

Zapytanie ofertowe

Zlecenie wykonania testów podatności stron internetowych

Przedsiębiorstwo Usług Komunalnych „USKOM” Sp. z o.o. w Kozuchowie zaprasza do złożenia oferty na wykonanie jednorazowych testów podatności wskazanych przez Zamawiającego stron internetowych i serwisów WWW, wraz z analizą ustaleń oraz sporządzeniem raportu i zaleceń naprawczych. Zamówienie jest realizowane w ramach projektu „Cyberbezpieczne Wodociągi”.

1. Zamawiający i kontakt

Przedsiębiorstwo Usług Komunalnych „USKOM” Sp. z o.o. w Kozuchowie, ul. Elektryczna 9, 67-120 Kozuchów; tel. 68 355 22 08; e-mail: sekretariat@uskom.eu. Osoba prowadząca postępowanie i adres do składania ofert: p.malczyk@uskom.eu.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest jednorazowe przeprowadzenie testów podatności stron internetowych i serwisów WWW wskazanych przez Zamawiającego, w celu identyfikacji podatności, błędów konfiguracji i innych słabości mogących wpływać na poufność, integralność lub dostępność badanych serwisów. Szczegółowe wymagania określa załącznik nr 1 – „Zlecenie wykonania testów podatności stron internetowych” (opis przedmiotu zamówienia, dalej: OPZ), stanowiący integralną część zapytania.

Zakres badania obejmuje wskazane domeny, subdomeny i serwisy WWW, a także inne komponenty dostępne z sieci Internet, bezpośrednio związane z funkcjonowaniem badanych stron i usług internetowych, w granicach upoważnienia udzielonego przez Zamawiającego. Badaniem mogą być objęte wyłącznie zasoby, w odniesieniu do których Zamawiający jest uprawniony do zlecenia testów. Nie dopuszcza się prowadzenia testów infrastruktury, usług ani systemów podmiotów trzecich poza zatwierdzonym zakresem.

Przed rozpoczęciem testów Zamawiający przekaze Wykonawcy zatwierdzony wykaz zasobów objętych badaniem, stanowiący jednocześnie upoważnienie do przeprowadzenia testów w określonym zakresie. Przekazanie i zatwierdzenie wykazu nastąpi w formie dokumentowej, w szczególności za pośrednictwem poczty elektronicznej. W przypadku zasobów utrzymywanych przez podmioty trzecie testy mogą zostać przeprowadzone wyłącznie w zakresie, do którego Zamawiający posiada odpowiednie uprawnienia, z uwzględnieniem wymaganych zgód i zasad usługodawców.

Zakres ilościowy stanowiący podstawę wyceny oferty: maksymalnie 4 serwisów WWW w obrębie maksymalnie 3 domen i subdomen. Zamawiający przekaze Wykonawcy szczegółową listę adresów URL i innych identyfikatorów zasobów przed rozpoczęciem realizacji usługi; lista określi dozwolony zakres testów i nie może wykraczać poza wskazany zakres ilościowy.

Testy muszą uwzględniać w szczególności: bezpieczeństwo konfiguracji serwera WWW i usług powiązanych; uwierzytelnianie i autoryzację, kontrolę dostępu i zarządzanie sesją; walidację danych wejściowych; ryzyko nieuprawnionego ujawnienia informacji; konfigurację HTTPS/TLS i mechanizmów szyfrowania; podatne lub nieaktualne komponenty oraz inne typowe słabości aplikacji internetowych. Jeżeli funkcjonalności serwisu tego wymagają, należy także zbadać logowanie, odzyskiwanie dostępu, separację uprawnień oraz możliwość obejścia autoryzacji. Zakres czynności należy dostosować do architektury i funkcji badanych serwisów.

Zamawiający nie dopuszcza ofert częściowych ani wariantowych. Zamówienie obejmuje jedną kompletną usługę zgodną z OPZ.

3. Termin wykonania, raport i odbiór

Termin wykonania usługi, w tym przeprowadzenia testów i przekazania kompletnego raportu: do 15 listopada 2026 r. Przed rozpoczęciem badania Wykonawca uzgodni z Zamawiającym szczegółowy zakres zasobów, termin i zasady bezpiecznego wykonywania czynności. Testy będą prowadzone wyłącznie w uzgodnionym zakresie.

Po zakończeniu badania Wykonawca przekaze raport w postaci elektronicznej (PDF), który musi zawierać co najmniej: zakres i termin testów, opis zastosowanej metodyki i technik badawczych, wykaz zidentyfikowanych

podatności i nieprawidłowości, przypisany każdemu ustaleniu zasób (adres URL, komponent lub funkcjonalność), poziom istotności lub ryzyka z uzasadnieniem, możliwe skutki wykorzystania podatności, dowody potwierdzające ustalenia (o ile ich przedstawienie jest możliwe i bezpieczne) oraz konkretne zalecenia usunięcia podatności lub ograniczenia ryzyka. Raport musi pozwalać na zaplanowanie działań naprawczych.

Raport musi zawierać także wykaz wszystkich serwisów WWW, domen, subdomen lub innych zasobów faktycznie objętych testami, wraz z informacją o przeprowadzonym zakresie badania. W przypadku zasobów, dla których nie zidentyfikowano podatności, należy zamieścić odpowiednią informację. Jeżeli wykonanie określonych testów nie było możliwe, Wykonawca wskaże ograniczenia badania oraz ich przyczyny.

Podatności należy sklasyfikować co najmniej w kategoriach: krytyczny, wysoki, średni i niski albo według równoważnej skali stosowanej przez Wykonawcę. Dla każdej podatności należy uzasadnić ocenę i opisać potencjalny wpływ na bezpieczeństwo serwisu. Jeżeli jest to możliwe i zasadne, należy podać wynik CVSS, wektor i wersję CVSS. W przypadku znanej podatności komponentu należy wskazać odpowiedni identyfikator CVE, a w przypadku klasy słabości aplikacji – identyfikator CWE, o ile istnieje.

Podstawą odbioru usługi będzie wykonanie testów w zatwierdzonym zakresie oraz przekazanie kompletnego raportu spełniającego wszystkie wymagania określone w OPZ.

Zamawiający dokona weryfikacji raportu pod względem jego kompletności, zgodności z zakresem zamówienia oraz przydatności przedstawionych ustaleń i zaleceń do zaplanowania działań naprawczych.

W przypadku stwierdzenia braków, nieścisłości lub konieczności doprecyzowania ustaleń Wykonawca zobowiązany będzie do ich wyjaśnienia lub uzupełnienia bez dodatkowego wynagrodzenia, w terminie nie dłuższym niż 3 dni robocze od otrzymania uwag, chyba że Zamawiający uzgodni inny termin.

Przekazanie raportu niespełniającego wymagań OPZ nie stanowi wykonania usługi w terminie. Odbiór nastąpi po potwierdzeniu przez Zamawiającego prawidłowego wykonania zamówienia i zostanie udokumentowany protokołem odbioru.

4. Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy posiadający doświadczenie w wykonywaniu testów bezpieczeństwa lub analiz podatności stron, aplikacji albo serwisów internetowych. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże należyte wykonanie co najmniej jednej usługi obejmującej testy bezpieczeństwa lub analizę podatności strony, aplikacji bądź serwisu internetowego.

Na potwierdzenie doświadczenia Wykonawca dołącza do oferty wykaz wykonanych usług według wzoru stanowiącego załącznik nr 4, z podaniem przedmiotu usługi, podmiotu, na rzecz którego ją wykonano, oraz daty wykonania. Na żądanie Zamawiającego Wykonawca przedstawi dokument lub inne dowody potwierdzające należyte wykonanie wskazanej usługi.

O udzielenie zamówienia nie może ubiegać się Wykonawca, wobec którego zachodzą przesłanki wykluczenia określone w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Wykonawca składa oświadczenie o braku podstaw wykluczenia w Formularzu oferty (załącznik nr 2). Zamawiający może zweryfikować oświadczenie w publicznie dostępnych rejestrach oraz wezwać Wykonawcę do wyjaśnień.

5. Metodyka i bezpieczeństwo wykonywania testów

Wykonawca przeprowadzi badanie z wykorzystaniem metod automatycznych oraz ręcznej weryfikacji wykrytych podatności, w sposób ograniczający ryzyko wyników fałszywie dodatnich. Należy stosować aktualne, powszechnie uznane metodyki i dobre praktyki testów bezpieczeństwa aplikacji i serwisów internetowych, w szczególności OWASP Web Security Testing Guide (WSTG) lub metodykę równoważną, z uwzględnieniem aktualnych kategorii ryzyk OWASP Top 10. Zamawiający nie narzuca produktu, skanera ani producenta narzędzi.

Testy podatności muszą być prowadzone w sposób kontrolowany, bezpieczny i możliwie nieinwazyjny, z ograniczeniem ryzyka zakłócenia dostępności lub prawidłowego działania badanych serwisów.

Wykonawca nie jest uprawniony do przeprowadzania testów DoS/DDoS, celowego przeciążania usług, usuwania lub nieuprawnionego modyfikowania danych, dokonywania trwałych zmian konfiguracji ani innych czynności wykraczających poza zatwierdzony zakres badania.

W przypadku konieczności przeprowadzenia czynności mogących wpływać na dostępność, integralność danych albo ciągłość działania usług Wykonawca zobowiązany jest uprzednio przedstawić Zamawiającemu zakres i cel

planowanych działań, związane z nimi ryzyka oraz proponowane środki bezpieczeństwa. Ich wykonanie wymaga uzyskania uprzedniej zgody Zamawiającego w formie dokumentowej.

Jeżeli w trakcie badania wystąpi ryzyko niedostępności usługi, utraty lub modyfikacji danych albo innego nieprzewidzianego zakłócenia, Wykonawca zobowiązany jest niezwłocznie przerwać daną czynność i poinformować Zamawiającego.

Wykonawca realizuje testy zdalnie lub w inny uzgodniony sposób, stosownie do charakteru udostępnionych zasobów. Jeżeli badanie wymaga kont testowych albo innego dostępu uwierzytelnionego, sposób ich udostępnienia i wykorzystywania zostanie odrębnie uzgodniony z Zamawiającym, zgodnie z zasadami bezpieczeństwa.

6. Cena i kryterium wyboru

Wykonawca podaje jedną łączną cenę za kompletną usługę w zakresie określonym w niniejszym zapytaniu i OPZ, wyrażoną w PLN z dokładnością do dwóch miejsc po przecinku. Łączna cena oferty oznacza całkowitą kwotę do zapłaty przez Zamawiającego, z uwzględnieniem podatku VAT, jeżeli ma zastosowanie.

Na potrzeby oceny ofert przez łączną cenę oferty rozumie się całkowity koszt nabycia usługi ponoszony przez Zamawiającego, z uwzględnieniem podatku VAT, jeżeli obowiązek jego rozliczenia występuje zgodnie z właściwymi przepisami.

Wykonawca zobowiązany jest wskazać, czy w odniesieniu do przedmiotu zamówienia jest podatnikiem VAT czynnym, korzysta ze zwolnienia z podatku VAT lub stosuje inny właściwy sposób rozliczenia podatku VAT. W przypadku opodatkowania usługi podatkiem VAT Wykonawca wskaże cenę netto, właściwą stawkę VAT, kwotę podatku VAT oraz łączną cenę brutto. W przypadku zastosowania zwolnienia Wykonawca wskaże podstawę jego zastosowania.

Jedynym kryterium oceny ofert spełniających wymagania jest łączna cena oferty – 100%. Liczba punktów = (najniższa łączna cena oferty spośród ofert podlegających ocenie / łączna cena badanej oferty) × 100. Wynik zostanie zaokrąglony do dwóch miejsc po przecinku. Maksymalnie można uzyskać 100 punktów. W przypadku ofert z taką samą najniższą ceną Zamawiający wezwie tych Wykonawców do złożenia ofert dodatkowych z ceną nie wyższą od pierwotnej.

7. Przygotowanie i złożenie oferty

Ofertę należy sporządzić na formularzu stanowiącym załącznik nr 2 i podpisać przez osobę uprawnioną do reprezentowania Wykonawcy. Dopuszcza się podpisanie oferty własnoręcznie i przesłanie skanu w formacie PDF albo sporządzenie oferty w postaci elektronicznej i opatrzenie jej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Jeżeli ofertę podpisuje pełnomocnik, należy dołączyć dokument potwierdzający umocowanie.

Ofertę wraz z załącznikami należy przesłać na adres e-mail: p.malczyk@uskom.eu. Temat wiadomości: „Oferta – testy podatności stron internetowych – USKOM”. Termin składania ofert: 26.10.2026 r. do godz. 09.00. O zachowaniu terminu decyduje wpływ wiadomości do Zamawiającego.

Pytania dotyczące zapytania należy kierować na adres: p.malczyk@uskom.eu, najpóźniej do 22.10.2026 r. Odpowiedzi na pytania Wykonawców, bez ujawniania danych podmiotu zadającego pytanie, oraz ewentualne zmiany treści zapytania zostaną udostępnione w miejscu publikacji zapytania ofertowego. Jeżeli zmiany będą mogły mieć istotny wpływ na przygotowanie ofert, Zamawiający odpowiednio przedłuży termin ich składania, zapewniając Wykonawcom możliwość uwzględnienia zmian. Wykonawca pozostaje związany ofertą przez 30 dni od upływu terminu składania ofert.

Wraz z ofertą Wykonawca składa:

- 1) Formularz oferty – załącznik nr 2 (w tym oświadczenie o braku podstaw wykluczenia);
- 2) Wykaz wykonanych usług – załącznik nr 4;
- 3) dokument potwierdzający umocowanie osoby podpisującej ofertę – jeżeli umocowanie nie wynika z właściwego rejestru lub ofertę podpisuje pełnomocnik.

Dokumenty potwierdzające należyte wykonanie usług wskazanych w wykazie składa się na żądanie Zamawiającego. Zamawiający może wezwać do złożenia wyjaśnień lub uzupełnienia dokumentów, wyznaczając odpowiedni termin, o ile nie prowadzi to do zmiany ceny ani istotnej zmiany oferowanego świadczenia. Nie będą oceniane oferty złożone po terminie, niezgodne z OPZ ani złożone przez Wykonawców podlegających wykluczeniu

lub niespełniających warunków udziału pomimo wezwania. O wyniku postępowania Zamawiający poinformuje Wykonawców, którzy złożyli oferty.

8. Poufność, dane osobowe i dokumentacja projektu

Wszelkie informacje pozyskane w związku z realizacją testów, w szczególności o podatnościach, adresach, konfiguracjach, kontach, mechanizmach zabezpieczeń oraz wynikach badania, stanowią informacje poufne. Wykonawca może je wykorzystywać wyłącznie do realizacji zamówienia. Udostępnienie ich osobom trzecim wymaga uprzedniej zgody Zamawiającego.

Raport, wyniki testów, dane uwierzytelniające i materiały robocze muszą być przechowywane oraz przekazywane z zastosowaniem środków zabezpieczających przed nieuprawnionym dostępem, ujawnieniem, utratą lub modyfikacją. Hasła do zaszyfrowanych materiałów należy przekazywać odrębnym kanałem komunikacji. Po zakończeniu realizacji i odbiorze usługi Wykonawca usuwa dane robocze i ich kopie, o ile przechowywanie nie jest niezbędne do wykonania obowiązków wynikających z umowy lub obowiązującego prawa; na żądanie Zamawiającego potwierdzi usunięcie.

Jeżeli realizacja usługi wymaga przetwarzania przez Wykonawcę danych osobowych w imieniu Zamawiającego, strony zawrą odpowiednią umowę powierzenia zgodnie z art. 28 RODO. Wykonawca zapewni dokumentację wykonania usługi niezbędną do rozliczenia projektu „Cyberbezpieczne Wodociągi”, z zachowaniem wymagań poufności określonych w OPZ.

Załączniki

1. Załącznik nr 1 – Opis przedmiotu zamówienia: „Zlecenie wykonania testów podatności stron internetowych”.
2. Załącznik nr 2 – Formularz oferty na wykonanie testów podatności stron internetowych.
3. Załącznik nr 3 – Projekt umowy na wykonanie testów podatności stron internetowych.
4. Załącznik nr 4 – Wykaz wykonanych usług testów bezpieczeństwa lub analizy podatności stron, aplikacji lub serwisów internetowych.