OPIS PRZEDMIOTU ZAMÓWIENIA – Testy bezpieczeństwa sieci i urządzeń sieciowych, analiza podatności

I. Zamawiający:

Województwo Opolskie z siedzibą w: Opole 45-082, przy ul. Piastowska 14

NIP: 7543077565, REGON: 531412421.

Marszałek województwa opolskiego zaprasza do składania ofert na realizację zadania pn. Testy bezpieczeństwa sieci i urządzeń sieciowych, analiza podatności w konkursie grantowym „Cyfrowe Województwo" realizowanym w ramach projektu „Cyfrowa Gmina". Projekt współfinansowany jest ze środków Unii Europejskiej w ramach działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU Programu Operacyjnego Polska Cyfrowa na lata 2014-2020.

II. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest realizacja audytu bezpieczeństwa (testy penetracyjne) aplikacji webowych oraz infrastruktury dla Urzędu, zgodnie z zakresem przedstawionym poniżej.

a) Testy bezpieczeństwa aplikacji webowej: pw2021.opolskie.pl (zdalne, blackbox-graybox)

- Testy bezpieczeństwa aplikacji webowej, która służy do składania wniosków w ramach funduszy
- Testy będą realizowane na środowisku nieprodukcyjnym
- max. ok 30 podstron (unikalnych widoków), 6 metod/endpointów API oraz max. 1 grupa użytkowników
- Szczegółowy zakres powyższych prac został przedstawiony w punktach 1, 2 oraz 3 poniżej

b) Testy bezpieczeństwa aplikacji webowej: opolskie.pl (zdalne, blackbox-graybox)

- Testy bezpieczeństwa aplikacji webowej, która służy jako Serwis Samorządu Województwa Opolskiego. Testy będą realizowane z perspektywy użytkownika anonimowego
- Audyt obejmie również próby uzyskania nieautoryzowanego dostępu do części administracyjnej aplikacji (panel administracyjny WordPress), ale bez pełnych testów tej części aplikacji
- Testy będą realizowane na środowisku nieprodukcyjnym
- Szczegółowy zakres powyższych prac został przedstawiony w punktach 1, 2, 3 oraz 4 poniżej

c) Testy bezpieczeństwa aplikacji webowej: bip.opolskie.pl (zdalne, blackbox-graybox)

- Testy bezpieczeństwa aplikacji webowej, która służy jako Biuletyn Informacji Publicznej Samorządu Województwa Opolskiego. Testy będą realizowane z perspektywy użytkownika anonimowego
- Audyt obejmie również próby uzyskania nieautoryzowanego dostępu do części administracyjnej aplikacji (panel administracyjny WordPress), ale bez pełnych testów tej części aplikacji
- Testy będą realizowane na środowisku nieprodukcyjnym
- Szczegółowy zakres powyższych prac został przedstawiony w punktach 1, 2, 3 i 4 poniżej.

d) Testy bezpieczeństwa aplikacji webowej: ekoplatnik.opolskie.pl (zdalne, blackbox-graybox)

- Testy bezpieczeństwa aplikacji webowej: Ekopłatnik
- Testy będą realizowane na środowisku nieprodukcyjnym
- max. ok 10 podstron (unikalnych widoków), max. 3 grupy użytkowników
- Szczegółowy zakres powyższych prac został przedstawiony w punktach 1, 2 poniżej.

e) Testy bezpieczeństwa aplikacji webowej: cuw.mapy.opolskie.pl (zdalne, blackbox-graybox)

- Testy bezpieczeństwa aplikacji webowej, która służy jako Centrum Usług Wspólnych – Portal GIS
- Testy będą realizowane na środowisku nieprodukcyjnym.
- max. ok 20 podstron (unikalnych widoków), 10 metod/endpointów API oraz max. 1 grupa użytkowników
- Szczegółowy zakres powyższych prac został przedstawiony w punktach 1, 2 oraz 3 poniżej.

f) Testy infrastruktury zewnętrznej (WAN, zdalne, blackbox)

- max. 2 publiczne adresy IP wskazany przez Zamawiającego 217.173.195.227, 217.173.195.233
- Szczegółowy zakres powyższych prac został przedstawiony w punkcie 5 poniżej.

g) Testy infrastruktury wewnętrznej (LAN, zdalne, blackbox)

- max. 900 adresów IP wskazany przez Zamawiającego
- Testy sieci wewnętrznej realizowane będą zdalnie z wykorzystaniem stacji przesiadkowej (Intel NUC), którą Wykonawca przekaże Zamawiającemu. Stacja zostanie zainstalowana w sieci, w której znajdują się maszyny objęte audytem, a dostęp do niej realizowany będzie poprzez zestawiony tunel VPN (dedykowany kanał dostępu do stacji przesiadkowej).
- Szczegółowy zakres powyższych prac został przedstawiony w punkcie 5 poniżej.

1. **Aplikacja webowa – testy bezpieczeństwa**

Rekonesans aktywny i pasywny (w przypadku aplikacji dostępnych w Internecie)

- Próby lokalizacji aplikacji dostępnej pod innym adresem (np. aplikacja deweloperska w infrastrukturze dostawcy, publicznie dostępna aplikacja w wersji testowej)
- Próby lokalizacji ukrytych katalogów i plików
- Próby wywołania błędów / wyjątków w aplikacji
- Poszukiwanie wycieków danych (np. technika Google Hacking, analiza pliku robots.txt).

Poszukiwanie podatności

- Podatności klasy injection (np. SQL injection, LDAP injection, XPATH injection, NoSQL injection).
- Podatność XXE (użycie zewnętrznych encji XML)
- Podatność XSS (Cross Site Scripting) – błędy typu reflected oraz stored.
- Analiza problemów z uwierzytelnianiem i autoryzacją (np. próby dostępu do zasobów bez uwierzytelnienia, próby dostępu do zasobów administracyjnych przez zwykłego użytkownika, próby przełamania ekranów logowania – w tym próby brute force danych dostępowych).
- Możliwości otrzymania nieautoryzowanego dostępu na poziomie systemu operacyjnego i uzyskanie w ten sposób dostępu do źródeł aplikacji, bazy danych, innych poufnych informacji.
- Próby realizacji aplikacyjnych ataków typu DoS (Denial of Service)
- Weryfikacja występowania błędów logicznych – klasa zagrożeń może obejmować podatności pozwalające na ominięcie kroków koniecznych do wykonania lub skutkujących możliwością ominięcia lub nadużycia procesów, które zaimplementowane są w aplikacji. Weryfikacji podlegać będzie max. kilka procesów wybranych przez audytora.
- Próby wykrycia innych, znanych podatności, np.: Path Traversal, Open Redirection, Cross Site Request Forgery, Server Side Request Forgery, Server Side Template Injection.
- Detekcja ogólnie znanego oprogramowania (aplikacje, biblioteki, systemy wspomagające).
- Po wykryciu nieaktualnych wersji, próby lokalizacji znanych, istotnych podatności w kilku wybranych źródłach

2. **Serwer webowy / serwer aplikacyjny – testy bezpieczeństwa**

Poszukiwanie podatności / problemów bezpieczeństwa

- Analiza konfiguracji SSL/TLS (certyfikat, skonfigurowane algorytmy kryptograficzne)
- Analiza dostępności ewentualnego panelu zarządzania komponentem (enumeracja panelu administracyjnego)
- Próby użycia domyślnych / prostych par login/haseł do panelu zarządzania
- Analiza ujawnienia dokładnej wersji komponentu (nagłówki odpowiedzi / komunikaty błędów)
- Po udanym pozyskaniu wersji komponentu, próba zlokalizowania publicznie dostępnych podatności w tej wersji
- Analiza domyślnych aplikacji typu „example” lub „demo” (dostarczanych domyślnie z serwerem webowym / aplikacyjnym)

- Kilka siłowych prób wymuszania wyświetlenia błędów / wyjątków (np.: przesłanie nieprawidłowego adresu URL, wysłanie niepoprawnego requestu)
- Analiza domyślnej domeny skonfigurowanej na komponencie (np. poprzez odwołanie się do adresu IP)
- Analiza obsługi nietypowych metod HTTP (TRACE, DEBUG, PUT, DELETE)

3. API – testy bezpieczeństwa

Poszukiwanie podatności

- Analiza dostępnych metod HTTP
- Próby obejść restrykcji nałożonych na metody HTTP (np. wykorzystanie nagłówka X-HTTP-Method-Override)
- Weryfikacja akceptowanych formatów wejściowych (JSON/XML/YAML/inne)
- Próby wykrycia w przekazywanych parametrach podatności charakterystycznych dla rozwiązań webowych (w szczególności: Server Side Request Forgery, problemy z uwierzytelnianiem i autoryzacją, SQL injection, OS command execution)
- Próba wykrycia podatnych bibliotek I konkretnych, znanych publicznie podatności w tych bibliotekach (na przykład: Jackson Remote Code Execution, Apache Struts REST plugin Remote Code Execution, Node-jose Library JSON Web Tokens Re-sign Vulnerability)
- Analiza bezpieczeństwa JWT (JSON Web Token; jeśli mechanizm jest używany) – próby ominięcia weryfikacji podpisu tokena, analiza ewentualnych wycieków danych w tokenach, weryfikacja sprawdzenia kluczowych deklaracji (claims)
- Analiza wykorzystania kluczy API (jeśli są używane) –analiza ewentualnej struktury i przekazywania klucza
- Analiza nałożonego ograniczenia na ilość requestów do API (rate limiting)

4. Testy bezpieczeństwa systemu Wordpress

- Ustalenie wykorzystywanej wersji systemu WordPress;
- Enumeracja wersji wykorzystywanych szablonów (themes) oraz wtyczek (plugins) - próby wykrycia nieaktualnych komponentów;
- Enumeracja wykorzystania nadmiarowych (niewykorzystywanych) szablonów i wtyczek;
- Weryfikacja ujawniania nadmiarowych informacji o systemie WordPress (pliki readme, możliwość enumeracji użytkowników systemu, etc);
- Weryfikacja zabezpieczenia dostępu do panelu administracyjnego WordPress;
- Weryfikacja obecności dodatkowych technik hardeningowych metodami blackbox (np. modyfikacja domyślnych ścieżek do plików szablonów oraz wtyczek);

5. Urządzenie sieciowe – zewnętrzny test bezpieczeństwa

- Skanowanie portów TCP oraz najpopularniejszych portów UDP (kilka typów – prostych oraz zaawansowanych) –wykorzystanie nmap.
- Tuning parametrów skanowania, w przypadku wykrycia agresywnego blokowania przez firewall.
- Wykorzystanie wybranych skryptów nmap NSE w celu realizacji enumeracji, wykrycia możliwych wycieków danych, czy wskazania podatności.
- Próba detekcji typu oraz wersji usług sieciowych działających w systemie.
- Próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu.

- Po udanej detekcji wersji oprogramowania systemowego / usług –próba lokalizacji znanych podatności w danych wersjach oprogramowania.
- Skanowanie podatności z wykorzystaniem komercyjnej wersji oprogramowania Nessus Vulnerability Scanner (ponad 90.000 pluginów atakujących) - punkt ma zastosowanie dla przypadków w których istnieje możliwość wykorzystania skanera
- Ataki typu brute force na uwierzytelnienie do popularnych usług działających na urządzeniu (np.ssh / telnet / snmp / ftp).
- W przypadku wykrycia serwerów aplikacyjnych/webowych –kilka podstawowych prób ataku: próby otrzymania dostępu na system operacyjny / ominięcie uwierzytelnienia / próba dostępu do poufnych zasobów (prace nie obejmują pełnych testów na warstwie aplikacji)
- Test obejmuje skanowanie dowolnego urządzenia sieciowego (np.: serwer, router, firewall, punkt dostępowy sieci bezprzewodowej)

Raport poaudytowy

Wykonawca przekaże zamawiającemu utworzony w wyniku prac Raport Poaudytowy, który będzie zawierać:

- Podsumowanie wykonanych prac.
- Skrótowy opis najistotniejszych znalezionych podatności (tj. błędów bezpieczeństwa).
- Metodologia prowadzenia audytu.
- Szczegółowe informacje o znalezionych podatnościach w testowanych elementach Środowiska Informatycznego.
- Wskazanie metod naprawy podatności (luk w bezpieczeństwie) - dla wykrytych podatności o stopniu niebezpieczeństwa wysokim i krytycznym.
- Sugerowane metody naprawy podatności w pozostałych przypadkach.
- Szacowany poziom zagrożenia.
- Prezentacja proof of concept realnego ataku na podatność (dla wybranych przypadków).

III. Wymagania dla wykonawcy

Wykonawca usługi musi przedstawić co najmniej 8 referencji potwierdzających kompetencje w testach penetracyjnych aplikacji lub infrastruktury z ostatnich 2 lat.

Zespół audytowy wykonawcy musi się składać z co najmniej 20 stale współpracujących pentesterów z co najmniej 2 letnim doświadczeniem, posiadających certyfikaty takie jak: OSCP, EWPTX, CEH, CISP, OSWE.

Stosowaną podczas audytu metodyką prac jest OWASP TOP 10 (Open Web Application Security Project TOP 10 vulnerabilities) w zakresie: bezpieczeństwa aplikacji webowych.

IV. Termin i sposób realizacji zamówienia

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie 40 dni od dnia zawarcia umowy.

- Prace realizowane są w dni robocze, w godzinach roboczych, jednakże Wykonawca może wykonywać prace poza tymi terminami po wcześniejszym uzgodnieniu z Zamawiającym.
- Zamawiający zobowiązuje się do udzielenia Wykonawcy konsultacji w zakresie działania audytowanych systemów.
- Zamawiający dysponuje prawami do testowanych systemów lub aplikacji w zakresie umożliwiającym wykonanie Audytu Bezpieczeństwa, w tym testów penetracyjnych, bez narażania się przez Wykonawcą na roszczenia podmiotów trzecich. Jeśli Zamawiający nie dysponuje prawami do systemu wówczas dostarczy Wykonawcy List Autoryzacyjny.
- W ramach realizacji audytu Wykonawca może korzystać ze Stacji przesiadkowej (urządzenie komputerowe wraz z oprogramowaniem Wykonawcy), umożliwiającej zdalny dostęp do Środowiska Informatycznego Zamawiającego. Zamawiający zainstaluje Stację przesiadkowa w Środowisku Informatycznym, zgodnie z wytycznymi Wykonawcy oraz umożliwi do niej dostęp przy użyciu tunelu VPN Wykonawcy. Wszelkie zmiany w tym zakresie wymagają uzgodnień stron przed rozpoczęciem prac.

Termin rozpoczęcia prac wynosi 2 - 3 tygodnie od pełnej gotowości Zamawiającego oraz podpisanej Umowy. Poszczególne moduły mogą być realizowane równolegle w celu najszybszego zakończenia całego zakresu.

V. Kryteria wyboru ocen

Przy wyborze oferty do realizacji zamawiający będzie się kierował:

1. Kryterium: Cena - 70% (max. 7 punktów)
2. Kryterium: Doświadczenie osoby skierowanej do realizacji zamówienia - 30% (max. 3 punkty)

Oferta może uzyskać łącznie maksymalnie 10 punktów.

Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

VI. Oferta ma zawierać:

1. Kompletny, wypełniony formularz ofertowy stanowiący załącznik nr 1;
2. Kompletne, wypełnione oświadczenie stanowiące załącznik nr 2;
3. Dokumenty potwierdzające spełnienie wymagań wobec wykonawcy określone w pkt. III OPZ.

Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

VII. Miejsce i termin składania ofert

Oferty proszę składać w formie elektronicznej na platformie:

https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

Termin składania ofert upływa z dniem: 30.08.2023 r. godz. 12:00

Oferty złożone po terminie nie będą rozpatrywane.

VIII. Termin związania ofertą

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.

IX. Postanowienia końcowe

1. Zamawiający zastrzega sobie prawo odstąpienia, bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu publikacji niniejszego zapytania ofertowego.
2. Zapytanie może zostać zmienione przed upływem terminu składania ofert przewidzianym w zapytaniu ofertowym. Zmiana oraz treść pytań wraz z wyjaśnieniami zostanie opublikowana na stronie: https://bazakonkurencyjnosci.funduszeeuropeiskie.gov.pl.

X. Załączniki

1. Załącznik nr 1 - Formularz ofertowy
2. Załącznik nr 2 - Oświadczenie o spełnieniu warunków udziału w postępowaniu
3. Załącznik nr 3 - Wzór umowy
4. Załącznik nr 4 - Klauzula informacyjna RODO