****

# 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** | **3-17-2022** | **Meagan Holub** |  |

## 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

Meagan Holub

## 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 value of secure communications is the main focus of the company to keep the customers confident in our services and that we will protect their information and personal data. “Security is everyones responsibilty” is their moto.

**Are there any international transactions that the company produces?**

Artemis financials is a fully online and web based company so they do deal with international transactions. Anyone who has access to a computer and their website can access the software.

**Are there governmental restrictions about secure communications to consider?**

There are many governmental restrictions that need to be considered for this software. Since the company deals with savings, retirements, investments, and insurance for their patrons so there are many restrictons and laws that have to be abided by. Policies are changed regularly and it must be monitored by staff very frequently to make sure all rules and policies are current to avoid trouble. The law allows the U.S government to access digital communications such as email, social media, messages, information on public cloud servers. We must help our customers understand that all of their data is secure but they must still abide by governmental restrictions that may affect their privacy. Policies change frequently when dealing with money so we must consider having to make frequent updates.

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

External threats that we may be facing in the present and immediate future is hackers. There is a big issue these days with people accessing private data illegally and it leads to identity theft etc. Phishing is a big problem these days which is a social engineering attack where hackers steal financial data, personal information, credit card numbers and account logins. This occurs when hackers send out fake emails that imitate a company or person that they can trust to obtain private information. My plan to keep this from happening is that if we need any financial information or any updates to accounts we will only send out secured emails that take them directly to our website. If any phishing emails are sent out imitating our software we will have the IT/security team block the IP address of the hackers and stop any security threats immediately.

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

Modernization requirements is all about taking security to the next level through updates and new technology. Technology evolves constantly and staying ahead of your competitors is crucial. If there is other softwares that companies release that are more advanced and work faster than ours we will lose our business. I will have a team that constantly builds updates and new features that stays ahead of our competition. We must offer unique services that makes us stand out from other platforms. With us being fully web based this will benefit the company from an open source library so our company can add extra layers of security and functionality to the program.

## 2. Areas of Security

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

API- API security is important because businesses use APIs to connect services and to transfer data, and so a hacked API can lead to a data breach. API abuse issues have roughly doubled over the past 4 years, according to the 2019 Application Security Risk Report by Micro Focus Fortify. We must assure that our security is tight and keep hackers from leaking personal data. Data breaches can destory or reputation and since we will have two or more applications to communicate together.

Cryptography- Is the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents. It provides secure communications that blocks malicious third parties from stealing data. We will send data through encryption which will help data from being decoded by unintended persons. This will level up our security and make our communications even safer.

Client/Server- Where the data base resides on a server, and client applications are written to access the data base. The server listens for requests for its services and the client makes requests which includes selecting, inserting, updating, and deleting data. Client servers have security features that secure data and they also have physical security that protects the hardware and network data that may potentially get breached. We must take security measures to the next level across all systems to live up to the company moto “Security is everyones responsibility”. All teams must be ready to fight against unwanted hackers.

Secure Coding- Is the practice of developing computer software in such a way that guards against the accidental introduction of security vulnerabilities. Bugs and logic flaws are the primary cause of commonly exploited software vulnerabilities. Ways that I plan secure my code is to validate input from all untrusted data sources. I will always pay attention to compiler warnings while running code every couple of lines to avoid waiting until the end to debug. It is important to constantly check for errors so it can be fixed quickly before a small problem becomes major. It is also important to avoid downloading strange packages that can leave a door open to hackers to gain access to code. External data should be sanitized regularly.

## 

## 3. Manual Review

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

Data Access:

There was a vulenrability within the DocData.java file which means unauthorized users can easily gain access to our system. This will make our users logins and passwords open with multiple vulnerabilities. The data access method is to access the data which gives the description of the location for the data and can leak the login information. It can make it easy for hackers to guess and gain access in our system by using the brute force attack.

Direct Object Reference:

CRUDController.java I was able to spot another vulnerability where the objects and classes can be accessed through a sequence of code injections. Business names are sent as request parameters within the CRUDController class which leaves the code extremely vulnerable and easily leak private information to hackers and unwanted users.

Other issues I noticed while manually scanning the code was HTTPS are not used, No authentification system for verification directed towards unwanted access, requests are not validated which leaves an opening to unwanted security breaches. We must tighten up these vulnerabilities to protect our software from data breaches.

## 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

A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.

CWE-20 Improper Input Validation  
  
CVSSv2:

* Base Score: MEDIUM (5.0)
* Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:

* Base Score: MEDIUM (5.3)
* Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

bcprov-jdk15on-1.46.jar - several vulnerabilities on 1.46, update to latest version.

bcprov-jdk15on-1.46.jar - several vulnerabilities on 1.46, update to latest version.

CVE-2013-1624

CVE-2015-6644

CVE-2015-7940

CVE-2016-1000338

CVE-2016-1000339

CVE-2016-1000341

CVE-2016-1000342

CVE-2016-1000343

CVE-2016-1000344

CVE-2016-1000345

CVE-2016-1000346

CVE-2016-1000352

CVE-2017-13098

CVE-2018-1000613

CVE-2018-5382

Log4j-api-2.12.1.jar - one vulnerability, update to latest version.

CVE-2020-9488

Snakeyalm-1.25.jar - one vulnerability, update to latest version.

CVE-2017-18640

Jackson-databind-2.10.2.jar - one vulnerability, update to latest version.

CVE-2020-25649

Tomcat-embed-core-9.0.30.jar - several vulnerabilities, update to latest tomcat version.

CVE-2019-17569

CVE-2020-11996

CVE-2020-13934

CVE-2020-13935

CVE-2020-13943

CVE-2020-17527

CVE-2020-1935

CVE-2020-1938

## 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.

After looking at all of the identified vulenarabilities from the static test and dependency check results I realized that our security team has a lot of work to do. There were way more errors than I am comftorable with and our software is not ready to launch to the public. We would have multiple data breaches and ways hackers could gain access. My first step to improve our security is to add HTTPS so we only have direct communication so we don’t have any leaks to outsiders. We must create a algorithim for stronger passwords and enable two step authentification to protect all user creditentials. We need to update all systems to the newest versions which was a big issue on the report. All systems were not up to date which weakens security. Every server will be updated immediately. Secure coding practices will be used and we will train all employees how to secure data. We must go through every error on the report and fix these issues before launching our software.