Szczecin, dnia 27.02.2020 r.

ZAPYTANIE OFERTOWE

na wykonanie audytu kodu i bezpieczeństwa serwisu oraz aplikacji webowej,

obsługujących tworzenie przewodników do zwiedzania atrakcji turystycznych z elementami gamifikacji, stworzonych w ramach projektu BalticMuseums: Love IT!

1. Zamawiający

Uniwersytet Szczeciński
Aleja Papieża Jana Pawła II, 22a
70-453 Szczecin
Projekt: BalticMuseums: Love IT!

2. Opis zamówienia

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa serwisu webowego obsługującego aplikacje-przewodniki do zwiedzania atrakcji turystycznych z elementami gamifikacji, stworzonego w ramach projektu BalticMuseums: Love IT!

Opis przedmiotu zamówienia:

Wykonawca zobowiązuje się do wykonania audytu bezpieczeństwa serwisu webowego o następujących parametrach:

- Technologie/biblioteki:

- https://www.djangoproject.com/
- https://www.django-rest-framework.org/
- https://pypi.org/project/django-cors-headers/
- https://pypi.org/project/django-extensions/
- https://pypi.org/project/django-filters/
- https://pypi.org/project/sorl-thumbnail/
- https://pypi.org/project/django-qr-code/

- https://pypi.org/project/django-crispy-forms/
- https://pypi.org/project/bootstrap4/
- https://pypi.org/project/django-private-storage/
- https://pypi.org/project/django-rest-framework-social-oauth2/
- https://getbootstrap.com/
- https://jquery.com/

- Statystyki plików:

=Python=

Liczba plików: 162

Linie: 12843

Klasy: 665

Metody/Funkcje: 418

=Javascript=

Liczba plików: 1

Linie: 106

Funkcje: 56

=CSS=

Liczba plików: 1

Linie: 78

=HTML=

Liczba plików: 35

Linie: 4213

Liczba endpoint-ów (na dzień 27.02.2020): 56

Dokumentacja dostępna na stronie:

http://bsg.bmloveit.usz.edu.pl/docs/

Przeprowadzony przez wykonawcę audyt bezpieczeństwa powinien obejmować analizę kodu źródłowego serwisu oraz testy manualne i

automatyczne, obejmujące pozorowane ataki na serwis:

1. Podstawowy audyt infrastruktury oraz sieci.

2. Detekcja defektów w kodzie serwisu powodujących luki bezpieczeństwa.

3. Odporność serwisu na ataki różnych typów, w szczególności:

- SQL injection.
- XSS (Cross Site Scripting) – błędy typu reflected oraz stored.
- Detekcja zabezpieczeń na podatność CSRF (Cross Site Request Forgery)
- Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia użytkownika) dla zasobów wymagających autoryzacji.
- Code Execution (próby wykonania wrogiego kodu na serwerze).
- Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania).
- Path Traversal.
- Open Redirection.
- Denial of Service (DoS).
- File Inclusion.
- Response Splitting.

Raport z przeprowadzonego przez wykonawcę audytu będzie zawierał ocenę bezpieczeństwa i rekomendacje (z podziałem na konieczne i zalecane).

Wykonawca oświadcza, że dysponuje odpowiednią wiedzą oraz doświadczeniem niezbędnymi do należytego zrealizowania przedmiotu umowy i zobowiązuje się wykonać przedmiot umowy w najlepszej woli, zgodnie z posiadaną wiedzą fachową, starannie, uczciwie i odpowiedzialnie z uwzględnieniem obowiązujących przepisów prawa i przyjętych standardów, z uwzględnieniem profesjonalnego charakteru prowadzonej przez siebie działalności, wykorzystując w tym celu wszystkie posiadane możliwości, a także mając na względzie ochronę interesów Zamawiającego.

Wykonawca oświadcza, że przy wykonywaniu przedmiotu umowy będzie wykorzystywał jedynie materiały, utwory, dane i informacje oraz programy komputerowe, które są zgodne z obowiązującymi przepisami prawa, a w szczególności nie naruszają dóbr osobistych i majątkowych oraz osobistych praw autorskich, praw pokrewnych, praw do znaków towarowych lub wzorów użytkowych bądź innych praw własności przemysłowej, a także danych osobowych osób trzecich. Gdyby doszło do takiego naruszenia, wyłączną odpowiedzialność względem osób i podmiotów, których prawa zostały naruszone, ponosi Wykonawca.

3. Sposób realizacji zamówienia

Zamówienie zostanie zrealizowane w całości maksymalnie do dnia 25.03.2020. Zamawiający udzieli Wykonawcy dostęp do serwisu i jego kodu źródłowego, dla których ma zostać wykonany audyt bezpieczeństwa.

Etapy:

1. Zamawiający wskaże Wykonawcy lokalizację audytowanego serwisu i zapewni dostęp do jego kodu źródłowego i dokumentacji technicznej w ciągu 2 dni roboczych.
2. Wykonawca w ciągu 8 dni roboczych wykona audyt bezpieczeństwa i prześle z niego raport Zamawiającemu.
3. Zamawiający zaakceptuje raport lub zgłosi ewentualne braki i błędy w raporcie Wykonawcy w ciągu 1 dnia roboczego.
4. Wykonawca w ciągu 2 dni roboczych uzupełni lub poprawi raport i prześle go Zamawiającemu.
5. Zamawiający w ciągu 1 dnia roboczego podejmie decyzję o zaakceptowaniu raportu lub odrzuceniu go w całości w przypadku gdyby jego treść nie odpowiadała wymogom opisanym w niniejszym zamówieniu.

4. Podstawy i tryb udzielenia zamówienia

Kryteria wyboru oferty

Wykonawca zostanie wyłoniony spośród oferentów na podstawie następujących kryteriów oceny:

Kryteria ocen:

50% - cena (max. 50 pkt) obliczana na podstawie wzoru:

Ilość punktów = C_{min}/C_{wn} x 100 pkt x waga kryterium

C_{min} – cena minimalna spośród zaproponowanych cen ofertowych, C_{wn} – cena zaproponowana przez wykonawcę n

50 % - kompetencje osób wskazanych przez Oferenta do wykonania audytu

Punkty:

- 5 punktów za każdy rok zaangażowania w projekcie lub za każdy ukończony projekt (Oferent może wskazać korzystniejszy dla niego wariant dla każdego wymienionego projektu) w technologii Python/Django, w którym w sposób udokumentowany uczestniczyły osoby wskazane przez Oferenta do wykonania audytu w charakterze programisty lub specjalisty ds. bezpieczeństwa (max. 25 pkt),

- 5 punktów za każdy audyt bezpieczeństwa serwisu internetowego wykonany przez osoby wskazane przez Oferenta do wykonania audytu w ciągu ostatnich 2 lat (max. 25 pkt).

Każdy punkt odpowiada 1%. Maksymalna ilość punktów do uzyskania w tym kryterium – 50 pkt (50% wagi oceny oferty)

W ostatnim etapie zostaną zsumowane oceny z poszczególnych kryteriów:

Suma kryteriów oceny 50% (cena) i 50% (kompetencje kadry): max ***100 pkt****.*

5. Termin i miejsce złożenia oferty

1. Ofertę wraz z wymaganymi dokumentami należy składać w wersji elektronicznej, skan oferty przesyłając przez platformę zakupową: https://platformazakupowa.pl/pn/usz
2. Oferty należy złożyć w nieprzekraczalnym terminie do dnia 10.03.2020 do godz. 12.00. 11.03.2020
3. Oferty niekompletne, niewłaściwie opisane lub złożone po wyznaczonym terminie pozostaną bez rozpatrzenia z przyczyn formalnych. Wykonawca ponosi wszelkie koszty związane z przygotowaniem oferty.
4. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.

6. Sposób przygotowania oferty

W treści oferty musi być zawarty:

- Adres zamawiającego
- Adres oferenta
- Cena (netto i brutto) za wykonanie przedmiotu zapytania ofertowego określonego w

opisie zamówienia

- Termin wykonania zamówienia
- Do oferty należy załączyć skan aktualnego wpisu do właściwego rejestru, uprawniającego Wykonawcę do wystąpienia w obrocie prawnym.

7. Prawa autorskie

Majątkowe prawa autorskie do przedmiotu umowy zostaną przy Wykonawcy. Zamawiający nie będzie rościł sobie po wykonaniu umowy żadnych praw majątkowych do dzieła. Wykonawca zobowiązuje się udzielić licencji na wykorzystanie dzieła do celów promocji i informacji dotyczącej projektu BalticMuseums: Love IT!

8. Osoba uprawniona do kontaktów z Wykonawcą

Agnieszka Miluniec, tel. 513 055 010, e-mail: agnieszka.miluniec@usz.edu.pl

R E K T O R

.....prof. dr hab. Edward Włodarczyk.....

W imieniu Zamawiającego

8.1 Załączniki

- formularz ofertowy