Module 8-2 Journal: Portfolio Reflection

Anthony Lee

SNHU

CS-405-T2851 Secure Coding 22EW2

Professor Aaron Demory

December 17, 2022

During this course, I learned many new techniques, philosophies, and strategies for improving secure coding. One of these are adoption of a secure coding standard and not leaving security to the end. The purpose behind adopting a secure coding standard is it helps mitigate possible vulnerabilities in security and works to remove errors that can put a system at risk (Foster, 2020). We used SEI CERT coding standards, although there are many other standards out there. SEI CERT coding standards works primarily with C, C++, and Java. As for not leaving security to the end, the philosophy behind this is to develop code that preventatively remove risk and tighten security from the start. Like how a chef season throughout the cooking process, developing code with secure measures from the start means that there is security in place throughout the code, making for an overall more secure finished product. Leaving security to the end will likely require rewriting code and testing, increasing the overall cost of development. It is always better to be proactive than reactive.

Evaluation and assessment of risk and cost benefit of mitigation is another topic we covered in this course. This framework is about the risk, costs, and benefits of adopting a particular practice or standard. We used a table to illustrate and identify threat level, severity, cost of remediation, and overall importance of errors and threats. We also discussed in this course the risks of waiting to implement security and the benefits of implementing early. It is always better to be proactive by developing with security in mind during development than to react to an attack (Bellairs, 2019). The cost of remediation will always be much higher than the cost of developing code with security in mind.

One topic we covered in this course is the AAA framework. One part of AAA framework in “Zero Trust”. The standard most people use is to trust but verify; people are not distrusting, but we need to verify access. Zero trust means to believe no one is safe and not to trust anything (Pratt, 2018). This means we need to verify everything, and nothing is safe.

Implementation and recommendations of security policies I can give now would be to always keep software up to date, not leave security to the end, follow AAA framework, and to install firewalls and other software for security software as a part of security and defense.

References

Bellairs, R. (2019). *What Is Secure Coding? | Perforce Software*. Perforce Software. <https://www.perforce.com/blog/sca/what-secure-coding>

Foster, S. (2020). *What Are Security Standards? Secure Coding Standards Overview | Perforce Software*. Perforce Software. <https://www.perforce.com/blog/qac/secure-coding-standards>

Pratt, M. K. (2018, January 16). What is Zero Trust? A model for more effective security. CSO Online. <https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html#:~:text=Zero%20Trust%20is%20a%20security,to%20don’t%20trust%20anyone>.