NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND
INFORMATION TECHNOLOGIES

INFORMATION SECURITY AND ASSURANCE

(Course Project Specification)

Project Requirement(s)

Implementation: Web Application and Server Security

Your team with expertise on Web Application development is tasked to design and develop a small-medium business enterprise web application (eCommerce, Inventory System, Information System or Thesis/Capstone-related Project) implementing industry best-practices and techniques in securing web application systems. Moreover, your team is also tasked to follow secure coding practices and properly implement web server security using security hardening techniques.

Documentation Requirement

Cover Page
Table of Contents

1. **Introduction**
   Provide a brief description and purpose of the developed web application system.
2. **Web Application Screen Designs**
   Provide all available web application user interface (UI) with proper label and description of its purpose or functionality.
3. **Threat Model**
   Provide the threat model design, threats identified, and mitigations plan (refer to your created threat model document).
4. **Secure Coding Practices Implementation**
   Provide the checklist summary of secure coding practices implemented in the development.
5. **Server Hardening Techniques Implementation**
   Provide the checklist summary of the server hardening techniques implemented in the web server configurations.
6. **Web Vulnerability Assessment Report (OWASP ZAP)**
   Provide the checklist summary of the OWASP ZAP vulnerability assessment (Initial and Post) report (refer to the results of your vulnerability assessment activity).
7. **Reflection (Individual)**
   Discuss thoroughly your learnings about performing secure coding practices and its implications on business applications.

Presentation Requirements

Be able to provide a video presentation of the overall course project implementation which highlights the discussion of the web application description, web application features, web application design (actual walkthrough), initial vulnerability assessment report (OWASP ZAP), threat model, secure coding practices and server hardening technique implementations (actual walkthrough), and post vulnerability assessment report (OWASP ZAP).

Submission Requirements

Final Documentation (Printed Copy and Softcopy)
Video Presentation

INFORMATION SECURITY AND ASSURANCE

(Course Project Rubrics)

Term / Academic Year	***T2 AY 2025-2026***	**Date**	13/02/2026
Group Name	ALTAEGIS INFINITE		
Members	**Surname, First Name MI. (Alphabetical)**	**Section**	**Program Specialization**
	CASTILLO, ALEXANDER	COM231	*BSCS-DF*
	MEDIO, CHARLES	COM231	*BSCS-ML*
	SALAMAT, TRISTAN JHAY	COM231	*BSCS-DF*
	TABERNA, MARK JHOSHUA	COM231	*BSCS-DF*
	TALOSIG, JAY ARRE	COM231	*BSCS-ML*

Project Component	SO	Unsatisfactory (0)	Needs Improvement (1)	Satisfactory (2)	Proficient (3)	Exceptional (4)	PTS
Secure Coding Practices Implementation	SO2	Failed implementation of secure coding practices with critical vulnerabilities. Lack of input validation, error handling, and secure data storage. No use of secure coding standards.	Poor implementation of secure coding practices with many vulnerabilities. Inconsistent use of input validation, error handling, and secure data storage. Limited use of secure coding standards.	Basic implementation of secure coding practices with several vulnerabilities. Use of input validation, error handling, and secure data storage with several issues. Basic use of secure coding standards.	Implementation of secure coding practices with minor vulnerabilities. Use of input validation, error handling, and secure data storage with minor issues. Good use of secure coding standards.	Implementation of secure coding practices with no vulnerabilities. Comprehensive use of input validation, error handling, and secure data storage. Effective use of secure coding standards (e.g., OWASP, SANS).	
Secure Web Application Development		Development of a web application with critical security issues. Lack of authentication and authorization mechanisms. No use of encryption for data in transit and at rest.	Development of a web application with many security issues. Poor implementation of authentication and authorization mechanisms. Inconsistent use of encryption for data in transit and at rest.	Development of a basic web application with several security issues. Basic implementation of authentication and authorization mechanisms with several issues. Use of encryption for data in transit and at rest with several issues.	Development of a functional and mostly secure web application with minor issues. Implementation of authentication and authorization mechanisms with minor issues. Use of encryption for data in transit and at rest with minor issues.	Development of a fully functional and secure web application. Implementation of robust authentication and authorization mechanisms. Effective use of encryption for data in transit and at rest.	
Security Testing and Vulnerability Assessment		Lack of security testing with critical vulnerabilities not identified or remediated. No vulnerability assessment report or mitigation strategies. No use of automated security tools or manual testing.	Poor security testing with many vulnerabilities identified and few remediated. Incomplete vulnerability assessment report with few mitigation strategies. Inadequate use of automated security tools and manual testing.	Basic security testing with several vulnerabilities identified and some remediated. Basic vulnerability assessment report with minimal mitigation strategies. Limited use of automated security tools and manual testing.	Extensive security testing with minor vulnerabilities identified and remediated. Detailed vulnerability assessment report with some mitigation strategies. Use of automated security tools and some manual testing.	Comprehensive security testing including penetration testing, static and dynamic analysis. Identification and remediation of all critical vulnerabilities. Detailed vulnerability assessment report with mitigation strategies. Use of automated security tools and manual testing.	
Documentation	SO5	Lack of documentation covering project aspects.	Incomplete documentation covering few aspects of the project.	Basic documentation covering some aspects of the project.	Detailed and organized documentation covering most aspects of the project.	Comprehensive and well-organized documentation covering all aspects of the project.	

Presentation		Unclear and unprofessional presentation of the project. No use of visuals and demonstrations. Very poor communication skills demonstrated during the presentation.	Poor presentation of the project with many issues. Limited use of visuals and demonstrations. Poor communication skills demonstrated during the presentation.	Basic presentation of the project with several issues. Some use of visuals and demonstrations. Basic communication skills demonstrated during the presentation.	Clear and professional presentation of the project with minor issues. Good use of visuals and demonstrations. Good communication skills demonstrated during the presentation	Clear, concise, and professional presentation of the project. Effective use of visuals and demonstrations to enhance understanding. Excellent communication skills demonstrated during the presentation.	

Total Score and Feedback			**TOTAL POINTS EARNED**	
☐ Exceptional	20	Outstanding performance in all project components with minimal to no issues		
☐ Proficient	16-19	Good performance in most project components with minor issues.		
☐ Satisfactory	12-15	Acceptable performance in basic aspects with several issues.		
☐ Needs Improvement	8-11	Below-average performance with many issues.		
☐ Unsatisfactory	0-7	Poor performance with critical issues in most project components.		

Evaluated by: Gaudencio Jeffrey G. Romano Name of Course Instructor/Date	**Remarks/Comments**

NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND
INFORMATION TECHNOLOGIES

INFORMATION SECURITY AND ASSURANCE

(Peer/Self Evaluation Rubrics)

Student Name(s) *All members including the evaluator.*	**Contribution to Team Effort**	**Communication Skills**	**Meeting Deadlines and Reliability**	**Quality of Work**	**Collaboration and Teamwork**	**PTS**
	Contributes meaningfully to group discussions.	Demonstrate excellence in written and verbal communication skills	Completes group assigned task(s) on time.	Prepares work in a quality manner	Demonstrate a cooperative and supportive attitude.	
	Using scale 0-4 (0=Unsatisfactory; 1=Needs Improvement; 2=Satisfactory; 3=Proficient; 4=Exceptional)					
CASTILLO, ALEXANDER						
MEDIO, CHARLES						
SALAMAT, TRISTAN JHAY						
TABERNA, MARK JHOSHUA						
TALOSIG, JAY ARRE						

Peer Evaluation Interpretation

□ Exceptional	20	Outstanding performance across all indicators.
□ Proficient	16-19	Strong performance with minor areas for improvement.
□ Satisfactory	12-15	Adequate performance with several areas for improvement.
□ Needs Improvement	8-11	Below-average performance with significant areas for improvement.
□ Unsatisfactory	0-7	Poor performance across most or all indicators.

Remarks/Comments