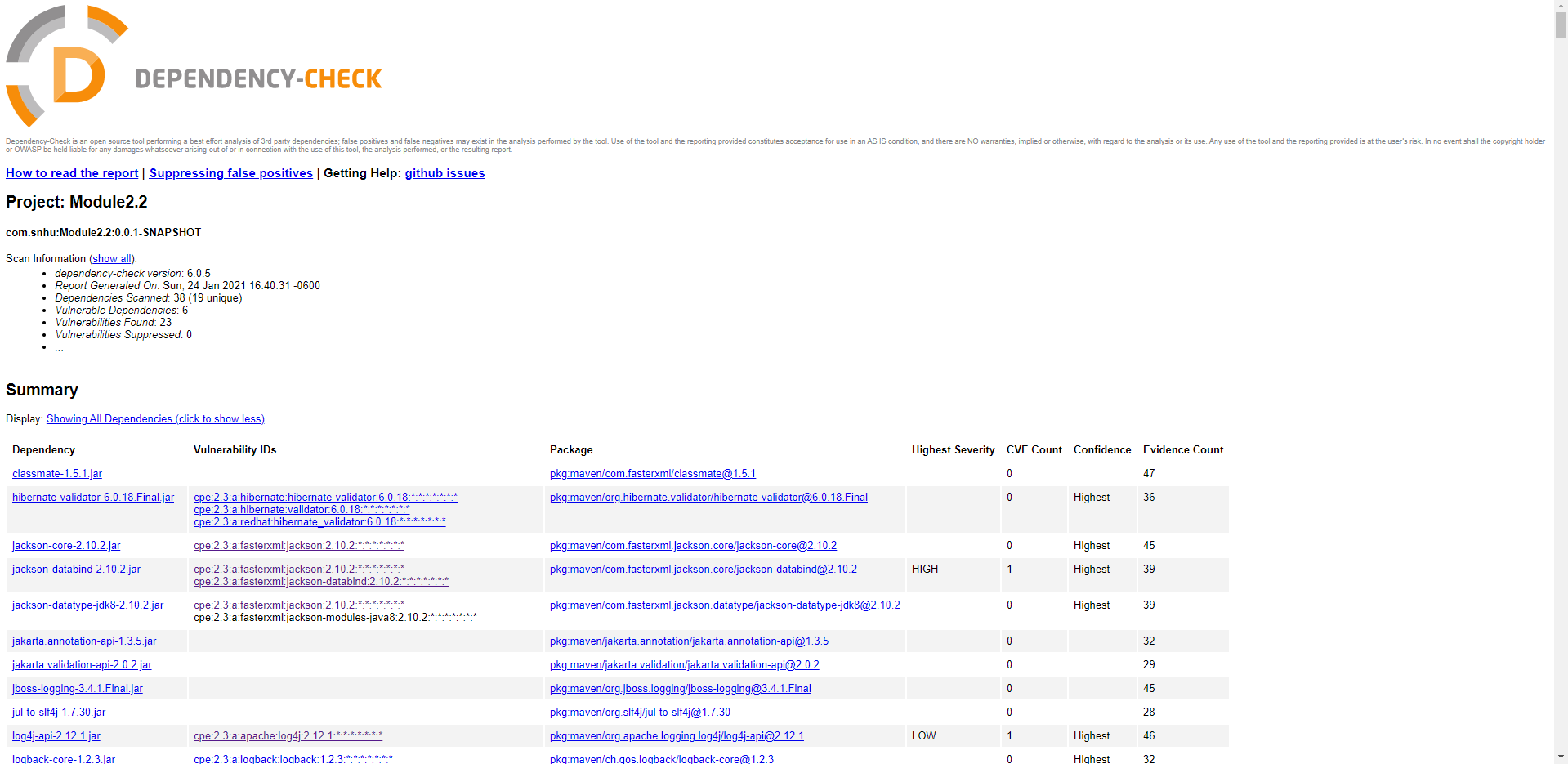
## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.



## Developer

Jovan Martinez-Saldana

## 1. Interpreting Client Needs

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

* What is the value of secure communications to the company?

**The main benefit of secure communications is that having them in place allows protection of customer data, such as companies that specialize in healthcare and finance. Also, it protects internal information, such as anything that stands out profitable or any documents that state what said company has over other companies.**

* Are there any international transactions that the company produces?

**Some, since these international transactions can apply if someone accesses data from them outside of the company’s country.**

* Are there governmental restrictions about secure communications to consider?

**There are actually no government restrictions when it comes to secure communications.**

* What external threats might be present now and in the immediate future?

**Any and all forms of hacking. Hacking is ever evolving with technology, so its important for companies and consumers alike to keep up to date with the best security software.**

* What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?

**Some requirements to think about would be that even with open source libraries, a form backdoor security should be in place.**

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financials’ software application. Justify your reasoning for why each area is relevant to the software application.

#1. Input Validation – There will have to be some sort of end-to-end encryption because of how crucial secure communications are.

#3. Cryptography – acknowledging and protecting the known vulnerabilities that we have found is important to just getting to that first step.

#5. Code Error – Although there were not “errors” per say in the provided code, its important that the fixes to the security implementation have the blanket of code error checking, else the remedies are of no use.

#6. Code Quality – When certain code for these security changes gets to the point where it could do more, proper coding principles will need to be in place for the next person who will be working on it, such as looping structures and not writing them out individually if they retain the same use.

#7. Encapsulation – I think I sort of described this unintentionally above, but I also feel that this is an area of security that is relevant.

## 3. Manual Review

Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

As I stated before, I’m very bad at identifying issues with code that aren’t flashing red to the compiler, but based on the classes I saw, I felt that CRUD, with the public strings, required some sort of exceptions for the inputs that could be provided. Something to stop an excessive number of characters, and maybe something to deal with numbers and special values. myDateTime seemed fine, but CRUD controller had a lot of import statements I wasn’t knowledgeable in. There should be a specification in place if Artemis Financial is asking for help (access to org.springframework.boot.autoconfigure. would be nice). I’m sure there were more but that is to the best of my ability.

## 4. Static Testing

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

1. The names or vulnerability codes of the known vulnerabilities
2. A brief description and recommended solutions provided by the dependency check report
3. Attribution (if any) that documents how this vulnerability has been identified or documented previously

* [jackson-databind-2.10.2.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l4_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) - General data-binding functionality for Jackson: works on core streaming API

A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

* [log4j-api-2.12.1.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) - The Apache Log4j API.

Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.

* [snakeyaml-1.25.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) - YAML 1.1 parser and emitter for Java

The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

* [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l16_3734223040040e8c3fecd5faa3ae8a1ed6da146b) - Spring Boot

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

* [tomcat-embed-core-9.0.30.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l17_ad32909314fe2ba02cec036434c0addd19bcc580) - Core Tomcat implementation

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

* [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\robos\eclipse-workspace\Module2.1\target\dependency-check-report.html#l19_33157f6bc5bfd03380ebb5ac476db0600a04168d) - Core Tomcat implementation

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financial’s software application.

I think that based on my findings, there will need to be added data integrity protection in place. Utilizing standard, tested, security services whenever its possible is also a must. Since there is an emphasis for secure communications, only send passwords or logins over a secure encrypted connection. Ultimately, the use of server side session objects for making and sort of authorization decisions.