James Soto

8-2-2023

CS-405 Secure Coding

8-2 Journal: Portfolio Reflection

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

It is important for the development team to adopt secure coding standards early in the development process, and not leave security to the end. Secure coding standards are a set of rules and guidelines like those provided by OWASP, SANS or CERT, that developers could follow to write and produce more secure code. These standards can help the developer prevent some of the most common security vulnerabilities such as SQL injection, buffer overflows, and cross-site scripting.

**Evaluation and assessment of risk and cost benefit of mitigation**

When evaluating the risk and cost benefits of mitigation, it is important to consider the likelihood of a threat occurring, the impact of the threat if it does occur, and the cost of mitigating the threat. To determine the likelihood of the threat occurring, the team would assess the organization’s security, most vulnerable areas within the organization, and the overall company profile. While every organization should consider the risks of a security threat, bigger organizations or organizations that hold data or secrets have a bigger potential to threats. The impact of the threat can be assessed by considering the integrity, importance, availability, and confidentiality of the data that is being protected. Lastly, the cost of mitigating the threat can be assessed by considering the costs of implementing the security controls the organization would put in place, the cost of training the development team, and the cost of any losses.

**Zero trust**

The zero trust policy is a security practice that assumes that no one, not even a user inside the network, can be trusted. The concept is that all access to any resources must be verified, regardless of where the user or device is located. Zero trust shows that security should be implemented in terms of least privilege, where users are only granted access to resources they are approved for or what is necessary to do their jobs. Zero trust is a more secure approach than the traditional security models that rely on perimeter security to protect the network. As we know a hacker could gain access to a network through a vulnerability in the network’s infrastructure or by hacking a user.

**Implementation and recommendations of security policies**

Security policies are a set of rules that an organization puts in place to protect its data, infrastructure and systems, based on the risk and threats that they face. The organization would perform a risk assessment, to understand any potential risks and threats the organization faces, so they could focus on the areas that are most vulnerable or areas that contain sensitive data. The security policy should cover all aspects of the organization, including network security, access control, data security, compliance and incident response. Every employee within the organization needs to understand the security policies and they should be provided training to ensure that the policies are understood and followed. Management needs to enforce and monitor the compliance of the policies to ensure the effectiveness. Lastly, the policies should be reviewed and updated based on the landscape of the organization.