Załącznik nr 2
Opis przedmiotu zamówienia

Opis Przedmiotu Zamówienia

Testy bezpieczeństwa dla systemu informatycznego Zintegrowanego Rejestru Kwalifikacji

Informacje dotyczące zamówienia

1. Zamawiający
   Instytut Badań Edukacyjnych
   ul. Górczewska 8, 01-180 Warszawa

2. Wstęp
   Instytut Badań Edukacyjnych w Warszawie (IBE) jest placówką badawczą prowadzącą interdyscyplinarne badania naukowe nad funkcjonowaniem i efektywnością systemu edukacji w Polsce. Jednym z projektów systemowych realizowanych przez IBE na zlecenie Ministerstwa Edukacji Narodowej współfinansowanych ze środków Unii Europejskiej, jest projekt pod nazwą „Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji" (projekt ZRK).

   Zintegrowany Rejestr Kwalifikacji stanowi ważne narzędzie systemowe służące realizacji polityki uczenia się przez całe życie. Rejestr pełni ważną rolę w integracji funkcjonujących w kraju systemów kształcenia: oświaty i szkolnictwa wyższego oraz obszaru edukacji pozaformalnej i nieformalnego uczenia się.

   ZRK gromadzi i udostępnia informacje na temat możliwych do uzyskania w Polsce kwalifikacji spełniających określone przez państwo (w ustawie) wymagania dotyczące m.in. standardu opisu kwalifikacji, przypisania poziomu PRK oraz zasad zapewniania jakości kwalifikacji. ZRK jest rejestrem publicznym w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

   ZRK jest rejestrem jawnym, a informacje o kwalifikacjach w nim gromadzone są powszechnie dostępne za pośrednictwem strony internetowej (portalu internetowego) w językach polskim i angielskim. Portal oferuje możliwość łatwego przeszukiwania, porządkowania i agregowania informacji. Portal polskiego rejestru, podobnie jak portale pozostałych krajów UE, będzie powiązany z portalem Europejskiej Ramy Kwalifikacji (ERK).

   IBE, od stycznia 2018 r. jest instytucją pierwszego wyboru, do którego zwracają się różne instytucje lub osoby z pytaniami dotyczącymi ZRK. Grupy osób zainteresowanych informacjami zawartymi w ZRK to np. uczniowie, pracobiorcy, pracodawcy, nauczyciele, doradcy zawodowi, administracja państwowa, jednostki samorządu terytorialnego, organizacje pracodawców, związki zawodowe, izby gospodarcze, itd.

   Podmiot prowadzący rejestr jest naturalnym punktem kontaktowym dla tych grup.

Rejestr pełni funkcję „jednego okienka” dla instytucji składających wnioski. Zadania ZRK wynikające z ustawy o ZSK to m.in.:

1. Dokonywanie wpisów w ZRK i ich aktualizacji.
2. Formalna ocena wniosków: o włączenie kwalifikacji rynkowych do ZSK, o przywrócenie kwalifikacji rynkowej statusu kwalifikacji funkcjonującej, o nadanie uprawnień do certyfikowania kwalifikacji, o wpis na listę podmiotów uprawnionych do pełnienia funkcji zewnętrznego zapewniania jakości. Wnioski składane są wyłącznie droga elektroniczną.
3. Prowadzenie portalu ZSK w części dotyczącej ZRK.
4. Gromadzenie, przechowywanie i udostępnianie ministrom właściwym, ministrowi koordynatorowi oraz Radzie Interesariuszy raportów i sprawozdań IC oraz PZZJ.
5. Gromadzenie informacji o: liczbie wydanych dokumentów potwierdzających nadanie poszczególnych kwalifikacji, wysokości opłat i przychodów za walidację i certyfikowanie.
6. Zapewnienie dostępu do informacji o Zintegrowanym Rejestrze Kwalifikacji, w szczególności za pośrednictwem Internetu.
7. Monitorowanie funkcjonowania ZRK.
8. Uzupełnianie informacji o wpisanych do ZRK kwalifikacjach o krótkie charakterystyki kwalifikacji w języku angielskim.

System informatyczny ZRK został zaprojektowany w IBE w latach 2013 - 2015 i uruchomiony w środowisku testowym w 2015 r., jeszcze przed wejściem w życie ustawy regulującej zasady działania ZRK (ustawa o ZSK). Rejestr został uruchomiony w lipcu 2016 r.

Materiały i informacje rejestru i sam rejestr kwalifikacji dostępny jest pod adresem rejestr.kwalifikacje.gov.pl

Przedmiot zamówienia

1. Przedmiotem zamówienia jest przeprowadzenie przez Wykonawcę na rzecz Zamawiającego 5 testów bezpieczeństwa systemu informatycznego ZRK.
2. Wykonawcą testów bezpieczeństwa nie powinien być Dostawca Systemu lub podmiot zależny od Dostawcy Systemu.
3. Planowany okres realizacji zamówienia to kwiecień 2019 - czerwiec 2020.
4. Celem realizowanego zamówienia jest zapewnienie wysokiego poziomu bezpieczeństwa systemu ZRK, który będzie odporny na ataki.
5. Testy będą podzielone na 5 etapów i wykonane zgodnie z wytycznymi z pkt. 1-3 “Zakres prac”

6. Termin wykonania każdego z etapów jest orientacyjny, ponieważ zależy od terminu wdrożenia danej aplikacji:
   a. etap I do wykonania do 30.06.2019 testy aplikacji webowej interkonektor POL-on,
   b. etap II do wykonania w 2019 roku - testy aplikacji webowej dla uprzywilejowanych użytkowników "Aktywne formularze",
   c. etap III do wykonania w 2019 roku - testy aplikacji webowej dla uprzywilejowanych użytkowników IC/PZZJ,
   d. etap IV do wykonania w 2019 roku - testy aplikacji mobilnej "zarządzanie kwalifikacjami",
   e. etap V do wykonania w 2020 roku - testy całościowe zmodernizowanego systemu ZRK .

   Dopuszcza się przesunięcia aplikacji między etapami a także przesunięcia terminów jednak nie później niż do czerwca 2020.

   Zakłada się przeprowadzenie nie więcej niż 1 testu w miesiącu.
7. Przykładowa aplikacja Zamawiającego planowana do objęcia testami: rejestr.kwalifikacje.gov.pl
8. Ogólny opis planowanych aplikacji
   - "Interkonektor POL-on" będzie aplikacją do jednokierunkowej wymiany danych pomiędzy Zintegrowanym Systemem Usług dla Nauki (API - pobieranie danych), bazą lokalną interkonektora POL-on (API - udostępnianie danych) oraz ZRK. Pobieranie będzie cykliczne a dostęp do aplikacji będzie miała tylko jedna osoba - administrator. Aplikacja będzie miała proste uwierzytelnianie dla administratora (podanie loginu, najlepiej adresu e-mail i hasła). Nie będzie wymagała profilowania uprawnień.

   - "Aktywne formularze" - aplikacja zastępująca obecne formularze rejestru pod adresem rejestr.kwalifikacje.gov.pl. Zakłada się zewnętrzne uwierzytelnianie przez Profil Zaufany lub opcjonalnie inne zewnętrzne mechanizmy autoryzacji. Będzie zawierała od kilku do kilkunastu formularzy wniosków, które będą przechodziły ścieżkę akceptacyjną i będą wypełniane przez osoby z zewnątrz (ministerstwa, szkoły, firmy prywatne). Zarządzanie będzie odbywać się poprzez interfejs webowy. Zakłada się wykorzystanie modelu LAMP, języków i bibliotek: HTML5, CSS3, Bootstrap i JQuery i JQuery UI. Po otrzymaniu formularza użytkownik w zależności od posiadanych uprawnień będzie mógł wyświetlić jego przepływ, wyświetlić zawartość, dokonać edycji pól lub całego formularza, zaimportować lub wyeksportować dane do formatów zewnętrznych a także decydować gdzie dalej skierować wniosek zgodnie z Workflow.

- "Aplikacja dla uprzywilejowanych IC/PZZJ"- Aplikacja webowa skierowana do konkretnych grup użytkowników: pracowników ministerstw, instytucji certyfikujących, podmiotów zewnętrznego zapewniania jakości i szkół wyższych. "IC/PZZJ" będzie aplikacją do gromadzenia i monitorowania danych uzyskiwanych od IC/PZZJ. Aplikacja będzie miała charakter webowy (zostanie zainstalowana na serwerze w modelu LAMP). Dostęp do aplikacji będzie odbywał się poprzez CAS aplikacji Aktywne Formularze.

- Aplikacja dla uprzywilejowanych użytkowników "zarządzanie kwalifikacjami". Aplikacja ta jest skierowana do konkretnych grup użytkowników: pracowników ministerstw i szkół wyższych. "Zarządzanie kwalifikacjami" będzie służyć właścicielom kwalifikacji lub podmiotom posiadającym uprawnienia w zarządzaniu "własnymi" danymi o kwalifikacjach wpisanych do rejestru. Jednym z wariantów jest zarządzanie danymi za pomocą aplikacji przygotowanej na urządzenia mobilne (np. Android, iOS).

- Zmodernizowany system ZRK.
  Planowane jest uruchomienie nowego portalu informacyjnego zarządzanego przez CMS z nowymi funkcjonalnościami, bazami danych oraz API.

8. Obecny system informatyczny ZRK działa w chmurze obliczeniowej:
   - 4 serwery Debian
   - 2 bazy danych: MariaDB
   - 2 serwery Apache

   Stacjonarnie w IBE:
   - 1 serwer Debian
   - 1 baza danych
   - 1 serwer Apache
9. Planowane aplikacje mogą być na serwerach w chmurze obliczeniowej lub stacjonarnie, w zależności od ustaleń podczas spotkań z wykonawcami aplikacji.

Zakres prac

1. Testy penetracyjne typów:"white-box", "black-box" dla wszystkich aplikacji WWW systemu ZRK w oparciu o metodykę OWASP (Open Web application Security Project) ASVS v3.0 a w szczególności:
   - walidację parametrów,

- sprawdzenie mechanizmów uwierzytelniających pod kątem próby ich przełamania (ataki słownikowe i siłowe na hasła, ataki z wykorzystaniem SQL Injection/Blind SQL Injection),
- próbę przejęcia kontroli nad aplikacją,
- podatność na ataki techniką Google Hacking,
- podatność aplikacji na możliwość nieautoryzowanego przerwania i/lub zakłócenia ciągłości działania (ataki Dos), z wyłączeniem ataków DDoS,
- ochrona przed enumeracją zasobów oraz haseł,
- podatność na atak Forcefull browsing,
- podatność na atak Path Traversal,
- podsłuchiwanie sesji i kradzież ciasteczek HTTP (zmuszenie przeglądarki ofiary do wykonania pewnej nieautoryzowanej akcji (wykonania requestu HTTP)),
- badanie podatności aplikacji na możliwość nieautoryzowanego ujawnienia kodu źródłowego,
- badanie podatności aplikacji na możliwość nieautoryzowanego wykonania poleceń systemowych (ataki typu Remote Code Execution)
- podatność na atak Shell injection,
- testy 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
- fuzzing

2. Testy penetracyjne infrastruktury informatycznej systemu ZRK zgodnie z metodyką PTES (The Penetration Testing Execution Standard) w tym m.in.:
   - weryfikację dostępności portów TCP/UDP dla hostów systemu ZRK (skanowanie portów), zwłaszcza dla protokołu ipv6,
   - ataki na bazy danych (SQL Injection, Blind SQL Injection, XML Injection, SOAP Injection)
   - sprawdzenie rodzaju, wersji oraz konfiguracji wykorzystywanego oprogramowania systemowego i usługowego,
   - sprawdzenie podatności hostów na ataki w warstwie systemowej,
   - badanie podatności hostów na możliwość dostępu do zasobów plikowych osoby nieuprawnionej,
   - badanie podatności hostów na próby łamania haseł

Testem objęte będą wyznaczone przez Zamawiającego adresy IP.

3. Analizę konfiguracji serwerów systemu ZRK pod kątem bezpieczeństwa, która będzie obejmowała:

- w przypadku bazy danych: weryfikację aktualności oprogramowania bazy danych, analizę zastosowanych metod uwierzytelniania, sprawdzenie polityki haseł, sprawdzenie mechanizmów przechowywania haseł, logowania zdarzeń, archiwizacji danych, analizę i ocenę mechanizmów kontroli dostępu fizycznego i logicznego,
- w przypadku serwera WWW: weryfikację aktualności oprogramowania serwera, analiza i ocena sposobu obsługi błędów, analizę metod kontroli dostępu fizycznego i logicznego, weryfikację obecności domyślnych kont użytkowników, weryfikację sposobu zarządzania serwerem, ocenę mechanizmów archiwizacji danych

Sposób realizacji zamówienia

1. Termin realizacji: Przedmiot zamówienia będzie realizowany w terminie od kwietnia 2019 do czerwca 2020 r.
2. W ciągu 10 dni roboczych od podpisania umowy w siedzibie Zamawiającego odbędzie się pierwsze spotkanie konsultacyjne, na którym zostanie ustalony zakres prac i szczegółowe warunki realizacji zamówienia oraz współpracy Wykonawcy z Zamawiającym.
   Kolejne spotkania konsultacyjne odbywać się będą po wdrożeniu nowych aplikacji, jednak nie później niż 5 dni roboczych od zainicjowania spotkania przez Zamawiającego. Zamawiający może zdecydować się przeprowadzenie spotkania w formie zdalnej
3. Po spotkaniu w ciągu 5 dni roboczych Wykonawca przygotuje “Plan testów” dla danego etapu uwzględniając wymagania z przedmiotu zamówienia.
4. Po wykonaniu każdego testu dotyczącego wybranego etapu realizacji zamówienia Wykonawca sporządzi raport. Raport będzie zawierał m.in.:
   - szczegółowy opis przeprowadzonych prac,
   - szczegółowy wykaz wykrytych podatności, wraz z dowodami na ich istnienie w postaci zrzutów ekranu oraz logów oprogramowania użytego podczas audytu
   - Co do zasady każda podatność powinna być oznaczone kodem ze słownika CVE (CommonVulnerabilities and Exposures),
   - rekomendacje w zakresie sposobu wyeliminowania wykrytych podatności wraz z podaniem zaleceń i instrukcji do wprowadzenia korekt konfiguracyjnych w celu ich eliminacji,
   - opis w formie streszczonej aktualnego poziomu bezpieczeństwa wraz z jego oceną
   - raport powinien być zabezpieczony przed możliwością przejęcia i odczytania zawartości przez podmioty niebiorące udziału w realizacji przedmiotu umowy

Wykonawca ma 20 dni roboczych na wykonanie każdego etapu testów i sporządzenie raportu

5. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu o którym mowa w pkt. 4 “Sposób realizacji zamówienia” w terminie 10 dni roboczych od otrzymania każdego raportu.
6. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego w terminie 5 dni roboczych.
7. Formuła realizacji zamówienia zostanie określona w uzgodnieniu z Wykonawcą w trakcie spotkań roboczych po podpisaniu umowy.

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 systemu ZRK nie wymienionych w przedmiocie zamówienia a dotyczących testów penetracyjnych aplikacji WWW, infrastruktury ZRK oraz analizy konfiguracji serwerów ZRK.
4. Realizacja przedmiotu zamówienia odbywać się będzie głównie zdalnie, niemniej jednak w uzasadnionych przypadkach Zamawiający akceptuje realizację zleconych prac w siedzibie Zamawiającego. 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 zatrudniona przez wykonawcę. Osoba ta będzie odpowiedzialna m.in. za:
   a) przestrzeganie terminów umownych dotyczących Wykonawcy,
   b) kontakty z Zamawiającym, w tym przekazywanie odpowiedzi na pytania Zamawiającego dotyczące realizacji umowy,
   c) przestrzeganie obowiązków Wykonawcy wynikających z umowy, w szczególności dotyczących zapisów odnośnie danych osobowych i poufności informacji.

Harmonogram płatności

Płatność za każdy etap realizacji zamówienia nastąpi po ostatecznym zaakceptowaniu przez Zamawiającego raportu z przeprowadzonych testów bezpieczeństwa.