Practical Assignment (ICA 30%)

(Individual Assignment)

Overview

This is an individual assignment.

Task :

To provide security implementations for the following web app features:

- Registration with photo upload feature
- Login
- Anti-Bot (Captcha)

Objectives

To implement recommended security features to a web application by applying knowledge learnt from App Web Security.

NOTE/WARNING

It is important that you create your solution from scratch and avoid copying from your friends. Design your own UI and adopt your own naming convention for variables and object ID. Do not share your codes with any friends to avoid plagiarisms.

Nanyang Polytechnic takes a serious view with regards to any student who commits the offence of plagiarism. Discipline with respect to students is governed by the school's Statutes and Regulations.

All submissions will be verified through "safe-assign" plagiarism checker which includes C# codes as well as reports.

Background

SITConnect is a stationary store that provide allow staff and students to purchase stationaries. SITConnect would like to engage your service to develop an online web application to allow staff and students to purchase stationary online. Below are there the application requirements for Registration and Authentication. For registration, it is preferred the user's email address is being used for the authentication.

You are tasked to create an ASP.NET Web Form Application from scratch by implementing the recommended security features highlighted in the table shown below.

Registration Form should consist of the following input fields:

- First Name
- Last Name
- Credit Card Info (to be encrypted)
- Email address (Must be unique)
- Password
- Date of Birth
- Photo

Web App Security Requirements

Complete the tasks below with the necessary database design :

Requirements	Tasks	Marks
Registration Form		
	Set Strong password • Perform password complexity checks. (Min 12 chars, Use combination of lower-case, upper-case, Numbers and special characters) • Offer feedback to user on STRONG password. • Implement both Client-based and Server-based checks.	10%
	Securing user data and passwords • Implement Password Protection • Encryption (Credit card to be encrypted)	10%

Session	• Provide a Secured Session (Fixed Sessions issues) • Session timeout • Route to homepage/login page after session timeout.	10%
Login/Logout	• Able to login to system after registration. • Account lockout after 3 login failures. • Clean logout • Perform audit log	10%
Anti-bot	Implement Google reCaptcha v3 service	5%
Proper Input Validation	• Prevent SQLi and XSS and perform proper input filtering, validation and verification. (e.g email) • Client and server input validation	10%
Proper Error handling	• Graceful error handling on all pages (including 404, 403 error pages etc) • Provide test cases in your report.	10%
Software Testing – Source code analysis	• Use external tools to perform software testing: - Github (check week 14 eLab) • Implement the recommendation to clear the security vulnerability for your source code. • Save your source code into Github and provide the public link.	5%
Advanced Features	Account Policies • Automatic account recovery after x mins of lockout. • Avoid password reuse (max 2 password history) • Change password • Minimum and Maximum password age (cannot change password within x mins from the last change of password and must change password after x mins) Authentication/Authorization • 2FA	15%
Demo	Prepare a 5-7 min web app demo to your tutor. - Working prototype with database - Error free demo - Demo according to the checklist (checklist will be provided)	5% 5-7min

Report	Create a report to explain how the above security features were implemented including a checklist of your completed features.	10%

Deadline and submission

- Demo of Practical assignment by week 17 during practical lesson.
- Submit your source code to bb as well as Github.
- Submit your report to bb. Report to include which part of the requirements (checklist) was accomplished. Include source code testing report and mitigation techniques.
- Print out a copy of the "**Statement on Plagiarism and Academic Dishonesty**" sheet and sign it. Submit to BB along with your submissions.