Mazowiecki
Urząd Wojewódzki w Warszawie

Mazowiecki Urząd Wojewódzki w Warszawie
Pl. Bankowy 3/5
00-950 Warszawa

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa i audytu kodu źródłowego wdrażanej Platformy e-usług, w ramach Projektu WiPER.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

Spis treści

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

Przyjęte definicje

1. **Audyt** – audyt bezpieczeństwa i audyt kodu źródłowego Platformy, wykonany według wytycznych określonych w niniejszym opisie przedmiotu zamówienia.
2. **Dokumentacja** – Raport audytorski i wszelka inna dokumentacja wytworzona w ramach realizacji Umowy.
3. **ePUAP** - Elektroniczna Platforma Usług Administracji Publicznej, w aktualnej wersji.
4. **ESB** – szyna usług, *(ang. Enterprise Service Bus)*.
5. **EZD** – system Elektronicznego Zarządzania Dokumentacją użytkowany w MUW autorstwa Podlaskiego Urzędu Wojewódzkiego.
6. **Komponent** – niezależnie wytworzony, skompilowany moduł programowy Platformy.
7. **Platforma** – wykonany na zlecenie Zamawiającego wewnętrzny system teleinformatyczny Zamawiającego, objęty Audytem.
8. **Projekt techniczny** – element dokumentacji projektowej opisujący sposób wykonania, wdrożenia i właściwości Platformy.
9. **Projekt WiPER** - projekt pod nazwą „Wdrożenie i popularyzacja e-usług realizowanych przez administrację rządową w województwie mazowieckim (WiPER)" realizowany przez Zamawiającego w ramach Działania 2.1 „E-usługi" Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020.
10. **Protokół Odbioru** – oznacza dokument potwierdzający prawidłową realizację przedmiotu zamówienia.
11. **Raport audytorski** – dokument zawierający szczegółowy opis i ocenę stanu wszystkich obszarów podlegających Audytowi, opracowany według wymagań niniejszego OPZ, na który składają się:
    1) szczegółowy raport z testów penetracyjnych;
    2) szczegółowy raport z audytu kodów źródłowych;
    3) szczegółowy raport z konfiguracji;
    4) raport podsumowujący wyniki raportów szczegółowych wraz z rekomendacjami dla kadry kierowniczej.
12. **Umowa** – Umowa zawarta pomiędzy Zamawiającym a Wykonawcą, na przeprowadzenie Audytu.
13. **Użytkownik** – osoba korzystająca z Platformy.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

14. **W3C** – *(ang. World Wide Web Consortium)* – organizacja, która zajmuje się ustanowieniem standardów pisania i przesyłu stron www.
15. **WAI** – *(ang. Web Accessibility Initiative)* – inicjatywa dostępności do sieci – inicjatywa W3C mająca na celu zwiększenie szeroko rozumianej dostępności stron www.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie Audytu Platformy, która jest wykonywana w ramach projektu p.n. „Zaprojektowanie, wykonanie i wdrożenie Platformy stanowiącej kompleksowe rozwiązanie informatyczne, zintegrowane z istniejącym systemem zarządzania dokumentacją (EZD), pozwalające na udostępnienie wysokiej jakości e-usług przez Zamawiającego oraz podległe Wojewodzie Mazowieckiemu jednostki administracji rządowej, wraz z wykonaniem Formularzy elektronicznych ePUAP", w ramach Projektu WIPER.

Realizacja zamówienia będzie składała się z następujących zadań:

1. Przedstawienie harmonogramu prac.
2. Audyt bezpieczeństwa Platformy.
3. Audyt kodu źródłowego Platformy.
4. Wykonanie i dostarczenie Raportu audytorskiego.

Zamawiający wymaga, aby zadania: audyt bezpieczeństwa i audyt kodu źródłowego Platformy były realizowane równolegle.

2. Termin realizacji zamówienia

Termin wykonania i odbioru zamówienia określa się na 20 grudnia 2018 roku.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

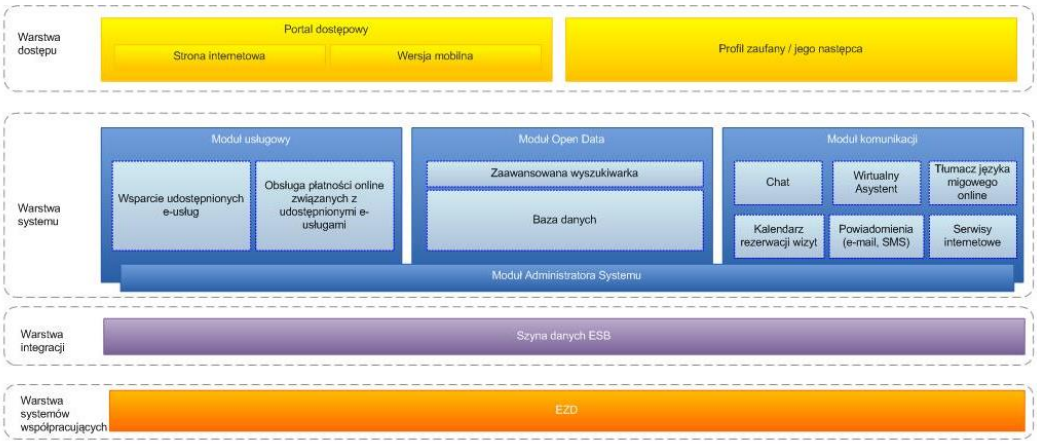
3. Architektura Platformy

Przedmiotem Audytu będzie Platforma stanowiąca kompleksowe rozwiązanie informatyczne, zintegrowane z istniejącym systemem zarządzania dokumentacją (EZD), pozwalające na udostępnienie wysokiej jakości e-usług przez Zamawiającego oraz podległe Wojewodzie Mazowieckiemu jednostki administracji rządowej.

Architektura Platformy składa się z następujących Komponentów:

1. Portalu dostępowego.
2. Modułu komunikacji.
3. Modułu Open Data.
4. Modułu usługowego.
5. Modułu administratora.
6. Szyny danych ESB umożliwiającej integrację rozwiązań.

Architekturę rozwiązania w podziale na warstwę dostępu, systemową, integracji oraz systemów współpracujących przedstawiono na rysunku 1.



Rysunek 1. Model architektury Platformy

Opis przedmiotu zamówienia zaprojektowania, wykonania i wdrożenia Platformy, Projekt techniczny i pozostała dokumentacja powdrożeniowa/wdrożeniowa, zostanie przekazana Wykonawcy po podpisaniu Umowy.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

4. Audyt bezpieczeństwa Platformy

Celem głównym Audytu jest określenie poziomu bezpieczeństwa wdrażanej Platformy e-usług, wskazanie punktów obniżających ten poziom oraz zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa.

Audyt bezpieczeństwa Platformy - będzie obejmował:

1. Kontrolę spójności oraz zgodności z przepisami obowiązującego prawa.
2. Weryfikacje bezpieczeństwa przetwarzania danych osobowych pod względem zgodności z obowiązującym prawem.
3. Weryfikacje bezpieczeństwa Platformy jako systemu teleinformatycznego.
4. Weryfikacje spełnienia wymagań określonych w opisie przedmiotu zamówienia Platformy w zakresie bezpieczeństwa.
5. Testy penetracyjne oraz analizę sposobu implementacji mechanizmów bezpieczeństwa.

4.1. Kontrola spójności oraz zgodności

Audyt będzie obejmował kontrolę spójności oraz zgodności z przepisami prawa, a także weryfikację poziomu przestrzegania tych regulacji. Zakres kontroli obejmie samą Platformę i dokumentacje bezpieczeństwa Platformy pod kątem aktualności, kompletności, poprawności, a także zgodności z obowiązującym prawem i standardami (w szczególności kontrola zgodności z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).

4.2. Bezpieczeństwo przetwarzania danych osobowych

Audyt będzie obejmował sprawdzenie aktualnego stanu przetwarzania danych osobowych zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań zgodnych z normą ISO 27001 i opisanych w ustawie o ochronie danych osobowych zgodnie z Dyrektywą RODO, jak również w Rozporządzeniu

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

MSWiA z dnia 29 kwietnia 2004 r. „w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych" (Dz.U. 2004 nr 100 poz. 1024).

4.3. Bezpieczeństwo Platformy jako systemu teleinformatycznego

Celem audytu jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub Użytkowników systemów. Przeprowadzenie audytu na etapie wytwarzania i przekazywania do użytkowania Platformy pozwolić ma na dostarczenie odbiorcom projektu rozwiązań gwarantujących osiągnięcie wymaganego poziomu bezpieczeństwa w fazie użytkowania.

Zakres obszarów podlegających audytowi:

4.3.1. Bezpieczeństwo środowiska utrzymywanego przez firmę hostującą w zakresie:

4.3.1.1. Konfiguracji systemów operacyjnych

W szczególności:

1. weryfikację udostępnionych usług sieciowych wraz ze wskazaniem ich podatności,
2. weryfikację zbędnych usług,
3. weryfikację dodatkowych metod zabezpieczeń (np. systemy antywirusowe, antymalware, HIPS, IPS/IDS itp),
4. weryfikację zaimplementowanych systemów aktualizacji i mechanizmów ich wdrażania,
5. weryfikację zaimplementowanych systemów kopii zapasowych,
6. weryfikację zaimplementowanych systemów logowania zdarzeń,
7. weryfikację mechanizmów administracji zdalnej,
8. weryfikację uprawnień Użytkowników oraz przypisania do właściwych grup, w szczególności weryfikację uprawnień do najważniejszych zasobów.

4.3.1.2. Konfiguracji baz danych

W szczególności:

1. weryfikację sposobu udostępniania baz na poziomie sieciowym,
2. weryfikację zaimplementowanych systemów kopii zapasowych,
3. analizę implementacji podstawowych zasad „utwardzania" bazy danych (np. logowanie zdarzeń, składowanie logów, partycjonowanie bazy, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL.),
4. analizę architektury bazy danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

uprawnień, przechowywanie oraz dostęp do danych wrażliwych, szyfrowanie danych),
5. analizę komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).

4.3.1.3. Bezpieczeństwo aplikacji

W szczególności:
1. wytypowanie wrażliwych punktów w systemie,
2. inspekcję mechanizmów uwierzytelniania/autoryzacji,
3. weryfikację implementacji mechanizmów ochronnych dla wszystkich serwerów aplikacyjnych i modułów dostępowych,
4. weryfikację wybranych elementów charakterystycznych dla serwera www,
5. weryfikację obsługi błędów,
6. analizę poziomu bezpieczeństwa oferowanego przez aplikację,
7. analizę architektury sieciowej.

4.3.1.4. Bezpieczeństwo sieci

W szczególności:

Analizę sieci LAN:
1. weryfikacja segmentacji sieci LAN na strefy sieciowe (z uwzględnieniem wykorzystania urządzeń typu firewall, access list oraz VLAN),
2. określenie usług działających w wybranych podsieciach,
3. poszukiwanie podatności w kilku wybranych podsieciach,
4. weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI/ISO,
5. weryfikacja dostępu do Internetu z LAN,
6. szczegółowa analiza wybranej komunikacji sieciowej,
7. weryfikacja zasad utrzymania sieci.

Analiza sieci WAN oraz styku z siecią Internet:
1. weryfikacja topologii/architektury sieci,
2. testy szczelności systemów klasy firewall, UTM,
3. ogólna analiza komunikacji sieciowej z poziomu sieci WAN oraz Internet,
4. skanowanie portów różnymi technikami,
5. wykrywanie usług sieciowych udostępnionych w sieci WAN oraz Internet,
6. próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych w szczególności z sieci Internet,
7. testowanie odporności wybranych usług wystawionych do sieci Internet na ataki Denied of Service,
8. testy penetracyjne usług VPN (w zakresie połączeń Zamawiający-Hosting).

4.3.2. Bezpieczeństwo środowiska Zamawiającego w zakresie:

Analizę sieci LAN:
1. weryfikacja segmentacji sieci LAN na strefy sieciowe (z uwzględnieniem wykorzystania urządzeń typu firewall, access list oraz VLAN),
2. określenie usług działających w wybranych podsieciach,

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

3. poszukiwanie podatności w kilku wybranych podsieciach,
4. weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI/ISO,
5. weryfikacja dostępu do Internetu z LAN,
6. szczegółowa analiza wybranej komunikacji sieciowej,
7. weryfikacja zasad utrzymania sieci.

Analiza sieci WAN oraz styku z siecią Internet:

1. weryfikacja topologii/architektury sieci,
2. testy szczelności systemów klasy firewall, UTM,
3. ogólna analiza komunikacji sieciowej z poziomu sieci WAN oraz Internet,
4. skanowanie portów różnymi technikami,
5. wykrywanie usług sieciowych udostępnionych w sieci WAN oraz Internet,
6. próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych w szczególności z sieci Internet,
7. testowanie odporności wybranych usług wystawionych do sieci Internet na ataki Denied of Service,
8. testy penetracyjne usług VPN.

4.4. Audyt wymagań określonych w opisie przedmiotu zamówienia Platformy w zakresie bezpieczeństwa

Audyt będzie obejmował analizę realizacji przez wykonawcę Platformy wymagań w zakresie funkcjonalności dotyczących bezpieczeństwa, określonych w opisie przedmiotu zamówienia zaprojektowania, wykonania i wdrożenia Platformy.

4.5. Testy penetracyjne

Zamawiający wymaga w ramach realizacji zadania, wykonywania testów penetracyjnych wykorzystania standardów testowania bezpieczeństwa:

a) OWASP (Open Web Application Security Project) ASVS 2014.

b) Open Source Security Testing Methodology Manual (OSSTMM).

c) Penetration Testing Execution Standard (PTES).

lub równoważnych (za równoważne Zamawiający uzna, standardy opisujące przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji).

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

4.5.1. Wykorzystanie zbiorów danych o znanych podatnościach i słabościach bezpieczeństwa

Zamawiający wymaga wykorzystania znanych zbiorów danych o podatnościach i słabościach bezpieczeństwa systemów teleinformatycznych, w trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, np.

a) SANS Top 20 Critical Security Controls.

b) Common Vulnerabilities and Exposures.

c) WASC (Web Application Security Consortium) Threat Classification.

lub równoważnych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych)

4.5.2. Wykorzystanie list kontrolnych

Zamawiający wymaga aby w ramach realizacji audytu bezpieczeństwa do oceny wykorzystywane były listy kontrolne udostępniane przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, tj.:

a) National Security Agency (NSA).

b) Center for Internet Security (CIS).

lub równoważnych (w szczególności takich, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych).

4.5.3. Typowe zadania dla testowania penetracyjnego

Zamawiający wymaga aby w ramach realizacji testów penetracyjnych obejmowały one typowe, wymienione niżej zadania (będące elementem każdej metodyki testów penetracyjnych):

a) Target Scoping (Zakres Docelowy – ustalenie charakteru i zasięgu testów)

b) Information Gathering (Gromadzenie Informacji – pasywne zbieranie informacji na temat obiektu testów)

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

c) Target Discovery (Odkrywanie Celu – pół-pasywne zbieranie informacji, poznanie celów, identyfikacja podsieci, rodzaju architektury, systemów operacyjnych)

d) Enumerating Target (Wyliczanie Elementów – aktywne zbieranie informacji, enumeracja usług, portów, wykrywanie systemów bezpieczeństwa IDS/UPS, FV)

e) Vulnerability Mapping (Mapowanie Podatności – poszukiwanie podatności w elementach znalezionych w poprzednich fazach)

f) Target Exploitation (Docelowa Eksploatacja – stworzenie wektora inicjalizującego atak, który ma na celu ominąć zabezpieczenia w celu naruszenia poufności, integralności oraz dostępności danych osobowych, przejęcia systemów, odcięcia systemu od sieci zewnętrznej)

g) Privilage Escalation (Eskalacja Uprawnień – zwiększenie uprawnień w przełamanym systemie i przeniesienie kontroli na kolejne usługi lub systemy)

h) Maintaining Access (Utrzymanie Dostępu – utrzymanie dostępu do skompromitowanego systemu, instalacja tylnych furtek, rootkit-ów.

i) Documentation & Reporting (Dokumentacja i Raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach)

4.5.4. Testy penetracyjne i symulowane ataki

Zamawiający wymaga aby w ramach realizacji zadania zostały przeprowadzone testy penetracyjne i symulowane ataki obejmujące:

4.5.4.1. Testy bezpieczeństwa Platformy pod kątem ataków typu:

1. Ataki semantyczne na adres URL,
2. Ataki związane z ładowaniem plików,
3. Ataki typu Cross-Site Scripting,
4. Ataki typu Cross-Site Request Forgery,
5. Ataki typu MITM (Man in the Middle),
6. Broken Authentication and Session Management (badanie losowości ID sesji, próba detekcji składni nazywania cookie sesyjnego, sprawdzenie bezpieczeństwa budowy formularza logowania),
7. Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia Użytkownika),
8. Code Execution (próby wykonania wrogiego kodu na serwerze),
9. Information Leakage (próby detekcji wycieku istotnych informacji – technicznych i biznesowych),

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

10. Insecure Communications (dostęp do istotnych danych w wyniku braku lub nieodpowiedniego poziomu szyfrowania),
11. Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania),
12. File Inclusion (załączanie plików lub do ich zawartości złośliwej zawartości),
13. Open Redirection (próby nieautoryzowanego przekierowania),
14. Fałszowanie żądania http,
15. Response Splitting (brak prawidłowej walidacji nagłówków http)
16. Ujawnienie danych przechowywanych w bazie,
17. Trawersowanie katalogów,
18. Ujawnianie kodu źródłowego,
19. Przepełnienie bufora lub stosu,
20. Wstrzykiwanie kodu wykonywalnego innych języków programowania.

4.5.4.2. Zbadanie co najmniej:

1. Enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu.
2. Możliwości podszywania się pod Użytkowników i uzyskania nieautoryzowanego dostępu do systemu.
3. Możliwości podszywania się pod Użytkowników uprzywilejowanych i uzyska-nie dostępu do systemu.
4. Możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej Użytkownikom.
5. Metody uwierzytelnienia dwustkładnikowego - próby podatności, weryfikacja działania, próby ominięcia mechanizmu.

4.5.4.3. Weryfikacja podatności systemu informatycznego na ingerencje ze strony osób trzecich

Weryfikacja powinna zostać przeprowadzona co najmniej poprzez:

1. Przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego (Platformy) z sieci Internet.
2. Przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego (Platformy) w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego.

4.5.5. Obszary bezpieczeństwa

Zamawiający wymaga aby zakres weryfikacji bezpieczeństwa adresował ryzyka występujące w poniższej przedstawionych obszarach:

1. Uwierzytelnianie

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

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

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

5. Audyt kodu źródłowego Platformy

Celem głównym audytu kodu źródłowego jest weryfikacja jakości kodu źródłowego Platformy do których Zamawiający posiada prawa autorskie, jego skalowalności, łatwości utrzymania, poprawności i stabilności działania, jak również identyfikacja naruszeń bezpieczeństwa.

Zakres usług realizowanych w ramach tego zadania obejmuje przeprowadzenie audytu kodu źródłowego, ze szczególnym uwzględnieniem poniższych aspektów:

1. Audyt architektury aplikacji.
2. Audyt zastosowanej technologii.
3. Analiza wydajności kodu.
4. Podstawowa analiza baz danych (normalizacja).
5. Audyt kosztów modyfikowania podczas utrzymania i rozwoju.
6. Analiza użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated") lub elementów posiadających znane luki bezpieczeństwa lub podatności.

W ramach audytu kodu źródłowego Platformy wymagane jest sprawdzenie dostępności strony internetowej, przeprowadzając pełną weryfikacje zgodności serwisu z międzynarodowymi standardami WCAG:

a) sprawdzenie zgodności z W3C,
b) sprawdzenie zgodności z W3C CSS,
c) sprawdzenie zgodności z WAI (WCAG 2.0).

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

6. Raport audytorski

W wyniku przeprowadzonego Audytu Wykonawca sporządzi i dostarczy Raport audytorski składający się z:

1. szczegółowego raportu z testów penetracyjnych,
2. szczegółowego raportu z audytu kodów źródłowych,
3. szczegółowego raportu konfiguracji,
4. raportu podsumowującego wyniki raportów szczegółowych wraz z rekomendacjami dla kadry kierowniczej.

Raport audytorski powinien zawierać:

1. Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających Audytowi
2. Wyniki testów i ich interpretację, w szczególności:
    a. Informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki Platformy, zawierające podsumowanie ilości stwierdzonych nieprawidłowości z oceną krytyczności.
    b. Opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność (Proof of Concept).
    c. Informacje na temat poziomu ochrony realizowanego przez Platformę zabezpieczeń.
3. Wnioski z Audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności).
4. Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń.
5. Rekomendacje i zalecenia dotyczące sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk (lista poprawek oraz szczegółowy opis zalecanych zmian).

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa

7. Gwarancja bezstronności

Wykonawca zobowiązuje się, że osoby zdolne do wykonania zamówienia złożą oświadczenie o bezstronności wykazując, że:

1. Nie brały i nie biorą udziału w pracach nad zaprojektowaniem, wykonaniem i wdrożeniem Platformy po stronie wykonawcy Platformy i podwykonawców.
2. Nie pozostają w żadnym stosunku faktycznym ani prawnym który może budzić uzasadnione wątpliwości co do bezstronności, z wykonawcą Platformy i podwykonawcami.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014-2020 oraz ze środków budżetu państwa