* Briefly summarize your client, Artemis Financial, and their software requirements. Who was the client? What issue did they want you to address?
  + The client, Artemis Financial, is a financial consulting company that develops personalized financial plans for savings, retirement, investments, and insurance for their patrons. Artemis wants to implement the most current and effective software security, specifically as it regards their existing RESTful web application API.
* What did you do particularly well in identifying their software security vulnerabilities? Why is it important to code securely? What value does software security add to a company’s overall wellbeing?
  + I believe I went well into detail about the various existing vulnerabilities found in the code base. As is highlighted in the vulnerability report, several of these vulnerabilities can result in catastrophic exposure of data – something highly damaging in the financial industry. Fortunately, most of these vulnerabilities had proven solutions, but the volume of vulnerabilities illustrates the importance of staying up to date on cybersecurity developments.
* What about the process of working through the vulnerability assessment did you find challenging or helpful?
  + The most difficult part of the process for me was the sheer number of discovered vulnerabilities given the short amount of time we had to develop this document. Had there been more than a week’s time or had I had more available time in that week, I would have liked to dive a bit deeper into the mitigation of some of the vulnerabilities.
* How did you approach the need to increase layers of security? What techniques or strategies would you use in the future to assess vulnerabilities and determine mitigation techniques?
  + The first point of reference I used in increasing security was the client’s demands. Since these were fairly vague and non-technical in their scope, I used the OWASP guidelines for secure web development. I also used the CVE database provided by the National Institute of Standards and Technology to find details on the vulnerabilities and various approved mitigation techniques.
* How did you ensure the code and software application were functional and secure? After refactoring code, how did you check to see whether you introduced new vulnerabilities?
  + Later in the course, we refactored the code base to introduce HTTPS functionality, certificate handling, and file verification via checksum generation. Using the Maven dependency tool, I was able to compare the vulnerability report before and after I refactored the code and found there were no introduced vulnerabilities.
* What resources, tools, or coding practices did you employ that you might find helpful in future assignments or tasks?
  + The Maven dependency tool was a great help in identifying known vulnerabilities. The OWASP guidelines were otherwise useful in manual identification of poor security practices. I would certainly continue to use these tools in the future.
* Employers sometimes ask for examples of work that you have successfully completed to demonstrate your skills, knowledge, and experience. What from this particular assignment might you want to showcase to a future employer?
  + This assignment shows my ability to assess the current state of security in particular code bases. I would also like to include a document from later on in the class to illustrate my understanding of certificate authorities, checksum generation, cryptographic algorithms, and HTTPS configuration – all steps I took to further secure this software.