Devin Wheeler

06/29/2025

8-2 Journal: Portfolio Reflection

Adopting a secure coding standard early on is very important because it can help catch issues before they grow out of control. If you wait until the end to add/think about security, it can become very expensive and much more complicated to fix. Using secure coding guidelines such as input validation, proper error handling, or even just Triple-A policies can make applications much stronger and secure from the start.

Looking at risks and weighing the cost and benefit of fixing a problem is also critical. Some risks are too big to ignore no matter the cost, while some might be ok to leave until you have the time, manpower, or money to fix. Xero trust supports this by assuming no user is safe or ius who they say they are. It requires verification for every action, which is great for a security forward approach but a little but annoying for users.

To help protect systems long term, it’s smart to recommend clear security policies from the start. These could include Authentication, securing data, regular updates, and least privilege access. It’s also very important to add layers of DiD, if one security measure was overlooked or failed it’s critical to have a backup or two to minimize damage. These steps can help to build a secure foundation for any application and help prevent breaches before they happen.