Warszawa, 2025-09-26

ZPPZ.230.1.2025

(208734)

Do wszystkich Wykonawców

dotyczy: **Zapytania w celu ustalenia szacunkowej wartości zamówienia** pn.: **„Zakup licencji oprogramowania do przeprowadzania zautomatyzowanych testów penetracyjnych i badań bezpieczeństwa aplikacji webowych oraz infrastruktury wewnętrznej."** Identyfikator CeZ: 207224.

Z uwagi na fakt, iż do przedmiotowego **Zapytania** wpłynęły pytania od Wykonawców, Zamawiający przytacza treść pytań i udziela odpowiedzi.

Pytanie 1.

Szczegółowy opis funkcjonalności oprogramowania w zakresie testowania wyszczególniony w punkcie 4.3 OPZ można podzielić na pięć głównych grup:

I. Testowanie aplikacji webowych.

II. Skanowanie hostów pod względem weryfikacji aktualności oprogramowania oraz identyfikacji znanych podatności (CVE) przypisanych do analizowanych komponentów.

III. Ocena mechanizmów kryptograficznych – analiza implementacji szyfrowania, weryfikacji siły algorytmów kryptograficznych oraz prawidłowość zarzadzania kluczami.

IV. Testowanie infrastruktury wewnętrznej – weryfikacja bezpieczeństwa usług.

V. Zdolność narzędzia do symulowania zaawansowanych technik ataków przez grupy APT zgodnie z matrycą MITRE ATT&CK.

W związku z tym zwracamy się do Państwa na następującymi pytaniami:

1. Które z wyszczególnionych funkcjonalności uważane są za krytyczne (must-have) — a które są opcjonalne (nice-to-have)?

Odpowiedź 1.

Zamawiający wymaga wszystkich wskazanych funkcjonalności (must-have).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37 NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Pytanie 2.

Czy narzędzie musi działać całkowicie offline / bez dostępu do Internetu (w izolowanym środowisku)? Chodzi o doprecyzowanie czy aktualizacje / synchronizacja sygnatur muszą być ręczne czy mogą być realizowane online.

Odpowiedź 2.

Aktualizacje mogą być online, wszystkie testy muszą być realizowane bez dostępu do internetu.

Pytanie 3.

Jak bardzo zaawansowane muszą być testy aplikacji WEB / API?

a) **Czy wymagane są wszystkie warianty np. SQLi, XSS (reflected, stored, DOM), CSRF, XML injection, LDAP injection, Command injection?**

b) **Czy wymagany jest tryu proxy z manipulacją żądań i odpowiedzi (man-in-the-middle) czy wystarczy skanowanie i ataki end-to-end?**

c) **Czy ma być pełne wsparcie testów dla API (REST / SOAP) i OWASP API Top10?**

Odpowiedź 3.

a) Wszystkie są wymagane;

b) Tryb proxy jest wymagany;

c) Tak.

Pytanie 4.

Czy wymagana jest funkcjonalność „proof-of-exploit" / walidacji wykrytych podatności („potwierdzenie, że dana luka jest realnie eksploatowalna") czy jedynie raportowanie o występowaniu potencjalnych luk.

Odpowiedź 4.

Tak.

(-) Anna Bułhak

podpis

Osoba sporządzająca: Marika Czarnecka

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37 NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl REGON: 001377706