Warszawa, dnia 23.07.2021 r.

Dotyczy postępowania nr: IBE/189/2021

PYTANIA I ODPOWIEDZI – ZESTAW NR 1

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

Pytanie nr 1

Czy zamawiający dopuszcza możliwość negocjacji treści zapisów umowy i jej załączników po złożeniu oferty i przed podpisaniem dokumentów? Z naszej perspektywy, analiza umowy oraz negocjacja jej zapisów jest niezbędnym krokiem w celu możliwości realizacji usług.

Opowiedź do pytania nr 1

Zamawiający informuje, iż jest w trakcie modyfikacji zapisów umowy i w najbliższym czasie opublikuje zmieniony wzór umowy. W związku z powyższym Zamawiający dokonuje przedłużenia terminu składania ofert do dnia **30.07.2021 r.**

Pytanie nr 2

Jaki jest cel prowadzenia testów penetracyjnych?

1. Identyfikacja podatności ukierunkowana na wykrycie możliwie wielu różnych typów podatności (najczęściej wybierane podejście).
2. Identyfikacja podatności ukierunkowana na wykrycie przede wszystkim podatności o najwyższych poziomach ryzyka. W podejściu tym z uwagi na skupienie się na najistotniejszych podatnościach, podatności o niskim poziomie ryzyka mogą zostać niewykryte.
3. Identyfikacja podatności ukierunkowana na wykrycie przede wszystkim podatności dotyczących wskazanych ryzyk (np. nieautoryzowany dostęp do danych). Prosimy o wskazanie na jakich ryzykach powinien skupić się test.

Opowiedź do pytania nr 2

Zgodnie z rozdziałem "Przedmiot zamówienia" zawartym w OPZ, celem realizowanego zamówienia jest zapewnienie wysokiego poziomu bezpieczeństwa aplikacji objętych testami, które będą odporne na ataki. W związku z tym identyfikacja podatności musi być ukierunkowana na wykrycie możliwie wielu różnych typów podatności. Zamawiający skłania się jednak do pkt 1 choć niewątpliwie wykrycie podatności krytycznych jest priorytetem.

Pytanie nr 3

Jakie jest oczekiwane miejsce przeprowadzenia prac oraz sposób dostępu do aplikacji będących przedmiotami testów? Prosimy o wybór spośród poniższych:

1. Zdalny dostęp do aplikacji w bezpośrednim połączeniu z sieci Internet
2. Zdalny dostęp do aplikacji udostępnionej poprzez tunel VPN zestawiony do Państwa siedziby
3. Zdalny dostęp do aplikacji udostępnionej poprzez tunel VPN zestawiony do zewnętrznego operatora hostingu
4. Lokalny bezpośredni dostęp do aplikacji
5. Lokalny dostęp do aplikacji przez tunel VPN

Prosimy o wskazanie, czy uzyskanie dostępu do aplikacji wymaga korzystania ze stacji przesiadkowej.

Opowiedź do pytania nr 3

Pkt. 1+2+3. Zamawiający nie wymaga dostępu do stacji przesiadkowej. Część aplikacji jest w chmurze a część będzie lokalnie, więc część będzie miało dostęp zwykły przez internet a część jak np. strona backendowa przez VPN.

Pytanie nr 4

Czy oczekiwane jest powtórzenie testów poprzez zweryfikowanie zidentyfikowanych podatności na jednym ze środowisk w innym środowisku? Przykładowo, czy podatności wykryte w ramach testów na środowisku testowym muszą być dodatkowo zweryfikowane na środowisku produkcyjnym?

Opowiedź do pytania nr 4

Nie, nie jest oczekiwane.

Pytanie nr 5

Prosimy o potwierdzenie naszego zrozumienia, czy wszystkie 7 aplikacji w zakresie prac będzie aplikacjami internetowymi, wymagającymi do pracy wyłącznie przeglądarki internetowej? Prosimy o informację w przypadku innego typu aplikacji i/lub potrzeby instalacji dodatkowego oprogramowania w celu ich obsługi (np. dodatku do przeglądarki internetowej, klienta oprogramowania Java itp.).

Opowiedź do pytania nr 5

Tak, potwierdzamy.

Pytanie nr 6

Prosimy o potwierdzenie naszego zrozumienia, czy w ramach testów penetracyjnych w podejściu ""white-box"" zamawiający oczekuje realizacji następujących obszarów prac dla każdej z 7 aplikacji:

1. - test penetracyjny aplikacji
2. - przegląd kodu źródłowego aplikacji
3. - przegląd konfiguracji oprogramowania infrastruktury wspierającej pracę aplikacji w zakresie serwera aplikacyjnego, serwera bazodanowego i systemu operacyjnego serwera
4. - analiza dostępu fizycznego i logicznego do serwerów aplikacji oraz mechanizmów archiwizacji danych aplikacji
5. - testy podatności infrastruktury wspierającej pracę aplikacji
6. - retest
7. - inny, jaki?

Opowiedź do pytania nr 6

Pkt. 1 – tak (zgodnie z rozdziałem "Zakres prac" zawartym w OPZ)
Pkt. 2 – tak, ale w celu wskazania nieoczywistych furtek bezpieczeństwa i pomocy testerom w pracy
Pkt. 3 - tak (zgodnie z rozdziałem "Zakres prac" zawartym w OPZ)
Pkt. 4 – z wyłączeniem dostępu fizycznego
Pkt. 5 – nie, za wyjątkiem prac określonych w pkt. 3
Pkt. 6 – tak, jednakże jest to uwzględnione w kryterium oceny ofert jako dodatek do oferty

Pytanie nr 7

Prosimy o potwierdzenie naszego zrozumienia, czy test penetracyjny z perspektywy administratora aplikacji jest poza zakresem w przypadku, jeżeli administracja tej aplikacji występuje wyłącznie za pośrednictwem zewnętrznego systemu? Pytanie dotyczy przykładowo aplikacji "Miasto Karier", której administracja zgodnie z opisem zapytania ofertowego będzie możliwa wyłącznie poprzez zewnętrzny system CAS.

Opowiedź do pytania nr 7

System CAS służy tylko do autoryzacji użytkowników a nie do administracji innymi aplikacjami.

Pytanie nr 8

Czy prace mają zostać przeprowadzone wyłącznie w warstwie technicznej (testy penetracyjne i podatności, przeglądy kodu i konfiguracji), czy również w warstwie procesowej (np. dla analizy dostępu fizycznego i logicznego do serwerów oraz mechanizmów archiwizacji danych)?

Opowiedź do pytania nr 8

Tylko warstwa techniczna.

Pytanie nr 9

Czy w ramach testów każdej z aplikacji, wykonany ma być zewnętrzny test podatności infrastruktury wspierającej testowaną aplikację? Test zewnętrzny oznacza test wykonany z perspektywy użytkownika systemu (zewnętrznego lub/i wewnętrznego).

Opowiedź do pytania nr 9

Nie.

Pytanie nr 10

Czy w ramach testów każdej z aplikacji, wykonany ma być wewnętrzny test podatności infrastruktury wspierającej testowaną aplikację? Test wewnętrzny oznacza test wykonany z sieci wewnętrznej do której podłączony jest bezpośrednio serwer WWW oraz inne elementy infrastruktury go wspierającej.

Opowiedź do pytania nr 10

Nie.

Pytanie nr 11

Czy testy podatności infrastruktury wspierającej każdą z testowanych aplikacji, mają być wykonane bez uwierzytelniania w docelowych hostach, czy z uwierzytelnianiem?

Opowiedź do pytania nr 11

Ze względu na negatywną odpowiedź na pkt 9 i 10 odpowiedź na to pytanie również jest negatywna.

Pytanie nr 12

Jaki jest dopuszczalny sposób przeprowadzenia przeglądu konfiguracji? Prosimy o wskazanie z poniższych:

1. Uruchomienie przez administratorów systemów dostarczonych przez nas autorskich skryptów i oprogramowania na hostach będących w zakresie prac (w większości przypadków wymaga to uruchomienia skryptów i oprogramowania z uprawnieniami administratora).
2. Przegląd konfiguracji z wykorzystaniem automatycznych narzędzi sieciowych (wymaga to zapewnienia dostępu sieciowego z naszego narzędzia do hostów, udostępnienia nam danych uwierzytelniających do hostów z uprawnieniami administratora, a także w niektórych przypadkach zmiana konfiguracji hostów, pozwalająca na działanie narzędzia - silnika skanującego).
3. Przegląd manualny konfiguracji w asyście administratora systemu.
4. Inny - jaki?

Prosimy również o wskazanie, który z powyższych dopuszczalnych sposobów jest przez Państwa preferowany.

Opowiedź do pytania nr 12

Pkt 1 z zastrzeżeniem, że uruchomienie skryptów wymaga każdorazowej zgody Zamawiającego.

Pytanie nr 13

Czy przegląd konfiguracji powinien być wykonany ściśle i wyłącznie w odniesieniu do wymagań weryfikacyjnych danego standardu lub wytycznych? Jeśli tak, prosimy o wskazanie nazwy standardu/wytycznych oraz poziomu weryfikacji jeśli został on rozróżniony w danym opracowaniu. W przeciwnym wypadku, przegląd konfiguracji obejmować będzie weryfikację względem najlepszych dobrych praktyk, zgodnie z autorską metodyką wykonawcy.

Opowiedź do pytania nr 13

Zamawiający zgadza się na wykorzystanie dobrych praktyk zgodnie z autorską metodyką Wykonawcy.

Pytanie nr 14

Jaka jest szacunkowa liczba statycznych / dynamicznych ekranów i formularzy w aplikacjach objętych testami uwzględniając wszystkie testowane role (profile uprawnień)?

Opowiedź do pytania nr 14

Ze względu na brak 5 z 7 testowanych aplikacji Zamawiający może odpowiedzieć na podstawie aplikacji „CAS" oraz „Kompas": nie więcej niż 20 dla CAS i nie więcej niż 15 dla „Kompas".

Pytanie nr 15

Jaki jest sposób uwierzytelniania użytkowników dla każdej z aplikacji w zakresie prac (np. logowanie poprzez formularz HTML na stronie aplikacji, logowanie poprzez formularz HTML na stronie zewnętrznego dostawcy tożsamości, uwierzytelnienie certyfikatem klienckim w połączeniu TLS, inny)?

Opowiedź do pytania nr 15

Logowanie do aplikacji odbywa się głównie przez zewnętrzny system autoryzacji CAS zainstalowany na serwerze w chmurze.

Pytanie nr 16

W jakim środowisku wykonywane będą testy aplikacji? Prosimy o wybór spośród następujących: 1) Produkcyjne, 2) Przedprodukcyjne, 3) UAT, 4) Deweloperskie, 5) Inne

Opowiedź do pytania nr 16

W środowiskach przedprodukcyjnych.

Pytanie nr 17

Czy prace będą prowadzone na urządzeniach wykonawcy, czy zostaną one przekazane przez zamawiającego test?

Opowiedź do pytania nr 17

Pytanie jest niezrozumiałe dla Zamawiającego.

Pytanie nr 18
Dla każdej z aplikacji w zakresie prac, jaki jest rozmiar kodu źródłowego aplikacji produkcyjnych (czyli bez kodów testowych) w poszczególnych technologiach (językach programowania) w tysiącach linii kodu (KLOC)? W przypadku aplikacji które zostaną wdrożone w późniejszym terminie, prosimy o oszacowanie spodziewanego rozmiaru ich kodu źródłowego (np. do 50 tysięcy linii kodu, do 100 tysięcy linii kodu itp.).

Opowiedź do pytania nr 18

Zamawiający nie jest w stanie oszacować ilości linijek kodu każdej niewytworzonej aplikacji. W przypadku jednak istniejących jest to liczba rzędu około 10 tyś linijek dla każdej.

Jednak zgodnie z odpowiedzią na pkt 6 podpunkt 2 Zamawiający nie będzie oczekiwał weryfikacji każdego pliku kodu a mają one służyć jako wykrycie nieoczywistych furtek bezpieczeństwa i wspierać pracę testerów.

Pytanie nr 19

Czy są w aplikacji wykorzystywane są biblioteki stron trzecich (np. odpowiadające za kryptografię albo interfejs użytkownika)? Jeżeli tak, jaka jest przybliżona liczba bibliotek zewnętrznych (open source lub komercyjnych) używanych przez poszczególne aplikacje?

Opowiedź do pytania nr 19

Tak wykorzystywane są biblioteki stron trzecich odpowiadające za kryptografię albo interfejs użytkownika. Nie jesteśmy w stanie określić liczby bibliotek.

Pytanie nr 20

W jakim języku jest udokumentowany i napisany kod źródłowy aplikacji w zakresie prac?

Opowiedź do pytania nr 20

Zamawiający może udzielić odpowiedzi tylko dla aplikacji CAS i Kompas. Aplikacje, które istnieją wykorzystują framework laravel/angular. Języki z których korzystają to m.in.: PHP, javascript, Python.

Pytanie nr 21
Kiedy najwcześniej może nastąpić rozpoczęcie prac w zakresie testów?

Opowiedź do pytania nr 21

Zgodnie z rozdziałem "sposób realizacji zamówienia" zawartym w Opisie Przedmiotu Zamówienia.

Pytanie nr 22

Kto, oprócz Instytut Badań Edukacyjnych, będzie beneficjenetem rezultatów naszych prac? Prosimy o wskazanie pełnych nazw Spółek.

Opowiedź do pytania nr 22

Zgodnie z wzorem umowy dołączonym do ogłoszenia Wykonawca przenosi całość praw majątkowych do utworu, a Zamawiający ma prawo do rozpowszechniania utworu.

Pytanie nr 23

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

Opowiedź do pytania nr 23

- CAS: między 10-15

- Miasto karier: szacunkowo 10-15

- Aplikacja „Małe ZRK": szacunkowo 10-15

- Kompas: między 10-15

- Narzędzie do automatycznego wspomagania doradztwa: brak informacji, będzie to jednak czatbot w ramach kwalifikacje.gov.pl

- Aplikacja dla uprzywilejowanych użytkowników ułatwiająca opisywanie kwalifikacji i przypisywanie im poziomu PRK: : brak informacji

- Narzędzie ułatwiające tworzenie odwołań do ZSK i kwalifikacji w ogłoszeniach o pracę: nie podjęto jeszcze prac projektowych, brak możliwości oszacowania

Pytanie nr 24
Ile różnych grup użytkowników (o różnych uprawnieniach) posiada aplikacja i ile spośród nich musi zostać objętych audytem (rekomendujemy testy max. 3-4 grup)?

Opowiedź do pytania nr 24

- CAS: obecnie jest 18 różnych ról. Do testów wybierzemy 3 wybrane role

- Miasto Karier: nie będzie logowania dla użytkowników, do panelu administracyjnego będzie logowanie przez CAS i będzie dostęp tylko dla administratora

- Małe ZRK: nie będzie logowania dla użytkowników, do panelu administracyjnego będzie logowanie przez CAS i będzie dostęp tylko dla administratora

- Kompas: nie będzie logowania dla użytkowników, do panelu administracyjnego będzie logowanie przez CAS i będzie dostęp tylko dla administratora

- Narzędzie do automatycznego wspomagania doradztwa: nie będzie logowania dla użytkowników, do panelu administracyjnego będzie logowanie przez CAS i będzie dostęp tylko dla administratora

- Aplikacja dla uprzywilejowanych użytkowników ułatwiająca opisywanie kwalifikacji i przypisywanie im poziomu PRK: aplikacja przed fazą projektowania jednak będzie moduł logowania dla uprzywilejowanych użytkowników. Planuje się objęcie testami maksymalnie 3 role

- Narzędzie ułatwiające tworzenie odwołań do ZSK i kwalifikacji w ogłoszeniach o pracę: nie podjęto jeszcze prac projektowych - nie będzie logowania dla użytkowników, do panelu administracyjnego będzie logowanie przez CAS i będzie dostęp tylko dla administratora

Pytanie nr 25

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).
Dodatkowo prośba o informację czy dopuszczają Państwo negocjacje zapisów umowy po dokonaniu wyboru Wykonawcy.

Opowiedź do pytania nr 25

Zamawiający nie ma informacji na ten temat w przypadku aplikacji planowanych natomiast w przypadku np. aplikacji CAS jest około 43 endpointy.