Portfolio Reflection

CS-405 Secure Coding

Mitchell Cabral

April 22nd, 2024

It is important to adopt a secure coding standard and not leave it to the very end. Secure coding practices are crucial when it comes to building strong and resilient software, adopting a secure coding standard ensures that security is a continuous thought throughout the development process and not an afterthought. It is good to start early when it comes to security, follow industry best practices, automate security checks, and even train staff to be aware of security flaws.

Evaluation and assessment of risk and cost-benefit mitigation is all part of the process of keeping a secure system. Identifying assets then possible threats towards then will help you be able to break down and prioritize what should be addressed first. Practices like creating risk matrices or qualitative assessments can help a team be able to start with the top priorities or most vulnerable first.

Zero trust is a security practice that assumes no trust, regardless of the location of the user, which could be inside or outside the network. Implementing a zero trust system would mean authenticating and authorize based of available data points, limit user access, assume breach from any request as if it came from an outside source, and have an end-to-end encryption. This type of practice can help keep a system safe and secure from possible attacks.

Some implementations and recommendations of security policies would be to develop policies around the company's business objectives, make sure they are comprehensive, and define how they will be enforced. Making your staff aware of what's important to protect the system will help keep everyones data protected. A system is only as safe as its security policies.