BAB 1 PENDAHULUAN

1.1. Latar Belakang

Berdasarkan era digital yang semakin kompleks, aplikasi *mobile* telah menjadi bagian integral dari kehidupan sehari-hari. Aplikasi *mobile* seperti XYZ, yang memberikan berbagai informasi, seperti jadwal kuliah, *XYZ Calender*, *XYZ life*, *XYZTuc* dan bahkan ada fitur *timeline* yang berisikan forum untuk saling diskusi atau berbagi informasi terkait tugas, acara dalam kampus dan berbagai macam informasi lainnya yang digunakan oleh mahasiswa/i. Namun, dengan meningkatnya penggunaan aplikasi *mobile*, juga meningkatkan risiko serangan *cyber* yang dapat menyebabkan kerusakan data, keamanan, dan reputasi perusahaan yang berkaitan dengan unit XYZ. Serangan *cyber* dapat dilakukan dengan menggunakan berbagai metode, termasuk serangan sosial, *phishing*, dan serangan keamanan lainnya. Salah satu metode yang paling efektif dalam mendeteksi dan menghentikan serangan *cyber* adalah dengan menggunakan metode VAPT (*Vulnerability Assessment and Penetration Testing*). VAPT adalah proses yang digunakan untuk menemukan dan mengidentifikasi kelemahan keamanan dalam sistem, serta untuk mengetahui bagaimana serangan *cyber* dapat dilakukan melalui sistem tersebut.

Aplikasi XYZ ini resmi diluncurkan pada tahun 2021 bisa terbilang masih sangat baru. Jika dihitung dari tahun 2025 umur aplikasi XYZ ini masih masuk tahun ke-empat yang masih bisa dikembangkan lebih banyak lagi fitur-fitur yang akan datang. Dengan umurnya tergolong kurang dari lima tahun aplikasi XYZ ini harus lebih *aware* terhadap keamanan informasi aplikasi yang bisa saja terjadinya celah. Suatu aplikasi tentu saja tidak ada yang sempurna dan harus melakukan beberapa *upgrade* ataupun evaluasi [1]. Berdasarkan hasil wawancara dengan unit internal XYZ terdapat satu masalah yang ditemukan pada data dari *service* API yang seharusnya keamanannya menggunakan berupa token dan harus melakukan otorisasi. Namun pada saat itu tim internal XYZ belum menerapkannya. Tim internal XYZ juga pernah menemuka celah disaat JWT (*JSON Web Token*) tidak digunakan pada aplikasi yang menjadikan adanya celah yang ingin meretas aplikasi XYZ. Maka dari itu masih diperlukannya evaluasi dan analisis kerentanan dan

upaya mitigasi pada aplikasi XYZ ini.

Berdasarkan *study literature* penggunaan metode *Vulnerability Assessment and Penetration Testing* (VAPT) yang digunakan untuk memberikan analisis terhadap keamanan sistem melakukan identifikasi celah terhadap keamanan dan melakukan pengujian terhadap percobaan celah itu dengan mitigasi seperti penelitian *website* layanan universitas XYZ [1]. Hasil evaluasi dari metode ini yaitu laporan kerentanan yang bisa dijadikan dasar acuan untuk menentukan rekomendasi mitigasi untuk menghentikan kerentanan yang ditemukan seperi pada penelitian *website* kerja praktek dan pengabdian masyarakat (KPPM) Universitas XYZ [2]. Percobaan pada celah yang dilakukan oleh serangan tidak sah tidak bisa direncanakan ataupun kapan akan terjadi, akan tetapi dengan dilakukannya pencegahan pada celah tersebut keamanan pada sistem aplikasi bisa meningkat [3]. Maka dari itu, harus dilakukannya mitigasi keamanan untuk mengidentifikasi, mengeksploitasi, dan memitigasi kerentanan keamanan seperti yang ada pada *website* absensi praktikan dan asisten laboratorium praktek [4]. Pentingnya kesadaran *cybersecurity* untuk pengguna internet mahasiswa/i Indonesia dan yang terpenting mahasiswa/i XYZ University pada kerentanan yang ada di internet untuk bisa menjaga dari serangan *cyber* [5].

Selain melakukan indentifikasi pada analisis kerentanan dan upaya mitigasi dengan metode *Vulnerability Assessment and Penetration Testing* (VAPT) peneliti perlu menggunakan alat *MboFS* untuk menguji identifikasi tersebut. *MobSF* adalah *framework* yang digunakan untuk melakukan pengujian penetrasi pada aplikasi seluler (Android, iOS dan Windows). *MobSF* mampu melakukan berbagai jenis analisis, termasuk analisis statis, dinamis, serta deteksi *malware. Framework* ini dirancang untuk memberikan analisis keamanan yang cepat dan efisien pada aplikasi berbasis Androis, iOS, dan Windows, baik bentuk file biner (seperti APK, IPA, dan APPX) maupun kode sumber dalam format zip.

Tujuan penelitian ini adalah untuk memperdalam pemahaman tentang kerentanan dan keamanan dalam aplikasi *mobile* XYZ dan memunculkan ide-ide langkah mitigasi yang sesuai. Hasil dalam penelitian ini diharapkan dapat menghasilkan konsep baru dalam pemahaman tentang serangan yang terjadi terhadap aplikasi *mobile* dan strategi mitigasi yang efektif. Konsep baru yang

diharapkan sebagai hasil penelitian ini adalah mendeteksi dan menghentikan serangan *cyber* dengan metode VAPT yang lebih efektif dan efisien untuk mendeteksi dan menghentikan serangan *cyber* terhadap aplikasi mobile XYZ. Dengan menggunakan MobFS, aplikasi *mobile* XYZ dapat meningkatkan keamanan dan mencegah serangan *cyber* yang dapat dilakukan melalui XYZ tersebut. Gap antara kondisi saat ini dan kondisi yang akan datang terletak pada aplikasi *mobile* XYZ yang sering terjadinya *maintenance.* Kondisi ini menimbulkan kekhawatiran tentang kerentanan terhadap serangan *cyber*. Oleh karena itu, perlu dilakukan analisis kerentanan dan upaya mitigasi terhadap serangan dengan metode VAPT untuk mengentikan dan mencegah serangan *cyber* yang dapat dilakukan melalui aplikasi *mobile* XYZ. Pentingnya suatu penelitian terlebihnya dalam bidang Teknologi Informasi adalah bahwa penelitian ini dapat membantu meningkatkan keamanan dan mencegah serangan *cyber*. Selain itu, penelitian ini juga dapat membantu meningkatkan kesadaran dan kemampuan Mahasiswa/i Telkom University dalam menghadapi serangan *cyber*, serta meningkatkan keamanan dan kestabilan sistem pada aplikasi *mobile* XYZ.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah pada penelitian ini adalah:

a. Apa peranan metode VAPT dalam mendeteksi dan menghentikan serangan *cyber* terhadap aplikasi *mobile* XYZ?
b. Bagaimana MobFS dapat membantu dalam analisis kerentanan dan upaya mitigasi terhadap serangan dengan metode VAPT pada aplikasi *mobile* XYZ?

1.3. Tujuan

Berdasarkan rumusan masalah, maka tujuan dari penelitian ini adalah:

a. Efektivitas metode VAPT dalam mendeteksi dan menghentikan serangan *cyber* dengan menganalisis dan mengidentifikasi kerentanan yang ditemukan.

b. Hasil dalam efektivitas MboFS dalam menganalisis dan upaya mitigasi saat proses *vulnerability scanning*.

1.4. Ruang Lingkup

Berikut adalah ruang lingkup proposal penelitian yang berisi batasa-batasan pada penelitian proposal:

a. Penelitian ini akan menganalisis kerentanan dan upaya mitigasi pada aplikasi XYZ versi 2.0.0.
b. Menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT) sebagai tolak ukuran penelitian.
c. Penelitian ini menggunakan standar *OWAPS mobile Top 10 2024.*

1.5. Rencana Kegiatan

Rencana kegiatan untuk penelitian Analisis Kerentanan dan Upaya Mitigasi Terhadap Serangan dengan Metode VAPT pada aplikasi *mobile* XYZ Menggunakan MobFS adalah sebagai berikut:

a. Kajian literatur terkini mengenai serangan *cyber*, metode VAPT, dan MobFS.
b. Analisis kelemahan keamanan dalam sistem aplikasi *mobile* XYZ.
c. Pengumpulan data mengenai serangan *cyber* yang terjadi pada aplikasi *mobile* XYZ, termasuk informasi jenis serangan, kelemahan keamanan, dan dampak serangan.
d. Menganalisis kerentanan aplikasi *mobile* XYZ dengan menggunakan metode VAPT.
e. Pengujian efektivitas metode VAPT dan MobFS dalam mendeteksi dan menghentikan seragan *cyber*.
f. Menyimpulkan hasil penelitian untuk mengetahui efektivitas metode VAPT dan MobFS dalam mendeteksi dan menghentikan serangan *cyber*.

1.6. Jadwal Kegiatan

Table 1.1 Jadwal Kegiatan

Kegiatan	Bulan							
	4	5	6	7	8	9	10	11
Research dan Pengumpulan judul								
Penulisan Proposal Bab 1								
Research Review Literature								
Penulisan Proposal Bab 2 dan Perancangan Metodologi								
Penulisan Proposal Bab 3								
Pengumpulan Data								
Analisi Data								
Penyusunan Buku TA								