

Title*:*

*“*SECURE APPLICATION DEVELOPMENT*”*

Program: BSC in Computing (Application Development)

Course: SECURE APPLICATION DEVELOPMENT

Supervisor: Fouzas Konstantinos

Student name: Manolis Saroukos

Word Count: 2.001

Table of Contents

[Introduction 2](#_Toc165284371)

[Requirements Analysis 3](#_Toc165284372)

[Analysis of the Code 3](#_Toc165284373)

[Basic Libraries: 3](#_Toc165284374)

[Database Design 4](#_Toc165284375)

[Login panel: 4](#_Toc165284376)

[Table of Recipes: 4](#_Toc165284377)

[User Design: 4](#_Toc165284378)

[Implementation: 4](#_Toc165284379)

[Safety: 4](#_Toc165284380)

[Continuous Integration: 4](#_Toc165284381)

[Security Measures 5](#_Toc165284382)

[Encrypt passwords: 5](#_Toc165284383)

[Data Validity Check: 5](#_Toc165284384)

[Protection against CSRF attacks: 5](#_Toc165284385)

[Access Restriction: 5](#_Toc165284386)

[Continuous Completion and Delivery 5](#_Toc165284387)

[Continuous Integration System 5](#_Toc165284388)

[Review process and problem solving 9](#_Toc165284389)

[Conclusions 18](#_Toc165284390)

[References 19](#_Toc165284391)

# Introduction

Computer program advancement could be a basic perspective of the cutting edge mechanical age and offers endless conceivable outcomes for creation and development. Be that as it may, the increment in complexity of applications combined with their far reaching open acknowledgment has made it essential to center on computer program security.

This investigate points to create a secure application computer program, utilizing present day hones and instruments that address the developing dangers from cybercriminals. The application created incorporates a database, a certification component and an get to control component, complying with the prerequisites of the errand.

The application too makes permits for planning of the tests and it is indispensable with Ceaseless Integration / Nonstop Conveyance (CI/CD) situations as well as the usage of inactive code analysis and security assessment instruments. SonarCloud may be a code investigation benefit. By coordination specifically with the CI pipeline or one of the backed DevOps stages, our code is tried against an broad set of rules covering numerous code traits, such as practicality, unwavering quality, and security issues in each merge/pull ask. In expansion, security measures were executed based on the OWASP security rules.

The application developed as part of the research is an online blog that gives users the opportunity to explore the world of gastronomy through a variety of recipes from around the world. By creating a personal account and logging in with their personal information, users open the door to a world full of flavors and aromas.

**Requirements Analysis**

Successful app development starts with a clear understanding of user requirements and the purpose of the app. This section details the functional requirements of our application and how they have been implemented.

* **User Login:** Users have the ability to log in to the app using a user email and password.
* **User Registration:**  Users have the ability to register in the application. All they need is a name, an email and a password.
* **Security:** The application ensures the security of user data by encrypting the data and protecting against attacks.
* View blog: users can see a list of great recipes from around the world.
* **User Response:** The application provides a quick response to user actions to ensure an excellent user experience.

# Analysis of the Code

## Basic Libraries:

The Python 3 Standard Library is a vast array of modules that you can use for developing various kinds of applications.

This application uses the libraries Flask, Flask-WTF, Flask-Bcrypt, Flask-MySQLdb and Flask-Login to develop a secure and functional web application. The use of these libraries allows the management of registration, logon and secure logout processes of users, as well as interaction with the MySQL database.

Bcrypt is a utility for encrypting files designed for various platforms. The utility uses the encryption blowfish algorithm.

# Database Design

MySQL, launched in 1995, has become the most popular open source database system. The popularity of MySQL and phpMyAdmin has allowed many non-IT specialists to create dynamic websites with MySQL support.

The application database consists of the following tables:

## Login panel:

* + Description: Stores information about users who have registered with the application.
  + Fields:
    - id: User ID number.
    - name: The name of the user.
    - email: The user's email.
    - password: The user's encrypted password.

## Table of Recipes:

* + - Id: ID number.
    - Title: the title of recipes.
    - Description: the description of recipes

## User Design:

* + A simple access control mechanism is implemented for the entry and registration of new users.

## Implementation:

* + The app implements the basic paths for entering, registering, logging out
  + Also, there are validity checks for email and password when registering new users.

## Safety:

* + The application uses secure practices to store passwords, using the bcrypt library for encryption.
  + In addition, there are checks on the validity of data entered by users.

## Continuous Integration:

* + The application is designed and implemented in order to develop a functional and secure web application, using software development best practices.

# Security Measures

Software security is a critical aspect to protect users and their data from various threats. Below are the security measures that have been implemented in the application:

## Encrypt passwords:

* + User passwords are encrypted before being stored in the database using the Bcrypt library. This ensures that even if the database is leaked, the codes remain secure.

## Data Validity Check:

* + Before saving to the database, the validity of the data entered by users is checked. For example, the format of the email and password is checked.

## Protection against CSRF attacks:

* + A secure CSRF (Cross-Site Request Forgery) mechanism is used using the Flask-WTF library.

## Access Restriction:

* + Some activities, such as viewing profiles or registering reviews, are protected from unauthorized access through Flask-Login's access control mechanism.

The above security measures are implemented in the application in order to provide maximum level of protection for its users.

## Continuous Completion and Delivery

This module demonstrates the use of continuous integration (CI) and delivery (CD) systems to automate the code development and testing process using SonarCloud and GitLab.

## Continuous Integration System

* CI/CD tool: The CI/CD process was implemented using GitLab CI to automate the completion and delivery process.
* SonarCloud integration: SonarCloud was used to continuously evaluate code quality and produce quality reports.
* CI/CD settings: Defined environment variables such as SONAR\_HOST\_URL and SONAR\_TOKEN, as well as sonarcloud-check to check the code in SonarCloud.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, εικονίδιο υπολογιστή

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

CI/CD process: Code changes are automatically reviewed with each commit using GitLab CI, while quality reports are automatically generated by SonarCloud.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

# Review process and problem solving

It appears that the audit found a Bandit security issue found in the code. This issue is related to running a Flask application with debug=True, which exposes the Werkzeug debugger and can potentially allow arbitrary code to run.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα To fix this issue, we should avoid running the Flask debug=True application in a production environment. Debugging can expose sensitive information and should only be used in development. We can set the debug parameter to False when running the Flask application in production:

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματα

Using remote artifacts without integrity checks can lead to malicious code execution in the application unexpectedly.

On the client side, where front-end code is running, malicious code could:

1. impersonating users' identities and exploiting their privileges in the application.
2. Add silent malware that monitors users' session and logs sensitive secrets.
3. Access sensitive customers' personal data.
4. alter or otherwise affect the general availability of the app.
5. Mine cryptocurrencies in the background.

Similarly, a compromised piece of software deployed in a server-side application could badly affect the security of the application. For example, server-side malware could:

1. Access and modification of sensitive technical and business data.
2. increase its privileges on the underlying operating system.
3. Use the compromised application as an axis to attack the local network.

By checking that a faraway thing is the right thing before using it, the app stays safe from any surprise changes made to it before getting it. Integrity checks can help find if something on a website was changed by malware or the author.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

Recommended secure coding practices

To check the integrity of a remote artifact, hash verification is the most reliable solution. It ensures that the file has not been modified since the fingerprint was calculated.

The src parameter specifies the URL from which the JavaScript script will be loaded.

The integrity parameter has the SHA-384 hash of the JavaScript code. This is used to make sure the script we are loading is the right one and has not been changed. If the code downloaded does not match the original code, the browser will not run it and will show an error.

The async and defer attributes are used to delay script execution until the entire HTML page is loaded, which can improve page performance.

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματα Because it is easy to extract strings from an application source code or binary, the credentials should not be encoded. This is especially true for distributed or open source applications.

Credentials must be stored outside of code in a configuration file, database, or secrets management service.

This rule highlights instances of hard-coded credentials that are used in database and LDAP connections. Looks for hard-coded credentials in connection strings and variable names that match any of the patterns from the provided list.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

I made an .env file containing the MY\_SECRET\_KEY then I can use the python-dotenv package to load these environment variables from the .env file into the Flask application.

Next, I use dotenv to load the environment variables from the .env file into the Flask application.

This way, the MY\_SECRET\_KEY will be loaded from the .env file and used as the secret key for the Flask application.

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματα

A CSRF attack happens when a hacker tricks a person using a website into doing things they didn't mean to do, like changing their profile or sending a message.

The bad person can trick the user into clicking on a link or visiting a bad website. This can make the user do something sensitive without knowing.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

CSRF is a way to hack into a website's security. There's a tool called OWASP ZAP that is often used to find security problems on websites.

By setting up CSRFProtect with Flask (csrf. init\_app(app)), you make sure that our app is safe from CSRF attacks. CSRFProtect helps protect our Flask app from CSRF attacks. By doing this, you make sure our app is safe from these attacks that could let someone do things they’re not supposed to do on behalf of someone who is allowed to.

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, λογισμικό, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματα

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, ιστοσελίδα

Περιγραφή που δημιουργήθηκε αυτόματα

# Conclusions

After looking at the app's security, we found that it has strong measures in place to keep data and users safe. Bcrypt makes sure passwords are safe from people who shouldn't have them. Furthermore, making sure the email and password are right when signing up makes the users' information more secure.

The CSRF (Cross-Site Request Forgery) measure also keeps app forms safe from cross-site request spoofing attacks. This makes sure that only requests from the same website can happen, so the application is safe from attacks.

Εικόνα που περιέχει κείμενο, λογισμικό, εικονίδιο υπολογιστή, λογισμικό πολυμέσων

Περιγραφή που δημιουργήθηκε αυτόματα

# References

Anon., 2023. *What is CI/CD?.* [Online]   
Available at: https://www.redhat.com/en/topics/devops/what-is-ci-cd

Ashutosh Kumar Sinha, S. T., 2019. *CookieArmor: Safeguarding against cross-site request forgery and session hijacking.* [Online]   
Available at: https://onlinelibrary-wiley-com.ezproxy.bolton.ac.uk/doi/full/10.1002/spy2.60

Bell, C., 2022. *MySQL Database Service Revealed: Running MySQL as a Service in the Oracle Cloud Infrastructure.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/mysql-database-service/9781484289457/?ar=&email=u0KPjMumntWAh2Q%2F1HtmBRg9cl6poWxc&tstamp=1713519296&id=254F853F0D66AB52D22F389CB3BA0C345B9AEC3E

Christopher Cowel, N. L. C. T., 2023. *Automating DevOps with GitLab CI/CD Pipelines.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/automating-devops-with/9781803233000/B18073\_FM.xhtml

Delisle, M., 2006. *Creating your MySQL Database: Practical Design Tips and Techniques.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/creating-your-mysql/9781904811305/?ar=&orpq=&email=u0KPjMumntWAh2Q%2F1HtmBRg9cl6poWxc&tstamp=1713519433&id=B741F37CBD4CD70BA5058DE3A7090801C1DDB8A4

GitLab, n.d. *Get started with GitLab CI/CD.* [Online]   
Available at: https://docs.gitlab.com/ee/ci/

Hellmann, D., 2017. *The Python 3 Standard Library by Example, Second Edition.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/the-python-3/9780134291154/

Ilham Firman Ashari, V. O. R. G. S. S. D., 2022. *Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools.* [Online]   
Available at: https://doaj.org/article/c6ccaf3674384f15b939208b1401fcb7

Jun Wang, W. L. K.-F. C., 2016. *Learning to Hash for Indexing Big Data—A Survey.* [Online]   
Available at: https://ieeexplore-ieee-org.ezproxy.bolton.ac.uk/document/7360966

Krogh, J. W., 2018. *MySQL Connector/Python Revealed: SQL and NoSQL Data Storage Using MySQL for Python Programmers.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/mysql-connector-python-revealed/9781484236949/?ar=&orpq=&email=u0KPjMumntWAh2Q%2F1HtmBRg9cl6poWxc&tstamp=1713514084&id=F8196F1747B40A04FC198947E9C2AB2AC79A52C0

Lott, S. F., 2018. *Functional Python Programming - Second Edition.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/functional-python-programming/9781788627061/

Molina, A., 2018. *Modern Python Standard Library Cookbook.* [Online]   
Available at: https://learning-oreilly-com.ezproxy.bolton.ac.uk/library/view/modern-python-standard/9781788830829/?ar=&orpq=&email=u0KPjMumntWAh2Q%2F1HtmBRg9cl6poWxc&tstamp=1713513418&id=865232EEB92882D4F0733BBFE830C7C1F2AA57B9

Paul, S. & Singh, A., 2020. *Hands-On Python Deep Learning for the Web.* [Online]   
Available at: https://prism.librarymanagementcloud.co.uk/bolton-ac/items/342198

Shelley, J., n.d. *Bcrypt.* [Online]   
Available at: https://www.solvusoft.com/el/file-extensions/software/johnny-shelley/bcrypt/

SonarCloud, n.d. *SonarCloud Documentation.* [Online]   
Available at: https://docs.sonarsource.com/sonarcloud/

Zhygulskyy, M., 2021. *Automated, Scheduled and Ci /Cd Web Injection.* [Online]   
Available at: https://www.proquest.com/docview/2586971494/fulltextPDF/159847D72E2C4A57PQ/1?accountid=9653&sourcetype=Dissertations%20&%20Theses