Adoption of a secure coding standard is important so that everyone working on the program knows what needs to be done. Having clear rules makes it easier to implement different security aspects such as prevention of a SQL injection by using prepared statements and validating the length of a username. Another important part of security is not leaving it until the end. You need to design your program with security in mind from the very start such as the use of unit testing. Design the unit tests first then develop code to satisfy those tests. Leaving it until the end can be extremely risky as you are more likely to miss a vulnerability as well as the cost of mitigation will be greater, especially if something needs to be completely redesigned to fix the vulnerability.

When a vulnerability is found, an assessment needs to be made on the risk and cost benefit of mitigation. For example, if the vulnerability can lead to a major data breach, this can be extremely costly. The brand name can be destroyed and a complete loss in trust from the users with the company, therefor, even though the cost of fixing the vulnerability may be great, it won’t be as great as having a major data breach. On the other hand, if the vulnerability is minor, it may not be worth it to completely fix the problem. Spending extra time and money into making something as secure as fort knox may not be necessary if you’re not dealing with sensitive data. Find the right balance of security is critical.

One key aspect of development is to never trust the user. You need to assume the user will have malicious tendencies and plan for them to act as such. For example, a typical user won’t try to have an extremely long username, but a malicious user might test the limits which could lead to an overflow. Another important part of this is giving the user the least number of privileges necessary to handle their role. For example, the average user shouldn’t have admin privileges as that isn’t necessary to complete their tasks. Also, a user for one sector shouldn’t have access to another sector unless there is a legitimate reason to do so. This can prevent a larger breach since even if a user account is compromised by a hacker, they won’t have free reign over the system.