BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan meningkatnya aplikasi berbasis android maka berdampak pada kenaikan jumlah pengguna sistem operasi berbasis android [1]. Menurut data dari Statcounter Global Stats dalam rentan waktu 2020-2022 terdapat sebanyak 72,% pengguna perangkat mobile menggunakan Android sebagai sistem operasi [2]. Selain menjadi sistem operasi ponsel yang sangat diminati android juga merupakan sistem operasi yang paling rentan terhadap keamanan keamanan [3]. Dari data bulettin keamanan android pada tahun 2022 terdapat 514 kerentanan yang ditemukan [4]. Namun, jumlah kerentanan tersebut menurun setiap tahunnya. Dalam perkembangan terbaru, perangkat seluler secara bertahap mulai menggantikan peran komputer dengan munculnya berbagai fitur dan aplikasi yang tersedia di dalamnya. Salah satu contoh aplikasi yang populer adalah aplikasi pesan instan (Instant Messaging/IM) [5]. Saat ini pengiriman pesan instan berkembang dengan cepat dan telah menjadi kebutuhan penting bagi pengguna internet di seluruh dunia. Saat ini, WhatsApp adalah aplikasi pengiriman pesan instan yang paling populer [6].

Penggunaan aplikasi WhatsApp dalam era digital yang semakin berkembang telah menjadi fenomena global. Aplikasi ini telah mengubah cara kita berinteraksi, memungkinkan pengiriman pesan instan, panggilan suara, panggilan video, dan berbagi berbagai jenis media. Dari data yang didapat dari website DataIndonesia whatsapp merupakan media sosial yang paling banyak digunakan oleh masyarakat indonesia, menurut laporan dari We Are Social presetase pengguna aplikasi whatsapp pada januari 2023 didalam negeri mencapai 91,1% pengguna [7]. Berkembangnya teknologi diiringi dengan banyaknya pengembangan aplikasi Android selalu menimbulkan masalah keamanan baru [1]. Hal ini menyebabkan munculnya aplikasi yang ada dan modifikasi baru membuat orang ingin mencoba fitur baru yang ditawarkan oleh berbagai aplikasi modifikasi, salah satunya adalah aplikasi chat pihak ketiga [8]. WhatsApp Mod merupakan versi WhatsApp yang sama seperti versi resmi pada umumnya.

Namun, perbedaannya terletak pada fitur-fiturnya. Ada beberapa orang yang memodifikasi atau menambahkan fitur yang tidak ada di WhatsApp resmi. Istilah "Mod" sendiri merujuk pada modifikasi, yang berarti melakukan perubahan atau penyesuaian pada aplikasi tersebut [9]. Dengan semua fitur standar WhatsApp Mod, termasuk kemampuan untuk mengubah tampilan, meningkatkan privasi, dan kemampuan untuk mengubah emoji atau font, penggunaan WhatsApp Mod dapat melanggar ketentuan penggunaan WhatsApp resmi. Modifikasi tersebut dapat dimanfaatkan oleh beberapa individu untuk menyisipkan kode yang mencuri data pengguna dan membebani kinerja perangkat. Mereka dapat mengeksploitasi perangkat dengan tujuan mendapatkan akses dan informasi pengguna untuk kepentingan pribadi, merugikan pengguna yang memiliki informasi pribadi tersebut [10]. Oleh karena itu, banyak orang beralih menggunakan WhatsApp mod yang dianggap memiliki keunggulan lebih dibandingkan versi resmi WhatsApp [11].

Berdasrkan latar belakang yang telah dipaparkan diatas maka penelitian ini melakukan analisis kemanan terhadap aplikasi whatsapp menggunakan metode analisis statis dengan tools Mobile Security Framework (MobSF). Mobile Security Framework (MobSF) adalah sebuah kerangka pengujian otomatis yang bersifat open-source. MobSF mampu melakukan analisis baik secara statis maupun dinamis terhadap aplikasi Android. Proses analisis yang dilakukan oleh MobSF menghasilkan laporan yang memberikan informasi detail mengenai aplikasi Android yang dianalisis [12]. Dengan menggunakan MobSF untuk melakukan analisis keamanan, diharapkan bahwa hasil analisis tersebut dapat meningkatkan kesadaran pengguna aplikasi agar menghidari penggunaan aplikasi ilegal agar terhindar dari kebocoran data yang dapat merugikan pengguna.

1.2 Rumusan Masalah

1. Apa perbedaan mendasar dalam hal keamanan antara aplikasi android Whatsapp versi resmi dengan versi modifikasi.
2. Bagaimana perbandingan nilai tingkat keamnan antara aplikasi Whatsapp resmi dengan versi modifikasi.

1.3 Batasan Masalah

Batasan masalah yang digunnakan untuk mempersempit permasalahan yang diangkat pada skripsi ini diberikan batasan-batasan yaitu :

1. Menggunakan aplikasi Whatsapp_2.23.13.76.apk dan GBWhatsApp_2.22.22.222_ggad_01_17_1540.apk sebagai permasalahan utama yang diangkat.
2. Menggunakan *Mobile Security Framework (MobSF)* sebagai framework pendeteksi keamanan aplikasi android yang digunakan.
3. Menggunakan Static analysis sebagai metode analisis.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini :

1. Untuk kemajuan dan pengembangan ilmu pengetahuan.
3. Untuk mengetahui potensi kerentanan, kelemahan, dan resiko keamanan pada aplikasi Whatsapp resmi dan Whatsapp versi modifikasi.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat menjadi refrensi bagi peneliti selanjutnya sehingga dapat menunjang perkembangan pengetahuan pada bidang analysis security dan dapat menjadi refrensi bagi peneliti lain sebagai acuan dan bahan pertimbangan bagi yang melakukan penelitian serupa.

1.6 Sistematik Penulisan

Bab I Pendahuluan, berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan sistematik penulisan.

Bab II Tinjauan Pustaka, berisi hasil penelitian sejenis yang pernah dilakukan sebelumnya, Penguraian mengenai aspek-aspek terkait analisis WhatsApp, dan penjelasan tentang tools yang digunakan dalam proses analisis.

Bab III Metodelogi Penelitian,berisi : berisi penjelasan mengenai alur penelitian, tahap-tahap yang dilakukan dalam proses analisis statis pada objek penelitian , dan penggunaan alat dan bahan dalam penelitian.

Bab IV Pembahasan, berisi penjelasan hasil dari analisis yang sudah dilakukan pada aplikasi andorid whatsapp.

Bab V Penutup, beris kesimpulan dari hasil penelitian yang dilakukan dan saran.