Wykonawca dostarczy wyniki testów bezpieczeństwa aplikacji/systemu/programu przeprowadzonych w zakresie:

1. Badanie podatności aplikacji webowej zgodnie z OWASP:

A1: 2017-Injection: badanie wad takich jak wstrzyknięcie kodu SQL, NoSQL, OS i LDAP – wysyłanie niezaufanych danych do interpretera jako część polecenia lub zapytania. Próba przesłania i wykonania przez atakującego poleceń lub uzyskania dostępu do danych bez odpowiedniej autoryzacji.

A2: 2017 - Broken Authentication: badanie funkcji aplikacji związane z uwierzytelnianiem i zarządzaniem sesjami są często wdrażane nieprawidłowo, co umożliwia atakującym złamanie haseł, kluczy lub tokenów sesji lub wykorzystanie innych błędów implementacji w celu tymczasowego lub trwałego przejęcia tożsamości innych użytkowników.

A3: 2017 - Sensitive Data Exposure: badanie aplikacji i interfejsów API, czy chroni odpowiednio dane. Próba kradzieży lub modyfikowania słabo chronionych danych w celu oszustwa związanego z kartami kredytowymi, kradzieży tożsamości lub innych przestępstw. Testy naruszenia danych niewłaściwie zabezpieczonych np. przechowywanych bez szyfrowania lub podczas przesyłania.

A4: 2017-XML External Entities (XXE): Testy starszych lub źle skonfigurowanych procesorów XML w celu oceny odniesienia do jednostek zewnętrznych w dokumentach XML. Próba wykorzystania jednostek zewnętrznych w celu ujawnienia plików wewnętrznych za pomocą modułu obsługi URI plików, wewnętrznych udziałów plików, skanowania portów wewnętrznych, zdalnego wykonywania kodu i ataków typu „odmowa usługi”.

A5: 2017 - Broken Access Control: Analiza ograniczeń uwierzytelnionych użytkowników. Próba wykorzystania błędów aplikacji w celu uzyskania dostępu do nieautoryzowanych funkcji i / lub danych, takich jak dostęp do kont innych użytkowników, przeglądanie poufnych plików, modyfikowanie danych innych użytkowników, zmiana praw dostępu itp.

A6: 2017-Błędna konfiguracja zabezpieczeń: Testy konfiguracji zabezpieczeń. Analiza niezabezpieczonych konfiguracji domyślnych, konfiguracji niekompletnych lub konfiguracji ad hoc, otwartej pamięci masowej w chmurze, błędnie skonfigurowanych nagłówków HTTP i pełnych komunikatów o błędach zawierających poufne informacje.

A7: 2017-Cross-Site Scripting XSS: Testy błędów XSS w celu analizy, czy aplikacja zawiera niezaufane dane na nowej stronie internetowej bez odpowiedniej weryfikacji lub zmiany znaczenia lub aktualizuje istniejącą stronę internetową danymi dostarczonymi przez użytkownika za pomocą interfejsu API przeglądarki, który może tworzyć HTML lub JavaScript. Testy XSS w celu weryfikacji, czy aplikacja umożliwia atakującym wykonywanie skryptów w przeglądarce ofiary, które mogą przechwytywać sesje użytkownika, niszczyć witryny internetowe lub przekierowywać użytkownika do złośliwych witryn.

A8: 2017-Niezabezpieczona deserializacja: Testy niezabezpieczonej deserializacja w celu weryfikacji możliwości zdalnego wykonania kodu.

A9: 2017-Używanie komponentów ze znanymi lukami w zabezpieczeniach: Testy komponentów takich jak biblioteki, frameworki i inne moduły oprogramowania.

A10: 2017-Niewystarczające rejestrowanie i monitorowanie: weryfikacja zakresu rejestrowania zdarzeń i monitorowania aplikacji w celu zbadania skuteczności reakcji na incydenty.