# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Welcome Green Pace to the Security Policy Presentation. |
| **2** | Let’s talk about defense in depth. As the illustration shows, security has many layers. Defense in Depth is a plan that practices implementations of multiple security layers to protect an organization’s assets. When one layer is broken, another layer may hold against a threat. |
| **3** | I have compiled a list of 10 security threats in coding practice. The matrix places threats in likely, priority, low priority, and unlikely. As a summary, the higher the likelihood, the higher the priority. In vice versa, the lower the likelihood, the lower the priority. |
| **4** | Here are the 10 coding principles. Validate Input Data, Heed Compile Warnings, Architect and Design for Security Policies, Keep It Simple, Default Deny, Adhere to the Principle of Least Privilege, Sanitize Data Sent to Other Systems, Proactive Defense in Depth, Use Effective Quality Assurance Techniques, Adopt a Secure Coding Standard. Security threats are listed next to each one. |
| **5** | This table shows the rule violation and many field topics such as severity and likelihood. My ranking is shown to the right of the table and is based on the following importance: priority, likelihood, remediation cost |
| **6** | Here are 3 stages of encryption strategy.  Encryption in rest is encryption of data that is stored on disk or hard memory. Most of the data is meant to be private and kept confidential. Using role-based accounts authentication and multi factor authentication are ways to secure data.  Encryption at flight is encryption of data that is in transit. Data moves fast all the time from client to server. Maintaining a secure network and proper security transfer protocol transfer data securely. A VPN is a tool that provides private, encrypted access to a network.  Encryption in use is encryption that prevents data visibility when data is at rest or in motion. Encryption in use covers access to databases and websites, and cloud infrastructure. Defense in depth is a strategy that adds multiple layers of security features to the customer. |
| **7** | I will discuss Triple A framework as a security practice.  Authentication uses user logins, passwords, RSAs, network sign ins, fingerprinting, MFA, and so on to check the identity of the user.  Authorization gains the role to do certain tasks. Enforcing policies determines the activities, resources, and services that are in use. Certain security levels give the user the ability to change personal data in a CRUD (create read update delete) application.  Accounting uses the features from authentication and authorization to keep records. The amount of system time or amount of data tracks the user during a session. Logging these statistics may prove to be an indicator of unauthorized use. |
| **8-10** | Unit Testing is an integral part of security testing and software development.  Here are negative and positive test cases for STR30-C.  A negative BufferVulnerabilityOverflowWithstrcpy test that yields a buffer overflow exception.  Another negative BufferVulnerabilityOverflowwithstrcat test that yields a buffer overflow exception again with strcat method  A positive PositiveTeststrcpy test that passes the Google Unit testing and causes no failures with implementation of strcpy |
| **11-12** | The diagram depicts the security in devops automation process.   * DevSecOps stands for development, security, and operations. DevOps stands for development and operations. * Starting at pre-production, Assess and Plan stage brainstorms the new threats and potential security attacks. * The architecture of the system provides components that are software or hardware addons. * Design stage may draw out security checks such as OWASP. * In the build stage, secure coding upholds strong security standards and is the bulk of the work. * In the Verify and test stage, certain security vulnerabilities are checked. * Monitor and detect stage use log collections, and analytics to catch security vulnerabilities. * The Respond stage adds blocking attacks and limiting services. * In the final stage of Maintain and stabilize, the application is reassessed for potential cyberattacks and held in stable state. |
| **13** | There are benefits and risks by using DevSecOps   * Benefits include but not limited to increase speed and efficiency in software development, enhanced security, improved collaboration in teams, improved compliance with regulations, and improve organization’s trust. * Risks include a shift of culture and mindset, requires some prior knowledge in software development and security, increase complexity of software projects. * Steps include to establish security goals objects, conduct a security risk assessment, add a security awareness for all employees, monitor and improve security. |
| **14** | Here are my recommendations to identify gaps in the security policy   * Lack of responsibilities in security management * Lack of training, such corporate training videos, and tests * More access controls * More incident response procedures, such as security audit * More physical security measures, such as video surveillance and fingerprint |
| **15** | Here are my conclusions. Standards that should be adopted to prevent future problems   * Adopt a security standard such as ISO or NIST cybersecurity framework * Identify and mitigate organizations security risks * Establish security goals such as Report all potential threats of http requests every month * Provide security training for all employees * Practice Defense in Depth in the organization, such as implement a firewall, limited traffic http protocols * Utilize external security programs and resources, such as a gray hat hacker |
| **16** | Thank you! Questions or Comments? |
|  |  |