# CS 405 Project Two Script Template

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

| **Slide Number** | | **Narrative** | |
| --- | --- | --- | --- |
| **1** | |  | |
| **2** | | Security policy set the standards, guidelines and best practices or procedures the organization should follow to reduce risk of vulnerabilities during the software development.  The goal is to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication, and availability. | |
| **3** | | This threats matrix indicates the risk associated with these rules, and the severity for each case, ow they are likely to happen, and the remediate cost. | |
| **5** | | Identifying security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements. This table show top 10 security principles in SEI CERT Coding practices that developers should follows for better software security. | |
| **6** | | Always follow coding standards and best practice to minimize risk.  Think of coding standards as a set of rules, techniques, and best practices to create cleaner, more readable, more efficient code with minimal errors. They offer a uniform format by which software engineers can use to build sophisticated and highly functional code. | |
| **7** | | The protection of data at rest , in transit and in use is crucial. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).  Make sure data are encrypted. | |
|  | Confirm users are who they claim to be, authentication, and session management is critical to protect against authentication-related attacks. | |
| **7** | | Unit testing  This code is an example of signed integer overflow. Signed integer overflow is an undefined behavior . it is important to ensure that operations on signed integer do not result in overflow, and Integer operations will overflow if the resulting value cannot be represented by the underlying representation of the integer.  This code is a perfect example of integer overflow when adding two value greater that maximum integer. So, the best solution is to ensures that the addition operation cannot overflow, regardless of representation | |
| **8** | | Always used automation to detect vulnerabilities that we may not see. There are so many tools available that can help build secure software. They can be used for vulnerability scanning, static analysis… so on.  Thinking about DevSecOps will help build a robust software.  But what is DevSecOps | |
| **9** | | To put it simply, DevSecOps refers to integrating security into your software development life cycle. So, a DevSecOps pipeline is a set of security practices incorporated into your SDLC to build, test, and deploy secure software faster and easier | |
| **10** | | The benefits are:   * Earlier identification of security vulnerabilities. * Improved speed and agility for security teams. * Secure software development. * Faster recovery speed in the event of a security incident | |
| **11** | | The recommendation I will give for a secure software development are follow:  Follow secure coding guidelines.  Build security into your application.  Scan and secure open source and third-party components.  Validate input data, content types, and responses.  Detect and block unusual behavior.  Automate security testing and protection.  Use a SAST tool to ensure that your code is secure, safe, and reliable. | |
| **12** | | Never leave security until the end, it will get harder and expensive to fix security related issues. Always implement security at early stage of the SDLC, and user proper tools to verify security is put in place | |
| **13** | | [Insert text.] | |
| **14** | | [Insert text. | |