BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa penerapan analisis keamanan statis dan dinamis menggunakan Mobile Security Framework (MobSF) mampu memberikan gambaran mengenai tingkat keamanan serta karakteristik kerentanan pada aplikasi media sosial berbasis Android, yaitu Instagram, Facebook, dan TikTok. Analisis statis berhasil mengidentifikasi potensi kelemahan pada struktur dan konfigurasi aplikasi, seperti penggunaan permission berisiko, konfigurasi SSL/TLS yang kurang optimal, serta penerapan kriptografi yang lemah, sedangkan analisis dinamis mampu mengungkap perilaku aplikasi saat runtime, meliputi aktivitas jaringan, pemanggilan API sensitif, penggunaan izin secara aktual, dan aktivitas latar belakang aplikasi yang tidak dapat sepenuhnya terdeteksi melalui analisis statis. Hasil perbandingan menunjukkan bahwa kedua metode analisis saling melengkapi dan memberikan evaluasi keamanan yang lebih komprehensif dibandingkan penggunaan satu metode saja, dengan tingkat risiko keamanan aplikasi berada pada kategori rendah hingga menengah berdasarkan hasil pemindaian MobSF. Namun demikian, hasil analisis menggunakan Mobile Security Framework (MobSF) tidak dapat dijadikan sebagai tolok ukur mutlak bahwa suatu aplikasi benar-benar berbahaya atau tidak, karena MobSF melakukan penilaian keamanan berdasarkan parameter dan variabel yang telah ditetapkan oleh framework tersebut.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya. Pertama, penelitian lanjutan disarankan untuk menggunakan atau mengombinasikan Mobile Security Framework (MobSF) dengan alat pengujian keamanan aplikasi Android lainnya, baik untuk analisis statis maupun dinamis, seperti penggunaan framework atau tools keamanan yang memiliki pendekatan dan mekanisme pendeteksian berbeda, sehingga hasil evaluasi keamanan dapat menjadi lebih beragam dan komprehensif.

Kedua, pada pengujian dinamis, penelitian selanjutnya dapat memperluas cakupan analisis dengan menambahkan parameter pengamatan perilaku aplikasi yang lebih detail, seperti pola komunikasi jaringan, interaksi API lanjutan, serta aktivitas latar belakang aplikasi dalam berbagai skenario penggunaan, tanpa harus bergantung pada penggunaan perangkat fisik. Ketiga, hasil penelitian ini dapat dijadikan sebagai bahan pertimbangan bagi pengembang aplikasi media sosial untuk meningkatkan aspek keamanan, khususnya dalam pengelolaan izin, konfigurasi komunikasi jaringan, serta penerapan kriptografi yang lebih kuat guna meminimalkan risiko kebocoran data dan pelanggaran privasi pengguna.