* Briefly summarize your client, Artemis Financial, and their software requirements. Who was the client? What issue did they want you to address?

Artemis Financial offers personalized financial plans covering savings, retirement, investments, and insurance. Protecting sensitive customer data, including SSN, address, phone number, and any sensitive data is a top priority. The company employs the latest software security measures, ensuring compliance with government regulations. Protect sensitive data and maintain the trust to customer is very important to prevent reputational damage.

In their use of RESTful APIs for services, Artemis Financial takes measures to secure communications and prevent data interception. Confidential information is transmitted securely, adopting best practices either in headers or communication bodies (request or responds). This proactive approach fortifies systems and ensures the security of customer information against evolving modern threats.

* What did you do very well when you found your client’s software security vulnerabilities? Why is it important to code securely? What value does software security add to a company’s overall wellbeing?
* Upgrade all systems from static testing result to the recommendations:
  + Upgrade Bouncy Castle JCE to at least 1.61 or newest and Bouncy Castle for Java after 1.74
  + Upgrade to the newest Spring-Boot
  + Do not use logback version 1.2.7 and prior versions and version 1.4.11
  + Upgrade Apache Log4j2 to at least 2.13.2
  + Recommend using SnakeYaml’s SafeConturctor and upgrading to version 2.0 and beyond. And do not use snakeYAML to parse untrusted YAML files may be vulnerable to DOS.
  + FasterXML Jackson Databind upgrade to newest version
  + Upgrade Apache Tomcat to at least 11.1.0 or newest
  + Do not use Hibernate Validator version 6.1.2. Final.
  + Do not use Spring MVC or Spring WebFlux application to run on JDK 9+
  + Upgrade Spring Framework to at least 6.1.0
* Fixing the code error such as to put validation during user input
* Implement HTTPS for secure online access
* Implement authentication during user login and access their information
* Code reviews
* Following the government’s guidelines

It is important to value software security within a company and to monitor it every day to prevent unauthorized access, mitigate financial losses, build customer trust, and prevent potential damage in the future

* What part of the vulnerability assessment was challenging or helpful to you?

I conduct static tests to ensure that we are using the best versions of all dependencies, review the code for any mistakes to prevent security errors, and find the most helpful aspect to be the static tests. Additionally, I have learned how to effectively suppress error catches.

* How did you increase layers of security? In the future, what would you use to assess vulnerabilities and decide which mitigation techniques to use?
* Upgrade all systems from static testing result to the recommendations.
* Fixing the code error such as to put validation during user input
* Implement HTTPS for secure online access
* Implement authentication during user login and access their information
* Code reviews
* Following the current government’s guidelines
* How did you make certain the code and software application were functional and secure? After refactoring the code, how did you check to see whether you introduced new vulnerabilities?

I always check the static testing results every time I make changes to my software application. If I discover additional vulnerabilities, I recognize that the changes I've made may not be optimal, and I work to find solutions. My goal is to ensure that my code and software application have zero vulnerabilities. Additionally, I prioritize coding in a better and more secure manner, such as consistently implementing authorization checks for data access and other security measures.

* What resources, tools, or coding practices did you use that might be helpful in future assignments or tasks?
* The National Vulnerability Database is instrumental in assessing the strength of security and identifying occurrences in each version, clarifying which version is superior.
* Conduct static testing to identify vulnerabilities in the software application.
* Perform code reviews and implement using HTTPS.
* Employers sometimes ask for examples of work that you have successfully completed to show your skills, knowledge, and experience. What might you show future employers from this assignment?

My skill in identifying code vulnerabilities, understanding the importance cybersecurity in tech world and enhancing code for better security has led me to delve into Maven, where I've learned how to manage dependencies efficiently. Additionally, I've gained knowledge about the importance of using HTTPS for secure online access. I've also become more aware of security issues in my code, such as the dangers of SQL injection, the importance of multiple input validation, the significance of cryptography, and much more.