NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND INFORMATION TECHNOLOGY

Student Name:	**Section:**	**Date:**

Activity 5

Server Hardening Technique

Instructions/Directions:

Be able to implement the necessary “Server Security Hardening” techniques on your web application server.

Laboratory Task(s):

1. Based on the web vulnerability assessment report of your web application, be able to implement all the necessary security hardening techniques on your server, database, and network (optional).
2. Provide a checklist of the vulnerability assessment and the recommended security hardening technique.
3. Provide a screenshot of the necessary configuration of a completed task from the checklist.
4. Upload the configuration file (.conf or .ini) of your server.

Show proof of your activity completion by providing clear screenshot of your entire desktop environment based on the tasks performed. Screenshot must be included in the activity template provided in MS Teams Assignment.

Submission Note (Individual Activity)

Use the Activity template attached in MS Teams Assignment.

Use file name convention (LASTNAME_CTINASSL_SECTION_TERM_AY_Activity5.pdf).

Submit a PRINTED document and upload the Softcopy (PDF file) in MS Teams

Submit http.config File separately.

Student Name:	**Section:**	**Date:**

SECURITY HARDENING

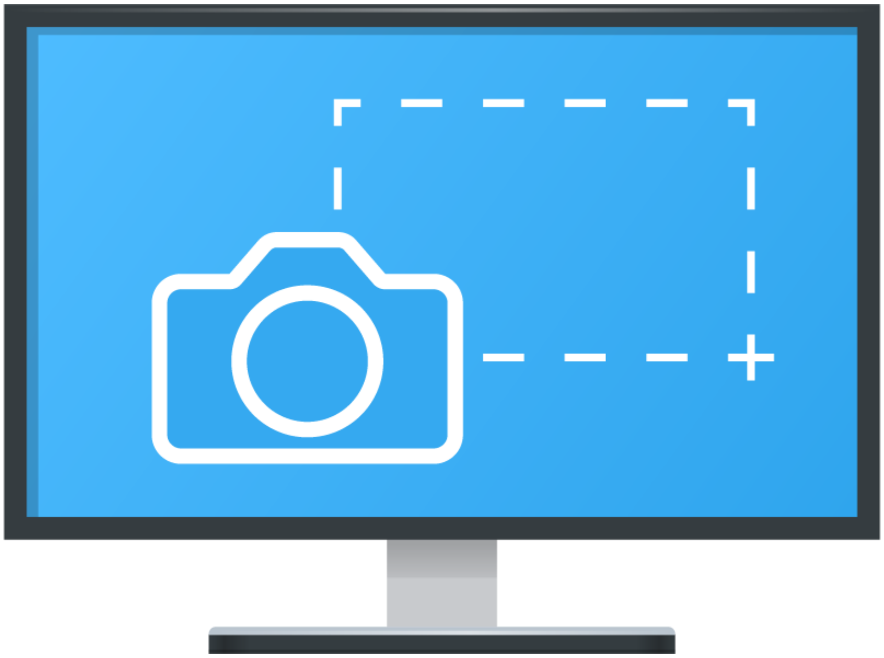
Based on the web vulnerability assessment report of your web application, be able to implement all the necessary security hardening techniques on your server, database, and network (optional).

System Vulnerability Checklist

Provide a checklist of system-related vulnerability based on OWASP web vulnerability results and the recommended security hardening technique.

Security Hardening Implementation

Provide a screenshot of the necessary configuration of a completed task from the checklist.



Student Name:	**Section:**	**Date:**

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	**Beginning (1 point)**	**Developing (2 points)**	**Proficient (3 points)**	**Exemplary (4 points)**	
Service Management	No attempt to manage XAMPP services.	Unnecessary services left enabled, creating vulnerabilities.	Some unnecessary services are running; partial service management.	Most unused services disabled; minor gaps in configuration.	Only required services (e.g., Apache, MySQL) are running; unused services disabled.	
Apache Configuration	No attempt to configure Apache service.	Apache left in default state; major vulnerabilities present.	Basic configurations applied; significant gaps in Apache security settings.	Most Apache configurations are secure; minor issues remain.	Apache configuration hardened (e.g., directory listing disabled, server signature hidden).	
Password Protection	No attempt to configure password protection.	Default passwords used for services.	Weak or default passwords used for some services	Passwords set but not strong or unique in some cases.	Strong, unique passwords set for all services (MySQL, phpMyAdmin, etc.).	
File and Directory Permissions	No attempt to configure file and directory Permissions.	Permissions not configured; files/directories are vulnerable.	Permissions partially configured; some files/directories are insecure.	Permissions mostly configured correctly with minor issues.	File and directory permissions configured to follow the principle of least privilege.	
Error Reporting and Logging	No attempt to configure error reporting and logging.	Error reporting enabled and logs missing or poorly managed.	Error reporting partially disabled; logs are incomplete or poorly configured.	Error reporting mostly disabled; logging is functional but not optimized.	Error reporting disabled for production; secure and useful logs configured.	
Reporting and Documentation	No documentation provided.	Poor or incomplete documentation with missing key information.	Basic documentation provided; several key details missing.	Documentation provided but lacks detail or has minor gaps.	Detailed and accurate documentation of hardening techniques provided.	

Total Score and Feedback			**TOTAL POINTS EARNED**	
☐ Exemplary	21-25	Demonstrates comprehensive hardening of XAMPP with no significant vulnerabilities and detailed documentation.		
☐ Proficient	16-20	Shows solid hardening with minor gaps or areas for improvement.		
☐ Developing	11-15	Basic hardening performed but with several vulnerabilities and weak documentation.		
☐ Beginning	6-10	Minimal hardening performed.		
☐ Not Attempted	0-5	No hardening performed, leaving the server highly vulnerable.		

Evaluated by:

____

Name of Course Instructor/Date

Remarks/Comments