Republic of the Philippines
University of Cabuyao
(Pamantasan ng Cabuyao)
COLLEGE OF COMPUTING STUDIES
Katapatan Mutual Homes, Brgy. Banay-banay, City of Cabuyao, Laguna 4025

Midterm Assessment
ITEW5 – Web Security and Optimization

Name: _____ **Score:** _____

Student Number: _____ **Section:** _____

Instructor: **RONNEL OCAMPO**

PHP Web Application Task: Implementing CSRF Protection and CSP

Objective:

Develop a simple PHP-based web application that incorporates Cross-Site Request Forgery (CSRF) protection and enforces a Content Security Policy (CSP) to enhance the application's security.

Requirements:

1. **Basic Web Application:**
   - Create a simple PHP application with user interaction that performs state changing requests like transferring funds, changing email address, resetting password, and so forth. It can be a basic form where users input data and submit it to the server.
2. **CSRF Protection:**
   - Implement CSRF protection in the form submission process.
3. **Content Security Policy (CSP):**
   - Configure a Content Security Policy (CSP) header in the application to mitigate the risk of Cross-Site Scripting (XSS) and other code injection attacks.
     - The CSP should block external scripts, and prevent external styles from being loaded.
4. **Form Handling:**
   - The form should process user input (e.g., save to a file, or just display it after submission).
   - Ensure that the form data is sanitized to prevent XSS vulnerabilities.
5. **Documentation:**
   - Include comments in a .txt, PDF, or a README file to explain how the CSRF protection works and the role of the CSP in improving security.

Submission:

- Submit your application with all relevant PHP, HTML, CSS files and images, along with a documentation explaining how to test the CSRF protection and CSP implementation.
- Submission link will be provided

Grading Criteria:

	Scale				
Criteria	**4 (Excellent)**	**3 (Good)**	**2 (Fair)**	**1 (Needs Improv)**	**Weight**
Basic Application Functionality	The PHP application runs perfectly. Form submission and data handling work as expected without any issues.	Application runs correctly with only minor issues in form submission or data handling.	Application runs but with some issues in form submission or data processing.	Application does not run or fails to handle form submissions and data properly.	10%
CSRF Protection Implementation	Proper CSRF protection is implemented, token is generated, validated, and secure against attacks.	CSRF protection is implemented but has minor issues (e.g., token validation logic needs improvement).	Basic CSRF protection is implemented but may have security flaws or incomplete validation.	CSRF protection is either not implemented or is non-functional.	25%
Content Security Policy (CSP)	Correct CSP header is set, preventing unsafe resources (e.g., external scripts), and policy fully enforced.	CSP header is set, but policy allows some insecure resources or is not as restrictive as needed.	CSP header exists but is weak, allowing most external resources or missing certain directives.	No CSP header or an incorrect/ineffective CSP policy is implemented.	20%
Security Practices (XSS, etc.)	Application is fully secure against XSS and other common vulnerabilities. Proper input sanitization applied.	Input is mostly sanitized, but some potential vulnerabilities (like XSS) remain unaddressed.	Basic input sanitization is applied, but several security risks remain.	Input sanitization is missing or completely ineffective, leaving the application vulnerable to XSS.	10%
Documentation	Thorough comments. README clearly explains the CSRF and CSP features.	With comments, but some parts may lack clarity or explanation.	Lack sufficient comments/documentation	Poorly written with no comments or explanations, making it difficult to understand.	15%
Creativity & Design	The student adds unique elements to the task, such as an innovative UI, extended functionality, or interesting ways of presenting the vulnerability. Demonstrates a deep understanding of the task and adds thoughtful extras.	Some creative elements are present (e.g., extra features or enhancements to the basic task), but they are limited or only somewhat original.	Creativity is minimal, with little effort to go beyond the basic requirements of the task.	No creative enhancements or original ideas; the application meets only the basic task requirements.	20%