Ethan M.E. Mills

Professor Bolton

Software Security

22 April 2024

Module 8 Journal

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 consulting company that develops financial plans for their customers, this includes savings, retirement, investing and insurance plans. They seeked outside help from us(Global Rain) to modernize and secure their operations. They want the most recent and current effective software security available. They want our help to protect the organization from external threats that could jeopardize the company and its clients. They wanted us to address the current vulnerabilities that their current security has. They also wanted to add a file verification step to their web application to ensure secure communications, they want this in the form of a checksum.

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?

When tasked with testing a client's product for security vulnerabilities, it is important to be thorough and take your time testing. For me using our software eclipse was a learning experience for me because I had never touched that client ever so this whole project and course was tough for me because I was learning as I went using it. I think I did good troubleshooting errors and problems that arose during this course. Coding securely is like making sure you lock your car when you are going into the store, if you lock your car doors when you go into a store even though there might be no crime at all like in my city where everyone knows everyone, you still cannot be too careful. Even though you know it will never happen it is still good to practice securing your belongings, you can apply this to coding. Sometimes you might not need to code securely but it is good practice to do so when you need to code securely it is already something you do. Having software security is just as important to a company as locking doors when closed. Why not go the extra mile to secure your business even though nothing has happened? You do this so that when something does happen, someone tries to breach your company, you are already prepared with the software security measures that are in place, just like if someone tries to break into your business after hours, the doors are locked and secure, not allowing them to get in.

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

For me, like I said, this whole course was a little rough for me. It has been 2 semesters since I took a coding class so I was a little out of touch which is my fault for not staying on top of my knowledge and languages that I have learned thus far. To top it off, never using eclipse ever was very challenging to me, spending hours trying to figure out how to even upload a project to be able to work from that work space. But through youtube videos and forums I was able to learn and get better at using the client. I personally think that the client is very outdated and is not a good client at all. It is a free client and it has been around for a while so it does have a lot of features that not many clients have. Through trial and error I was able to slowly get the hang of eclipse, I do not mind the client anymore compared to the start of the class when I was getting frustrated and unable to do basic 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?

Throughout this course we were tasked to secure Artemis Finacial’s software, in the midst of that I discovered SHA-256. SHA-256 is one of the most used encryption algorithm ciphers used today. Myself and I am sure many other people in the course decided to go with SHA-256 because of its success in being one of the strongest has functions available .With the knowledge on software security that I have now and the knowledge using maven dependency, I now have maven at my disposal to do basic vulnerability checks for software.

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?

After doing the Maven Dependency checks a html is produced in the target folder that brings you to the dependency check report that allows you to see all vulnerabilities with said code. It breaks down what the vulnerabilities are and what level they are. This allows you to access the code and do what's called a suppression. When you can suppress false positives for vulnerabilities to better see what is actually going on with said code. Once you do said suppression for the x amount of false positives you can run another dependency check report and check how many vulnerabilities are actually left and how many that are now suppressed, then you can move forward attacking said vulnerabilities.

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

With the knowledge I now have on Maven and spring tools, I am confident with these tools I am able to correctly assess code and be able to secure code confidently. Although I am not a fan of the client Eclipse I am now more confident using the client, the tools and resources available with Eclipse. After taking this course I now know the importance of coding securely as you go to help mediate security vulnerabilities either in the present or in the future.

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?

If I was asked to speak about my skills and success in the Software Security department, I would tell them about this course and its assignments. I would tell them I was able to assess a project's security vulnerabilities using the client Eclipse with the plugin Maven Dependency check. I would tell them I am capable of incorporating said plugin into a project, populating a report on said project and being able to read and assess the report on the project. I would also include that I practice coding securely with all coding that I do to better mitigate any type of security concern. Lastly I would include that I am able to troubleshoot problems that arise when doing this type of coding.