****

# 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** | **03/18/2023** | **Daniel Anderson** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for 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 choose to include images or supporting materials. If you include them, make certain to insert them in all 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

Daniel Anderson

## Interpreting Client Needs

Having secure communication is very important to any company and should always be a huge priority. Having secure communications is important to protecting the data from any cyberattacks. The main goal of having security is to protect the data, integrity, and the companies clients. The PCI-DSS is set of compliance standards set forth for credit cards along with the GDRP that sets standards for any business that is done locally and internationally. The government sets a bunch of standards that relate to any business done locally that relates to how things must be encrypted. The government also has standards set surveillance regulations that may vary depending on where the company is located and every location that they may deal with. There are many different threats that the company must prepare against that can come through the network or even in person. Some of the biggest threats that can happen digitally are malware, SQL injections and phishing attacks. Some of the in-person threats is someone committing what is classified as a social engineering threat. When it comes to modernizing the software there are many things to be careful of, one thing that is dangerous is open-source libraries. Open-source libraries are helpful with updating security measures but almost come with the threat of anyone that is creating said sources. When updating web application, if not careful can cause unintended openings within your software that could allow intrusions if not careful.

## Areas of Security

When reviewing the vulnerability assessment process flow diagram there are many areas that need be secured to ensure that safety of the software. The following is a list of things that are areas of concerns:

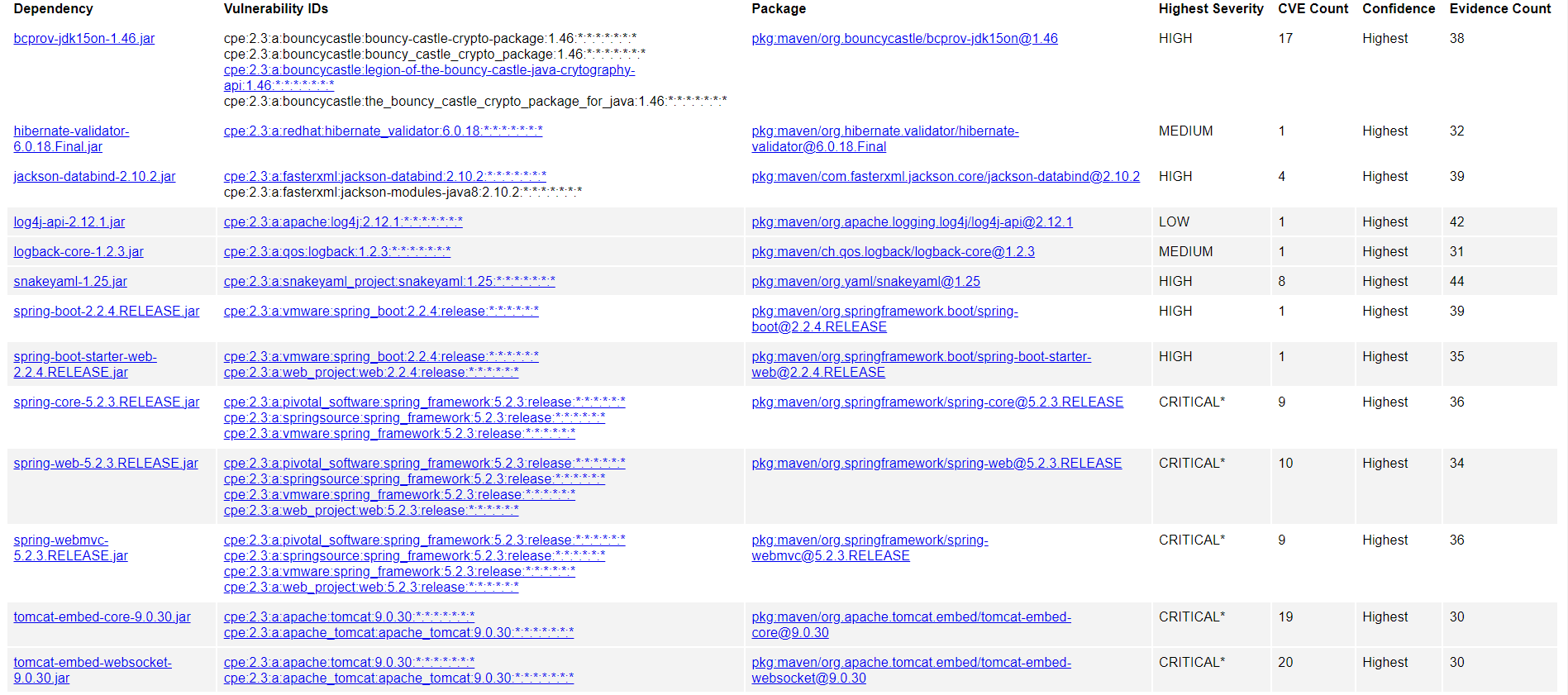
* Input Validation, important to ensure customers can securely access their information.
* Cryptography, this allows secure communication of information between the servers and clients.
* Client/Server, by having these secure and protected from threats allows the company to maintain its integrity with its clients.
* Code error/quality, these two areas go hand in hand because if the code is not error free and in good form it could allow vulnerabilities through the software.

## Manual Review

Upon reviewing the code one of the first things I noticed that could cause an error is DocData.java file. When reviewing this code, you can see that the information is defined wrong for the method. It is defined as a public when it should be public to protect the database from cyber-attacks. The CRUDController.java also allows access directly to the database which could leave the web application open to an SQL injection attack which could break the integrity of the company.

## Static Testing

After the testing was ran there was many vulnerabilities that were detected that need to be taken care of to ensure the security of the software. I have attached a list of all the known vulnerabilities.



## Mitigation Plan

After reviewing the code and running a dependency check which showed many vulnerabilities in the code there is many steps that should be taken to ensure its security. The first big that needs to be addressed is shoring up the log in system of the software. By changing how the signature is validated and confirmed should help prevent any SQL injection attack through the log in credentials. The next step should be reviewing the code to and changing it to protect the database information that is set to public. Changing this code should allow the information to be more secure and safe from digital threats. The dependency checker also noticed that the Apache version is an old and outdated version, updating Apache will help ensure some extra security that the older versions did not have built into them already. The checker also picked up an error in how the credentials are validated while using the cryptography certifications. The software should be updated and changed to ensure that the certifications are verified correctly and securely.