Politechnika Warszawska

WYDZIAŁ ELEKTRONIKI
I TECHNIK INFORMACYJNYCH

Dokumentacja naprawy aplikacji mobilnej KINO

stworzonej na potrzeby projektu w ramach przedmiotu
Bezpieczeństwo oprogramowania testy penetracyjne

Maciej Krysiak
300574
Łukasz Śleboda
300519

Opiekun projektu:
dr inż. Mariusz Sepczuk

Warszawa 2021

Spis treści

1. Cel raportu

Celem poniższego raportu jest wskazanie odnalezionych przez zespół pentesterów podatności aplikacji mobilnej CinemaApp, jak i API serwera aplikacji i wyjaśnienie, czy i w jaki sposób zostały one naprawione.

2. Naprawa znalezionych podatności

Raport z testów penetracyjnych wykazał odnalezienie 5 podatności, w tym 4 o poziomie zagrożenia wskazującym na lukę krytyczną.

Podatność	Status naprawy	Zagrożenie
Zapis danych uwierzytelnienia do logu	naprawiono	wysokie
Możliwość zmiany parametrów kupowanego biletu	naprawiono	wysokie
Wyciek wrażliwych danych	naprawiono	wysokie
Tymczasowy zapis biletu do pliku	naprawiono	średni
Zakodowany na stałe PIN do aplikacji	naprawiono	wysokie

a. Zapis danych uwierzytelniania do logu

Podatność ta została wyeliminowana poprzez usunięcie fragmentu kodu w pliku *LoginActivity.java* odpowiedzialnego za zapis loginu i hasła do logów.

b. Możliwość zmiany parametrów kupowanego biletu

Podatność ta została wyeliminowana poprzez modyfikację API serwera aplikacji. Żądanie */Tickets/Buy* (punkt 3.5.3 dokumentacji aplikacji) zostało zmienione na zapytanie typu POST, a wszystkie wymagane dane potrzebne do zakupu samego biletu zostały umieszczone w ciele samego żądania. Dodatkowo wprowadzono wymóg posiadania tokenu autoryzacji do użycia odpowiedniego API.

c. Wyciek wrażliwych danych

Podatność ta została wyeliminowana poprzez usunięcie wadliwego przycisku, który wywoływał zapytanie SQL zwracające bilety wszystkich użytkowników zarejestrowanych w aplikacji.

d. Tymczasowy zapis biletu do pliku

Podatność ta została wyeliminowana poprzez zmianę sposobu prezentacji biletu. Od teraz bilet nie jest wyświetlany z wykorzystaniem komponentu webView, a za pomocą klasycznego Activity z labelami. Dzięki temu plik HTML zawierający wrażliwe dane nie jest już przechowywany na urządzeniu.

e. Zakodowany na stałe PIN do aplikacji

Podatność ta została wyeliminowana poprzez rezygnacje z zabezpieczenia aplikacji kodem PIN. Stwierdzono, że zabezpieczenie pinem dostępu do activity logowania i rejestracji nie ma sensu, gdyż taki pin musiałby zostać udostępniony publicznie wszystkim użytkownikom pobierającym aplikacje.

3. Podsumowanie

Wszystkie luki aplikacji wykryte w raporcie pentesterskim zostały naprawione. API serwera zostało zabezpieczone poprzez wprowadzenie wymogu podawania tokena autoryzacji sesji, wszystkie wrażliwe dane są przenoszone w ciele metod, a sama komunikacja odbywa się poprzez protokół HTTPS. Wyeliminowano również wszystkie luki odnalezione w aplikacji mobilnej, szczególnie usuwając logi przenoszące wrażliwe dane użytkownika czy pozostałość po niefrasobliwości programisty, czyli przyciski pozwalające na dostęp do nieautoryzowanych danych innych użytkowników.