Vincent Snow

CS 405 – Module 8 Journal

2-27-2024

Adoption of a secure coding standard helps keep a development team using practices that prevent problems before they start, and uses standards developed over time through experience and reflecting on observed vulnerabilities and attacks. These standards are part of a DevSecOps process that keeps security in mind rather than leaves it to the end. Incorporating security along the way rather than leaving it as a step on its own later in the process saves time, hassle, and money as well as better protects your users.

Using security tools and coding standards and changing to a DevSecOps operation may be an investment at first. It will take training, new tools, and perhaps more time up-front during the development process. A product could be released quicker under a regular DevOps process. However, the benefit of keeping security in mind sooner is greater than this up-front investment. You will avoid many common problems and be able to deliver a better-quality experience to user immediately and be able to handle problems more quickly because of AAA security and logging, as well as your unit tests and assertions narrowing down a great deal of potential causes of a bug or vulnerability.

Zero Trust is the mindset behind good security. We should never trust anything that we have not confirmed. The value of a variable, the output of a function, the input from a field, or the identity of a user should never be assumed. Doing so opens the door for attacks and bugs. If we never open that door in the first place, we save ourselves the trouble of dealing with these issues at all. There is a tradeoff between user experience and good security sometimes, so these options must be weighed and discussed. Ultimately, we must keep in mind that the user experience will be very unpleasant when the service is disrupted, or hackers obtain their personal data. So, this must be prevented and handled effectively.

Security policies can always improve. They should be reviewed for holes in the plan, and implemented at part of a defense-in-depth strategy that employs security measures at every physical and digital entry point in a system or program. There is physical security of the building where equipment is stored and monitoring of activity in the building, and then there is digital security such as authorization at every API call and monitoring of user activity. Together these layers all create an effective modern approach to cybersecurity.