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)
- To demo your assignment to your tutor. This is a pre-requisite to complete this module.

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

EZYSoft is a software developer company helping companies to transform their traditional business model to online presence. Several companies have engaged EZYSoft service to help develop a secure website based on their initial requirements. The various companies are organized by module-groups and have different project requirements. You are to develop the initial website features based on module-group.

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 a **.Net Core Web Application (Razor Pages)** from scratch by implementing the recommended security features highlighted in the table shown below. Avoid using ASP.NET MVC core.

For Registration and displaying info on your homepage, please taker reference from the table below. The requirements is based on Module Group.

IT2163-01 to ITN2163-03	Company Name : Ace Job Agency (Membership Service) Membership Registration Form should consist of the following input fields: • First Name • Last Name • Gender • NRIC (Must be encrpyped) • Email address (Must be unique) • Password • Confirm Password • Date of Birth • Resume (.docx or .pdf file) • WhoamI (allow all special chars)
IT2163-04 to IT2163-07	Company Name : Fresh Farm Market (Membership Service) Membership Registration Form should consist of the following input fields: • Full Name • Credit Card No (Must be encrpyped) • Gender • Mobile No • Delivery Address • Email address (Must be unique) • Password • Confirm Password • Photo (.JPG only) • AboutMe (allow all special chars)

Table 1.1 Membership form user requirements

Web App Security Requirements

Taking reference from TABLE 1.1, please complete the tasks below with the necessary database design :

Requirements	Tasks	Marks
Registration Form	Registration process • Successfully saving member info into Database • Check for duplicate email and rectify issue.	4%
Securing credential	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 of customer data (encrypt data in database) • Decryption of customer data (display in homepage)	6%
Session	Session Management • Create a Secured Session upon successful login. • Perform Session timeout. • Set session timeout value. • Route to homepage/login page after session timeout. • Detect multiple logins from different devices (different browser)	10%
Login/Logout	Credential Verification • Able to login to system after registration. Redirect user to login page if user is not authenticated • Rate Limiting (E.g Account lockout after 3 login failures) • Perform proper and safe logout (Clear session and redirect to login page) • Perform audit log (save user activities in Database) • Redirect to homepage after successful credential verification. Home page displays the user info including encrypted data.	10%

Anti-bot	Implement Google reCaptcha v3 service	5%
Proper Input Validation	Input Validation checks • Prevent Injection (e.g SQLi), CSRF and XSS attack. • Perform proper input sanitation, validation and verification. (e.g email, HP, date etc) • Client and server input validation • Display error or warning message on improper input requirements. • Perform proper encoding before saving into database.	10%
Proper Error handling	Customed Error Message • Graceful error handling on all pages (including 404, 403 and any other possible error pages etc) • Display proper customed error pages.	5%
Software Testing – Source code analysis	Testing • Use external tools to perform software testing (Static code analysis). • Implement the recommendation to clear the security vulnerability for your source code.	5%
Advanced Features	Account policies and recovery • Automatic account recovery after x mins of lockout. • Avoid password reuse (max 2 password history) • Change password and Reset Password (using Email link / SMS) • Minimum and Maximum password age (cannot change password within x mins from the last change of password and must change password after x mins) • Login to account with external login providers (e.g Google or Twitter etc)	10%
	• Implement 2FA (1st Factor - Authentication, 2nd Factor – OTP. • Implement role-based authorization. Create and assign user to roles. Set role-based authorization to a page.	10%
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%

Report	• Write a report on how the above security features were implemented. • Submit security checklist (Annex A)	10%

Deadline and submission

- Demo of Practical assignment by week 15/16 during practical lesson or tutorial lessons.
- Submit your source code to Learning Management System (LMS)
- Submit your report to LMS.
- Print out a copy of the "**Statement on Plagiarism and Academic Dishonesty**" sheet and sign it. Submit to LMS along with your submissions.