**Proposal Tugas Akhir**

|  |  |  |
| --- | --- | --- |
| **NIM** | **Nama** | **Persentase kontribusi** |
| 11320038 | Donianto Siahaan |  |
| 11320052 | Agnes Mebyolla Turnip |  |
| 11320058 | Vivi Nessa Tampubolon |  |

**Usulan judul (sementara) : Mobile Android App Security Testing**

**Pembimbing : Togu Novriansyah Turnip, S.S.T., MIM**

**Program studi : D3 Teknologi Informasi**

**Jenis Tugas Akhir : (Pengembangan perangkat lunak)**

**Matakuliah yang pernah diambil terkait dengan Tugas Akhir ini:**

* **Rekayasa Perangkat Lunak**
* **Pembangunan Perangkat Lunak**
* **Pengembangan Aplikasi Mobile**

# Latar Belakang

Sistem operasi perangkat mobile android adalah salah satu yang populer dan banyak digunakan di dunia. Pengguna android saat ini mencapai lebih dari 3 miliar pengguna aktif yang tersebar di seluruh dunia, hal ini disampaikan Sameer Samat selaku Vice President Google. Salah satu faktor yang menyebabkan android populer adalah sumber kodenya dirilis secara open source. Namun disisi lain android merupakan sistem operasi yang paling rentan sehingga banyak pihak yang tidak bertanggung jawab memanfaatkan celah keamanannya (Aldy et al., 2022). Hal tersebut dikarenakan aplikasi android bersifat *open sources* sehingga aplikasi bebas untuk diunduh melalui *play store* dan mudah dikembangkan oleh pengguna maupun pihak yang tidak bertanggung jawab yang memungkinkan dalam melakukan hal – hal yang merugikan pengguna android. Terdapat beberapa ancaman keamanan seperti *Malware, Denial of ServiceAttacks, Colluding, repackinging apps to inject malicious code, pemission escalation,* dan *unauthorize* antar aplikasi (Ahmed & Sallow, 2017). Dalam memastikan keamanan data pada aplikasi mobile khususnya android diperlukan adanya pengujian keamanan.

Terdapat banyak aplikasi yang dapat melakukan pengujian keamanan. Hampir setiap aplikasi seluler berbicara tentang layanan backend, dan layanan tersebut rentan terhadap jenis serangan yang sama seperti aplikasi web pada desktop. Namun aplikasi seluler berbeda karena permukaan serangan yang lebih kecil dan karenanya lebih aman terhadap injeksi dan serangan serupa. Sebaliknya yang menjadi prioritas adalah perlindungan data dan jaringan dalam meningkatkan keamanan seluler. *Open Web Application Security Project (*OWASP*) Mobile Security Testing Guide (*MSTG*)* adalah salah satu metode yang menyediakan panduan dalam melakukan proses pengujian keamanan terhadap aplikasi perangkat seluler yang memiliki sistem operasi iOS maupun android (Yumnun et al., 2020). OWASP (MASVS) mendefinisikan model keamanan aplikasi seluler dan mencantumkan persyaratan keamanan umum untuk aplikasi seluler. Ini dapat digunakan untuk mendefinisikan dan memahami kualitas aplikasi seluler yang aman. MSTG memetakann ke perangkat dasar persyaratan keamanan yang sama yang ditawarkan oleh MASVS dan tergantung pada konteksnya, kedua hal tersebut dapat digabungkan untuk mencapai tujuan yang berbeda (Bernhard Mueller, Scen Schleier, 2018).

Sebuah penelitian yang membahas tentang celah keaman aplikasi android. Pada penelitian Fitrinurindasari dan Bita yang berjudul : ”Security Static Analysis Of Android-Based Vidio Streaming Application Using Mobile Security Framework (MOBSF)”. Penelitian ini berfokus untuk menemukan celah keamanan yang terdapat pada aplikasi vidio streaming berbasis android dengan metode kuantitatf. Komponen yang diteliti meliputi permissions, weak crypto, root detection, SSL bypass, dan domain malware check dengan menggunakan mobiile security framework dan dilakukan analisis statik. Sehingga disimpulkan bahwa aplikasi Y (inisial) yang tidak memiliki root detection. Namun pada penelitian tersebut tidak menjelaskan keefektifan dari MOBSF dalam melakukan pengujian keamanan terhadap sebuah aplikasi android. Penelitian yang diharapkan oleh penulis adalah peneliti selanjutnya dapat melakukan analisis aplikasi vidio streaming lainnya dengan mengunakan metode analisis lainnya, sehingga dapat memberikan kesadaran terhadap masyarakat untuk menyadari akan resiko keamanan.

Pada pengerjaan tugas akhir ini akan dilakukan metode kuantitatif dengan uji analisis statik terhadap tingkat akurasi aplikasi android yang dapat melakukan deteksi celah keamanan aplikasi lain. Salah satu penelitian Wei Wang, Meichen Zhao, Zhenzhen Gao, Guangquan Xu, Hequn Xian, Yuanyuan Li, Xiangliang Zang yang berjudul ”*Constructing Features for Detectiing Android Malicious Applications: Issues, Taxonomy and Directions”*. Penelitian tesubut memberikan survai dan penjelasan tentang malicious apps (malapps) dengan berbagai jenis fitur (Wang et al., 2019). Penelitian tersebut menyatakan bahwa dengan analisis statis dapat menghemat waktu dan sumber daya. Dengan demilian metode ini relatif lebih cepat. Uji analisis akan dilakukan ke beberapa aplikasi keamanan berbasis android dengan acuan *OWASP Mobile Secutiry Testing Guide*. Adapun hasil yang diharapkan dalam penelitian ini adalah mengetahui tingkat akurasi dari aplikasi – aplikasi keamanan berbasis android dan dapat merekomendasikan aplikasi keamanan yang paling tepat sesuai dengan kebutuhan.

# Tujuan

Adapun tujuan yang ingin dicapai penelitian ini adalah dapat melakukan mengujian dan analisis terhadap aplikasi keamanan yang berbasis android sesuai dengan standard keamanan aplikasi OWASP MASVS (Mobile Application Security Verification Standard). Sehingga dari penelitian ini pembaca dapat mengetahui tingkat bagaimana keakuratan aplikasi keamanan yang digunakan. Sehingga dapat meningkatkan kepeduli terhadap keamanan data dan cara dalam mencegah celah keamanan.

# Ruang Lingkup

Pada penelitian ini akan dilakukan pengujian terhadap beberapa aplikasi keamanan berbasis android. OWASP MSTG akan memetakan ke perangkat dasar persyaratan keamanan yang ditawarkan oleh MASVS pada pengujian aplikasi. Adapun cakupan dalam keamana aplikasi mobile itu sendiri meliputi : Local Data Storage, Communication with Trusted Endpoints , Authentication and Authorization, Interaction with the Mobile Platform, Code Quality and Exploid Mitigation dan Anti-Tampering/Anti-Reversing.

# Research Question

Adapun rumusan masalah dari penelitian Tugas Akhir ini adalah ;

1. Bagaimana standard keamanan aplikasi mobile saat ini ?
2. Apa yang menjadi acuan bahwa sebuah aplikasi disebutkan memiliki keamanan yang baik ?
3. Aplikasi keamanan manakah yang memiliki tingkat akurasi menajaga keamanan yang paling baik ?

# Metodologi Penelitian

Adapun pendekatan penelitian yang digunakan dalam menyelesaikan tugas akhir ini dapat dilihat pada Gambar 1.

1. Pernyataan Masalah

Tahapan pernyataan masalah merupakan tahap menentukan topik, menentukan permasalahan yang terdapat pada topik penelitian, dan menemukan poin-poin yang penting untuk penelitian.

1. Studi Literatur

Studi literatur mencakup beberapa hal yaitu mengumpulkan, membaca, dan mencatat informasi dari literatur yang berkaitan dengan topik TA. Tahap ini bertujuan sebagai pembelajaran dari penelitian atau proyek yang sudah pernah dilakukan yang dimana dapat menjadi landasan dalam *browser extension* yang akan dibangun untuk menggambarkan teknik dan metode serta algoritma yang telah ditentukan dan dipakai dalam penelitian ini.

1. Analisis Data dan Metode Testing

Proses tahap ini bertujuan untuk dapat memahami masalah yang sedang terjadi agar dapat menentukan metode yang tepat dalam memecahkan masalah tersebut dan untuk memastikan bahwa pemenuhan kebutuhan yang tepat sasaran, dimana dalam penelitian tugas akhir ini akan menganalisis model testing yang digunakan dalam melakukan testing terhadap aplikasi mobile*.* Pada tahapan ini juga dilakukan perancangan model testing yang akan dipakai dengan masing – masin aspek keamanan yang akan diteliti.

1. Implementasi

Proses implementasi berupakan pengujian terhadap beberapa aplikasi keamanan berbasis android. Selanjutnya akan dibangun sebuah prototype berbasis web yang akan menampilkan proses penggujian atau analisis keamanan yang dapat dilakukan aplikasi tersebut dalam pemenuhan checklist yang telah ditetapkan.

1. Evaluasi

Tahap evaluasi merupakan tahap dimana peneliti mengamati seluruh aspek yang diuji, dan memastikan bahwa setiap fungsi yang berjalan sesuai dengan protoype yang akan dibangun.

1. Penyusunan Hasil dan Pembahasan

Pada tahap ini akan dilakukan penulisan laporan hasil penelitian yang berisi hasil analisa dan kesimpulan yang dilakukan berdasarkan tujuan dan rumusan masalah yang telah diteliti.

# Resiko

Risiko yang mungkin terjadi dalam pengerjaan tugas akhir ini adalah hasil yang diperoleh saat melakukan implementasi tidak sesuai dengan hasil yang dihara

# Referensi

Ahmed, O., & Sallow, A. (2017). Android Security: A Review. *Academic Journal of Nawroz University*, *6*(3), 135–140. https://doi.org/10.25007/ajnu.v6n3a97

Aldy, I. K., Ardita, O., Ngurah, I. G., Cahyadi, A., & Rizky, M. (2022). *Analisis Keamanan Aplikasi Android Dengan Metode Vulnerability Assessment*. *10*(3), 279–286.

Bernhard Mueller, Scen Schleier, J. W. (2018). *Table of Contents iOS Testing Guide*. 1–480.

Wang, W., Zhao, M., Gao, Z., Xu, G., Xian, H., Li, Y., & Zhang, X. (2019). Constructing Features for Detecting Android Malicious Applications: Issues, Taxonomy and Directions. *IEEE Access*, *7*, 67602–67631. https://doi.org/10.1109/ACCESS.2019.2918139

Yumnun, L., Kusyanti, A., & Kartikasari, D. (2020). Implementasi OWASP Mobile Security Testing Guide (MSTG) Untuk Pengujian Keamanan Pada Aplikasi Berbasis Android. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(11), 10579–10585.

# Rencana Kerja

Berikut jadwal rencana kerja dalam pengerjaan TA I dapat dilihat pada tabel 1.

Tabel 1. Rencana Kerja TA I

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jenis Kegiatan | **Minggu** | | | | | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| Konsultasi dengan pembimbing |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Penentuan topik dan judul tugas akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengerjaan proposal tugas akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Review proposal dari pembimbing, perbaikan proposal, dan studi literatur |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| UTS (Ujian Tengah Semester) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Seminar proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perbaikan proposal sesuai dengan hasil seminar proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengerjaan laporan TA Bab I dan II |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Melakukan analisis terkait dengan solusi yang tepat pada permasalahan yang ada. Pengerjaan laporan tugas akhir bab III |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perbaikan dan melakukan finalisasi laporan TA Bab I - III |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| UAS – Seminar TA I |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |