warsaw new tech university FOUNDATION

ul. Przasnyska 4, lokal U2
01-756 Warszawa,
katecheo@wntuf.pl,
www.wntuf.pl

katecheo.pl

Zapytanie ofertowe
na przeprowadzenie kompleksowego audytu platformy katecheo.pl.

DANE ZAMAWIAJĄCEGO:
Warsaw New Tech University Foundation
ul. Przasnyska 4, lok

I. WPROWADZENIE

1. Cel zamówienia

Celem zamówienia jest przeprowadzenie kompleksowego audytu platformy katecheo.pl, ukierunkowanego na ocenę jej bezpieczeństwa, wydajności, interoperacyjności i dostępności.

2. Kontekst przedmiotu zamówienia

Katecheo.pl to aplikacja internetowa budowana w ramach projektu "Katecheo.pl" finansowanego z budżetu państwa w ramach programu NAUKA DLA SPOŁECZEŃSTWA II. Jej celem jest integracja działania środowiska związanego z nauczaniem katechetycznym i nowym modelem kształcenia. Powstająca obecnie aplikacja oferuje nieograniczony dostęp do materiałów dydaktycznych dla katechetów, instytucji katolickich i innych osób, zainteresowanych poszerzaniem wiedzy z zakresu religii w formie cyfrowej biblioteki. Materiały dotyczące zagadnień katechetycznych podane są w sposób uporządkowany poprzez multifunkcyjną wyszukiwarkę. Katecheci mogą tworzyć i udostępniać własne sylabusy i lekcje w postaci interaktywnych materiałów (teksty/konspekty/prezentacje multimedialne/filmy wideo/ linki do materiałów źródłowych).

II. ZAKRES ZAMÓWIENIA

W ramach prac Wykonawca powinien wykonać:
1. analizę techniczną aplikacji katecheo.pl
2. analizę w zakresie cyberbezpieczeństwa

katecheo.pl - Projekt finansowany ze środków budżetu państwa, przyznanych przez Ministra Nauki i Szkolnictwa Wyższego w ramach Programu „Nauka dla Społeczeństwa II".

Ministerstwo Nauki i Szkolnictwa Wyższego

NAUKA DLA SPOŁECZEŃSTWA

3. ocenę zgodności z zasadami opisanymi w ustawie o interoperacyjności
4. badanie i ocenę spełnienia zasad dostępności cyfrowej
5. przygotowanie dokumentacji audytowej

Poniżej opisano szczegółowy zakres każdego z obszarów.

1. Analiza techniczna aplikacji

Analiza techniczna aplikacji Katecheo musi obejmować:

- analizę architektury systemu, w szczególności: ocenę przyjętej architektury systemu, przegląd poszczególnych modułów składowych aplikacji, identyfikację odstępstw od założonego wzorca architektonicznego i czynników mogących utrudnić rozwój i skalowanie aplikacji
- ocenę jakości kodu źródłowego, w szczególności: przegląd kodu źródłowego pod kątem czytelności, spójności, nazewnictwa, wydajności, zgodności ze standardami języka, zduplikowanego kodu, analizę testowalności i pokrycia testami, analizę struktury katalogów kodu źródłowego,
- ocenę wydajności, stabilności i skalowalności rozwiązania, w szczególności: przeprowadzenie testów wydajnościowych aplikacji pod obciążeniem w celu identyfikacji wąskich gardeł wydajnościowych oraz miejsc potencjalnych i faktycznych wycieków zasobów, ocenę efektywności czasowej zapytań do bazy danych, analizę rzeczywistego zużycia pamięci przez aplikację.
- identyfikację potencjalnych obszarów ryzyka technologicznego, w szczególności: identyfikację przestarzałych bibliotek i frameworków, identyfikację fragmentów kodu pochodzących z zewnętrznych źródeł.

2. Analiza w zakresie cyberbezpieczeństwa

Analiza w zakresie cyberbezpieczeństwa musi obejmować:

- przeprowadzenie testów penetracyjnych w formule Gray-box testing, obejmujące rekonesans, analizę i próbę obejścia mechanizmów uwierzytelniania i autoryzacji, próby eskalacji uprawnień, ataki typu injection i XSS

- próbę ataków z wykorzystaniem gotowych narzędzi (np. OWASP ZAP, Nmap, Metasploit)
- przegląd kodu źródłowego oraz analizę statyczną kodu w celu identyfikacji podatności i zagrożeń w zakresie co najmniej OWASP Top 10
- analizę zależności, obejmującą ręczny przegląd bibliotek pod kątem znanych podatności oraz analizę z użyciem automatycznych skanerów (np. Snyk, OWASP Dependency-Check)
- analizę środowiska, w tym weryfikację konfiguracji serwera WWW, systemu operacyjnego, usług sieciowych i portów,
- rekomendacje działań naprawczych i zabezpieczających.

3. Ocena zgodności z zasadami opisanymi w ustawie o interoperacyjności

Ten obszar obejmuje ocenę zgodności z zasadami interoperacyjności systemów teleinformatycznych używanych przez podmioty publiczne opisanymi w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r.w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Ocena ma obejmować zgodność z minimalnymi wymaganiami dla systemów teleinformatycznych w następujących obszarach:

- Wymagania przy projektowaniu, wdrażaniu i eksploatacji systemów teleinformatycznych
- Umożliwienie wymiany danych z innymi systemami teleinformatycznymi
- Standardy kodowania znaków
- Formaty udostępniania zasobów informacyjnych i przyjmowania danych elektronicznych
- System zarządzania bezpieczeństwem informacji
- Elektroniczne zapisy w dziennikach systemów (logi)

4. Badanie i ocena spełnienia zasad dostępności cyfrowej

Badanie i ocena spełnienia zasad dostępności cyfrowej, zgodnie z wymaganiami ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych musi obejmować poniższe zadania:

- audyt interfejsu użytkownika (UI) pod kątem dostępności,
- analiza kodu aplikacji pod względem zgodności z WCAG 2.1 na poziomie AA,
- opracowanie zaleceń usprawniających dostępność aplikacji.

Podczas każdego badania Wykonawca przeanalizuje co najmniej 8 aktywnych ekranów aplikacji reprezentujących możliwie jak najszerszy zakres funkcjonalności. Zdefiniowana próba badawcza powinna zawierać:

- ekran startowy;
- funkcja logowania;
- komponent nawigacji głównej aplikacji;
- ekran z informacjami kontaktowymi;
- ekrany pomocy technicznej;
- ekrany zawierające informacje prawne;
- co najmniej jeden ekran istotny dla każdego rodzaju usługi świadczonej poprzez interfejs aplikacji;
- co najmniej jeden dokument do pobrania lub wyświetlenia istotny dla każdego rodzaju usługi;
- ekran z deklaracją dostępności.

5. Przygotowanie dokumentacji audytowej

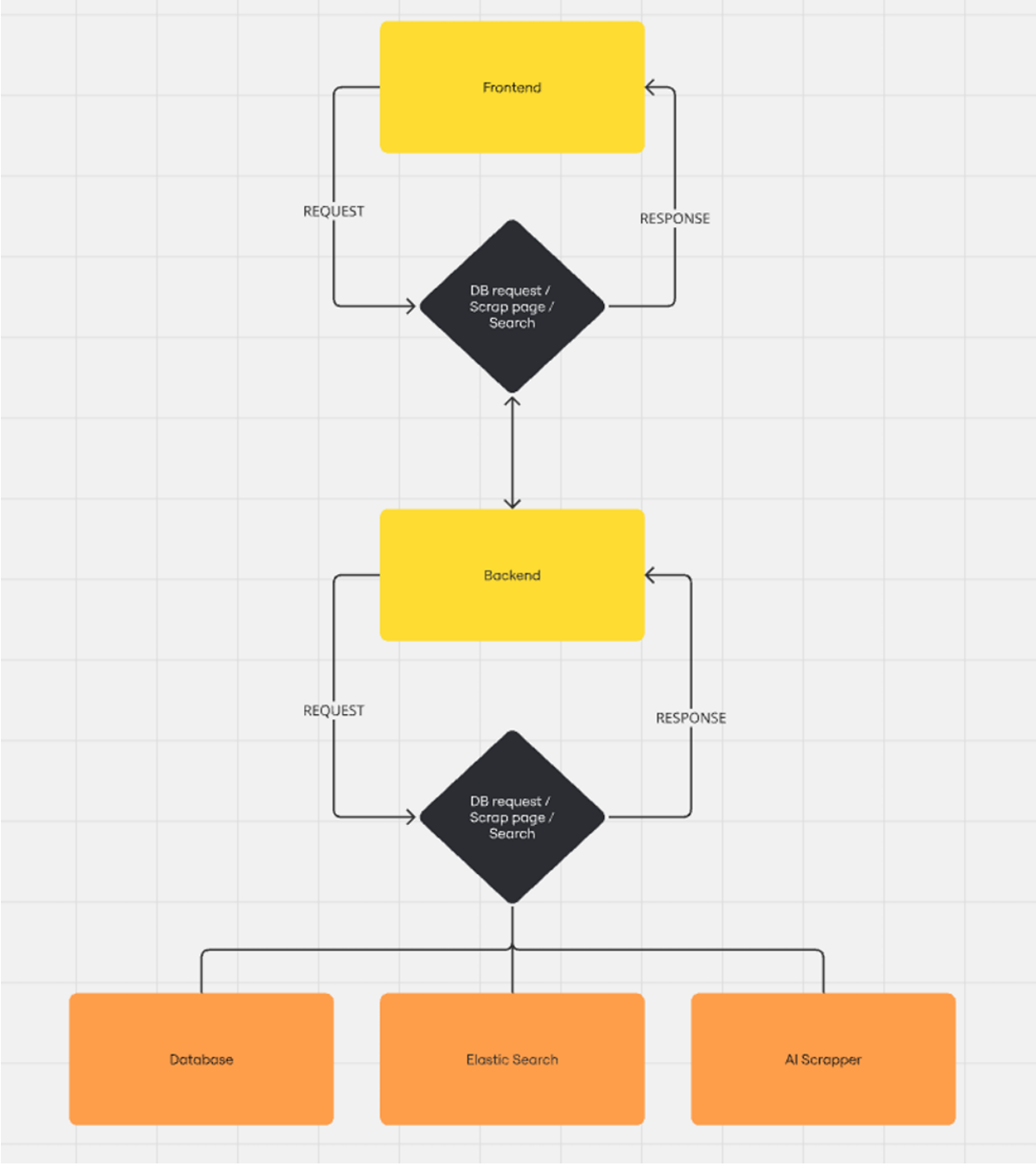
Dla każdego z wymienionych obszarów powinien przygotować dokument zawierający:

- szczegółowy raport z przeprowadzonej analizy, obejmujący wszystkie aspekty wymienione w opisie zakresu dla danego obszaru
- wykaz wykrytych niezgodności
- rekomendacje naprawcze

III. OPIS TECHNICZNY APLIKACJI

1. Architektura aplikacji

Aplikacja posiada architekturę frontend-backend. Architekturę aplikacji przedstawia poniższy diagram:



Najważniejsze komponenty wchodzące w skład aplikacji:

- **Frontend** – aplikacja frontendowa wykonana w technologii Next.js (React) odpowiedzialna za renderowanie treści, komunikację z bazą danych oraz wysyłanie zapytań użytkownika do serwera ElasticSearch oraz scrappera AI za pośrednictwem aplikacji backendowej.
- **Backend** – aplikacja backendowa wykonana w technologii NestJS (Node.js). Odpowiada za komunikację pomiędzy warstwą frontendową, a bazą danych, serwerem ElasticSearch oraz scraperem AI.
- **Baza danych** – relacyjna baza danych MySQL
- **Scrapper AI** – aplikacja wykonana w technologii Python odpowiedzialna za scrapowanie stron internetowych do formatu kompatybilnego ze strukturą danych w bazie mysql. Aplikacja odbiera żądanie ze strony backendu, łączy się ze wskazaną witryną internetową, pobiera jej treść, przetwarza do formatu JSON i odsyła do serwera backendowego
- **ElasticSearch** – silnik indeksowania treści i optymalizacji procesu wyszukiwania. W bazie ElasticSearch zapisywane są wyłącznie materiały zatwierdzone do publikacji przez administratorów serwisu

Zamawiający udostępni Wykonawcy pełne kody źródłowe wraz z instrukcją uruchomienia aplikacji.

2. Wykorzystane technologie

Aplikacja wykorzystuje poniżej wymienione technologie:

- Node.js - środowisko uruchomieniowe komponentu Backend
- NestJS - podstawowy framework komponentu Backend
- NextJS - framework komponentu Frontend
- MySQL - relacyjny silnik bazy danych
- ElasticSearch - silnik indeksowania treści i optymalizowania procesu wyszukiwania

3. Środowisko wdrożeniowe

Aplikacja wdrożona jest na pojedynczej maszynie wirtualnej. Specyfikacja maszyny jest następująca:

- CPU 8 rdzeni 3,5 Ghz

- RAM 12 GB

4. Baza danych

Baza danych aplikacji to baza relacyjna oparta o silnik MySQL. Model danych składa się z 31 tabel.
Baza wdrożona jest na serwerze w postaci pojedynczej instancji.
Backup całościowy bazy wykonywany jest 1 raz dziennie. Przechowywany jest backup z 7 ostatnich dni.

IV. WARUNKI ŚWIADCZENIA USŁUGI

1. Zamawiający w terminie do 2 dni roboczych od dnia podpisania Umowy, przekaże Wykonawcy kod źródłowy oraz dokumentację techniczną aplikacji.
2. Wykonawca w terminie do 2 dni roboczych od dnia podpisania Umowy, przedstawi Zamawiającemu szczegółową metodykę audytu oraz harmonogram audytu. W ramach ww. prac Wykonawca przedstawi:
    a. procedurę przeprowadzenia audytu;
    b. opis narzędzi, urządzeń i oprogramowania wykorzystywanego w audycie;
    c. harmonogram audytu.
3. Po zatwierdzeniu harmonogramu przez Zamawiającego, Wykonawca będzie mógł wprowadzić zmiany do harmonogramu jedynie za pisemną zgodą Zamawiającego.
4. Wykonawca na potrzeby wykonania usługi musi zapewnić niezbędne narzędzia, oprogramowanie, licencje wspierające przeprowadzenie analizy.
5. Zamawiający udostępni Wykonawcy kod źródłowy aplikacji, instrukcję uruchomienia oraz zapewni dostęp do wybranych środowisk wdrożeniowych.
6. W ramach audytu Wykonawca zapewni wsparcie w interpretacji wyników oraz konsultacje w przypadku jakichkolwiek pytań lub wątpliwości.
7. Wykonawca zobowiązany jest do stałej roboczej współpracy z Zamawiającym. Komunikacja będzie odbywać się pomiędzy

wyznaczonymi przedstawicielami Zamawiającego oraz przedstawicielami Wykonawcy. Za podstawową formę wymiany informacji uznaje się drogę elektroniczną.

8. Wykonawca będzie zobowiązany do zachowania trwałości zespołu realizującego przedmiot zamówienia. Wszelkie zmiany będą wymagały akceptacji Zamawiającego oraz weryfikacji dokumentów potwierdzających kompetencje, doświadczenie i certyfikaty.
9. Wykonawca będzie świadczył usługi zgodnie z umową.
10. Wszystkie prace muszą zostać wykonane w uzgodnionym harmonogramie, nieprzekraczającym 10 dni roboczych od dnia podpisania umowy.
11. Wykonawca zapewnia, że wszystkie dane oraz informacje pozyskane podczas audytu będą traktowane jako poufne i chronione.
12. Wykonawca zobowiązuje się wykonać przedmiot Umowy ze starannością wynikającą z zawodowego charakteru prowadzonej przez niego działalności, zgodnie z zasadami profesjonalizmu zawodowego, a także zgodnie z obowiązującymi w tym zakresie przepisami.
13. Wykonawca oświadcza, że posiada odpowiednią wiedzę specjalistyczną, doświadczenie i personel, gwarantujące prawidłowe wykonanie przedmiotu Umowy.
14. Wykonawca zobowiązuje się do udzielania Zamawiającemu pełnej informacji na temat postępu i zakresu wykonanych przez Wykonawcę prac.

V. WYMAGANIA DOTYCZĄCE ZESPOŁU WYKONUJĄCEGO AUDYT

1. Wymaga się, aby Wykonawca dysponował zespołem, w skład którego wejdą co najmniej 3 osoby, które posiadają poniżej opisane kwalifikacje:

a) Ekspert ds. cyberbezpieczeństwa

- Wykształcenie wyższe informatyczne
- Minimum 3 lata doświadczenia w zakresie audytów bezpieczeństwa aplikacji webowych
- Doświadczenie w przeprowadzaniu testów penetracyjnych (Gray-box)

- Znajomość narzędzi takich jak: OWASP ZAP, Burp Suite, Nmap, Metasploit, Snyk, OWASP Dependency-Check
- Znajomość standardów OWASP Top 10 i ISO/IEC 27001
- Umiejętność analizy kodu źródłowego pod kątem bezpieczeństwa
- Certyfikaty (co najmniej jeden z poniższych):
    - CEH (Certified Ethical Hacker)
    - OSCP (Offensive Security Certified Professional)
    - CompTIA Security+
    - CISA lub CISM

b) Ekspert ds. analizy technicznej aplikacji webowych

- Wykształcenie wyższe informatyczne
- Minimum 3 lata doświadczenia w analizie architektury i kodu aplikacji webowych
- Doświadczenie w pracy z technologiami: Node.js, NestJS, Next.js, MySQL, ElasticSearch
- Umiejętność przeprowadzania testów wydajnościowych i identyfikacji wąskich gardeł
- Znajomość zasad projektowania skalowalnych systemów
- Znajomość narzędzi do analizy jakości kodu (np. SonarQube, ESLint)

c) Ekspert ds. dostępności cyfrowej i zgodności z WCAG

- Znajomość WCAG 2.1 na poziomie AA
- Doświadczenie w przeprowadzaniu audytów dostępności dla aplikacji webowych
- Znajomość narzędzi do analizy dostępności (np. axe, WAVE, Lighthouse)
- Znajomość przepisów ustawy o dostępności cyfrowej

2. Wymogi dodatkowe dla całego zespołu:
    - Co najmniej jedna osoba w zespole musi posiadać doświadczenie w projektach dla podmiotów publicznych lub w audytach systemów zgodnych z KRI (Krajowe Ramy Interoperacyjności)
    - Wszyscy członkowie zespołu muszą posługiwać się językiem polskim w mowie i piśmie na poziomie umożliwiającym swobodną komunikację z Zamawiającym

VI. KRYTERIA OCENY OFERT

Kryterium oceny ofert stanowi cena - waga 100%
Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do przedłożenia dokumentów potwierdzających kwalifikacje do realizacji zadania.

VII. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

1. Oferta powinna być przesłana za pośrednictwem poczty elektronicznej na adres email: katecheo@wntuf.pl lub dostarczona do biura na adres ul. Przasnyska 4, lokal U2, 01-756 Warszawa w terminie do 30 kwietnia 2025 r. do godziny 11.00.
2. Oferent powinien stworzyć ofertę na formularzu opublikowanym razem z niniejszym zapytaniem.
3. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
4. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania bez podania przyczyny.