| Student Name: | Section: | Date: |
|---|---|---|

# Activity 4
# Secure Coding Practices

Instructions/Directions:

Be able to implement the necessary "Secure Coding Practices – Input Validation & Data Sanitization, Authentication & Session Management, Authorization & Access Control, Secure Data Storage & Encryption, and Error Handling & Logging" techniques on your application development based on your Laboratory Activity 2 (Web Application Development). Please refer to your notes for the guide on "OWASP Secure Coding".

Laboratory Task(s):

1. Implement Secure Coding Practices specified in the checklist (applicable items).
2. Provide a checklist of the completed tasks.
3. Provide a screenshot of the source code snippet of a completed task from the checklist.
4. Upload the web application source file compressed as zip file.

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_Activity3.pdf).
Submit a PRINTED document and upload the Softcopy (PDF file) in MS Teams
Submit OWASP ZAP HTML Generated Report File

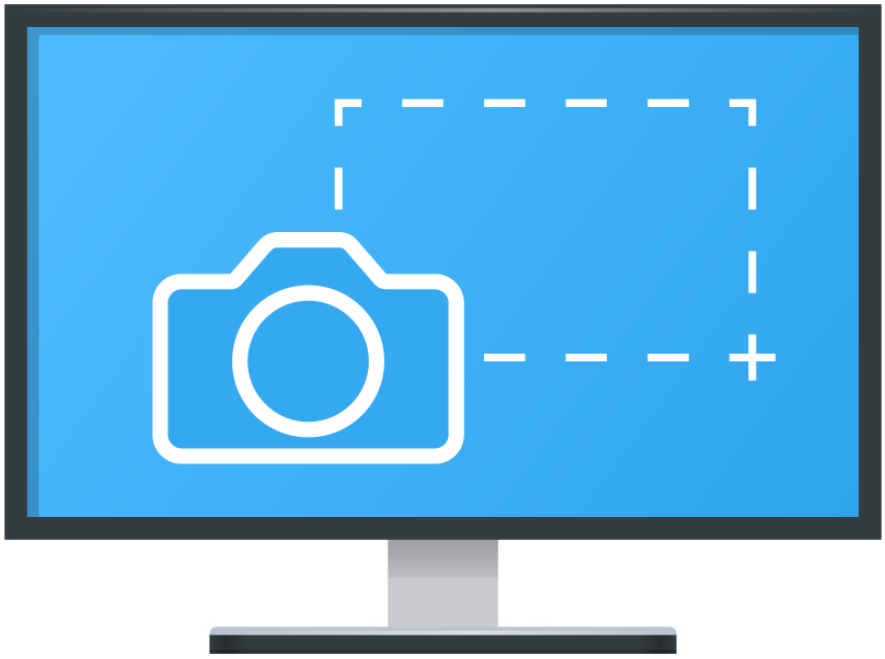
| Student Name: | Section: | Date: |
|---|---|---|

# SECURE CODING PRACTICES

## Input Validation and Data Sanitation

**Secure Coding Practices Implementation**
**Provide a checklist of the completed tasks according to the need.**

**Source Code Snippet**
**Provide a screenshot of the source code snippet of a completed task from the checklist.**

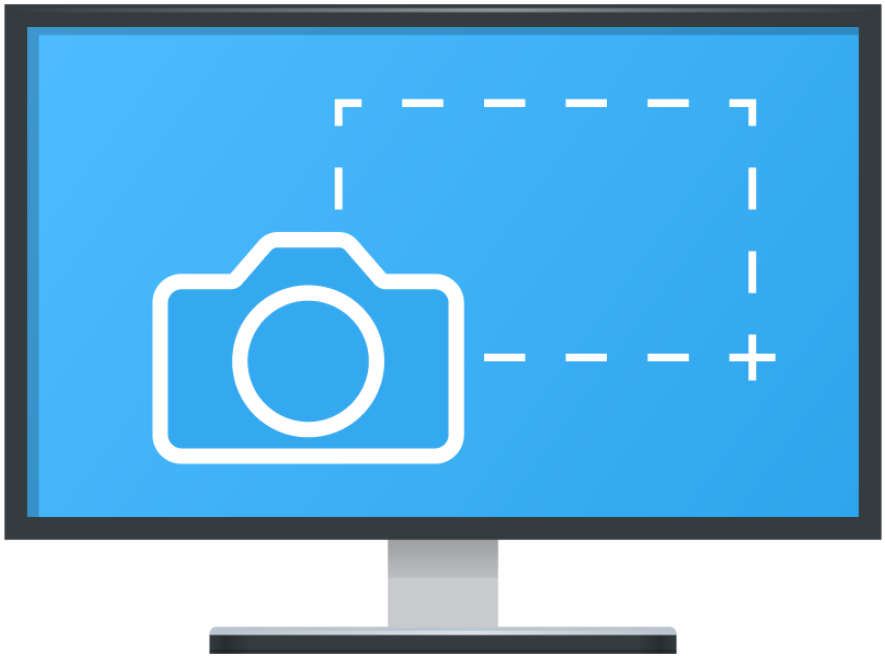


# SECURE CODING PRACTICES

## Authentication and Session Management

**Secure Coding Practices Implementation**
**Provide a checklist of the completed tasks according to the need.**

**Source Code Snippet**
**Provide a screenshot of the source code snippet of a completed task from the checklist.**

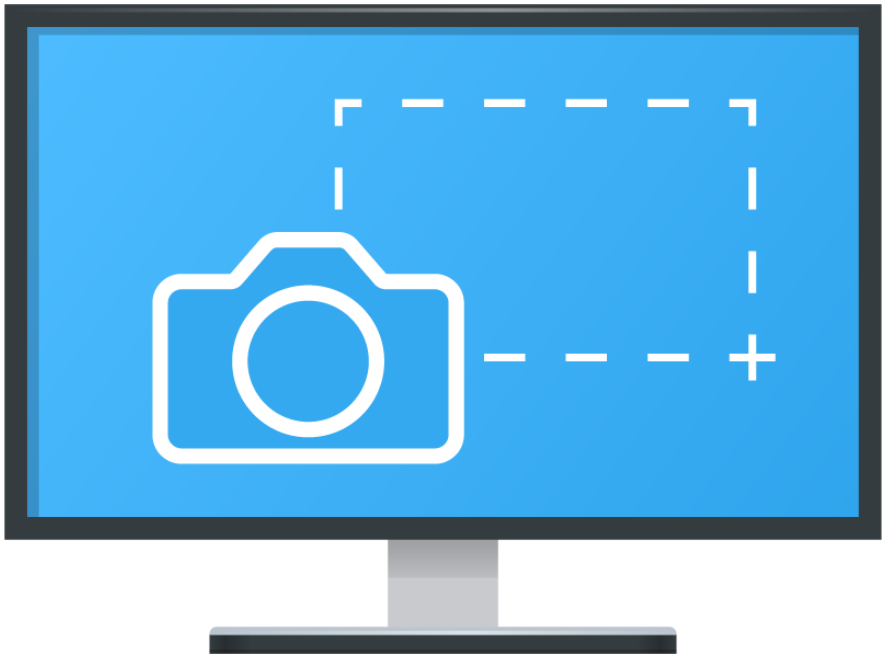


# SECURE CODING PRACTICES

## Authorization and Access Control

**Secure Coding Practices Implementation**
**Provide a checklist of the completed tasks according to the need.**

**Source Code Snippet**
**Provide a screenshot of the source code snippet of a completed task from the checklist.**

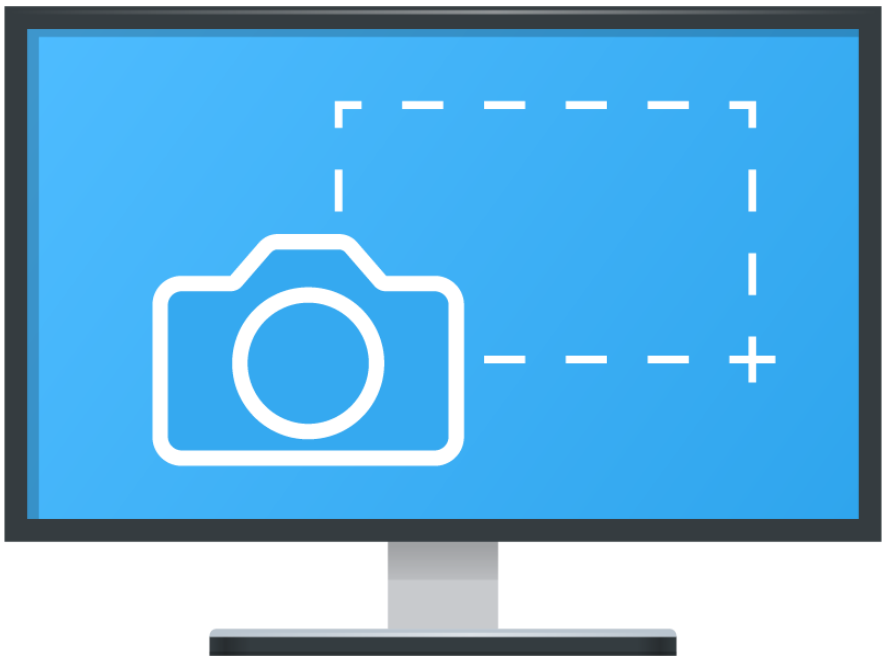


# SECURE CODING PRACTICES

## Secure Data Storage & Encryption

**Secure Coding Practices Implementation**
**Provide a checklist of the completed tasks according to the need.**

**Source Code Snippet**
**Provide a screenshot of the source code snippet of a completed task from the checklist.**

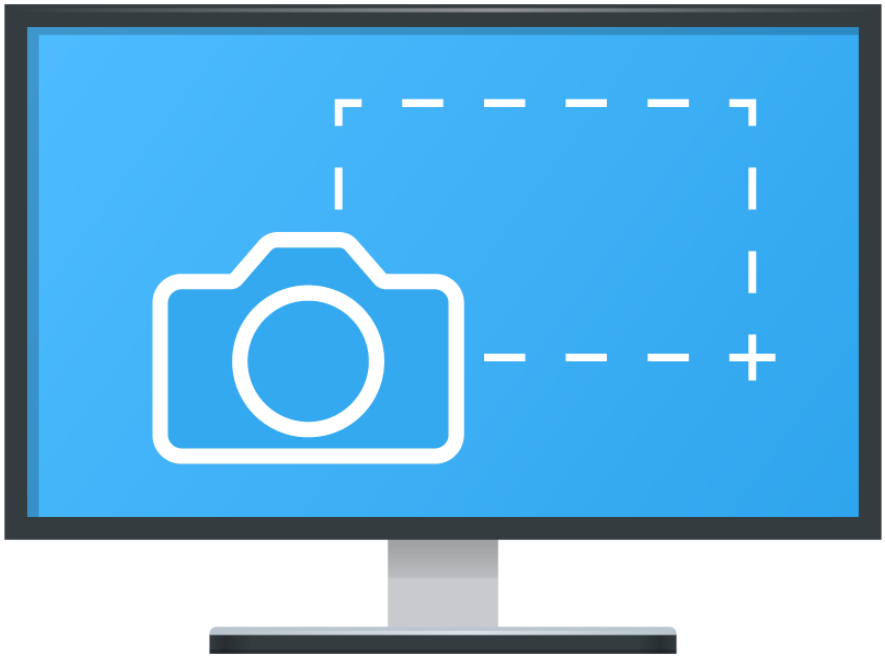


# SECURE CODING PRACTICES

## Error Handling & Logging

**Secure Coding Practices Implementation**
**Provide a checklist of the completed tasks according to the need.**

**Source Code Snippet**
**Provide a screenshot of the source code snippet 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) | |
| **Input Validation & Data Sanitization** | No input validation and data sanitization. | Basic input validation and no data sanitization. | Basic input validation, minimal data sanitization. | Validates and sanitizes most inputs, but some edge cases missed. | Comprehensive input validation and data sanitization for all inputs. | |
| **Authentication & Session Management** | No authentication or session management implemented. | Weak or missing session management, weak authentication practices. | Strong authentication and session management with minor issues. | Robust authentication, session management with MFA. | Robust authentication, session management with MFA, secure token handling, and session expiration. | |
| **Authorization & Access Control** | No access control mechanisms. | Some access control mechanisms, but several privileges not properly restricted. | Some access control mechanisms, minor privileges not properly restricted. | Access control is implemented, but some areas lack fine-grained control. | Strict role-based access control and least-privilege enforcement throughout the application. | |
| **Secure Data Storage & Encryption** | Sensitive data stored in plain text, no encryption. | Some encryption used, but key management and data not fully secure. | Some encryption used, but key management and data at rest or in transit minimally secure. | Encryption is in place for most sensitive data, but some weaknesses in implementation. | End-to-end encryption implemented for data at rest and in transit with proper key management. | |
| **Error Handling & Logging** | No error handling or sensitive information exposed in error messages. | Inconsistent error handling, revealing sensitive information in some cases. | Minimal error handling, revealing minimal sensitive information in some cases. | Proper error handling, but some logs not fully secured or sensitive info is logged. | Comprehensive error handling with no sensitive data exposure, logs securely stored and regularly reviewed. | |
| **Reporting and Documentation** | No documentation provided. | Poor or incomplete documentation with missing key information. | Basic documentation provided with several gaps or omissions. | Documentation mostly complete with minor omissions | Thorough and well-organized documentation of all steps, findings, and decisions. . | |

| **Total Score and Feedback** | | | **TOTAL POINTS EARNED** | |
|---|---|---|---|---|
| ☐ Exemplary | 21-25 | Secure coding practices are fully implemented, and security is well-integrated into all stages of development. | | |
| ☐ Proficient | 16-20 | Secure coding practices are largely implemented, with only minor gaps. | | |
| ☐ Developing | 11-15 | Secure coding practices are partially implemented, with several key areas needing improvement. | | |
| ☐ Beginning | 6-10 | Secure coding practices are minimal or incomplete, and significant improvement is needed. | | |
| ☐ Not Attempted | 0-5 | Secure coding practices are not implemented, and the application is highly vulnerable. | | |

| Evaluated by:<br><br>_____<br>Name of Course Instructor/Date | **Remarks/Comments** |
|---|---|