Aamir Rahman

CS405 Secure Coding

3/4/2023

# 6-1 Journal: Don't Leave Security to the End

Security is very important in all aspects of our lives. Security is also very important for software. Security is important to protect user data and protect the software that’s created to make sure it doesn’t get hacked. The statement “Don’t leave security to the end.”, means exactly that. Security implementation should not be left until the end. When creating software and building applications, security should always be in mind. It’s ideal to consider security implementations and figure it out as part of the design in the early stages rather than later. It’s important to consider safety implementations early in software design rather than the end, to avoid flaws in the system.

There are various security implementations that can be part of a software design and build process to system hacks. Multi-factor authentication can be implemented to improve software security, so the users have to go through various security “gates” to get to the user data. This multilayer security authentication will greatly improve software security. Testing has to be complemented to verify security measures implemented are actually working. Thorough security testing has to be completed prior to software release to make sure the software is secure and protected. Software security measures needs to be kept updated to the latest and greatest to make sure security breach does not occur.

The use of unit testing is a great way to make sure security is implemented correctly. The developers writing the code needs to write proper and precise unit tests that can be executed. If these unit tests are automated, even better. It’s a terrible idea to leave security implementations until an issue/bug/defect is discovered. It’s better to flush out security concerns early on rather than someone discovering these security flaws when it’s delivered to the customer.