8-2 Journal: Portfolio Reflection

Antonio Sobalvarro

CS 405 Secure Coding, Southern New Hampshire University

Professor West

August 21, 2022

The importance of not leaving security to the end has been a constant reminder throughout this class and throughout this degree program. Leaving security to the end can prove disastrous on many levels, but especially on a financial and time-scope level. What I mean by this is that updating code or trying to fix an entire program after a problem has taken root can prove very costly because of the resources that would be needed to fix the issues or even the additional programmers to consult with; as for time-scope, it can take many hours, and perhaps days, to remedy an issue that could have been avoided by not ignoring security during the development process. This class also served to, once again, highlight the added importance of adopting a secure coding standard that everyone can adhere to in order to assure that the system is protected at all stages of development, no matter who is working on it. This also serves to protect the system from the inside out because many layers of protection can be built into the system, thus providing added security that protects from outside threats.

Another important topic from this class was the value in having a system by which to evaluate and assess risks. Having such a system in place not only allows everyone to be on the same page and attack the threat using the same parameters and implement effective defenses, it also saves money by ensuring that a problem is attacked and defeated early on before it can escalate into a bigger issue that can, and very often times, does prove extremely costly.

I’m personally glad to see that zero trust has gained more ground and that it will seemingly continue to do so as newer systems are built. Some people might argue that this policy only serves to make a system cumbersome to users with the constant authentication process, but I think it’s safe to argue that it is better to have users navigate these hurdles if it means that they can be provided with a secure system, where their private information is safe.

Threats are constantly evolving, and security policies need to keep pace with this reality. As we become more reliant on technology for a myriad of reasons, developers need to recognize the undeniable risks that present themselves with each new threat. The best way to protect a system is to integrate security at the core and to implement it at every stage in order to provide the highest levels of protection. Many programs and systems now contain mass amounts of personal data that need to be protected; this is especially true for large companies, and their success and/or reputation sometimes hinges on how well they can protect such data. The best security offers the highest protection due to its deep integration into the system itself, while also keeping up to date with new threats and such a system should always be the best that money can buy – it’s better to spend a little extra and avoid headaches down the road.