Chris Blair

CS-405

12/16/2023

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

Having a secure coding standard helps protect against potential attacks from hackers. Leaving as few as possible vulnerabilities in your code and starting from a secure foundation will set you up for success. Not leaving security to the end can start from the very beginning of the project when you’re designing your application.

**Zero trust**

Zero trust is a good process to implement in your application because it doesn’t have any real effect on end users, but keeps your code and application secure. Assuming no trust from anywhere in the application is a good practice in general.

**Implementation and recommendations of security policies**

Implementing your security policy as a first initial step in the process is the best. If it cannot be done first, it should be done as early in the process as possible.