

OGŁOSZENIE

o zamówieniu o wartości mniejszej niż 130 000,00 PLN lub wyłączonym spod stosowania przepisów ustawy – Prawo zamówień publicznych

Zamawiający:

Skarb Państwa - Generalna Dyrekcja Dróg Krajowych i Autostrad
z siedzibą w Warszawie, ul. Wronia 53

Przedmiot zamówienia:

Przedmiotem zamówienia jest przeprowadzenie testów bezpieczeństwa (penetracyjnych) webaplikacji zgodnie z poniższymi założeniami:

1. Przeprowadzenie testów typu „gray box” w oparciu o OWASP a w szczególności:
 - a. próba detekcji typu i wersji serwera WWW. Po udanej detekcji próba zlokalizowania znanych podatności.
 - b. sprawdzenie obsługi błędów na serwerze (testy bazujące na błędnie wysyłanych requestach)
 - c. sprawdzenie dostępności domyślnych katalogów
 - d. sprawdzenie dostępności oraz konfiguracji protokołów szyfrujących
 - e. sprawdzenie metod http udostępnianych na serwerze
2. Przeprowadzenie testów penetracyjnych w zakresie walidacji danych wejściowych (pliki cookie, nagłówki) parametrów wysyłane metodami http tj.:
 - a. badanie sesji użytkowników aplikacji,
 - b. badanie komunikatów błędów,
 - c. badanie mechanizmów przekierowań,
 - d. badanie danych zapisywanych do bazy danych,
 - e. badanie integralności logów aplikacji,
 - f. szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS),
 - g. badanie podatności na zagrożenia typu SQL Injection, Cross Site Scripting, LFI i RFI, Cross-Site Request Forgery, Click Jacking, Code Execution (próby wykonania wrogiego kodu na serwerze) itp.
 - h. badanie błędów logicznych aplikacji w miejscach krytycznych.
3. Sporządzenie i przedstawienie Zamawiającemu raportu z audytu.
4. Wsparcie Zamawiającego po przeprowadzonym audycie – konsultacje zakresie zidentyfikowanych podatności oraz przedstawionych w raporcie rekomendacji przez minimum 5 dni roboczych.

Dodatkowe wymagania:

Przed rozpoczęciem pracy Wykonawca sporządzi harmonogram audytu i przekaze do Zamawiającemu.

Raport przedstawiony zostanie w języku polskim i będzie zawierał przynajmniej:

1. Ogólną ocenę bezpieczeństwa testowanej strony WWW przygotowaną w języku nietechnicznym.
2. Wnioski i zalecenia dot. kolejnych działań i strategicznych zmian w infrastrukturze.

3. Szczegółową ocenę bezpieczeństwa testowanej infrastruktury przeznaczoną dla programistów.
4. Opis wykonanych testów i metodyki pracy
5. Listę znalezionych podatności wraz z określeniem dla każdej z nich:
 - a. miejsc wystąpienia;
 - b. szczegółowego opisu stwarzanego zagrożenia;
 - c. oceny ryzyka ewentualnego ataku, w kontekście procesów biznesowych świadczonych przez testowaną stronę WWW;
 - d. rekomendacji i sugestii dotyczące dokładnego usunięcia podatności.

Warunek udziału w postępowaniu

Zamawiający uzna ww. warunek za spełniony, jeżeli wykonawca wykaże, że:

1. Testerem wiodącym skierowanym do realizacji zlecenia będzie osoba posiadająca jeden lub więcej poniższych certyfikatów:
 - a. Offensive Security Certified Professional (OSCP)
 - b. OSSTMM Professional Security Tester (OPST)
 - c. GIAC Web Application Penetration Tester (GWAPT)
 - d. Certified Ethical Hacker (CEH)
 - e. eWPTX – eLearn Security Advanced Web Application Penetration Tester
 - f. Offensive Security Certified Expert (OSCE)
2. Wykonawca przeprowadził w okresie ostatnich 2 lat, a jeżeli działalność podmiotu jest krótsza, to w tym okresie, przynajmniej 10 testów bezpieczeństwa webaplikacji.

Oferta musi zawierać:

1. **Formularz ofertowy** (załączony do ogłoszenia)
2. Protokoły odbioru lub oświadczenia zlecniodawcy potwierdzające należyte wykonanie testów bezpieczeństwa.
3. Potwierdzenie spełnienia wymogów dotyczących certyfikatów przez testerów skierowanych do realizacji zlecenia.

Formularz ofertowy oraz dokumenty potwierdzające warunek udziału należy przesłać na adres:

mpanasiuk@gddkia.gov.pl **do 22 maja 2023 r. (włącznie).**

Osoba prowadząca sprawę: Małgorzata Panasiuk, tel.: 22 375 89 45

Dodatkowe informacje:

W wyborze oferty będą brane pod uwagę:

- cena brutto - 100%

Niniejsze zamówienie jest wyłączone spod stosowania ustawy Prawo zamówień publicznych.

Termin realizacji zamówienia

Dokładny termin rozpoczęcia testów zostanie uzgodniony z Wykonawcą po podpisaniu umowy.

Nie może być on jednak późniejszy niż 60 dni od popisania umowy.

Warunki płatności

Płatność wynagrodzenia po akceptacji protokołu odbioru usługi na rachunek bankowy wykonawcy nastąpi w terminie 14 dni od dnia otrzymania przez zamawiającego prawidłowo wystawionych faktur VAT. Za datę realizacji płatności uważa się datę, w którym zamawiający wydał swojemu bankowi dyspozycję polecenia przelewu pieniędzy na konto wykonawcy.