ANALISIS PERBANDINGAN KEAMANAN APLIKSI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN *MOBILE SECURITY FRAMEWORK* (MOBSF)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

TRIYAWAN BAGUS SUBAKJA
12050312553

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2024

LEMBAR PERSETUJUAN

ANALISIS PERBANDINGAN KEAMANAN APLIKSI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN *MOBILE SECURITY FRAMEWORK* (MOBSF)

TUGAS AKHIR

Oleh:

TRIYAWAN BAGUS SUBAKJA
12050312553

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 20 Desember 2024

Ketua Program Studi	Pembimbing
Eki Saputra, S.Kom., M.Kom.	**Mona Fronita, S.Kom., M.Kom.**
NIP. 198307162011011008	**NIP. 198403032023212027**

LEMBAR PENGESAHAN

ANALISIS PERBANDINGAN KEAMANAN APLIKSI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN *MOBILE SECURITY FRAMEWORK* (MOBSF)

TUGAS AKHIR

Oleh:

TRIAWAN BAGUS SUBAKJA
12050312553

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 03 Desember 2024

Pekanbaru, 20 Desember 2024
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Hartono, M.Pd.	**Eki Saputra, S.Kom., M.Kom.**
NIP. 196403011992031003	**NIP. 198307162011011008**

DEWAN PENGUJI:

Ketua : **Syafril Siregar, S.Th.I., M.Ag.**

Sekretaris : **Mona Fronita, S.Kom., M.Kom.**

Anggota 1 : **Eki Saputra, S.Kom., M.Kom.**

Anggota 2 : **Tengku Khairil Ahsyar, S.Kom., M.Kom.**

SURAT PERNYATAAN

Nama	:TRIYAWANBAGUSSUBAKJA
Nim	: 12050312553
Program Studi	:Sistem Informasi
Judul Tugas Akhir	: Analisis Perbandingan Keamanan Aplikasi Transportasi Online Berbasis Android Menggunakan Mobile Security Framework (MOBSF)

Menyatakan bahwa melengkapi seluruh kelengkapan administrasi Tugas Akhir Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau berupa **bukti publish secara lengkap.** Demikian yang dapat saya sampaikan saya sampaikan dengan sungguh-sungguh. Saya ucapkan Terimakasih.

Pekanbaru, 20 Desember 2024

Hormat saya,

TRIYAWANBAGUSSUBAKJA
Nim. 12050312553

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada peneliti. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin peneliti dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 20 Desember 2024
Yang membuat pernyataan,

TRIYAWAN BAGUS SUBAKJA
NIM. 12050312553

LEMBAR PERSEMBAHAN

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Alhamdulillahi Rabbil 'Alamin, segala puji bagi Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. *Sholawat* beserta salam tak lupa pula kita ucapkan kepada junjungan dan suri tauladan kita Nabi Muhammad *Shallallahu 'Alaihi Wa Sal- lam* dengan mengucapkan *Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafa'at-Nya di dunia maupun di akhirat, *aamiin ya rabbal'alaamiin*.

Dengan penuh rasa syukur dan kebanggaan, peneliti menyusun Tugas Akhir ini sebagai bagian dari pencapaian akademik saya. Tugas Akhir ini tidak hanya merupakan wujud dari hasil kerja keras dan dedikasi peneliti selama ini, tetapi juga merupakan bentuk penghargaan dan terima kasih peneliti kepada kedua orang tua yang telah memberikan dukungan dan kasih sayang yang tiada henti.

Terima kasih Ayah, Ibu, Abangku, kakakku, dan Adikku yang tersayang atas setiap do'a, bimbingan serta, dukungan semangat yang telah kalian berikan kepada saya sampai sekarang ini. Terima kasih atas segala kebaikan dan selalu ada saat keadaan tersulit sekalipun. Saya akan selalu mendoakan yang terbaik untuk Ayah, Ibu, Abang, Kakak, dan Adik Saya semoga Allah *Subhanahu Wa Ta'ala* selalu menjaga mereka dimanapun berada, bahagia dunia dan akhirat serta diberikan tempat istimewa di sisi-Nya sehingga kita bisa berkumpul kembali bersama-sama di *Jannah*-Nya.

Saya ucapkan terima kasih kepada Ibu Mona Fronita, S.Kom., M.Kom yang telah berjasa dalam menyelesaikan Tugas Akhir ini. Saya ucapkan terima kasih juga kepada bapak dan ibu dosen Program Studi Sistem Informasi yang telah mewariskan ilmu yang bermanfaat dan arahan kepada saya untuk menyelesaikan studi di Program Studi Sistem Informasi ini serta teman-teman yang selalu memberikan dukungan, semangat dan inspirasi kepada saya. Semoga kita semua selalu diberikan ke- mudahan, rahmat, serta karunia-Nya. *Aamiin*.

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, bersyukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini dengan baik dan tepat waktu yang berjudul "Analisis Perbandingan Keamanan Aplikasi Transportasi Online Berbasis Android Menggunakan Mobile Security Framework". *Sholawat* serta salam kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer di Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau. Pada penulisan Tugas Akhir ini, terdapat beberapa pihak yang sudah berkontribusi dan mendukung peneliti baik berupa materi, moril, dan motivasi. Peneliti ingin mengucapkan banyak terima kasih kepada:

1. Bapak Prof. Dr. Hairunas, M.Ag sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Hartono, M.Pd sebagai Dekan Fakultas Sains dan Teknologi.
3. Bapak Eki Saputra, S.Kom., M.Kom sebagai Ketua Program Studi Sistem Informasi dan sebagai Dosen Penguji I peneliti yang telah banyak memberikan arahan, masukan, serta nasihat dalam perkuliahan dan penyelesaian Tugas Akhir ini.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak Tengku Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi dan sebagai Dosen Penguji II peneliti yang telah memberikan arahan, masukan, serta nasihat dalam penyelesaian Tugas Akhir ini.
6. Ibu Nurmaini Dalimunthe, S.Kom., M.Kes sebagai Dosen Pembimbing Akademik yang telah banyak memberikan peneliti arahan, bimbingan, dan masukan serta motivasi dalam perkuliahan hingga penyelesaian Tugas Akhir ini.
7. Ibu Mona Fronita, S.Kom., M.Kom sebagai Dosen Pembimbing Tugas Akhir yang selalu memberikan bimbingan serta masukan yang sangat berharga hingga penyelesaikan Tugas Akhir ini perkuliahan dan proses penyelesaian Tugas Akhir ini.
8. Bapak Syafril Siregar, S.Th.i., M.Ag sebagai Ketua Sidang peneliti yang telah banyak memberikan arahan, masukan, serta nasihat dalam perkuliahan dan penyelesaian Tugas Akhir ini.

9. Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah banyak memberikan ilmunya kepada peneliti. Semoga ilmu yang diberikan dapat peneliti amalkan dan menjadi amal *jariyah*.
10. Seluruh Pegawai dan Staf Fakultas Sains dan Teknologi yang telah membantu dan mempermudah proses administrasi selama perkuliahan ini.
11. Teristimewa untuk kedua orang tua peneliti, Ayahanda Cholikur Rahman, Ibunda Umi Salmiah Lubis, Kakanda Wajhul Hadi, dan Liqqua Anggraini Dwi Pamungkas, serta Adinda MHD Rizky Maulidiansyah Alfarizi yang selalu mendo'akan, dan terus memberi semangat kepada peneliti.
12. Teman-teman terbaik dan seperjuangan, yakni Furqan Anwari, Aditya Pratama Putra, Dwi Erlangga, Bintang Rahmat Riadi, Muhammad Agung Al affan, Muhamad Ivandra, dan Nazhifatunnisa, serta anggota kost waqaf, dan anggota sos yang selalu mendukung segala aktivitas dan kesibukan serta menyemangati peneliti dalam menyelesaikan penulisan Tugas Akhir.
13. Kepada Kakanda sepupu saya Muhammad Rabiul Muslim Purba yang sudah berpartisipasi mendukung kegiatan dalam perkuliahan serta memberikan motivasi selama pengerjaan Tugas Akhir.
14. Kepada kakanda Piere Agung Pribadi, Wendra, dan Joko. Terima kasih atas motivasi dan arahan serta masukannya untuk perkuliahan ini.
15. Serta semua pihak yang namanya tidak dapat disebutkan satu persatu, yang telah banyak membantu dalam pelaksanaan dan menyelesaikan penelitian Tugas Akhir.

Semoga segala doa dan dorongan yang telah diberikan selama ini menjadi amal kebajikan dan mendapat balasan setimpal dari Allah *Subhanahu Wa Ta'ala*. Peneliti menyadari bahwa penulisan Tugas Akhir ini masih banyak terdapat kekurangan dan jauh dari kata sempurna. Untuk itu kritik dan saran atau pertanyaan dapat diajukan melalui *e-mail* 12050312553@students.uin-suska.ac.id. Semoga laporan ini bermanfaat bagi kita semua. Akhir kata peneliti ucapkan terima kasih.

Pekanbaru, 20 Desember 2024

Peneliti,

TRIYAWAN BAGUS SUBAKJA

NIM. 12050312553

ISSN : 2540-8984

Letter of Acceptance

Tulungagung, 26 Juli 2024

No : 046/JIPI.PTI.UBHI/X.II/IV/2024
Lamp : -
Hal : Penerimaan artikel JIPI Vol. 10 No.2 2025

Kepada
Triyawan Bagus Subakja, Mona Fronita, Syaifullah, Tengku Khairil Ahsyar
Di Tempat

Assalamu'alaikum Wr. Wb.

Bersama surat ini, redaksi Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI) Program Studi Pendidikan Teknologi Informasi Universitas Bhinneka PGRI menginformasikan kepada Bapak/Ibu bahwa naskah dengan judul : "**ANALISIS PERBANDINGAN KEAMANAN APLIKASI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MOBSF)**" telah diterima untuk diterbitkan pada Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI) Vol.10 No.2 2025.

Kami mengucapkan terima kasih dan selamat atas diterimanya artikel tersebut. Kami juga mengharapkan artikel – artikel berikutnya untuk diterbitkan pada JIPI

Demikian surat kami, atas perhatian dan kerjasamanya kami sampaikan ucapan terimakasih.

Wassalamu'alaikum Wr. Wb.

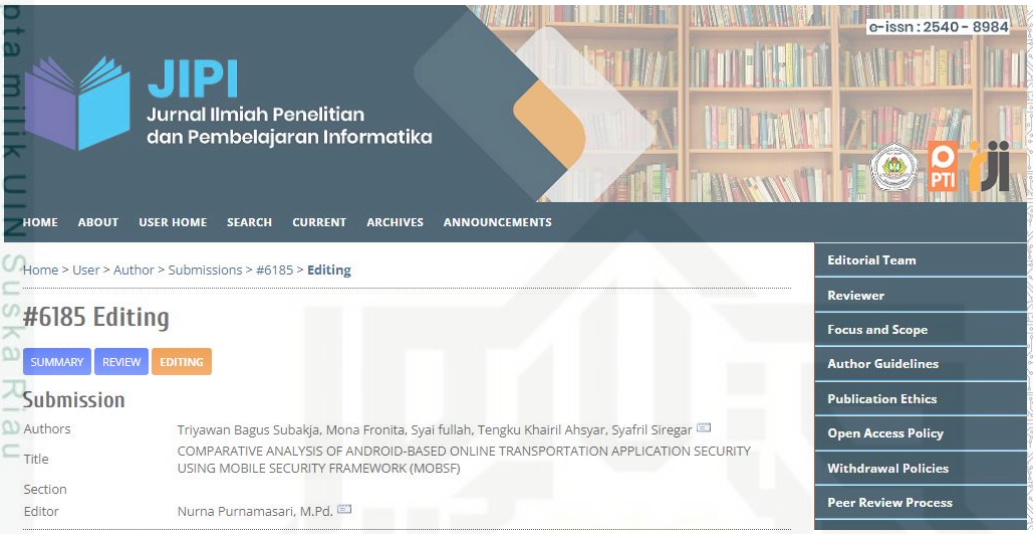
Ketua Redaksi

Fahrur Rozi, M.Kom.

Program Studi Pendidikan Teknologi Informasi
Universitas Bhinneka PGRI
Jl. Mayor Sujadi Tim. No. 24 Plosokandang
Tulungagung, Jawa Timur 66229
E-mail : jipistkippti@gmail.com
Website : jurnal.stkippgritulungagung.ac.id/index.php/jipi

LAMPIRAN A

BUKTI PENDAFTARAN JURNAL



LAMPIRAN B
BUKTI ACCEPTED AND EDITOR DECISION

JIPI Journal <jipistkippti@gmail.com> 24 Jul 2024, 11.53
kepada saya

Triyawan Bagus Subakja, Mona Fronita, Syaifullah, Tengku Khairil Ahsyar:

Kami telah mencapai keputusan terkait pengajuan jurnal Anda ke JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) dengan judul "**ANALISIS PERBANDINGAN KEAMANAN APLIKASI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MOBSF)**".

Keputusan kami adalah: **Revisions**

- Untuk melihat hasil review dan cara upload hasil revisi cek di https://jurnal.stkippgritulungagung.ac.id/index.php/jipi/pages/view/cekRevisi
- Lengkapi biodata penulis pada meta data sesuai dengan jumlah penulis yang ada pada artikel
- **Upload hasil revisi dalam bentuk doc/docx (Maks File 5MB)**

Mohon untuk dapat dilakukan block warna kuning terhadap hasil revisi yang telah dilakukan

Upload hasil revisi ke akun JIPI -> Submission -> Review ->

Editor Decission -> Upload Author Version

JIPI Journal <jipistkippti@gmail.com> Jum, 26 Jul, 12.58
kepada saya

Triyawan Bagus Subakja, Mona Fronita, Syaifullah, Tengku Khairil Ahsyar:

Kami telah mencapai keputusan terkait pengajuan artikel/jurnal anda ke JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), yang berjudul **"ANALISIS PERBANDINGAN KEAMANAN APLIKASI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MOBSF)"**.

Dengan senang hati saya informasikan bahwa makalah Anda telah dinyatakan **ACCEPTED** dan akan dipublikasikan di JIPI (e-ISSN: 2540 - 8984). Selamat!

Untuk menutupi sebagian biaya publikasi, setiap makalah yang diterima dikenakan biaya: Rp 600.000,-

---

Bank Account name (please be exact)/Beneficiary: FAHRUR ROZI

Bank Name: Bank MANDIRI

Bank Account # : 1710001359879

Cell. Phone: +6285646149638

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984

ANALISIS PERBANDINGAN KEAMANAN APLIKASI TRANSPORTASI ONLINE BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MOBSF)

Triyawan Bagus Subakja *[1)], Mona Fronita [2)], Syaifullah [3)], Tengku Khairil Ahsyar [4)]
1. Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
2. Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
3. Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
4. Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia

Article Info
Kata Kunci: Analisis Statik; Android; Keamanan; MobSF; Transportasi Online

Keywords: *Android; MobSF; Online Transportation; Security; Static Analysis*

DOI :
https://doi.org/10.29100/jipi.v4i1.781

* Corresponding author.
Triyawan Bagus Subakja
E-mail address:
12050312553@students.uin-suska.ac.id

ABSTRAK
Transportasi online adalah layanan transportasi yang tersedia melalui internet. Layanan ini merupakan inovasi teknologi yang bertujuan memudahkan masyarakat indonesia saat melakukan perjalanan. Penggunaan aplikasi transportasi online menjadi alternatif daripada taksi dan ojek pangkalan. Aplikasi ini menawarkan banyak kemudahan seperti fleksibilitas dalam penggunaan, serta sistem pembayaran digital yang keamananannya sudah terjamin. Meskipun demikian, pengguna aplikasi transportasi online tetap harus waspada terhadap kejahatan digital yang dilakukan oleh Cracker. Penyalahgunaan aplikasi transportasi online dapat berakibat fatal. Maka dari itu, tujuan dari penelitian ini adalah menemukan celah keamanan dan perbandingan keamanan pada aplikasi transportasi online berbasis android. Mobile Security Framework (MobSF) akan digunakan dalam penelitian ini sebagai metode analisis berdasarkan beberapa parameter seperti dangerous permissions, weak crypto, root detection, SSL bypass dan domain malware check. Hasil analisis berdasarkan beberapa parameter berbeda telah memberikan tingkat keamanan yang berbeda-beda pula pada ketiga aplikasi. Pada aplikasi Gojek, tingkat keamanannya adalah 44/100 atau kategori sedang. Selanjutnya pada aplikasi Maxim mendapatkan skor 47/100 atau kategori sedang. Sedangkan pada aplikasi Grab mendapatkan skor 50/100 yang juga masuk ke dalam kategori sedang. Pada ketiga aplikasi ini juga ditemukan beberapa celah keamanan. Pada aplikasi Gojek, Maxim dan Grab, ditemukan celah keamanan berdasarkan *dangerous permissions* dan *weak crypto*. Pada parameter *SSL Bypass*, hanya aplikasi Maxim saja yang terdeteksi memiliki celah keamanan. Berdasarkan analisis parameter *root detection* ketiga aplikasi menunjukkan tidak adanya *root detection*. Lalu parameter terakhir *domain malware check* juga menunjukkan status baik pada ketiga aplikasi.

ABSTRACT
Online transportation is a service provided over the internet, representing a technological innovation that has significantly facilitated travel for Indonesians. These applications have gained widespread adoption in Indonesia, serving as alternatives to conventional transport modes like taxis and traditional motorcycle taxis. They offer convenience and speed in booking rides, along with secure transactions through digital payment systems. Despite the user-friendly experience and advantages offered by these applications, their security cannot be overlooked. The increasing accessibility of Android-based online transportation applications has made them a prime target for malicious actors ("Crackers") who may exploit vulnerabilities for nefarious purposes. This research aims to identify security vulnerabilities and compare the security found in Android-based online transportation applications. The researcher utilized the Mobile Security Framework (MobSF) to conduct static security analysis focusing on parameters such as dangerous permissions, weak cryptography, root detection, SSL bypass, and domain malware checks. The security assessments of Gojek, Maxim, and Grab revealed moderate security risks. Gojek scored

44/100, Maxim 47/100, and Grab 50/100 in terms of security ratings. All three applications were found to have vulnerabilities related to dangerous permissions and weak cryptography. Specifically, Maxim was also susceptible to SSL bypass attacks. None of the applications had implemented root detection, but their domain malware checks were deemed satisfactory.

I. PENDAHULUAN

Pemanfaatan alat teknologi seperti komputer dan ponsel telah meningkat seiring dengan kemajuan teknologi yang pesat. Ponsel dan komputer menjadi perangkat yang lebih banyak digunakan oleh masyarakat, karena dapat mendukung pekerjaannya [1].

Salah satu alasan utama yang menyebabkan perkembangan teknologi informasi kian pesat adalah kemunculan internet. Internet dimanfaatkan oleh pelaku bisnis untuk mengembangkan bisnisnya. Khususnya penyedia jasa transportasi dengan menghadirkan aplikasi transportasi online. Alat tranportasi sudah dikenal masyarakat sedari dahulu sebagai media untuk memindahkan manusia dan barang dari satu tempat ke tempat yang lain [2].

Tranportasi online adalah inovasi teknologi yang menawarkan kemudahan bagi masyarakat Indonesia saat akan bepergian. Beberapa aplilkasi ternama yang banyak digunakan masyarakat adalah Gojek, Grab, dan Maxim. Layanan ini secara perlahan telah menggantikan peranan penyedia transportasi konvensional seperti taksi dan ojek pangkalan. Nilai tambah dari aplikasi transportasi online adalah kemudahan dan kecepatan akses saat akan melakukan pemesanan, serta tersedianya pembayaran menggunakan dompet digital. Sejauh ini, aplikasi transportasi online terus menunjukkan perkembangan yang signifikan. Terbukti melalui peningkatan layanan serta penambahan fitur-fitur ringkas seperti pesan antar makanan, antar belanja, dan pengiriman barang [3].

Meskipun telah menyediakan kemudahan, bukan berarti pengguna boleh abai terhadap sistem keamanan dari aplikasi transportasi online. Peningkatan jumlah penggunaan dan akses pada aplikasi ini berisiko menjadikannya lebih rentan sebagai target penyarangan Cracker [4].

Teknologi smartphone berbasis android menawarkan banyak layanan, fitur dan aplikasi yang dapat mendukung produktivitas. Inilah alasan mengapa android menjadi perangkat seluler pintar yang menguasai sekitar 82,8% pangsa pasar [5].

Meskipun berhasil menjadi penguasa pangsa pasar, tidak dapat disangkal bahwa android adalah sistem operasi yang paling rentan di retas oleh oknum tidak bertanggung jawab seperti Cracker. Banyak peretas yang memanfaatkan celah dalam sistem dan aplikasi pihak ketiga [6].

Pada android, terdapat banyak sekali celah keamanan yang bisa dimanfaatkan oleh Cracker untuk mencuri data dan informasi pengguna. Bentuk informasi pada android dapat disimpan sebagai catatan, lisan, elektronik, pos dan audio visual [7].

Pada tahun 2020, laporan-laporan menunjukkan banyaknya data akun yang beredar di forum kejahatan darkweb. Hasil audit mengungkapkan bahwa 15 miliar login telah dicuri dari 100 pelanggaran, dengan peretas yang membagikan 386 juta catatan curian secara gratis. Basis data yang tidak aman dengan cepat menjadi ancaman besar bagi perlindungan data, sehingga data pribadi hampir 235 juta pengguna Instagram dan TikTok terekspos dan bisa diakses oleh siapa saja [8].

Kasus serupa juga telah tercatat, bahwa 70 ribu data pengguna Tinder berjenis kelamin perempuan telah menjadi korban kejahatan digital. Laporan perusahaan keamanan cyber whith ops11 menyebutkan bahwa 70 ribu data dan foto pengguna Tinder tersebut telah tersebar pada forum kejahatan cyer. Kasus lainnya pernah terjadi yaitu Cambrige Analytica yang menyerang sekitar 87 juta pengguna Facebook. Mereka telah kehilangan data pribadinya dan disalahgunakan oleh pihak ketiga [9].

Selain itu terdapat juga berita tentang bocornya data pengguna aplikasi transportasi online asal Dubai (Careem), akibat bocornya data pengguna aplikasi tersebut nama, alamat email, dan nomor telepon pengguna aplikasi online maupun driver telah dicuri. Hal ini terjadi akibat ada oknum yang menerobos masuk kedalam sistem peyimpanan data pada tanggal 14 Januari 2018 [10].

Kemungkinan ini dapat saja terjadi kepada aplikasi transportasi online di Indonesia. Penyebab utamanya adalah keharusan memberikan informasi pribadi pengguna saat pertama kali melakukan registrasi aplikasi. Informasi tersebut merupakan informasi elektronik yang akan tersimpan di dalam database aplikasi transportasi online. Informasi semacam inilah yang akan dimanfaatkan driver dalam melaksanakan pekerjaannya, seperti menghubungi konsumen, mengetahui alamat dan keberadaan konsumen, serta memberikan layanan sesuai jasa

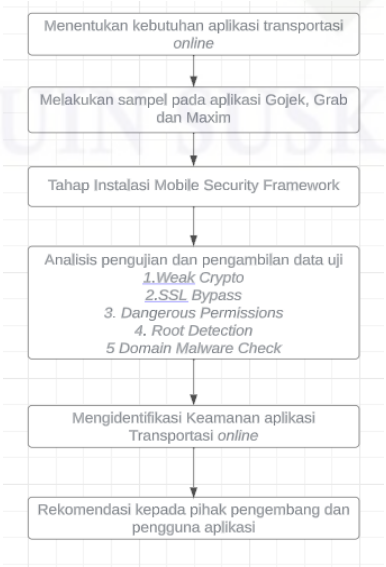
yang telah dipilih oleh konsumen. Permasalahan yang terjadi adalah, saat konsumen memasukkan infromasi pribadi, aplikasi tidak menjamin keamanan dan kerahasiaan sepenuhnya [11].

Pada penelitian ini, penulis akan menggunakan Mobile Security Framework, Mobile Security Framework (MobSF) adalah framework pengujian otomatis bersifat open-source, yang mampu melakukan analisis statis dan dinamis dalam melakukan proses analisis akan menampilkan hasil berupa laporan mengenai aplikasi android tersebut [12]. Analisis statis menggunakan mobile security framework dapat menghasilkan True Positive hingga 97%. Validitas dari hasil analisis tersebut dilakukan pembuktian validitas yang terbukti tidak ada perubahan dari nilai True Positive yang dihasilkan. Dalam mobile security framework mencakup beberapa framework, salah satunya ialah framework Open Web Application Security Project (OWASP) Mobile Application Security. Framework OWASP MASTG membantu mobile security framework dalam melakukan analisis dan mengkategorikan risiko keamanan mobile berdasarkan panduannya [13]. OWASP MASTG merupakan standar keamanan yang digunakan pada aplikasi mobile yang disertai dengan panduan pengujian yang komprehensif yang mencakup proses, teknik, tools, dan studi kasus yang berkaitan dengan pelaksanaan pengujian keamanan aplikasi mobile. Menurut penelitian sebelumnya, OWASP MASTG dapat menemukan lebih banyak kerentanan aplikasi Android dibandingkan dengan hasil analisis pada framework AndroBugs [14]. Sementara analisis statik akan mendekompilasi kode APK menjadi format yang dapat terbaca oleh manusia. Dengan demikian, kerentanan aplikasi dapat lebih mudah teridentifikasi [15], pada aplikasi transportasi online dengan subyek yang digunakan yaitu Gojek, Grab dan Maxim. Diharapkan penelitian ini menimbulkan kesadaran kepada pengguna untuk menjaga keamanan data pribadinya, serta menjadi masukan kepada pihak pengembang aplikasi transportasi online. Tahapan penelitian yang dilakukan adalah melakukan analisis terhadap beberapa parameter berbeda. Yaitu dangerous, weak crypto, root detection, SSl bypass dan domain malware check. Hasil dari analisis beberapa parameter tersebut akan menunjukkan celah keamanan aplikasi tranportasi online jika memang ditemukan. Selanjutnya, berdasarkan celah keamanan yang ditemukan akan dilakukan analisis statik untuk memberikan rekomendasi.

Dari uraian diatas maka untuk mengetahui tingkat keamanan serta pengujian sebuah aplikasi transportasi online diperlukan adanya penelitian yang diharapkan dapat memberikan kesadaran terhadap pengguna aplikasi dan memberikan masukan kepada pihak pengembang aplikasi transportasi online. Oleh karena itu, dalam tugas akhir ini dilakukan analisa statik keamanan terhadap aplikasi transportasi online berbasis android dengan menggunakan Mobile Security Framework (MobSF) dengan subjek yang digunakan yaitu aplikasi Gojek,Grab dan Maxim.

II. METODE PENELITIAN

Metodologi pada penelitian ini terdiri dari lima tahapan yaitu: Menentukan kebutuhan aplikasi transportasi online, Tahap melakukan sampel pada aplikasi Gojek, Grab dan Maxim, Tahap instalasi *Mobile Security Framework* Tahap Analisis pengujian dan pengambilan data uji, Tahap mengidentifikasi keamanan pada aplikasi transportasi online dan Rekomendasi oleh pengembang dan pengguna aplikasi.



Gambar 1. Metode Penelitian

A. Menentukan Kebutuhan Aplikasi Transportasi Online

Tahap awal dalam penelitian ini adalah mengidentifikasi masalah atau fenomena yang akan diteliti. Masalah atau fenomena yang akan diteliti adalah studi analisis statis keamanan aplikasi transportasi online berbasis android menggunakan framework mobile security framework (MobSF). MobSF adalah kerangka kerja keamanan yang dirancang untuk melakukan analisis statis dan dinamis pada aplikasi mobile, termasuk Android. Kelebihan utama dari MobSF adalah kemampuannya untuk menyediakan analisis statis dan dinamis secara bersamaan. MobSF dapat melakukan pemeriksaan kode sumber, mendeteksi kerentanan keamanan, dan menyimulasikan serangan terhadap aplikasi Android untuk mengidentifikasi celah keamanan potensial [16].

B. Melakukan Sampel pada Aplikasi Transportasi Online

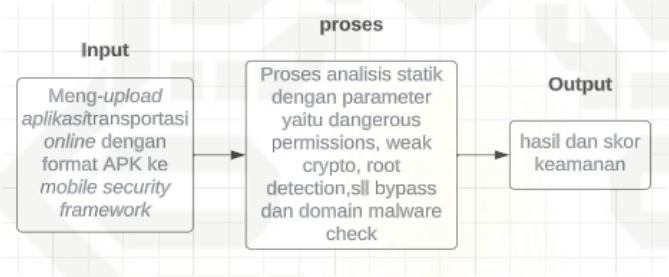
Aplikasi transportasi online sangat beragam. Tiga diantaranya yang paling populer di Indonesia adalah Gojek, Grab dan Maxim. Maka dari itu, penelitian ini difokuskan pada ketiga aplikasi tersebut dengan melakukan analisis statik menggunakan mobile security framework.

C. Analisis Pengujian dan Pengambilan Data Uji

Pada tahap ini, dilakukan pengujian terhadap aplikasi transportasi online berbasis android menggunakan mobile security framework.

1) Cara pengujian

Pada gambar 2. Ditunjukkan alur analisis statik yang dilakukan menggunakan Mobile Security Framework (MobSF).



Gambar 2. Blok diagram analisis MobSF

2) Prosedur pengujian
   a. Phyton 3.6+
   b. Oracle JDK 1.7 atau diatasnya
   c. Windows App Static analysis membutuhkan Host Windows atau VM Windows jika menggunakan Mac dan Linux
   d. Jika menggunakan Linux, harus mengaktifkan 32bit execution support
   e. Pengguna Mac OS harus install Command-line tools
3) Cara install
   a. Pastikan untuk meng install Python 3.6+, Oracle JDK 1.7 atau diatasnya, dan Docker terlebih dahulu.
   b. Pull Image Docker MobSF
      Untuk melakukan Pull Image Docker MobSF, kita bisa menggunakan command dibawah ini.
      "docker pull opensecurity/mobile-security-framework-mobsf"
   c. Maka tampilan akan seperti dibawah ini.

   d. Untuk menjalankan MobSF, gunakan command seperti dibawah ini.

"docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf"
Tampilan akan berlanjut seperti dibawah ini.

e. buka url http://0.0.0.0:8000/ maka akan tampil halaman utama dari MobSF seperti pada gambar pertama pada bagian hasil dan pembahasan.

4) Parameter yang Di Uji

Pada penelitian ini, pengujian tingkat keamanan aplikasi transportasi online dilakukan berdasarkan beberapa parameter berbeda. Parameter yang akan diujikan dan dianalisis adalah

a. Dangerous permissions
Analisis terhadap permission dilakukan dengan melihat pada seberapa banyak dangerous permissions yang digunakan oleh aplikasi[8]. Hal ini bertujuan untuk mengindari kebocoran informasi privasi pengguna dari aplikasi transportasi online kepada pihak ketiga di ponsel.

b. Weak crypto
Analisis weak crypto dilakukan dengan acuan ada atau tidaknya implementasi algoritma kriptografi yang lemah atau penggunaan algoritma kriptografi yang sudah usang atau sudah dianggap tidak layak[8].

c. Root detection
Mendeteksi perangkat yang di root, karena hal ini dapat berakibat adanya serangan spyware atau virus

d. SSL Bypass
Analisis SSL bypass dilakukan dengan melakukan cek ada atau tidaknya service yang melibatkan protokol http yang tidak mewajibkan penggunaan SSL sebagai persyaratan keamanan transaksi dalam protokol http menggunakan SSL seperti mengizinkan http di manifest, atau terdapat string berkonten http:// yaitu weak implementation[8]

e. Domain malware check
Analisis domain malware check dilakukan dengan melakukan cek ada atau tidaknya domain yang terdapat dalam aplikasi terindikasi dalam kategori domain yang mengandung malware[7]

5) Data Output

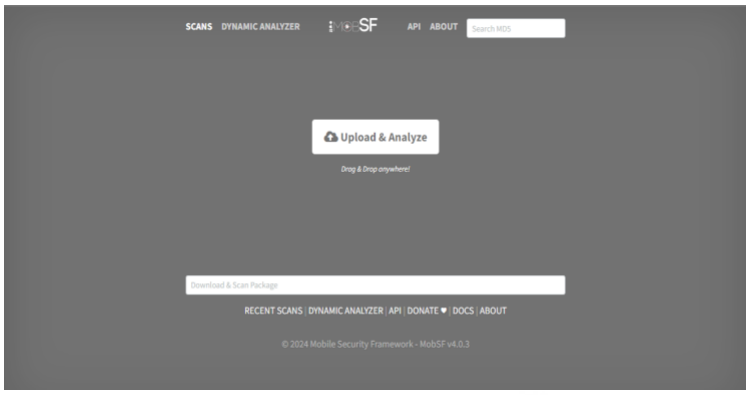
Hasil yang diharapkan dari penelitian ini adalah tingkat dan celah keamanan dari 3 aplikasi transportasi online berbeda yang diujikan yaitu, Gojek, Grab dan Maxim.

D. Mengidentifikasi Keamanan pada Aplikasi Transpotasi Online

Berdasarkan pengujian yang telah dilakukan terhadap setiap parameter, selanjutnya dilakukan analisis untuk menentukan hasil pengujian dan menarik kesimpulan. Tahap ini juga berisi saran untuk penelitian selanjutnya.

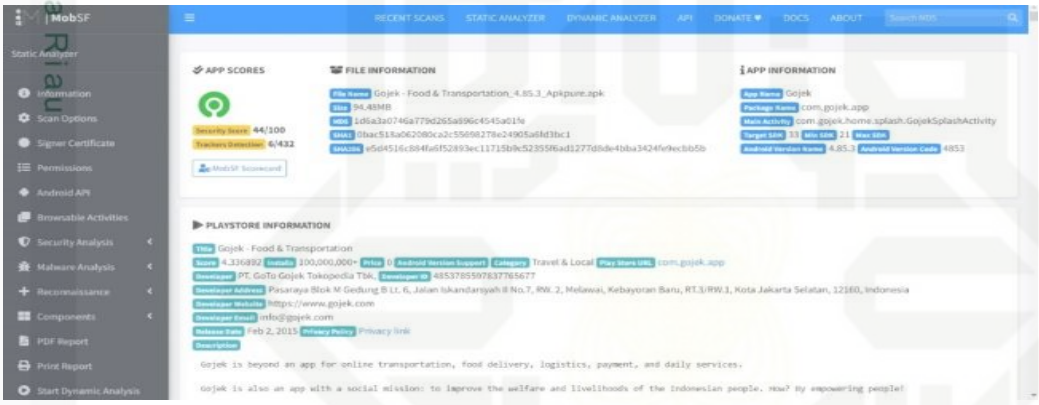
III. HASIL DAN PEMBAHASAN

Pada Gambar 3. adalah tampilan halaman landing page dari framework MobSF.



Gambar 3. Halaman utama MobSF

Untuk melakukan pengujian, file aplikasi transportasi online berformat APK harus diunduh terlebih dahulu. Selanjutnya, file tersebut di upload ke framework MobSF. Pada Gambar 4. ditunjukkan halaman yang memuat hasil analisis file APK aplikasi Gojek.



Gambar 4. Halaman hasil analisis file aplikasi Gojek pada *Mobile Security Framework*

Hasil pengujian pada apalikasi Gojek bagian app score adalah:
1) Security score atau tingkat keamanan aplikasi ini berada pada nilai 44/100. Nilai ini menunjukkan bahwa aplikasi memiliki tingkat resiko yang sedang.
2) Selanjutnya pada trackers detection mendapatkan nilai 6/432. Nilai ini menunjukkan bahwa aplikasi Gojek memiliki 6 tracker atau pelacak yang teridentifikasi.

Pada file information terdapat beberapa masalah yang teridentifikasi, yaitu:
1) Nama file, gojek-food & transportation_4.85.3_Apkpure.Apk.
2) Ukuran pada aplikasi sebesar 94.45MB.

Pada *app information* telah ditemukan:
1) Nama Aplikasi Gojek dengan *Package name com.gojek.app.*
2) Aktivitasutama pada aplikasi ialah *com.gojek.home.splash.GojekSplashActivity.*
3) *Software Development Kit* (SDK) adalah sekumpulan alat pengembangan perangkat lunak yang bisa diinstal. Target dari SDK adalah versi platform yang menjadi sasaran aplikasi. Pada aplikasi Gojek, diketahui nilai SDK adalah 29. Nilai minimun SDK menunjukkan versi minimun dari platform atau sistem operasi yang dapat menjalankan suatu aplikasi. Minimun SDK pada aplikasi Gojek adalah 21, sedangkan versi maksimumnya tidak tersedia.
4) Nama versi android 4.85.3 dan code versi android 4853.

Pada *Playstore information* telah ditemukan:
1) Judul Gojek-food&transportation dengan score 4.336892.
2) Gojek di instal sebanyak lebih dari 100.000.000 kali dengan harga aplikasi sebesar 0.
3) Kategori aplikasi ialah travel dan local dan URL aplikasi adalah *com.gojek.app.*
4) Tanggal gojek dirilis pada 2 februari 2015 dan kebijakan privasi yaitu privasi link.

Gambar 5. Halaman hasil analisis file aplikasi Maxim pada *Mobile Security Framework*

Pada aplikasi Maxim bagian *App Score* telah teridentifikasi:
1) Skor keamanan 47/100 yang artinya aplikasi Maxim memiliki tingkat resiko tergolong sedang dan terdapat 7 pelacak.

Pada *file information* ditemukan:
1) Nama file berupa maxim-order taxi, food_3.15.16_Apkpure(1).apk dengan ukuran aplikasi sebesar 41.84MB.

Pada *app information* ditemukan:
1) Terdapat nama aplikasi maxim dengan package name com.taxsee.taxsee.
2) Target SDK 34, min SDK 21 serta tidak terdapat max SDK.
3) Nama versi android adalah 3.15.16 dan kode versi android 10900.

Pada *Playstore information* telah ditemukan:
1) Terdapat nama Judul yaitu Maxim-order taxi,*food* dengan nilai 4.606928.
2) Aplikasi telah di instal lebih dari 50.000.000 kali dengan harga aplikasi 0.
3) Kategori aplikasi yaitu auto dan vehicles alamat play store URL adalah com.taxsee.taxsee.
4) Aplikasi maxim dirilis pada tanggal 9 juni 2012 dengan kebijakan privasi adalah *privacy link.*

Pada gambar 6. ditampilkan hasil pengujian pada file aplikasi Grab menggunakan *mobile security framework* (MobSF).

Gambar 6 . Halaman hasil analisis file aplikasi Grab pada *Mobile Security Framework*

Pada aplikasi Grab pada bagian *App Score* terdapat:
1) Skor keamanan 50/100 yang artinya aplikasi Grab memiliki tingkat resiko tergolong sedang dan terdapat 7 pelacak.

Pada *file information* telah ditemukan:
1) File bernama Grab-Taxi & food Delivery_5.302.0_Apkpure.apk dengan ukuran aplikasi sebesar 117.08MB

Pada *app information* telah ditemukan:

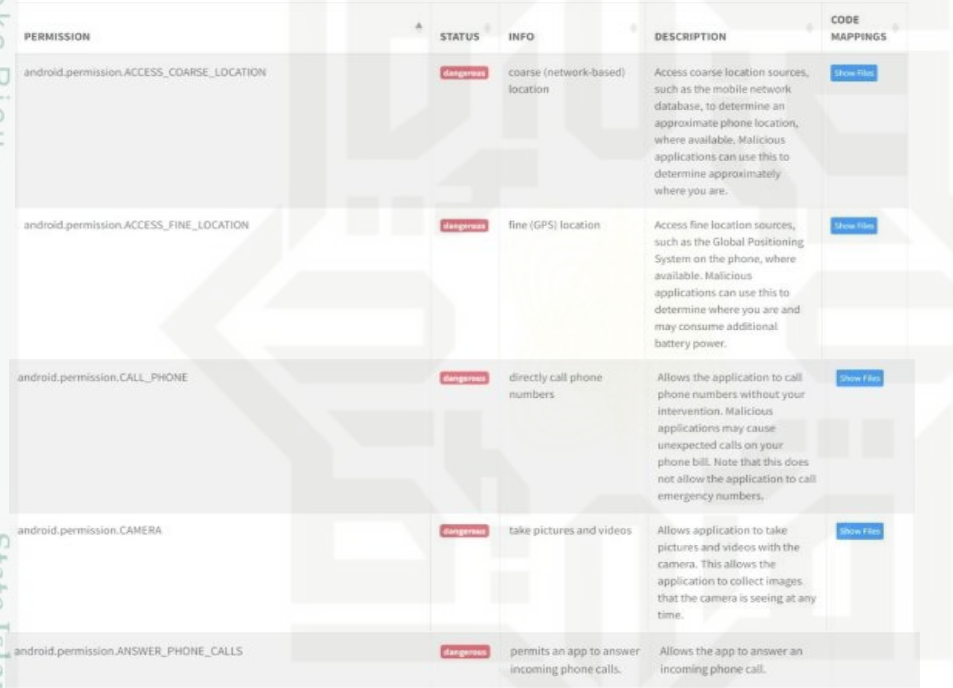
1) Sebuah aplikasi Grab dengan *package name* com.grabtxi.passengger.
2) Aktivitas utama adalah com.garb.pax_newface.presentation_newface.NewFace
3) Target SDK 33, min SDK 21 serta tidak terdapat max SDK.
4) Nama versi android adalah 5.302.0 dan kode versi android 53020000.

Pada *Playstore information* telah ditemukan:

1) Terdapat nama Judul yaitu Grab-taxi & food Delivery dengan nilai 4.8272,
2) Sebanyak lebih dari 100.000.000 kali di instal dengan harga aplikasi 0.
3) Kategori aplikasi yaitu trravel dan local alamat play store URL adalah com.grabtaxi.passenger.
4) Aplikasi Grab dirilis pada tanggal 30 May 2013 dengan kebijakan privasi berupa *Privacy link.*

A. Dangerous Permissions

Pada gambar 7. ditampilkan hasil pengujian pada file aplikasi Gojek menggunakan *mobile security framework* (MobSF) bagian *application permissions.*



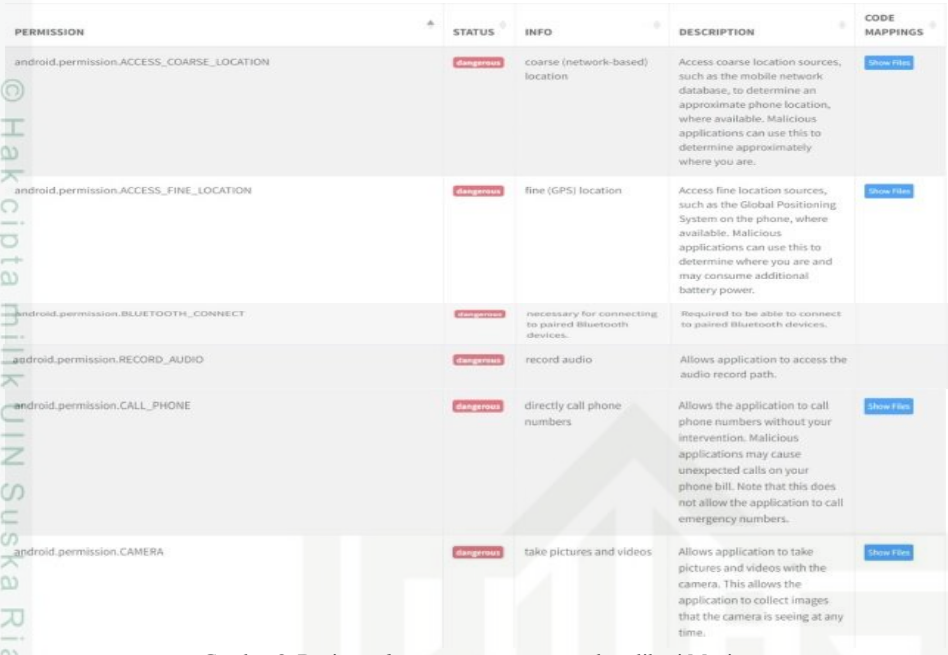
PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	Show Files
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	Show Files
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	Show Files
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	Show Files
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.	

Gambar 7. Bagian *aplications permissions* pada aplikasi Gojek

Pada apliksi gojek terdapat 5 *dangerous permissions* yaitu:

1) android.permissions.ACCESS_COARSE_LOCATION yang mengizinkan akses sumber lokasi secara kasar seperti database dan jaringan seluler untuk menentukan lokasi telepon, jika tersedia. Aplikasi dapat menggunakan ini untuk mengetahui kira-kira keberadaan pengguna.
2) android.perissions.ACCESS_FINE_LOCATION yang mengizinkan akses sumber lokasi secara baik seperti sistem pemosisian global di telpon, jika tersedia. Aplikasi berbahaya dapat menggunakan ini untuk mengetahui keberadaan pengguna dan menghabiskan daya baterai tambahan.
3) android.permission.ANSWER_PHONE_CALLS artinya menggizinkan aplikasi untuk menjawab panggilan masuk.
4) android.permissions.CALL_PHONE yang mengizinkan aplikasi untuk memanggil nomor telpon tanpa campur tangan pengguna, hal ini dapat menyebabkan panggilan tak terduga pada daftar riwayat panggilan pengguna, akan tetapi tidak berlaku pada nomor darurat.
5) android.permissions.CAMERA yang mengizinkan aplikasi mengambil gambar dan video dengan kamera. Hal ini memungkinkan aplikasi mengumpulkan gambar yang dilihat kamera kapan saja.

Pada gambar 8. ditampilkan hasil pengujian pada file aplikasi Maxim menggunakan *mobile security framework* (MobSF) pada parameter *application permissions*.



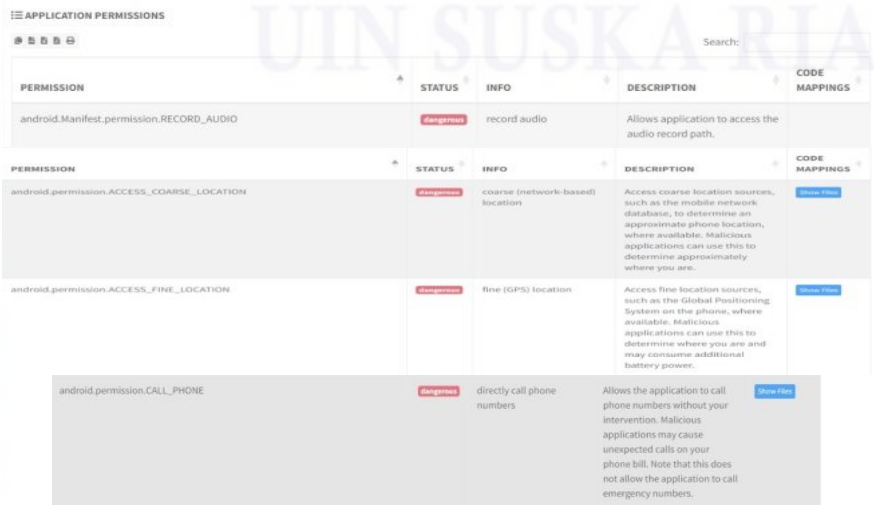
PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	Show Files
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	Show Files
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.	
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.	
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	Show Files
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	Show Files

Gambar 8. Bagian *aplications permissions* pada aplikasi Maxim

Pada apliksi Maxim terdapat 6 *dangerous permissions* yaitu:

1) android.permissions.ACCESS_COARSE_LOCATION yang mengizinkan akses sumber lokasi secara kasar seperti database dan jaringan seluler untuk menentukan lokasi telepon, jika tersedia. Aplikasi dapat menggunakan ini untuk mengetahui kira-kira keberadaan pengguna.
2) android.perissions.ACCESS_FINE_LOCATION yang mengizinkan akses sumber lokasi secara baik seperti sistem pemosisian global di telpon, jika tersedia. Aplikasi berbahaya dapat menggunakan ini untuk mengetahui keberadaan pengguna dan menghabiskan daya baterai tambahan.
3) android.permissions.BLUETOOTH_CONNECT artinya memerlukan untuk dapat terhubung ke perangkat Bluetooth yang dipasangkan.
4) Selanjutnya ditemukan android.permissions.RECORD_AUDIO yang mengizinkan aplikasi untuk mengakses jakur perekaman suara.
5) android.permissions.CALL_PHONE yang mengizinkan aplikasi untuk memanggil nomor telpon tanpa campur tangan pengguna, hal ini dapat menyebabkan panggilan tak terduga pada daftar riwayat panggilan pengguna, akan tetapi tidak berlaku pada nomor darurat.
6) android.permissions.CAMERA yang mengizinkan aplikasi mengambil gambar dan video dengan kamera. Hal ini memungkinkan aplikasi mengumpulkan gambar yang dilihat kamera kapan saja.

Pada gambar 9. ditampilkan hasil pengujian pada file aplikasi Grab menggunakan *mobile security framework* (MobSF) pada parameter *application permissions*.



APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.Manifest.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	Show Files
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	Show Files
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	Show Files

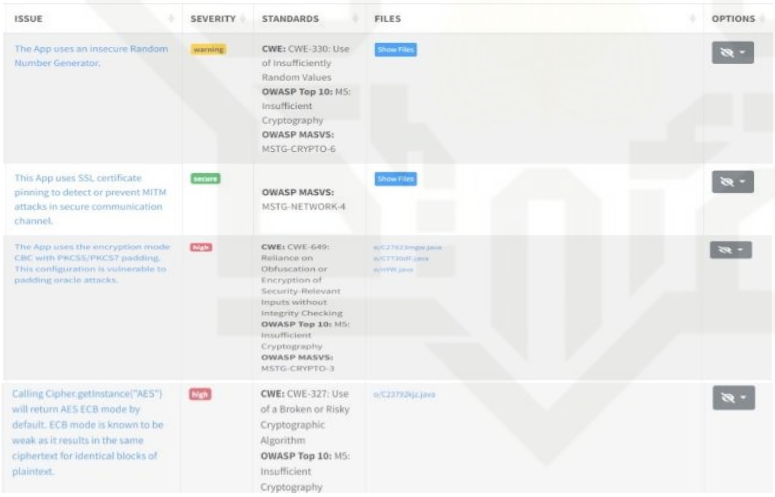
Gambar 9. Bagian *aplications permissions* pada aplikasi Grab

Pada apliksi Maxim terdapat 6 *dangerous permissions* yaitu:

1) android.permissions.RECORD_AUDIO yang berfungsi untuk mengizinkan aplikasi mengakses jakur perekaman suara.
2) android.permissions.ACCESS_COARSE_LOCATION yang mengizinkan akses sumber lokasi secara kasar seperti database dan jaringan seluler untuk menentukan lokasi telepon, jika tersedia. Aplikasi dapat menggunakan ini untuk mengetahui kira-kira keberadaan pengguna.
3) android.perissions.ACCESS_FINE_LOCATION yang mengizinkan akses sumber lokasi secara baik seperti sistem pemosisian global di telpon, jika tersedia. Aplikasi berbahaya dapat menggunakan ini untuk mengetahui keberadaan pengguna dan menghabiskan daya baterai tambahan.
4) android.permissions.CALL_PHONE yang mengizinkan aplikasi untuk memanggil nomor telpon tanpa campur tangan pengguna, hal ini dapat menyebabkan panggilan tak terduga pada daftar riwayat panggilan pengguna, akan tetapi tidak berlaku pada nomor darurat.
5) android.permissions.CAMERA yang mengizinkan aplikasi mengambil gambar dan video dengan kamera. Hal ini memungkinkan aplikasi mengumpulkan gambar yang dilihat kamera kapan saja.
6) android.permissions.WRITE_EXTERNAL_STORAGE mengizinkan aplikasi untuk menyimpan di penyimpanan eksternal.

B. Weak Crypto

Pada gambar 10. ditampilkan hasil pengujian pada file aplikasi Gojek menggunakan *mobile security framework* (MobSF) pada parameter *weak crypto.*



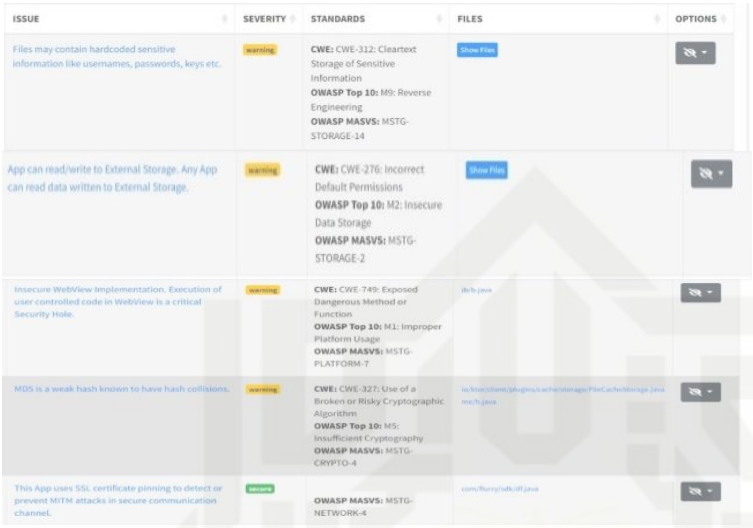
Gambar 10. Bagian *weak crypto* pada aplikasi Gojek

Pada aplikasi Gojek terdapat 1 *warning severity*, 2 *high severity* dan 1 *secure severity*:

1) *Common Weakness Enumeration* (CWE) adalah daftar yang menampilkan keberadaan *bug* pada *software* atau *hardware* yang berbahaya, terdeteksi CWE-330 yang angka ini hanya tergolong (warning), artinya dimana aplikasi ini menggunakan angka acak yang tidak aman.
2) OWASP *The Mobile Application Security Verification Standard* (MASVS) adalah kode analisis sekaligus standar untuk mengukur tingkat keamanan aplikasi seluler. Hasil pengujian menunjukkan bahwa MSTG-CRYPTO-4 yang artinya tergolong aman, aplikasi menggunakan penyematan sertifikat SSL untuk mendeteksi atau mencegah serangan di saluran komunikasi yang aman.
3) Selanjutnya, ditemukan adanya CWE-649 yang mengindikasikan sebuah ketergantungan pada enkripsi input keamanan tanpa adanya pemeriksaan integritas sebelumnya. Aplikasi ini juga diketahui menggunakan mode enkripsi CBC dengan padding PKCS5/PKCS7, yang diketahui sangat rentan terhadap serangan oracle padding. Serangan ini memanfaatkan validasi padding dari pesan terenkripsi dan mengubahnya menjadi ciphertext.
4) Selain ditemukan CWE-649, selanjutnya telah ditemukan pula keberadaan CWE-327. Keberadaan CWE-327 ini menunjukkan adanya penggunaan algoritma kriptografi yang sudah rusak atau usang sehingga

cukup membahayakan. Kode analisis tergolong tinggi (high), aplikasi dapat mengembalikan mode AES ECB secara *default*. Mode ECB diketahui lemah karena mnghasilkan *ciphertext* yang sama untuk *blokplaintext* yang identik.

Pada gambar 11. ditampilkan hasil pengujian pada file aplikasi Maxim menggunakan *mobile security framework* (MobSF) bagian *weak crypto.*

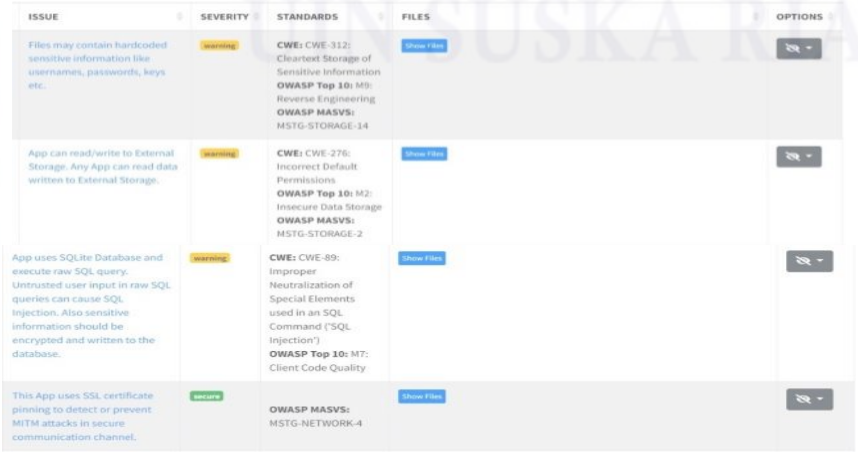


Gambar 11. Bagian *weak crypto* pada aplikasi Maxim

Pada aplikasi Maxim terdapat 4 *warning severity* dan 1 *secure severity*:

1) Terdeteksi CWE-312 penghapusan file yang mungkin berisikan nama pengguna, kata sandi, pada penyimpanan informasi yang sensitif. Kode analisis tergolong (warning).
2) Terdeteksi CWE-276 izin pembawaan yang salah, kode analisis tergolong (warning), dimana aplikasi dapat membaca/menulis ke penyimpanan eksternal.
3) Terdeteksi CWE-749 yang mengungkap metode atau fungsi yang berbahaya, kode analisis tergolong (warning), dimana terdapat implementasi web view tidak aman, eksekusi kode yang dikontrol pengguna di web view adalah lumbung keamanan yang penting.
4) Terdeteksi CWE-327 terdapat penggunaan algoritma kriptografi yang rusak dan tidak aman, kode analisis tergolong (warning), terdapat dimana MD5 yang merupakan *hash* lemah yang memiliki tabrakan *hash*.
5) Terdeteksi kode analisis OWASP MASVS: MSTG-CRYPTO-4, kode analisis ini tergolong aman (secure), aplikasi menggunakan penyematan sertifikat SSL untuk mendeteksi atau mencegah serangan di saluran komunikasi yang aman.

Pada gambar 12. ditampilkan hasil pengujian pada file aplikasi Grab menggunakan *mobile security framework* (MobSF) bagian *weak crypto*.



Gambar 12. Bagian *weak crypto* pada aplikasi Grab

Pada aplikasi Grab terdapat 4 *warning severity* dan 1 *secure severity:*

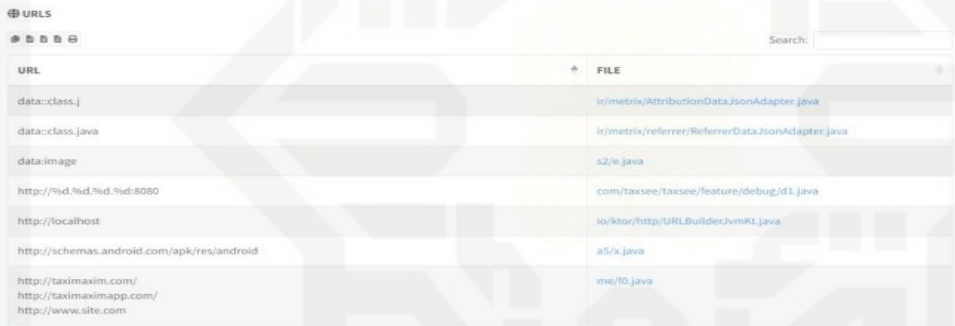
1) Terdeteksi CWE-312 penghapusan file yang mungkin berisikan nama pengguna, kata sandi, pada penyimpanan informasi yang sensitif. Kode analisis tergolong (warning).
2) Terdeteksi CWE-276 izin pembawaan yang salah, kode analisis tergolong (warning), dimana aplikasi apapun dapat membaca/menulis ke penyimpanan eksternal.
3) Terdeteksi CWE-89 netralisasi elemen khusus yang tidak benar yang digunakan dalam perintah sql, kode analisis tergolong (warning), aplikasi menjalankan kueri SQL mentah yang dapat menyebabkan SQL injection, seharus nya infoermasi sensitif harus di enkripsi dan ditulis ke database.
4) Kode analisis OWASP MASVS telah teridentifikasi: MSTG-CRYPTO-4, kode analisis ini telah tergolong aman (secure), karena aplikasi menggunakan penyematan sertifikat SSL untuk mendeteksi atau mencegah serangan di saluran komunikasi yang aman.

C. Root Detection

Root detection adalah analisis yang bertujuan untuk memeriksa apakah aplikasi memiliki kemampuan mendeteksi akses root pada perangkat Android yang digunakan. Pada ketiga aplikasi, yaitu Gojek, Grab, dan Maxim, tidak ditemukan akses root terhadap perangkat. Ini disebabkan oleh super user yang tidak dapat diretas, sehingga aplikasi dianggap aman.

D. SSL Bypass

Pada gambar 13. ditampilkan hasil pengujian pada file aplikasi Maxim menggunakan *mobile security framework* (MobSF) bagian *SSL Bypass*.

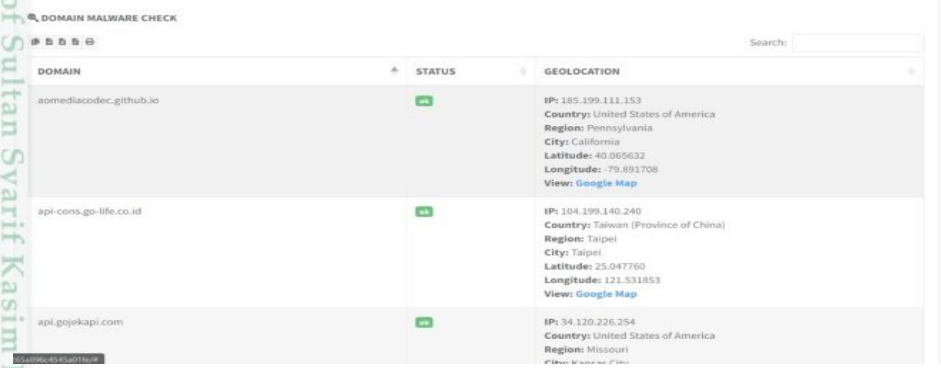


Gambar 13. Bagian URL pada aplikasi Maxim

Hasil pengujian pada aplikasi Maxim ditemukan celah keamanan pada protokol jaringan yang tidak dilengkapi dengan secure socket layers (SSL) sehingga cukup rentan dilakukan peretasan. Pada gambar http://taximaxim.com/ dapat dilihat bahwa url tersebut hanya menggunakan HTTP saja. Akan lebih baik jika url tersebut menggunakan HTTPS agar memiliki perlindungan tambahan dan meminimalisir peretasan dari pihak ketiga.

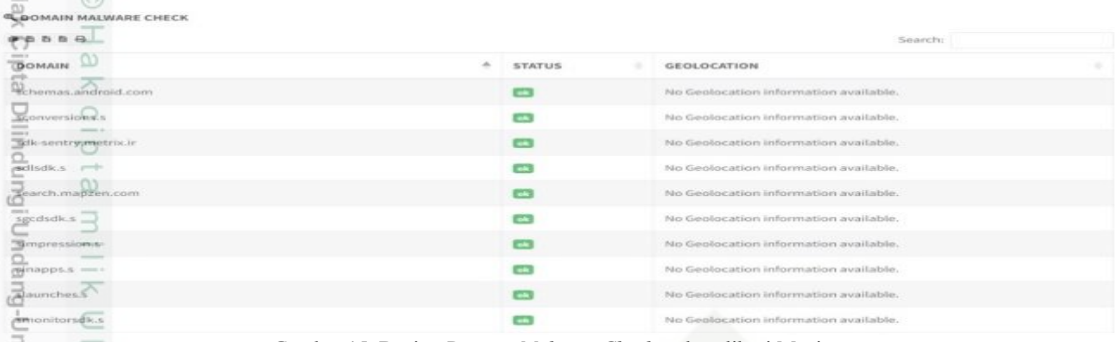
E. Domain Malware Check

Pengujian pada aplikasi Gojek menunjukkan hasil yang baik. Tidak ditemukan domain dengan malware karena status pengujian menunjukkan good. Pada Gambar 14. ditunjukkan hasil analisis pada aplikasi Gojek.



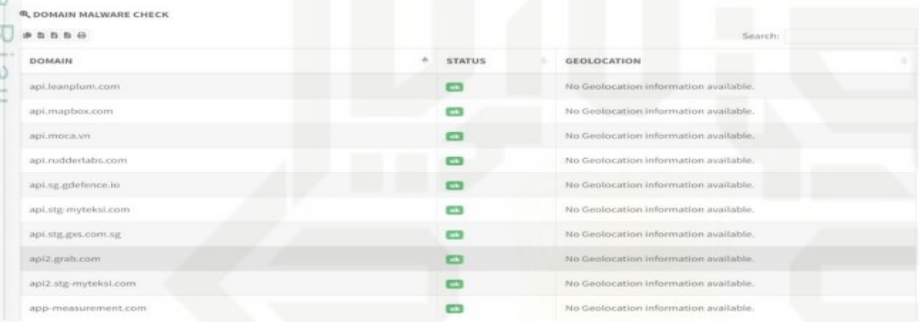
Gambar 14. Bagian *Domain Malware Check* pada aplikasi Gojek

Pengujian pada aplikasi Maxim menunjukkan hasil yang baik. Tidak ditemukan domain dengan malware karena status pengujian menunjukkan good. Pada Gambar 15. ditunjukkan hasil analisis pada aplikasi Maxim.



Gambar 15. Bagian *Domain Malware Check* pada aplikasi Maxim

Pengujian pada aplikasi Grab menunjukkan hasil yang baik. Tidak ditemukan domain dengan malware karena status pengujian menunjukkan good. Pada Gambar 16. ditunjukkan hasil analisis pada aplikasi Grab.



Gambar 16. Bagian *Domain Malware Check* pada aplikasi Grab

Tabel Hasil Analisis Statik

Apk	*Dangerous Permissions*	*Weak Crypto*	*Root Detection*	SSL *Bypass*	*Domain Malware Check*	*Security Score*
Gojek	Ada	Ada	Tidak Ada	Tidak Ada	Baik	44
Maxim	Ada	Ada	Tidak ada	Ada	Baik	47
Grab	Ada	Ada	Tidak ada	Tidak ada	Baik	50

Berdasarkan pengujian pada aplikasi Gojek, Grab dan Maxim dapat disimpulkan bahwa ketiga aplikasi ini memiliki tingkat keamanan yang sedang. Dari ketiganya juga didapatkan aplication permissions yang berstatus dangerous seperti pada gambar 7, 8 dan 9. Pada versi android 11, pengguna memiliki kebebasan untuk memilih memberikan izin akses hanya kali ini saja. Pertanyaan ini biasanya muncul setiap kali ada aplikasi yang membutuhkan izin akses dari pengguna. Misalkan saja izin akses lokasi, mikrofon ataupun kamera. Peneliti dapat memberikan rekomendasi kepada pengguna untuk bijak dalam memanfaatkan fitur izin akses aplikasi. Pengguna harus mempertimbangkan dengan bijak apabila ingin memberikan izin akses kepada daftar penyimpanan dan daftar akun. Jika dirasa tidak terlalu perlu, maka izin akses dapat diabaikan saja guna meminimalisir adanya pencurian data-data pribadi.

Ketiga aplikasi ini juga memiliki celah keamanan atau status perlemahan pada kriptografi, yang berakibat pada pelemahan enkripsi data bagian password seperti pada Gambar 10, 11 dan 12. Maka dari itu, peneliti dapat memberikan rekomendasi agar pihak pengembang menggunakan algoritma lain untuk pembuatan kriptografi. Misalkan kombinasi antara MD5 dengan Vigenere chiper. Vigenere chiper diketahui dapat melakukan beberapa pergeseran yang diwakilkan oleh satu kata kunci. Jika dibandingkan dengan MD5 saja, kombinasi antara MD5 dan vigenere chiper akan memberikan hasil yang lebih optimal karena melakukan proses enkripsi sebanyak dua kali. Selanjutnya, pihak pengembang aplikasi dapat mempertimbangkan penggunaan SHA-3 daripada SHA-1 yang diketahui lebih rentan terhadap serangan brute-force. SHA-3 menjamin keamanan yang lebih baik daripada SHA-1, dan lebih kebal terhadap jenis serangan cyber seperti brute-force. Pada SHA-3, waktu tempuh untuk mendapatkan plaintext 8, 9 dan 10 karater hash diketahui lebih lama [17].

Hasil analisis menunjukkan bahwa ketiga aplikasi transportasi online Gojek, Grab dan Maxim tidak melakukan root terhadap handphone pengguna. Tidak adanya root kepada handphone pengguna akan meminimalisir serangan spyware atau virus. Selain itu, tidak adanya root juga menjadikan pengguna tidak memiliki akses untuk melakukan modifikasi pada aplikasi yang bisa menyebabkan kerusakan dan akhirnya menjadi rentan terhadap peretasan dan memungkinkan dapat masuk ke dalam sistem termasuk data-data yang dimiliki aplikasi

Selanjutnya, pada aplikasi Maxim diketahui bahwa alamat url menggunakan protokol jaringan HTTP saja yang menigkatkan resiko pertukaran data terjadi, berpotensi diserang oleh malware dan virus, serta dapat menurunkan peringkat keamanan apliksi. Pentingnya website bagi perusahaan, maka penting juga untuk mengamankan pertukaran data yang terjadi di website agar client dan perusahaan tidak dirugikan dengan data yang mereka bagikan. Untuk menjamin hal tersebut, salah satu cara untuk mengamankan website adalah dengan cara menggunakan protokol SSL (Secure Socket Layer) [18]. Peneliti memberikan rekomendasi agar pengembang menggunakan protokol HTTPS yang sudah dilengkapi dengan sistem keamanan tambahan dan terenkripsi, HTTPS adalah protokol jaringan dengan SSL. *Secure Socket Layers*(SSL) adalah lapisan keamanan tambahan untuk melindungi komunikasi data antara client dan server. sehingga meminimalisir celah bagi peretas untuk mengakses data pribadi pengguna. url dengan protokol jaringan HTTPS baiknya diterapkan pada saat login, dan data profil pengguna [19].

Ketiga aplikasi transportasi online ini terbebas dari malware. Tujuan domain Malware Check adalah untuk mengetahui segala informasi yang ada di aplikasi Transportasi online agar selalu aman dari dalam, sehingga ketika pengguna meng install aplikasi tidak akan terkena virus-virus atau malware yang membahayakan. Namun, pihak pengembang tetap harus waspada mengingat ada banyak sekali jenis-jenis malware yang tersebar saat ini. Misalkan virus, trojan, spyware dan semacamnya yang memiliki tingkat resiko tinggi apabila menyerang perangkat lunak. Serangan dari malware semacam ini dapat mengganggu bahkan melumpuhkan fungsional dari perangkat lunak [20]. Peneliti merekomendasikan agar pengembang melakukan scanning antivirus secara berkala.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, MobSF dapat digunakan untuk menilai keamanan pada aplikasi transportasi online. Caranya dengan mengunduh file aplikasi transportasi online berformat APK, kemudian mengupload file tersebut ke halaman website MobSF. Selanjutnya, MobSF akan melakukan analisis dan memberikan hasilnya kepada pengguna. Pada aplikasi Gojek, tingkat keamanannya berada pada skor 44. Skor ini membutkikan bahwa aplikasi Gojek memiliki risiko keamanan yang sedang. Lalu pada aplikasi Maxim skor keamanan yang didapatkan adalah 47, artinya aplikasi ini memiliki risiko keamanan yang sedang. Selanjurtnya aplikasi Grab memiliki skor keamanan 50, tingkat risiko tergolong sedang.

Celah keamanan telah ditemukan pada ketiga aplikasi ini berdasarkan analisis parameter dangerous permissions dan weak crypto. Sedangkan analisis menggunakan parameter SSL Bypass hanya menunjukkan aplikasi Maxim yang memiliki celah keamanan. Selanjutnya pada analisis parameter root detection diketahui ketiga aplikasi tidak memiliki root detection.

DAFTAR PUSTAKA

[1] I. Himawan, K. Septianzah, and I. Setiadi, "Analisis Keamanan Informasi Malware Terhadap Aplikasi Apk Dengan Metode Static Analysis Menggunakan Mobsf," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 2, no. 02, pp. 122–127, 2022, doi: 10.30998/jrkt.v2i02.6734.

[2] A. Apriliani, M. Budhiluhoer, A. Jamaludin, and K. Prihandani, "Systematic Literature Review Kepuasan Pelanggan terhadap Jasa Transportasi Online," *Systematics*, vol. 2, no. 1, p. 12, 2020, doi: 10.35706/sys.v2i1.3530.

[3] R. Renaldi and M. Pradana, "SEIKO : Journal of Management & Business Analisis Ekspektasi Penggunaan Aplikasi Transportasi Online Menggunakan Pendekatan Importance Performance Analysis (IPA)," *SEIKO J. Manag. Bus.*, vol. 6, no. 1, pp. 887–897, 2023, doi: 10.37531/sejaman.v6i1.4114.

[4] A. A. Putra, O. D. Nurhayati, and I. P. Windasari, "Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071," *J. Teknol. dan Sist. Komput.*, vol. 4, no. 1, p. 60, 2016, doi: 10.14710/jtsiskom.4.1.2016.60-66.

[5] N. Anwar, S. A. Akbar, A. Azhari, and I. Suryanto, "Ekstraksi Logis Forensik Mobile pada Aplikasi E-Commerce Android," *Mob. Forensics*, vol. 2, no. 1, pp. 1–10, 2020, doi: 10.12928/mf.v2i1.1791.

[6] F. Awanda Alviansyah and E. Ramadhani, "Implementasi Dynamic Application Security Testing pada Aplikasi Berbasis Android," *Automata*, vol. 2, no. 1, pp. 85–90, 2021.

[7] C. Hanifurohman and D. D. Hutagalung, "Analisis Statis Menggunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E-Commerce Berbasis Android," *Sebatik*, vol. 24, no. 1, pp. 22–28, 2020, doi: 10.46984/sebatik.v24i1.920.

[8] F. Nurindahsari and B. Parga Zen, "Analisis Statik Keamanan Aplikasi Video Streaming Berbasis Android Menggunakan Mobile Security Framework (Mobsf)," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 2, pp. 63–80, 2022, doi: 10.14421/csecurity.2021.4.2.3373.

[9] M. H. Rumlus and H. Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik," *J. HAM*, vol. 11, no. 2, p. 285, 2020, doi: 10.30641/ham.2020.11.285-299.

[10] P. Edward and A. N. S. Haprasari, "Analisi Kapabilitas SIPKD BKD Kota Salatiga," *Aiti*, vol. 16, no. 1, pp. 65–87, 2019, doi: 10.24246/aiti.v16i1.65-87.

[11] K. N. Afrina, M. Irwan, and P. Nasution, "Perlindungan Terhadap Penyalahgunaan Data Pribadi Dalam Layanan Transportasi Berbasis Online," *IJM Indones. J. Multidiscip.*, vol. 1, no. 2, pp. 834–840, 2023.
[12] A. Kartono, A. Sularsa, and S. J. I. Ismail, "Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf," *eProceedings ...*, vol. 5, no. 1, pp. 146–151, 2019, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/8563%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/viewFile/8563/8431
[13] P. Studi, S. Informasi, F. Sains, D. A. N. Teknologi, U. Islam, and N. Syarif, "2023 m / 1444 h," 2023.
[14] C. Anwar, C. Herli Sumerli A, N. Rahayu, and K. Kraugusteeliana, "The Application of Mobile Security Framework (MOBSF) and Mobile Application Security Testing Guide to Ensure the Security in Mobile Commerce Applications," *J. Inf. Syst. Technol.*, vol. 5, no. 2, pp. 97–102, 2023, doi: 10.37034/jsisfotek.v5i1.231.
[15] H. Shahriar, M. Arabin Talukder, and M. Saiful Islam, "An Exploratory Analysis of Mobile Security Tools," *KSU Conf. Cybersecurity Educ. Res. Pract.*, 2019, [Online]. Available: https://digitalcommons.kennesaw.edu/ccerphttps://digitalcommons.kennesaw.edu/ccerp/2019/research/4
[16] D. AlQausar, "Tools Penetration Testing Android Terbaik untuk Mendeteksi Kerentanan Aplikasi Mobile," *Biztech.Proxsisgroup.Com*. 2024. [Online]. Available: https://biztech.proxsisgroup.com/tools-penetration-testing-android-terbaik-untuk-mendeteksi-kerentanan-aplikasi-mobile/
[17] F. Kurniawan, A. Kusyanti, and H. Nurwarsito, "Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 803–812, 2017, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/247
[18] R. M. Wahyudi, "Mengimplementasikan SSL/TLS pada Web Server Apache di dalam Jaringan Internal Praktikum untuk Pengembangan Web Server," *J. Majemuk*, vol. 3, no. 1, pp. 13–31, 2024, [Online]. Available: https://jurnalilmiah.org/journal/index.php/majemuk/article/view/655
[19] D. Prayama, Yuhefizar, and Amelia Yolanda, "Protokol HTTPS, Apakah Benar-benar Aman?," *J. Appl. Comput. Sci. Technol.*, vol. 2, no. 1, pp. 7–11, 2021, doi: 10.52158/jacost.v2i1.118.
[20] S. Sinambela, A. R. Pangestu, and R. Feriyanto, "Analisis Aplikasi Malware pada Android dengan Metode Statik," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 3, no. 2, pp. 88–94, 2020, doi: 10.47324/ilkominfo.v3i2.101.

DAFTAR RIWAYAT HIDUP

Triyawan Bagus Subakja, lahirkan di Muara Bungo, Jambi, pada tanggal 26 Juli 2002 dari pasangan Bapak Cholikur Rahman dan Ibu Umi Salmiah Lubis. Peneliti merupakan anak ke-3 dari 4 bersaudara. Pengalaman pendidikan dimulai dengan menyelesaikan (SD) di Sekolah Dasar Negeri 182 kabupaten Tebo pada tahun 2008-2014. Sekolah Menengah Pertama (SMP) di SMPN 2 Bungo pada tahun 2014-2017. Sekolah Menengah Pertama (SMA) di SMAN 1 Bungo pada tahun 2017-2020 dengan jurusan IPA. Pendidikan Sarjana (S1) di Program Studi Sistem Informasi di Universitas Islam Negeri Sultan Syarif Kasim Riau yang terletak di Kota Pekanbaru pada tahun 2020-2025. Selama menjalani masa studi sebagai mahasiswa, telah melaksanakan Kerja Praktek (KP) di Saint Cinnamon Pekanbaru. Disamping itu, juga mengikuti pengabdian Kuliah Kerja Nyata (KKN) di Kelurahaan Sungai Pakning, Bengkalis, Riau. Semoga laporan Tugas Akhir ini mampu memberikan kontribusi pengetahuan yang positif terhadap dunia pendidikan dan perkembangan teknologi yang baru. Terkait pertanyaan dan diskusi mengenai penelitian ini, dapat menghubungi melalui *e-mail* 12050312553@students.uin-suska.ac.id atau instagram @triyawanbaguss.