1. **Na jakie testy (funkcjonalne, wydajności, bezpieczeństwa) należy według Ciebie położyć szczególny nacisk i dlaczego?**

W przypadku usługi sieciowej udostępniającej informacje prywatne, takie jak umowy ubezpieczeniowe, należy szczególnie zwrócić uwagę na testy bezpieczeństwa. Należy zweryfikować, czy usługa jest odporna na ataki typu SQL Injection, XSS czy inne ataki sieciowe. Istotne jest również testowanie autoryzacji i uwierzytelnienia, aby zapobiec nieautoryzowanemu dostępowi do informacji.

Jednocześnie należy przetestować funkcjonalność usługi, aby upewnić się, że działa ona zgodnie z dokumentacją i spełnia wymagania biznesowe. Testy wydajnościowe powinny również być wykonane, aby upewnić się, że usługa jest w stanie obsłużyć przepływ ruchu sieciowego oraz przetwarzanie danych w czasie rzeczywistym.

**2. Jakie testy usługi mógłbyś wykonać jako analityk (masz dostęp wyłącznie do danych źródłowych, usługi i dokumentacji, nie masz dostępu do kodu usługi czy logów serwera)?**

Jako analityk mógłbym przeprowadzić następujące testy usługi:

Testy jednostkowe weryfikujące poprawność działania poszczególnych funkcji w usłudze na podstawie dokumentacji.

Testy integracyjne sprawdzające, czy interakcje między poszczególnymi komponentami usługi działają poprawnie, zgodnie z dokumentacją i wymaganiami biznesowymi.

Testy funkcjonalne polegające na weryfikacji zgodności z wymaganiami biznesowymi oraz dokumentacją.

Testy bezpieczeństwa, w tym testowanie ataków typu SQL Injection, XSS oraz innych podobnych ataków.

Testy wydajnościowe weryfikujące, czy usługa działa zgodnie z oczekiwaniami pod względem czasu odpowiedzi oraz wydajności przetwarzania danych.

**3. Jakie zmiany zaproponowałbyś w celu poprawienia użyteczności, wydajności i bezpieczeństwa tej usługi?**

Aby poprawić użyteczność, można dodać możliwość filtrowania umów według określonych kryteriów, na przykład daty zawarcia umowy, wysokości składki, czy też rodzaju ubezpieczenia. Dodanie funkcjonalności sortowania wyników pozwoliłoby użytkownikom na łatwe i szybkie znalezienie poszukiwanych informacji.

W celu poprawy wydajności można zastosować mechanizmy pamięci podręcznej (cache), które przechowywałyby wyniki zapytań dla określonych peseli, co umożliwiłoby szybsze i bardziej efektywne przetwarzanie zapytań. Można także ograniczyć liczbę zwracanych wyników lub wprowadzić limit czasu na przetwarzanie zapytań, co zmniejszyłoby obciążenie serwera.

W celu zwiększenia bezpieczeństwa, należy zadbać o uwierzytelnianie użytkowników, np. poprzez implementację autoryzacji OAuth2, co pozwoli na zabezpieczenie dostępu do usługi przed nieuprawnionymi użytkownikami. Należy także zadbać o to, aby przesyłane dane były szyfrowane (np. poprzez protokół HTTPS), co zabezpieczyłoby je przed podsłuchiwaniem oraz zapobiegłoby możliwości ich modyfikacji przez osoby trzecie. Dodatkowo, warto monitorować logi zapytań i odpowiedzi, aby wykryć i zwalczać próby ataków z zewnątrz oraz wewnętrznych zagrożeń.  
  
*Informacja: Odpowiedź na pytanie wygenerowana przy pomocy ChatGPT-3*