8-2: Portfolio Reflection

Stephen Blackburn

Southern New Hampshire University

# Reflection

It is important to adopt secure coding standards, which help make sure the system doesn’t have any vulnerabilities that could lead to damage to a system, loss of money, remediation costs, and data leaks. This class has shown me how writing simple SQL statements can be disastrous if implemented incorrectly from SQL injection. This is just one example as there are many other things such as buffer overflow and underflow. In many classes it was important to write code that works, but aside from the code doing what it was supposed to do, I didn’t really check or now how to check if it was secure or not. After this class, I look at coding in a whole new way and will be critical of how and what I put in the code and continue to test it. It is also important to not leave security until the end. Most company’s use an agile approach now, which means testing and security is implemented in every step, yet somehow companies are getting breached. I think that’s why it’s important to also implement DevSecOps. A company could pay a lot of money for security and might not want to spend that much at first on security, but ultimately security will save them money and their reputation. The Zero Trust Policy is a great. It states that no device or user can be trusted, inner or outer of the perimeter. It often has multifactor authentication, which is annoying, but works great. In my opinion, every company should implement secure coding standards, Triple-A, encryption, DiD and the Zero Trust Policy, which would make the company about as secure as it can be.