# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **07/23/24** | **Kirklen Allen** |  |

## 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

Kirklen Allen

**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?

The value of secure communications is a nonfunctional requirement necessary when handling important financial personal data between the client and server. Encryption is the most effective way of protecting the data between transmission if it is not secured by the HTTPS protocol. Artemis Finacial's ability to process sensitive data from potential users around the world requires a necessary attention to detail when finding vulnerabilities. Following the OWASP procedure protects users from vulnerabilities, it creates more secure software.

Moreover, Governmental Regulated Database such as the National Vulnerabilities Database help protect java applications with solutions provided by developers who experience the same obstacles while testing. The demand for testing will always be an investment for a secure SDLC because the ability to target vulnerabilities in the earlier phase saves a lot on the front side while keeping the potential for new bugs found to be less likely.

Prioritizing security is one of the essential functions that help develop a critical business system. The modernization of requirements has helped evolve the SDLC even to a DevSecOps adaptation. This model helps combine the necessary business foundation while implementing the IT architecture to help provide a secure application. Web-based applications have changed the way users interact with software and this displays software beyond the problem it faces in its designed OS. The uniformity in the scenarios the software faces is what allows developers to understand the importance of debugging across all software. Critical, and High-risk bugs are the most important to be cautious of in modern technology because it can be identified as an introduction to a potential Cyber Attack that leaks more sensitive data. Open-Source Libraries helped develop because the functions can connect to servers or local hosts to implement functions that improve software performance. This saves the developer time because the library establishes the architecture process necessary to create an overall Secure Data Structure.

**2. Areas of Security**

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

1. Cryptography
   1. It is important to have cryptography as an area of security for Artemis Financial. This process helps secure client transactions. If the server’s security has been compromised the encryption of data itself will add an extra level of security that protects the user from personal information being compromised.
2. Encapsulation
   1. Creating a Secure Data Structure allows many companies to process data that is received on a massive scale through daily data processing. A good structure has the potential to scale while also protecting it from vulnerabilities at an early stage. In the event an update is pushed out to the audience, the previous version of an application being debugged can help tremendously save developers cost during an app's lifecycle.

**3. Manual Review**

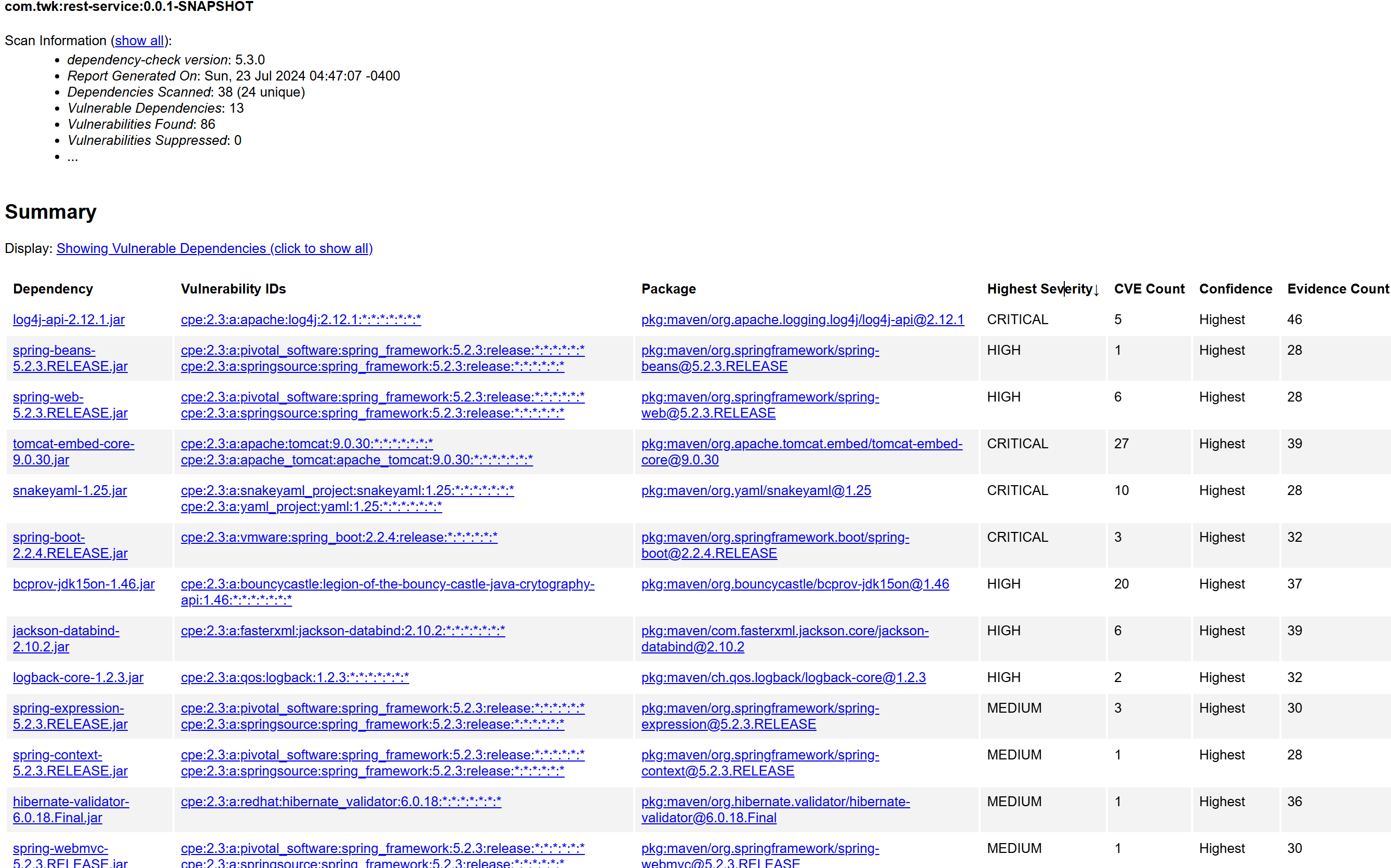
Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

The vulnerabilities analyzed in the report identify high risk security exploitations that have been protected against by The National Vulnerability Database to protect enterprise database from major data breaches. Ranking from critical to low, dependencies scanned support the severity of potential breaches with evidence count identifying how many times it can be found in the application. Interacting with global data can vary from accessing local data for many reasons including time, volume, capacity, and efficiency.

1. [bcprov-jdk15on-1.46.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) (Critical)
2. [spring-boot-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) (High)
3. [logback-core-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) (High)
4. [log4j-api-2.12.1.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb) (Critical)
5. [snakeyaml-1.25.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) (Critical)
6. [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) (Critical)
7. [tomcat-embed-core-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l13_ad32909314fe2ba02cec036434c0addd19bcc580) (High)

**4. Static Testing**

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



* [bcprov-jdk15on-1.46.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) - [**CVE-2013-1624**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624) **-** The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.
* [spring-boot-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) - [**CVE-2022-27772**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772) **- Spriing Boot Vulnerabiltiy found based on Software Version**
* [logback-core-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) - [**CVE-2021-42550**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42550) - In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.
* [log4j-api-2.12.1.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb) - [**CVE-2020-9488**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9488) **-** 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. Fixed in Apache Log4j 2.12.3 and 2.13.1
* [snakeyaml-1.25.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) - [**CVE-2017-18640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640) **-** The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.
* [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) - [**CVE-2020-25649**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649) **-** 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.
* [tomcat-embed-core-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l13_ad32909314fe2ba02cec036434c0addd19bcc580) - [**CVE-2019-17569**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569) **- T**he 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**

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

The Vulnerability report provided for Artemis Financial shows a detailed report on Critical, and High Risk bugs that have the potential to leave opening for a big data breach. Reports such as [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) are extemely important to be aware of because they leave access to the most important area of security, which is data integrity. Most bugs (5) require the developer to update the framework to the latest version, which solves most high-risk bugs that rely on open-source libraries.

* [bcprov-jdk15on-1.46.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) - Updating the Bouncy Council to the latest Version solves this bug.
* [spring-boot-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) - Updating the version of the spring boot helps fix this bug
* [logback-core-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) - Setting the log back to read only and updating the version to the latest update can solve this vulnerability.
* [log4j-api-2.12.1.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb) - According to the Java Version (6,7,8) a specific Log4j update is required to remove this vulnerability
* [snakeyaml-1.25.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) - Updating the library can help address this bug issue found.
* [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) - Updating to the latest version helps properly secure the entity expansion which is the highest threat of data integrity.
* [tomcat-embed-core-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fkirklen_allen_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F834b3f2735bc4e2ea70adf37da48f550&wdorigin=AuthPrompt.OFFICECOM-WEB.START.EDGEWORTH&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=f871d1f4-9ed5-4668-8b75-768be7ec266b&wdenableroaming=1&mscc=1&wdodb=1&hid=B1CB40A1-F015-6000-1E10-429936AE893F.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=22a50333-ac89-9b44-2591-39920d396396&usid=22a50333-ac89-9b44-2591-39920d396396&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l13_ad32909314fe2ba02cec036434c0addd19bcc580) - Updating to the latest version protects the user from a potential Cyber Attack through a reverse [rpxy.