INTISARI

Mobile JKN merupakan aplikasi yang dikeluarkan oleh BPJS Kesehatan yang didalamnya memuat data informasi penting yang bersifat privasi milik peserta BPJS Kesehatan. Data informasi tersebut sering menjadi target bagi pelaku kejahatan siber untuk mendapatkan keuntungan pribadi dari data informasi yang dicurinya dengan cara memanfaatkan celah keamanan pada aplikasi. Untuk itu, perlu dilakukan analisis untuk mendeteksi celah keamanan pada aplikasi Mobile JKN. Aplikasi Mobile JKN dianalisis menggunakan tools Mobile Security Framework (MobSF) dengan melakukan analisis statis dan dinamis. MobSF merupakan alat yang bersifat open source dan digunakan untuk mendeteksi celah keamanan pada aplikasi mobile. Hasil dari analisis statis menunjukkan bahwa aplikasi tidak mengandung program berbahaya dalam pengecekkan domain malware check, mampu mendeteksi perangkat yang telah di root, serta menggunakan SSL Pinning yang aman. Namun juga ditemukan beberapa potensi celah keamanan seperti terdeteksi adanya izin akses yang berbahaya, penggunaan metode kriptografi yang lemah, adanya service, activity, serta penggunaan hardcoded secret yang rentan. Selain itu, aplikasi terdeteksi rentan terhadap serangan janus, SQL Injection, dan serangan padding oracle. Sedangkan hasil analisis dinamis, diketahui bahwa aplikasi telah menerapkan SSL Pinning untuk mengamankan jalur komunikasi, dan tidak ditemukan penurunan performa pada uji activity yang dijalankan, Namun pada saat dilakukan uji root detection bypass saat menjalankan analisis dinamis, belum diterapkan root detection pada aplikasi dan tidak mendeteksi adanya debugger yang terhubung ke dalamnya pada saat aplikasi berjalan.

Kata kunci: MobSF, statis, dinamis, Mobile JKN

ABSTRACT

Mobile JKN is an application issued by BPJS Kesehatan which contains important information data that is private to BPJS Kesehatan participants. This information data is often a target for cybercriminals to gain personal benefits from the stolen information data by utilizing security gaps in the application. For this reason, it is necessary to analyze to detect security gaps in the JKN Mobile application. The JKN Mobile application is analyzed using the Mobile Security Framework (MobSF) tool by performing static and dynamic analysis. MobSF is an open source tool used to detect security holes in mobile applications. The results of the static analysis show that the application does not contain malicious programs in the malware check domain check, is able to detect rooted devices, and uses secure SSL Pinning. However, several potential security holes were also found such as the detection of malicious access permissions, the use of weak cryptographic methods, the presence of services, activities, and the use of vulnerable hardcoded secrets. In addition, the application was detected to be vulnerable to janus attacks, SQL Injection, and oracle padding attacks. While the results of dynamic analysis, it is known that the application has implemented SSL Pinning to secure the communication path, and no performance degradation was found in the activity test that was run, but when the root detection bypass test was carried out when running dynamic analysis, root detection had not been applied to the application and did not detect a debugger connected to it when the application was running.

Keywords: MobSF, static, dynamic, Mobile JKN