8-2 Journal

Aaron Campbell

CS-405-T4240 Secure Coding 23EW4

Southern New Hampshire University

Professor Mike Prasad

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

I’ve mentioned this in previous discussions/journals, but I believe that while adopting a secure coding standard might add a monetary and time cost to a project from the start, it will ultimately save money and time down the line. It is much more difficult and expensive to address security issues post-deployment than it is to account for them in the beginning. However, doing this does not guarantee the complete eradication of vulnerabilities. Some are still bound to be found after deployment, but by adopting a secure coding standard, it should be easier and cheaper to address them.

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

In general, I think that medium or high risk vulnerabilities should always be addressed regardless of the cost to do so. The only exceptions could be vulnerabilities that are very unlikely to occur, in that case the cost to remediate should be taken into account. For low risk vulnerabilities, I would save these for last, and take into account the time and monetary cost for addressing them.

1. **Zero trust**

In future projects, I will strive to adopt a policy of zero trust. After looking into this policy, I believe that it is an essential policy when designing a program that either houses sensitive data or interfaces with other systems or connects to a network. For programs that do not house sensitive data or interface with other systems, I do not believe that this policy is necessary, although it would still be best practice to implement it regardless.

1. **Implementation and recommendations of security policies**

I spoke about this prior, but I believe now that it is necessary to implement a security policy from the start, despite the investment it requires. As mentioned, adopting a security policy will help in not only making a more secure program, but will help reduce maintenance and vulnerability remediation costs down the line. When recommending security policies to others, it is important to consider the program being worked on. Not every policy is the same, and one might be more appropriate than another. For instance, a security policy might emphasize a certain vulnerability, and if the program being worked on is not susceptible to such a vulnerability, it would be better to adopt/recommend another policy in its place.