I. PENDAHULUAN

I.1 Latar Belakang

Perkembangan layanan jaringan komunikasi secara *online* meningkat pesat seiring bermunculannya situs-situs dan aplikasi berbasis web yang diminati oleh banyak pengguna Internet di seluruh dunia. WhatsApp Messenger merupakan contoh aplikasi layanan komunikasi berbasis Internet untuk pengguna smartphone dengan fitur telepon, video *call/converence*, dan *chatting*. Dalam beberapa tahun terakhir, komunikasi WhatsApp banyak digunakan oleh individu, perusahaan dan instansi. WhatsApp merupakan aplikasi pesan yang paling banyak digunakan secara global oleh lebih dari 600 juta pengguna di dunia, pada Oktober 2014 [1]. Memang tidak mengejutkan karena WhatsApp menyediakan layanan komunikasi pesan antar *mobile* dengan harga layanan yang murah.

Dengan kegunaan dan manfaat yang bisa didapatkan dengan mudah oleh semua orang memunculkan pertanyaan mengenai tingkat keamanan pada aplikasi tersebut. Komunikasi WhatsApp memiliki isu-isu keamanan antara lain pada Mei 2011 dilaporkan terdapat lubang pada keamanan akun pengguna WhatsApp dimana komunikasi tersebut tidak terenkripsi dan data yang ditransmisikan merupakan plaintext [2][3], pada 6 Januari 2012 *hacker* yang tidak diketahui identitasnya telah mempublikasikan situs webnya yang menjelaskan cara yang memungkinkan pengguna untuk mengubah status pengguna WhatsApp lain selama nomor telepon target diketahui [4], pada Mei 2012 peneliti keamanan mendapatkan *update*-an terbaru bahwa WhatsApp tidak lagi mengirimkan data secara plaintext [5][6][7] namun metode kriptografi yang diimplementasikan rusak [8][9], dan isu-isu keamanan lainnya mengenai aplikasi WhatsApp. Oleh karena itu, aplikasi WhatsApp perlu dilakukan analisa dan pengujian terhadap sistem kemamanannya. Metode pengujian penetrasi diajukan untuk meneliti kerentanan sistem otentikasi WhatsApp dan mengevaluasi tingkat potensial kerentanan.

Metode pengujian penetrasi adalah sebuah metode untuk menguji kerentanan dan metode verifikasi yang dapat meniru serangan aktif dan melakukan eksploitasi dengan membangun kasus pengujian penetrasi yang efektif dan ringkas. Metode yang disajikan dapat menentukan kelayakan serangan dan mengevaluasi keamanan sistem otentikasi. Metode yang diusulkan dapat berfungsi sebagai calon yang layak dan efektif untuk deteksi keamanan sistem otentikasi [10].

Namun pada aplikasi seperti WhatsApp aspek keamanannya terdapat pada area studi yang belum dipelajari secara mendalam. Maka dari itu dibutuhkan pengujian untuk mengetahui tingkat keamanan aplikasi WhatsApp.

Tahapan yang akan dilakukan yaitu pengujian keamanan pada aplikasi WhatsApp dengan menggunakan standar pembuktian keamanan aplikasi (ASVS) yang dikeluarkan oleh OWASP pada tahun 2014 [11].

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, berikut uraian permasalahan yang diangkat pada penelitian ini:

1. Bagaimana mengetahui tingkat keamanan aplikasi WhatsApp?
2. Bagaimana mendetailkan penggunaan standar *Application Security Verification Standard* (ASVS) yang dikeluarkan oleh OWASP (*Open Web Application Security Project*)?

I.3 Tujuan

Tujuan yang akan dicapai pada penelitian ini adalah:

1. Melakukan pengujian dengan metode *penetration testing* untuk menganalisa tingkat keamanan pada aplikasi WhatsApp menggunakan standar ASVS.
2. Mengumpulkan bukti yang didapat berdasarkan metode dari OWASP.
3. Melakukan analisis pada setiap tahap pengujian dan menentukan tingkatan keamanan aplikasi yang diujikan yaitu antara termasuk dalam kategori 'tidak terpenuhi' atau 'terpenuhi' berdasarkan hasil pembuktian.
4. Melakukan pemetaan dari tingkatan yang didapat dari hasil penelitian ke tingkatan standar pembuktian (ASVS), kemudian melakukan analisis untuk mendapatkan hasil akhir tingkatan kemanan dari aplikasi WhatsApp.
5. Membuat daftar *countermeasures* berdasarkan kerentanan yang terdeteksi dari hasil penelitian yang dilakukan.

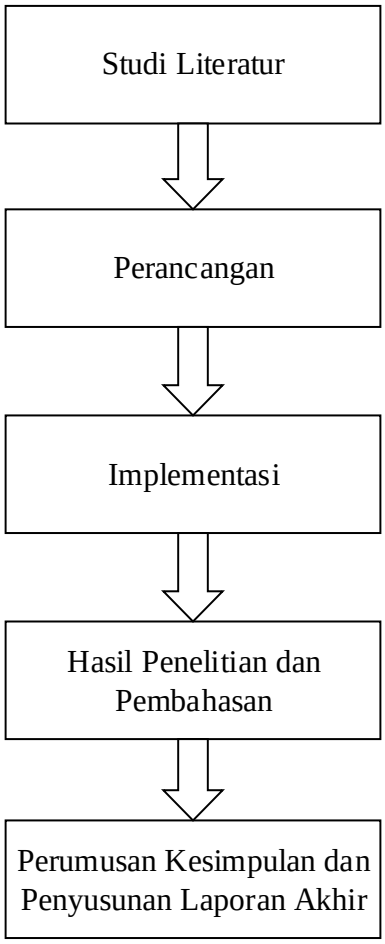
I.4 Batasan Masalah

Berikut merupakan batasan masalah dari tugas akhir ini:

1. Metode utama yang dilakukan pada penelitian Tugas Akhir ini adalah pengujian penetrasi (*penetration testing*) dan metode pembuktian yang dilakukan berdasarkan standar pembuktian keamanan aplikasi yang dikeluarkan oleh OWASP pada tahun 2014, dengan disesuaikan oleh studi kasus dan batasan masalah.
2. Penelitian terfokus pada aplikasi WhatsApp berbasis Android.
3. Aplikasi WhatsApp yang digunakan adalah versi 2.12.376, dan Android yang digunakan adalah KitKat versi 4.4.4.
4. Tidak melakukan kesepakatan atau *agreement* dengan pihak perusahaan WhatsApp.

I.5 Metodologi penyelesaian masalah

Berdasarkan rumusan masalah diatas, berikut merupakan metodologi penelitian untuk mencapai penyelesaian masalah:



Gambar I-1 Metodologi Penyelesaian Masalah

a. Studi Literatur
   Pada tahap ini akan dilakukan pengumpulan informasi (*information gathering*) yaitu pencarian materi-materi yang berkaitan dengan penelitian guna mendukung penulisan tugas akhir. Referensi yang menjadi acuan antara lain jurnal, paper, artikel, maupun buku mengenai pengujian penetrasi dan metode pembuktian untuk menganalisis tingkat keamanan aplikasi WhatsApp.
b. Perancangan
   Pada tahap ini, akan dilakukan pemodelan ancaman (*threat modeling)* yaitu mengidentifikasi ancaman pada aplikasi WhatsApp, kemudian menjabarkan daftar ancaman tersebut untuk dijadikan materi penelitian. Terdapat pula penjelasan langkah-langkah penggunaan *tools* yang akan dipakai untuk melakukan analisa kerentanan (*vulnerability analysis)* sesuai dengan daftar ancaman. Daftar ancaman yang akan dijadikan materi penelitian yaitu berdasarkan daftar kebutuhan pembuktian tingkat keamanan aplikasi *mobile* sesuai standar ASVS.
c. Implementasi
   Pada tahap ini akan dilakukan analisa kerentanan (*vulnerability analysis)* yaitu mengidentifikasi kerentanan pada aplikasi dengan kasus-kasus

pengujian yang telah dibuat sebelumnya, kemudian mengeksekusi kasus-kasus pengujian tersebut.

d. Hasil Penelitian dan Pembahasan
   Tahap ini peneliti akan menampilkan hasil dari penelitian yaitu analisa kerentanan yang telah dilakukan, kemudian melakukan penilaian kerentanan (*vulnerability assessment)* berdasarkan hasil penelitian tersebut sesuai standar pembuktian keamanan aplikasi yang dikeluarkan oleh OWASP (*The Open Web Application Security Project*) pada tahun 2014.
e. Perumusan Kesimpulan dan Penyusunan Laporan Tugas Akhir
   Pada tahap ini akan dilakukan perumusan kesimpulan berupa hasil tingkat keamanan yang didapat dari tingkatan dari proses penelitian yang dipetakan ke tingkatan ASVS dan saran *countermeasures* berdasarkan kerenatan yang terdeteksi, dan saran pengembangan penelitian ini untuk dilakukan di kemudian hari, lalu melakukan penyusunan tugas akhir, dan pengumpulan dokumen.

I.6 Sistematika Penulisan

Berikut merupakan sistematika penulisan pada buku tugas akhir ini, yaitu,

1. Bab I : Latar Belakang, Perumusan Masalah, Tujuan, Batasan Masalah, Metodologi Penyelesaian Masalah, Sistematika Penulisan
2. Bab II : Pengertian Pengujian Penetrasi, Standar Pembuktian Keamanan Aplikasi (2014) (*Application Security Verification Standard* (2014)), Panduan Pengujian Keamanan Aplikasi *Mobile*, Wireshark, *Code Audit*, Pengertian dan Proses Validasi Sertifikat (*Certificate)*, dan *WhatsApp*
3. Bab III: Gambaran Umum Sistem; Penggunaan Standar Pembuktian Keamanan Aplikasi (*Application Security Verification Standard*); Rancangan Sistem: Proses Pembuktian berdasarkan Lampiran 1 pada nomor urut 1, 3, 4, 7, 9, 11, 13, 14, 15, 21, 23, 25, 26, dan nomor urut 1 untuk area Komunikasi; dan Kebutuhan Sistem
4. Bab IV: Hasil Penelitian dengan Metode Pengujian Penetrasi dari Standar OWASP pada Aplikasi WhatsApp, Penilaian Tingkat Keamanan Aplikasi WhatsApp, Pemetaan dari Tingkatan pada Hasil Penelitian ke Tingkatan ASVS, dan Daftar *Countermeasures* berdasarkan Kerentanan-Kerentanan yang Terdeteksi
5. Bab V : Kesimpulan, Saran