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

* + Artemis Financial is a hypothetical company for the sake of immersion. They are a multinational corporation that deals with government and overseas operations. Their area of business encompasses portfolio management, savings, and retirement accounts.

Sy is it important to code securely? What value does software security add to a company’s overall well-being?

* + On initial assessment, I uncovered several concerns about sanitation and a lack of Least Privileges. These types of oversights in combination could lead to a major data breach and cost the company gravely. Especially if the company works with the EU. The loss in customer trust would be incalculable for a corp. that deals with personal finance.

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

* + The part of this assessment I would need to spend more time on is combing through the vulnerabilities via NVD.NIST.GOV and supporting sites. This is a time-consuming task. Even with the aid of open AI 3.5 summarizing the tasks.

·  How did you increase layers of security? In the future, what would you use to assess vulnerabilities and decide which mitigation techniques to use?

* + My approach was to look at the fundamentals. ‘Quis custodiet ipsos custodes’ is a Latin saying that means ‘who will guard the guards themselves?’ I think AI is going to be at the center of cybersecurity before long. The ability to see areas of concern like access points in the 7 layers of cybersecurity and CIA (confidentiality, integrity, and availability), as well as where to gather information about known vulnerabilities (NVD.NIST.GOV and others) in tangent with access to more powerful AIs will allow for better static, white and black box testing.

·  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 used the knowledge I’ve gained from multiple cybersecurity courses and the wealth of knowledge available on the web to target my focus on areas of weakness. After that, I fell back on the help of an OWASP plugin to aid in assessing code in supporting libraries and frameworks.

·  What resources, tools, or coding practices did you use that might be helpful in future assignments or tasks?

* + I used the maven plugin for a Java dependency check with OWAPS as well as open AI to aid in the assessment of known vulnerabilities. I used fundamental concepts like Least Privileges, the 7 levels of cybersecurity, CIA, and best coding practices to spot areas of concern in the code. However, the heaviest lifting came from NVD.NIST.GOV and the development community which allowed me to find so many known vulnerabilities via the OWASP plugin.

·Employers sometimes ask for examples of work that you have completed to show your skills, knowledge, and experience. What might you show future employers from this assignment?

* + This assignment provides a glimpse of my skills, knowledge, and experience by demonstrating the following. The first thing this project shows is, that I can add edit, compile, and run a fussy yet powerful language like Java to unveil and improve security. This unquestionably displays skill beyond that of someone who can merely write code. Secondly, it shows I am knowledgeable of best coding practices, and more importantly, have the respect to understand their gravity and thus implement them beyond what I have done thus far. Third, it shows my experience by conveying my foresight into the impact of my code. This is important because without sound reasoning business objectives can jeopardize the safety and well-being of not only the company but its end users.