BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan *smartphone* di Indonesia telah berkembang dengan pesat. Indonesia bahkan tercatat sebagai negara dengan jumlah pengguna *smartphone* terbesar keempat setelah Cina, India, dan Amerika Serikat (Statista Research Department, 2022). Bahkan, secara global pertumbuhan pengguna *smartphone* mencapai 5,3 miliar pada juli tahun 2021 (Kranjec, 2021).

Berdasarkan riset dari (Hootsuite (We Are Social), 2022) perangkat *mobile* yang terhubung di Indonesia mengalami peningkatan sebesar 370,1 juta yang mana meningkat sebesar 3,6% dari tahun sebelumnya. Peningkatan ini mempengaruhi penggunaan aplikasi yang juga meningkat pesat. Tercatat terdapat 2,68 juta aplikasi yang tersedia di Google playstore (Ceci, 2022). Aplikasi yang ditawarkan beraneka ragam mulai dari sosial media, *e-commerce*, hingga *m-banking*.

Dengan adanya peningkatan tersebut maka risiko kerentanan pada aplikasi juga semakin meningkat. Tercatat bahwa serangan siber terhadap organisasi meningkat sebesar 13% yang mana serangan tersebut menargetkan perangkat *mobile* (Parks, 2021). Hal ini dapat menjadi celah keamanan bagi para *threat actor* untuk melakukan serangan dan mengeksploitasi data-data sensitif pada aplikasi. Maka dari itu aplikasi harus mempunyai keamanan yang mumpuni, mengingat sebagian besar aplikasi menyimpan data pribadi seperti *username*, *password*, NIK, data pembayaran, dan lainnya (Aljawarneh et al., n.d.). Pencegahan terhadap serangan dapat dilakukan dengan melakukan pengujian keamanan untuk mengetahui kerentanan apa saja yang ada dalam aplikasi dan dapat membantu meningkatkan keamanan aplikasi (Alanda et al., 2020). Salah satu metode untuk melakukan pengujian kemanan pada aplikasi

mobile adalah *Open Web Application Security Project(OWASP) mobile application security testing guide.*

OWASP merupakan komunitas yang didirikan pada 21 April 2004 yang mempunyai tujuan untuk melawan serangan siber dan kerentanan, juga memberikan informasi dan beragam *tools* secara gratis (Fajaryanto et al., 2015). Pada 2018, OWASP membuat panduan tentang pengujian keamanan pada aplikasi *mobile* yang dikemas dalam OWASP *Mobile App Security Testing Guide*(MASTG). OWASP MASTG merupakan standar pengujian keamanan yang digunakan untuk aplikasi *mobile* yang dilengkapi dengan panduan mulai dari proses, teknik, alat, dan studi kasus terkait pengujian keamanan pada aplikasi *mobile* (Carlos et al., 2022).

Aplikasi PRIFAT adalah sebuah aplikasi *mobile* yang menyediakan *platform* untuk jasa instruktur atau pengajar di bidang seni, olahraga, dan musik. Dalam aplikasi PRIFAT pengguna dapat memilih *role* siswa atau pengajar. Pengguna dengan *role* siswa dapat memilih dan memesan pengajar berdasarkan bidang maupun rating dari si pengajar. Setelah memesan maka murid dapat membayar biaya instruktur dan dapat mengikuti pelatihan secara daring maupun luring. Pengguna dengan *role* pengajar dapat mendaftarkan dan mempromosikan jasanya sebagai pengajar dan mempromosikan *event* pelatihan. Pengajar akan mendapat bayaran saat ada siswa yang melakukan pendaftaran pada kelas yang dibukanya. Dari berbagai macam fitur tersebut aplikasi PRIFAT menyimpan banyak data-data privasi seperti *username*, *password*, NIK, NPWP, data akun bank, alamat tempat tinggal, dan tanggal lahir, yang mana data tersebut termasuk kedalam data pribadi yang harus dijaga kerahasiaannya. Berdasarkan uraian diatas maka isu keamanan aplikasi PRIFAT menjadi sangat penting, karenanya diperlukan pengujian keamanan aplikasi *mobile.* Tujuan pengujian ini adalah untuk pencegahan terhadap serangan dari *threat actor* dengan mengetahui kerentanan dan kelemahan

aplikasi dan memberikan rekomendasi keamanan untuk meminimalisir tingkat kerentanan pada aplikasi PRIFAT.

Berdasarkan latar belakang tersebut, penulis melakukan penelitian dengan judul **"PENGUJIAN KEAMANAN APLIKASI MOBILE BERBASIS ANDROID MENGGUNAKAN OWASP MOBILE APPLICATION SECURITY TESTING GUIDE (MASTG) (STUDI KASUS: PT PRIFAT TALENTA INDONESIA)".** Penelitian ini bertujuan untuk melakukan pengujian keamanan aplikasi *mobile* PRIFAT dengan menerapkan metode OWASP MASTG.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukakan diatas, masalah dapat diidentifikasi sebagai berikut:

1. Bagaimana melakukan pengujian keamanan pada aplikasi *mobile* berbasis android?
2. Bagaimana mengetahui kerentanan keamanan apa saja yang terdapat pada aplikasi *mobile* PRIFAT?
3. Bagaimana menentukan daftar rekomendasi kerentanan keamanan yang perlu diperbaiki pada aplikasi *mobile* PRIFAT?

1.3 Tujuan Penelitian

Berdasarkan identifikasi masalah yang telah dijabarkan diatas, penelitian ini memiliki tujuan, yaitu:

1. Melakukan pengujian keamanan aplikasi *mobile* berbasis android dengan menggunakan metode OWASP *mobile application security testing guide*.
2. Melakukan klasifikasi kerentanan yang ditemukan pada aplikasi *mobile* PRIFAT berdasarkan OWASP *mobile top ten* 2016.
3. Membuat rekomendasi perbaikan keamanan berdasarkan pada kerentanan yang ditemukan pada aplikasi *mobile* PRIFAT.

1.4 Manfaat Penelitian

Berdasarkan latar belakang yang telah dikemukakan diatas, manfaat dari penelitian ini adalah sebagai berikut:

1. Dengan dilakukannya pengujian keamanan pada aplikasi *mobile* PRIFAT ini maka dapat diketahui kerentanan apa saja yang terdapat pada aplikasi ini.
2. Berdasarkan kerentanan yang ditemukan dapat dilakukan perbaikan keamanan pada aplikasi *mobile* PRIFAT sehingga membuat aplikasi lebih aman.
3. Dengan aplikasi yang lebih aman dapat melindungi data-data yang penting dalam aplikasi PRIFAT.

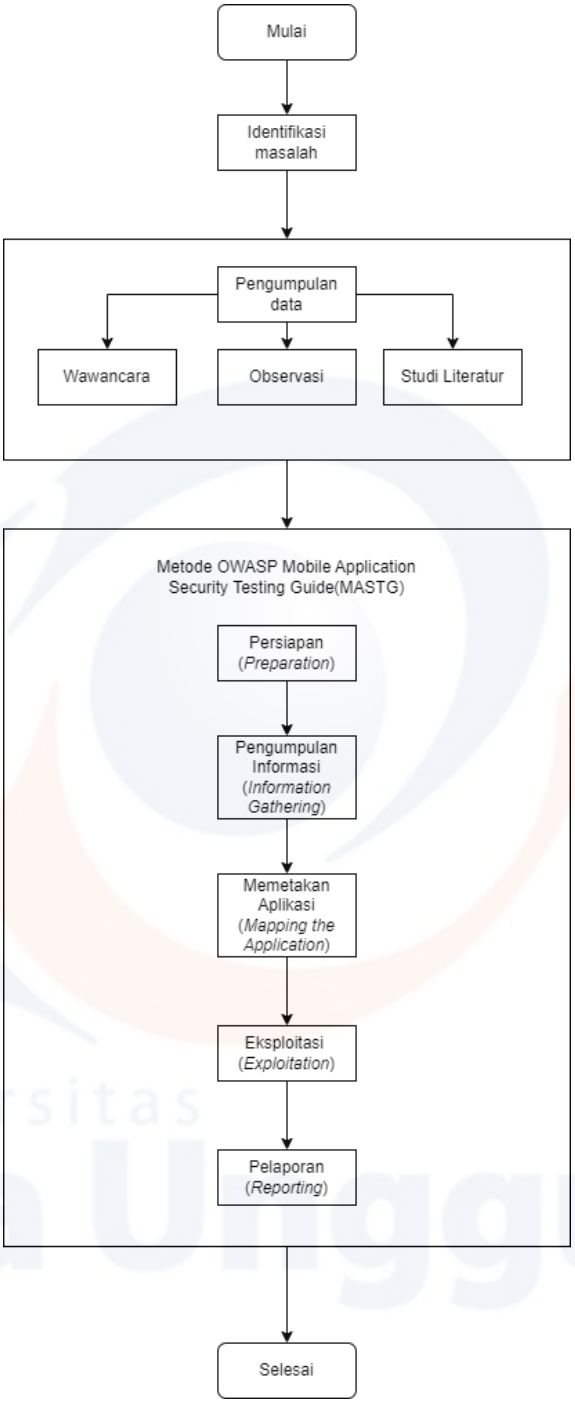
1.5 Lingkup Tugas Akhir

Ruang lingkup pembahasan diutamakan pada masalah-masalah dalam lingkup tugas akhir ini, antara lain:

1. Pengujian keamanan akan dilakukan pada aplikasi *mobile* android PRIFAT
2. Pengujian keamanan tidak dilakukan pada backend aplikasi PRIFAT.
3. Metode yang digunakan adalah OWASP *mobile application security testing guide.*
4. Kerentanan yang diuji hanya yang termasuk ke dalam OWASP *mobile top ten* 2016.

1.6 Kerangka Berfikir

Kerangka berfikir adalah gambaran sebuah penelitian yang digambarkan dari awal penelitian hingga akhir. Berikut merupakan kerangka berfikir pada penelitian yang dijelaskan pada gambar sebagai berikut:



Gambar 1. 1 *Kerangka Berfikir*

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini diuraikan dalam 5 (lima) bab dan mengenai isi bab-bab tersebut diuraikan sebagai berikut:

BAB 1: PENDAHULUAN

Pada bab ini berisikan Latar Belakang penelitian, identifikasi masalah, Tujuan penelitian, Manfaat penelitian, Ruang Lingkup, Kerangka Berfikir dan Sistematika Penulisan.

BAB 2: TINJAUAN PUSTAKA

Bab ini membahas teori-teori yang berhubungan dengan penelitian yang mencakup kajian pustaka dari beberapa penelitian yang pernah dilakukan sebelumnya dan landasan teori dari yang terkait dengan masalah penelitian dan metode yang digunakan pada penelitian.

BAB 3: METODE PENELITIAN

Pada bab ini berisi pembahasan atau pemaparan metode yang digunakan dalam penelitian dan menjelaskan langkah-langkah dalam melakukan penelitian.

BAB 4: HASIL DAN PEMBAHASAN

Pada bab ini akan dilakukan penjelasan dan pembahasan mengenai hasil dari pengujian keamanan pada aplikasi PRIFAT.

BAB 5: KESIMPULAN DAN SARAN

Pada bab ini berisi mengenai garis besar kesimpulan yang dibuat oleh penulis dan saran-saran yang diusulkan untuk meingkatkan keamanan pada aplikasi.