B Assignment 2: Developing a secure application

B.1 Assessment Overview

In this assignment you will work in groups to develop an application with a focus on integrating security into your software development practice. You will be given a codebase for a basic website with some initial documentation and will be tasked with performing a security analysis as well as feature development with a focus on secure software development practices. The focus of this assignment is on secure design and and analysis, so you are encouraged to focus on security principles and practices rather than coding all of your proposed features.

B.1.1 Overview of what to submit and when

- **On Monday of week 13**: A group presentation from all group members discussing the progress your group has made and some of the things your group has found - (assessed with both group and individual components). *Note, that groups will need to pre-submit a PDF copy of their slides by* **9am Monday of week 13** *before any of the groups will be presenting (to keep things fair for all groups). Your group will also have an opportunity to nominate some time slots in which your entire group will be able to present. There will be no "prac material" in week 13, so the practical rooms will be used for the presentation assessment*
- **By 5pm Sunday 4 June 2023 - last day of week 13**: A group report detailing the results of your analysis and some recommendations. Your report should be about 10 pages long.
- **By 5pm Sunday 4 June 2023 - last day of week 13**: A snapshot of your group repository with any modifications to the initial codebase based on what your group has identified.
- An individual contribution form indicating the contribution levels of each group member which may be used to determine individual grades if there is a disparity in the agreed workloads that the group members decide to allocate to each other. This may be submitted after the group has submitted all of their other components for this assignment.

B.1.2 *Related Unit Learning Outcomes*

ULO1: Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.
ULO2: Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.
ULO3: Understand and apply security related best practices to the application development process and address the common security issues for secure application development.
ULO4: Communicate professionally in written and oral with technical and non-technical audience such as software developers/testers, business analysts, security managers, users, etc.

B.1.3 *Referencing*

For this assignment you may use code available on the internet provided that you cite your sources in your code and in your report. For other aspects of this project you must cite sources in your report using standard bibliographic referencing.

B.2 *Assignment Description*

The codebase that your group will be starting with is a basic website for displaying restaurant listings. The code is written in Python 3 using the Flask framework. Instructions for setting up the github repository and getting the basic website up and running are available on iLearn and in the README.md file in the code repository.

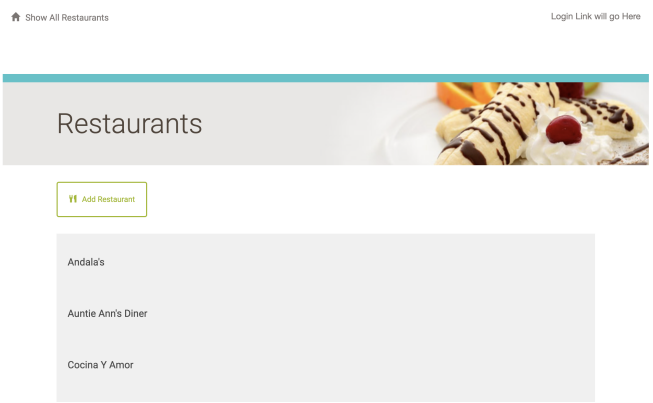

Figure B.1: Basic restaurant listings website.

The website includes a number of restaurant listings with some menu items for each restaurant. Notice that there is no restriction on who can create, edit or delete listings.

B.2.1 *Security analysis*

For the first part of your assignment you need to perform a security analysis of the existing codebase. You may use any tools to assist you

(eg. CodeQL), but you should also perform a manual code review. Your security analysis should address the following questions:

1. With reference to the OWASP top 10 and security principles, are there any vulnerabilities or insecure coding practices in the codebase?
2. Are there any attacks that this codebase might be vulnerable to?
3. Which lines of code are problematic? Which security principles are violated?
4. What solution would you recommend?

For the analysis completed above, make appropriate changes to the codebase to address one or more of the security issues you identified. Include comments in the code to identify the issue addressed.

B.2.2 *Authentication mechanism*

The next part of this assignment is to propose an authentication mechanism to restrict access to certain functions of the website to particular users. The website owner provides the following requirements specification:

- There are 3 types of users: administrators, restaurant owners and public users.
- An administrator user may add, edit and delete restaurant owners, restaurants and menu items.
- A restaurant owner may add, edit and delete restaurants and menu items.
- Public users can view restaurants and menu items but have no editing capabilities.

Given the above specification, complete the following tasks:

1. Analyse the requirements specification and identify any potential security or design issues. You may rewrite or modify the requirements specification incorporating any of your changes. You may write it in the form of user stories or in the form above.
2. Propose a design for your authentication mechanism. Your design could be in the form of new workflows and/or new urls with access controls indicated. With reference to security principles, describe security features incorporated into your proposal.
3. Implement some aspects of your authentication mechanism using secure coding principles. Identify where in the code these principles are applied.
4. Design and/or implement tests to demonstrate the security features of your implementation.

B.2.3 *Additional Features*

For this part of the assignment your group should propose 2 additional features which you would add to the website to improve its functionality. You should choose 1 feature from the below list and also invent one feature of your own.

1. Public users can rate restaurants (eg 1 to 5 star).
2. Public users can leave comments on restaurants.
3. Restaurant owners can customise their restaurant listing with external links to their website and uploaded images.
4. Restaurants are searchable via a search query form on the website.

For the features you choose you should include a proposed design (eg. user stories, code workflows), a security analysis (eg. identifying potential threats and how your design and/or implementation mitigates them), and a proposed suite of tests. You should provide an implementation of some aspects of the proposed features demonstrating secure coding practices.

B.3 *Submission*

For this assignment your group is required to submit the following for marking:

1. A report detailing your analyses and changes above. In particular your report should:
   - outline what changes you made to fix security issues identified in Sec. B.2.1,
   - outline what authentication mechanism you proposed and what changes you made to the design and to the code, and
   - outline which features that your group has added to the codebase and where in the code to look (and also detail how successful you were in implementing them).
2. The code committed to your group GitHub repository demonstrating the changes you made, including:
   - any security fixes to the codebase
   - any implementation of the authentication mechanism and new features
   - any tests or use of automated tools
3. An interim presentation to be presented in your group's allocated time slot in week 13.

B.3.1 *Marking Guide*

Assignment 2 is worth a total of *40%* of your final grade. The breakdown of the marks is as follows:

Submission	Marks	Individual/Group
Report	20	Group
Code submission	10	Group
Presentation	10	Individual

Marking rubrics for each of the above will be provided on iLearn.