# CS 405 Project Two Script Template

Complete this template by replacing the bracketed text with the relevant information.

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello everyone, this is my presentation on security policies. |
| **2** | When defending a system, more than one defense is always needed. There is no golden software to protect the system from all threats. The system should have multiple layers of defense to protect from all threats. Some examples are a firewall, malware protection and a VPN. |
| **3** | The automated levels that be implemented to detect these coding vulnerabilities are Likely: threats that have high possibility of occur, Unlikely: threats with less possibility to happen, Priority standards: standards with high relevancy and Low priority standards: standard with reduced relevancy. |
| **4** | These are the 10 principles of coding standards in addition to examples where these standards are being used. |
| **5** | This system prioritizes each instance based on the likely hood of the threat happening. Threats that have a higher chance of happening have a high priority. |
| **6** | Encryption in flight is the process of encrypting data as it is getting transferred. An example of that is when visiting secure websites, there is a protocol for HTTPS instead of HTTP.  Encryption at rest is ensuring data is safe from hackers. An example of this is encrypting your hard drives. The hacker might be able to get into the computer but without the key, can’t access the data.  Encryption in use is allowing access to encrypted information at rest or in flight. |
| **7** | Authentication is the process of confirming who is getting access to the system. This is done with passwords and usernames. A more modern version is 2 step authentications in addition to biometric login.  Authorization is the process of giving certain parties or groups certain privileges in the system. Not every user in the system needs full administration commands.  Accounting is monitoring all activity in the system making sure to keep track of all changes in case of a break in. |
| **8** | Unit Tests are important at the beginning of the project in addition to throughout the project. It can isolate the code and test it to make sure there aren’t any issues with continuing to use it. If used correctly it can detect flaws early in development that might cause major issues in later stages. |
| **9** | This diagram shows the DevSecOps automation process. By following this, the product can be automated and have fewer human interactions when running. |
| **10** | * Automation is the act of developing and implementation of technology to deliver goods and services with close to no human intervention. The DevOps process is used to speed up the production of the product and ensure the process can continue without human intervention. This process ensures that planning, building, design and testing will be monitored to ensure everything is going smoothly in addition to making sure the security is up to date. * The compiler is a great tool to use when developing applications. It can help detect bugs when coding and lets the coder know where it’s happening. * Cppcheck is also a great tool to use to see where there are unused variables or code that is not needed. It also detects syntax errors and other types of errors as well. |
| **11** | * There is always risk in the security department when coding since nothing can ever be 100% secure. * There are many factors on what could be the issue, like bad authentication, bad coding practice, and other flaws that could give the users issues. * To prevent these issues, there needs to be a good coding practice in addition to communication with the team. This can help ensure that security is in mind from the start of the program until the end. * The benefits of this are by starting early with the security portions of the project, this will cause less issues in the later testing of the program. It’s easier to add security as you go instead of doing it all at once at the end. |
| **12** | The system should always be monitored in case of security threats. By monitoring the activity, there is a chance issues can be found earlier preventing a data leak.  The code should be simple and to the point. Each function should only have one duty, by simplifying each function to do one task, this will prevent bugs and issues.  When coding and setting up security, feedback should be received from clients or other coders and then implemented to help the system stay healthy. |
| **13** | When coding, it’s important to develop a skill to make sure the program starts and ends with security in mind. This skill then needs to be maintained throughout the career in coding. By using encryption, privacy and data needs to be secure for all parties connected to the application. |
| **14** | N/a |