# **Nazwa use casu’u**

Logowanie użytkownika do systemu

# **Wstęp**

Przypadek użycia opisuje proces logowania użytkownika do systemu, który wymaga weryfikacji tożsamości poprzez sprawdzenie nazwy użytkownika i hasła.

# **Cel use casu’u**

Celem jest autoryzacja użytkownika do dostępu do zasobów systemu po pomyślnym uwierzytelnieniu.

# **Lista aktorów**

* Użytkownik
* Administrator (w przypadku problemów z logowaniem)

# **Przebieg use case’u**

**Krok 1:** Użytkownik wprowadza swoją nazwę użytkownika.

**Krok 2:** Użytkownik wprowadza swoje hasło.

**Krok 3:** System weryfikuje wprowadzone hasło.

* **Jeśli hasło jest poprawne:** Przejdź do kroku 4.
* **Jeśli hasło jest niepoprawne:** Przejdź do kroku 5.

**Krok 4:** System wyświetla pulpit klienta, udostępniając dostęp do zasobów.

**Krok 5:** System sprawdza liczbę prób logowania:

* **Jeśli liczba prób < 3:** Użytkownik może ponownie wprowadzić hasło.
* **Jeśli liczba prób ≥ 3:** Przejdź do kroku 6.

**Krok 6:** System blokuje możliwość dalszych prób i powiadamia administratora o problemie z logowaniem.

# **Wyjątki**

**E1:** Niepowodzenie trzech prób logowania skutkuje czasowym zablokowaniem konta i powiadomieniem administratora.

# **Przebiegi alternatywne**

Brak

# **Zagadnienia implementacyjne**

* **Bezpieczeństwo:** Ważne jest, aby system korzystał z bezpiecznych metod przechowywania i weryfikacji haseł, np. poprzez szyfrowanie.
* **Wydajność:** System powinien być w stanie szybko reagować na próby logowania, nawet przy dużym obciążeniu.
* **Zarządzanie błędami:** Powinny być zaimplementowane mechanizmy informujące użytkownika o błędach logowania oraz zalecenia co do dalszych kroków.

# **Warunki rozpoczęcia use case’u**

Użytkownik nie może być zalogowany

# **Stan końcowy**

Użytkownik jest zalogowany i ma dostęp do swojego pulpitu klienta lub jego próby logowania są zablokowane i sprawa została przekazana administratorowi.

# **Nierozwiązane problemy**

# Mechanizmy zabezpieczające przed atakami brute-force: Obecnie system nie ma pełnych mechanizmów obrony przed atakami typu brute-force, które mogą prowadzić do nieautoryzowanego dostępu.