Szczegółowy o przedmiotu zamówienia

Przedmiotem zamówienia jest:
opracowanie planu testów bezpieczeństwa systemu API BDL, ich wykonanie oraz przygotowanie raportu z testów i rekomendacji w zakresie zalecanych zasad bezpieczeństwa dla testowanego systemu.

Zakres działań Wykonawcy będzie obejmował:
1) opracowanie dokumentu z planem testów oraz szczegółowego harmonogramu prac jego realizacji,
- dokument z planem testów opisywał będzie koncepcję i metody przeprowadzenia testów, ich zakres przedmiotowy, a także charakterystykę narzędzi testowych,
2) zapoznanie się z audytowanym systemem i jego dokumentacją techniczną,
3) przeprowadzenie testów bezpieczeństwa manualnych i automatycznych systemu pod kątem :
a) wykrywania luk i podatności systemu w obszarze jego konfiguracji i elementów tj. systemu operacyjnego, bazy danych , aplikacji oraz usług, na których funkcjonuje,
b) analizę ewentualnych luk i podatności, wskazanie sposobów przeciwdziałania możliwości ich wykorzystania, rekomendacje sposobów ich eliminowania
4) Zasięg testów bezpieczeństwa obejmie interfejs aplikacyjny dostępny z sieci wewnętrznej.
5) Organizacja i prowadzenie testów będą oparte m.in. o listę kontrolną np.: OWASP - „Web Application Security Testing Cheat Sheet" w zakresie najczęściej występujących ataków – z listy TOP 10 2017 – publikowanej przez OWASP.
6) Testy automatyczne powinny zostać przeprowadzone przy użyciu co najmniej jednego narzędzia takiego jak: Acunetix, Burp Suite,IBM AppScan. Jako dodatkowe mogą być wykonane testy przy użyciu narzędzia open source OWASP ZAP.
7) Do realizacji testów manualnych aplikacji należy wykorzystywać dostępne narzędzia wspierające takie jak: HTTP Proxy, narzędzia diagnozujące protokół SSL/TLS, zapytania, instrukcje lub scenariusze umożliwiające identyfikację, a następnie wykorzystanie podatności w systemie,
8) Wytworzenie dokumentacji (w tym: raportu podsumowującego testy bezpieczeństwa), zawierającej m.in.:
a) zidentyfikowane ryzyka i wektory ataków,
b) zakres przedmiotowy testów,
c) wyłączenia z zakresu testów,
d) listę i opis narzędzi testowych,
e) metody i koncepcje testowania,
f) opis przebiegu testów, wykonywane czynności,
g) harmonogram testów,
i) wyniki przeprowadzonych testów (w tym: tytuł i opis wykrytych luk i podatności, lokalizacja wykrytych luk),
j) ocenę ryzyka poszczególnych luk i podatności,
k) materiał poglądowy (dowodowy), wycinek kodu, zrzut ekranu,
l)możliwości wykorzystania wykrytych podatności,
m) ocenę skutków wykorzystania podatności,
n) odnośniki do zewnętrznych źródeł, baz wiedzy, dokumentów,
o) rekomendacje oraz instrukcje w kierunku wyeliminowania wykrytych ewentualnych podatności,
p) informacje podsumowujące,
q) syntetyczną ocenę poziomu bezpieczeństwa testowanego systemu.
r) przeprowadzenie warsztatowego przekazania wiedzy dla użytkowników audytowanego systemu

Systemy objęty testami bezpieczeństwa będzie posiadał interfejsy dostępne z sieci wewnętrznej.

Nie przewiduje się wykonywania testów wewnętrznych poza siedzibą Zamawiającego .

Zamawiający na życzenie Wykonawcy, po zawarciu Umowy udostępni w swojej siedzibie dostęp do dokumentacji i systemu oraz umożliwi spotkanie z administratorami systemów w celu jak najlepszego zaplanowania procesu testów.

Spotkania robocze Zamawiającego z Wykonawcą będą odbywać się w zakładzie Zamawiającego w Radomiu.

Na potrzeby opracowania przedmiotu zamówienia Zamawiający udostępni w siedzibie Zamawiającego i po podpisaniu umowy posiadane materiały i dokumenty, jak również zapewni współpracę właściwych pracowników.

Infrastruktura bezpieczeństwa i informatyczna zlokalizowana jest w budynku GUS.