Bob Johnson

CS-405 Secure Coding

12/13/2022

8-2 Journal Portfolio Reflection

With the vast number of ways a system could be attacked and compromised, it is necessary for every company that handles data to adopt a secure coding standard and not leave security until the end. Companies should start projects with security in my from the very beginning. A security standard allows a company to have rules set for everyone involved to follow and know what is expected when it comes to implementing security. This also allows some security for the company by having a standard in place that shows the company is doing something to protect employees, clients and privileged information. By utilizing defense in depth and triple A policies, this makes projects secure over various levels since more than one layer of security is in place. By requiring users to verify identity and log their activity, this results in a log of who did what and when in case an issue arises. This information provides easy access to help identify a problem as well as fixes to any damage done and insight into ways to prevent future issues of the same type. These policies may slow down a project initially but can help prevent developers from adding security as an afterthought or worse, waiting to see if an attack happens and trying to remedy the situation after damage has been done.

With deadlines and budget in mind, there may be a time where every issue cannot be rectified immediately. Luckily we have tools available to use to help prioritize vulnerabilities like Cppcheck and websites to help us prioritize the order. While every vulnerability should be addressed, it’s nice to see what a vulnerability entails and how serious it is. The confluence website is a great tool for this. It allows developers the chance to evaluate and assess risks so that serious issues can be handled immediately and help keep projects on time and within budget.

With how dangerous it is on the internet and how advanced tools have become for people to gain access to information, often with malicious intent, the policy of zero trust can be used to help protect users and information. Using technology building blocks like transport encryption and session protection, this helps implement least privilege access and allows users to complete work. It only gives access to parts of a system necessary to complete work and helps keeps systems secure. Since limiting access can impact the user experience, using tools like single sign-on provides some security and helps with the user experience. Developers can also use isolation with applications to help with everything running smoothly and being secure.

My recommendation is for companies to implement a security policy and follow it. It would also be wise to keep it updated as time goes on. People will come up with new ways to break systems and gain access to sensitive information. Developers and companies need to be careful so they don’t get to comfortable and forget that things evolve with time, or worse, start to make exceptions and shortcuts when it comes time to implement security. By keeping DiD and triple A policies in mind from the beginning, this helps ensure systems, developers, users and information stay safe and secure.

References:

*A Practical Guide to Zero-Trust Security*. (n.d.). Threatpost.com. <https://threatpost.com/practical-guide-zero-trust-security/151912/>

*Confluence Mobile - Confluence*. (n.d.). Wiki.sei.cmu.edu. Retrieved December 13, 2022, from <https://wiki.sei.cmu.edu/confluence/plugins/servlet/mobile?contentId=88046682#content/view/88046682>

Dunham, R. (2018, July 26). *Information Security Policies: Why They Are Important to Your Organization*. Linford & Company LLP. <https://linfordco.com/blog/information-security-policies/>

‌