CS 405 Project Two Guidelines and Rubric

Competency

In this project, you will demonstrate your mastery of the following competency:

- Use external testing methods to identify potential vulnerabilities

Green Pace

Scenario

You have been asked to present the Green Pace security policy guide and to provide implementation guidelines and recommendations for maintaining it in the future. The developers have been employing best practices and, as the team grows, it's critical that everyone remains in sync with principles and best practices. Your job is to take the implicit policies that are applied daily in practice and explain how they have been standardized. You will explain your Green Pace security standards and policies, including the surface area of an attack and assumption of vulnerability. It is your job to demonstrate how the coding and architectural issues are organized using a set of 10 guiding security principles. You will demonstrate how you apply external testing methods to identify potential vulnerabilities by adding screenshots from your coding exercises and explaining how external testing methods will catch the vulnerabilities. You will be writing unit tests to check for the vulnerabilities using the unit testing framework for C++ in Visual Studio.

Your presentation will follow the format of the security policy. First, you will produce a matrix illustrating the threat levels for each of the vulnerabilities you covered in your policy document. Next, you will spend time going through each of the coding policy standards. Following the coding standards, you will cover the use of encryption and then explain how the Triple-A framework will be used and applied. Then you will discuss the risks and benefits of mitigating current issues, such as which ones should be addressed first and why? Finally, you will present a vision for the future of policy creation: Based on current gaps, where should the focus be in preventing threats? What are ways to get in front of potential threats? Your final presentation will represent principles and best practices for coding and systems architecture for Green Pace developers.

Directions

You have been tasked with presenting your brand-new security policy to the whole development team. Your presentation contains policies, standards, principles, and best practices that help prevent the threat of potential security vulnerabilities in both code development and systems architecture.

Specifically, you will need to use the PowerPoint template provided in Supporting Materials and follow the steps outlined below to create a presentation. Your presentation will follow the outline by documenting your policies and demonstrating that they are clear, repeatable, and ready to implement. The security policy ensures compliance and is part of an overarching defense-in-depth strategy.

Follow the template by populating each of the slides and completing the threat matrix. The threat matrix will be used to frame your policy because it shows all of the coding vulnerabilities you have identified and how you view them as potential threats to the system. You will complete the matrix by adding each of the 10 coding standards using their reference numbers. In addition to completing the slide deck, you will prepare a script that you will read to produce a narrated presentation. Use the script template in the Supporting Materials to produce a narrated PowerPoint presentation. You may use a screen-capture program or the internal recording feature in PowerPoint. The script will become a transcript, which is necessary for accessibility.

1. **Title Page (1 slide)**
    a. Add your name to the template.

2. **Overview (2 slides)**
    a. Introduce your security policy. Summarize why it was needed and how it will be used to support the defense-in-depth best practice. (The slide already contains the illustration.)
    b. Populate the Threats Matrix table and provide explanations to summarize all of your security risks.
    c. Demonstrate how you can use automation to detect these coding vulnerabilities.
3. **Principles (1 slide)**
    a. List the 10 principles, and list the coding standards that apply to each principle. This shows the alignment between principles and standards.
4. **Coding Standards (1 slide)**
    a. List the 10 coding standards in priority order, and then explain your system of prioritization.
5. **Encryption Strategy (1 slide)**
    a. Summarize the policies for encryption in flight, at rest, and in use.
6. **Triple-A Framework (1 slide)**
    a. Summarize the policies that support authentication, authorization, and accounting.
7. **Unit Testing**
    a. Add a slide for each of the unit tests, adding points on how to take it a step further.
        - Show how to apply the unit testing frameworks.
8. **Automation Summary (1 slide)**
    a. DevSecOps Diagram: Explain where the security tools reside in the flow of automation. State which stages will contain security automation. For instance, when will the compiler be used?
9. **Risks and Benefits (1 or more slides)**
    a. State the problems, solutions, and the risks or benefits involved if you act now or decide to wait.
10. **Recommendations and Conclusion (2 slides)**
    a. Moving forward, explain your gap analysis of the existing security policy and future potential gaps and improvements. You will be graded on the quality of the supporting details you provide. Do you offer real-world examples to support your claims? If the explanation is logical, it will be considered proficient. If you provide evidence (e.g., a real-world example, link, or citation), you will exceed expectations.
        - What current gaps in the security policy still need to be addressed?
        - What standards should be adopted to prevent future problems?
11. **References (1 slide)**
    a. Any sources you cite throughout your presentation must be referenced using APA style.

What to Submit

To complete this project, you must submit the following:

Script
Submit a written script, formatted as a Word document, that will serve as the transcript for the narrated presentation. Include the video link under your heading, which should include your name, the date, the assignment name (Project Two: Security Policy Presentation), and a link to your YouTube video.

Narrated Presentation
Submit a narrated presentation that has been saved as an MP4 and uploaded to YouTube so it may be shared. It is recommended to make your YouTube video unlisted (see article in Supporting Materials for guidance). Your presentation should demonstrate the use of external testing methods to identify coding vulnerabilities.

Supporting Materials

The following resource(s) may help support your work on the project:

Template: Project Two PowerPoint Template PPT
Use this template with the images provided as the basis for your presentation. It contains an outline with each of the rubric criteria. You may modify the presentation to accommodate your own presentation style or include additional images that align with your script.

Template: Project Two Script Template Word Document

Use this template to produce a script for your narrated PowerPoint presentation. The script will become a transcript, which is necessary for accessibility. You may add slides as needed to stay in sync with your presentation.

Video: How to Create Voice-Over Narration for Your PowerPoint Presentation (3:06)

Watch this video for a guide to creating voice-over narration in a PowerPoint presentation.

Video: How to Add Narration to Your PowerPoint Presentation (11:41)

Watch this video to gain clarity on how best to create a narrated slideshow.

Reading: How to Upload an "Unlisted" Video to YouTube

This article provides guidance on how to upload your presentation as an unlisted YouTube video.

Project Two Rubric

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
Overview	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Includes threats matrix with all identified threats and uses logic to justify placement of threats in the matrix (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements (55%)	Does not attempt criterion (0%)	5
Identify Coding Vulnerabilities	N/A	Identifies all coding vulnerabilities using automation (100%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include additional coding vulnerabilities (55%)	Does not attempt criterion (0%)	10
Coding Standards Policy	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states the rationale for each of the coding standards and provides a supporting example of when the policy should be applied (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include additional standards or clarity (55%)	Does not attempt criterion (0%)	15
Encryption Strategies	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states the rationale for the proposed design and provides a supporting example of why the strategy should be applied (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include additional examples or instances when the policy may be applied (55%)	Does not attempt criterion (0%)	10
Triple-A Framework	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states the rationale for the identified policies and provides one or more supporting examples of where they should be applied (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include additional examples or instances when the policy may be applied (55%)	Does not attempt criterion (0%)	10
Unit Testing	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states the purpose of the unit-testing frameworks and provides a supporting example of where and how they should be applied (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include additional examples or instances when the policy may be applied (55%)	Does not attempt criterion (0%)	20
Risks, Benefits, and Recommendations	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states method for determining the risks and benefits, and gives examples of which issues should be	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include more	Does not attempt criterion (0%)	15

		addressed first and why (85%)	logical explanation of the risks and benefits and a need for supported recommendations (55%)		
Conclusion	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly states an understanding of what still needs to be done to ensure security in the future; recommends next steps that are logical and supported with case studies or articles (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include next steps that are more logical and supported with case studies or articles (55%)	Does not attempt criterion (0%)	10
Articulation of Response	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly conveys meaning with correct grammar, sentence structure, and spelling, demonstrating an understanding of audience and purpose (85%)	Shows progress toward proficiency, but with errors in grammar, sentence structure, and spelling, negatively impacting readability (55%)	Submission has critical errors in grammar, sentence structure, and spelling, preventing understanding of ideas (0%)	5
				Total:	100%