BAB 1 PENDAHULUAN

1.1. Latar Belakang

Perkembangan transformasi digital global telah mengubah cara perguruan tinggi di Indonesia menyediakan layanan kepada akademisi [1]. Hal ini dapat dilihat dari berbagai perguruan tinggi terkemuka seperti Institut Teknologi Bandung (ITB), Universitas Indonesia (UI), Universitas Gadjah Mada (UGM), dan Universitas Telkom, yang telah mengembangkan sistem informasi akademik berbasi mobile yang meningkatkan aksebilitas layanan kampus. Informasi sensitif seperti data pribadi, akses kredensial, dan informasi pendidikan disimpan dan dikelola melalui aplikasi mobile ini [2].

Di sisi lain, beberapa studi menyoroti masalah dalam aplikasi mobile. Titiakarawongse *et al*. [3] menyatakan bahwa peningkatan penggunaan aplikasi mobile juga meningkatkan risiko keamanan dalam penanganan data sensitif. Utama *et al*. [4] menyatakan bahwa sebagian besar institusi pendidikan tinggi tidak memiliki prosedur standar untuk mengevaluasi keamanan aplikasi mobile mereka. Kesenjangan saat ini adalah perbedaan signifikan dalam kerentanan di antara beberapa aplikasi mobile kampus dan bagaimana perbedaan ini memengaruhi keamanan data di sektor pendidikan, yang merupakan masalah besar.

Terdapat berbagai framework yang dapat menguji kerentanan dalam aplikasi mobile, termasuk aplikasi mobile kampus. Di antara framework tersebut, OWASP (*Open Web Application Security Project*) menawarkan berbagai pendekatan yang lebih spesifik, seperti OWASP Mobile Top 10 2024, yang dirancang khusus untuk mengidentifikasi dan menangani risiko kerentanan dalam aplikasi mobile. Keunggulan OWASP Mobile Top 10 2024 terleta pada cakupan risiko kerentanan yang luas, rutinitas pembaruan, dan dukungan luas dari komunitas global [5], sehingga menjadikannya pilihan yang tepat sebagai

alat keamanan aplikasi mobile kampus. Dalam beberapa studi yang dilakukan pada aplikasi mobile kampus, seperti yang dilakukan oleh Dhingraa *et al*. [6], disebutkan bahwa OWASP Mobile Top 10 merupakah tolok ukur global yang diakui untuk mengklasifikasikan kerentanan kerentanan keamanan aplikasi mobile. Dalam studi lain, Wicaksono *et al*. [7] mencatat bahwa framework ini memiliki metodologi sistematis untuk mengidentifikasi dan mengevaluasi kerentanan aplikasi mobile, terutama dalam konteks pendidikan. Meskipun banyak studi telah menyoroti pentingnya OWASP Mobile Top 10 secara global, penerapan framework ini di sektor pendidikan masih terbatas, terutama di Indonesia. Oleh karena itu, penelitian ini menggunakan kesempatan untuk memanfaatkan OWASP Mobile Top 10 2024 sebagai framework yang dapat berfungsi sebagai acuan untuk mengklasifikasikan kerentanan pada aplikasi mobile di lingkungan kampus.

Studi ini menggunakan OWASP Mobile Top 10 2024 untuk melakukan analisis perbandingan antara aplikasi mobile kampus di berbagai universitas, mulai dari universitas negeri hingga swasta. Dalam pelaksanaanya, diperlukan alat untuk menilai kerentanan aplikasi mobile kampus. Studi ini menggunakan tiga alat pengujian keamanan aplikasi statis (SAST): Androbugs, *Mobile Security Framework* (MobSF), dan *Quick Android Review Kit* (QARK) sebagai alat unutk peniliaian kerentana pada aplikasi mobile kampus. Ketiga alat ini dipilih karena kemampuannya mendeteksi berbagai jenis kerentanan yang tercakup dalam OWASP Mobile Top 10 2024. Dengan membandingkan hasil analisis kerentanan pada aplikasi mobile kampus yang berbeda, penelitian ini bertujuan untuk mengidentifikasi pola kerentanan yang umum dan merekomendasikan perbaikan berdasakan standar keamanan OWASP Mobile Top 10 2024. Ruang lingkup studi ini hanya membatasi penggunaan penilaian aplikasi mobile pada platform Android saja. Aplikasi iOS tidak termasuk karena perbedaan arsitektur antara Android dan iOS. Selain itu, studi ini hanya berfokus pada analisis statis dan tidak termasuk analisis dinamis.

Sejauh yang kami ketahui, belum pernah ada studi yang secara komprehensif membandingkan analisis kerentana pada aplikasi mobile dengan framework OWASP Mobile Top 10 2024 di Indonesia. Studi sebelumnya lebih berfokus pada satu aplikasi atau satu institusi, tanpa membandingkan antara universitas dan tanpa juga menggunakan pendekatan multi-alat dalam deteksi kerentanan. Selain itu, sebagian besar studi yang ada dilakukan pada sektor lain seperti sektor perbankan, kesehatan, atau e-commerce, yang memiliki karakteristik dan kebutuhan keamanan yang berbeda dari lingkungan akademik. Oleh karena itu, daftar berikut ini merupakan kontribusi dari studi ini:

1. Metodologi penelitian yang memperkuat bahwa Androbugs, MobSF, dan QARk daapt diandalkan untuk menguji M2 (Inadequate Supply Chain Security), M6 (Inadequate Privacy Controls), dan M8 (Security Misconfiguration) dalam kategori OWASP Mobile Top 10 2024.
2. Pengetahuan bahwa QARK adalah alat SAST yang menghasilkan berbeda dalam mendeteksi kerentanan dibandingkan dengan Androbugs dan MobsF.
3. Pengetahuan bahwa kerentanan M6 dan M8 dalam kategori OWASP Mobile Top 10 2024, yaitu Inadequate Privacy Controls dan Security Misconfiguration, masing-masing, memerlukan perhatian paling bersar pada aplikasi mobile kampus, terutama dari empat kampus Indoensia: Universitas Telkom, ITB, UI, dan UGM.

Sisa studi ini memiliki struktur sistematis: Bab 2 untuk membahasa penelitian terkini terkait topik ini; Bab 3 menjelaskan metodologi penelitian; Bab 4 menyajikan hasil dan mendiskusikannya; dan Bab 5 menyimpulkan hasil temuan penelitian dan memberikan sara untuk penelitian selanjutnya.

1.2. Rumusan Masalah

- Bagaimana mengidentifikasi kerentanan keamanan pada aplikasi mobile kampus menggunakan tools AndroBugs, MobSF, dan QARK?

- Bagaimana hasil temuan kerentanan dari tools tersebut dapat dipetakan ke dalam framework OWASP Mobile Top 10?
- Bagaimana membandingkan profil kerentanan antar aplikasi mobile kampus yang diuji?

1.3. Tujuan dan Manfaat

Penelitian ini diharapkan dapat memberikan pengetahuan bagaimana kerentanan dapat teridentifikasi menggunakan alat SAST. Kedua, mempetakan hasil kerentanan yang ditemukan alat SAST ke dalam kategori OWASP Mobile Top 10 2024. Ketiga, membandingkan profil kerentanan antar aplikasi mobile menggunakan analisis statistik.

1.4. Batasan Masalah

- Penelitian hanya berfokus pada 4 aplikasi mobile kampus berbasis Android: MyTel-U, MySIX ITB, We Are UI, dan Simaster UGM, tidak termasuk versi iOS atau platform lainnya.
- Analisis keamanan hanya menggunakan 3 tools static application security testing (SAST): AndroBugs versi 1.0.0, MobSF versi 4.13, dan QARK versi 4.0.0.
- Analisis kerentanan hanya dilakukan pada aplikasi mobile (client-side) dan tidak mencakup pengujian langsung terhadap eksploitasi kerentanan yang ditemukan atau analisis keamanan server.

1.5. Metode Penelitian

Penelitian ini menggunakan pendekatan studi literature dan studi teorits untuk mengkaji framework OWASP Mobile Top 10 2024 dan juga alat SAST seprti Androbugs, MobSF, dan QARK. Kedua, menggunakan pengukuran empirik dengan empat aplikasi mobile kampus diuji menggunakan tiga alat SAST. Terakhir, data yang sudah diperoleh dianalisis menggunakan mean, standar deviasi, t-value, dan p-value.

1.6. Jadwal Pelaksanaan

Jadwal Pelaksaan Tugas Akhir di sajikan lewat Tabel 1.1

Tabel 1.1 Jadwal Pelaksaan Tugas Akhir

No.	Deskripsi Tahapan	Bulan 1	Bulan 2	Bulan 3	Bulan 4	Bulan 5	Bulan 6
1	Studi Literatur						
2	Pengumpulan Data						
3	Perancangan Sistem						
4	Pengujian						
5	Analisis						
6	Penyusunan Laporan/Buku TA						