8-2 Journal: Portfolio Reflection

Written by: Leah Marshall

* Adoption of a secure coding standard, and not leaving security to the end & Evaluation and assessment of risk and cost benefit of mitigation

While coding any piece of software, it’s important to concentrate on the security aspect. The statement “Don’t leave security to the end” essentially means that security shouldn’t be an after-thought and should be thought of during the entire process of creating this software. Adoption of both a secure coding standard and not leaving security to the end ensures a cost-effective way to mitigate potential risks and threats. By not leaving both aspects to the end, you are preventing a massive “blow-up” later on in the line, which would be a hefty cost to fix.

* Zero trust

A zero trust policy ensures everything is checked out and thus verified as not everything is automatically trusted. Especially with the rise in remote work and the cloud, it’s imperative to ensure no stone is left unturned.

* Implementation and recommendations of security policies

A few recommendations for this system would be to simplify these standards for non-technical users as having all employees, not just those working with code, to understand and implement these standards is important. Moreover, emphasizing the importance of these secure policies to non-technical departments will help reduce the chance of phishing scams or other social engineering attacks.

References

Marshall, Leah. (2024). 6-1 Journal 405. Unpublished Manuscript, Southern New

Hampshire University.

Marshall, Leah (2024). CS 205 Project Two Script LM. Unpublished Manuscript, Southern New

Hampshire University.