CSSECDV Machine Project Specifications

Introduction

The goal of this project is to improve the security of an existing web application by applying best practices such as authentication, authorization, input validation, and error handling and logging.

It is highly suggested that the existing project is an output from a previous course such as CCAPDEV to lessen the time for development and the focus can be shifted to applying the prescribed security controls. Alternatively, students may also decide to make a new web application from scratch, but must comply with all requirements in this specifications documents upon demonstration.

User Roles and Permissions

The application must support at least three primary roles, each with different levels of access control:

- Administrator
    - Has the highest level of privilege
    - Can create/delete/assign Role A and administrator accounts
    - The only role that has read-only access to the application logs
- Role A (Example: Manager)
    - Has elevated permissions but not full system control
    - Can manage Role B users within their assigned scope such as assigning tasks to them or managing orders
- Role B (Example: Customer/ Regular Employee)
    - The most common user role
    - Can view/update/delete their own content/data
    - Limited access to system-wide information, mostly only their own

Components

- Frontend – User Interface
- Backend – APIs, business logic implementation, user authentication and authorization, database

Suggested CRUD Operations

- Administrator
    - Add new Administrator and Role A accounts

    - Assign/Change user roles for Administrator and Role A
    - Read-Access and filter comprehensive audit trails of all system activities from the frontend
    - Change password
- Role A
    - Add/View/Modify/Remove objects/transactions*
    - Change password
- Role B
    - Create account via the registration page
    - Add/View/Modify/Remove own objects/transactions*
    - Change password

*Depending on the nature of the application, define your own CRUD operations for these roles. While some permissions may be shared across some or all roles, there must still be permissions unique for each role, particularly in the case of Roles A and B.

Security Control Requirements

See the rubric/checklist for the complete list of security controls.

Group Composition

The project is to be accomplished by group with maximum of three (3) members per group.

Submission and Demo

Submission of the full project (source code and necessary dependencies) is during Week 14 (may be subject to change).