Załącznik nr 1

Opis przedmiotu zamówienia

Dotyczy zamówienia na przeprowadzenie testów bezpieczeństwa dla aplikacji webowej „Moja Walidacja”

1. Cel

Celem zamówienia jest przeprowadzenie testów bezpieczeństwa informatycznego dla aplikacji webowej „Moja Walidacja” przeznaczonej dla interesariuszy Zintegrowanego Systemu Kwalifikacji, w tym: osób pełniących funkcję asesorów, doradców walidacyjnych, projektantów walidacji, koordynatorów i administratorów systemu w Instytucjach Certyfikujących, oraz osób chcących przystąpić do walidacji efektów uczenia się w danej Instytucji Certyfikującej.

Aplikacja „Moja Walidacja” składa się z trzech narzędzi webowych ułatwiających planowanie i prowadzenie walidacji:

1. Schematora – narzędzia przeznaczonego do tworzenia schematów walidacji;
2. E-Asesora - narzędzia przeznaczonego do tworzenia arkuszy oceny kandydatów dopasowanych do różnych metod walidacji oraz do wypełniania gotowych arkuszy, zatwierdzonych w danej walidacji;
3. Menedżera Walidacji – narzędzia przeznaczonego do kompleksowego zarządzania walidacją zarówno po stronie instytucji, jak i kandydata.

Aplikacja jest zintegrowana z innymi narzędziami webowymi: Bazą Efektów Uczenia się (BEU) powiązaną z zasobami Zintegrowanego Rejestru Kwalifikacji (ZRK), oraz „Moim Portfolio” (MP) – aplikacją służącą m.in. do gromadzenia dowodów w cyfrowym portfolio oraz udostępniania ich zainteresowanym osobom z Instytucji Certyfikujących.

W ramach zamówienia zostaną zrealizowane trzy moduły testów bezpieczeństwa:

1) Testy penetracyjne typu „white-box” i „black-box” dla aplikacji „Moja Walidacja” oraz powiązanych z nią MP i BEU znajdującej się na serwerze Zleceniodawcy w oparciu o metodykę OWASP (Open Web Application Security Project) ASVS v3.0;
2) Testy penetracyjne infrastruktury informatycznej, na której wdrożono aplikację „Moja Walidacja”, MP i BEU zgodnie z metodyką PTES (The Penetration Testing Execution Standard);
3) Testy konfiguracji serwerów Zamawiającego, na których będzie zlokalizowana aplikacja „Moja Walidacja”, MP i BEU.

Testy bezpieczeństwa mają na celu sprawdzenie poziomu bezpieczeństwa zarówno samej aplikacji, jak i danych w niej przechowywanych. Bazy danych będą zawierać szyfrowane dane poufne wielu instytucji certyfikujących, w tym dane dotyczące prowadzonych procesów walidacyjnych, dane osobowe pracowników oraz kandydatów chcących przystąpić do walidacji efektów uczenia się dla wybranej kwalifikacji.

2. Informacje na temat projektu

W projekcie „Wspieranie realizacji II etapu wdrażania Zintegrowanego Systemu Kwalifikacji na poziomie administracji centralnej oraz instytucji nadających kwalifikacje i zapewniających jakość nadawania kwalifikacji”,

finansowanym ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój, zaplanowano szereg działań mających na celu wdrażanie, rozwój i wsparcie funkcjonowania Zintegrowanego Systemu Kwalifikacji (ZSK).

W obszarze walidacji zaplanowano m.in. działania mające na celu wspieranie interesariuszy ZSK w obszarze walidacji efektów uczenia się, ze szczególnym uwzględnieniem podmiotów pełniących funkcje instytucji certyfikujących odpowiedzialnych za przeprowadzanie walidacji i nadawanie kwalifikacji funkcjonujących w systemie. Jedną z form wsparcia jest opracowanie i rozwijanie kompleksowych narzędzi cyfrowych przeznaczonych do projektowania, prowadzenia i zarządzania procesem walidacji (np. aplikacji webowych).

3. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie przez Wykonawcę kompleksowych testów bezpieczeństwa informatycznego dla aplikacji webowej „Moja Walidacja" oraz powiązanych z nią narzędzi: Mojego Portfolio i BEU. Wykonawcą testów bezpieczeństwa nie może być podmiot, który jest dostawcą aplikacji lub inny podmiot od niego zależny.

Aplikacja będzie bezpłatna, dostępna także w wersji instalacyjnej na licencji open-source.

„Moja Walidacja" jest aplikacją webową wykonaną z użyciem następujących technologii: środowisko serwerowe - .NET Core 3.1 i C#, środowisko klienckie: Angular i Typescript. Powiązane z nią aplikacje Moje Portfolio i BEU zostały zaprogramowane w oparciu o Laravel i PHP. Bazy danych zaimplementowane w aplikacji Moje Walidacja, Moje Portfolio i BEU działają w oparciu o MySQL.

Aplikacja Moje Portfolio jest dostępna w starej wersji pod adresem: https://mojeportfolio.ibe.edu.pl/dashboard (przykładowe portfolio) lub po zarejestrowaniu. Baza Efektów Uczenia się (http://beuzsk.ibe.edu.pl) czerpie dane z API ZRK. Więcej o API ZRK można znaleźć tutaj: https://rejestr.kwalifikacje.gov.pl/dokumenty-komunikaty/api. Dostęp do Bazy po zalogowaniu na dane użytkownika Mojego Portfolio.

Aplikacja Moja Walidacja wykorzystuje ok. 100-200 endpointów i 500-700 operacji Rest API (powiązane z nią Moje portfolio: około 50 endpointów). Szacunkowa liczba unikalnych widoków dostępnych dla 10 różnych ról użytkowników to ok. 100-200.

Testy mają zostać przeprowadzone na serwerach Zamawiającego, działających w oparciu o systemy Debian, Apache i bazy danych MySQL.

W skład przedmiotu zamówienia wchodzą następujące elementy:

3.1. Moduł testów penetracyjnych typu „white-box" i „black-box" dla aplikacji „Moja Walidacja" w oparciu o metodykę OWASP[1]

Przeprowadzenie testów penetracyjnych zostanie poprzedzone zebraniem informacji na temat aplikacji. Wykonawca planując zakres testów penetracyjnych uwzględni następujące rodzaje podatności:

1) testowanie podatności na wstrzykiwanie złośliwego kodu (*injection*)
2) testowanie uwierzytelniania (*broken authentication*) i zarządzania sesją (*session management testing*)
3) ekspozycji wrażliwych danych (*sensitive data exposure*)
4) testowanie podatności związane z XML External Entities (XXE)

[1] The OWASP Foundation (2017). *OWASP Top 10-2017. The Ten Most Critical Web Application Security Risks.* https://owasp.org.

5) testowanie podatności typu Broken Access Control
6) testowanie podatności typu błędna konfiguracja bezpieczeństwa (*security misconfiguration*)
7) testowanie podatności typu Cross-Site Scripting (XSS) i Cross-Site Request Forgery (CSRF)
8) testowanie DoS (*Denial of Service testing*)
9) testowanie podatności związanych z deserializacją niezaufanych obiektów (*insecure deserialization*)
10) testowanie podatności związanych z użyciem komponentów ze znanymi lukami bezpieczeństwa (*using components with known vulnerabilities*)
11) testowanie typu fuzz testing (*fuzzing*)

Wykonawca uwzględni w testach przynajmniej:

- sprawdzenie skuteczności walidacji danych np.: niepoprawnej walidacji danych wejściowych, „wstrzykiwania" złośliwego kodu (np. SQL Injection, Command Injection, JSON injection), skrypty krzyżowe, złośliwe wykonywanie plików i binariów, fałszowanie żądań;
- sprawdzenie mechanizmów związanych z uwierzytelnianiem i zarządzaniem sesją pod kątem próby ich przełamania (np. ataki słownikowe i siłowe na hasła i klucze, credential stuffing, ataki z wykorzystaniem SQL /Blind SQL Injection, wyświetlanie ID sesji w URL, zła obsługa uwierzytelnienia i sesji, źle skonfigurowane kończenie sesji, etc.);
- sprawdzenie czy występuje podatność na ujawnianie danych wrażliwych, wycieki i fałszowanie informacji, np.: kradzież słabo zabezpieczonych lub nieodpowiednio szyfrowanych kluczy, haseł i innych danych wrażliwych, brak szyfrowania wrażliwych danych lub niepoprawna obsługa błędów, kradzież czystych danych tekstowych z serwera lub przeglądarki (dotyczy HTTP, SMTP), ataki typu „man in the middle", podszywanie się pod użytkowników aplikacji", spoofing; niezabezpieczona wymiana informacji, komentarze w kodzie źródłowym;
- sprawdzenie czy występuje podatność aplikacji na Cross-Site Scripting (XSS), np.: wykonanie kodu HTML i JavaScript w celu przechwycenia sesji użytkownika, przekierowanie na inną stronę, wyrenderowanie własnego kodu HTML, zmiany wyglądu strony;
- sprawdzenie czy występuje podatność aplikacji na Cross-Site Request Forgery (CSRF) tj. zdalne wykonanie akcji aplikacji przez atakującego, np.: osadzenie skryptu czy arkusza stylów CSS odnoszącego się bezpośrednio do podatnej akcji i wykonanie go;
- sprawdzenie czy występują podatności związane z XXE (XML eXternal Entity); ocena ryzyka związanego z importem pliku do Schematora;
- sprawdzenie czy występuje podatność typu Broken Access Control (na nieprawidłowo skonfigurowane uprawnienia użytkowników np. do kont innych użytkowników, podglądu wrażliwych plików, modyfikacji danych innych użytkowników, zmiany prawa dostępu z konta użytkownika na konto administratora etc.);
- sprawdzenie czy występuje podatność typu Security Misconfiguration (niezałatanych luk, niebezpiecznych ustawień defaultowych kont, nieużywanych stron, niezabezpieczonych plików i katalogów, niepotrzebnych portów, usług, kont, uprawnień, niekompletnych konfiguracji, źle skonfigurowanych nagłówków http etc.);
- sprawdzenie czy występuje podatność aplikacji na możliwość nieautoryzowanego przerwania i/lub zakłócenia ciągłości działania poprzez ataki typu DoS;
- sprawdzenie czy występuje podatność związana z deserializacją niezaufanych obiektów, np. PHP Object Injection, JSON deserialization vulnerability, ataki związane ze strukturą obiektów i danych, typowe ataki związane z fałszowaniem danych (np. ataki związane z kontrolą dostępu), usuwanie dowolnych plików i folderów na serwerze; ocena ryzyka w przypadku aplikacji posiadającej API;
- sprawdzenie czy występuje podatność związana z użyciem komponentów ze znanymi lukami bezpieczeństwa (*using components with known vulnerabilities*), w szczególności w Schematorze; ocena ryzyka w przypadku aplikacji posiadającej API;
- sprawdzenie skuteczności mechanizmów ochrony przed enumeracją zasobów oraz haseł; ocena ryzyka w przypadku aplikacji posiadającej API;

- sprawdzenie czy występuje podatność na atak *Forcefull browsing*; ocena ryzyka w przypadku aplikacji posiadającej API;
- sprawdzenie czy występuje podatność na atak *Path Traversal*; ocena ryzyka w przypadku aplikacji posiadającej API;
- badanie podatności aplikacji na możliwość nieautoryzowanego ujawnienia kodu źródłowego (sprawdzenie, czy strona błędu nie ujawnia danych z pliku konfiguracyjnego np. danych dostępowych do bazy danych);
- sprawdzenie czy występuje podatność w postaci niezabezpieczonego bezpośredniego dostępu do zasobów np. modułów aplikacji, akcji w których biorą udział „obiekty" (zasoby systemu) np. dane pobierane z bazy danych;
- badanie podatności aplikacji na możliwość nieautoryzowanego wykonania poleceń systemowych (ataki typu Remote Code Execution) np. poprzez importowanie plików;
- przeprowadzenie testowania typu fuzz testing (*fuzzing*), tj. wysyłanie do aplikacji różnego typu danych wejściowych (z linii poleceń, plików otwieranych w aplikacji, za pomocą protokołów internetowych) i rejestrowanie niepożądanych wydarzeń takich jak crash, wycieki pamięci czy nieautoryzowany dostęp.

Ostateczny zakres testów Wykonawca ustali we współpracy z Zamawiającym na etapie przygotowania koncepcji i planów testów bezpieczeństwa.

3.2. Moduł testów penetracyjnych infrastruktury informatycznej, na której wdrożono aplikację „Moja Walidacja" zgodnie z metodyką PTES (The Penetration Testing Execution Standard), w tym:

- analiza działających usług, otwartych portów TCP/UDP dla hostów aplikacji „Moja Walidacja" (skanowanie portów), zwłaszcza dla protokołu IPv6;
- ataki na bazy danych w aplikacji (SQL Injection, Blind SQL Injection, XML Injection, SOAP Injection),
- sprawdzenie rodzaju, wersji oraz konfiguracji wykorzystywanego oprogramowania systemowego i usługowego;
- penetracja słabości i próba ich wykorzystania (np. exploity);
- próba zwiększenia uprawnień użytkownika (np. ze zwykłego użytkownika na administratora);
- testowanie podatności typu „backdoor", „tylnego" dostępu do badanego środowiska;
- badanie podatności hostów na możliwość dostępu do zasobów plikowych przez osoby nieuprawnione;
- analiza możliwości usunięcia śladów logowania, aktywności użytkowników;
- inne (jeśli Wykonawca uzna je za potrzebne).

3.3. Testy konfiguracji serwerów Zamawiającego, na których będzie zlokalizowana aplikacja „Moja Walidacja", w tym:

- w przypadku bazy danych: weryfikację aktualności oprogramowania bazy danych, analizę zastosowanych metod uwierzytelniania, sprawdzenie polityki haseł, sprawdzenie mechanizmów przechowywania haseł, logowania zdarzeń, wykonywania kopii zapasowych;
- w przypadku serwera WWW: weryfikację aktualności oprogramowania serwera, analiza i ocena sposobu obsługi błędów, analizę metod kontroli dostępu, weryfikację obecności domyślnych kont użytkowników, weryfikację sposobu zarządzania serwerem, ocenę mechanizmów backupowania;
- inne (jeśli Wykonawca uzna je za potrzebne).

4. Zasady współpracy z Zamawiającym

4.1. 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:

Małgorzata Musialik, e-mail: m.musialik@ibe.edu.pl lub Iwona Gmaj e-mail: i.gmaj@ibe.edu.pl.

4.2. Do obowiązków Wykonawcy będzie należało:

4.2.1. udział w spotkaniach konsultacyjno-roboczych z członkami zespołu Zamawiającego, których celem będzie ustalenie sposobu realizacji zamówienia. Zamawiający będzie dostępny dla Wykonawcy w dni robocze w godzinach 11:00-16:00. Spotkania mogą się odbywać w siedzibie Zamawiającego w godzinach 11:00-16:00 lub zdalnie w formie telekonferencji.

4.2.2. przygotowanie we współpracy z Zamawiającym:

1) koncepcji testów bezpieczeństwa,
2) harmonogramu testów bezpieczeństwa,
3) planów testów bezpieczeństwa;

przekazanie ich Zamawiającemu do konsultacji w wersji elektronicznej w terminie max. 5 dni roboczych od momentu zawarcia umowy; Zamawiający przekaże swoje uwagi do koncepcji i harmonogramu w ciągu 3 dni roboczych, a Wykonawca ma 3 dni robocze na poprawienie ich według uwag Zamawiającego;

4.2.3. przeprowadzenie testów bezpieczeństwa przewidzianych w ramach 1 modułu zgodnie z metodyką OWASP w ciągu 10 dni roboczych od momentu zaakceptowania planu testów;

4.2.4. przeprowadzenie testów bezpieczeństwa przewidzianych w ramach 2 modułu zgodnie z metodyką PTES w ciągu 10 dni roboczych od momentu zaakceptowania planu testów;

4.2.5. przeprowadzenie testów konfiguracji serwerów Zamawiającego w ramach 3 modułu testów bezpieczeństwa w ciągu 10 dni roboczych od momentu zaakceptowania planu testów;

4.2.6. W przypadku wykrycia na jakimkolwiek etapie podatności krytycznej (czyli np. dającej nieautoryzowany dostęp do danych czy aplikacji) wykonawca przekaże taką informację od razu w momencie jej wykrycia- tak by można było od razu ją usunąć.

4.2.7. sporządzenie raportu z przeprowadzonych testów bezpieczeństwa uwzględniającego 3 moduł; raport będzie zawierał m.in.:

1) opis metodologii;
2) szczegółowy opis przeprowadzonych prac, zestawienie wyników badań, ogólne wnioski na temat aktualnego poziomu bezpieczeństwa wraz z jego oceną;
3) szczegółowy wykaz wykrytych podatności, wraz z dowodami na ich istnienie w postaci zrzutów ekranu oraz logów oprogramowania użytego podczas audytu; dowód musi dokumentować wystąpienie podatności, a nie np. nieaktualną wersję programu;
4) każda podatność powinna być oznaczona kodem ze słownika CVE (Common Vulnerabilities and Exposures);
5) opis w formie streszczonej;
6) raport powinien być zabezpieczony przed możliwością przejęcia i odczytania zawartości przez podmioty niebiorące udziału w realizacji przedmiotu umowy.

4.2.8. przedstawienie rekomendacji w zakresie odkrytych luk bezpieczeństwa i możliwych działań naprawczych w kodzie źródłowym z uwzględnieniem wszystkich nieprawidłowości opisanych w raporcie;

4.2.9. Wykonawca ma 20 dni roboczych na wykonanie wszystkich modułów testowych, oraz sporządzenie raportu i rekomendacji;

4.2.10. prowadzenie testów zdalnie lub - jeśli będzie tego wymagała specyfika określonych rodzajów testów – w siedzibie Zamawiającego w godz. 11:00-16:00; możliwe jest wykonanie testów całkowicie zdalnie (do uzgodnienia z Zamawiającym);

4.2.11. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu i rekomendacji w terminie 5 dni od momentu przekazania raportu i rekomendacji; Wykonawca uwzględni uwagi Zamawiającego w ciągu 3 dni roboczych od otrzymania uwag.

4.3. Obowiązki Wykonawcy w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych przechowywanych w aplikacji zgodnie z wymogami RODO

Działania objęte umową będą realizowane zgodnie z wymogami zawartymi w ustawie o RODO po zawarciu umowy z Wykonawcą o przestrzeganiu poufności informacji i ochronie danych osobowych będącej załącznikiem nr x do Umowy.

5. Terminy i harmonogram realizacji zamówienia

1. Zamówienie zostanie zrealizowane w terminie **do 16.11.2020 r.**
2. W ciągu **3 dni roboczych** od podpisania umowy Wykonawca przedstawi Zamawiającemu do akceptacji proponowany harmonogram prac.

3. Wykonawcy zostanie wypłacona zaliczka w wysokości **30% wartości zamówienia**, płatna w ciągu 7 dni od momentu zawarcia umowy.

4. Przekazanie elementów składowych zamówienia, tj.:

   a) Przeprowadzonych 3 modułów testów bezpieczeństwa:

      - testów penetracyjnych typu „white-box" i „black-box" dla aplikacji „Moja Walidacja", Moje Portfolio i BEU znajdujących się na serwerze Zleceniodawcy w oparciu o metodykę OWASP (Open Web Application Security Project) ASVS v3.0;
      - testów penetracyjnych infrastruktury informatycznej, na której wdrożono aplikację „Moja Walidacja", MP i BEU zgodnie z metodyką PTES (The Penetration Testing Execution Standard);
      - testów konfiguracji serwerów Zamawiającego, na których będzie zlokalizowana aplikacja „Moja Walidacja", MP i BEU.

   b) raportu z przeprowadzonych testów bezpieczeństwa (metodologii, wyników badań, wniosków z przeprowadzonych testów),
   c) rekomendacji w zakresie odkrytych luk bezpieczeństwa i możliwych działań naprawczych,

   zostanie potwierdzone protokołem przekazania, przygotowanym przez Wykonawcę na podstawie wzorów dostarczonych wcześniej przez Zamawiającego **do 16.11.2020 r.**

5. Odbiór danej składowej zamówienia będzie potwierdzony przez wyznaczoną w umowie osobę na protokole zdawczo-odbiorczym, przygotowanym przez Wykonawcę, na podstawie wzorów dostarczonych wcześniej przez Zamawiającego.

   Podpisanie protokołów zdawczo-odbiorczych ostatecznego rezultatu zamówienia tj. 3 modułów testów bezpieczeństwa, raportu z badania i rekomendacji, powinno nastąpić nie później niż: **do 16.11.2020 r.**

6. Wynagrodzenie dla Wykonawcy zostanie wypłacone na podstawie podpisanego protokołu zdawczo-odbiorczego.

7. Wykonawca powinien być dyspozycyjny i gotowy do bieżącego kontaktu telefonicznego lub mailowego w miarę potrzeb oraz do prowadzenia testów bezpieczeństwa zdalnie lub w siedzibie Zamawiającego.