8-2 Journal Danielle O’Bier

Site Protection and Trust

Having your own secure coding standard policy is a good way to keep in mind the security required in each project. The saying not to leave security to the end refers to the idea to incorporate security procedures throughout the development process and continue to do so in the review and update. One layered security is defense in depth. With the idea of putting up multiple layers of defense making it harder to hack.

The concept of making security a point throughout the development allows developers to avoid unnecessary steps in building the site. It continues to protect against basic hacks. Protection of your site just like your home must be a thought process. While we never expect our homes to be broken into, just like our sites, it can happen. Therefore, it is important to implement protocols to stop or hinder an attack. It gives the developer the advantage of either stopping an attack or finding the leak quickly and ending it as soon as possible.

When looking at protection it is important to include the zero-trust policy. Accepting that our world is changing and that we can now access information from any location. The best way to protect, is to give access, without giving too much trust. The zero-trust policy requires users to sign in and masks whether they are signing in through the cloud or through the premise making it harder for attackers to access whatever they want.

There are many tools we can use to help in attacks such as Cppcheck and infection monkey. It is important to use as many protocols and tools as possible to ensure protection. The last thing any developer wants is to lose all their hard work to an attacker and lose the trust of their clients. By designing their own security policy, the developer has the advantage of focusing on specific aspects. This policy can easily be changed with time with certain policy becoming more important over time.