8-2 Journal:

Portfolio Reflection

Karen Bevis

CS 405 Secure Coding

Southern New Hampshire University

08/21/2021

This is a course that I had to take a second time here at SNHU. The first time that I took it, I had some extenuating circumstances that caused me to turn in my work very late. Due to SNHU policy, the Professor would not accept any of my late assignments therefore making me have an F in the class. When I came into this class, I had a very bitter attitude. I do understand policy and I don’t expect better treatment as I understand excuses. I work in for the IT Department at a local college. To say the least I was very dismayed and to be honest, I was more than depressed.

Things happen for a reason though because within one session with Professor Mills and I learned more in 15 minutes than I had the whole semester in the other term. I was amazed! Also, there were other things that helped me with this class. After that one session, I was more inspired to go back and redo my coding assignments as none of them had worked in the previous semester. I didn’t fully understand them how to make the code work out. Professor Mills helped not only my attitude but helped me to understand the coding assignments in a way that I did not think was possible. There was another student in the class that was a huge help as well. I was able to get my curiosity as well as strive to finish up back. So, thank you, thank you, thank you!!!!

Now I am on the reflection portion 😊

Developers must understand what secure coding is in order to design and develop it. So, what is secure coding? According to an article in Software Testing Help, the definition of secure coding is to “design and develop software by avoiding the weaknesses that lead to security-related vulnerabilities by adhering to specified security standards, and industry best practices.”

As I studied the secure coding standards and how implementing them throughout coding, it also impressed on me that this is the way that things should be done in everything in life. Protection is key! Although, we are mainly talking about securing code, this will also give me the tools needed for my career. I will take what I have learned and use it in my professional development. Taking the principles and the coding standards will be a nice addition to my cyber playbook as well.

Security should never be put off to the end whether that is in coding or in networking. All of it works together to secure data for the clients.

In many organizations change is hard for people, take security for example. People just want to access their “stuff”, do their jobs and go home! What most of them don’t understand is that when they can access their “stuff” freely without any restrictions, they are most likely compromising the network and if they can access their “stuff” without any restrictions, so can anyone else. This is where the IT Department is looked at as the “bad guy” for implemented security controls! Believe me! I have been on the receiving end of some of those calls. What some of the end users don’t understand is that all of this has been discussed, evaluated, and assessed by all the people at the top. The benefits far outweigh the risk and security is implemented. I work for a local community college in the IT Department. Our users were able to login with a username/password into their accounts. Several years ago, we implemented 2FA. Now before we did this, we sent out emails letting them know it was going to happen. To prepare them, we sent out emails several months in advance, then another one 2 months in advance, then another 1 month in advance, then another 1 week in advance, and the final email went out the day before. How many calls do you think our IT Help Desk got on the day of the switch and the weeks after? People don’t like change for sure and they don’t care for security!

I would recommend that all companies have and implement security policies into their organizations. The security policies would need to fit the organization as not all organizations are the same. Policies/procedures should be strong and in place from the start. If the organization doesn’t have a policy or procedure, how do the people know what they are to follow? They should be given out at new employee orientation and updated on a regular basis.

One of the things that I was really impressed to learn about was the Zero Trust Networks. I will go forward with this and keep learning about these networks. The videos that we had for Zero Trust Networks has also helped me on a project that I am working on at work.

This course has helped me with my professional career as I am deeply involved with a new company that is developing a new software project. Although, I don’t work directly for the software company; my co-worker and I are directly involved with helping to shape the outcome of the way the product will eventually turn out as we are helping to test the product. This has been a tremendously long and tedious process but it will be so worth it in the long run, for education as we know it and especially if this software company can bring the Windows platform up to sped with the MAC platform.

**References**

Secure Coding Guidelines And Best Practices For Developers. (n.d.). Www.softwaretestinghelp.com. Retrieved August 22, 2021, from <https://www.softwaretestinghelp.com/guidelines-for-secure-coding/>