CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 9, No. 1, Mei 2026, hlm. 66-80

Analisis Statik Keamanan Aplikasi Micro-Drama Berbasis Android Menggunakan Mobile Security Framework (MOBFS)

Fransiskus Panca Juniawan[1*], Dwi Yuny Sylfania[2]

[1,2] Program Studi Teknologi Informasi, Universitas Bangka Belitung
Email: [1*]fransiskuspj@ubb.ac.id, [2]dysylfania@ubb.ac.id

Abstrak

Pertumbuhan pesat aplikasi dengan konsep micro-drama berbasis android memberikan pengalaman baru bagi pengguna dalam menonton video berdurasi singkat dengan mode portrait, sehingga meningkatkan kenyamanan dalam mengakses konten digital tersebut. Saat ini telah tersedia banyak aplikasi micro-drama yang dapat dipilih pengguna sesuai preferensi personal sehingga berdampak pada peningkatan penggunaan secara masif sehingga berdampak pula pada pendapatan keuangannya. Namun, aplikasi favorit juga dapat menjadi sasaran bagi penyerang untuk dapat dieksploitasi kelemahannya, seperti penggunaan izin berlebihan, kelemahan konfigurasi kriptografi, penyimpanan data sensitif yang tidak aman, serta potensi kebocoran informasi masih kerap ditemukan pada aplikasi pihak ketiga yang beredar luas di toko aplikasi resmi. Penelitian ini bertujuan untuk menganalisis tingkat keamanan tiga aplikasi micro-drama terbaik berbasis android pada Play Store menggunakan pendekatan Static Application Security Testing (SAST) dengan tool Mobile Security Framework (MobSF). Metodologi penelitian terdiri dari lima tahapan meliputi penentuan kebutuhan aplikasi, instalasi MobSF, pengujian dan pengambilan data uji berdasar lima kriteria, analisis hasil temuan serta rekomendasi kepada pengembang dan pengguna. Hasil analisis menunjukkan bahwa ketiga aplikasi memiliki pola kerentanan yang mirip, namun dengan jumlah yang berbeda. Kerentanan pada kriteria weak crypto menunjukkan bahwa ketiga aplikasi masih memiliki high severity, terutama DramaBox dengan 6 temuan. Pada kategori dangerous permissions, masih ditemukan permission dengan klasifikasi dangerous pada ketiga aplikasi, terutama FreeReels dengan 5 temuan. Pada kategori Domain *Malware Check* memiliki persentase 100%. Sebaliknya, untuk kategori SSL Bypass serta Root Detection, ketiga aplikasi telah memenuhi seluruh standar keamanan pengujian sehingga memiliki hasil analisis yang baik. Selanjutnya dijabarkan rekomendasi kepada pengembang aplikasi berdasarkan hasil analisis statik secara keseluruhan, serta rekomendasi kepada pengguna dengan tujuan agar pengguna aplikasi micro-drama dapat memahami resiko terbesar dari celah keamanan yang ada pada aplikasi. Kebaruan dari penelitian ini adalah adanya pembahasan serta analisis mendalam mengenai issue kerentanan yang ditemukan, mulai dari penyebab, resiko, dampak, hingga skenario nyata yang dapat terjadi pada pengguna aplikasi micro-drama.

Kata kunci: Static Application Security Testing (SAST), Mobile Security Framework (MobSF), Aplikasi Micro-Drama, Weak Crypto, SSL Bypass, Dangerous Permissions, Root Detection, Domain *Malware Check*

*Static Security Analysis Of Android-Based Micro-Drama Application Using Mobile Security Framework (*MOBFS*)*

Abstract

The rapid growth of Android-based micro-drama applications provides a new experience for users in watching short videos in portrait mode, thus increasing the convenience in accessing digital content. Currently, there are many micro-drama applications available for users to choose according to their personal preferences, resulting in a massive increase in usage and thus impacting their financial income. However, favorite applications may be targets for attackers to exploit their vulnerabilities, such as excessive use of permissions, cryptographic configuration weaknesses, insecure storage of sensitive data, and the potential for information leaks are still often found in third-party applications widely circulated in official application stores. This study aims to analyze the security level of the best three of Android-based micro-drama applications on the Play Store using the Static Application Security Testing (SAST) approach with the Mobile Security Framework (MobSF) tool. The research methodology consists of five stages including determining application requirements, installing MobSF, testing and collecting test data based on five criteria, analyzing the findings, and making recommendations to developers and the users. The analysis results show that the three applications have similar vulnerability patterns, but with different numbers. Vulnerabilities in the weak crypto criteria indicate that all three applications still have a high severity, especially DramaBox with 6 findings. In the Dangerous permissions category, permissions classified as dangerous were still found in all three applications, especially FreeReels

with 5 findings. In the Domain Malware Check category, the percentage was 100%. Conversely, for the SSL Bypass and Root Detection categories, all three applications met all security testing standards, resulting in good analysis results. Furthermore, recommendations are outlined for application developers based on the overall static analysis results, as well as recommendations for users with the aim of helping micro-drama application users understand the greatest risks from security vulnerabilities in the application. The novelty of this research is the in-depth discussion and analysis of the vulnerability issues found, starting from the causes, risks, impacts, and real-life scenarios that could occur to micro-drama application users.

***Keywords**: Static Application Security Testing (SAST), Mobile Security Framework (MobSF), Micro-Drama Application, Weak Crypto, SSL Bypass, Dangerous Permissions, Root Detection, Domain Malware Check*

1. PENDAHULUAN

Perkembangan teknologi pada perangkat mobile telah mengubah cara manusia mengakses konten-konten digital secara signifikan. Micro-drama merupakan jenis baru video entertainment yang berasal dari Negara China yang menampilkan vertical video dengan format baru. Karakteristiknya adalah memiliki durasi yang singkat, namun dengan alur cerita yang menarik sehingga mampu mencuri perhatian pengguna internet dari seluruh dunia (Chen, 2025). Terdapat banyak pilihan video micro-drama, serta adanya fitur penghasilan tambahan yang bisa didapatkan pengguna dengan menonton video yang ada dengan konsep pay-per-view, menjadikan aplikasi ini memiliki popularitas yang meningkat dengan signifikan diantara pengguna. Kondisi ini membuat aplikasi micro-drama menjadi industri baru bernilai multi-billion-yuan (Hanney, 2025). Indonesia menjadi negara yang paling banyak menyumbang jumlah viewer micro-drama pada regional Asia Pasifik, dengan 39% dari total penontonnya (Masna, 2025). Hal ini juga didukung dari survey yang diadakan oleh IDN Research Institute kepada generasi Z dan Milenial di Indonesia terhadap durasi tonton micro-drama. 32% dari total responden menonton micro-drama beberapa kali per minggu, dan 29% dari total responden menonton micro-drama hampir setiap hari (Muhamad, 2025). Hal ini membuktikan bahwa micro-drama telah memiliki tempat di hati masyarakat Indonesia.

Terdapat banyak aplikasi dengan kategori Micro-Drama yang tersedia pada Google Play. Pada penelitian ini dipilih tiga aplikasi dengan kriteria: 1) Merupakan aplikasi top 5 pada kategori Entertainment di Google Play; 2) Tidak berbayar; 3) Memiliki review terbanyak; serta 4) Memiliki unduhan terbanyak.

Aplikasi micro-drama menawarkan pengalaman baru dalam mengakses video secara instan melalui perangkat mobile, namun di sisi lain juga membawa tantangan besar dalam aspek keamanan informasi dan perlindungan data pribadi penggunanya. Dengan jutaan unduhan setiap bulannya, aplikasi-aplikasi ini menyimpan dan memproses data sensitif pengguna mulai dari identitas, preferensi konten, lokasi, hingga token otentikasi sehingga menjadi target yang menarik bagi penyerang untuk melakukan eksploitasi kerentanan. Kondisi ini menjadikan aplikasi berpotensi memiliki masalah keamanan, termasuk resiko reverse engineering serta penggunaan izin yang berlebihan yang dapat dieksploitasi. Hal ini dikarenakan banyaknya third-party libraries, API eksternal, dan permintaan izin yang digunakan untuk mendukung fitur pada aplikasi (Kusuma and Putra, 2025).

Penelitian ini bertujuan untuk menganalisis dengan metode statik keamanan dari aplikasi micro-drama berbasis Android yang populer, dengan pendekatan analisis menggunakan Static Application Security Testing (SAST). Tool yang digunakan adalah Mobile Security Framework (MobSF) yang merupakan tool analisis keamanan aplikasi yang mampu melakukan pemeriksaan statik dan dinamis secara otomatis serta menyeluruh terhadap paket aplikasi seperti APK. MobSF juga dikenal karena keunggulannya sebagai penetration testing, analisis malware, dan penyedia framework keamanan terhadap aplikasi mobile pada berbagai sistem operasi (Cahya *et al.*, 2024). MobSF menyediakan kemampuan untuk mengurai struktur aplikasi Android, menilai penggunaan izin, konfigurasi jaringan, kriptografi, serta komponen lain yang berpotensi menimbulkan celah keamanan (Rizkika *et al.*, 2024). Dengan memanfaatkan MobSF, peneliti dapat menghasilkan laporan keamanan terperinci yang menunjukkan area risiko dan rekomendasi mitigasi sejak awal proses pengembangan aplikasi.

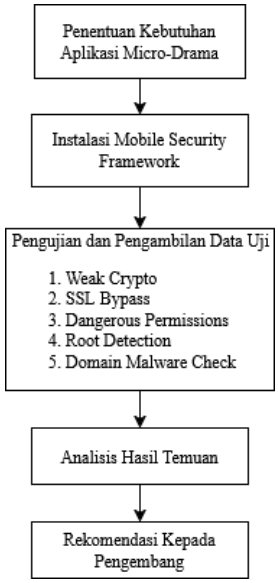
Keunggulan MobSF sebagai alat analisis telah dibuktikan dalam berbagai penelitian sebelumnya, di mana tool ini tidak hanya efektif mendeteksi kerentanan, tetapi juga membantu pengembang memperbaiki kelemahan sebelum aplikasi dirilis kepada publik. Penelitian sebelumnya menggunakan MobSF sebagai tool SAST (Static Application Security Testing) serta AppSweap sebagai tool IAST (Interactive Application Security Testing) dengan hasil adanya peningkatan skor security dari 43 (B) menjadi 78 (A) (Rahayuda, Putu and Santiari, 2026). Penelitian lainnya melakukan analisis statik menggunakan MobSF pada tiga aplikasi video streaming berbasis android dengan hasil ketiganya memiliki dangerous permissoins, weak crypto, dan SSL Bypass (Nurindahsari and Zen, 2021). Uhti melakukan analisis pada aplikasi Mobile JKN

dengan menggunakan pendekatan statik dan dinamis dengan hasil temuan celah keamanan pada Janus, SQL Injection, dan padding oracle attack, s ementara hasil analisis dinamis berupa rendahnya *Root Detection* (Kusreynada and Barkah, 2024). Penelitian oleh Oki melakukan analisis statik keamanan aplikasi Jogo Malang Presisi menggunakan tool MobSF dengan hasil analisa perlunya tindakan untuk mengatasi potensi kelemahan keamanan kriptografi dan sertifikat SSL (Syahputra, Jatmiko and Sanusi, 2024). Dilakukan juga analisis statik pada aplikasi APK android menggunakan tool MobSF dengan hasil skor 56/100 (Himawan, Septianzah and Setiadi, 2023). MobSF juga dapat digunakan untuk melakukan analisis statis terhadap empat aplikasi smart home yang umum digunakan dengan menggunakan metodologi OWASP. Dengan parameter CVSS score, Security score, Tracker detection, dan SSL Certificate Pinning, didapat hasil keempat aplikasi memiliki performa keamanan yang baik (Abdillah, Trinoto and Himawan, 2023). Aplikasi berbasis android yang terpilih di Negara Palestina juga dianalisis keamanannya menggunakan MobSF dengan hasil adanya rekomendasi terhadap aplikasi tersebut untuk mengambil tindakan yang tepat agar dampak negatif dapat dikurangi (Sawalha, Salous and Sawalha, 2025). MobSF juga digunakan untuk melakukan analisis statik terhadap tiga aplikasi transportasi dengan hasil pada parameter *Root Detection* dan Domain *Malware Check* memiliki hasil baik (Subakja, Fronita and Ahsyar, 2025). MobSF juga dapat diterapkan pada berbagai metode pengujian, seperti ISO 27001:2013 untuk melakukan analisis statik dan dinamis dengan melakukan penetration testing pada website Simpel Desa. Dengan menggunakan kontrol 9 (access control) dan 10 (cryptography), analisis statiknya menemukan adanya celah pada aspek kriptografi dan permission access. Analisis dinamisnya menemukan *Root Detection* dan Debugger Check Bypass belum diterapkan (Isnaini *et al.*, 2023). Selain itu metode Vulnerability Assessment juga dapat dikombinasikan dengan MobSF dengan hasil pengujian mendapat skor keamanan aplikasi sebesar 46/100 sehingga harus diperbaiki agar dapat ditingkatkan keamanannnya (Chanarly, Munir and Surasa, 2024). Metode Vulnerability Assessment and Penetration Testing (VAPT) sesuai OWASP Top 10 juga dapat menggunakan MobSF sebagai tool analisisnya dengan hasil beberapa kerentanan seperti M2 Insecure Data Storage, M3 Insecure Communication, M8 Code Tampering, dan M9 Reverse Engineering (Haryanto, Nuraeni and Ahmadi, 2023).

Penggunaan MobSF menunjukkan bahwa analisis statik dapat memberikan wawasan penting tentang bagaimana langkah yang harus dilakukan sebuah aplikasi dalam menangani aspek seperti pemberian izin yang berbahaya, kriptografi, deteksi root, dan konfigurasi terkait keamanan jaringan. Kontribusi penelitian ini adalah adanya rekomendasi praktis berdasar hasil analisis statik yang dapat membantu pengembang dalam mengadopsi praktik keamanan terbaik sehingga publikasi aplikasi dapat dilakukan dalam kondisi keamanan yang lebih baik.

Dari penjabaran penelitian terdahulu diatas, masih banyak ditemukan bahwa hasil analisis masih bersifat teknis dan tidak membahas penyebab, resiko, dampak, serta contoh skenario nyata dari setiap kerentanan yang ditemukan. Penelitian ini mengisi gap penelitian terdahulu tersebut sehingga memiliki kebaruan dengan menampilkan pembahasan inovatif mulai dari penyebab, resiko, dampak, serta contoh skenario nyata setiap kerentanan. Analisis yang ditampilkan bertujuan agar pengguna aplikasi micro-drama dapat mengetahui resiko serta dampak terburuk yang dapat terjadi apabila celah keamanan tersebut dimanfaatkan oleh penyerang.

2. METODE PENELITIAN



Gambar 1. Tahapan Penelitian

Penelitian ini terdiri dari lima tahapan sebagaimana ditampilkan pada Gambar 1. Penelitian ini menggunakan pendekatan eksperimental dengan metode static application security testing untuk mengevaluasi tingkat keamanan aplikasi online streaming berbasis Android. Analisis dilakukan terhadap tiga aplikasi populer yang tersedia secara publik melalui toko aplikasi resmi, dengan tujuan memperoleh gambaran objektif mengenai kondisi keamanan dari sudut pandang kode dan konfigurasi internal aplikasi. Seluruh proses penelitian dilaksanakan secara terstruktur melalui lima tahapan utama, yaitu penentuan kebutuhan aplikasi micro-drama, instalasi MobSF, Pengujian dan pengambilan data, analisis hasil temuan, serta rekomendasi kepada pengembang dan pengguna. Alur ini dirancang agar mampu menghasilkan evaluasi

keamanan yang sistematis, dapat direplikasi, serta relevan dengan praktik audit keamanan aplikasi mobile di lingkungan akademik maupun industri.

2.1. Penentuan Kebutuhan Aplikasi Micro-Drama

Tahap pertama adalah penentuan kebutuhan untuk analisis berupa permasalahan maupun fenomena yang terjadi. Aplikasi micro-drama dipilih karena maraknya penggunaan aplikasi tersebut pada masyarakat saat ini. Adapun kriteria aplikasi micro-drama yang dipilih adalah dapat digunakan di Smartphone, tidak berbayar, merupakan lima aplikasi terbaik pada kategori Entertainment di Google Play, serta memiliki review terbanyak. Untuk itu dipilih tiga aplikasi terbaik, yakni FreeReels, Melolo, dan DramaBox.

Selanjutnya dilakukan ekstraksi ketiga aplikasi menggunakan tools APK Extractor untuk mendapatkan file .apk. Pada tahap ini, setiap APK diverifikasi integritasnya melalui pemeriksaan hash value untuk memastikan bahwa berkas tidak mengalami korup maupun modifikasi selama proses ekstraksi. Detail ketiga aplikasi dapat dilihat pada Tabel 1.

Tabel 1. Aplikasi Online Streaming yang Dianalisis

Nama Aplikasi	Ukuran (MB)	Peringkat	OS minimum	Jumlah Review	Rating
FreeReels	51,49	1	6.0	575.479	4,8
Melolo	49,81	2	6.0	1.692.197	4,8
DramaBox	46,93	4	6.0	4.236.137	4,4

2.2. Instalasi Mobile Security Framework

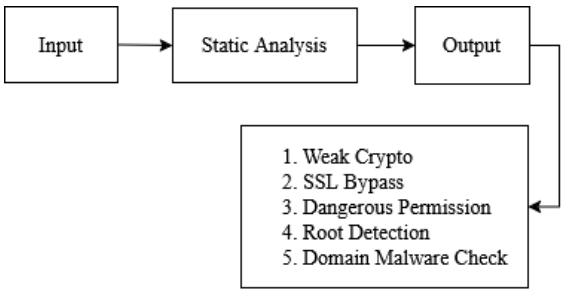
Penggunaan Mobile Security Framework (MobSF) dipilih karena kemampuannya dalam menyajikan analisis statik dan dinamis dari aplikasi berbasis mobile. MobSF juga dapat melakukan pemeriksaan kode sumber, deteksi kerentanan keamanan, serta mensimulasikan serangan terhadap aplikasi berbasis mobile untuk mengidentifikasi celah keamanan yang berpotensi. Pada tahapan ini dilakukan instalasi MobSF versi 4.4.4 yang dijalankan pada lingkungan pengujian dengan sistem operasi Windows 10, prosesor Intel Core i5, dan RAM 8GB. Adapun metode deployment yang digunakan adalah melalui Docker Container untuk menjamin konsistensi environment dan dependensi tools selama proses analisis berlangsung.

2.3. Pengujian dan Pengambilan Data Uji

Tahapan berikutnya adalah menentukan parameter pengujian. Parameter yang diuji pada penelitian ini adalah sebagai berikut:

1. Weak Crypto
2. SSL Bypass
3. Dangerous Permissions
4. Root Detection
5. Domain *Malware Check*

Pengujian menggunakan pendekatan Static Applicatin Security Testing (SAST) dimana menggunakan fitur analisis statik dari tool MobSF. Pengujian selanjutnya dilakukan berdasarkan kelima parameter untuk dapat dianalisis lebih lanjut sebagaimana ditampilkan pada Gambar 4.



Gambar 4. Alur Analisis Statik

2.4. Analisis Hasil Temuan

Tahap keempat adalah analisis hasil temuan, yang merupakan inti dari penelitian ini. Pada tahap ini, data yang telah dikelompokkan dianalisis secara deskriptif dan komparatif antar ketiga aplikasi streaming yang diuji. Analisis mencakup identifikasi pola kerentanan yang paling sering muncul, perbedaan tingkat risiko antar aplikasi, serta area keamanan yang paling membutuhkan perhatian pengembang. Selain itu, setiap kategori temuan dievaluasi berdasarkan implikasinya terhadap privasi pengguna, integritas sistem, dan potensi eksploitasi oleh pihak ketiga, sehingga memungkinkan perumusan rekomendasi mitigasi yang realistis dan aplikatif, seperti pengurangan izin yang tidak perlu, penguatan mekanisme kriptografi, penerapan konfigurasi jaringan yang lebih ketat, serta penggunaan teknik perlindungan kode.

2.5. Rekomendasi Kepada Pengembang dan Pengguna

Tahap terakhir adalah pembuatan rekomendasi kepada pengembang dan pengguna dari ketiga aplikasi yang dianalisis. Pada tahap ini, rekomendasi serta temuan yang ditemukan dari hasil analisis diberikan kepada pengembang sebagai masukan hasil analisis keamanan untuk dapat ditindaklanjuti dengan cara melakukan perbaikan terhadap celah dan kerentanan yang ditemukan. Selain itu juga diberikan rekomendasi berupa edukasi kepada pengguna aplikasi micro-drama.

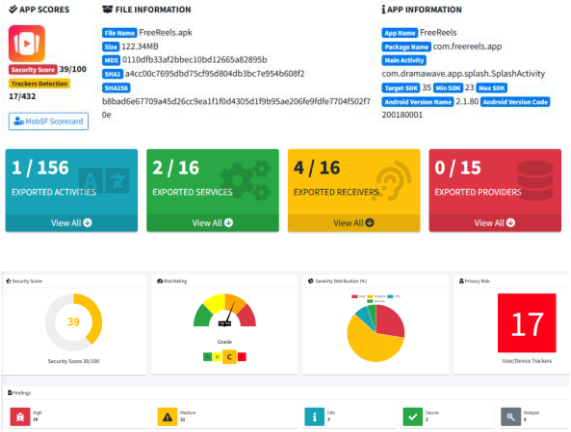
3. HASIL DAN PEMBAHASAN

3.1. Tampilan awal

1. FreeReels

Tampilan MobSF dari hasil analisis aplikasi FreeReels ditampilkan pada Gambar 5. Informasi ditampilkan dengan visual yang baik menggunakan data statistik sehingga menarik untuk dilihat.

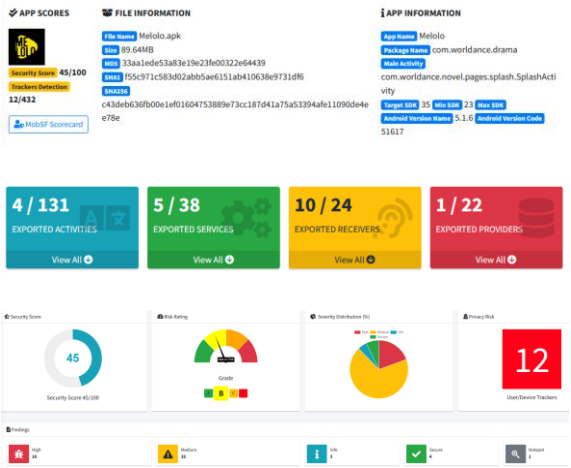
Beberapa data yang ditampilkan berupa File name, Size, MD5, SHA1, SHA256, Target SDK, Min SDK, Max SDK, Exported Activities, Exported Services, Exported Receivers, serta Exported Providers.



Gambar 5. Tampilan Hasil Analisis Statik Aplikasi FreeReels

2. Melolo

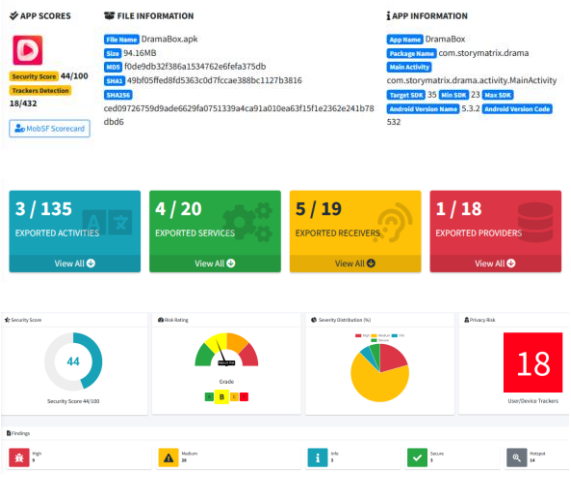
Tampilan hasil analisis statik pada aplikasi Melolo sebagaimana Gambar 6 berikut.



Gambar 6. Tampilan Beranda Analisis Statik Melolo

3. DramaBox

Gambar 7 berikut merupakan tampilan dari hasil analisis statik MobSF dari aplikasi DramaBox.



Gambar 7. Tampilan Hasil Analisis Statik Aplikasi DramaBox

3.2. Weak Crypto

1. FreeReels

Hasil pengujian aplikasi FreeReels untuk parameter Weak Crypto pada Tabel 2. Terdapat variabel issue dan severity dari setiap data.

Tabel 2. Hasil Pengujian Parameter Weak Crypto Aplikasi FreeReels

Issue	Severity
Remote WebView debugging is enabled.	High
The file or SharedPreference is World Writable. Any App can write to the file	High
Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	High
The file or SharedPreference is World Readable. Any App can read from the file	High
The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	High

2. Melolo

Ditampilkan hasil pengujian aplikasi Melolo untuk parameter Weak Crypto pada Tabel 3.

Tabel 3. Hasil Pengujian Parameter Weak Crypto Aplikasi Melolo

Issue	Severity
The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	High
The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	High
The file or SharedPreference is World Readable. Any App can read from the file	High
The file or SharedPreference is World Writable. Any App can write to the file	High

3. DramaBox

Tabel 4 merupakan tampilan hasil pengujian aplikasi DramaBox untuk parameter Weak Crypto.

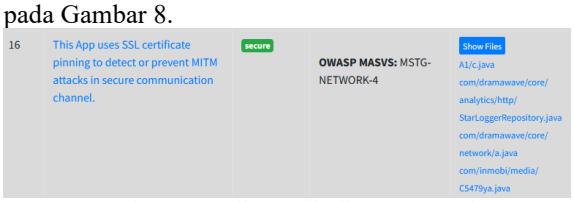
Tabel 4. Hasil Pengujian Parameter Weak Crypto Aplikasi DramaBox

Issue	Severity
The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	High
Remote WebView debugging is enabled.	High
The file or SharedPreference is World Writable. Any App can write to the file	High
Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	High
The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	High
The file or SharedPreference is World Readable. Any App can read from the file	High

3.3. SSL Bypass

1. FreeReels

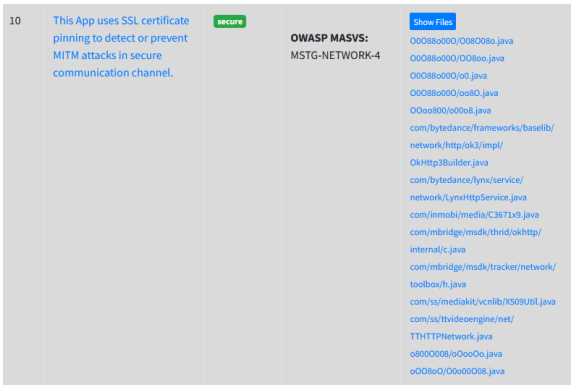
Hasil pengujian SSL Bypass pada aplikasi FreeReels adalah bahwa aplikasi telah menggunakan sertitikat SSL pinning sebagaimana ditampilkan pada Gambar 8.



Gambar 8. Tampilan Hasil Uji SSL FreeReels

2. Melolo

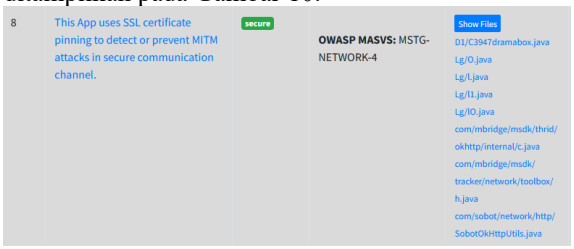
Hasil pengujian SSL Bypass pada aplikasi Melolo adalah bahwa aplikasi telah menggunakan sertifikat SSL pinning yang ditampilkan pada Gambar 9.



Gambar 9. Tampilan Hasil Uji SSL Melolo

3. DramaBox

Hasil pengujian SSL Bypass pada aplikasi DramaBox adalah bahwa aplikasi juga telah menggunakan sertifikat SSL pinning sebagaimana ditampilkan pada Gambar 10.



Gambar 10. Tampilan Hasil Uji SSL DramaBox

3.4. Dangerous Permissions

1. FreeReels

Ditampilkan hasil pengujian aplikasi FreeReels dengan parameter *Dangerous permissions* pada Tabel 5 sebagai berikut.

Tabel 5. Hasil Analisis Parameter *Dangerous permissions* Aplikasi FreeReels

Permissions	Info	Description
android.permission.POST_NOTIFICATIONS	allows an app to post notification	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	read external storage contents	Allows an application to read from external storage
android.permission.READ_PHONE_STATE	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_CALENDAR	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	allow application to recognize physical activity	Allows an application to recognize physical activity.

2. Melolo

Ditampilkan hasil pengujian aplikasi Melolo dengan *Dangerous permissions* yang memiliki status Dangerous pada tabel 6.

Tabel 6. *Dangerous permissions* Aplikasi Melolo

Permissions	Info	Description
android.permission.POST_NOTIFICATIONS	allows an app to post notification	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	read external storage contents	Allows an application to read from external storage
android.permission.WRITE_EXTERNAL_STORAGE	read/modify/delete external storage contents	Allows an application to write to external storage

3. DramaBox

Ditampilkan hasil pengujian aplikasi DramaBox dengan parameter *Dangerous permissions* yang memiliki status Dangerous pada Tabel 7 sebagai berikut:

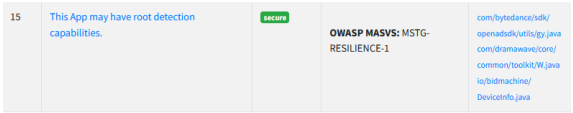
Tabel 7. *Dangerous permissions* Aplikasi DramaBox

Permissions	Info	Description
android.permission.POST_NOTIFICATIONS	allows an app to post notification	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	read external storage contents	Allows an application to read from external storage
android.permission.WRITE_EXTERNAL_STORAGE	read/modify/delete external storage contents	Allows an application to write to external storage

3.5. Root Detection

1. FreeReels

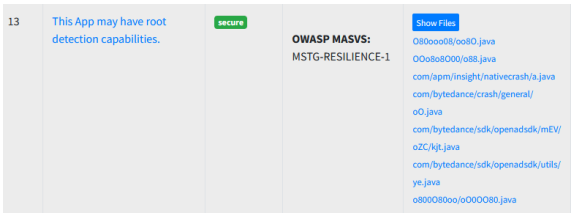
Root Detection adalah analisis yang bertujuan untuk memeriksa apakah aplikasi memiliki kemampuan mendeteksi akses root pada perangkat Android yang digunakan. Tidak ditemukan akses root terhadap perangkat pada aplikasi FreeReels sebagaimana Gambar 11. Hal ini disebabkan oleh super user yang tidak dapat diretas sehingga aplikasi dianggap aman.



Gambar 11. Tampilan Hasil Uji Domain *Root Detection* Aplikasi FreeReels

2. Melolo

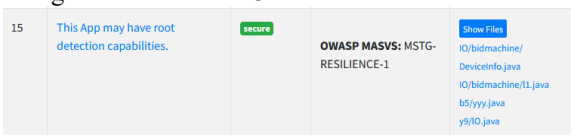
Hasil pengujian *Root Detection* pada aplikasi Melolo menunjukkan bahwa tidak ditemukannya akses root sebagaimana ditampilkan pada Gambar 12.



Gambar 12. Tampilan Hasil Uji Domain *Root Detection* Aplikasi Melolo

3. DramaBox

Hasil pengujian *Root Detection* pada aplikasi DramaBox turut menunjukkan bahwa tidak ditemukannya akses root pada aplikasi DramaBox sebagaimana Gambar 13.

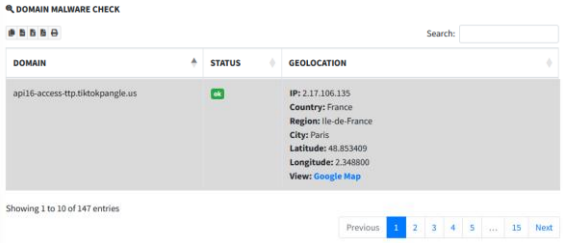


Gambar 13. Tampilan Hasil Uji Domain *Root Detection* Aplikasi DramaBox

3.6. Domain *Malware Check*

1. FreeReels

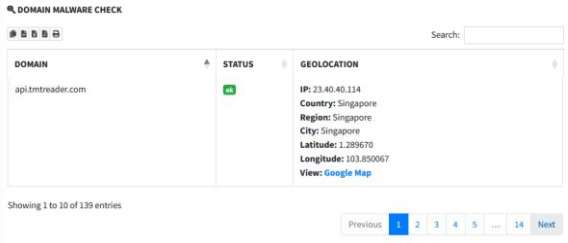
Pengujian Domain Malware pada aplikasi FreeReels sebagaimana Gambar 14 menunjukkan hasil yang baik dimana seluruh 147 data tersebut memiliki status baik.



Gambar 14. Tampilan Hasil Uji Domain Malware FreeReels

2. Melolo

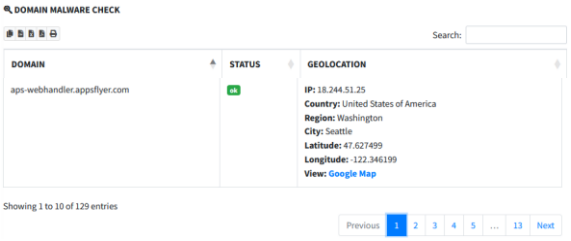
Gambar 15 menampilkan hasil pengujian Domain Malware pada aplikasi Melolo dengan hasil yang baik dimana seluruh 139 data yang diuji memiliki status baik.



Gambar 15. Tampilan Hasil Uji Domain Malware Melolo

3. DramaBox

Pengujian Domain Malware pada aplikasi DramaBox menunjukkan hasil yang baik dimana seluruh 129 data yang diuji memiliki status baik, seperti ditampilkan pada Gambar 16.



Gambar 16. Tampilan Hasil Uji Domain Malware DramaBox

3.7. Pembahasan

Pada bagian ini menjabarkan pembahasan dari hasil temuan analisis statik yang telah dikelompokkan. Tabel 8 menampilkan hasil analisis statik keseluruhan berdasarkan lima parameter yang digunakan.

Tabel 8. Hasil Analisis Statistik Keseluruhan Berdasarkan Lima Parameter

Apk	Weak Crypto		SSL Bypass	Dangerous Permission	Root Detection	Domain *Malware Check*	Security Score	Grade
	High	Warning						
FreeReels	5	9	Ada	5	Ada	147/147	39/100	C
Melolo	4	9	Ada	3	Ada	139/139	45/100	B
DramaBox	6	10	Ada	3	Ada	129/129	44/100	B

Berdasarkan pengujian pada ketiga aplikasi micro-drama FreeReels, Melolo, dan DramaBox, dapat disimpulkan bahwa ketiga aplikasi ini memiliki tingkat keamanan yang beragam. Dibuktikan dengan FreeReels mendapatkan grade C, serta Melolo dan DramaBox mendapatkan grade B dari score board.

3.8. Rekomendasi Pengembang

Dari hasil analisis statik yang telah dilakukan, telah ditelaah dan diberikan rekomendasi perbaikan kepada pengembang aplikasi untuk setiap kasus yang diketahui. Adapun detail perbaikan dijabarkan sebagai berikut:

3.8.1. Weak Crypto

Rekomendasi perbaikan untuk pengembang ketiga aplikasi diatas untuk kategori WeakCrypto adalah sebagai berikut:

1. *Remote WebView debugging is enabled.* Fitur ini memungkinkan akses dan inspeksi konten secara bebas sehingga menjadi security loophole terhadap privasi data pengguna. Untuk itu harus dinonaktifkan pada build produksi, dan hanya dipanggil dalam mode debug saat pengembangan (Anwar and Anderson, 2025)
2. *The file or SharedPreference is World Writable. Any App can write to the file.* Menghapus penggunaan mode MODE_WORLD_WRITEABLE/MODE_WORLD_READABLE dan menggantinya dengan Context.MODE_PRIVATE untuk menghindari risiko manipulasi atau injeksi data oleh aplikasi lain (Mary, 2024).
3. *Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks.* Validasi sertifikat dan konfigurasi yang benar amat diperlukan untuk mencegah potensi MITM (Kusreynada and Barkah, 2024).
4. *The file or SharedPreference is World Readable. Any App can read from the file*. Ganti mode MODE_WORLD_READABLE yang membuka akses read ke file atau SharedPreferences karena memungkinkan aplikasi lain membaca data sensitif yang tersimpan menjadi MODE_PRIVATE atau mekanisme yang aman seperti ContentProvider atau EncryptedSharedPreferences. Pastikan data sensitif dienkripsi sebelum disimpan untuk melindungi dari akses tidak sah. (Martinelli, Mercaldo and Nardone, 2018).
5. *The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext*. Terapkan mode enkripsi modern yang menyediakan authenticated encryption dengan integritas dan kerahasiaan yang lebih kuat seperti AES-GCM atau ChaCha20-Poly1305, serta pastikan diterapkan dengan benar melalui code review dan security testing otomatis sehingga tidak ada konfigurasi ECB di rilisan aplikasi (Heid *et al.*, 2023).
6. *The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks*. Gunakan authenticated encryption seperti AES-GCM atau ChaCha20-Poly1305 yang sekaligus memberikan integritas serta kerahasiaan, serta terapkan Message Authentication Code (MAC) sebelum dekripsi (Kusreynada and Barkah, 2024).

3.8.2. SSL Bypass

Hasil analisis kategori SSL Bypass membuktikan bahwa ketiga aplikasi telah menerapkan sertifikat SSL pinning. Pengembang tetap perlu mengintegrasikan sertifikat SSL pinning sebagai bagian dari strategi pertahanan berlapis (defense in depth) dalam komunikasi aplikasi. Selain itu juga perlu menggabungkannya dengan HTTPS/TLS enforcement, enkripsi kuat, dan audit berkala untuk memastikan proteksi pinning tetap efektif (Ashokan and Kumar, 2024).

3.8.3. Dangerous Permissions

Rekomendasi bagi pengembang ketiga aplikasi untuk kategori *Dangerous Permission* adalah sebagai berikut:

1. android.permission.POST_NOTIFICATIONS. Terapkan prinsip least privilege dalam merancang manifest aplikasi, serta mengevaluasi setiap izin termasuk POST_NOTIFICATIONS dengan teliti untuk memastikan izin tersebut benar-benar diperlukan oleh fitur inti (Pathak, Kumar and Barman, 2024).
2. android.permission.READ_EXTERNAL_STORAGE. Gunakan Scoped Storage, MediaStore API, atau Storage Access Framework (SAF) yang memberikan akses terpilih sesuai kebutuhan aplikasi dan meminimalkan paparan data sensitif tanpa memerlukan izin berbahaya tersebut (Alkinoon *et al.*, 2025).
3. android.permission.READ_PHONE_STATE. Pastikan permission ini diijinkan bila benar-benar diperlukan oleh fitur inti aplikasi, jelaskan juga di kebijakan privasi alasan serta cara pemakaian datanya, serta pertimbangkan alternatif API yang lebih terbatas aksesnya, untuk mematuhi prinsip least privilege dalam desain aplikasi (Tu *et al.*, 2024).
4. android.permission.WRITE_CALENDAR. Tinjau secara kritis kebutuhan WRITE_CALENDAR dengan prinsip least privilege, berikan izin ini ketika aplikasi memiliki fitur inti yang jelas yang membutuhkan kemampuan menulis ke kalender,

dan tambahkan fallback ketika ijinnya ditolak untuk menghindari paparan data sensitif tanpa persetujuan (Alkinoon *et al.*, 2025).

5. com.google.android.gms.permission.ACTIVITY_RECOGNITION. Pastikan bahwa permission ACTIVITY_RECOGNITION hanya diminta ketika benar-benar dibutuhkan oleh fitur inti aplikasi, berikan penjelasan konteks yang jelas kepada pengguna sebelum memintanya. Jika akses aktivitas fisik tidak esensial, sebaiknya hindari permintaan permission ini (Practices, Seray and Google, 2024).
6. android.permission.WRITE_EXTERNAL_STORAGE. Penggunaan izin ini tanpa kontrol yang ketat memungkinkan aplikasi mengakses dan mengubah file shared external storage yang mungkin berisi data pribadi atau konten dari aplikasi lain, sehingga menciptakan jalur bagi aplikasi jahat untuk mengekspos, menimpa, atau menyisipkan konten berbahaya di storage (Liu and Wang, 2024).

3.8.4. Root Detection

Hasil analisis kategori *Root Detection* membuktikan bahwa ketiga aplikasi telah menerapkan deteksi root dengan baik. Namun tetap disarankan untuk mengintegrasikan beberapa metode deteksi root yang robust, menyebar pemeriksaannya diberbagai lapisan aplikasi, serta melakukan uji ketahanan secara berkala terhadap teknik bypass root terbaru (Elsersy, W.F., Anuar, N.B. & Razak, 2023).

3.8.5. Domain *Malware Check*

Hasil analisis kategori Domain *Malware Check* menampilkan hasil yang baik untuk keseluruhan pengujian malware pada ketiga aplikasi. Namun perlu memperkuat proses evaluasi malware dengan menambahkan dynamic feature monitoring pada pipeline keamanan dengan teknik pembelajaran mesin yang memodelkan perilaku runtime aplikasi untuk membantu mendeteksi pola komunikasi terhadap domain berbahaya yang belum teridentifikasi oleh analisis statis (Aldhafferi, 2024).

3.9. Rekomendasi Pengguna

Bagian ini menjabarkan rekomendasi berupa edukasi kepada pengguna aplikasi micro-drama untuk setiap kerentanan yang diketahui. Hal ini bertujuan agar pengguna aplikasi dapat mengetahui penyebab, resiko, dampak, hingga skenario nyata yang dapat terjadi apabila dimanfaatkan oleh penyerang.

Untuk kategori Weak Crypto, terdapat total 6 high issue yang hasil analisisnya dijabarkan pada Tabel 9 berdasarkan penyebab, resiko, dampak, serta skenario nyata yang dapat terjadi pada pengguna aplikasi microdrama. Pada issue [1] dan [3], kesalahan konfigurasi WebView adalah pintu masuk utama bagi serangan injeksi data di ekosistem Android (Wang *et al.*, 2016). Hal ini dapat beresiko penyerang dapat menyuntikkan skrip JS yang berdampak pencurian data maupun pengambilalihan pengguna secara penuh. Selain itu dapat beresiko terjadi serangan Man In The Middle (MITM) karena data yang dikirim tidak terenkripsi secara valid lagi. Pada issue [5] dan [6] penggunaan mode ECB dan CBC tanpa adanya perlindungan tambahan dapat menjadi resiko sistemik (Chatzikonstantinou *et al.*, 2016). Begitu juga dengan issue [2] dan [4] dimana penggunaan SharedPreference yang readable dan writable dapat beresiko terjadinya pencurian identitas digital yang tersimpan di dalam SharedPreference. (Sikder *et al.*, 2020).

Meskipun aplikasi micro-drama tampak tidak berbahaya, temuan beberapa risiko kritis pada fitur WebView, implementasi kriptografi (ECB/CBC), serta SharedPreference menunjukkan bahwa infrastruktur keamanan aplikasi ini masih jauh dari standar industri yang aman karena menempatkan data privasi pengguna microdrama pada posisi yang rentan.

Selain itu hasil analisis ini juga membuktikan bahwa kerentanan yang ditemukan pada kategori Weak Crypto pada aplikasi micro-drama bukan sekadar kesalahan teknis, melainkan hasil dari pertukaran (trade-off) antara kecepatan distribusi konten dengan standar keamanan. Penggunaan mode enkripsi deterministik (ECB) dan pengabaian validasi SSL membuktikan bahwa prioritas pengembang lebih tertuju pada retensi pengguna dan kemudahan akses konten daripada perlindungan integritas transaksi digital pengguna.

Tabel 9. Analisis Kategori Weak Crypto

No	*Issue*	Penyebab	Resiko	Dampak	Real Skenario
1.	*Remote WebView debugging is enabled.*	Pengembang lalai menonaktifkan setWebContentsDebuggingEnabled (true) pada fase produksi	• Penyerang dapat menyuntikkan skrip JS melalui Chrome DevTools jika perangkat terhubung • Penyerang dapat mengeksekusi perintah JavaScript di dalam konteks aplikasi.	Pencurian data menggunakan *session hijacking* dan pengambilalihan akun pengguna secara penuh.	• Penyerang dengan modus tertentu mendapatkan akses fisik ke ponsel korban • Penyerang menghubungkan ponsel ke laptop dan mengaktifkan USB Debugging. • Penyerang dapat melihat seluruh isi WebView aplikasi drama yang sedang terbuka, kemudian menjalankan perintah

No	*Issue*	Penyebab	Resiko	Dampak	Real Skenario
					JavaScript di konsol untuk mencuri Auth-Token atau Cookie akun premium korban.
2.	*The file or SharedPreference is World Writable. Any App can write to the file*	Menggunakan flag MODE_WORLD_WRITABLE dalam penyimpanan lokal.	Adanya manipulasi konfigurasi oleh aplikasi pihak ketiga yang dapat mengubah parameter operasional aplikasi.	Kerusakan integritas data dan potensi sabotase fungsi aplikasi	• Pengguna mengunduh aplikasi lain yang mengandung malware • Malware memindai direktori /data untuk mencari file yang bersifat World Writable. • Malware menemukan file preferensi aplikasi micro-drama dan mengubah isi filenya (misalnya mengganti URL API Endpoint menjadi server milik penyerang) • Saat aplikasi micro-drama dibuka, data pribadi pengguna dikirim ke server penyerang, bukan ke server resmi.
3.	*Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks*	Pengembang mengabaikan verifikasi sertifikat SSL agar aplikasi tetap dapat berjalan meskipun terdapat isu sertifikat SSL di server (Fahl *et al.*, 2012)	Kegagalan validasi SSL memungkinkan penyerang melakukan intersepsi karena berada di tengah jalur komunikasi melalui serangan Man in the Middle (MITM)	Data yang dikirim tidak lagi terenkripsi secara valid, hingga penyadapan seluruh lalu lintas data antara aplikasi dan server.	• Pengguna yang terhubung ke jaringan Wi-Fi publik mendapat serangan MITM dari penyerang. • Penyerang menyajikan sertifikat SSL palsu (self-signed) kepada perangkat korban. • Karena aplikasi diatur untuk mengabaikan kesalahan SSL, aplikasi tidak memberikan peringatan kepada pengguna, sehingga penyerang dapat membaca username, password, dan data kartu kredit saat pengguna melakukan top-up koin drama secara real-time.
4.	*The file or SharedPreference is World Readable. Any App can read from the file*	Menggunakan flag MODE_WORLD_READABLE pada penyimpanan lokal.	Pelanggaran privasi pengguna dan kebocoran informasi rahasia dengan melakukan eksfiltrasi data lokal, maka data sensitif yang seharusnya terisolasi dapat terlihat oleh aplikasi lain tanpa izin.	Data sensitif (user info, API keys) dapat dilihat oleh semua aplikasi lain tanpa izin khusus.	• Aplikasi pihak ketiga meminta izin akses penyimpanan umum, yang secara diam-diam memindai folder data aplikasi micro-drama. • Karena file bersifat World Readable, file SharedPreference berhasil dibaca. • Aplikasi mencuri riwayat tontonan, unik ID perangkat, dan nomor telepon, agar dikirim ke server broker iklan untuk membuat profil pemasaran agresif tanpa seizin pengguna.
5.	*The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.*	Penggunaan algoritma enkripsi Cipher Block Chaining tanpa verifikasi integritas seperti HMAC (Hash-based Message Authentication Code).	Serangan Padding Oracle dimana penyerang dapat mendekripsi pesan tanpa mengetahui kunci sehingga memungkinkan penyerang membedah isi pesan terenkripsi dengan memanfaatkan error messages dari server.	Hilangnya kerahasiaan data meskipun data telah dienkripsi menggunakan standar industri.	• Penyerang mencegat paket data terenkripsi yang dikirim aplikasi • Penyerang mengubah bit terakhir dari blok data terenkripsi dan mengirimkannya kembali ke server. • Server memberikan respon berbeda jika padding salah (misal: error 500) dibanding jika data salah (misal: "invalid data"). • Penyerang mengulangi proses ini ribuan kali secara otomatis untuk menebak isi teks asli blok demi blok, hingga akhirnya berhasil mengetahui isi data asli atau memanipulasi status User Free menjadi Premium.
6.	*The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for*	Menggunakan mode enkripsi tanpa Initialization Vector (IV) sehingga bersifat deterministic (Egele *et al.*, 2013)	Keberhasilan cryptanalysis melakukan Pattern Analysis (analisis pola) teks sandi yang berulang membuat informasi sensitif dapat teridentifikasi	Kebocoran informasi struktural yang memudahkan penyerang menebak data tanpa perlu memecahkan enkripsi secara total	• Penyerang dapat mengakses database aplikasi yang berisi data terenkripsi, dimana terdapat banyak pengguna memiliki blok ciphertext yang identik pada kolom password. • Penyerang mendaftarkan akun baru dengan password yang umum (misal: "123456") dan melihat hasil enkripsinya di database. • Penyerang mencari kecocokan pola

No	*Issue*	Penyebab	Resiko	Dampak	Real Skenario
	identical blocks of plaintext.				tersebut pada ribuan pengguna lain di database. Tanpa perlu memecahkan kunci enkripsi, semua pengguna berpassword lemah berhasil teridentifikasi.

Pada kategori *Dangerous permissions* juga memiliki total 6 permission dengan kategori *Dangerous permissions* yang ditampilkan pada Tabel 10. Analisis dijabarkan berdasarkan resiko, dampak, serta skenario nyata yang penting diketahui oleh pengguna aplikasi microdrama. Permissions yang memiliki status aktif dan sebagaimana Tabel 10 dapat menjadi celah keamanan bagi penyerang untuk masuk pada aplikasi pengguna, yang dijabarkan secara detail sebagai berikut:

Tabel 10. Analisis Kategori Dangerous Permissions

No.	Permissions	Resiko	Dampak	Real Scenario|
1	android.permission.READ_EXTERNAL_STORAGE	Memberikan akses penuh ke penyimpanan publik untuk file foto, video, atau dokumen (Kireet *et al.*, 2019)	Kebocoran data pribadi di luar folder aplikasi dan modifikasi file sistem oleh aplikasi.	• Pengguna memberikan izin penyimpanan agar aplikasi dapat melakukan caching video drama. • Aplikasi secara diam-diam menjalankan fungsi latar belakang untuk memindai folder /DCIM atau /Documents. • Aplikasi mengidentifikasi foto, video, hingga dokumen yang tersimpan di memori ponsel. • Aplikasi mengunggah metadata atau file tersebut ke server pengembang tanpa notifikasi kepada pengguna. • Data tersebut digunakan untuk membangun profil perilaku atau dijual ke pihak ketiga untuk kepentingan iklan tertarget.
2	android.permission.WRITE_EXTERNAL_STORAGE			
3	android.permission.READ_PHONE_STATE	Memberikan akses ke informasi sensitif seperti nomor telepon, IMEI, dan status panggilan.	Pelacakan persisten (persistent tracking) yang tidak dapat dihindari pengguna meskipun aplikasi telah di-instal ulang.	• aplikasi meminta izin mengelola panggilan telepon (READ_PHONE_STATE) saat pertama kali dijalankan • Aplikasi mengambil nomor IMEI dan nomor seri kartu SIM (ICCID), yang dikirim dan disimpan secara permanen di database server pengembang sebagai Unique ID pengguna. • Meskipun pengguna menghapus akun atau mengganti email, pengembang tetap bisa mengenali perangkat tersebut. • Pengembang dapat memblokir akses atau terus mengirimkan iklan yang sangat spesifik berdasarkan riwayat perangkat tersebut secara permanen.
4	android.permission.WRITE_CALENDAR	Penyerang berkemampuan untuk membaca, menambah, atau mengubah jadwal di kalender pribadi pengguna.	Gangguan privasi berupa spamming dan manipulasi jadwal pengguna.	• Aplikasi meminta izin akses kalender pengguna, misalnya dengan modus "mengingatkan jadwal rilis drama baru". • Tanpa konfirmasi eksplisit untuk setiap entri, aplikasi menyuntikkan puluhan jadwal tayang ke kalender utama pengguna. • Aplikasi menyisipkan tautan (URL) promosi di dalam deskripsi acara kalender tersebut. • Pengguna menerima notifikasi terus-menerus dari aplikasi kalender sistem (bukan dari aplikasi drama), yang seringkali sulit untuk dihentikan, sehingga menciptakan gangguan visual dan memaksa pengguna untuk melihat promosi konten setiap kali membuka agenda harian.
5	android.permission.POST_NOTIFICATIONS	Pengiriman notifikasi secara agresif tanpa batasan frekuensi.	Penurunan pengalaman pengguna (UX) dan potensi penggunaan teknik dark patterns untuk memaksa interaksi.	• Pengguna memberikan izin notifikasi agar tidak ketinggalan episode drama. • Aplikasi menggunakan algoritma untuk mendeteksi kapan pengguna sedang tidak aktif. • Aplikasi mengirimkan notifikasi dengan judul yang memancing klik (clickbait) secara repetitif setiap 1 jam. Notifikasi seringkali tidak bisa ditutup dengan mudah atau muncul kembali segera setelah dihapus. • Aktivitas ini menguras baterai perangkat dan dapat mengganggu konsentrasi pengguna melalui gangguan suara dan getaran notifikasi.
6	com.google.android.gms.permission.ACTIVITY_RECOGNITION	Pemantauan aktivitas fisik (berjalan, berlari, berkendara, atau diam) melalui sensor perangkat.	Profiling gaya hidup pengguna secara mendalam yang melampaui kebutuhan fungsional aplikasi video. Data selanjutnya dijual ke pengiklan untuk menentukan profil gaya hidup.	• Aplikasi mengakses sensor akselerometer melalui API Google Play Services. • Aplikasi mencatat waktu kapan pengguna sedang diam (beristirahat) dan kapan pengguna sedang bergerak cepat (berkendara). • Aplikasi menyimpulkan bahwa waktu terbaik untuk mengirimkan iklan drama adalah saat pengguna terdeteksi sedang "diam/istirahat". • Data ini digabungkan dengan lokasi (jika tersedia) untuk mengetahui kebiasaan rutin pengguna. • Informasi privasi tingkat tinggi ini kemudian dikonversi menjadi data pemasaran berharga untuk dapat dijual kepada biro iklan pihak ketiga.

Dari rincian hasil analisis *Dangerous permissions* pada Tabel 10, dapat dilihat bahwa terdapat permintaan izin pada aplikasi micro-drama yang menunjukkan adanya fungsionalitas tersembunyi yang tidak berkaitan dengan pemutaran video micro-drama. Hal ini sejalan dengan penelitian TaintDroid (Enck *et al.*, 2010) yang menyatakan bahwa aplikasi gratis sering kali melakukan eksploitasi data sensor sebagai kompensasi biaya operasional mereka, yang secara langsung mengancam privasi pengguna. Terdapat tiga *Dangerous permissions* yang harus diperhatikan pada aplikasi micro-drama karena penerapannya tidak relevan untuk aplikasi micro-drama.

Fungsi ACTIVITY_RECOGNITION yang dapat mengenali aktivitas fisik dan profiling perilaku pengguna tidaklah relevan dengan aplikasi micro-drama, dan lebih tepat penggunaannya pada aplikasi Kesehatan (Liandana, 2021). Ketidaksesuaian fungsional tersebut dapat menjadi alat pelacakan perilaku pengguna secara harian. Aplikasi dapat membedakan kapan pengguna sedang berjalan cepat, bergerak, berkendara, atau sedang diam. Momen paling berharga bagi aplikasi micro-drama adalah saat pengguna sedang diam dimana pengguna dianggap memiliki waktu luang untuk menonton maupun menerima iklan. Untuk itu pengembang harus menghormati privasi perilaku pengguna. Pengiriman iklan dapat dilakukan melalui analisis data keterlibatan dalam aplikasi (In-app engagement) tanpa harus mengeksploitasi data sensor fisik yang secara fundamental melanggar privasi harian pengguna (Kröger and Raschke, 2019).

Fungsi READ_PHONE_STATE yang merupakan four-tuple *Dangerous permissions* (Gashi, 2018) juga tidak relevan untuk diaktifkan karena menyangkut hak akses ke data identitas perangkat yang sangat sensitif dan bersifat permanen yang sering kali disalahgunakan oleh pengembang untuk kepentingan shadow profiling. Dengan mengantongi identitas permanen ini, pengembang dapat membangun profil pengguna yang tetap ada meskipun pengguna telah menghapus aplikasi, membersihkan cache, atau mengganti akun email.

Selain itu menonton video micro-drama juga tidaklah membutuhkan akses agenda, dimana fungsi WRITE_CALENDAR tidak seharusnya diaktifkan sehingga dapat digunakan sebagai gangguan yang menerapkan pola berulang (Nagging). Nagging merupakan teknik desain manipulatif yang terus-menerus memunculkan gangguan untuk memaksa pengguna melakukan tindakan yang diinginkan pengembang (Gray *et al.*, 2018). Aplikasi seharusnya hanya memanggil fungsi intent setiap kali pengguna secara sadar mengklik tombol 'Ingatkan Saya'. Dengan cara ini, pengguna tetap memegang kendali penuh atas agenda mereka tanpa memberikan akses baca/tulis total kepada aplikasi.

Fungsi READ & WRITE_EXTERNAL_STORAGE juga harus diperhatikan, mengingat aplikasi seharusnya cukup menggunakan Internal Storage tanpa meminta akses ke memori eksternal atau folder publik lainnya. Adanya akses tersebut memungkinkan pemindaian terhadap media lain seperti foto dan video pengguna, sehingga dapat diketahui metadatanya seperti GPS yang tertanam pada foto/video. Untuk mengatasinya, pengembang dapat menggunakan fungsi Scoped Storage. Yang memungkinkan aplikasi melakukan caching video di direktori miliknya sendiri tanpa perlu meminta izin READ/WRITE_EXTERNAL_STORAGE yang berisiko mengintip data pribadi pengguna.

Fungsi POST_NOTIFICATION bertujuan memberikan informasi terkait micro-drama dalam bentuk notifikasi yang muncul pada system tray ponsel pengguna. Post Notification seharusnya bersifat opsional sehingga pengguna dapat memilih apakah ingin diaktifkan atau tidak. Dalam kondisi interupsi paksa, terdapat beberapa resiko yang harus disadari oleh pengguna seperti adanya spam notification yang dapat berdampak pada kenyamanan pengguna. Untuk mengatasinya, pengembang dapat mengkategorikan notifikasi ke dalam beberapa channels seperti Update Episode, Promosi, atau Keamanan Akun. Dengan begitu, pengguna bisa menonaktifkan notifikasi promosi tanpa kehilangan notifikasi rilis episode.

4. KESIMPULAN DAN SARAN

Penelitian ini menganalisis keamanan statik tiga aplikasi Micro-drama berbasis Android menggunakan Mobile Security Framework (MobSF) untuk memperoleh gambaran objektif mengenai postur keamanan aplikasi dari sisi struktur kode dan konfigurasi internal. Melalui tahapan penelitian yang telah dilakukan mulai dari penentuan kebutuhan aplikasi, instalasi MobSF, pengujian dan pengambilan data uji menggunakan lima kriteria, analisis hasil temuan, serta rekomendasi kepada pengembang dan pengguna. Kebaruan pada penelitian ini adalah identifikasi berbagai risiko keamanan yang diketahui pada aplikasi micro-drama dari sudut pandang penyebab, resiko, dampak, serta skenario nyata bagi pengguna aplikasi micro-drama. Temuan utama mencakup penggunaan izin berlebihan serta konfigurasi weak crypto yang masih menggunakan fungsi lama. Kondisi ini membuat diperlukannya update fitur untuk dapat menutup celah keamanan yang ada. Untuk itu diberikan sejumlah rekomendasi bagi pengembang aplikasi, antara lain pembatasan izin berdasarkan prinsip least privilege, penguatan konfigurasi komponen aplikasi, penerapan certificate pinning, penggunaan algoritma

kriptografi modern, serta obfuscation kode yang lebih menyeluruh. Secara umum analisis statik menggunakan MobSF merupakan pendekatan yang relevan dan aplikatif dalam mengevaluasi keamanan aplikasi micro-drama berbasis android. Temuan-temuan yang dihasilkan memperkuat urgensi penerapan prinsip security by design serta audit keamanan berkelanjutan guna menghadapi dinamika ancaman siber pada lingkungan mobile yang terus berkembang. Selain itu dengan adanya rekomendasi berupa edukasi kepada pengguna, diharapkan terjadi peningkatan pengetahuan akan pentingnya mengetahui dampak yang dapat terjadi apabila kerentanan berhasil dieksploitasi.

Penelitian selanjutnya dari penelitian ini dapat melakukan kombinasi analisis statik dengan analisis dinamik, simulasi serangan terkontrol, hingga pemetaan temuan terhadap framework standar keamanan yang komprehensif seperti NIST, OWASP MASVS, hingga ISO/IEC 27001.

5. UCAPAN TERIMA KASIH

Terimakasih yang sebesar-besarnya kami ucapkan kepada Universitas Bangka Belitung yang telah memberikan pendanaan melalui RKA-KL Program Studi Teknologi Informasi tahun anggaran 2026 sehingga penelitian ini dapat terlaksana.

DAFTAR PUSTAKA

Abdillah, R., Trinoto, A.A. and Himawan, I. (2023) "Static Analysis Using Mobile Security Framework For Smart Home Appliances," *Journal of Information System, Applied, Management, Accounting and Research*, 7(3), pp. 760–765. Available at: https://doi.org/10.52362/jisamar.v7i3.1161.

Aldhafferi, N. (2024) "Android Malware Detection Using Support Vector Regression for Dynamic Feature Analysis," *information*, 15(10), pp. 1–23. Available at: https://doi.org/10.3390/info15100658.

Alkinoon, A. *et al.* (2025) "A Comprehensive Analysis of Evolving Permission Usage in Android Apps : Trends , Threats , and Ecosystem Insights," *Journal of Cybersecurity and Privacy*, 5(58), pp. 1–30. Available at: https://doi.org/10.3390/jcp5030058.

Anwar, S. and Anderson, J. (2025) "Privacy-Driven Classification of Contact Tracing Platforms : Architecture and Adoption Insights," *cryptography*, 9(4), pp. 1–42. Available at: https://doi.org/10.3390/cryptography9040060.

Ashokan, P. and Kumar, R. (2024) "Exploring API Security Protocols in ML-Powered Mobile Apps : A Study on IOS and Android Platforms," *Sarcouncil Journal of Engineering and Computer Sciences*, 3(7), pp. 1–7. Available at: https://doi.org/10.5281/zenodo.14423517.

Cahya, A. *et al.* (2024) "Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (Mobile Security Framework) Berdasarkan Beberapa Standar," *Jurnal Info Kripto*, 18(1).

Chanarly, R.A., Munir, A. and Surasa, H. (2024) "Analisis Keamanan Aplikasi Rememberme! Menggunakan Metode Vulnerability Assessment," *Jurnal Kharisma Tech*, 19(2), pp. 27–35.

Chatzikonstantinou, A. *et al.* (2016) "Evaluation of Cryptography Usage in Android Applications," *9th EAI International Conference on Bio-inspired Information and Communications Technologies*. New York: European Union Digital Library. Available at: https://doi.org/10.4108/eai.3-12-2015.2262471.

Chen, Z. (2025) "Micro-drama in the Digital Era: An Analytical Overview of the Emerging Micro-drama Industry," *ICIHCS 2025 Symposium: Integration & Boundaries: Humanities/Arts, Technology and Communication*. Kunming, pp. 159–164. Available at: https://doi.org/10.54254/2753-7064/2025.KM27560.

Egele, M. *et al.* (2013) "An Empirical Study of Cryptographic Misuse in Android Applications," *SIGSAC conference on Computer & communications security*. ACM, pp. 73–83. Available at: https://doi.org/https://doi.org/10.1145/2508859.251669.

Elsersy, W.F., Anuar, N.B. & Razak, M.F.. (2023) "ROOTECTOR: Robust Android Rooting Detection Framework Using Machine Learning Algorithms," *Arabian Journal for Science and Engineering*, 2023, pp. 1771–1791. Available at: https://doi.org/10.1007/s13369-022-06949-5.

Enck, W. *et al.* (2010) "TaintDroid : An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," *USENIX Symposium on Operating Systems Design and Implementation*. USENIX.

Fahl, S. *et al.* (2012) "Why Eve and Mallory Love Android : An Analysis of Android SSL (In) Security Categories and Subject Descriptors," *Conference on Computer and communications secur*. ACM, pp. 50–61. Available at:

https://doi.org/https://doi.org/10.1145/2382196.238220.

Gashi, E. (2018) "Permission-based Privacy Analysis for Android Applications," *International Journal of Business and Technology*, 6(3), pp. 1–11. Available at: https://doi.org/10.33107/ijbte.2018.6.3.02.

Gray, C.M. *et al.* (2018) "The Dark (Patterns) Side of UX Design," *CHI Conference on Human Factors in Computing System*. ADM, pp. 1–14. Available at: https://doi.org/https://doi.org/10.1145/3173574.3174108.

Hanney, R. (2025) *Micro-Drama : From Chinese Phenomenon to Global Trend (Preprint)*. Available at: https://doi.org/10.5281/zenodo.16798457.

Haryanto, M.T., Nuraeni, A. and Ahmadi, A. (2023) "Analsis Keamanan Pada Aplikasi Android Menggunakan Metode Static Vulnerability Assessment and Penetration Testing (VAPT)," *Jurnal Infosecure*, 4(2), pp. 25–32.

Heid, K. *et al.* (2023) "Tracing Cryptographic Agility in Android and iOS Apps," *International Conference on Information Systems Security and Privacy*. Scitepress, pp. 38–45. Available at: https://doi.org/10.5220/0011620000003405.

Himawan, I., Septianzah, K. and Setiadi, I. (2023) "Analisa Resiko Malware Dengan Static MobSF Terhadap Aplikasi Android APK," *Jurnal Technologia*, 14(4), pp. 364–367.

Isnaini, K.N. *et al.* (2023) "Security Analysis of Simpel Desa using Mobile Security Framework and ISO 27002 : 2013," *Jornal Intensif*, 7(1), pp. 84–105.

Kireet, M. *et al.* (2019) "Investigation Of Contemporary Attacks In Android Apps," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 8(12), pp. 1789–1794.

Kröger, J.L. and Raschke, P. (2019) "Privacy Implications of Accelerometer Data : A Review of Possible Inferences," *3rd International Conference on Cryptography, Security and Privacy*. ADM, pp. 81–87. Available at: https://doi.org/10.1145/3309074.3309076.

Kusreynada, S.U. and Barkah, A.S. (2024) "Android Apps Vulnerability Detection with Static and Dynamic Analysis Approach using MOBSF," *Journal of Computer Science an Engineering (JCSE)*, 5(1), pp. 46–63. Available at: https://doi.org/10.36596/jcse.v5i1.789 46.

Kusuma, R.S. and Putra, M.D.P. (2025) "Android Malware Threats : A Strengthened Reverse Engineering Approach to Forensic Analysis," *JISKA (Jurnal Informatika Sunan Kalijaga)*, 10(1), pp. 122–138.

Liandana, M. (2021) "Deteksi Langkah Kaki Berdasarkan Total Akselerasi dan Sudut Kemiringan Menggunakan Sensor Accelerometer pada Smartphone," *Jurnal Explore*, 11(2), pp. 1–7. Available at: https://doi.org/10.35200/explore.v11i2.427.

Liu, M. and Wang, Q. (2024) "Research on android user privacy permission analysis and protection mechanism under big data environment," *International Conference on Physics, Computing and Mathematical*, pp. 1–6. Available at: https://doi.org/10.1051/matecconf/202439501028.

Martinelli, F., Mercaldo, F. and Nardone, V. (2018) "Identifying Insecure Features in Android Applications using Model Checking," *International Conference on Information Systems Security and Privacy*, pp. 589–596. Available at: https://doi.org/10.5220/0006758105890596.

Mary, S.S. (2024) "Common Security Vulnerabilities in Android Apps : A Comprehensive Guide," *International Journal for Multidisciplinary Research (IJFMR)*, 6(6), pp. 1–15. Available at: https://doi.org/10.36948/ijfmr.2024.v06i06.32931.

Masna, A. (2025) *Short dramas are booming in Indonesia with a 39 percent audience share in APAC*.

Muhamad, N. (2025) *Ini Frekuensi Anak Muda RI dalam Mengonsumsi Konten Microdrama*.

Nurindahsari, F. and Zen, B.P. (2021) "ANALISIS STATIK KEAMANAN APLIKASI VIDEO STREAMING BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MOBSF) SECURITY STATIC ANALYSIS OF ANDROID-BASED VIDEO STREAMING APPLICATION USING MOBILE SECURITY FRAMEWORK (MOBSF)," *CyberSecurity dan Forensik Digital*, 4(2), pp. 63–80.

Pathak, A., Kumar, T.S. and Barman, U. (2024) "Static analysis framework for permission - based dataset generation and android malware detection using machine learning," *EURASIP Journal on Information Security*, 2024(33), pp. 1–12. Available at: https://doi.org/10.1186/s13635-024-00182-3.

Practices, B., Seray, G. and Google, T. (2024) "Android Permissions : Evolution , Attacks ," *IEEE Security & Privacy*, 22(6), pp. 40–

49. Available at: https://doi.org/10.1109/MSEC.2024.3461629.

Rahayuda, I.G.S., Putu, N. and Santiari, L. (2026) "Evaluasi Keamanan OTP Firebase pada Aplikasi Android : Perbandingan SAST dan IAST dalam Identifikasi Kerentanan," *JISKA (Jurnal Informatika Sunan Kalijaga)*, 11(1), pp. 13–31.

Rizkika, P. *et al.* (2024) "Analisis Keamanan Pada Aplikasi Himfo Berbasis Android Menggunakan MobSF," *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(4), pp. 5945–5952.

Sawalha, D., Salous, S. and Sawalha, M. (2025) "Security Analysis of Android Applications a Case Study of Applications in Palestine," *Journal of Computer Science and Technology Studies*, 7(6), pp. 49–56. Available at: https://doi.org/10.32996/jcsts.

Sikder, R. *et al.* (2020) "A survey on android security: development and deployment hindrance and best practices," *Telkomnika*, 18(1), pp. 485–499. Available at: https://doi.org/10.12928/TELKOMNIKA.v18i1.13288.

Subakja, T.B., Fronita, M. and Ahsyar, T.K. (2025) "Analisis Perbandingan Keamanan Aplikasi Transportasi Online Berbasis Android Menggunakan Mobile Security Framework (MobSF)," *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI)*, 10(2), pp. 1823–1837.

Syahputra, O.K., Jatmiko, A.R. and Sanusi, A.P. (2024) "Evaluasi Keamanan Aplikasi Jogo Malang Presisi dengan Metode Mobile Security Framework (MOBSF) melalui Analisis Statis," *Seminar Nasional Sistem Informasi*. Malang, pp. 4796–4802.

Tu, T. *et al.* (2024) "Intelligent analysis of android application privacy policy and permission consistency," *Artificial Intelligence Review*, 57(7), pp. 1–21. Available at: https://doi.org/10.1007/s10462-024-10798-z.

Wang, W. *et al.* (2016) "Privacy Leakage Detection of WebView Based on TaintDroid Extension," *Computer Engineering*, 42(10), pp. 169–175. Available at: https://doi.org/10.3969/j.issn.1000-3428.2016.10.030.