Warszawa, dnia 08.10.2020 r.

Dotyczy postępowania nr IBE/244/2020

PYTANIA I ODPOWIEDZI – ZESTAW NR 1

W związku z pytaniami, które wpłynęły do Zamawiajacego od uczestników postępowania poniżej zamieszczamy ich treść wraz z odpowiedziami

Zestaw odpowiedzi nr 1

Treść zapytania:

Uprzejmie prosimy o odpowiedź na pytania.

Schematora – narzędzia przeznaczonego do tworzenia schematów walidacji;

1. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).

2. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).

3. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).

4. Lista / Orientacyjna liczba stron / podstron.

5. Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.

6. Orientacyjna liczba pól we wszystkich formularzach.

7. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.

E-Asesora - narzędzia przeznaczonego do tworzenia arkuszy oceny kandydatów dopasowanych do różnych metod walidacji oraz do wypełniania gotowych arkuszy, zatwierdzonych w danej walidacji;

1. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).

2. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).

3. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).

4. Lista / Orientacyjna liczba stron / podstron.

5. Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.

6. Orientacyjna liczba pól we wszystkich formularzach.

7. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.

Menedżera Walidacji – narzędzia przeznaczonego do kompleksowego zarządzania walidacją zarówno po stronie instytucji, jak i kandydata.

1. Lista metod logowania i uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms).

2. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token, kod sms, urządzenia HSM (Hardware Security Module)).

3. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników).

4. Lista / Orientacyjna liczba stron / podstron.

5. Lista / Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych.

6. Orientacyjna liczba pól we wszystkich formularzach.

7. Szacunkowa (orientacyjna) liczba wszystkich używanych zmiennych (GET, POST, nagłówków - z uwzględnieniem ew. zmiennych przyjmowanych np. przez elementy Flash - jeśli występują) w całym testowanym systemie. Chodzi o sumaryczną / całkowitą liczę parametrów w całej aplikacji, która ma być przedmiotem testów.

Integracja

8. Czy zakres prac obejmuje testy interfejsów z innymi narzędziami webowymi: Bazą Efektów Uczenia się (BEU) powiązaną z zasobami Zintegrowanego Rejestru Kwalifikacji (ZRK), oraz „Moim Portfolio" (MP) – aplikacją służącą m.in. do gromadzenia dowodów w cyfrowym portfolio oraz udostępniania ich zainteresowanym osobom z Instytucji Certyfikujących?

Testy infrastruktury

9. Prosimy o specyfikację komponentów infrastruktury, które mają być objęte testami:

   a. Nazwa komponentu

   b. Producent

c. Wersja

d. Liczba komponentów

Testy konfiguracji serwerów

10. Prosimy o specyfikację serwerów, które mają być objęte testami:

a. Producent

b. Wersja

c. Liczba komponentów

Odpowiedź:

Ad. 1. Elementy składowe aplikacji „Moja Walidacja" tj. Schemator, E-Asesor i Menedżer Walidacji stanowią jedną całość, która ma jeden wspólny mechanizm logowania oparty o hasło.

Ad. 2. Elementy składowe aplikacji „Moja Walidacja" tj. Schemator, E-Asesor i Menedżer Walidacji stanowią jedną całość, która ma jeden wspólny mechanizm autoryzacji operacji oparty o pliki cookies.

Ad. 3. W aplikacji „Moja Walidacja" przewidziane są następujące role, które mają różne poziomy dostępu do narzędzi Schemator, E-Asesor i Menedżer Walidacji:

1. Administrator główny – ma dostęp do wszystkiego
2. Administrator CMS - ma dostęp do: Schematora, E-Asesora i Menedżera Walidacji
3. Administrator IC - ma dostęp do: Menedżera Walidacji
4. Zwykły użytkownik - ma dostęp do: Menedżera Walidacji
5. Główny Asesor - ma dostęp do: E-Asesora i Menedżera Walidacji
6. Asesor – ma dostęp do: E-Asesora i Menedżera Walidacji
7. Doradca - ma dostęp do: E-Asesora i Menedżera Walidacji
8. Ekspert ds. Walidacji - ma dostęp do: Schematora, E-Asesora i Menedżera Walidacji
9. Koordynator - ma dostęp do: Schematora, E-Asesora i Menedżera Walidacji
10. Dodatkowo istnieje rola dla użytkownika API.

Ad. 4, 5 i 6. Ze względu na zintegrowanie poszczególnych elementów aplikacji tj. Schematora, E-Asesora i Menedżera Walidacji oraz fakt, że prace rozwojowe nad nimi jeszcze trwają, możemy podać tylko szacunkowe wartości dla tych parametrów. Dla całej aplikacji mamy około 100 - 150 ekranów oraz około 50 endpointów. Ponieważ funkcjonalności E-Asesora i Menedżera Walidacji obejmują ok. 40% funkcjonalności całej aplikacji, a Schematora – ok. 20%, ponadto około 80% ekranów służy do wprowadzania danych, w liczbie ok. 5 wartości to:

Podpunkt zapytania	Parametr	Schemator	E-Asesor	Menedżera Walidacji
4	Orientacyjna liczba stron / podstron	20-30	40-60	40-60

5	Orientacyjna liczba formularzy (podstron, na której użytkownik może wprowadzać dane np. strona logowania, formularz kontaktowy, składanie zamówień itp.) dynamicznie generowanych	16-24	32-48	32-48
6	Orientacyjna liczba pól we wszystkich formularzach	80-120	160-240	160-240

Ad. 7. Zamawiający nie może udostępnić tak szczegółowych informacji. Zostanie to uzgodnione z Wykonawcą na etapie planowania koncepcji testów.

Ad. 8. Tak, Zamawiający przewiduje, że testy obejmą też aplikacje „Moje Portfolio" oraz „Baza Efektów Uczenia się". Tak jak napisano w OPZ – "Ostateczny zakres testów Wykonawca ustali we współpracy z Zamawiającym na etapie przygotowania koncepcji i planów testów bezpieczeństwa."

Ad. 9. Testy infrastruktury

Zamawiający zamierza poddać testom bezpieczeństwa infrastrukturę obejmującą jeden serwer o następującej specyfikacji: Debian, Apache, bazy danych MySQL lub MariaDB.

Co do pytania o wersję i liczbę komponentów, które mają zostać poddane testom, to zapis w podpunkcie 3.2. OPZ (patrz: Opis Przedmiotu Zamówienia - załącznik nr 2, str. 4) stwierdza, że moduł testów penetracyjnych infrastruktury informatycznej, na której wdrożono aplikację „Moja Walidacja" ma obejmować:

"- sprawdzenie rodzaju, wersji oraz konfiguracji wykorzystywanego oprogramowania systemowego i usługowego". Tym samym to Wykonawca zamówienia powinien sprawdzić rodzaj, wersję i konfigurację serwera, oraz czy jest podatna na ataki.

Ad. 10. Testy konfiguracji serwerów

Patrz odpowiedź na pytanie 9.

Zestaw odpowiedzi nr 2

Zapytanie:

W punkcie 3 c załącznika 1 mowa jest o certyfikatach, których posiadanie przez Eksperta/Zespół Ekspertów jest wymagane. Czy dobrze rozumiem, że do postępowania może być dopuszczony jedynie Zespół Ekspertów, którego członkowie posiadają co najmniej jeden z poniższych certyfikatów: CISA, CISM, CISSP oraz jeden z następujących certyfikatów: OSCE lub OSCP?

Odpowiedź:

Nie, do postępowania może być dopuszczony jedynie Zespół Ekspertów, którego członkowie łącznie posiadają certyfikaty: CISA, CISM, CISSP oraz jeden z następujących certyfikatów: OSCE lub OSCP lub równoważne.

Inaczej mówiąc w zespole musi być przynajmniej:
- 1 osoba, która będzie miała CISA lub równoważny
- 1 osoba, która będzie miała CISM lub równoważny
- 1 osoba, która będzie miała CISSP lub równoważny
- 1 osoba, która będzie miała OSCE lub OSCP lub równoważny.

Zamówienie może wykonać także:
- Podmiot, który dysponuje Ekspertem/zespołem ekspertów tj. osobami zdolnymi do wykonania zamówienia, posiadającymi łącznie ww. certyfikaty,
- 1 osoba, która dysponuje wszystkimi 4 certyfikatami.

Zestaw odpowiedzi nr 3

Zapytanie:

1. W treści ogłoszenia pkt 3c, wskazane jest wymaganie posiadania certyfikatów CISA, CISM, CISSP oraz OSCP lub OSCE. Żaden z tych certyfikatów nie poświadcza wiedzy i umiejętności potrzebnej do wykonania większej części prac dot. przedmiotu zamówienia tj. testów bezpieczeństwa aplikacji webowych. W związku tym prosimy o zmianę wskazanej listy certyfikatów na takie, które mają znaczenie, po jednym dla każdego obszaru kompetencji np. eWAPT oraz GWAPT dla testów aplikacji webowych; GPEN, GXPN, OSCP, OSCE dla testów infrastruktury. Prosimy również o dopuszczenie akceptacji innych równoważnych certyfikatów.
2. W opisie przedmiotu zamówienia wskazane jest, że testy mają być zrealizowane w oparciu o metodykę OWASP ASVS 3.0. Prosimy o aktualizację wersji standardu (obecna wersja to 4.0.1) oraz wskazanie oczekiwanego poziomu weryfikacji. Poziom weryfikacji wpływa bezpośrednio na pracochłonność zadania, przy czym jedyny poziom ograniczony do technik penetracyjnych to poziom najniższy czyli "Level 1".
3. Czy istnieje możliwość przekazania dodatkowych informacji nt. systemu? Właściwe zwymiarowanie prac wymaga m.in. informacji o liczbie hostów, adresów IP, stron formularzy itp. - jeśli jest taka możliwość, to przekażemy Państwu szczegółową listę pytań.

Odpowiedź:

Ad.1. Zamawiający wskazał certyfikaty CISA, CISM i CISSP jako wystarczające potwierdzenie doświadczenia i kompetencji w zakresie szeroko rozumianego bezpieczeństwa informatycznego. Ponieważ oferta certyfikatów na rynku usług bezpieczeństwa IT jest obecnie bardzo szeroka, a jakość tych szkoleń różna - Zamawiający dopuszcza posiadanie innych certyfikatów. Jednak by zapewnić sobie odpowiednią jakość usługi wymagamy, by certyfikat ten znajdował się na uznanej liście czołowych certyfikatów w branży, np.:
https://builtin.com/cybersecurity/penetration-testing-certification
https://resources.infosecinstitute.com/top-5-penetration-testing-certifications-security-professionals/
https://alpinesecurity.com/blog/top-penetration-testing-certifications/.
Przy czym Oferent zobowiązany powinien wykazać, że jego certyfikat jest na tej liście (np. załączając wydruk strony rankingu).

Ad.2. Zamawiający wskazał wersję OWASP ASVS 3.0 jako referencyjną, niemniej jednak informację tą należy interpretować jako „wersja ASVS **nie niższa niż v3.0**". Zakładamy, że poziom weryfikacji L2 będzie optymalny ze względu na dane wrażliwe pochodzące od instytucji certyfikujących i pozostałych użytkowników systemu. Zostanie to uzgodnione z Wykonawcą na etapie planowania koncepcji testów.

Ad. 3. Dodatkowe informacje o aplikacji, nie objęte OPZ (patrz: Opis Przedmiotu Zamówienia - załącznik nr 2) można znaleźć w Zestawie odpowiedzi nr 1. Liczba hostów i adresów IP objętych testami zostanie uzgodniona na etapie planowania testów.

Zestaw odpowiedzi nr 3

Zapytanie:
Czy Zamawiający uzna certyfikat CEH za równoważny do certyfikatu OSCE lub OSCP?

Odpowiedź:

Tak, certyfikat CEH znajduje się na liście czołowych certyfikatów, które Zamawiający dopuścił jako równoważne.
https://alpinesecurity.com/blog/top-penetration-testing-certifications/