Podsumowanie testów bezpieczeństwa

dla eRecruitment Solutions Sp. z o. o.

Warszawa, 5 kwietnia 2018

Podsumowanie testów bezpieczeństwa

Niniejszy dokument stanowi podsumowanie wyników testów bezpieczeństwa, które zostały przeprowadzone przez ISEC Sp. z o. o. w dniach 19–23 marca 2018 roku. Zakres prac obejmował identyfikację podatności bezpieczeństwa w aplikacji webowej https://system.erecruiter.pl/, opracowanie raportu z testów, przedstawienie rekomendacji naprawczych oraz ocenę skuteczności ich wdrożenia.

Badanie zostało przeprowadzone zdalnie w oparciu o metodykę *grey-box* na środowisku produkcyjnym. W tym celu wykorzystano testowe organizacje i użytkowników oraz narzędzia takie jak Burp Suite Pro, dodatki do przeglądarek, *fuzzery* itd. Testy skupiły się na identyfikacji błędów wynikających m.in. z braku walidacji danych wejściowych i wyjściowych, braku należytej kontroli dostępu, niewłaściwego zarządzania sesją użytkownika, błędów konfiguracyjnych, braki należytej obsługi wyjątków.. Badanie kodu źródłowego nie wchodziło w zakres prac.

Po raz kolejny poziom bezpieczeństwa badanej aplikacji został oceniony bardzo wysoko. Zespół przeprowadzający testy zidentyfikował jednak dwie podatności typu *Stored Cross-Site Scripting*. Ich przyczyną był brak walidacji danych wejściowych i wyjściowych, nad którymi kontrolę ma użytkownik aplikacji. Stwierdzono także, że aplikacja ujawnia zbędne informacje na temat rodzaju i wersji wykorzystywanego oprogramowania a także o wewnętrznym adresie IP.

Zalecenia ukierunkowane na eliminację podatności zostały wdrożone przez zespół developerów niezwłocznie oraz skutecznie, czego dowiodła weryfikacja przeprowadzona przez zespół testujący w dniu 5 kwietnia 2018 r.

Ufamy, że dzięki naszej pracy przyczyniliśmy się do podniesienia poziomu bezpieczeństwa aplikacji eRecruiter.

Piotr Szeptyński

Piotr Szeptyński
Członek Zarządu
ISEC Sp. z o. o.