

Podsumowanie dla Kierownictwa

Niniejszy raport dokumentuje wyniki oceny bezpieczeństwa aplikacji **whiblo.pl** przeprowadzonej przez SISOFT s.c. w dniach **1 - 9 lipca 2021** roku z sieci publicznej Internet. Ocena bezpieczeństwa została przeprowadzona z perspektywy podejścia gray-box z wykorzystaniem danych uwierzytelniających do aplikacji.

Ocena bezpieczeństwa aplikacji dostarczyła firmie Braf.Tech wgląd w odporność aplikacji na ataki ze strony nieuprawnionych użytkowników oraz możliwość nadużycia uprawnień i dostępu przez użytkowników aplikacji. Wszystkie czynności zostały przeprowadzone zgodnie z ogólnie przyjętą metodologią OWASP ASVS 4.0.2 oraz najlepszymi praktykami.

Klasyfikacja ryzyka

Po wykryciu jakiegokolwiek podatności, którą można wykorzystać, prowadzone były analizy w celu określenia jej poziomu krytyczności. Ryzyko obliczane jest według następujących kryteriów:

- **Zagrożenie:** wpływ na bezpieczeństwo aplikacji w przypadku wykorzystania podatności przez atakującego. To kryterium wskazuje na korzyść ataku dla atakującego.
- **Łatwość wykorzystania:** poziom trudności wykorzystania podatności przez atakującego. Trudność może wzrosnąć ze względu na złożoność techniczną, potrzebę wcześniejszej znajomości sieci lub inne czynniki. To kryterium wskazuje nakład czasu i zasobów ataku dla atakującego.
- **Popularność i łatwość identyfikacji podatności:** to kryterium uwzględnia publiczną dostępność informacji i narzędzi do wykrywania podatności. Podatności, które są wykorzystywane przez ogólnie dostępny złośliwy kod lub które mają łatwy w użyciu kod exploita dostępny w Internecie, otrzymałyby wyższą ocenę. To kryterium wskazuje na prawdopodobieństwo ataku.

Poniższy wykres przedstawia wyniki oceny ryzyka przeprowadzonej po wykonaniu oceny bezpieczeństwa aplikacji, której wartość w skali 0 – 10 (niskie – wysokie) wyniosła **4.2**. Po przeprowadzeniu re-testu stwierdzono, że **wszystkie podatności zostały usunięte**.

