Załącznik nr 1

- Szczegółowy opis przedmiotu zamówienia

Przedmiotem Zamówienia jest przeprowadzenie Audytu wydajności oraz bezpieczeństwa kodu i aplikacji Systemu Informatycznego. Audyt obejmować będzie spełnienie przez Wykonawcę Systemu wymagań pozafunkcjonalnych dotyczących bezpieczeństwa Systemu oraz bezpieczeństwa przetwarzanych w nim danych.

Celem audytu jest ustalenie, czy wydajność aplikacji osiąga zakładany poziom oraz wykrycie faktycznych oraz potencjalnych podatności i luk Systemu oraz jego Kodu źródłowego wraz z identyfikacją błędów konfiguracji i błędów programowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub Użytkowników Systemu. Przeprowadzenie audytu na etapie wytwarzania i przekazywania do użytkowania Systemu pozwolić ma na dostarczenie odbiorcom projektu rozwiązań gwarantujących osiągnięcie wymaganego poziomu bezpieczeństwa w fazie użytkowania.

W ramach Przedmiotu Zamówienia Wykonawca Audytu zobowiązany jest do wykonania poniższych Zadań:

1. audyt wydajności
2. audyt Kodu źródłowego
3. audyt bezpieczeństwa Systemu
4. testy penetracyjne Systemu
5. ocena bezpieczeństwa przetwarzania danych osobowych
6. ocena końcowa bezpieczeństwa Systemu

Audyt zostanie przeprowadzony w dwóch etapach, obejmujących:

1. Istniejące obecnie elementy Systemu
2. Warstwę wymiany danych z SIO (Systemem Informacji Oświatowej) za pośrednictwem API (moduł w trakcie implementacji, planowany termin ukończenia: wrzesień 2023)

Wykonawca po wykonaniu audytów i testów przedstawi raporty, które zawierać będą m.in. przyjęte założenia badawcze i uzasadnienie wyboru technik i metod badania, dokumentację wykonanych prac, wyniki wraz z ich interpretacją, identyfikację niezgodności z wymaganiami i założeniami oraz luk i błędów Systemu, analizę wyników oraz rekomendacje dotyczące usunięcia niezgodności oraz luk i błędów Systemu, a także rekomendacje dotyczące poprawy bezpieczeństwa Systemu, zmian w architekturze oraz Kodzie źródłowym, ze szczególnym uwzględnieniem punktu widzenia potrzeb dalszego jego utrzymania oraz rozwoju, uwzględniając najlepsze praktyki stosowane przy wytwarzaniu, utrzymaniu, rozwoju oraz dokumentowaniu systemów informatycznych.

Audyt bezpieczeństwa Systemu, testy penetracyjne Systemu oraz audyt Kodu źródłowego obejmują wykonanie po jednym re-teście/re-audycie w ramach realizacji Przedmiotu Zamówienia, po dokonaniu przez Wykonawcę zmian w Systemie na podstawie rekomendacji przedstawionych w raportach poaudytowych i potestowym. Ponowne audyty i testy oznaczają weryfikację wszystkich podatności wymienionych w danym raporcie.

Podsumowaniem prac będzie Raport końcowy bezpieczeństwa Systemu oraz Raport bezpieczeństwa przetwarzania danych osobowych. Wyniki ponownych audytów oraz testów zostaną uwzględnione w ocenie końcowej bezpieczeństwa Systemu i ujęte w obydwu raportach

końcowych. Raport końcowy bezpieczeństwa Systemu będzie zawierał identyfikację i ocenę długu technologicznego wraz z rekomendacjami.

Zakres prac

W ramach Zamówienia, Wykonawca Audytu będzie zobowiązany do świadczenia usług polegających na wykonywaniu Zadań wskazanych w Przedmiocie Zamówienia w zakresie bezpieczeństwa Systemu i przetwarzanych w nim danych, w tym ich poufności, integralności, dostępności, autentyczności, rozliczalności, niezaprzeczalności oraz niezawodności.

Zakres prac będzie obejmował analizę i ocenę realizacji przez Wykonawcę Systemu wymagań w zakresie bezpieczeństwa, zleconych Wykonawcy.

Audyty wydajności aplikacji będą przeprowadzone przy realizowaniu 2 scenariuszy z planowanym obciążeniem 15 000 – 20 000 użytkowników równocześnie i obejmować będą:

1. przygotowanie scenariuszy
2. przygotowanie skryptów
3. wynajęcie serwerów do zasymulowania obciążenia wraz z konfiguracją
4. wykonanie testów
5. analizę wyników
6. przygotowanie raportu

Audyty bezpieczeństwa Systemu oraz Kodu źródłowego obejmować będą co najmniej:

1. określenie powierzchni ataku
2. określenie obszarów podwyższonego ryzyka
3. identyfikacja klas podatności oraz stopnia zagrożenia

Ocena bezpieczeństwa Systemu oraz Kodu źródłowego z perspektywy podatności na ataki obejmować będzie co najmniej:

1. weryfikację metod uwierzytelniania i autoryzacji
2. weryfikację metod dostępu do baz danych
3. weryfikację procesu logowania
4. weryfikację istnienia backdoorów
5. weryfikację wykorzystania zewnętrznych bibliotek (i ich wersji) pod kątem użycia podatnych (niebezpiecznych lub niewspieranych) wersji bibliotek
6. weryfikacji kodu na możliwość przeprowadzenia ataków z uwzględnieniem metodologii OWASP

Zakres audytu Kodu źródłowego będzie obejmować co najmniej:

1. audyt podatności na ataki, w tym co najmniej:
    - SQL Injection
    - Cross-Site Scripting (XSS)
    - Cross-Site Request Forgery (CSRF)
    - Server-Side Request Forgery (SSRF)
    - ataki Man-In-The-Middle
    - ataki na hasła
2. audyt jakości wykonanych testów automatycznych (zasięg i pokrycie)

3. audyt czytelności kodu źródłowego oraz obecności i jakości komentarzy w nim umieszczonych
4. audyt wydajności Kodu źródłowego wraz ze wskazaniem najistotniejszych „wąskich gardeł” („bottleneck”), jeśli takowe zostaną zidentyfikowane
5. audyt optymalizacji oraz normalizacji baz danych
6. audyt kosztów modyfikacji podczas utrzymania i rozwoju Systemu.

Testy penetracyjne Systemu Informatycznego zostaną zrealizowane poprzez określenie faktycznego stanu bezpieczeństwa polegające na symulacji prób złamania lub ominięcia zabezpieczeń. W trakcie testów zastosowane będą metody i narzędzia, którymi zwykle posługują się potencjalni napastnicy. Zidentyfikowane podatności są wykorzystywane do przejęcia kontroli nad testowanymi systemami oraz do dalszych prób eskalacji ataku. Umożliwi to określenie potencjalnej skali naruszenia bezpieczeństwa, która wystąpi, jeśli te podatności zostaną wykorzystane przez atakujących. Testy obejmować będą następujące obszary:

1. testy penetracyjne serwera WWW
2. testy penetracyjne serwera aplikacyjnego
3. testy penetracyjne aplikacji (komponenty dostępne publicznie)
4. testy penetracyjne aplikacji (po uwierzytelnieniu)
5. testy penetracyjne interfejsów bazy danych
6. testy penetracyjne bazy danych z poziomu użytkownika
7. do 5 rbh konsultacji z testerami przy realizacji projektu

Realizacja Przedmiotu Zamówienia obejmie wykonanie testów automatycznych (identyfikacja podatności występujących w Systemie i jego Kodzie źródłowym przy pomocy automatycznych narzędzi testujących) oraz testów manualnych (przeprowadzanych ręcznie przez testera).

W ramach testów penetracyjnych zostaną wykorzystane dwa rodzaje testów:

1. black box (z minimalną wiedzą o audytowanym Systemie)
2. white box (z pełną wiedzą i kontem użytkownika w audytowanym Systemie)

Audytom oraz testom penetracyjnym podlegać będzie System Informatyczny funkcjonujący w określonym środowisku Zamawiającego. Baza danych udostępnionego Systemu będzie pusta, w gestii wykonawcy leżeć będzie wypełnienie jej danymi testowymi.
Testy penetracyjne Systemu będą przeprowadzane na instancjach przeznaczonych do testowania (nieprodukcyjnych).
Prace mogą wymagać obecności Wykonawcy w siedzibie Zamawiającego.

Opis Systemu

Środowisko

Serwer DB:

- Rocky Linux 8.6
- PostgreSQL 14.4

Serwer WWW:

- Rocky Linux 8.6

- nginx 1.23.1

Serwer aplikacji:

- Rocky Linux 8.6
- JRE 17.0.4
- Spring, Spring Boot

Kod

Wartości przybliżone.

Język / technologia	**Pliki**	**Linie kodu**
Java	150	20 000
HTML	60	7 800
Javascript	49	6 300
CSS	35	4 900