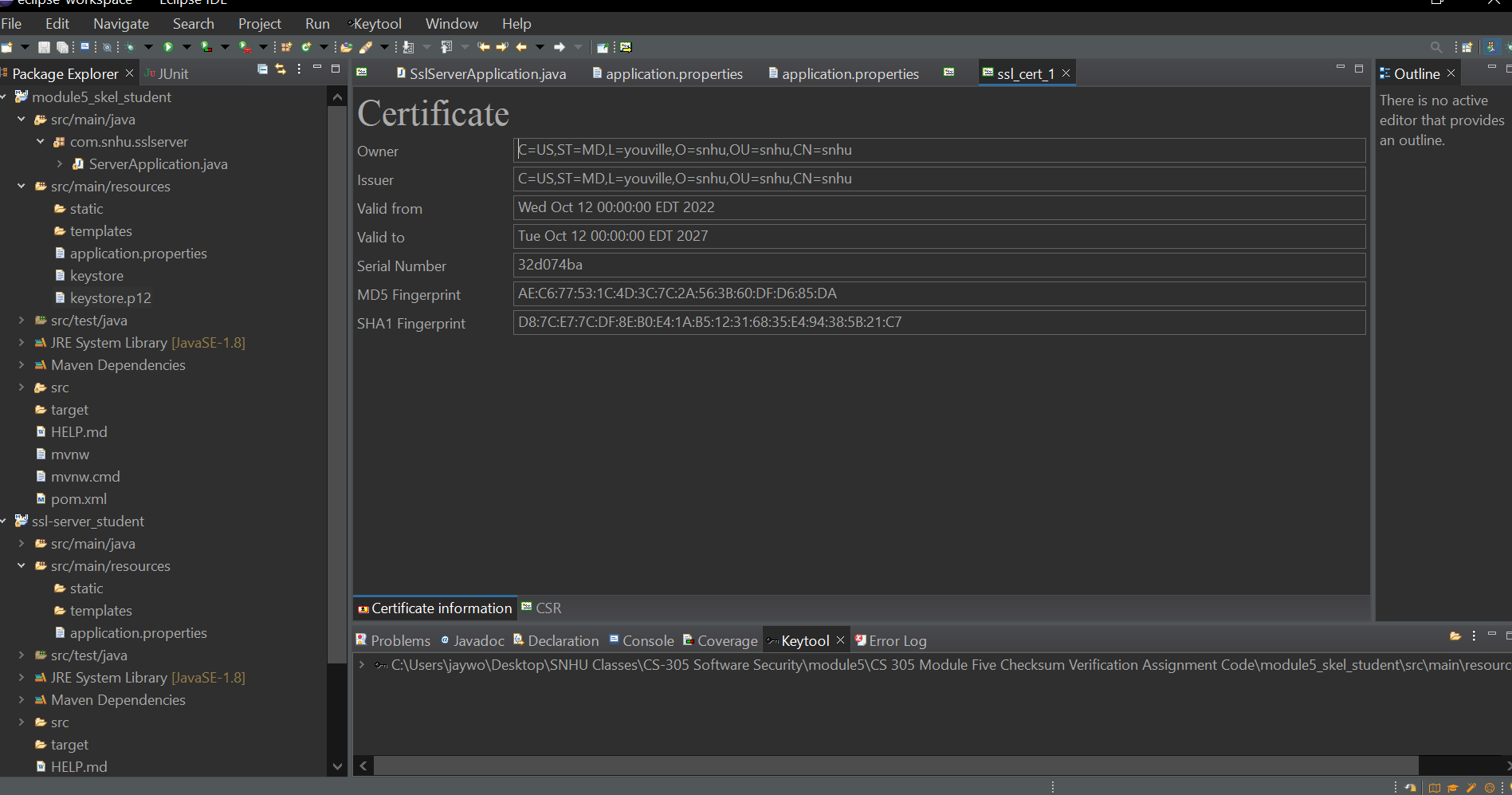
Jason O’Connell

10/15/2022

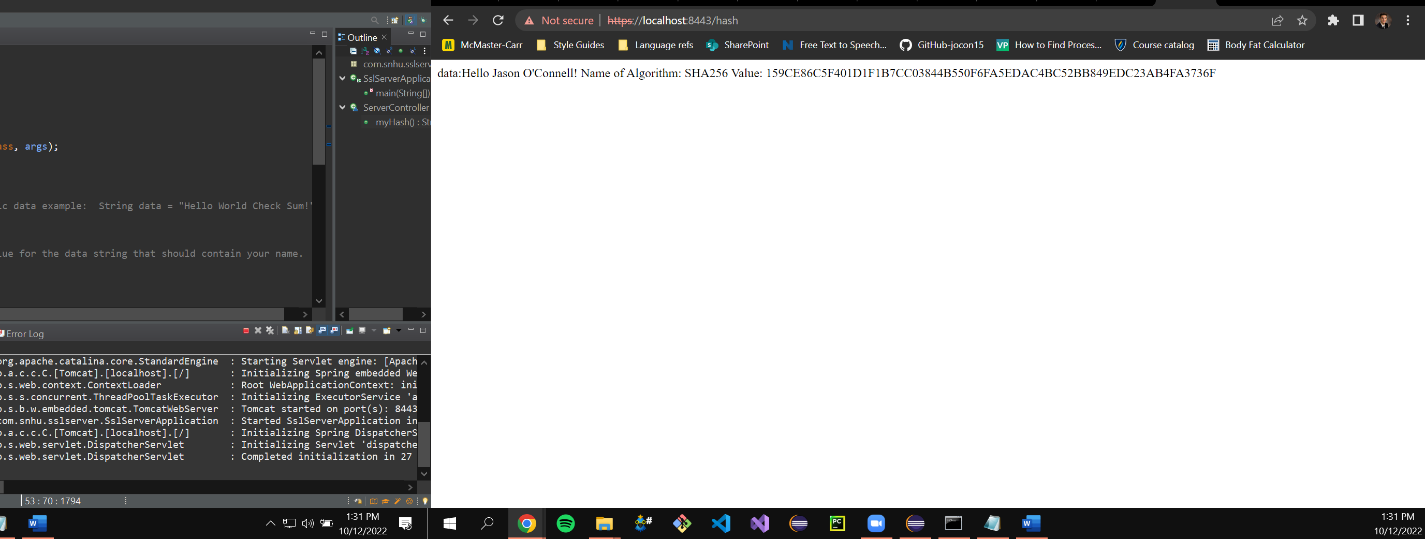
Project 2

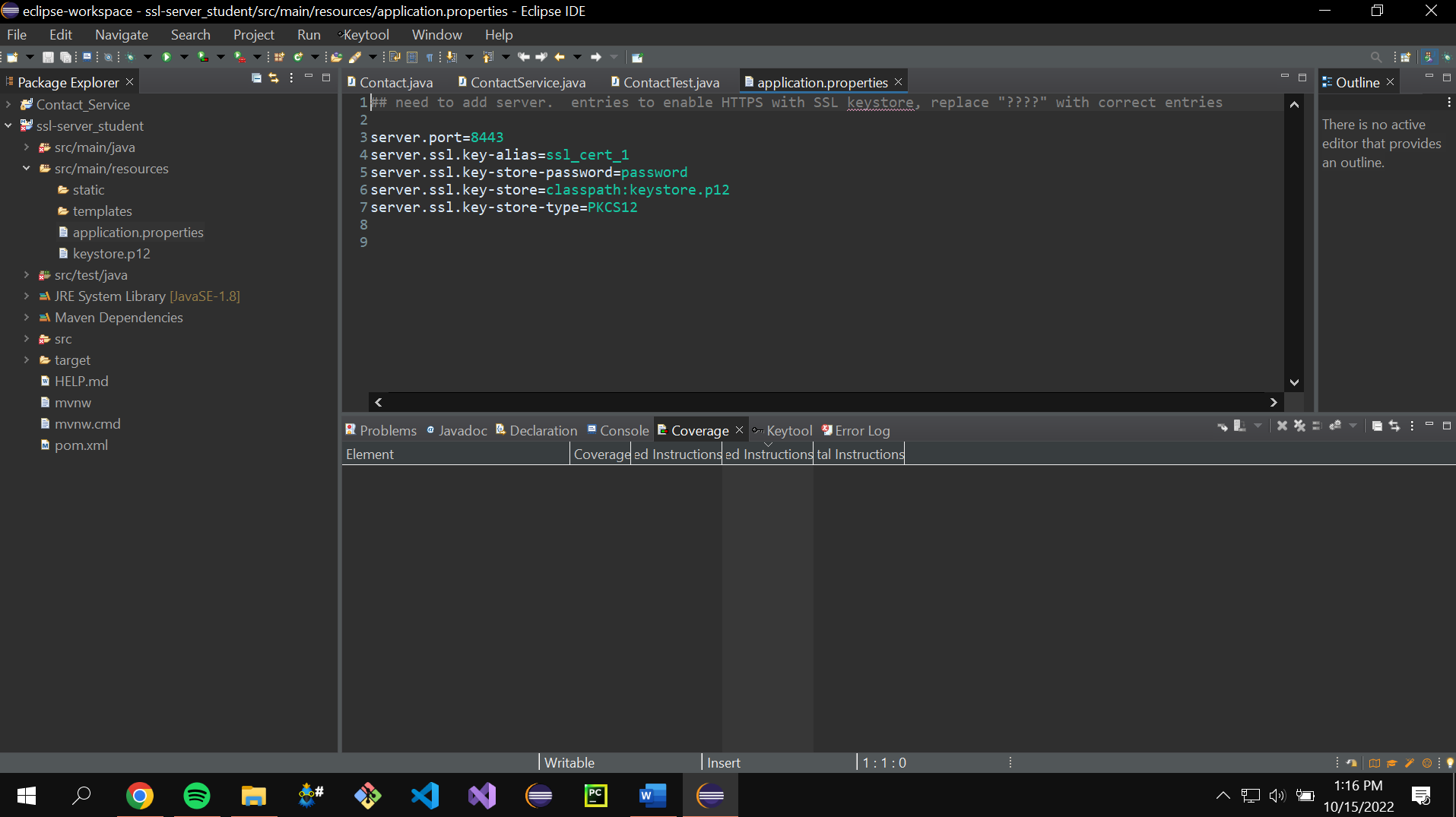
Secure communication is going to involve encrypting the data that is being transferred between 2 computers. In a previous assignment, we chose the symmetric AES-256 as our encryption method for encrypting archive files on a single machine. Now that we have multiple machines that are accessing data, a different encryption style is needed. This is where asymmetric encryption comes into play. Asymmetric encryption uses the public and private key method for establishing a secure connection much more efficiently than symmetric. One of the most common and strong asymmetric encryption algorithms is RSA. Since our domain is financial technology, we are going to want a bit size that is strong enough. According to IBM, RSA 2048 bit and higher is considered “high-strength” ("IBM Documentation", 2022). The recommended encryption cipher for this application is RSA-2048. IBM also specifies that RSA 2048 and higher ciphers use the SHA-256 hashing algorithm for certificate signing ("IBM Documentation", 2022).

CER FILE:



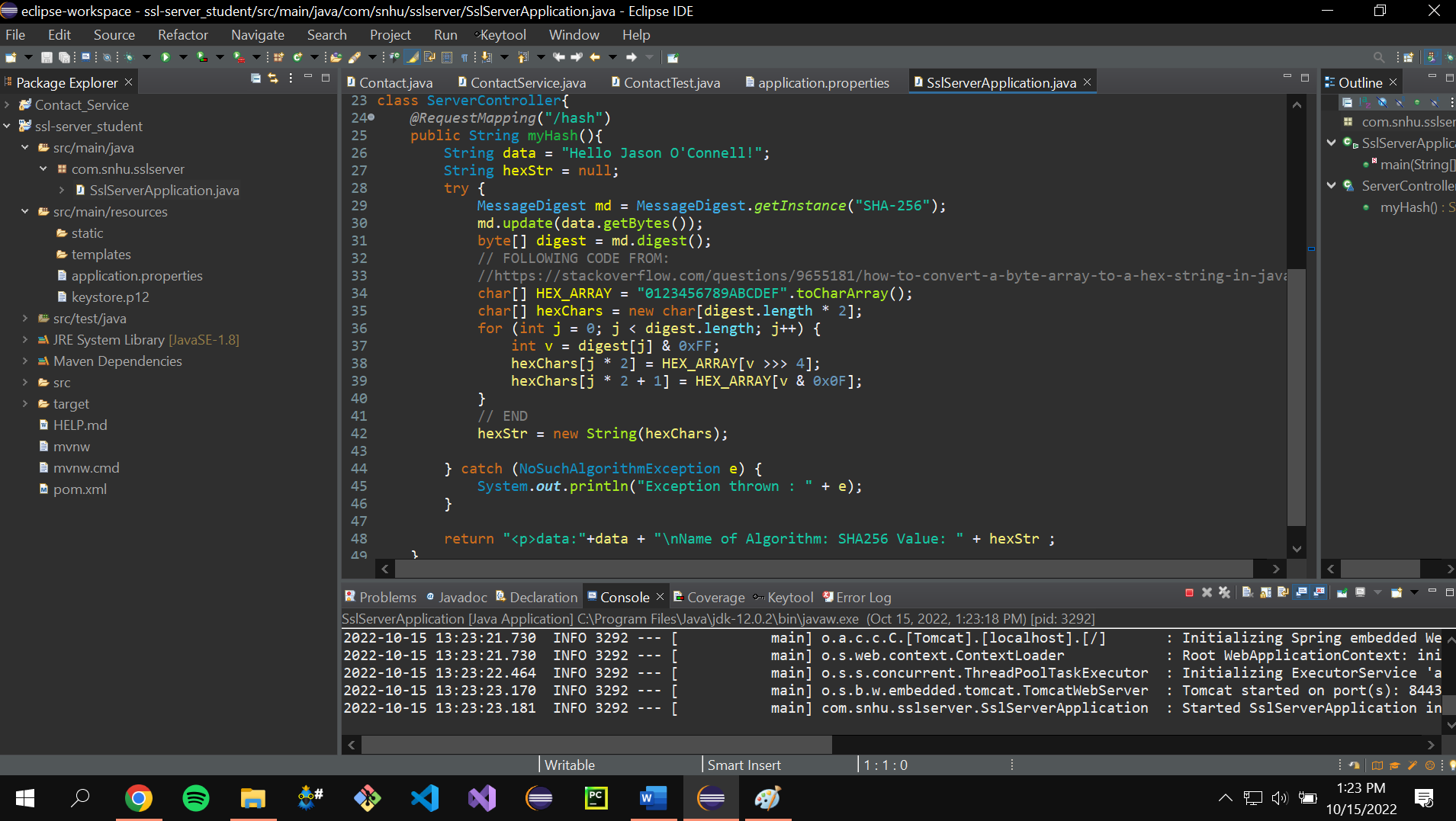
CHECKSUM VERIFICATION:

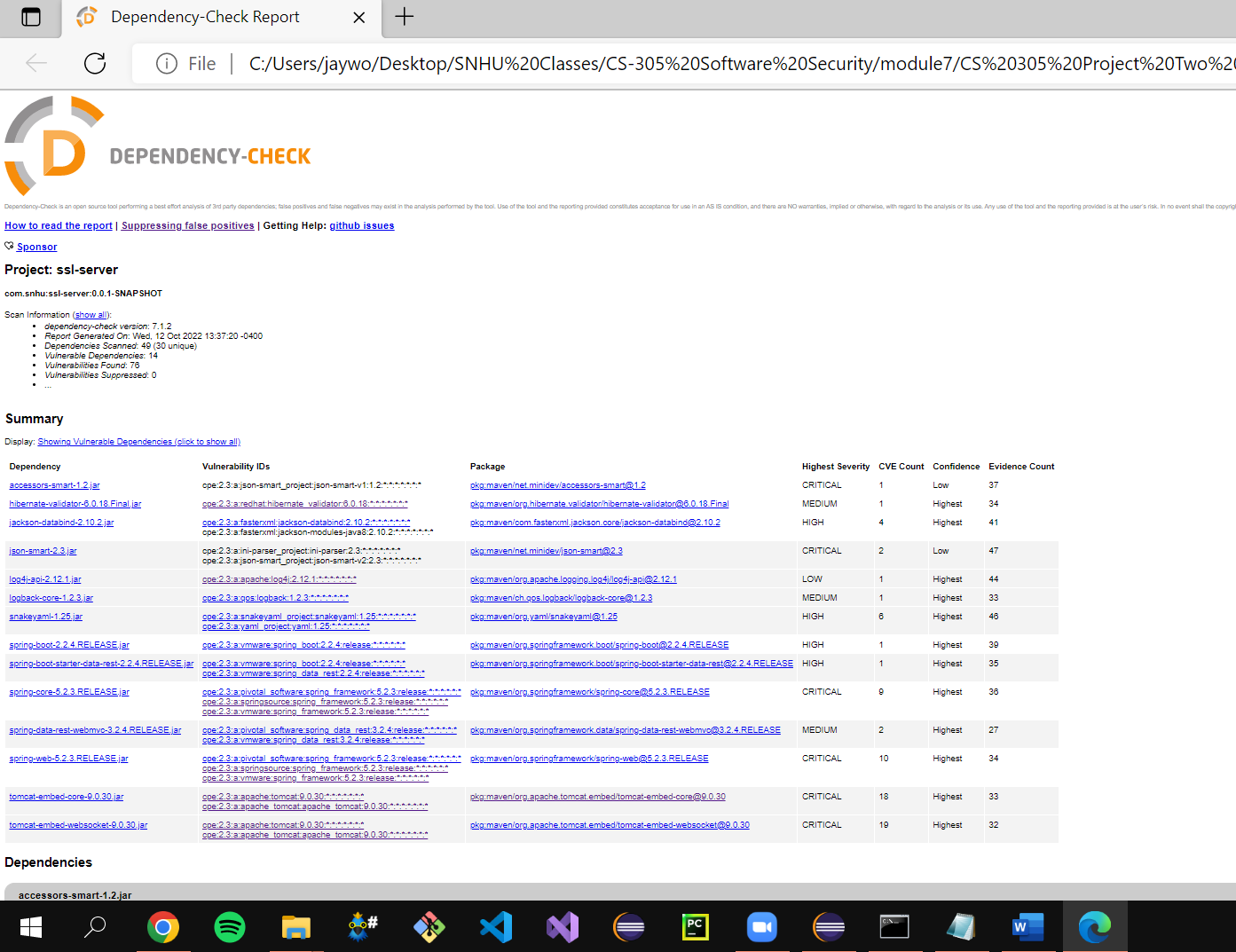


APPLICATION.PROPERTIES:

SEE THE “CHECKSUM VERIFICATION” IMAGE FOR PROOF OF SECURE COMMUNICATIONS

REFACTORED CODE BEING EXECUTED



STATIC TESTING:

CODE REVIEW

The application in its current state is quite small. This means that the attack surface is small. As of the current application source code, there are no apparent vulnerabilities beyond those defined by the dependency check report. The only webpage endpoint active currently is the /hash page, which is view only, the server does not take in any client side inputs. In the future, the Artemis system is going to have many more pages available with inputs taken from the client. Once these are implemented, it is crucial that the input be sanitized before it is used by the business logic. As the system come online, Artemis should be watching traffic and building blacklists if any malicious intent is identified. Even better, if circumstances allow, a whitelist should be enacted to additionally prevent malicious intent.

SUMMARY

The application has been refactored form its original state. We created a certificate for the application. We then linked to that certificate using the “application.properties” file. This allowed the application to only be available via http secure (https). Now, the data between the client and the server is encrypted while in transit. This is going to protect the financial data from man in the middle attacks. The certificate is going to ensure that clients of Artemis financial are in fact interacting with the legitimate Artemis business and not some malicious actor trying to spoof the domain name. We also implemented a SHA-256 hashing algorithm That Artemis can use for things like password hash storing and file integrity verification.

One of the biggest industry standards when it comes to communication over the internet is ensuring that the address you are communicating with is the entity that you believe it is. Best practice uses certificated to verify that a particular entity is as advertised. We implemented a certificate to do exactly that. Once you have the 2 verified entities that want to exchange information over the internet, industry standards indicate that the information should be encrypted while in transit between entities. This prevents unwanted 3rd parties from intercepting the communications. Unencrypted communication is especially risky if the data being transferred is sensitive. We implemented the http secure (https) protocol to encrypt our communications between client and server. Lastly, though not fully implemented, we supplied Artemis financial with the hashing algorithm logic that will largely be used to verify file integrity.

Security is going to be very important for Artemis. They are a financial technology company which means the information they deal with is highly sensitive and thus highly valued by attackers. They are likely going to be sniffed frequently by attackers for any vulnerabilities. Implementing security features such as the ones discussed are going to ensure the integrity of Artemis Financial as a reputable business.

References

*IBM Documentation*. Ibm.com. (2022). Retrieved 15 October 2022, from https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys.