Projekt „Wirtualna książka kucharska”

STUDIUM PRZYPADKU – PROGRAMOWANIE W GRUPIE PROGRAMISTYCZNEJ

Autorzy: Krzysztof Domian, BARTOSZ PIĄTKOWSKI, BARTOSZ SZTACHAŃSKI, JACEK FILIP – GRUPA c6

Spis treści

[**1.** **Struktura zespołu** 2](#_Toc124702418)

[**2.** **Założenia wstępne projektu** 2](#_Toc124702419)

[**3.** **Wnioski po rozmowie z inwestorami** 3](#_Toc124702420)

[**4.** **Bezpieczeństwo** 3](#_Toc124702421)

[**5.** **Prototypowanie i implementacja** 4](#_Toc124702422)

[**6.** **Testowanie** 5](#_Toc124702423)

# **Struktura zespołu**

Team Leader – Krzysztof Domian

Prototyp oraz implementacja – Bartosz Piątkowski

Bezpieczeństwo – Bartosz Sztachański

Testowanie – Jacek Filip

Nasz zespół jest spółką partnerską – jest to forma prawna, w której wiele osób łączy swoje siły i środki finansowe, w celu prowadzenia wspólnej działalności gospodarczej. Wszyscy wspólnicy solidarnie odpowiadają za zobowiązania spółki, a także są aktywnie zaangażowani w działalność spółki. Wspólnicy decydują solidarnie o kierunku rozwoju spółki i podejmują decyzje dotyczące jej działalności.

# **Założenia wstępne projektu**

Projekt ma na celu stworzenie wirtualnej książki kucharskiej, na której użytkownicy będą mogli przeglądać i przeszukiwać przepisy kulinarne oraz udostępniać i wprowadzać własne przepisy. Strona zawierać będzie przepisy podzielone na kategorie (deser, przystawka, danie główne, zupa i tym podobne) oraz opcje wyszukiwania i filtrowania przepisów według wielu konkretnych kryteriów takich jak np. składniki, czas przygotowania czy poziom trudności przyrządzenia dania, co pozwoli im korzystać z książki wedle swoich własnych preferencji, swojej własnej diety, a także wielu innych czynników. Użytkownicy będą mogli zakładać swoje własne konta, w celu zapisywania przepisów i posiadania ich „pod ręką”. Planujemy również dodać opcję komentowania i oceniania przepisów innych użytkowników. Wirtualna książka będzie responsywna oraz dostępna na wielu urządzeniach, a także zgodna ze standardami web designu. Będzie ona również zabezpieczona, zgodna ze standardami ochrony danych osobowych, a także testowana. Nadzór nad całym projektem prowadził będzie nasz Team Leader – Krzysztof Domian, który również stworzył założenia wstępne projektu. Za bezpieczeństwo całego projektu odpowiadać będzie Bartosz Sztachański. Implementacją oraz prototypem całej książki zajmie się Bartosz Piątkowski. Jeśli chodzi o testowanie, to nasz specjalista – Jacek Filip całkowicie poświęci temu zagadnieniu uwagę.

# **Wnioski po rozmowie z inwestorami**

Po rozmowie z inwestorami, nasz Team Leader – Krzysztof Domian doszedł do wielu wniosków oraz wymagań, z którymi wirtualna książka kucharska powinna się zgadzać, a także je spełniać. Wymienione są one poniżej:

* Wirtualna książka kucharska powinna być tworzona w zgodzie z najnowszymi standardami web designu
* Inwestorzy zwracają szczególną uwagę na potrzebę wysokiej funkcjonalności, aby ułatwić korzystanie ze strony
* Według inwestorów, wysokim priorytetem jest wysokie bezpieczeństwo oraz prywatność użytkowników
* Jedną z sugestii inwestorów było rozważenie opcji reklamowych dla firm zajmujących się gastronomią
* Kolejnym wnioskiem jest kompatybilność książki z wieloma urządzeniami, zarówno mobilnymi jak i stacjonarnymi
* Regularna aktualizacja przepisów i sprawowanie administracji nad książką, aby zwiększyć zainteresowanie ze strony potencjalnych użytkowników
* Personalizacja całej wirtualnej książki według preferencji użytkowników
* Inwestorzy sugerują również opcję integracji z platformami społecznościowymi takimi jak Facebook czy Instagram
* Możliwy jest kontakt z zespołem tworzącym projekt i sprawującym nad nim pieczę
* Inwestorzy sugerują utrzymanie wysokiej aktywności użytkowników poprzez organizowanie różnych konkursów czy wręczanie nagród najbardziej aktywnym użytkownikom
* Jednym z głównych priorytetów jest też stworzenie przyjaznego dla użytkownika interfejsu, który będzie łatwy w obsłudze

# **Bezpieczeństwo**

Aby utworzyć bezpieczną stronę wirtualnej książki kucharskiej z możliwością logowania i płatności, należy zastosować następujące zabezpieczenia:

1. Szyfrowanie połączenia: Wszelkie informacje przesyłane przez stronę powinny być szyfrowane za pomocą protokołu SSL/TLS, aby zapobiec przechwyceniu i ujawnieniu danych przez osoby trzecie.

2. Ochrona haseł: Hasła użytkowników powinny być przechowywane w bezpieczny sposób, np. za pomocą funkcji hashowania i soli. Warto również wymagać od użytkowników, aby tworzyli hasła o odpowiedniej sile.

3. Uwierzytelnianie dwustopniowe: Można rozważyć wprowadzenie uwierzytelniania dwustopniowego, aby zwiększyć bezpieczeństwo logowania użytkowników.

4. Ochrona przed atakami typu cross-site scripting (XSS): Strona powinna być zabezpieczona przed atakami typu XSS, które pozwalają atakującemu na wstrzykiwanie złośliwego kodu JavaScript do strony internetowej.

5. Ochrona przed atakami typu SQL injection: Strona powinna być również zabezpieczona przed atakami typu SQL injection, które pozwalają atakującemu na wstrzykiwanie złośliwego kodu SQL do bazy danych.

6. Ochrona przed atakami typu cross-site request forgery (CSRF): Strona powinna być zabezpieczona przed atakami typu CSRF, które pozwalają atakującemu na wykonywanie nieautoryzowanych żądań z poziomu strony internetowej.

7. Płatności: W przypadku obsługi płatności warto korzystać z bezpiecznych i sprawdzonych systemów płatniczych, takich jak np. PayPal czy Blik.

Oprócz tych zabezpieczeń warto również regularnie wykonywać testy penetracyjne, aby sprawdzić, czy strona jest odporna na różne rodzaje ataków i czy nie ma żadnych luk w zabezpieczeniach. Ponadto, warto zainstalować skanery bezpieczeństwa, które będą monitorować stronę i w razie wykrycia jakichkolwiek niepokojących zachowań lub potencjalnych ataków, natychmiast zawiadamiać o tym administratora.

Ważne jest również, aby zapewnić odpowiednie zabezpieczenia dla serwera, na którym będzie hostowana strona, oraz aby regularnie aktualizować oprogramowanie i system, aby zapobiec ewentualnym atakom.

Oprócz tych zabezpieczeń, należy również pamiętać o konieczności ochrony danych osobowych użytkowników zgodnie z przepisami o ochronie danych osobowych, takimi jak RODO.

Oprócz zabezpieczeń technicznych, istotne jest również zapewnienie odpowiedniego zarządzania bezpieczeństwem informacji na stronie. Można to zrobić poprzez:

1. Tworzenie polityki bezpieczeństwa informacji: Można opracować politykę bezpieczeństwa informacji, w której określi się zasady dotyczące ochrony danych osobowych, haseł, płatności itp.

2. Ustanowienie procedur postępowania w razie incydentu: Warto mieć przygotowane procedury postępowania w razie incydentu, takie jak wyciek danych osobowych czy atak hakerski, aby móc szybko i skutecznie reagować w takich sytuacjach.

# **Prototypowanie i implementacja**

Prototyp wirtualnej książki opublikowany został na githubie, pod linkiem <https://github.com/Rui0o/cook-book-C7>, znajduje się tam cały prototyp, który wykonał Bartosz Piątkowski, a po późniejszym skonsultowaniu się z Team Leaderem – Krzysztofem Domianem, dokonali oni poprawek i ulepszeń, co nie zmienia faktu, że jest to wersja testowa książki kucharskiej.

# **Testowanie**

**Testy przeprowadzone na stronie internetowej**

* Testy funkcjonalne

Weryfikacja systemu bez wnikania w kod źródłowy. Testowane zostały elementy takie jak poprawność wyświetlania elementów na stronie (menu, grafiki, tekst), przechodzenie pomiędzy podstronami oraz powrót do strony głównej, działanie koszyka zakupowego. Sprawdzone zostały także odnośniki oraz poprawność językowa oraz stylistyczna.

* Testy kompatybilności

Weryfikacja czy strona działa na różnych przeglądarkach. Zostały również przeprowadzone testy kompatybilności oraz skalowania strony na urządzeniach mobilnych takich jak smartfon oraz tablet.

* Testy wydajnościowe

Przeprowadzono testy wydajnościowe mające na celu weryfikacje działania strony internetowej pod jej oczekiwanym obciążeniem.

* Testy przeciążeniowe

Przeprowadzono testy weryfikujące działanie strony internetowej na granicy swoich zasobów takich jak pamięć oraz procesor.

* Testy obciążeniowe

Zweryfikowano działanie strony internetowej podczas gdy potęguję się jej obciążenie. Zwiększano liczbę użytkowników zalogowanych na stronie.

* Testy bezpieczeństwa

Z racji z tego, że nasza strona posiada możliwość logowania oraz dokonywania płatności zostały przeprowadzone testy bezpieczeństwa pod kątem osłony oraz mechanizmów bezpieczeństwa, które chronią system przed atakami z zewnątrz.