# COLCHESTER GROCERIES README

### Contents

[1. Introduction](#_Toc172565878)

[2. System Overview](#_Toc172565879)

[3. Prerequisites](#_Toc172565880)

[4. Operating Instructions](#_Toc172565881)

[5. Benefits and Improvements](#_Toc172565882)

[6. Future enhancements](#_Toc172565883)

[7. Sources](#_Toc172565884)

## Introduction

This application highlights the security technologies that were proposed for the Colchester Groceries Online Shopping System. The system uses a login mechanism integrated with SQL, adapted from a Codeshack tutorial (Adams, 2024). The HTML templates are adapted from the same tutorial. Two Factor Authentication is also provided, and adapted from a tutorial by Miguel Grinberg (Grinberg, 2015).

## System Overview

The front end of the system is written in HTML and JavaScript. This has created a minimalistic yet intuitive user interface. The backend is powered by Python and Flask, leveraging the use of object oriented programming to provide modularity and flexibility in expanding the system. Inventory and account data is stored in an SQL database.

A diagram of a server

Description automatically generated“Defence in depth” has been provided by the use of two factor authentication (2FA). By using a separate smartphone application to provide secure tokens, costs are minimised because no licencing is necessary. Regular expressions are used to ensure resistance to SQL injection attacks. Passwords are also hashed, ensuring no sensitive data has been stored in the databases. Diagram One provides a high level overview of the system.

*Diagram One (Above): A high level overview of the interactions between the system’s components.*

## Prerequisites

* **2FA Authentication Smartphone Application.** Google Authenticator was used in testing, however any 2FA application that can scan QR codes will suffice.

## Operating Instructions

The Online Shopping System is hosted at <https://jamesedney.eu.pythonanywhere.com/colchestergroceries/> . It can be used on any platform, without the need for prerequisites and preconfiguring.

From the homepage, the user is able to register for an account. Once their details have been submitted, they will be taken to a QR code. Scanning the QR code with a 2FA application such as Google Authenticator will supply them with a TOTP that changes every 30 seconds.

The user can then login by providing their username, password and TOTP from their authentication app.

## Benefits and Improvements

The biggest security benefit of this application is the use of two factor authentication. This provides an extra layer of security, and acts as a preventative measure to a repudiation threat. In future iterations, the user experience can be improved by using SMS or email based authentication, which will negate the need for an extra application. Many services which provide this however are subscription based (Systemforce, 2024), which is why a QR code is currently the preferred course of action.

To further improve the security of the system, it is recommended the configuration is kept away from the source code, and not in plaintext (Snyk, 2024). Furthermore, the use of secure cookies will assist in protecting the user’s session (Singh, 2020).

## Future enhancements

This initial iteration of the system is used to demonstrate the proposed security measures for Colchester Groceries. Future enhancements will include:

* **Administrator Panel** This will provide the owner with the ability to modify stock from the system.
* **User enhancements** The user will be able to amend their details from the profile page, and change their password if forgotten.
* **Third party payment integration** The system will use a third party to securely handle payment options.

These enhancements will improve the user experience and leverage the flexibility provided by the use of object oriented programming.

## Sources

* Adams, D. (2024) Login System with Python Flask and MySQL. Available from <https://codeshack.io/login-system-python-flask-mysql/> [Accessed 01 July 2024].
* Grinberg, M. (2015). Two Factor Authentication with Flask. Available from: <https://blog.miguelgrinberg.com/post/two-factor-authentication-with-flask> [Accessed 09 July 2024].
* Singh, T. & Meenakshi (2020) Prevention of session hijacking using token and session id reset approach. *International journal of information technology* 12 (3): 781–788. DOI: 10.1007/s41870-020-00486-w
* Snyk.io. (2024) How to secure python flask applications. Available from: <https://dev.to/snyk/how-to-secure-python-flask-applications-2156> [Accessed 18 July 2024].
* Systemforce. (2024) Why Two-Factor Authentication is Important for Business Computer Security. Available from: <https://systemforce.co.uk/why-two-factor-authentication-is-important-for-business-computer-security/#:~:text=The%20cost%20of%20implementing%20two,several%20pounds%20per%20user%20annually>. [Accessed 22 July 2024].