

Znak Sprawy ZP.CYBER.U03.2026

L.p.	Wymaganie	Opis minimalnych wymagań
1	Przedmiot zamówienia	Przedmiotem zamówienia jest wykonanie jednorazowych testów podatności wskazanych przez Zamawiającego stron internetowych i serwisów WWW, w ramach zadania pn. „Zlecenie wykonania testów podatności stron internetowych”. Celem usługi jest identyfikacja podatności, błędów konfiguracji oraz innych słabości mogących wpływać na poufność, integralność lub dostępność badanych serwisów internetowych. Testy muszą umożliwić wskazanie wykrytych podatności oraz sformułowanie zaleceń dotyczących ich usunięcia lub ograniczenia związanego z nimi ryzyka. Usługa zostanie wykonana dla serwisów internetowych wskazanych przez Zamawiającego przed rozpoczęciem realizacji zamówienia.
2	Zakres badania	Zakres badania obejmuje wskazane przez Zamawiającego domeny, subdomeny, serwisy WWW oraz inne komponenty dostępne z sieci Internet, bezpośrednio związane z funkcjonowaniem badanych stron i usług internetowych. Szczegółowa lista adresów URL oraz zasobów objętych testami zostanie przekazana Wykonawcy przed rozpoczęciem realizacji usługi. Wykonawca jest zobowiązany do prowadzenia testów wyłącznie w zakresie wskazanym i zaakceptowanym przez Zamawiającego.

		Zakres badania musi umożliwiać identyfikację podatności i słabości mogących mieć wpływ na bezpieczeństwo wskazanych serwisów internetowych. Testami mogą zostać objęte wyłącznie zasoby wskazane przez Zamawiającego, w stosunku do których Zamawiający posiada uprawnienie do zlecenia przeprowadzenia testów bezpieczeństwa. Wykonawca nie jest uprawniony do prowadzenia testów wobec infrastruktury, usług lub systemów podmiotów trzecich, jeżeli nie zostały one wyraźnie wskazane przez Zamawiającego jako objęte zakresem badania. Przed rozpoczęciem testów Zamawiający przekaze Wykonawcy wykaz zasobów objętych badaniem, obejmujący w szczególności domeny, subdomeny, adresy URL lub inne identyfikatory zasobów. Przekazany wykaz stanowi jednocześnie określenie dozwolonego zakresu testów.
3	Zakres testów podatności	Testy podatności muszą obejmować w szczególności weryfikację bezpieczeństwa konfiguracji serwera WWW i powiązanych usług, mechanizmów uwierzytelniania i autoryzacji, kontroli dostępu, zarządzania sesją, walidacji danych wejściowych oraz możliwości nieuprawnionego ujawnienia informacji. Badanie musi również uwzględniać ocenę konfiguracji mechanizmów szyfrowania i komunikacji HTTPS/TLS, identyfikację podatnych lub nieaktualnych komponentów i oprogramowania oraz innych typowych podatności występujących w aplikacjach i serwisach internetowych. Zakres testów musi być dostosowany do rzeczywistej architektury i funkcjonalności badanych serwisów oraz umożliwiać identyfikację istotnych podatności mogących wpływać na ich bezpieczeństwo.

		Jeżeli funkcjonalność badanego serwisu tego wymaga, testy muszą obejmować również weryfikację mechanizmów logowania, odzyskiwania dostępu, separacji uprawnień użytkowników oraz możliwości uzyskania dostępu do funkcji lub danych z pominięciem przewidzianych mechanizmów autoryzacji.
4	Metodyka wykonania testów	Testy podatności muszą zostać przeprowadzone z wykorzystaniem metod automatycznych oraz ręcznej weryfikacji wykrytych podatności, w sposób pozwalający na ograniczenie ryzyka wystąpienia wyników fałszywie dodatnich. Wykonawca zobowiązany jest stosować aktualne, powszechnie uznane metodyki i dobre praktyki w zakresie testowania bezpieczeństwa aplikacji i serwisów internetowych, w szczególności OWASP Web Security Testing Guide (WSTG) lub metodykę równoważną. Przy określaniu obszarów wymagających weryfikacji należy uwzględnić również aktualne kategorie ryzyk wskazane w OWASP Top 10. Zamawiający nie narzuca wykorzystania konkretnego produktu, skanera ani producenta narzędzi. Dobór narzędzi i technik badawczych pozostaje po stronie Wykonawcy, pod warunkiem zapewnienia rzetelności i kompletności przeprowadzonych testów.
5	Sposób prowadzenia testów	Testy muszą być prowadzone w sposób kontrolowany, bezpieczny i możliwie nieinwazyjny, z ograniczeniem ryzyka zakłócenia działania badanych serwisów oraz powiązanych z nimi usług. W ramach realizacji zamówienia Wykonawca nie może celowo powodować niedostępności usług, usuwać ani modyfikować danych ani wykonywać działań

		wykraczających poza zakres uprzednio uzgodniony z Zamawiającym. Wszelkie czynności o potencjalnie destrukcyjnym charakterze lub mogące wpłynąć na dostępność, integralność danych albo ciągłość działania systemów mogą być wykonywane wyłącznie po uprzednim uzgodnieniu ich zakresu i uzyskaniu zgody Zamawiającego. W przypadku stwierdzenia, że wykonywane czynności mogą powodować niedostępność usługi, utratę lub modyfikację danych albo inne nieprzewidziane zakłócenie funkcjonowania systemu, Wykonawca zobowiązany jest niezwłocznie przerwać daną czynność oraz poinformować Zamawiającego o zaistniałej sytuacji.
6	Raport z wykonania usługi	Po zakończeniu testów Wykonawca zobowiązany jest do przekazania Zamawiającemu raportu z przeprowadzonego badania. Raport musi zawierać co najmniej: - zakres oraz termin wykonania testów; - opis zastosowanej metodyki i wykorzystanych technik badawczych; - wykaz zidentyfikowanych podatności i nieprawidłowości; - ocenę poziomu istotności lub ryzyka poszczególnych podatności; - opis możliwych skutków wykorzystania wykrytych podatności; - dowody potwierdzające występowanie podatności, o ile ich przedstawienie jest możliwe i bezpieczne; - zalecenia dotyczące sposobu usunięcia podatności albo ograniczenia związanego z nimi ryzyka;

		wskazanie zasobu, adresu URL, komponentu lub funkcjonalności, której dotyczy dane ustalenie; Raport musi być sporządzony w sposób czytelny i umożliwiający Zamawiającemu podjęcie działań naprawczych na podstawie przedstawionych ustaleń.
7	Klasyfikacja podatności	Zidentyfikowane podatności muszą zostać sklasyfikowane według poziomu ich istotności lub ryzyka, co najmniej w kategoriach: krytyczny, wysoki, średni, niski albo według równoważnej skali stosowanej przez Wykonawcę. Dla każdej podatności Wykonawca musi wskazać uzasadnienie przyjętej klasyfikacji oraz jej potencjalny wpływ na bezpieczeństwo badanego serwisu. Jeżeli jest to możliwe i zasadne, dla podatności Wykonawca musi wskazać wynik CVSS wraz z wektorem wykorzystanym do jego wyliczenia oraz zastosowaną wersją CVSS. Jeżeli ustalenie dotyczy znanej podatności określonego komponentu, należy wskazać właściwy identyfikator CVE, a jeżeli dotyczy klasy słabości aplikacji – odpowiedni identyfikator CWE, o ile taki identyfikator istnieje.
8	Wyjaśnienie wyników	Na żądanie Zamawiającego Wykonawca zobowiązany będzie do przedstawienia dodatkowych wyjaśnień dotyczących zidentyfikowanych podatności, w szczególności ich charakteru, poziomu ryzyka, możliwych skutków oraz rekomendowanych działań naprawczych lub ograniczających ryzyko. Wyjaśnienia mogą zostać przekazane w formie pisemnej lub podczas krótkiego spotkania konsultacyjnego z przedstawicielem Zamawiającego odpowiedzialnym za obszar IT.

		W ramach wyjaśnień Wykonawca musi umożliwić Zamawiającemu właściwą interpretację wyników badania oraz zaplanowanie adekwatnych działań naprawczych.
9	Poufność i bezpieczeństwo informacji	Wszelkie informacje pozyskane przez Wykonawcę w związku z realizacją testów, w szczególności dotyczące wykrytych podatności, konfiguracji systemów, adresów, kont, mechanizmów zabezpieczeń oraz wyników badania, muszą być traktowane jako informacje poufne. Wykonawca nie może udostępniać tych informacji osobom trzecim ani wykorzystywać ich w celu innym niż realizacja przedmiotu zamówienia, chyba że Zamawiający wyrazi na to uprzednią zgodę. Po zakończeniu realizacji usługi i jej odbiorze Wykonawca zobowiązany jest usunąć zgromadzone dane robocze oraz ich kopie, które nie są niezbędne do dalszej realizacji obowiązków wynikających z umowy lub obowiązujących przepisów prawa. Na żądanie Zamawiającego Wykonawca potwierdzi wykonanie tego obowiązku.
10	Wymagania wobec Wykonawcy i odbiór	Wykonawca musi posiadać doświadczenie w wykonywaniu testów bezpieczeństwa lub analiz podatności stron, aplikacji lub serwisów internetowych. Na potwierdzenie spełnienia tego wymagania Wykonawca przedstawi wykaz co najmniej jednej należycie wykonanej usługi obejmującej przeprowadzenie testów bezpieczeństwa lub analizy podatności strony, aplikacji lub serwisu internetowego, wraz z podaniem przedmiotu usługi, podmiotu, na rzecz którego została wykonana, oraz daty jej wykonania.

		Na żądanie Zamawiającego Wykonawca przedstawi dokument lub inne dowody potwierdzające należyte wykonanie wskazanej usługi. Podstawą odbioru usługi będzie: • wykonanie testów w zakresie określonym przez Zamawiającego; • przekazanie kompletnego raportu z przeprowadzonych testów; • usunięcie lub wyjaśnienie ewentualnych braków i niejasności w raporcie; • udzielenie, na żądanie Zamawiającego, wyjaśnień dotyczących wykrytych podatności i rekomendowanych działań naprawczych.
11	Termin wykonania	Do 15 listopada 2026 r.

