Jurnal Ilmiah Wahana Pendidikan, Maret 2026, 12 (3.C), 35-46
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/12754
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Analisis Keamanan Aplikasi Café Egg And Butter Berbasis Android Menggunakan Mobile Security Framework (MobSF)

Adhitya Rizkyawan Fadillah[1] , Aji Primajaya[2], Carudin[3]

[1,2,3]Universitas Singaperbangsa Karawang

Received: 06 Februari 2026
Revised: 16 Februari 2026
Accepted: 28 Februari 2026

Abstract

Mobile application security is a crucial aspect of software development, particularly on the Android platform, which has a broad user base and an open-source nature. This study aims to analyze the security level of the Android-based Café EggAndButter application using the Static Application Security Testing (SAST) approach through the Mobile Security Framework (MobSF) tool. The main focus of this research is to determine the security score, identify potential vulnerabilities, and assess the application's security risk level. The analysis result show that the application received a Security Score of 37/100 with Risk Rating Grade of C, indicating a relatively high security risk. Three major vulnerabilities were found: Exported Activity without access control, Insecure Logging, and unencrypted storage of login tokens. Additionally, the use of weak cryptographic algorithms (MD5 and SHA-1) and two requests for dangerous permissions were identified. However, no vulnerabilities related to SSL of malicious domains were found. In conclusion, the application still has several weaknesses that need to be addressed, especially in component management and data protection.

Keywords: *Mobile Application Security, MobSF, Static Analysis, Android*

(*) Corresponding Author: adit.rizki18256@student.unsika.ac.id. aji.primajaya@staff.unsika.ac.id. carudin@staff.unsika.ac.id.

How to Cite: Fadillah, A., Primajaya, A., & Carudin, C. (2026). Analisis Keamanan Aplikasi Café Egg And Butter Berbasis Android Menggunakan Mobile Security Framework (MobSF). *Jurnal Ilmiah Wahana Pendidikan*, *12*(3.C), 35-46. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/12754.

PENDAHULUAN

Dalam beberapa tahun terakir, perkembangan teknologi telah menunjukan peningkatan yang signifikan. Data global dan regional mengindikasikan bahwa adopsi teknologi digital semakin merata dan meluas, seiring dengan peningkatan penetrasi internet dan penggunaan perangkat seluler. Menurut laporan International Telecommunication Union (ITU) dan World Bank, penetrasi internet global telah meningkat dari sekitar 60% pada tahun 2020 menjadi lebih dari 66% pada tahun 2023. Perkembangan ini didorong oleh faktor-faktor seperti peniingkatan ketersediaan infrasruktur jaringan, penurunan biaya perangkat teknologi, serta inovasi dalam layanan digital yang mencakup kecerdasan buatan (AI) Internet of Things (IoT), dan komputasi awan.

Perkembangan teknologi informasi yang pesat telah mendorong peningkatan penggunaan aplikasi seluler dalam berbagai sector, termasuk industri kafe. Aplikasi kafe tidak hanya berperan dalam mempermudah proses pemesanan dan pembayaran, tetapi juga menjadi sarana pengelolaan data pelanggan serta pemasaran digital. Dengan semakin kompleksnya fitur dan layanan yang

ditawarkan, keamanan aplikasi menjadi aspek krusial yang tidak dapat diabaikan. Kerentanan dalam aplikasi dapat membuka celah bagi serangan siber seperti malware, spyware, dan berbagai jenis ancaman lainnya yang berpotensi mengganggu operasional bisnis serta merugikan pengguna.

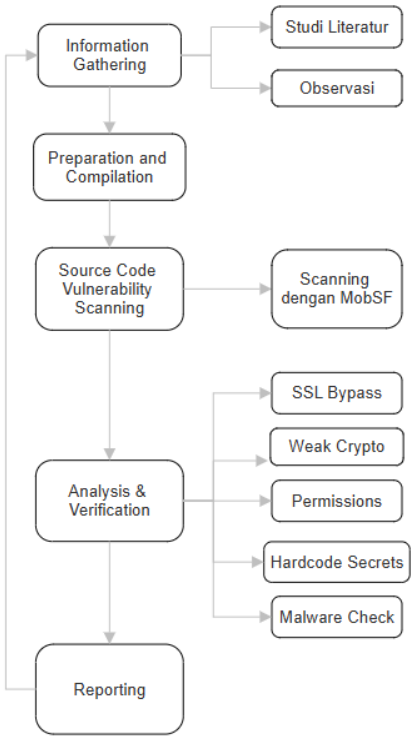
Penggunaan perangkat seluler merupakan salah satu aspek tekologi informasi yang kini berkembang pesat. Dalam beberapa tahun terakir, penggunaan aplikasi seluler telah meningkat di berbagai bidang masyarakat Indonesia. Namun, kejahatan siber seperti kebocoran data juga semakin meningkat di Indonesia. Salah satunya adalah kasus pencurian data pada aplikasi perdagangan seluler di Indonesia, dimana sebanyak lebih dari 90 juta data pengguna diperdagangkan secara illegal oleh peretas di situs gelap. Aplikasi perdagangan seluler juga menyimpan data pengguna yang sensitive untuk digunakan dalam proses bisnisnya, seperti email, kata sandi, alamat, nomor telepon, dan nomor akun (Chairul Anwar, 2023).

Dalam konteks ini, analisis keamanan aplikasi seluler sangat penting untuk mendeteksi dan mengatasi potensi kerentanan sebelum aplikasi digunakan secara luas. Mobile Security Framework (MobSF) merupakan salah satu alat yang banyak digunakan untuk meIakukan pengujian keamanan aplikasi secara otomatis. MobSF mampu melakukan analisis statis dan dinamis, sehingga dapat mengidentifikasi berbagai celah keamanan pada tahap awal pengembangan aplikasi. Dengan kemampuannya untuk menghasilkan laporan yang komprehensif, MobSF membantu pengembang dan pemilik aplikasi untuk mengambil langkah-langkah perbaikan yang diperlukan guna meningkatkan keamanan aplikasi.

Oleh karena itu, diperlukan analisis keamanan apIikasi dengan cara menguji dan mengukur tingkat keamanannya. Salah satu metode yang dapat digunakan untuk menilai keamanan aplikasi adalah Mobile security framework (MobSF). Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan aplikasi café Egg and Butter, serta menambah wawasan mengenai implementasi MobSF dalam mengindentifikasi dan mengatasi kerentanan pada aplikasi seluler. Hasil penelitian ini nantinya diharapkan menjadi acuan bagi pengembang aplikasi dalam meningkatkan sistem keamanan serta memberikan perlindungan yang optimal bagi pengguna.

METODOLOGI PENELITIAN

Dalam penelitian ini menggunakan metodologi Static Application Security Tesing (SAST). Berdasarkan penelitian sebelumnya, banyak yang menggunakan metodologi tersebut dan telah terbukti dapat menemukan kerentanan dalam sebuah aplikasi.



Gambar 1. Rancangan Penelitian

Tahapan untuk menyelesaikan penelitian ini adalah sebagai berikut:

1) *Information Gathering*

Tahap ini penulis menggunakan dua metode yaitu:

a. Studi literatur

Penulis akan mengumpulkan informasi dari berbagai literatur seperti buku, *e-book*, artikel, jurnal, penelitian terdahulu, serta situs internet yang berhubungan dengan masalah dan tujuan penelitian

b. Observasi

Penulis melakukan observasi langsung dengan cara menggunakan dan berinteraksi dengan berbagai fitur yang ada pada aplikasi *café Egg and Butter*. Pendekatan langsung ini dapat memudahkan penulis dalam memahami serta mengumpulkan informasi yang disediakan oleh aplikasi tersebut.

2) *Preparation and Compilation*

Pada tahapan ini penulis akan mempersiapkan bahan-bahan dan alat-alat yang akan digunakan seperti aplikasi *café Egg and Butter* dan juga melakukan instalasi MobSF untuk pengujian.

3) *Source Code Vulnerability Scanning*

Pada tahapan ketiga ini menggunakan MobSF untuk melakukan pemindaian menyeluruh terhadap *source code* aplikasi *café Egg and Butter* yang telah dipersiapkan. penulis memilih MobSF karena MobSF dapat melakukan analisis statis dan dinamis secara otomatis serta dapat melakukan analisis *malware* yang terdapat pada sebuah aplikasi.

4) *Analysis & Verification*

Setelah melakukan pemindaian, hasilnya akan digunakan untuk menganalisis parameter yang telah ditentukan pada MobSF yaitu : *Weak Crypto, SSL Bypass, Hardcode secrets, Dangerous Permissions, Domain Walware Check.*

5) *Reporting*

Setelah melakukan analisis maka akan mendapatkan hasil berupa laporan dari MobSF, dari hasil tersebut maka penulis akan membuat sebuah kesimpulan tentang keamanan aplikasi yang telah di analisis dengan parameter yang telah di tentukan sebelumnya. Yang selanjutnya akan disusun menjadi sebuah kesimpulan dalam bentuk laporan, serta dirangkum agar mudah dipahami dan dibaca

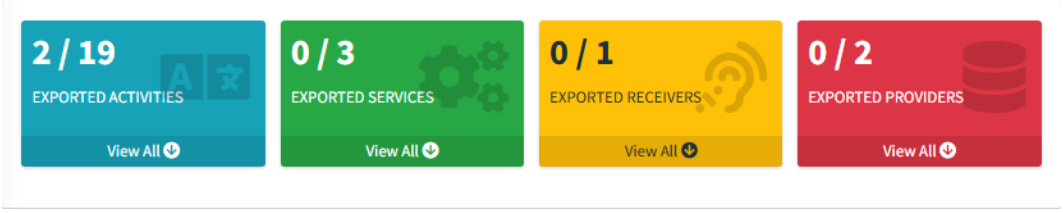
HASIL DAN PEMBAHASAN

Berikut ini merupakan hasil dari tahapan yang dilakukan pada penelitian ini. Perangkat yang digunakan pada penelitian ini adalah sebuah komputer dengan spesifikasi sebagai berikut:

1. AMD Ryzeb 5 3600 6-Core 12 CPUs
2. 16GB RAM
3. Sistem Operasi Windows 10

Tahap 1 – Information Gathering

Melakukan proses pengumpulan informasi terkait lingkungan dan arsitektur dari aplikasi Café EggAndButter berbasis Android. Informasi yang diperoleh bertujuan untuk memberikan pemahaman awal mengenai struktur dan karakteristik aplikasi yang menjadi objek penelitian. Analisis statis dilakukan dengan menggunakan Mobile Security Framework (MobSF), di mana file APK (Application Package File) dari aplikasi Café EggAndButter diunggah ke dalam tools MobSF yang telah dikonfigurasi sebelumnya. Berdasarkan hasil dari MobSF, diketahui bahwa file APK yang dianalisi merupakan aplikasi Cafe EggAndButter versi 1.0 dengan version code 1. Aplikasi ini dikembangkan untuk platform Android dan dirancang agar kompatibel dengan perangkat yang menggunakan minimum API level 24 (Android 7.0 Nougat) serta target SDK pada API level 32 (Android 12). Selain informasi versi dan kompatibilitas, keaslian file APK juga dapat diverifikasi melalui nilai hash yang dihasilkan oleh MobSF, yaitu menggunakan algoritma MD5 (Message Digest 5) dan SHA1 (Secure Hash Algorithm 1).



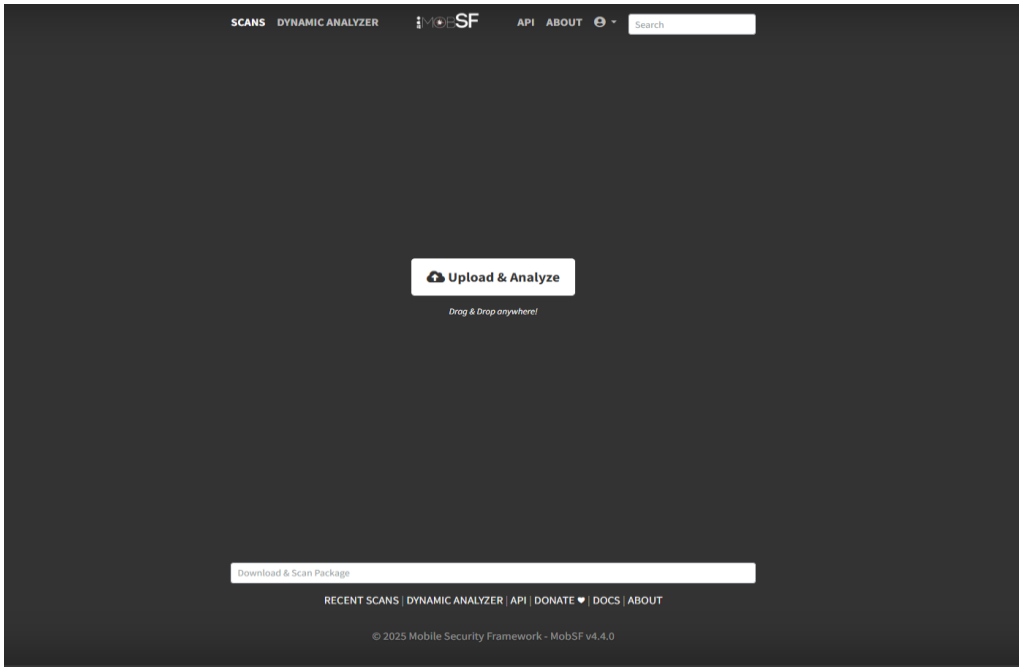
Gambar 2 komponen Aplikasi Café EggAndButter

Berdasarkan gambar 2, MobSF menunjukkan informasi detail terkait komponen-komponen Android yang terdapat dalam aplikasi Cafe EggAndButter. Komponen tersebut meliputi Activities, Services, Receivers, dan Content Providers. Dari hasil pemindaian, diketahui bahwa aplikasi ini memiliki total 19 Activities, 3 Services, 1 Receiver, dan 2 Content Providers. MobSF mengidentifikasi adanya potensi risiko keamanan yang berkaitan dengan konfigurasi komponen. Tercatat bahwa dari 19 komponen activity, terdapat 2 buah

activity yang bersifat exported, artinya komponen tersebut dapat diakses oleh aplikasi lain di luar aplikasi Cafe EggAndButter itu sendiri.

Tahap 2 – Preparation and Compilation

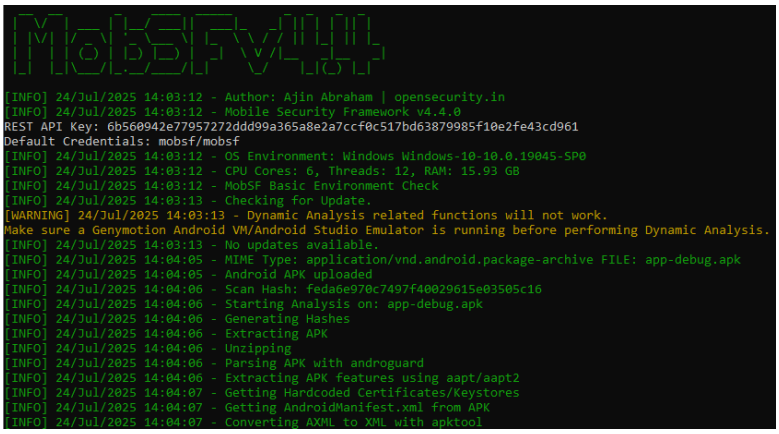
Tahapan ini mencakup proses pengumpulan sumber daya yang diperlukan untuk melakukan pengujian terhadap aplikasi *Café EggAndButter*. Bahan utama yang digunakan adalah file APK dari aplikasi tersebut, yang nantinya akan dianalisis menggunakan alat bantu khusus. Adapun alat yang digunakan dalam proses pengujian adalah *Mobile Security Framework* (MobSF). MobSF akan diunduh dan diinstal pada sistem operasi Windows 10 yang telah disiapkan sebelumnya sebagai lingkungan pengujian.



Gambar 3 Tampilan awal MobSF

Tahap 3 – Source Code Vulnerabillity Scanning

Pada tahapan ini akan dilakukan pemindaian terhadap aplikasi Café EggAndButter, untuk memulai pemindaian yang diperlukan hanyalah mengunggah file APK Café EggAndButter ke MobSF. setelahnya MobSF akan secara otomatis menganalisis Struktur aplikasi (Activities, Services, Receivers, dan Providers), File konfigurasi (AndroidManifest.xml), Penggunaan API dan library, Hardcoded, credentials, Permission dan komponen yang terekspos, dan pola insecure coding secara menyeluruh seperti yang terlihat pada Gambar 4



Gambar 4 Proses analisis statis MobSF

Berdasarkan dari pemindaian kode sumber pada aplikasi *EggAndButter*, MobSF mendeteksi komponen dan potensi kerentanan :

Tabel 1 komponen android

Komponen	Jumlah	Keterangan
Activities	19	2 di antaranya berstatus exported=true
Services	3	Tidak ada yang rentan
Receivers	1	Tidak terekspos
Providers	2	Tidak ditemukan masalah

Tabel 2 Kerentanan yang terdeteksi

Jenis Kerentanan	Lokasi	Deskripsi	Severity
Exported Activity	*LoginActivity, MainActivity*	Komponen dapat diakses aplikasi lain tanpa izin khusus	Medium
Insecure Logging	*MainActivity.java*	Penggunaan *Log.d()* yang mencetak data sensitif	Low
SharedPreferences Tanpa Enkripsi	*SessionManager.java*	Penyimpanan token login tanpa proteksi	Medium

Dari tabel 2, terdapat beberapa potensi kerentanan yang dapat mengancam keamanan data dan pengguna aplikasi jika tidak segera diperbaiki. Berikut penjelasan masing-masing:

1. Exported Activity

Dua aktivitas utama (*LoginActivity* dan *MainActivity*) terdeteksi memiliki properti *android:exported=”true”* tanpa disertai mekanisme pembatasan akses sehingga dapat dimanfaatkan oleh pihak ketiga.

2. Insecure Logging.

Pada file *MainActivity.java*, ditemukan penggunaan perintah *Log.d()* untuk mencetak data ke logcat. Jika data tersebut sensitive (misalnya token, email, atau kata sandi), maka berisiko bocor terutama pada perangkat yang telah di-root.

3. SharedPreferences Tidak Aman

Token login disimpan secara plaintext dalam *SharedPreferences,* tanpa enkripsi

tambahan. Hal ini memungkinkan data tersebut diakses oleh aplikasi lain atau malware pada perangkat, terutama jika sistem keamanan perangkat lemah.

Tahap 4 – Analysis & Verification

Pada tahap ini aplikasi EggAndButter dianalisis menggunakan MobSF (Mobile Security Framework) untuk mengidentifikasi kerentanan keamanan berbasis statis pada file APK, Lima parameter utama yang digunakan dalam analisis ini adalah Weak Crypto, SSL Bypass, Hardcode secrets, Dangerous Permissions, Domain Walware Check.

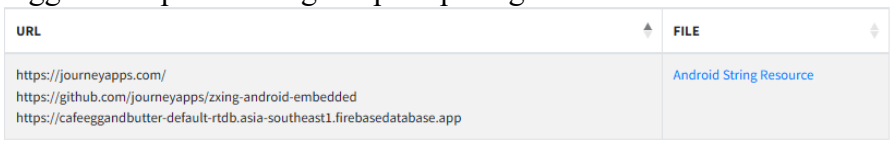
1. *Weak Crypto*

Berdasarkan hasil dari analisis statis yang dilakukan oleh MobSF, ditemukan penggunaan algoritma kriptografi yang dianggap lemah seperti MD5 dan SHA-1 dalam kode aplikasi. Algoritma ini diketahui rentan terhadap serangan *collision* attack dan tidak lagi direkomendasikan dalam standar keamanan modern seperti pada gambar 5.

Gambar 5 *Weak Crypto*

2. *SSL Bypass*

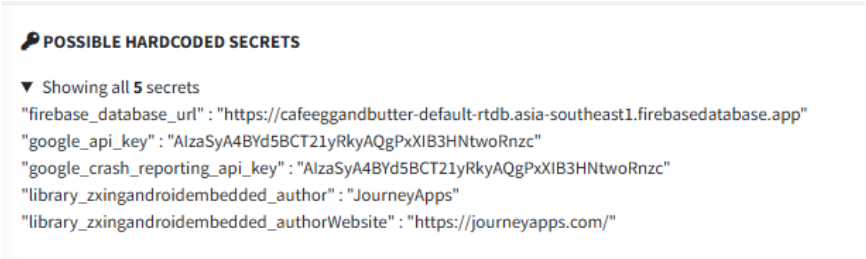
Berdasarkan hasil analisis MobSF, tidak ditemukan kerentanan *SSL Bypass* pada aplikasi *EggAndButter*. MobSF tidak mendeteksi penggunaan *TrustManager* atau *HostnameVerifier* yang mengabaikan proses validasi sertifikat, serta semua domain API yang digunakan aplikasi sudah menggunakan protocol HTTPS. HTTPS (*Hypertext Transfer Protocol Secure*) merupakan pengembangan dari protokol HTTP yang dirancang untuk memberikan keamanan lebih dalam pertukaran data melalui internet. Protokol ini menggunakan teknologi SSL/TLS sebagai metode enkripsi dan autentifikasi, sehingga data yang dikirim antara server dan pengguna tetap terlindungi. Seperti pada gambar 6



Gambar 6 hasil analisis SSL Bypass

3. *Hardcoded Secrets*

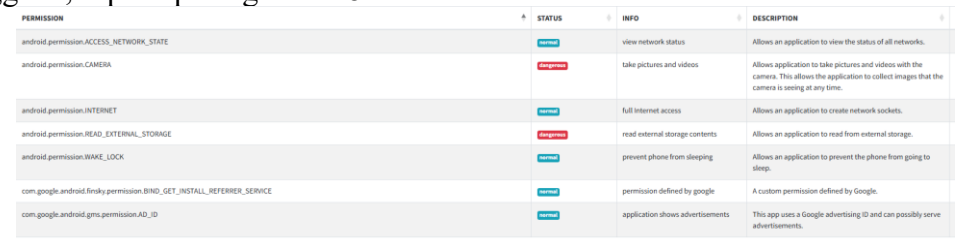
Salah satu temuan yang cukup umum dalam laporan kerentanan keamanan pada aplikasi Android adalah keberadaan *Hardcoded Secrets*, yaitu informasi bersifat rahasia seperti *password, API key,* atau *credential* lainnya yang disisipkan langsung di dalam kode sumber aplikasi. Proses analisis terhadap *Hardcoded Secrets* dilakukan dengan cara menelusuri apakah terdapat data rahasia yang ditanamkan secara langsung ke dalam file APK, baik dalam bentuk teks, konfigurasi, maupun bagian dari kode program. Data yang dimaksud mencakup *credentials, authentication tokens, password,* maupun kunci enkripsi yang semestinya disimpan secara aman di luar kode sumber aplikasi. Berdasarkan hasil analisis yang dilakukan MobSF pada aplikasi *EggAndButter* berkemungkinan terdapat *Hardcoded Secrets,* seperti pada gambar 7



Gambar 7 Hasil analisis *Hardcoded Secrets*

4. *Dangerous Permissions*

Pada aplikasi *EggAndButter* terdapat 7 status perizinan, 5 status perizinan bersifat normal dan 2 status perizinan bersifat *dangerous*. Status perizinan normal adalah perizinan yang tidak berdampak besar terhadap privasi pengguna dan diberikan secara otomatis saat aplikasi diinstal. Sedangkan status perizinan *dangerous* ialah izin yang memungkinkan aplikasi mengakses informasi sensitive atau mengendalikan fitur perangkat yang dapat memengaruhi privasi dan keamanan pengguna, seperti pada gambar 8

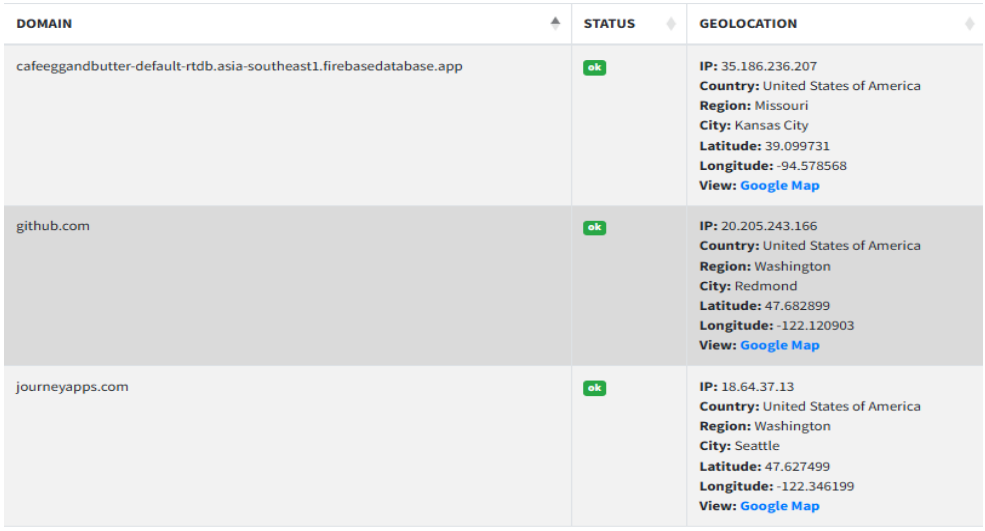


PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

Gambar 8 hasil analisis *Dangerous Permission*

5. *Domain Malware Check*

Analisis terhadap potensi *domain malware* dilakukan dengan memeriksa apakah domain-domain yang digunakan oleh aplikasi termasuk dalam kategori berbahaya atau terindikasi sebagai sumber penyebaran *malware*. Pemeriksaan ini bertujuan untuk mengindentifikasi apakah terdapat koneksi dari aplikasi ke domain yang dicurigai sebagai ancaman keamanan. Berdasarkan hasil analisis pada aplikasi *EggAndButter*, tidak ditemukan adanya domain yang terindikasi sebagai domain berbahaya. Seluruh domain yang terdeteksi diklasifikasi dalam status "OK" atau "GOOD", yang menandakan bahwa domain-domain tersebut aman dan tidak termasuk dalam daftar hitam (*blacklist*) atau sumber *malware* yang diketahui, seperti pada gambar 9



DOMAIN	STATUS	GEOLOCATION
cafeeggandbutter-default-rtdb.asia-southeast1.firebasedatabase.app	ok	**IP:** 35.186.236.207 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
journeyapps.com	ok	**IP:** 18.64.37.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

Gambar 9 Hasil analisis *Domain Malware Check*

Tahap 5 - Reporting

Berdasarkan pada tahap *Source code Vulnerability Scanning* pada aplikasi *Café EggAndButter* terdeteksi sejumlah komponen dan potensi kerentanan. Pada komponen ada *Activity* berjumlah 19 dan 2 di antaranya *exported, Services* berjumlah 3, *Receiver* berjumlah 1, dan *Provider* berjumlah 2. Dan untuk potensi kerentanan terdapat *Exported Activity* yang berlokasi pada *LoginActivity, MainActivity* dengan tingkat *serevity* medium, lalu ada *Insecure Logging* yang berlokasi pada *MainActivity.java* dengan tingkat *severity* Low, dan *SharedPreferences* Tanpa Enkripsi yang berlokasi pada *SessionManager.java* dengan tingkat *serevity* medium

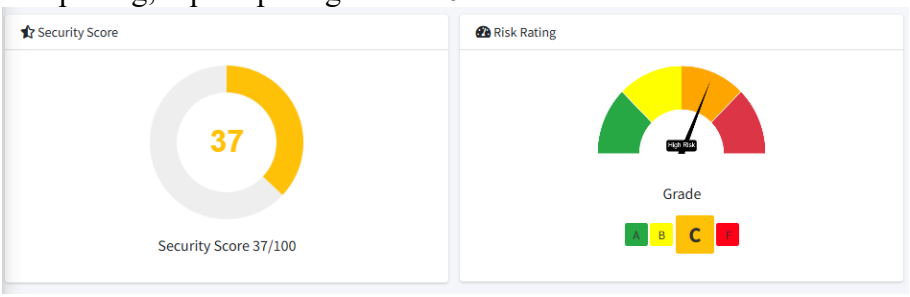
Berdasarkan pada tahap Analysis & Verification yang telah dilakukan dari 5 (lima) parameter yaitu *Weak Crypto, SSL Bypass, Hardcoded Secrets, Dangerous Permision,* dan *Domain Malware Check*. Berikut ringkasan dari hasil analisis berdasarkan parameter yang telah disebutkan:

Tabel 3 Ringkasan analisis 5 parameter

Parameter	Status Temuan	Tingkat Risiko	Rekomendasi
Weak Crypto	Ditemukan	Sedang-Tinggi	Ganti MD5/SHA1 dengan algoritma lebih kuat
SSL Bypass	Tidak ditemukan	Rendah	Tambahkan SSL Pinning sebagai penguat
Hardcoded Secrets	Ditemukan	Tinggi	Jangan simpan API key langsung di dalam kode
Dangerous Permission	Ditemukan	Sedang	Gunakan runtime permission dan batasi izin
Domain Malware Check	Tidak Ditemukan	Rendah	Monitor domain dan pastikan koneksi aman (HTTPS)

Berdasarkan hasil analisis statis pada aplikasi *EggAndButter* dengan menggunakan MobSF, aplikasi tersebut memiliki nilai *Security Score* yang cukup rendah yaitu 37/100 dan *Risk Rating Grade* C, yang menandakan bahwaaplikasi *EggAndButter* sangat berisiko apabila digunakan karna menurut MobSF skor

37/100 merupakan skor yang rendah dan dapat membahayakan perangkat apabila aplikasi dipasang, seperti pada gambar 10



Gambar 10 Tingkat *Security Score* dan *Risk Rating*

CONCLUSION

1. Berdasarkan hasil analisis MobSF aplikasi *EggAndButter* memiliki nilai *Security Score 37/100* dan *Risk Rating Grade* C dan terdapat beberapa potensi kerentanan yang dapat mengancam keamanan data dan pengguna, jenis kerentanan yang ditemukan ada tiga yaitu *Exported Activity, Insecure Logging, dan* SharedPreferences.
2. Pada *Weak Crypto* masih menggunakan algoritma kriptografi yang telah using seperti MD5 dan SHA-1, lalu pada *SSH Bypass* menunjukan bahwa aplikasi tidak memiliki kerentanan terhadap SSL Pinning Bypass, dan telah menggunakan protokol HTTPS secara aman. Pada *Hardcoded Secrets* aplikasi *EggAndButter* berkemungkinan terdapat *Hardcoded Secrets. Pada Dangerous Permissions terdapat 2 status perizininan yang berbahaya yaitu android.permission.CAMERA* dan *android.permission.READ_EXTERNAL_STORAGE . Domain Malware Check* tidak ditemukan domain atau URL yang masuk dalam daftar berbahaya semua komunikasi jaringan diarahkan ke domain yang valid dan menggunakan enkripsi, sehingga risiko eksploitasi dari sisi konektivitas tergolong rendah.
3. Secara keseluruhan, pada aplikasi *EggAndButter* masih memiliki beberapa kelemahan keamanan, terutama pada aspek penyimpanan rahasia dan pengelolaan izin perangkat. Meskipun tidak ditemukan kerentanan kritis, hal terbaik dalam pengembangan aplikasi tetap perlu diterapkan secara menyeluru

REFERENCES

Santoso, B., Ghofur, M. A., & Kuswanto, J. (2021). Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods. Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO), 3(November), 213–222. https://doi.org/10.54706/senastindo.v3.2021.128

Asyaky, M. S., Widiyasono, N., & Gunawan, R. (2018) Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. Jurnal & Penelitian Teknik Informatika. Vol. 3, No. 1.

Sari, D., & Nugroho, A. (2022). Analisis Keamanan Aplikasi Mobile Pada Industri Kafe: Studi Kasus pada Aplikasi XYZ. Jurnal Keamanan Siber, 10(1), 45-56.

Rahman, F., & Pratama, B. (2023). Implementasi Mobile Security Framework

(MobSF) untuk Deteksi Kerentanan Aplikasi Android. Jurnal Teknologi Informasi, 15(2), 101-112.

Wulandari, E., & Gunawan, R. (2024). Pengujian Kemanan Aplikasi Mobile Menggunakan Pendekatan Analisis Statis dan Dinamis. Jurnal Ilmiah Sistem Informasi, 12(1), 67-80.

Nugroho, H., et al. (2025). Evaluasi Keamanan Aplikasi Berbasis Mobile di Era Digital: Pendekatan MobSF. Jurnal Riset Keamanan Digital, 18(3), 89-102.

Gunawan, I., & Melania, E. D. (2021). Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensik Pendekatan Statis Dan Dinamis. SIMETRIS Vol. 15, No. 2. e-ISSN 2686-312X

Hutagalung, D. D., & Hanifurohman, C. (2020). ANALISIS STATIS MENGGUNAKAN MOBILE SECURITY FRAMEWORK UNTUK PENGUJIAN KEAMANAN APLIKASI MOBILE E-COMMERCE BERBASIS ANDROID.SEBATIK. Vol. 24, No. 1.

Setiadi, I., Septianzah, K., & Himawan, I. (2022). ANALISIS KEAMANAN INFORMASI MALWARE TERHADAP APLIKASI APK DENGAN METODE STATIC ANALYSIS MENGGUNAKAN MOBSF. Jurnal Rekayasa Komputasi Terapan (JRKT). Vol. 2, No. 2.

Zhang, Y., Zhou, Y., Qin, z., & Wang, X. (2019). Cryptographic API Misuse in Android Application: A Large-scale Empirical Study. IEEE Transactions on Dependable and Secure Computing, 16(4), 646-660. https://doi.org/10.1109/TDSC.2017.2754492

Ismail, S. J. I., Sularsa, A., & Kartono, A. (2019) MEMBANGUN SISTEM PENGUJIAN KEAMANAN APLIKASI ANDROID MENGGUNAKAN MOBSF. e-Proceeding of Applied Science. Vol. 5, No. 1. 146

Oyetoyan, T. D., Milosheska, B., & Grini M. (2018) Myths and Facts About Static Application Security Testing Tools: An Action Research at Telenor Digital. LNBIP 314, pp. 86-103. https://doi.org/10.1007/978-3-319-91602-6_6

Ardita, K. A., Putra, G. N., & Kustiadie, M. R. (2022) Analisis Keamanan Aplikasi Android Dengan Metode Vulnerability Assessment. Jurnal Elektronik Ilmu Komputer Udayana. Vol 10, No. 3

Kassar, F. A., Clerici, G., & Compagna, L. (2022) Testability Tarpits: the Impact of Code Patterns on the Security Testing of Web Applications. Network and Distributed Systems Security (NDSS).

Yudatama, A. K., & Gunawan, I. (2023) Analisis Keamanan Aplikasi Dompet Digital Pendekatan Statis dan Dinamis. SIMETRIS Vol. 17, No. 1. e-ISSN 2686-312X.

Nugraha, A. C. F., & Yasa, R. N. (2024) Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (*Mobile Security Framework*) Berdasarkan Beberapa Standar. Jurnal Info Kripto, Volume 18 Nomor 1.

Abdillah, R., Trinoto, A. A., & Himawan, I. (2023) STATIC ANALYSIS USING MOBILE SECURITY FRAMEWORK FOR SMART HOME APPLIANCES. JISAMAR Vol. 7 No.3 e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed). 10.52362/jisamar.v7i3.1161.

Anwar, C., Chevy, H, S, A., Sultan, H., Novi, R., & Kraugusteeliana. (2023) The Application of Mobile Security Framework (MOBSF) and Mobile Application Security Testing Guide to Ensure the Security in Mobile

Commerce Appllications. Jurnal Sistim Informasi dan Teknologi. Vol.5 No.2. e-ISSN: 2686-3154

Ilmi, A., Seta, H. B., & Pradnyana, I. W. W. (2022) Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open-Source Security Testing Methodology Manual (OSSTMM) Pada Aplikasi Web Terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta. JURNAL INFORMATIK Edisi ke-18, Nomor 2. ISSN: 2655-139X (ONLINE)

International Telecommunication Union (ITU). (2022) Measuring digital development: Facts and figures 2022.

Al-Delayel, S. A. (2022). Security Analysis of Mobile Banking Application in Qatar. http://arxiv.org/abs/2202.00582

World Bank. (2023). Global Economic Prospects: Digital Dividends.

Abraham, A. 2019. *Mobile Security Framework MobSF*. Available at: https://github.com/MobSF/Mobile-Security-Framework-MobSF