

Plan testów aplikacji e-commerce

1. Cel testów

Celem testów jest weryfikacja, czy aplikacja e-commerce działa zgodnie z założeniami funkcjonalnymi i niefunkcjonalnymi. Testy mają na celu zidentyfikowanie błędów związanych z działaniem aplikacji, interakcjami użytkownika oraz bezpieczeństwem danych.

2. Zakres testów

Testy będą obejmować:

- Rejestrację i logowanie użytkowników.
- Dodawanie, edycję i usuwanie produktów w koszyku.
- Proces zakupowy, w tym wyświetlanie ceny produktów, łącznej wartości koszyka oraz finalizację zamówienia.
- Panel administracyjny dostępny dla użytkowników o roli "admin".
- Zabezpieczenia danych użytkowników (szyfrowanie hasła, ochrona przed atakami typu Rainbow Table i brute-force).
- Bezpieczeństwo transmisji danych przez HTTPS.

3. Strategia testowania

Testowanie aplikacji zostanie przeprowadzone przy użyciu następujących technik:

- **Testy funkcjonalne:** Testowanie zgodności działania aplikacji z wymaganiami (np. dodawanie produktów do koszyka, logowanie).
- **Testy bezpieczeństwa:** Testy ochrony danych użytkowników (szyfrowanie haseł, zabezpieczenia przed SQL Injection).
- **Testy wydajnościowe:** Sprawdzanie, jak aplikacja reaguje na duże obciążenia (np. jednoczesne zakupy przez wielu użytkowników).
- **Testy regresyjne:** Sprawdzanie, czy wprowadzenie zmian nie wprowadza nowych błędów.
- **Testy akceptacyjne:** Potwierdzenie, że aplikacja spełnia oczekiwania użytkowników końcowych i może być wdrożona.

4. Elementy do przetestowania

- Formularz rejestracji i logowania.
- Koszyk: dodawanie, edycja, usuwanie produktów.
- Przycisk "Buy" i przekierowanie do płatności.
- Wyświetlanie cen i łącznego kosztu.
- Panel administracyjny.
- Szyfrowanie haseł i zabezpieczenia danych.
- Transmisja danych przy użyciu HTTPS.

5. Elementy, które nie będą testowane

- Integracja z zewnętrznymi systemami płatności (zakładamy, że jest testowana niezależnie).
- Optymalizacja graficzna i interfejsu użytkownika (UI) (testy wizualne są przeprowadzane osobno).

6. Zasoby

- **Testerzy:** 2 osoby do testów manualnych, 1 osoba do testów bezpieczeństwa.
- **Narzędzia:**
 - Testowanie funkcjonalności: Cypress.
 - Testowanie bezpieczeństwa: OWASP ZAP.
 - Testowanie wydajności: JMeter.
 - Narzędzie do zarządzania testami: JIRA/Trello.

7. Harmonogram testów

Etap	Czas trwania	Opis
Przygotowanie przypadków testowych	2 dni	Przygotowanie test cases dla wszystkich funkcjonalności
Testy funkcjonalne	4 dni	Testowanie rejestracji, logowania, koszyka, procesu zakupowego
Testy bezpieczeństwa	3 dni	Testowanie szyfrowania haseł, ochrony przed atakami brute-force, SQLi
Testy wydajnościowe	2 dni	Testy obciążeniowe przy zakupach i dodawaniu produktów do koszyka
Testy regresyjne	2 dni	Sprawdzanie zgodności po wprowadzeniu ewentualnych poprawek
Testy akceptacyjne	1 dzień	Testowanie aplikacji z udziałem klienta lub zespołu produktowego

8. Kryteria zakończenia testów

Testy zostaną zakończone, jeśli:

- Wszystkie krytyczne i wysokie błędy zostaną naprawione.
- 95% przypadków testowych zakończy się sukcesem.
- Testy bezpieczeństwa potwierdzą brak krytycznych podatności.

9. Kryteria wejścia i wyjścia

Kryteria wejścia:

- Specyfikacja wymagań funkcjonalnych i technicznych została ukończona.
- Środowisko testowe jest gotowe do testów.
- Przypadki testowe zostały przygotowane i zatwierdzone przez zespół QA.

Kryteria wyjścia:

- Wszystkie testy funkcjonalne zostały przeprowadzone.
- Wszystkie błędy krytyczne zostały naprawione.
- Wyniki testów wydajnościowych są zgodne z wymaganiami.

10. Ryzyka i ograniczenia

- Możliwość opóźnień z powodu naprawy błędów krytycznych.
- Ograniczenia sprzętowe lub zasoby serwera mogą wpłynąć na wyniki testów wydajnościowych.
- Zmiany w specyfikacji w trakcie testowania mogą wymagać aktualizacji przypadków testowych.