PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

NR BST-P6/076/10/2021

Warszawa, dnia 29.03.2021 r.

Z A P Y T A N I E O I N F O R M A C J Ę

Zwracamy się do Państwa o udzielenie informacji cenowej dotyczącej wykonania usługi audytu wydajności, możliwości rozwoju oraz audytu bezpieczeństwa systemu Bilkom (OPCJA) wraz z przygotowaniem raportów z przeprowadzonych audytów.

W szczególności przedmiot zamówienia obejmuje:

I. Przeprowadzenie audytu wydajności i możliwości rozwoju systemu Bilkom na podstawie analizy kodu źródłowego wraz z przygotowaniem raportu z audytu.
II. Przeprowadzenie audytu kodu źródłowego systemu Bilkom pod kątem bezpieczeństwa wraz z przygotowaniem raportu z audytu (OPCJA).
III. Dodatkowe wymagania względem Wykonawcy.

I. <u>Przeprowadzenie audytu wydajności i możliwości rozwoju systemu Bilkom na podstawie analizy kodu źródłowego wraz z przygotowaniem raportu z audytu</u>:

1. Zamawiający przekaże Wykonawcy kod źródłowy, dokumentację oraz skrypty testów systemu Bilkom po podpisaniu umowy o zachowaniu poufności.
2. Zakres prac analitycznych:
   2.1. Analiza architektury i jakości kodu powinna objąć następujące obszary:
      2.1.1. analizę jakości kodu w zakresie architektury, rozumianą jako weryfikację stosowania dobrych praktyk wytwarzania oprogramowania oraz zastosowania wzorców projektowych,
      2.1.2. analizę jakości kodu w zakresie czytelności, rozumianą jako weryfikację dobrych praktyk i zasad dotyczących czytelności i czystości kodu, implementacji zasad formatowania, nazewnictwa modułów, klas, metod i zmiennych, organizacji kodu oraz odpowiedniego dokumentowania kodu,
      2.1.3. identyfikację odstępstw od standardów,
      2.1.4. identyfikację zastosowanych technologii (w tym frameworki), ocenę ich zasadności i poprawności ich użycia, analiza kosztów ich utrzymania, kosztów rozwoju i kosztów wprowadzania zmian, stopień łatwości w pozyskaniu pracowników znających technologie użyte w aplikacji,
      2.1.5. weryfikację wykorzystanych bibliotek w ramach wykonywanych procesów biznesowych oraz zgodności przekazanego kodu projektu i kodu bibliotek,

2.1.6. identyfikację i oszacowanie ryzyk architektonicznych w kontekście wzrostu ilości danych wynikające z działalności operacyjnej,
2.1.7. identyfikację ryzyk związanych z unikalnością stosowanych technologii informatycznych,
2.1.8. ocenę łatwości utrzymania i rozwoju oprogramowania,
2.1.9. ocenę stabilności i poprawności działania,
2.1.10. ocenę skalowalności kodu źródłowego,
2.1.11. ocenę modularności i łatwości rozwoju kodu,
2.1.12. ocenę stopnia pokrycia testów jednostkowych oraz ich jakości,
2.1.13. ocenę stopnia pokrycia testów integracyjnych i systemowych,
2.1.14. analizę optymalizacji i stopnia normalizacji bazy danych,
2.1.15. oszacowanie długu technologicznego, braków dokumentacji itp.,
2.1.16. ocenę zgodności ze standardem WCAG 2.0.,
2.1.17. ocenę zgodności z pracą w trybie RWD.

2.2. Testy wydajności:
2.2.1. analiza skalowalności, testy obciążeniowe, analiza możliwości zwiększenia obciążenia i ilości użytkowników pracujących na aplikacji i w systemach (przy założeniu 5 tys. aktywnych użytkowników).

II. Przeprowadzenie audytu kodu źródłowego systemu Bilkom pod kątem bezpieczeństwa wraz z przygotowaniem raportu z audytu:

1. Wykonawca w ramach usługi audytu bezpieczeństwa systemu Bilkom przeprowadzi:
   1.1. analizę podatności serwisów www w trybie black-box oraz w trybie white-box,
   1.2. analizę bezpieczeństwa konfiguracji serwerów aplikacji, baz danych, mechanizmów bezpieczeństwa,
   1.3. analizę bezpieczeństwa kodu źródłowego (statyczna analiza kodu, inspekcji kodu).
2. W ramach prac zostaną przeprowadzone następujące działania:
   2.1. realizacja audytu bezpieczeństwa, połączenie audytu automatycznego i manualnego,
   2.2. analiza, przygotowanie i ustalenie scenariusza testów, wykonanie testów, analiza powykonawcza,
3. W ramach świadczenia usługi audytu dostarczony zostanie raport końcowy zawierający minimum, następujące sekcje:
   3.1. sumaryczną ocenę poziomu bezpieczeństwa serwisów www,
   3.2. jednostkową ocenę poziomu bezpieczeństwa serwisów www,
   3.3. trendy wskazujące kierunki podnoszenia bezpieczeństwa serwisów www,

3.4. sumaryczną klasyfikację wykrytych podatności bezpieczeństwa dla każdego serwisu www, objętego analizą podatności,
3.5. klasyfikację wykrytych podatności bezpieczeństwa dla każdego serwisu www objętego analizą podatności,
3.6. opis zagrożeń bezpieczeństwa wynikających ze zidentyfikowanych podatności dla każdego serwisu www, objętego analizą podatności,
3.7. opis aktualnego poziomu bezpieczeństwa dla serwisu www objętego analizą podatności,
3.8. rekomendację wskazującą kierunki dalszego podnoszenia bezpieczeństwa dla każdego serwisu www objętego analizą podatności.

4. W ramach audytu dostarczone zostaną szczegółowe raporty bezpieczeństwa wskazujące kierunki dalszego podnoszenia bezpieczeństwa usług, stanowiące załączniki do raportu końcowego z analizy podatności serwisów www, zawierające minimum następujące sekcje:
   4.1. wprowadzenie (Introduction),
   4.2. podsumowanie (Summary),
   4.3. wykryte podatności posortowane według typu (Issues Sorted by Issue Type),
   4.4. zalecenia dotyczące usunięcia wykrytych podatności (Fix Recommendations),
   4.5. porady dotyczące wykrytych podatności (Advisories),
   4.6. dane, parametry i adresy wykorzystane podczas analizy podatności (Application Data).
5. Dostarczone szczegółowe raporty bezpieczeństwa muszą przyjąć formę nawigowalnego dokumentu PDF, wygenerowanego z narzędzia do badania/wykrywania podatności serwisów www.
6. Analiza podatności serwisów www przeprowadzona zostanie z wykorzystaniem narzędzia do badania/wykrywania podatności serwisów www klasy Enterprise. Producent ww. narzędzia znajduje się w grupie/kwadracie „Leaders”, zgodnie z raportem Gartner – Magic Quadrant for Application Seciurity Testing (Kwiecień 2019 r.).
7. Narzędzie wykorzystane do przeprowadzania badania/wykrywania podatności serwisów www musi posiadać funkcjonalność zautomatyzowanego skanowania serwisów www (WAS - Web Application Scanner).
8. Narzędzie wykorzystane do przeprowadzania badania/wykrywania podatności serwisów www musi posiadać funkcjonalność zautomatyzowanego skanowania serwisów www, w zakresie WebService (WSDL), w technologiach .NET oraz Java.

III. Dodatkowe wymagania względem Wykonawcy:

1. Wykonawca przez cały okres trwania umowy musi mieć aktywną umowę o zachowaniu poufności z Zamawiającym.
2. Pracownicy Wykonawcy muszą posiadać odpowiednie doświadczenie poparte certyfikatami:

PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

2.1. OSCP (Offensive Security Certified Professional) lub równoważne,
2.2. Offensive Security Certified Expert (OSCE) lub równoważne,

3. Wykonawca musi posiadać doświadczenie w przeprowadzaniu audytów w powyższym zakresie ujętym w pkt I – na tą okoliczność zobowiązany jest legitymować się co najmniej 5 zakończonymi audytami przeprowadzonymi w okresie ostatnich 3 lat.
4. Wykonawca musi posiadać doświadczenie w przeprowadzaniu audytów w powyższym zakresie ujętym w pkt II – na tą okoliczność zobowiązany jest legitymować się co najmniej 5 zakończonymi audytami przeprowadzonymi w okresie ostatnich 3 lat.
5. Metodologia testowania aplikacji:
   5.1. OWASP ASVS,
   5.2. PCI DSS,
   5.3. PTES.

Odpowiedź powinna zawierać:

Lp.	Nazwa	Ilość	Czas przeprowadzenia audytu (ilość dni)	Cena netto (PLN)	Podatek vat (PLN)	Cena łączna brutto (PLN)
I.	Przeprowadzenie audytu wydajności i możliwości rozwoju systemu Bilkom na podstawie kodu źródłowego wraz z przygotowaniem raportu z audytu	**1**				
II.	Przeprowadzenie audytu kodu źródłowego systemu Bilkom pod kątem bezpieczeństwa wraz z przygotowaniem raportu z audytu (OPCJA)	**1**				

**Zamawiający dopuszcza możliwość złożenia informacji cenowej na jeden ze wskazanych w tabeli przedmiotów zapytania.*

Termin składania informacji upływa **w dniu 09.04.2021 r. o godzinie 12:00**
(ewentualne pytania prosimy kierować **do dnia 01.04.2021 r. do końca dnia.**
Odpowiedź proszę przesłać w formie e-mail na adres: **it@intercity.pl**

„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.