Załącznik nr 1 do Umowy ……...

SZCZEGÓŁOWY ZAKRES AUDYTU

Zakres audytu:
1. Przeprowadzenie testów penetracyjnych typu blackbox i greybox,

2. Badanie aplikacji pod kątem odporności na ataki w zakresie:

- autoryzacji, uwierzytelniania i kontroli dostępu,

- zarządzania sesją,

- walidacji wejścia,

- mechanizmów kryptograficznych oraz danych wrażliwych,

- konfiguracji systemu,

- logowania,

3. Analizę podatności i zagrożeń,

4. Analizę konfiguracji (serwery, systemy operacyjne, bazy danych, usługi, porty),

5. Podczas testów szukane będą podatności w oparciu o OWASP TOP 10:

- Injection,

- Cross Site Scripting,

- Broken Authentication and Session Management,

- Insecure Direct Object References,

- Cross Site Request Forgery,

- Security Misconfiguration,

- Insecure Cryptografic Storage,

- Failure to Restrict URL Access,

- Insufficient Transport Layer Protection,

- Unvalidated Redirects and Forwards.

6. Dodatkowo powinny być analizowane takie elementy aplikacji webowych jak:

- Nagłówki wysyłane przez serwer

- Pliki cookie

- Skrypty javascript

- Elementy RIA aplikacji webowych (pliki SWF, aplety java)

- Czasy odpowiedzi serwera przy poszczególnych operacjach

- Reakcja na dane wejściowe w zapytaniach (nagłówki, agent przeglądarki, wadliwe zapytania protokołu HTTP)

- Próby aplikacyjnych ataków DoS

Testy zakładają również badanie pod kątem bezpieczeństwa zachowania logiki aplikacji.
W tej części testów osoby audytujące utworzą szereg scenariuszów, które następnie będą przetestowane. Scenariusze są opracowywane pod kątem logiki działania danego systemu.

Dodatkowo przeprowadzone testy będą symulowały próby przeprowadzenia ataków na aplikację z strony:

- Użytkownika niezalogowanego

- Klienta aplikacji

7. Prace powinny być wykonywane z uwzględnieniem najlepszych praktyk oraz metodyk takich jak OSSTMM v3 oraz ISSAF.

8. Konsultacje

Wykonawca powinien udzielić konsultacji administratorom testowanych aplikacji w zakresie przeprowadzonego Audytu. Porady merytoryczne będą udzielane mailowo w zakresie zidentyfikowanych podatności oraz przedstawionych w raporcie rekomendacji wyłącznie pracownikom Zamawiającego, którzy uczestniczyli w prezentacjach i omówieniu metodyki Audytu.