Opis Przedmiotu Zamówienia

Testy penetracyjne Systemu Monitorowania Jakości Internetu (SMJI) oraz e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS*

Urząd Komunikacji Elektronicznej

30 listopada 2022 r.

Spis treści

1. Definicje 2
2. Cel zamówienia 2
3. Wymagania w zakresie testów penetracyjnych 3
4. Przepisy i wymogi prawne 6

1. Definicje

Termin	Definicja
E-Usługa	E-usługa p.n. *Dostęp do bieżącej informacji o jakości usług IAS*, udostępniona w ramach realizacji projektu *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* realizowanego w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.
Projekt	Realizowany przez Zamawiającego projekt p.n. *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00
System, SMJI	System Monitorowania Jakości Internetu – oprogramowanie, urządzenia, usługi i baza danych realizujące cele, założenia i wymagania określone w Specyfikacji Warunków Zamówienia w ogłoszonym przez Zamawiającego postępowaniu o udzielenie zamówienia pod nr BA.WZP.26.21.2022[1].
Zamówienie Główne	Zamówienie udzielone przez Zamawiającego, którego przedmiotem jest zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu (SMJI) oraz wdrożenie e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS*, w ramach postępowania nr BA.WZP.26.21.2022.

2. Cel zamówienia

Zamówienie realizowane jest w ramach projektu p.n. *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.

Celem zamówienia jest realizacja założeń projektowych w zakresie bezpieczeństwa Systemu SMJI i E-Usługi, dotyczących sprawdzenia poziomu bezpieczeństwa poprzez realizację testów penetracyjnych.

Testy penetracyjne stanowią element weryfikacji w procesie wytwarzania oprogramowania oraz budowania rozwiązań dla realizacji Zamówienia Głównego. Ich celem jest zidentyfikowanie w Systemie oraz E-Usłudze, podatności umożliwiających naruszenie integralności, poufności i dostępności przetwarzanych danych.

Przedmiotem testów, jest System SMJI oraz E-Usługa zaprojektowane, zbudowane i wdrożone w ramach realizacji Zamówienia Głównego.

[1] Ogłoszenie o zamówieniu BA.WZP.26.21.2022 Zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu (SMJI), Biuletyn Informacji Publicznej Urzędu Komunikacji Elektronicznej, https://bip.uke.gov.pl/zamowienia-publiczne/ogloszenie-o-zamowieniu-ba-wzp-26-21-2022-zaprojektowanie-i-zbudowanie-systemu-monitorowania-jakosci-internetu-smji,691.html

3. Wymagania w zakresie testów penetracyjnych

WTP-1. Przy realizacji zamówienia, Wykonawca zobowiązany jest do współpracy z Wykonawcą Zamówienia Głównego.

WTP-2. Przedmiotem testów penetracyjnych będzie wydanie Systemu SMJI (wersja), które pozytywnie przeszło I fazę testów akceptacyjnych u Zamawiającego.

Termin realizacji testów

WTP-3. Testy penetracyjne zostaną zrealizowane w terminie przewidzianym w harmonogramie realizacji Zamówienia Głównego, odpowiadającym pierwszej fazie testów akceptacyjnych Systemu SMJI.

WTP-4. Zamawiający przewiduje realizację poszczególnych zadań testów penetracyjnych w szczegółowych terminach uzgodnionych przez Strony za porozumieniem z Wykonawcą Zamówienia Głównego w okresie od maja do czerwca 2023 r., przy czym Zamawiający oczekuje gotowości Wykonawcy do realizacji testów do 15 listopada 2023 r.

WTP-5. Ostateczny termin przeprowadzenia testów będzie zależny od terminu uzyskania pozytywnego wyniku I fazy testów akceptacyjnych Systemu SMJI przygotowywanego przez Wykonawcę Zamówienia Głównego. Harmonogram realizacji Zamówienia Głównego przewiduje realizację I fazy testów akceptacyjnych w okresie od 2 maja do 30 czerwca 2023 r.

WTP-6. Wykonawca w porozumieniu z Zamawiającym, biorąc pod uwagę poziom zaawansowania prac Wykonawcy Zamówienia Głównego, przygotuje w terminie nie krótszym niż 5 Dni Roboczych od dnia zawarcia Umowy i nie późniejszym niż 5 Dni Roboczych od planowanego rozpoczęcia testów penetracyjnych Systemu lub E-Usługi Plan Testów, zawierający w szczególności Harmonogram Szczegółowy.

WTP-7. Harmonogram Szczegółowy zawiera szczegółowy wykaz i terminy realizacji poszczególnych zadań Wykonawcy. Harmonogram Szczegółowy musi uwzględniać wymagania wskazane w OPZ.

Standardy do realizacji testów

WTP-8. W ramach realizacji testów penetracyjnych Wykonawca zobowiązany jest do zachowania następujących standardów testowania bezpieczeństwa:

1. Open Web Application Security Project (OWASP) Web Security Testing Guide, Application Security Verification Standard;
2. Open Source Security Testing Methodology Manual (OSSTMM);
3. Penetration Testing Execution Standard (PTES).

Zakres testów penetracyjnych

WTP-9. Testy penetracyjne dotyczą dwóch podstawowych obszarów:

1. Aplikacji,
2. Infrastruktury.

WTP-10. Testy penetracyjne aplikacji przeprowadzane będą w środowisku zbieżnym z produkcyjnym. Ich zadaniem jest zidentyfikowanie podatności możliwych do wykorzystania w trakcie użytkowania aplikacji.

WTP-11. Wykonawca zrealizuje testy penetracyjne aplikacji w dwóch modelach:

1. Grey-Box;

2. Black-Box.

WTP-12. W przypadku testów Grey-Box, Zamawiający przekaże Wykonawcy dokumentację projektową oraz dedykowane konta testowe użytkowników. Wykonawca będzie również uprawniony do pozyskiwania wiedzy od Zespołu Projektowego.

WTP-13. W przypadku testów Black-Box, Wykonawca dokona badania bezpieczeństwa Systemu i E-Usługi przy założeniu publicznego, zewnętrznego dostępu do Systemu i E-Usługi bez posiadania jakiegokolwiek konta użytkownika czy usługi w momencie rozpoczęcia testów.

WTP-14. Testy penetracyjne infrastruktury zostaną przeprowadzone w środowisku produkcyjnym lub w środowisku testowym replikującym konfigurację i mają na celu zweryfikowanie poprawności instalacji i konfiguracji mechanizmów bezpieczeństwa infrastruktury sprzętowo-programowej, w tym:

1. urządzeń sieciowych, serwerów oraz macierzy, systemów operacyjnych;
2. urządzeń pomiarowych: próbników sieciowych i próbników konsumenckich;
3. usług sieciowych, aplikacji serwerowych;
4. baz danych;
5. zewnętrznych komponentów bezpieczeństwa;
6. Zapór sieciowych, urządzeń HSM.

WTP-15. Testowanie będzie obejmować ryzyka występujące m. in. w następujących obszarach:

1. uwierzytelnianie;
2. zarządzanie sesją;
3. kontrola dostępu;
4. walidacja wejścia;
5. kryptografia;
6. obsługa błędów i logowanie;
7. ochrona danych;
8. bezpieczeństwo komunikacji;
9. wyszukiwanie złośliwego kodu;
10. logika biznesowa;
11. weryfikacja zasobów i plików.

WTP-16. Zamawiający dopuszcza wykorzystanie zidentyfikowanej podatności (exploit) tylko za wyraźną, wyrażoną na piśmie zgodą Zamawiającego pod warunkiem zapewnienia przez Wykonawcę pełnej kontroli nad zakresem wykorzystania podatności lub wyizolowania środowiska, na którym stosowane będzie wykorzystanie podatności (exploit).

Analiza bezpieczeństwa kodu

WTP-17. Wykonawca dokona automatycznej analizy bezpieczeństwa kodu Systemu SMJI (ang. *SAST – Static Application Security Testing*), mającej na celu zidentyfikowanie ewentualnych błędów związanych z konstrukcją kodu źródłowego, definiowaniem zmiennych, wywołaniami metod, użyciem poszczególnych funkcji.

WTP-18. Automatyczna analiza statyczna musi zostać przeprowadzona co najmniej w zakresie wystąpień wzorców wskazujących na prawdopodobieństwo wystąpienia błędu programistycznego jako Common Weakness Enumeration wg aktualnego na dzień

przedstawienia do odbioru (akceptacji Zamawiającego) planu testów zestawienia CWE/SANS TOP 25 Most Dangerous Software Weaknesses[2].

WTP-19. Swoim zakresem obejmuje cały kod Systemu SMJI.

WTP-20. Wykonawca Zamówienia Głównego zobowiązany jest do stosowania wykonywania automatycznej analizy statycznej kodu. W związku z tym, że analiza ta przeprowadzana jest przy wykorzystaniu dedykowanych narzędzi, niezbędne jest opracowanie reguł i szablonów określających sposób weryfikacji dla zastosowanych języków programowania. Zadaniem wykonawcy będzie weryfikacja reguł stosowanych przez Wykonawcę Zamówienia Głównego.

WTP-21. Do przeprowadzenia automatycznej analizy bezpieczeństwa kodu Wykonawca może wykorzystać reguły stosowane przez Wykonawcę Zamówienia Głównego, jeżeli w wyniku ich weryfikacji, Wykonawca wykaże iż spełniają one wymagania Zamawiającego.

WTP-22. Wykonawca w ramach współpracy z Wykonawcą Zamówienia Głównego dokona przeglądu manualnego kodu. Raport z przeglądu zawierający między innymi listę zidentyfikowanych błędów lub podatności, poziom ich krytyczności oraz rekomendacje związane ze sposobem ich usunięcia Wykonawca uwzględni w procesie przygotowania i prowadzenia testów penetracyjnych.

Przebieg testów i raport

WTP-23. Proces testowania musi zapewnić, że każdorazowe badanie z uwzględnieniem metodyki zawartej w normach branżowych, będzie składało się z następujących, wyróżnionych etapów:

1. przeprowadzenie badań i testów;
2. opracowanie oceny eksperckiej;
3. przedstawienie wiążącego stanowiska;
4. przedstawienie rekomendacji zmian.

WTP-24. W wyniku testów penetracyjnych, Wykonawca opracuje raport zawierający co najmniej:

1. opis wszystkich elementów, które zostały poddane testom w ramach zakresu;
2. przyjęte kryteria oceny ryzyka na podstawie prawdopodobieństwa wykorzystania i wpływu wykrytej podatności;
3. podział podatności ze względu na ryzyko, wpływ wykrytej podatności na poufność, integralność i dostępność informacji (poziom krytyczności), prawdopodobieństwo wykorzystania podatności, złożoność (trudność) wprowadzenia naprawy – usunięcia podatności;
4. listę oraz szczegółowy opis zidentyfikowanych błędów i podatności zawierający:
    i. poziom ryzyka,
    ii. poziom krytyczności,
    iii. prawdopodobieństwo wykorzystania podatności,
    iv. złożoność wprowadzenia naprawy,
    v. klasyfikację CWE,
    vi. wektor oceny CVSS,
    vii. sposób, w jaki została wykryta podatność oraz szczegółowe kroki do odtworzenia procesu, pozwalające Zamawiającemu na odtworzenie dojścia do podatności,

[2] https://cwe.mitre.org/top25/

viii. dowody wystąpienia podatności (tzw. Proof of Concept, PoC);

5. rekomendacje związane ze sposobem usunięcia podatności;
6. podsumowanie zarządcze testu.

WTP-25. Testy penetracyjne muszą zostać wykonane przez zespół testowy Wykonawcy, przygotowujący i realizujący testy penetracyjne, przy czym co najmniej dwóch członków tego zespołu musi posiadać wiedzę i doświadczenie poparte co najmniej jednym z niżej wymienionych certyfikatów:

1. Offensive Security Certified Professional (OSCP);
2. Certified Ethical Hacker (CEH);
3. CompTIA Pentest+;
4. Certified Information Systems Auditor (CISA);
5. GIAC Penetration Tester (GPEN);
6. Certified Information Systems Security Professional (CISSP).

Zamawiający dopuszcza certyfikaty równoważne do wymienionych powyżej, przy czym za certyfikat równoważny uważany będzie certyfikat potwierdzający zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana przez Wykonawcę. Wykonawca, który powołuje się na certyfikaty równoważne jest zobowiązany wykazać, że wskazywane przez niego certyfikaty potwierdzają zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana.

4. Przepisy i wymogi prawne

Wykonawca jest zobowiązany do zapewnienia zgodności przedmiotu zamówienia z przepisami prawa obowiązującymi na terytorium Polski w dniu przekazania przedmiotu zamówienia do Odbioru Końcowego.