Załącznik Nr 4

Nazwa przedmiotu zamówienia: Wykonanie audytów i testów bezpieczeństwa, wydajnościowych i zgodności z WCAG 2.0 systemu bibliotecznego, portalu internetowego oraz aplikacji mobilnej

Numer referencyjny sprawy: PBWR-9/2018/PEBP

Szczegółowy opis przedmiotu zamówienia

Wykonanie audytów i testów bezpieczeństwa, wydajnościowych i zgodności z WCAG 2.0 wytworzonego portalu www, katalogu elektronicznego oraz aplikacji mobilnych w ramach projektu Podkarpackie e-biblioteki pedagogiczne w niniejszym postępowaniu dofinansowany jest w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2014-2020 działanie 2.1 Podniesienie efektywności i dostępności e-usług, konkurs nr RPPK.02.01.00-IZ.00-18-002/16.

Uwagi:

1. Ilekroć w niniejszym opisie wymagań używane są słowa „należy", „powinien" lub „musi", niezależnie od formy i konstrukcji gramatycznej w której występują, należy je rozumieć jako wyrażające obowiązek Wykonawcy do wykonania określonych działań, zastosowania się do wskazanego obowiązku lub wypełnienia kryterium.
2. Ilekroć w niniejszym opisie jest użyte sformułowanie portal należy przez to rozumieć system obejmujący:
    a. stronę Biblioteki Pedagogicznej w Tarnobrzegu dostępnej pod adresem http://tarnobrzegbeta.pbw.org.pl docelowo dostępna pod adresem http://tarnobrzeg.pbw.org.pl wraz z Biuletynem Informacji Publicznej
    b. strona Pedagogicznej Biblioteki Wojewódzkiej w Rzeszowie dostępna pod adresem http://rzeszowbeta.pbw.org.pl docelowo dostępna pod adresem http://rzeszow.pbw.org.pl wraz z Biuletynem Informacji Publicznej
    c. strona Pedagogicznej Biblioteki Wojewódzkiej w Krośnie dostępna pod adresem http://krosnobeta.pbw.org.pl docelowo dostępna pod adresem http://krosno.pbw.org.pl wraz z Biuletynem Informacji Publicznej
    d. strona Pedagogicznej Biblioteki Wojewódzkiej w Przemyślu dostępna pod adresem http://przemyslbeta.pbw.org.pl docelowo dostępna pod adresem http://przemysl.pbw.org.pl wraz z Biuletynem Informacji Publicznej
    e. witrynę agregującą wiadomości ze stron internetowych bibliotek dostępną pod adresem http://beta.pbw.org.pl docelowo dostępna pod adresem http://pbw.org.pl.
    f. Stronę e-learningową bibliotek dostępną pod adresem http://elearning.pbw.org.pl.

    Szczegółowy opis funkcjonalny portalu dostępny jest w Szczegółowym Opisie Przedmiotu Zamówienia, umieszczonym w BIP PBW Rzeszów, postępowanie numer: PBWR-4A/2017/PEBP, adres: http://bip.rzeszow.pbw.org.pl/index.php?id=112&p=25.

3. System biblioteczny należy przez to rozmieć katalog elektroniczny Kompleksowego Systemu Zarządzania Biblioteką Prolib dostępny pod adresem: http://opac.pbw.org.pl/integro/ integrujący ze sobą katalogi 4 ww. bibliotek.

   Szczegółowy opis funkcjonalny katalogu dostępny jest w Szczegółowym Opisie Przedmiotu Zamówienia, umieszczonym w BIP PBW Rzeszów, postępowanie numer: PBWR-2/2017/PEBP, adres: http://bip.rzeszow.pbw.org.pl/index.php?id=112&p=20

4. Aplikacje mobilne należy przez to rozmieć aplikacje na systemy mobilne: Android, iOS oraz Windows Phone/Mobile.

   Szczegółowy opis funkcjonalny aplikacji mobilnych dostępny jest w Szczegółowym Opisie Przedmiotu Zamówienia, umieszczonym w BIP PBW Rzeszów, postępowanie numer: PBWR-5/2017/PEBP, adres: http://bip.rzeszow.pbw.org.pl/index.php?id=112&p=27

5. Ilekroć w niniejszym opisie są przytaczane wymagania WCAG 2.0 należy przez to rozumieć wytyczne zawarte w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526 z późn. zm.)

I. Audyt i testy bezpieczeństwa

Wykonanie testów penetracyjnych mających za zadanie wykrycie jak największej liczby błędów, mogących wpływać na integralność, autentyczność, niezaprzeczalność i poufność danych w uruchomionych usługach. Testy powinny obejmować co najmniej walidację parametrów, niepoprawne kodowanie, mechanizmy uwierzytelniające oraz logikę biznesową. Zamawiający wymaga wykonania kontrolowanych prób przełamania zabezpieczeń bez znajomości szczegółów budowy systemu (tzw. testy black-box).

W ramach testów zamawiający wymaga wykonania audytu portalu e-biblioteki, katalogu elektronicznego oraz aplikacji na systemy mobilne android, ios oraz windows phone. Każda z aplikacji mobilnych powinna zostać przetestowana osobno.

Katalog i portal powinny być przetestowane w oparciu o metodykę OWASP (Open Web Application Security Project), a w szczególności o klasyfikację OWASP Top 10, OWASP ASVS (Application Security Verification Standard) zawierający najlepsze praktyki w zakresie testów bezpieczeństwa.

Testy penetracyjne katalogu elektronicznego oraz portalu muszą obejmować co najmniej:

- wstrzyknięcia kodu (ang. injections) - SQL/XML Injection, podatności umożliwiające nieautoryzowany dostęp do danych - błędy: SQL, OS shell, LDAP, XPath Injection,
- file include - nieautoryzowany dostęp (i odczyt) do plików systemowych,
- błędy typu Cross-Site Scripting (XSS) - umożliwiające wykonanie szeregu nieautoryzowanych akcji w aplikacji webowej, np.: podmiany zawartości strony po stronie klienta, wykonanie czynności jako inny użytkownik lub ataki typu phishing,
- ujawnienie informacji - najczęściej dotyczących systemu oraz stosowanych zabezpieczeń, umożliwiających przeprowadzenie dalszych ataków wymierzonych w aplikację lub infrastrukturę,

- podatności związane z zarządzaniem sesją - np. przechwycenie sesji i dostęp do serwisu jako inny użytkownik, itp.,
- testowanie mechanizmów uwierzytelniających,
- testowanie podatności SSL/TLS,
- testy eskalacyjne - dotyczące błędów w systemach uprawnień,
- nieaktualne oprogramowanie,
- błędy typu Cross Site Request Forgery (CSRF) – umożliwiające wykonanie szeregu nieautoryzowanych akcji w aplikacji web,
- testowanie aplikacji pod katem występowania błędów logicznych,
- niebezpieczne przekierowania,
- testowanie podatności HTTP Parameter Pollution.

Wykonawca testów przystępując do audytu będzie miał poziom wiedzy o serwisie na poziomie analogicznym jak inni jej użytkownicy - przyjęta zostanie technika BlackBox.

Po wykonaniu audytów/testów zamawiający wymaga utworzenia raportu podatności, który zostanie przedstawiony wykonawcy portalu, katalogu elektronicznego oraz aplikacji mobilnych. Wykonawcy testowanych systemów będą musieli usunąć przedstawione podatności. Po ich usunięciu wykonane zostaną ponowne testy wcześniej znalezionych podatności i wygenerowany ponownie raport.

II. Testy wydajnościowe

Testy portalu, katalogu elektronicznego oraz aplikacji mobilnych.

Wykonanie testów wydajnościowych:

- badanie czasu odpowiedzi krytycznych funkcji systemu
- porównywanie czasu odpowiedzi przejścia pojedynczego vs. wielu użytkowników przez aplikację
- przeciążeniowych:
    - założenie: zbyt wielu użytkowników, wykonywanych akcji w aplikacji oraz malejące zasoby systemowe
    - wyszukiwanie defektów w aplikacji działającej w trybie awaryjnym - sprawdzanie konsekwencji utraty danych po awarii wywołanej nadmiernym obciążeniem
- obciążeniowych:
    - duża liczba jednocześnie działających użytkowników / przeprowadzanych akcji - utrzymanie takiego stanu przez określony czas i analiza jak wiele zapytań (requests) jest w stanie obsłużyć system w określonym przedziale czasu.

W ramach testów wykonawca powinien przeprowadzić analizę typowych zachowań użytkowników i zbudować model obciążenia zawierający informacje o akcjach użytkowników i czasie ich pobytu na stronie a także procent użytkowników wykonujących akcję. Dzięki modelowi możliwe będzie symulowanie dowolnej liczby użytkowników.

Przeprowadzenie testów weryfikujących czy wydajność aplikacji jest założonymi wymaganiami

Po wykonaniu testów wykonawca powinien przedstawić raport zawierający informacje odnośnie zapytań lub elementów strony, które mogą być odpowiedzialne za niewystarczającą wydajność aplikacji. Pomoc przy poszukiwaniu przyczyn niskiej wydajności.

Po optymalizacji aplikacji wykonanie ponownych re-testów.

III. Audyt i testy zgodności z WCAG 2.0

Testy portalu oraz katalogu elektronicznego.

Wykonanie testów zgodności z wytycznymi WCAG 2.0 zawartymi w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526 z późn. zm.) dla portalu, katalogu elektronicznego.

Testy dostępności powinien być wykonany w dwóch etapach:

1. Badania eksperckiego przeprowadzonego przez ekspertów z zakresu programowania i dostępności. Polegającego na sprawdzeniu przez eksperta szeregu elementów mających wpływ na dostępność serwisu zgodnie z listą kontrolną WCAG 2.0.
2. Badania z użytkownikami niepełnosprawnymi. Będzie to audyt User Experience, czyli badanie z osobami niewidomymi, niedowidzącymi i głuchymi. Podzielone ono będzie na dwie części. W pierwszej sprawdzone zostaną kluczowe elementy serwisu. Osoby niesłyszące sprawdzają zrozumiałość i przejrzystość treści i ich wpływ na odbiór serwisu, osoby niewidzące z wykorzystaniem oprogramowania asystującego sprawdzą możliwość nawigowania i pozyskania informacji w serwisie. W drugiej części badający wykonają serię zadań wytypowanych dla danego serwisu.

Badanie powinno być zrealizowane pod kątem:

- Zgodności ze standardem WCAG 2.0.
- Współpracy z technologiami asystującymi używanymi w najpopularniejszych systemach mobilnych.
- Użyteczności i funkcjonalności zarówno z poziomu ekranów dotykowych jak i innych zewnętrznych urządzeń (zewnętrzne klawiatury, linijki brajlowskie, itp.).
- Prawidłowej prezentacji treści na urządzeniach o różnej wielkości matrycy i dynamicznie zmieniającej się orientacji obrazu.
- Użyteczności opcji ustawień.

Po przeprowadzeniu testów powinien zostać przygotowany raport z badania zawierający:

- Wskazanie niezgodności ze standardem WCAG 2.0.
- Opis problemów na jakie napotkali niepełnosprawni użytkownicy.
- Sposoby rozwiązania problemów.

Termin realizacji

Poszczególne testy/audyty mogą odbywać się równolegle. Szczegółowy harmonogram prac zostanie ustalony z wybranym wykonawcą.

Szacowane daty rozpoczęcia testów:

- bezpośrednio po podpisaniu umowy dla aplikacji mobilnych oraz portalu,
- 01 czerwiec 2018r dla systemu bibliotecznego.

Czas wykonanie testów, re-testów

- zgodnie z deklaracją wykonawcy w formularzu ofertowym dla aplikacji mobilnej oraz portalu,
- dla systemu bibliotecznego nie więcej niż 20 dni na testy i nie więcej niż 14 dni na re-testy.

Szacowane daty zakończenia re-testów:

- 18 maj dla portalu,
- 25 maj dla aplikacji mobilnych,
- 31 lipiec dla systemu bibliotecznego.