Załącznik nr 2
do zamówienia nr IBE/82/2023
Opis przedmiotu zamówienia

Szczegółowy Opis Przedmiotu Zamówienia

Testy i re-testy bezpieczeństwa dla aplikacji webowej “Moje Portfolio”

Informacje dotyczące zamówienia

1. Zamawiający:

Instytut Badań Edukacyjnych

ul. Górczewska 8, 01-180 Warszawa

2. Informacje o Zamawiającym

Zamówienie będzie wykonane w ramach realizowanego przez Instytut Badań Edukacyjnych (IBE) projektu systemowego „Wspieranie funkcjonowania i doskonalenie ZSK na rzecz wykorzystania oferowanych w nim rozwiązań do realizacji celów strategii rozwoju kraju", współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach programu Operacyjnego Wiedza, Edukacja, Rozwój, Priorytet II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji, Działanie 2.13 Przejrzysty i spójny Krajowy System Kwalifikacji.

Głównym celem tego projektu jest wspieranie rozwoju Zintegrowanego Systemu Kwalifikacji (ZSK) w Polsce. Jednym z działań realizowanych w jego ramach jest rozwój metod i narzędzi walidacji efektów uczenia się.

3. Cel zamówienia

Celem zamówienia jest przeprowadzenie testów bezpieczeństwa informatycznego dla aplikacji webowej „Moje Portfolio" (dalej jako „aplikacji") po udoskonaleniach wdrożonych w 2023 r. przez zewnętrznego wykonawcę.

4. Charakterystyka aplikacji

Aplikacja "Moje Portfolio" (https://mojeportfolio.ibe.edu.pl/), uruchomiona w 2018 r., to narzędzie, w którym można opisywać swoje kompetencje i gromadzić dowody na ich posiadanie (np. w formie dokumentów, zdjęć, nagrań), a także inne związane z tym informacje. Przeznaczona jest dla użytkowników indywidualnych i dostępna dla każdego bez ograniczeń. Posiada obecnie ponad 3000 użytkowników. Od czerwca 2021 r. aplikacja zawiera nowe funkcjonalności rozszerzające możliwości jej wykorzystania (m.in. do pracy z doradcą zawodowym za pomocą Metody Bilansu Kompetencji, zob. stronę: https://mbk.ibe.edu.pl/).

Aplikacja jest sprzężona z narzędziem wspierającym, jakim jest Baza Efektów Uczenia się ZSK (dalej jako BEU), gromadząca efekty uczenia się z kwalifikacji opublikowanych w Zintegrowanym Rejestrze Kwalifikacji. Są one pobierane z niego za pośrednictwem dedykowanego API. BEU jest oparta na wspólnej z Moim Portfolio bazie danych (MySQL).

W Moim Portfolio są wykorzystywane następujące technologie:

- PHP

- Laravel
- MySQL,
- HTML CSS – Boostrap
- Google Analytics

Aplikacja jest w architekturze własnej (nie w chmurze publicznej). Na czas realizacji zamówienia aplikacja będzie dostępna w środowisku testowym.

Obecnie aplikacja "Moje Portfolio" jest w przebudowie, w ramach prac programistycznych nastąpi m.in. aktualizacja PHP, MySQL oraz zmieni się struktura tabel.

Testy bezpieczeństwa będące przedmiotem zamówienia obejmują nową wersję aplikacji.

Makiety UX (low-fi) są dostępne tutaj:

UI: https://xd.adobe.com/view/64ad28b2-70ad-4e89-ba6e-9fd20363fdfd-31fe/

UI doradca: https://xd.adobe.com/view/c9edaeab-e9a0-4f8a-8e14-cfa60ae78a9a-9cbe/

Aplikacja w wersji docelowej będzie miała następujące unikalne funkcjonalności:

1. logowanie - w parze login/hasło, a ponadto
    a. z wykorzystaniem logowania FB,
    b. z wykorzystaniem logowania google,
    c. docelowo: z wykorzystaniem logowania za pomocą oddzielnej aplikacji Moja Walidacja (aplikacja planowana - powinna być gotowa w III kwartale 2023 roku),
2. rejestracja,
3. dodawanie doświadczeń użytkownika,
4. dodawanie kompetencji użytkownika,
5. budowanie teczki do udostępnienia doradcy,
6. budowanie CV z możliwością wygenerowania do pliku .doc oraz udostępnienie doradcy,
7. mechanizm wiadomości wewnętrznych,
8. mechanizm udostępnienia podglądu do całego konta doradcy,
9. mechanizm budowania planów rozwoju.

Moje Portfolio w docelowej wersji (po trwającej przebudowie) będzie zawierać następujące formularze:

1. Użytkownik
    a. użytkownik niezalogowany
        i. kontakt,
        ii. rejestracja,
        iii. logowanie,
        iv. przypomnij hasło,
    b. użytkownik zalogowany
        i. formularz edycji danych danych podstawowych konta,
        ii. edycja danych do logowania,
        iii. formularze budowane na bazie jednego wzoru:
            1. dodawanie wykształcenia,
            2. dodawanie doświadczenia zawodowego,
            3. dodawanie kursu / szkolenia,
            4. dodanie zainteresowana,
            5. dodawanie kompetencji,
            6. dodawanie znajomości języka,
            7. dodanie kompetencji społecznych,
        iv. formularz dodawania teczki,
        v. formularz dodawania cv,
        vi. formularz dodawania celu - w planach rozwoju,
        vii. formularz wysyłania wiadomości wewnętrznej.
2. Doradca

Konto doradcy posiada niżej wymienione formularze, które same w sobie są identyczne jak w koncie użytkownika - tylko jest ich mniej.

    a. doradca niezalogowany
        i. kontakt,

ii. rejestracja,

iii. logowanie,

iv. przypomnij hasło,

b. doradca zalogowany

i. formularz wysyłania wiadomości wewnętrznej.

Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie przez Wykonawcę na rzecz Zamawiającego testów oraz re-testów bezpieczeństwa dla aplikacji "Moje Portfolio" w nowej wersji, pokazanej powyżej na makietach.

Wykonawcą testów i re-testów bezpieczeństwa nie powinien być dostawca danej aplikacji ani też podmiot od niego zależny.

Celem realizowanego zamówienia jest zapewnienie wysokiego poziomu bezpieczeństwa aplikacji, która będzie odporna na ataki.

Zakres prac

1. Przeprowadzenie testów penetracyjnych typu "white-box" i "black-box" dla aplikacji WWW w oparciu o metodykę OWASP (Open Web Application Security Project) ASVS 4.0 a w szczególności:
    a. przeprowadzenie walidacji parametrów,
    b. sprawdzenie podatności na wstrzyknięcie w przeglądarkę fragmentu kodu np. javascript, który może być uruchomiony w przeglądarce tzw. Cross-Site Scripting (XSS),
    c. sprawdzenie mechanizmów uwierzytelniających pod kątem próby ich przełamania (ataki słownikowe i siłowe na hasła, ataki z wykorzystaniem SQL Injection/Blind SQL Injection),
    d. przeprowadzenie próby przejęcia kontroli nad aplikacją,
    e. sprawdzenie podatności na ataki techniką Google Hacking,
    f. sprawdzenie bezpieczeństwa zarządzania kluczami API,
    g. zweryfikowanie czy hasła, integracje z bazami danych i systemami zewnętrznymi zarządzane są w bezpieczny sposób i nie zawarte w kodzie źródłowym lub przechowywane w repozytoriach,
    h. sprawdzenie podatności aplikacji na możliwość nieautoryzowanego przerwania i/lub zakłócenia ciągłości działania (ataki Dos), z wyłączeniem ataków DDoS,

i. sprawdzenie zabezpieczeń przed enumeracją zasobów oraz haseł,

j. sprawdzenie podatności na atak Forcefull browsing,

k. sprawdzenie podatności na atak Path Traversal,

l. podsłuchiwanie sesji i kradzież ciasteczek HTTP (zmuszenie przeglądarki ofiary do wykonania pewnej nieautoryzowanej akcji - wykonania requestu HTTP),

m. zbadanie podatności aplikacji na możliwość nieautoryzowanego ujawnienia kodu źródłowego,

n. zbadanie podatności aplikacji na możliwość nieautoryzowanego wykonania poleceń systemowych (ataki typu Remote Code Execution),

o. zbadanie podatności na atak Shell injection,

p. przeprowadzenie testów mechanizmów zarządzania sesją (m.in. obsługa parametrów sesji przez aplikacje: pliki Cookies), próby podszywania się pod zalogowanego użytkownika, weryfikacja mechanizmów wygaszania sesji, weryfikacja istnienia podatności typu CSRF,

q. fuzzing.

2. Przeprowadzenie testów penetracyjnych infrastruktury informatycznej zgodnie z metodyką PTES (The Penetration Testing Execution Standard) w tym m.in.:

   a. zweryfikowanie dostępności portów TCP/UDP dla hostów aplikacji Moje portfolio (skanowanie portów), dla protokołu ipv4 i ipv6,

   b. przeprowadzenie ataków na bazy danych (SQL Injection, Blind SQL Injection, XML Injection, SOAP Injection),

   c. sprawdzenie rodzaju, wersji oraz konfiguracji wykorzystywanego oprogramowania systemowego i usługowego,

   d. sprawdzenie podatności hostów na ataki w warstwie systemowej,

   e. zbadanie podatności hostów na możliwość dostępu do zasobów plikowych osoby nieuprawnionej,

   f. zbadanie podatności hostów na próby łamania haseł.

   Testem objęty zostanie wyznaczony przez Zamawiającego wskazany adres IP.

3. Dokonanie analizy konfiguracji serwerów, na których została umieszczona aplikacja, pod kątem bezpieczeństwa. Analiza będzie obejmowała:

   a. w przypadku bazy danych: weryfikację aktualności oprogramowania bazy danych, analizę zastosowanych metod uwierzytelniania, sprawdzenie polityki haseł,

sprawdzenie mechanizmów przechowywania haseł, logowania zdarzeń, archiwizację danych, analizę i ocenę mechanizmów kontroli dostępu fizycznego i logicznego,

b. w przypadku serwera WWW: weryfikację aktualności oprogramowania serwera, analizę i ocenę sposobu obsługi błędów, analizę metod kontroli dostępu fizycznego i logicznego, weryfikację obecności domyślnych kont użytkowników, weryfikację sposobu zarządzania serwerem, ocenę mechanizmów archiwizacji danych.

4. Przygotowanie raportu z przeprowadzonych testów bezpieczeństwa wraz z rekomendacjami w zakresie odkrytych luk bezpieczeństwa i możliwych działań naprawczych. Raport będzie zawierał m.in.:

   a. szczegółowy opis przeprowadzonych prac,

   b. szczegółowy wykaz wykrytych podatności, wraz z dowodami na ich istnienie w postaci zrzutów ekranu oraz logów oprogramowania użytego podczas audytu,

      uwaga: każda podatność powinna być oznaczona kodem ze słownika CVE (Common Vulnerabilities and Exposures),

   c. rekomendacje w zakresie sposobu wyeliminowania wykrytych podatności wraz z podaniem zaleceń i instrukcji do wprowadzenia korekt konfiguracyjnych w celu ich eliminacji,

   d. opis w formie streszczonej aktualnego poziomu bezpieczeństwa wraz z jego oceną.

Raport powinien zostać zabezpieczony przez Wykonawcę przed możliwością przejęcia i odczytania zawartości przez podmioty niebiorące udziału w realizacji przedmiotu umowy.

Raporty powinny zostać dostarczone w wersji elektronicznej, w formacie pozwalającym na edycję tekstu.

Z uwagi na to, że raporty będą przygotowywane w ramach projektu finansowanego z UE, wymagane jest umieszczenie logotypów przekazanych przez Zamawiającego. Logotypy wraz z formatką raportu zostaną przekazane Wykonawcy w trybie roboczym.

5. Przeprowadzenie re-testów:

   a. re-testy zostaną przeprowadzone przez Wykonawcę po wprowadzeniu zmian do aplikacji na podstawie rekomendacji z raportu.

   b. metodologia re-testów powinna być identyczna z opisaną w punktach 1-3.

6. Przygotowanie raportu prezentującego wnioski z przeprowadzonych re-testów.

Sposób realizacji zamówienia

1. Termin realizacji zamówienia: od podpisania umowy i nie później, niż ~~27 marca~~ 11 kwietnia do ~~21 kwietnia~~ 5 maja 2023, w tym przeprowadzenie testów i re-testów bezpieczeństwa w terminie do ~~**17 kwietnia**~~ **2 maja 2023**.

2. W ciągu 2 dni roboczych od podpisania umowy w odbędzie się spotkanie konsultacyjne, na którym zostanie ustalony zakres, harmonogram prac i szczegółowe warunki realizacji zamówienia oraz współpracy Wykonawcy z Zamawiającym. Zamawiający może zdecydować się na przeprowadzenie spotkania w formie zdalnej.

3. Po spotkaniu konsultacyjnym Wykonawca w ciągu 2 dni roboczych prześle drogą elektroniczną konspekt testów i re-testów bezpieczeństwa zawierający ich ogólną koncepcję oraz szczegółowy harmonogram.

4. Zamawiający zastrzega sobie prawo do zorganizowania kolejnych spotkań o charakterze roboczym, w celu uzyskania informacji nt. przebiegu prowadzonych działań oraz poczynienia bieżących ustaleń. Spotkania robocze mogą być organizowane w dni robocze oraz mogą zostać przeprowadzone w formie zdalnej.

5. **Przeprowadzenie testów i re-testów bezpieczeństwa: do ~~17 kwietnia~~ 2 maja 2023.**

6. Wykonawca w ciągu 3 dni kalendarzowych od zakończenia testów sporządzi raport. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, w terminie 2 dni roboczych od otrzymania raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego w terminie kolejnych 2 dni kalendarzowych.

7. W terminie maksymalnie 10 dni roboczych po wprowadzeniu zmian w aplikacji na podstawie rekomendacji z raportu, Wykonawca przeprowadzi re-testy bezpieczeństwa.

8. W terminie 2 dni kalendarzowych od zakończenia re-testów bezpieczeństwa, Wykonawca przedstawi raport podsumowujący wyniki re-testów.

Kalendarz zamówienia:

max. n_1 +2 dni robocze (n_1 = data podpisania umowy)	Zamawiający zorganizuje spotkanie konsultacyjne
max. n_1 + 4 dni robocze	Wykonawca prześle drogą elektroniczną konspekt testów i re-testów bezpieczeństwa
maks. ~~17.04.2023~~ 02.05.2023	Wykonawca przeprowadzi testy oraz re-testy bezpieczeństwa aplikacji
max. n_2 + 2 dni kalendarzowe (n_2 = data zakończenia re-testów bezpieczeństwa aplikacji)	Wykonawca przekaże raport z przeprowadzonych re-testów.

Warunki realizacji zamówienia

1. Zamówienie realizowane będzie przez osobę lub osoby posiadające wiedzę i doświadczenie adekwatne do wykonania testów bezpieczeństwa w oparciu o najbardziej aktualne metody jego naruszeń wraz z udokumentowanymi certyfikatami bezpieczeństwa informacji.

2. Prace realizowane w ramach zamówienia będą prowadzone z uwzględnieniem potrzeb Zamawiającego.

3. Wykonawca dołoży wszelkich starań do uwzględnienia ważnych elementów mogących mieć wpływ na naruszenie bezpieczeństwa aplikacji Moje Portfolio nie wymienionych w przedmiocie zamówienia, a dotyczących testów penetracyjnych aplikacji WWW, oraz analizy konfiguracji serwerów IBE.

4. Realizacja przedmiotu zamówienia odbywać się będzie głównie zdalnie, niemniej jednak w uzasadnionych przypadkach Zamawiający akceptuje realizację zleconych prac w siedzibie Zamawiającego, w dniach roboczych w godzinach 10:00-16:00. Realizacja zleconych zadań będzie wymagać obecności Wykonawcy w siedzibie Zamawiającego, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania zlecenia jednostkowego.

5. Realizując zlecenie, Wykonawca zweryfikuje całość udostępnionego kodu, nie stosując próbkowania.

6. Wykonawca oddeleguje do nadzorowania umowy osobę, która będzie odpowiedzialna m.in. za:

    - przestrzeganie terminów umownych dotyczących Wykonawcy,
    - kontakty z Zamawiającym, w tym przekazywanie odpowiedzi na pytania Zamawiającego dotyczące realizacji umowy,
    - przestrzeganie obowiązków Wykonawcy wynikających z umowy, w szczególności dotyczących zapisów odnośnie danych osobowych i poufności informacji.

7. Forma kontaktu: W ramach bieżącej współpracy Zamawiający i Wykonawca będą się kontaktować za pomocą poczty elektronicznej, a gdy wymaga tego sytuacja – również telefonicznie.

    Osoby wskazane do kontaktu ze strony Zamawiającego:

    - Roksana Pierwieniecka, e-mail: r.pierwieniecka@ibe.edu.pl
    - Stefan Kurszel, e-mail: s.kurszel@ibe.edu.pl.

Harmonogram płatności

Płatność za realizację zamówienia nastąpi po ostatecznym zaakceptowaniu przez Zamawiającego raportu z przeprowadzonych re-testów bezpieczeństwa oraz podpisaniu protokołu zdawczo-odbiorczego.