Darrell Chism

CS-405

02/26/23

Southern New Hampshire University

8-2 Journal: Portfolio Reflection

* Adoption of a secure coding standard, and not leaving security to the end

As we have learned throughout this semester, ensuring data security is vital, whether it be company data or user data. As software engineers, we play a direct role in the safety of those who use our software. If we are asking users to input sensitive information, such as SSN, first and last name, birthday, etc.. we need to ensure that our defensive security layers are done properly. Not only this, having a secure coding standard means that our work has as few vulnerabilities as we can manage. Obviously, we will never be able to eliminate 100% of vulnerabilities, but we can still try.

* Evaluation and assessment of risk and cost benefit of mitigation

Spending the extra money to ensure that defense is not an afterthought outweighs the cost of repair. As our software reaches the hands of users, there is a level of trust that the developers had the best intentions of the user in mind. If a security breach takes place and their information is stolen, you have broken that trust and lost your reputation. It isn’t just money that is lost when these types of things happen, your companies reputation and your reputation is at stake.

* Zero trust

Do not trust anything not written in house. Anytime you need to input data that is not developed by you or your fellow engineers, default to the thought that the data you are inputting is not safe. Follow the correct protocols to ensure that the data is scrubbed and is safe.

* Implementation and recommendations of securities policies

The zero trust that I just discussed above is one of the things that need to go in your company’s security policy. Your security policy should be written for you and your company, but I have a few suggestions: adhere to the principle of least privilege, practice defense in depth and adopt a secure coding standard. Adhere to the principle of least privilege means to design your software to only give the user the least amount of privilege to do what they need to do. This keeps users who have malicious intent from doing anything. Practice defense in depth means to have multiple layers of defense, along with staying on top of new vulnerabilities being used. Lastly, adopt a secure coding standard means exactly what it says. Learn how to properly code, following all principles and standards and never cutting corners.