Grodzisk Mazowiecki, 02.06.2021

DOT: Pytania do postępowania pn. Wykonanie testów bezpieczeństwa i rekontrola systemu informatycznego (ID 464157)

ZESTAW I

Pytanie nr 1

Do czego służy aplikacja? Jakie funkcje udostępnia?

Odpowiedź:

Aplikacja o nazwie eBOK , służy do prezentacji informacji związanych z rozliczeniami pomiędzy ZWiK a klientami oraz daje możliwość składania różnego rodzaju wniosków

Pytanie nr 2

Jak rozbudowana jest aplikacja (szacunkowa liczba unikalnych ekranów/formularzy, np. do 10, 50, 100, etc)?

Odpowiedź:

Zamawiający informuje, iż szacunkowa liczna wynosi ok 20.

Pytanie nr 3

Ile różnych grup użytkowników (o różnych uprawnieniach) posiada aplikacja i ile spośród nich musi zostać objętych audytem (rekomendujemy testy max. 3-4 grup)?

Odpowiedź:

Jedna grupa

Pytanie nr 4

Ile endpointów/metod API wykorzystuje aplikacja (np. 10 endpointów/metod dla REST API, 10 operacji/metod w ramach 2 usług SOAP)? Pytanie odnosi się do tych metod i endpointów, które dostępne są bezpośrednio z poziomu aplikacji (nie należy wliczać metod/endpointów wewnętrznych, do których nie można odwołać się w bezpośredni sposób).

Odpowiedź:

Brak endpointów.

Pytanie 5

Czy aplikacja współdzieli backend (np. API) z innymi aplikacjami (np. z aplikacją mobilną)?

Odpowiedź:

Nie

Pytanie nr 6

W jakiej technologii wykonany jest system?

Odpowiedź:

Zamawiający nie posiada wiedzy i testy mają by realizowane bez wiedzy w tym temacie

Pytanie nr 7

W miarę możliwości proszę o przesłanie 2-3 zrzutów ekranowych z aplikacji.

Odpowiedź:

Zrzuty ekranu stanowią załącznik do pisma.

Pytanie nr 8

Czy zależy Państwu na testach ręcznych (bardziej dokładne, badające logikę aplikacji) czy tylko automatycznych?

Odpowiedź:

Test manualne, typu gray-box, bez dostępu do kodów źródłowych, na środowisku produkcyjnym.

Pytanie nr 9

Jeśli audyt systemu ma obejmować audyt infrastruktury typu whitebox (analiza konfiguracji) proszę o podanie informacji jakie elementy miałyby zostać poddane testom – serwer HTTP (ile, jakie), baza danych (ile, jakie), system operacyjny (ile, jakie), np. 2 x Debian, 1 x PostgreSQL, 3 x Apache HTTPD

Odpowiedź:

Zamawiający udzielił odpowiedzi w pytaniu nr 8

Pytanie nr 10

Czy możliwe są testy zdalne (np. z wykorzystaniem tunelu VPN)?

Odpowiedź:

Zamawiający wymaga by testy odbyłaby się tylko zdalnie

Pytanie nr 11

Na jakim środowisku będzie przeprowadzany audyt (testowe/produkcyjne)?

Odpowiedź:

Środowisko produkcyjne

Pytanie nr 12

Czy są jakieś ograniczenia czasowe w trybie przeprowadzania audytu (np. godziny nocne, etc.)?

Odpowiedź:

Audyt powinien być przeprowadzany w godzinach pracy tj. 7:30-15:30

Pytanie nr 13.

Jaki jest pożądany termin wykonania audytu?

Odpowiedź:

7 tygodni od dnia podpisania umowy

Pytanie nr 14

Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)?

Odpowiedź:

Tak, zgodnie z projektem umowy, która stanowi załącznik do postępowania

Pytanie nr 15

W jaki sposób zrealizowane jest uwierzytelnianie do aplikacji (standardowa para login i hasło, certyfikaty, tokeny 2FA, etc)?

Odpowiedź:

Login hasło + możliwość logowania przez Węzeł Krajowy

Pytanie nr 16

Czy aplikacja wykorzystuje dodatkowe metody autoryzacji wrażliwych operacji (np. przy pomocy kodów SMS, tokenów sprzętowych, tokenów mobilnych, certyfikatów kwalifikowanych, etc)?

Odpowiedź:

Nie

Pytanie nr 17

Czy aplikacja zawiera funkcje znane z systemów ecommerce (np. integracja z bramką płatności, funkcja kodów rabatowych, pobieranie faktur, etc)?

Odpowiedź:
Z systemu backoffice pobierany jest skan umowy oraz realizowana jest wymiana danych
Pytanie nr 18
Czy istnieje możliwość uzyskania dostępu do aplikacji przed złożeniem oferty (np. do wersji demo)?
Odpowiedź:
Nie