

Opole, 19.02.2020r.

Zapytanie ofertowe nr AT/2/02/2020

Wykonanie testów bezpieczeństwa aplikacji mobilnej O!polskie Muzea z systemem CMS oraz serwera.

Zamawiający

Muzeum Polskiej Piosenki w Opolu
Pl. Kopernika 1, 45-040 Opole
NIP: 754-296-52-52, REGON: 160234900

I. Tryb udzielenia zamówienia

Zamówienie o wartości szacunkowej poniżej 30.000 EUR nieobjęte przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2010 r. nr 113, poz. 759 ze zm.).

II. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest wykonanie testów aplikacji mobilnej O!polskie Muzea z systemem CMS oraz analiza konfiguracji serwerów WWW, baz danych. Aplikacja mobilna „O!Polskie Muzea” jest projektem dofinansowanym przez Ministerstwo Kultury i Dziedzictwa Narodowego w ramach programu „Kultura Cyfrowa”. Zakres przedmiotu zamówienia obejmuje:

- 1) Testy aplikacji mobilnych Android oraz iOS (ok. 7 unikalnych widoków). Testy metodą whitebox lub greybox powinny dotyczyć w szczególności:
 - a. analizy podatności Cross-Site Scripting
 - b. sprawdzenia, czy zaimplementowany został mechanizm pinningu certyfikatów,
 - c. analizy sposobu nawiązywania połączenia SSL/TLS z komponentem serwerowym pod kątem poprawności sprawdzania certyfikatu serwera,
 - d. analizy sposobu przechowywania przez aplikację danych uwierzytelniających oraz innych poufnych danych w pamięci masowej telefonu (np. w plikach konfiguracyjnych, plikach cache, plikach tymczasowych, bazach sqlite, we

współdzielonej pamięci masowej itp.) pod kątem możliwości wycieku tych danych w razie kradzieży telefonu lub zainstalowania złośliwej aplikacji,

2) Testy systemu CMS (ok. 10 podstron, 2-3 grupy użytkowników). Testy metodą blackbox powinny dotyczyć w szczególności:

- a. próby lokalizacji ukrytych katalogów i plików
- b. próby wywołania błędów / wyjątków w aplikacji
- c. poszukiwania wycieków danych (np. technika google hacking, analiza pliku robots.txt).
- d. poszukiwania podatności klas: SQL Injection, Xpath Injection, NoSQL Injection, XXE, XSS - reflected oraz stored
- e. analizy problemów z uwierzytelnianiem i autoryzacją (np. próby dostępu do zasobów bez uwierzytelnienia, próby dostępu do zasobów administracyjnych przez zwykłego użytkownika, próby przełamania ekranów logowania – w tym próby brute force danych dostępowych)
- f. możliwości otrzymania nieautoryzowanego dostępu na poziomie systemu operacyjnego i uzyskanie w ten sposób dostępu do źródeł aplikacji, bazy danych, innych poufnych informacji
- g. analiza błędów logicznych
- h. próby wykrycia innych, znanych podatności, np.: path traversal, open redirection, cross site request forgery, server side request forgery, server side template injection.
- i. detekcja ogólnie znanego oprogramowania (aplikacje, biblioteki, systemy wspomagające). Po wykryciu nieaktualnych wersji, próby lokalizacji znanych, istotnych podatności w kilku wybranych źródłach

3) Analiza konfiguracji serwerów (dwie instancje systemu operacyjnego Ubuntu, jedna instancja serwera WWW Apache, jedna instancja bazy danych MySQL). Testy metodą blackbox powinny dotyczyć w szczególności:

- a. analizy konfiguracji SSL (certyfikat, skonfigurowane algorytmy kryptograficzne)
- b. analizy ujawnienia dokładnej wersji komponentu (nagłówki odpowiedzi / komunikaty błędów)

α

- c. po udanym pozyskaniu wersji komponentu, próba zlokalizowania publicznie dostępnych podatności w tej wersji
- d. analizy domyślnych aplikacji typu „example” lub „demo” (dostarczanych domyślnie z serwerem webowym / aplikacyjnym)
- e. siłowych prób wymuszania wyświetlenia błędów / wyjątków (np.: przesłanie nieprawidłowego adresu URL, wysłanie niepoprawnego requestu)
- f. analizy domyślnej domeny skonfigurowanej na komponencie (np. poprzez odwołanie się do adresu IP)
- g. analizy obsługi nietypowych metod HTTP (TRACE, DEBUG, PUT, DELETE)

Testy powinny być wykonane zgodnie z metodologiami:

- OWASP TOP 10 (bezpieczeństwo aplikacji webowych, bezpieczeństwo aplikacji mobilnych)
- OWASP ASVS w zakresie testów aplikacji webowych
- OSSTMM ogólne prowadzenie prac audytowych

Wykonawca zobowiązuje się do ponownego wykonania testów oraz w razie potrzeby retestów (max 3 retesty) po usunięciu zgłoszonych błędów przez Zamawiającego.

2. Dla potrzeb realizacji przedmiotu zamówienia, Wykonawca będzie zobowiązany zapewnić, korzystając z własnych zasobów kadrowych, zespół projektowy do wykonania przedmiotu zamówienia w skład którego wchodzić będzie przynajmniej 1 osoba, posiadająca ważny certyfikat Certified Information Systems Security Professional oraz OSCP (Offensive Security Certified Professional). **Kopie certyfikatów jw. poświadczone za zgodność z oryginałem Wykonawca zobowiązany jest przedłożyć Zamawiającemu wraz z ofertą.**
3. Wykonawca powinien wykazać wraz ze złożeniem oferty a to pisemnym dokumentem referencji wystawionym przez zleceniodawcę tego zadania doświadczenie własne w prawidłowej realizacji – nie wcześniejszej niż 3 lata przed datą ogłoszenia niniejszego zapytania ofertowego - minimum dwóch (dwóch) realizacji z zakresu testu i audytu bezpieczeństwa aplikacji udostępnianych za pośrednictwem sieci Internet o wartości każdej takiej realizacji z osobna nie mniejszej niż 5000,00 zł netto.

III. Termin wykonania zamówienia

Termin wykonania przedmiotu zamówienia: do 30.06.2020 r.. Składowe przedmiotu zamówienia do wykonania testów będą systematycznie udostępniane Wykonawcy z odpowiednim wyprzedzeniem w sposób uzgodniony w trybie roboczym, po wykonaniu aplikacji mobilnej i skonfigurowaniu serwerów przez wykonawcę ww. zadań.

IV. Kryterium oceny ofert oraz sposób obliczenia ceny oferty

1. Zamawiający dokona oceny ważnych ofert na podstawie następujących kryteriów

Kryteria wyboru i sposób oceny ofert	Waga
Kryterium 1 – Cena Pod uwagę brana będzie cena brutto za realizację zamówienia. Zamawiający określi liczbę punktów uzyskaną w w/w kryterium wg następującego wzoru $\text{cena najniższa} / \text{cena badanej oferty} * 60 \text{ pkt}$	60%
Kryterium 2 – Doświadczenie Za każdą wykazaną przez Wykonawcę wg pkt II ppkt 3 niniejszego zapytania ofertowego prawidłową, nie wcześniejszą niż 3 lata przed datą ogłoszenia niniejszego zapytania ofertowego, realizację testu i audytu bezpieczeństwa aplikacji udostępnianych za pośrednictwem sieci Internet o wartości każdej takiej realizacji z osobna nie mniejszej niż 5000,00 zł netto, Wykonawca otrzyma 5 pkt. Maksymalna liczba punktów, jaką może uzyskać każda oferta na ww. zasadach to 40 pkt. Zamawiający określi liczbę punktów uzyskaną w w/w kryterium wg następującego wzoru: $\text{Liczba punktów badanej oferty w kryterium Doświadczenie} / \text{Najwyższa liczba punktów w kryterium Doświadczenie spośród rozpatrywanych ofert} * 40 \text{ pkt}$	40%

- Obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku, bez zaokrągleń.
- Wybór najkorzystniejszej oferty – jak również punktacja odbywa się na posiedzeniu komisji oceniającej oferty składającej się z pracowników lub współpracowników Zamawiającego.
- W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonych ofert.
- W przypadku stwierdzenia w ofercie oczywistych omyłek pisarskich, oczywistych omyłek rachunkowych bądź innych oczywistych omyłek polegających na niezgodności ofert z przedmiotem zapytania ofertowego Zamawiający poprawi te pomyłki w treści złożonych ofert i niezwłocznie drogą elektroniczną email lub faks poinformuje o nich Wykonawców w celu wyrażenia przez nich zgody na dokonaną zmianę oferty. W przypadku gdy Wykonawca w wyznaczonym terminie nie wyrazi zgody na dokonaną poprawę oferty przez Zamawiającego jego oferta może zostać odrzucona.
- Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów, będącą sumą podanych wyżej kryteriów oceny ofert.

7. Zamawiający zastrzega sobie prawo do podjęcia negocjacji z Wykonawcą, którego oferta jest najkorzystniejsza, w szczególności gdy cena oferowana przekroczy kwotę jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.

V. Oferta powinna zawierać

1. Wartość netto i brutto za całość zamówienia.
2. W cenie zaoferowanej za wykonanie zamówienia Wykonawca zobowiązany jest ująć wszystkie przewidywane koszty związane z realizacją zamówienia plus podatek VAT naliczony zgodnie z obowiązującymi przepisami na dzień składania ofert oraz wszystkie koszty wynikające z zapisów niniejszego zapytania, bez których realizacja zamówienia nie byłaby możliwa.
3. Cena oferty musi być wyrażona w złotych polskich.
4. Ceny określone przez Wykonawcę zostaną ustalone na okres trwania umowy i nie będą podlegały zwiększeniu.
5. Faktura przelewowa na podstawie, której Zamawiający dokona wypłaty wynagrodzenia musi przewidywać termin płatności wynoszący przynajmniej 30 dni.
6. Nie dopuszcza się ofert wariantowych ani częściowych.
7. Podpisane oświadczenie o przetwarzaniu danych (załącznik 2).
8. Dokumenty wg pkt II ppkt 2 i 3 niniejszego zapytania.

VI. Miejsce realizacji zamówienia w tym szkoleń i wsparcia technicznego

Budynek Muzeum Polskiej Piosenki w Opolu przy ulicy Piastowskiej 14A.

VII. Osoby upoważnione do kontaktu z Wykonawcami

Dawid Garczarek, tel. 534 831 500

Email: dawid.garczarek@muzeumpiosenki.pl

Sylwia Gawłowska, tel. 507 359 792

Email: sylwia.gawlowska@muzeumpiosenki.pl

Kontakt w dni robocze w godzinach od 9:00. do 14:00

VIII.

Miejsce i termin składania ofert

Ofertę należy złożyć drogą elektroniczną za pomocą poczty na adres dawid.garczarek@muzeumpiosenki.pl lub osobiście w biurze Muzeum przy ul. Piastowskiej 14A w Opolu, do dnia 28.02.2020 r., do godz. 15:00 W każdym przypadku oferta powinna być opatrzona podpisem lub podpisami osób umocowanych do reprezentacji wykonawcy.

Uwagi

- Każdy wykonawca może złożyć tylko jedną ofertę.
- Treść ofert musi odpowiadać treści zapytania ofertowego.
- Złożenie oferty niezgodnej z obowiązującym prawem lub zapytaniem ofertowym, spowoduje odrzucenie oferty.
- Zamawiający udzieli zamówienia Wykonawcy, którego oferta spełni warunki określone przez Zamawiającego oraz uzyska największą liczbę punktów.
- Niezwłocznie po wyborze najkorzystniejszej oferty informacja zostanie przesłana do wybranego Wykonawcy.
- Zamawiający nie przewiduje zwrotu kosztów udziału w niniejszym postępowaniu, w tym przygotowania ani złożenia oferty.
- Od decyzji Zamawiającego dotyczących postępowania lub rozstrzygnięcia zapytania ofertowego nie przysługują środki odwoławcze.
- Oferty złożone po terminie nie będą rozpatrywane.
- Zamawiający zastrzega sobie możliwość unieważnienia postępowania na każdym jego etapie z dowolnej przyczyny.
- Wzór umowy na realizację przedmiotu umowy stanowi załącznik nr 3 do niniejszego zapytania. Wykonawca – w przypadku wybrania jego oferty - zobowiązuje się zawrzeć na wezwanie Zamawiającego umowę wg ww. wzoru.
- Zamawiający niezwłocznie - najpóźniej w następnym dniu roboczym - potwierdzi każdemu Wykonawcy, że jego oferta złożona w formie mailowej dotarła do Zamawiającego, także w formie mailowej. Brak potwierdzenia Zamawiającego faktu złożenia oferty jak w zdaniu poprzednim, obliguje Wykonawcę do zweryfikowania u Zamawiającego faktu dotarcia tej oferty do Zamawiającego, a to jeszcze przed upływem terminu do składania ofert. W przypadku zaniechania przez Wykonawcę działań jak w zdaniu poprzednim, Wykonawca nie może powoływać się względem Zamawiającego na fakt złożenia oferty, która nie dotarła do Zamawiającego.
- Klauzula informacyjna RODO Zamawiającego stanowi załącznik do niniejszego zapytania.

Dyrektor
Muzeum Polskiej Piosenki w Opolu
Jarostaw Wasik