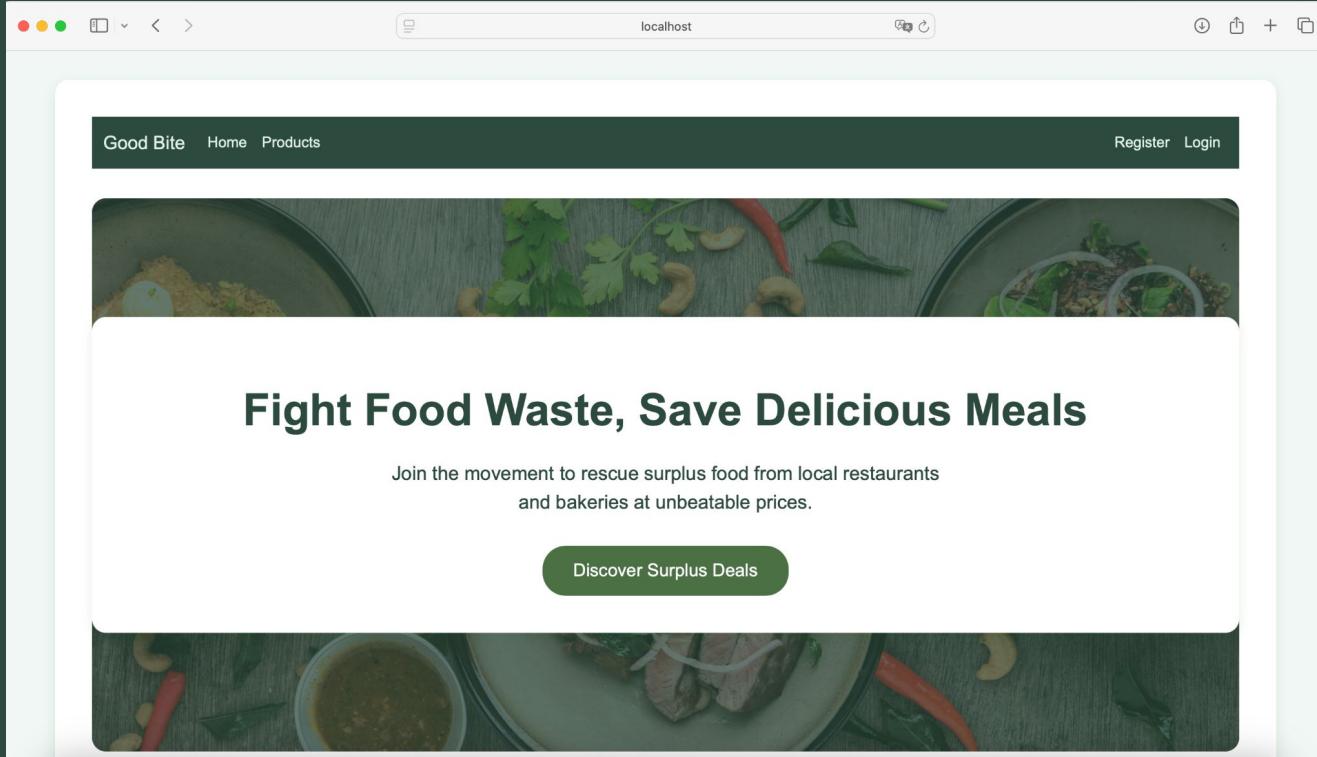




Good Bite App



The screenshot shows a web browser window for 'localhost' displaying the 'Good Bite' application. The header bar includes the 'Good Bite' logo, 'Home', 'Products', 'Register', and 'Login' links. Below the header is a large image of various food items like bowls of soup, sandwiches, and fresh vegetables. A central call-to-action text reads 'Fight Food Waste, Save Delicious Meals'. Below it, a subtext encourages users to join the movement to rescue surplus food from local restaurants and bakeries at unbeatable prices. A green button labeled 'Discover Surplus Deals' is visible. The footer of the page features a repeating image of the same food items.

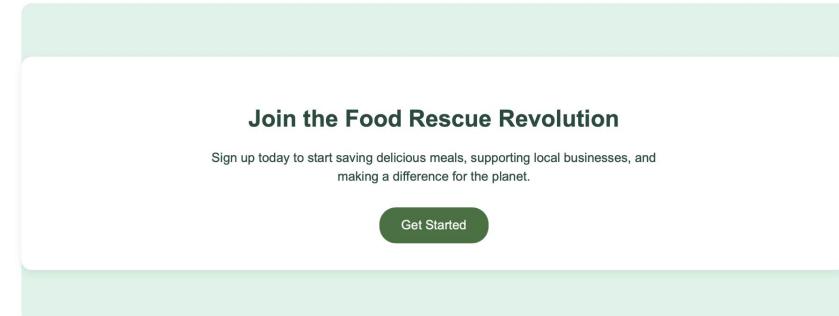
Good Bite Home Products Register Login

Fight Food Waste, Save Delicious Meals

Join the movement to rescue surplus food from local restaurants and bakeries at unbeatable prices.

Discover Surplus Deals

- Introduction and Basic Functionalities
- Security Features
 - Policies (Password, username, email, birthdate, phone)
 - Password protection in the database
 - Secure file uploads (only JPG and PNG files and a size not bigger than 5Mb)
 - Role-Based Access Control
 - MFA
 - Creating and installing an HTTPS server certificate
- Vulnerability Checks
- Problems Found
- Possible Improvements and Conclusion



The image shows a screenshot of a website for "Food Rescue Revolution". The header features the title "Join the Food Rescue Revolution" in bold black text. Below it is a subtext: "Sign up today to start saving delicious meals, supporting local businesses, and making a difference for the planet." At the bottom of the main content area is a green button labeled "Get Started".

Our project repository

GoodBite - Surplus Food Marketplace. 2025.
<https://github.com/sissamrcorreia/AS-project>

Home page.

Inspired by Too Good To Go

Goal: Reduce food waste by connecting sellers with surplus food to customers

Why Choose Good Bite?



Grab Surprise Bags

Enjoy curated mystery bags filled with delicious surplus food at up to 70% off.
Every bag is a tasty adventure!



Support Local

Partner with nearby eateries to save their unsold meals, helping small businesses thrive.



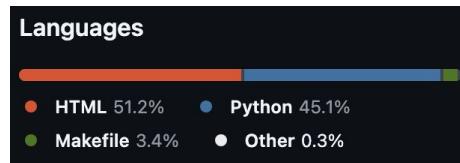
Save the Planet

Every bag you rescue reduces food waste and cuts CO2 emissions, making a real impact.



Commits over time: weekly from 6 Oct to 24 Nov.

Home page.



Programming languages used.

User Registration and Login

- Custom forms
- Password complexity and email validation
- Auto-login after signup
- New users start as Customer, request to be a Seller via email

Product Management

- Sellers: Create / Edit / Delete own products (name, description, price, stock, image)
- Everyone: View all products on products page
- Search bar (by name, description, seller name)

Profile Management

- Edit personal info, phone, birthday (min age 16)
- Upload / change profile picture
- Delete own account

Purchase Flow

- Customers can “buy” products
- Stock automatically updated

Admin Panel

- Change user roles and delete accounts
- Statistics dashboard (revenue, top sellers, low stock alerts...)

Policies (Password, username, email, birthdate, phone)

- Password: Size, difficulty
- Username, first name, last name: Size
- Email: Valid email address
- Birthdate: At least 16 years old
- Phone: Valid phone number

Password protection in the database

- PBKDF2 with SHA256 hash
- By Default (Recommended by NIST)
- Iterations: Slow down attackers
- Salt: Protect against rainbow attacks
- Other options:
 - Pbkdf2_sha1
 - Argon2
 - Scrypt

Password*

Your password can't be too similar to your other personal information.

Your password must contain at least 8 characters.

Your password can't be a commonly used password.

Your password can't be entirely numeric.

Password (again)*

[Home](#) [Login](#) [Register](#)

Register page. Password.

uriCustomer

Username:

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Password:

algorithm: pbkdf2_sha256 iterations: 100000 salt: GXqfs***** hash: MnZ7u8*****

[Reset password](#)

Raw passwords are not stored, so there is no way to see the user's password.

Admin page. Example of the password of a user.

Secure file uploads (only JPG and PNG files and a size not bigger than 5Mb)

Mitigated risks

- File upload attacks
- MIME type spoofing
- Oversized files causing DoS
- Improved UX with clear messages

The validations are implemented also in the profile where the user can have a profile photo.

Profile image:

Seleccionar archivo large-photo.jpg

- File too large. Size should not exceed 5 MB.

Profile page. File exceeding size example.

Image

Seleccionar archivo AS 25-26 Q1 v5.pdf



Upload a valid image. The file you uploaded was either not an image or a corrupted image.

Products page. Invalid file type example.

Image

Seleccionar archivo large-photo.jpg



File too large. Size should not exceed 5 MB.

Products page. File exceeding size example.

Role-Based Access Control

3 Available Roles

Admin: Full access, can assign/change roles for any user

Customer: End customer (view products, place orders, manage own account)

Seller: Vendor (manage products, manage own account)

Role Flow

- Every new user starts automatically as **Customer**
- Only **Admin** can promote or demote users to **Seller** or **Customer**

Technical Implementation

- Roles = Django Groups (Customer, Seller)
- Specific permissions defined per app/model
- Access control using `@permission_required`, `user.has_perm()`
- Role assignment done via Django Admin



Contact us if you want to be a seller: seller@goodbite.com

Source

Fahim Ahmed. (2024, Sep 25). Role-Based Access Control (RBAC) in Django.

Profile page of a Customer.

Role-Based Access Control

Good Bite Home Products

Logout Enable 2FA Profile

Products Page

Search by name, description or seller

SEARCH

CLEAR



Iberian Ham

Iberian ham from acorn-fed pigs, artisanally cured with an exceptional flavor.

Price: \$120.00**Stock:** 5 in stock

Seller: Oriol Ramos Puig

[BUY NOW](#)

Potato Omelette

Classic juicy Spanish omelette, with free-range eggs and garden potatoes.

Price: \$8.50**Stock:** 2 in stock

Seller: Cecilia Maria Rodrigues Correia

[BUY NOW](#)

Bread with Tomato

Slices of crispy bread with grated tomato and extra virgin olive oil.

Price: \$4.00**Stock:** 20 in stock

Seller: Cecilia Maria Rodrigues Correia

[BUY NOW](#)Contact support if you have any problems: support@goodbite.com*Products page of a Customer.*

Good Bite Home Products

Logout Enable 2FA Profile

Products Page

Search by name, description or seller

SEARCH

CLEAR



Iberian Ham

Iberian ham from acorn-fed pigs, artisanally cured with an exceptional flavor.

Price: \$120.00**Stock:** 5 in stock

Seller: Oriol Ramos Puig



Potato Omelette

Classic juicy Spanish omelette, with free-range eggs and garden potatoes.

Price: \$8.50**Stock:** 2 in stock

Seller: Oriol Ramos Puig

[Edit](#)[Delete](#)

Bread with Tomato

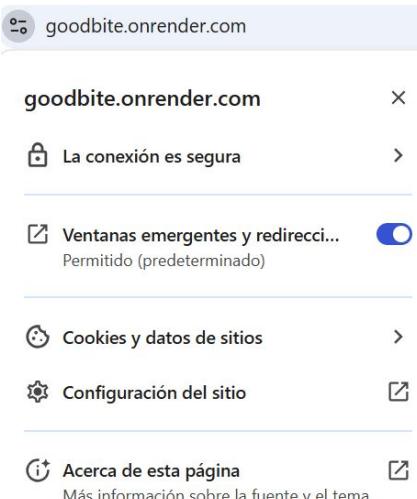
Slices of crispy bread with grated tomato and extra virgin olive oil.

Price: \$4.00**Stock:** 20 in stock

Seller: Cecilia Maria Rodrigues Correia

[Create New Product](#)Contact support if you have any problems: support@goodbite.com*Products page of a Seller.*

Creating and installing an HTTPS server certificate



goodbite.onrender.com

goodbite.onrender.com

La conexión es segura

Ventanas emergentes y redirecc... Permitido (predeterminado)

Cookies y datos de sitios

Configuración del sitio

Acerca de esta página



Seguridad goodbite.onrender.com

La conexión es segura

Tu información (por ejemplo, tus contraseñas o números de tarjeta de crédito) es privada cuando se envía a este sitio web. [Más información](#)

El certificado es válido



Visor de certificados: onrender.com

General Detalles

Enviado a

Nombre común (CN)	onrender.com
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	WE1
Organización (O)	Google Trust Services
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	jueves, 2 de octubre de 2025, 21:27:00
Vencimiento el	miércoles, 31 de diciembre de 2025, 21:26:56

Huellas digitales SHA-256

Certificado	d3788d482d4f24c5f8420e480eedcbef586cce40e6ee837360aa2087010d88af
Clave pública	61bc89d44874ba2ca54686fb6a889586860b827ec98ecd479e25d40eda5c5570

Render uses **Let's Encrypt** and **Google Trust Services** to issue certificates for your custom domain and automatically renews them before their expiration date.

Source

- Render. (n.d.). Fully Managed TLS Certificates – Render Docs. Retrieved from <https://render.com/docs/tls>
- Render. (n.d.). Cloud Application Platform | Render. Retrieved from <https://render.com/>

MFA

- As an additional layer of security to protect the login process.
- 2FA: user / password + code
- Time based One Time Password: TOTP (RFC6238)
 - Generates a code based on HMAC of a secret and the current time.
 - Temporal code generated by an auth app
- Django-AllAuth.MFA module



MFA - Flow

New users

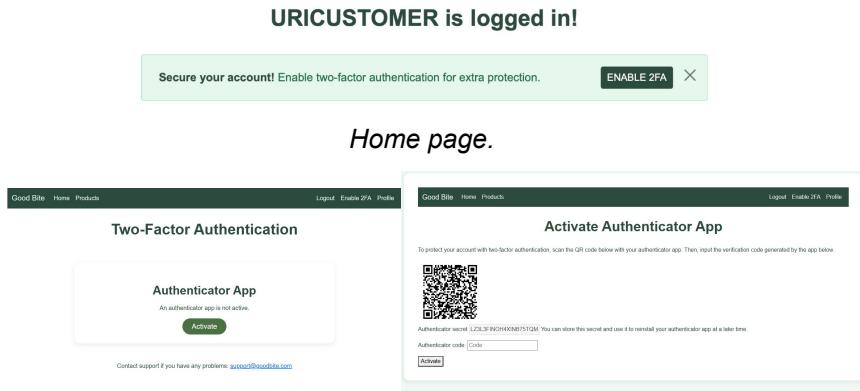
- User registration.
- Activate option.
- Select Auth App and scan QR.
- Auth App is enabled to perform 2FA.
- Next login, user is able to login with 2FA.



Good Bite Home Products Logout Enable 2FA Profile

URICUSTOMER is logged in!

Secure your account! Enable two-factor authentication for extra protection. **ENABLE 2FA** X



Good Bite Home Products Logout Enable 2FA Profile

Two-Factor Authentication

An authenticator app is not active.

Activate Authenticator App

To protect your account with two-factor authentication, scan the QR code below with your authenticator app. Then, input the verification code generated by the app below.

Authenticator secret: L2L5FJNQHDXNB75GQM. You can store this secret and use it to reinitialise your authenticator app at a later time.

Authenticator code: **Activate**

Contact support if you have any problems: support@goodbite.com

Enable 2FA page.

Users

- User log-in
- 2FA page.
- Insert Time based One Time Password.
- User enter to the web page.



Good Bite Home Products Register Login

Multi-Factor Authentication

Enter authentication code

Code*

Verify

Login page.

1st Vulnerabilities Check

Tools: pip-audit, Bandit

Findings:

- Hardcoded SECRET_KEY (low)
- App exposed via 0.0.0.0 (Medium)

Outcome: Minimal code review

2nd Vulnerabilities Check ASVS Review

Focus on OWASP ASVS 4.0.3 L1

Findings:

- Invalid data accepted (email, phone, birthdate)
- Long input broke UI (>500 chars)
- Weak MFA (no reauth)
- DEBUG=True & unsafe ALLOWED_HOSTS

Outcome: Several issues NOT OK.

Sources

Security linter for Python. <https://bandit.readthedocs.io>

Dependency vulnerability auditor. <https://pypi.org/project/pip-audit>

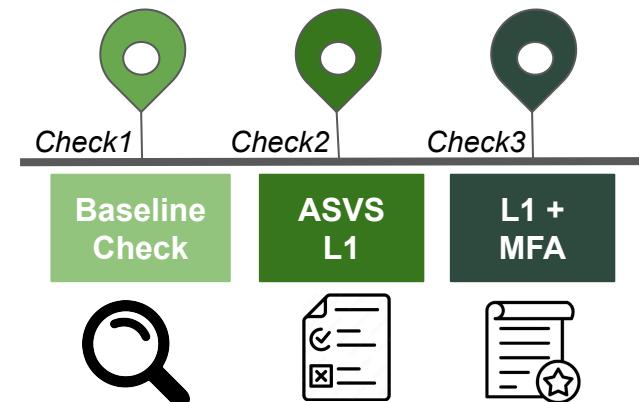
Application Security Verification Standard 4.0.3-es.pdf

3rd Vulnerabilities Check - Fix Validation + MFA

All previous issues fixed

- Robust input validation
- File upload protections working
- MFA functioning correctly
- RBAC & IDOR confirmed secure
- ALLOWED_HOSTS restricted
- DEBUG controlled via env variables

Outcome: Stable L1 compliance with targeted L2 improvements.



MFA

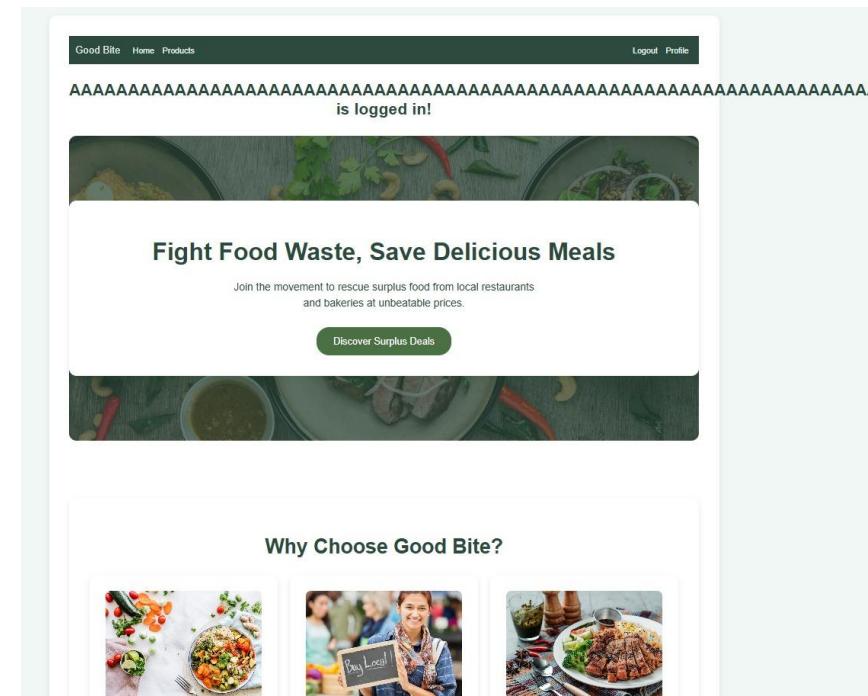
- The MFA library (allauth) removed the original registration form from our previous implementation.
- Challenging to maintain our desired user flow because of library constraints.
- Difficulties encountered when applying custom template styling to default MFA pages.

Certificate

- Initial attempt with a simple self-signed certificate resulted in a browser warning page.
- Created a Certificate Authority and signed the certificate, but the warnings persisted.
- Successfully resolved by deploying to production environment via Render.com.

Layout

- Lack of character limits on username, first name, and last name fields caused layout inconsistencies.



Home page with exceeded layout.

Possible improvements

- Implement content encryption, beginning with user profile photos.
- Expand payment options beyond the current "cash only" model to include card payments.
- Enhance product details with additional features such as allergen tags.
- Introduce filtering capabilities to complement the existing search functionality
- Add MFA requirements for high-risk actions.

Conclusions

- Using Django combined with Docker for environment consistency enabled more agile development.
- Integrating OWASP ASVS 4.0.3 throughout the development process allowed early vulnerability identification and ensured security was embedded from the ground up.
- Regular audit cycles facilitated the detection and resolution of coding and configuration errors, including validation gaps and insecure default settings.
- Resulting in a secure web application designed to combat food waste through controlled food sharing and comprehensive traceability.



Thank you!

The screenshot shows a web browser window with a dark green header bar. The header contains the logo "Good Bite" and navigation links "Home" and "Products" on the left, and "Register" and "Login" on the right. Below the header is a large banner image featuring various bowls of food and fresh ingredients like herbs and nuts. Overlaid on this banner is a white call-to-action box containing the text "Fight Food Waste, Save Delicious Meals" in bold, dark green font. Below this, a smaller text reads "Join the movement to rescue surplus food from local restaurants and bakeries at unbeatable prices." At the bottom of the call-to-action box is a green button with the text "Discover Surplus Deals".