

**ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE  
MENGUNAKAN ANALISIS STATIS DENGAN TOOLS  
MOBILE SECURITY FRAMEWORK (MOBSF)**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**MUHAMMAD PRIANDIKA BAYU FIRDAUS**

**22.83.0798**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2026**

**ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE  
MENGUNAKAN ANALISIS STATIS DENGAN TOOLS  
MOBILE SECURITY FRAMEWORK (MOBSF)**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**MUHAMMAD PRIANDIKA BAYU FIRDAUS**

**22.83.0798**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2026**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE  
MENGUNAKAN ANALISIS STATIS DENGAN TOOLS MOBILE  
SECURITY FRAMEWORK (MOBSF)**

yang disusun dan diajukan oleh

**Muhammad Priandika Bayu Firdaus**

**22.83.0798**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 24 Februari 2026

Dosen Pembimbing,

**Dr. Dony Arvus, S.S., M.Kom.**

**NIK. 190302128**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE  
MENGUNAKAN ANALISIS STATIS DENGAN TOOLS MOBILE  
SECURITY FRAMEWORK (MOBSF)**

yang disusun dan diajukan oleh

**Muhammad Priandika Bayu Firdaus**

**22.83.0798**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 24 Februari 2026

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Melwin Syafrizal, S.Kom., M.Eng., Ph.D.**  
**NIK. 190302105**



**Rina Pramitasari, S.Si., M.Cs.**  
**NIK. 190302335**



**Dr. Dony Ariyus, S.S., M.Kom.**  
**NIK. 190302128**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 24 Februari 2026

**DEKAN FAKULTAS ILMU KOMPUTER**



**Prof. Dr. Kusriani, M.Kom.**  
**NIK. 190302106**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Priandika Bayu Firdaus  
NIM : 22.83.0798

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE  
MENGUNAKAN ANALISIS STATIS DENGAN TOOLS MOBILE  
SECURITY FRAMEWORK (MOBSF)**

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 24 Februari 2026

Yang Menyatakan,



Muhammad Priandika Bayu Firdaus

## HALAMAN PERSEMBAHAN

Dengan tulus dan penuh rasa syukur, penulis ingin menyampaikan penghargaan dan persembahan kepada pihak yang telah memberikan dukungan dan kontribusi dalam penulisan skripsi ini. Oleh karena itu dengan bahagia saya ucapkan rasa syukur dan terima kasih kepada:

1. Allah SWT, atas rahmat dan hidayah-Nya yang telah melimpahkan kemudahan dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini dengan penuh ketenangan dan kesabaran.
2. Dengan ini saya persembahkan karya ini untuk kedua orang tua saya.
3. Terima kasih atas keluarga besar yang telah memberi doa serta dukungan secara emosional.
4. Bapak Dr Dony Ariyus, S.S., M.Kom. selaku dosen pembimbing selama skripsi, terima kasih atas bimbingan, arahan, dan masukan yang berharga selama proses penulisan skripsi ini.
5. Ucapan terima kasih saya persembahkan juga untuk seluruh teman teman saya di prodi Teknik Komputer Angkatan 2022.
6. Teman-teman terdekat. Terima kasih atas dukungan, semangat, dan keceriaan yang selalu menjadi penyeimbang dalam setiap Langkah penulisan skripsi ini.

## KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi yang berjudul "ANALISIS KERENTANAN PADA APLIKASI MARKETPLACE MENGGUNAKAN ANALISIS STATIS DENGAN TOOLS MOBILE SECURITY FRAMEWORK (MOBSF)" ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Komputer di Universitas Amikom Yogyakarta. Penulis menyadari bahwa tanpa dukungan dari berbagai pihak, penyelesaian skripsi ini tidak akan dapat terlaksana dengan baik. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr Dony Ariyus, S.S., M.Kom. selaku Dosen Pembimbing yang telah memberikan bimbingan, arahan, dan masukan yang sangat berharga selama proses penyusunan skripsi ini.
2. Tim Dosen Penguji, yang telah memberikan kritik, saran, dan evaluasi yang membangun untuk meningkatkan kualitas skripsi ini.
3. Orang tua penulis, yang selalu memberikan dukungan moral, material, dan doa yang tak terhingga sepanjang perjalanan pendidikan ini.

Penulis juga mengucapkan terima kasih kepada teman-teman, rekan sejawat, serta semua pihak yang tidak dapat disebutkan satu per satu, atas dukungan dan bantuan yang telah diberikan.

Semoga skripsi ini dapat memberikan kontribusi positif bagi perkembangan ilmu pengetahuan, khususnya di bidang cyber. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk penyempurnaan karya ini.

Yogyakarta, 24 Februari 2026

Penulis

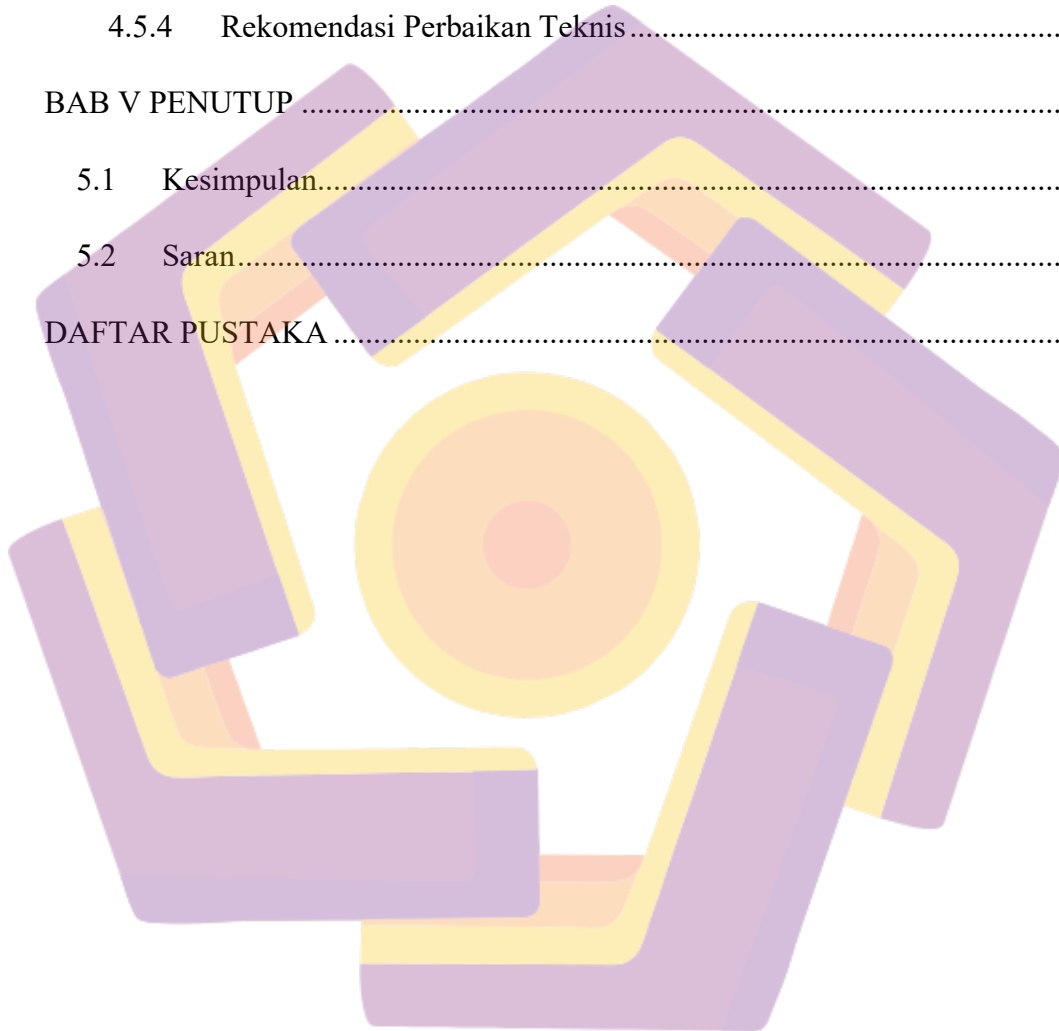
## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iv
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR .....	xiii
DAFTAR LAMBANG DAN SINGKATAN .....	xiv
DAFTAR ISTILAH .....	xv
INTISARI .....	xvii
<i>ABSTRACT</i> .....	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA .....	6

2.1	Studi Literatur .....	6
2.2	Dasar Teori.....	10
2.2.1	Keamanan Aplikasi Mobile ( <i>Mobile Application Security</i> ).....	10
2.2.2	Analisis Keamanan ( <i>Security Analysis</i> ).....	10
2.2.3	<i>Mobile Security Framework</i> (MobSF).....	11
2.2.4	OWASP <i>Mobile Top 10</i> .....	12
2.2.5	Marketplace ( <i>E-Commerce</i> ).....	14
BAB III METODE PENELITIAN .....		16
3.1	Objek Penelitian .....	16
3.2	Alur Penelitian.....	17
3.3	Alat dan Bahan .....	19
3.3.1	Perangkat Keras ( <i>Hardware</i> ) .....	19
3.3.2	Perangkat Lunak ( <i>Software</i> ).....	20
3.4	Desain Pipeline Analisis.....	21
3.5	Prosedur Penelitian.....	23
3.5.1	Instalasi MobSF pada Windows .....	23
3.5.2	Akuisisi Data (Ekstraksi APK) .....	23
3.5.3	Pelaksanaan Analisis Statis.....	24
3.6	Analisis Data .....	24
3.6.1	Analisis Izin ( <i>Permission Analysis</i> ).....	24
3.6.2	Analisis Keamanan Kode & Kriptografi.....	24
3.6.3	Klasifikasi Risiko ( <i>Risk Scoring</i> ).....	25

BAB IV HASIL DAN PEMBAHASAN .....	26
4.1 Implementasi Lingkungan dan Prosedur Pengujian.....	26
4.1.1 Konfigurasi Lingkungan Analisis .....	26
4.1.2 Prosedur Akuisisi Objek Penelitian .....	27
4.2 Hasil Analisis Statis Aplikasi Tokopedia.....	27
4.2.1 Verifikasi Identitas dan Integritas Berkas ( <i>File Integrity</i> ).....	27
4.2.2 Penilaian Skor Keamanan ( <i>Security Score &amp; Grade</i> ).....	29
4.2.3 Statistik Kerentanan ( <i>Findings Severity</i> ) .....	31
4.2.4 Analisis Pelacak Pihak Ketiga ( <i>Trackers Analysis</i> ).....	33
4.2.5 Analisis Manajemen Izin Aplikasi ( <i>Permissions Analysis</i> ).....	35
4.3 Hasil Analisis Statis Aplikasi Shopee .....	41
4.3.1 Verifikasi Identitas dan Integritas Berkas ( <i>File Integrity</i> ).....	41
4.3.2 Penilaian Skor Keamanan ( <i>Security Score &amp; Grade</i> ).....	43
4.3.3 Statistik Kerentanan ( <i>Findings Severity</i> ) .....	44
4.3.4 Analisis Pelacak Pihak Ketiga ( <i>Trackers Analysis</i> ).....	46
4.3.5 Analisis Manajemen Izin Aplikasi ( <i>Permissions Analysis</i> ).....	49
4.4 Hasil Analisis Statis Aplikasi Lazada .....	58
4.4.1 Identifikasi dan Integritas Berkas ( <i>File Integrity</i> ).....	58
4.4.2 Penilaian Skor Keamanan ( <i>Security Score &amp; Grade</i> ).....	59
4.4.3 Statistik Kerentanan ( <i>Findings Severity</i> ) .....	61
4.4.4 Analisis Pelacak Pihak Ketiga ( <i>Trackers Analysis</i> ).....	62
4.4.5 Analisis Manajemen Izin Aplikasi ( <i>Permissions Analysis</i> ).....	65

4.5	Pembahasan Komparatif ( <i>Comparative Discussion</i> ) .....	72
4.5.1	Komparasi Tingkat Keamanan Kode ( <i>Security Score</i> ).....	72
4.5.2	Komparasi Agresivitas Izin ( <i>Permission Aggressiveness</i> ).....	73
4.5.3	Paradoks Privasi: Keamanan Kode vs. Minimalisme Data.....	74
4.5.4	Rekomendasi Perbaikan Teknis .....	75
BAB V PENUTUP .....		77
5.1	Kesimpulan.....	77
5.2	Saran.....	78
DAFTAR PUSTAKA .....		81

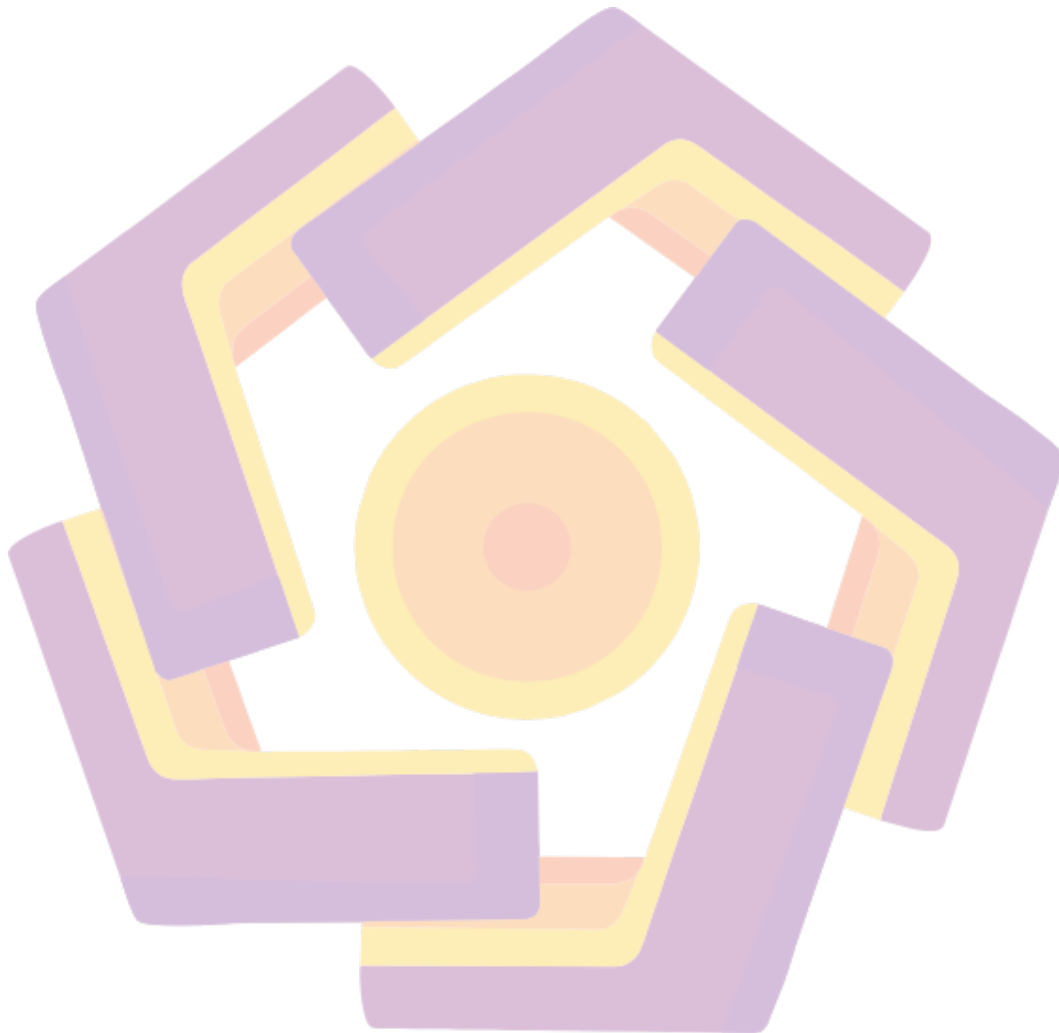


## DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian.....	8
Tabel 3. 1 Objek Sampel Penelitian.....	16
Tabel 4. 1 Rincian Informasi Berkas Aplikasi Tokopedia.....	28
Tabel 4. 2 Matriks Penilaian Keamanan Tokopedia.....	30
Tabel 4. 3 Distribusi Tingkat Kerentanan Tokopedia.....	31
Tabel 4. 4 Identifikasi Pelacak (Trackers) pada Tokopedia.....	33
Tabel 4. 5 Daftar Izin Berbahaya Tokopedia.....	36
Tabel 4. 6 Analisis Izin Berbahaya pada Tokopedia.....	38
Tabel 4. 7 Rincian Informasi Berkas Aplikasi Shopee.....	41
Tabel 4. 8 Matriks Penilaian Keamanan Shopee.....	43
Tabel 4. 9 Distribusi Tingkat Kerentanan Shopee.....	45
Tabel 4. 10 Identifikasi Pelacak (Trackers) Shopee.....	47
Tabel 4. 11 Identifikasi Pelacak (Trackers) pada Shopee.....	47
Tabel 4. 12 Daftar Izin Berbahaya Shopee.....	51
Tabel 4. 13 Analisis Izin Berbahaya pada Shopee.....	54
Tabel 4. 14 Rincian Informasi Berkas Aplikasi Lazada.....	58
Tabel 4. 15 Matriks Penilaian Keamanan Lazada.....	60
Tabel 4. 16 Distribusi Tingkat Kerentanan Lazada.....	61
Tabel 4. 17 Identifikasi Pelacak (Trackers) Lazada.....	63
Tabel 4. 18 Identifikasi Pelacak (Trackers) pada Lazada.....	63
Tabel 4. 19 Daftar Izin Berbahaya Lazada.....	66

Tabel 4. 20 Analisis Izin Berbahaya pada Lazada .....69

Tabel 4. 23 Rekomendasi Perbaikan Keamanan Aplikasi .....75



## DAFTAR GAMBAR

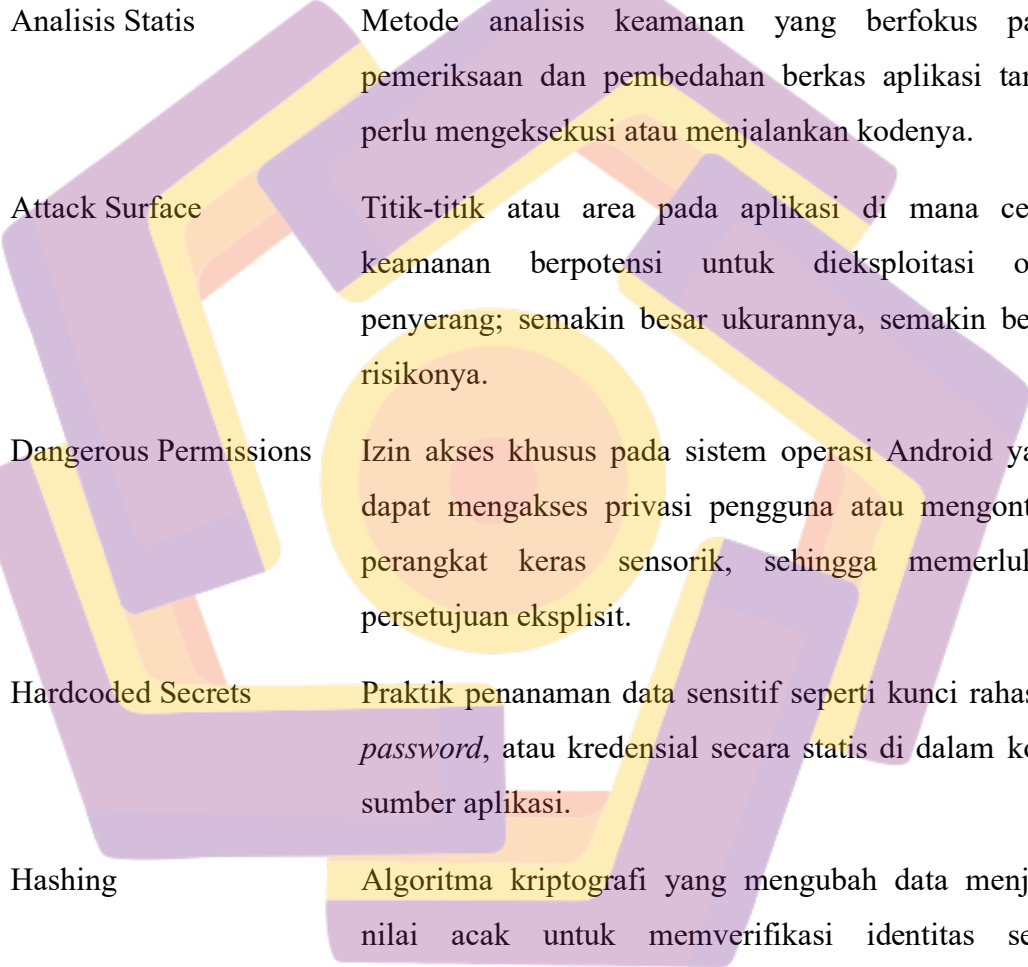
Gambar 2. 1 Mitigasi Kerentanan OWASP Mobile Top 10 .....	15
Gambar 3. 1 Alur Penelitian .....	18
Gambar 3. 2 Pipeline Analisis .....	21
Gambar 4. 1 Header Laporan Tokopedia.....	29
Gambar 4. 2 Skor Keamanan Tokopedia.....	31
Gambar 4. 3 Temuan Kritis Tokopedia.....	33
Gambar 4. 4 Header Laporan Shopee.....	43
Gambar 4. 5 Skor Keamanan Shopee.....	44
Gambar 4. 6 Temuan Kritis Shopee.....	46
Gambar 4. 7 Header Laporan Lazada.....	59
Gambar 4. 8 Skor Keamanan Lazada.....	60
Gambar 4. 9 Temuan Kritis Lazada.....	62
Gambar 4. 10 Grafik Perbandingan Skor Keamanan Aplikasi Marketplace.....	72
Gambar 4. 11 Grafik Persentase Izin Berbahaya dari Total izin.....	74

## DAFTAR LAMBANG DAN SINGKATAN



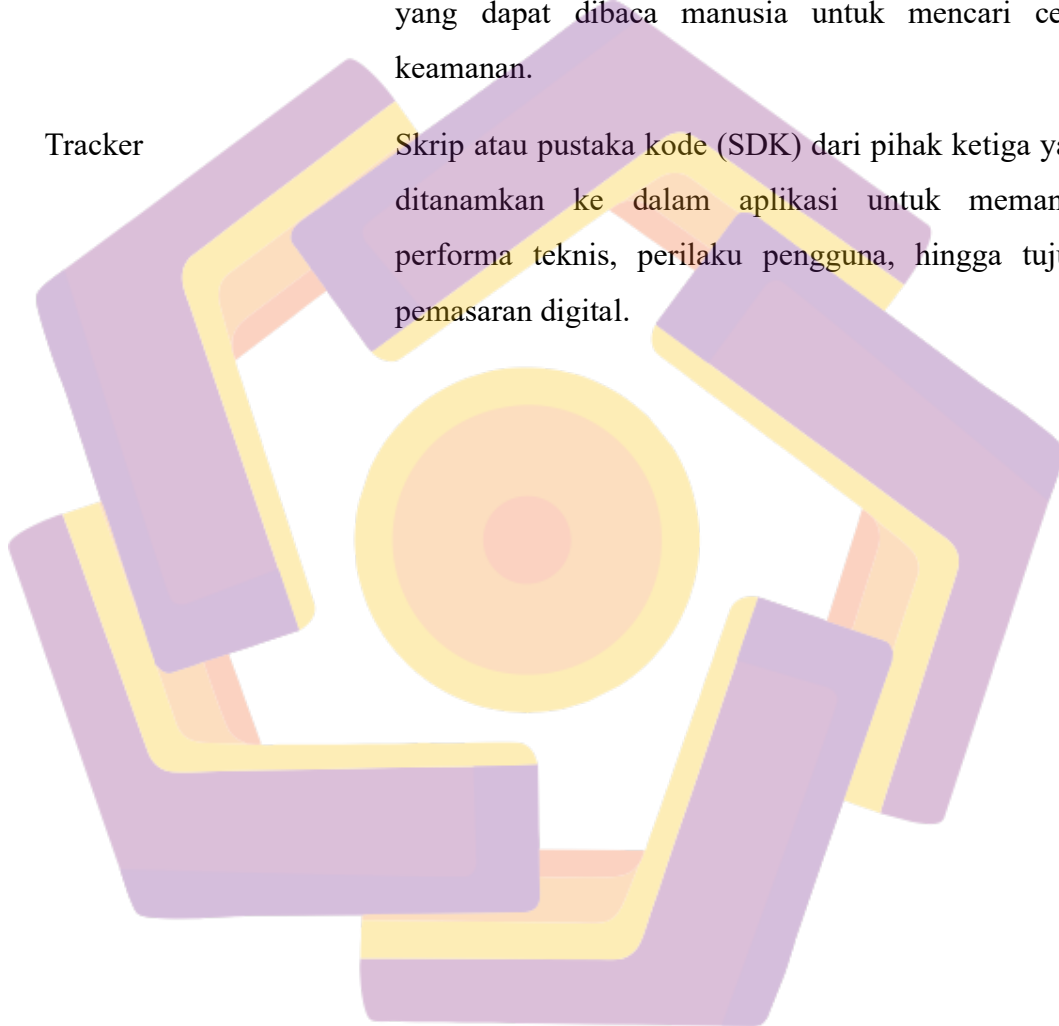
API	<i>Application Programming Interface</i>
APK	<i>Android Package Kit (atau Application Package File)</i>
DAST	<i>Dynamic Application Security Testing</i>
GPS	<i>Global Positioning System</i>
IMEI	<i>International Mobile Equipment Identity</i>
IMSI	<i>International Mobile Subscriber Identity</i>
JDK	<i>Java Development Kit</i>
KYC	<i>Know Your Customer</i>
MD5	<i>Message-Digest Algorithm 5</i>
MitM	<i>Man-in-the-Middle</i>
MobSF	<i>Mobile Security Framework</i>
OS	<i>Operating System</i>
OWASP	<i>Open Web Application Security Project</i>
SAST	<i>Static Application Security Testing</i>
SHA	<i>Secure Hash Algorithm (misalnya SHA-1, SHA-256)</i>
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>

## DAFTAR ISTILAH



Analisis Dinamis	Metode analisis keamanan yang dilakukan dengan menjalankan aplikasi pada lingkungan yang aman dan terkontrol ( <i>sandbox</i> atau emulator) untuk mengamati perilaku aplikasi saat sedang berjalan.
Analisis Statis	Metode analisis keamanan yang berfokus pada pemeriksaan dan pembedahan berkas aplikasi tanpa perlu mengeksekusi atau menjalankan kodenya.
Attack Surface	Titik-titik atau area pada aplikasi di mana celah keamanan berpotensi untuk dieksploitasi oleh penyerang; semakin besar ukurannya, semakin besar risikonya.
Dangerous Permissions	Izin akses khusus pada sistem operasi Android yang dapat mengakses privasi pengguna atau mengontrol perangkat keras sensorik, sehingga memerlukan persetujuan eksplisit.
Hardcoded Secrets	Praktik penanaman data sensitif seperti kunci rahasia, <i>password</i> , atau kredensial secara statis di dalam kode sumber aplikasi.
Hashing	Algoritma kriptografi yang mengubah data menjadi nilai acak untuk memverifikasi identitas serta memastikan integritas berkas agar tidak korup.
Least Privilege	Prinsip keamanan informasi yang mengharuskan sebuah aplikasi hanya meminta hak akses yang benar-benar mutlak diperlukan untuk menjalankan fungsi utamanya.

Man-in-the-Middle	Jenis serangan siber di mana penyerang menyadap dan memanipulasi data transaksi pada lalu lintas jaringan komunikasi.
Reverse Engineering	Proses di mana kode biner aplikasi dapat dengan mudah didekompilasi kembali menjadi kode sumber yang dapat dibaca manusia untuk mencari celah keamanan.
Tracker	Skrip atau pustaka kode (SDK) dari pihak ketiga yang ditanamkan ke dalam aplikasi untuk memantau performa teknis, perilaku pengguna, hingga tujuan pemasaran digital.



## INTISARI

Pesatnya pertumbuhan ekosistem perdagangan elektronik (*marketplace*) di Indonesia menuntut standar keamanan siber yang tinggi guna melindungi data sensitif pengguna. Penelitian ini bertujuan untuk mengevaluasi dan membandingkan postur keamanan serta privasi data pada tiga aplikasi *marketplace* dengan basis pengguna terbesar di Indonesia, yaitu Tokopedia, Shopee, dan Lazada.

Metode penelitian yang digunakan adalah analisis statis (*Static Application Security Testing*) menggunakan perangkat lunak *open-source Mobile Security Framework* (MobSF). Objek penelitian berupa berkas aplikasi resmi (*APK*) versi terbaru per Januari 2026 yang diekstraksi dari perangkat Android. Analisis difokuskan pada penilaian skor keamanan (*Security Score*), statistik kerentanan kode (*Findings Severity*), manajemen izin aplikasi (*Permissions*), dan deteksi pelacak pihak ketiga (*Trackers*).

Hasil penelitian menunjukkan bahwa ketiga aplikasi masih berada pada tingkat risiko menengah dengan predikat cukup baik. Shopee mencatatkan tingkat keamanan kode tertinggi dengan kerentanan kritis paling sedikit, namun memiliki risiko privasi tertinggi karena ditemukannya banyak pelacak pihak ketiga dan izin akses kontak yang invasif. Sebaliknya, Lazada memiliki tingkat keamanan kode terendah dengan kerentanan kritis terbanyak, namun menerapkan prinsip minimalisme data terbaik dengan jumlah pelacak paling sedikit. Sementara itu, Tokopedia berada di posisi tengah dengan kerentanan tingkat menengah yang mendominasi.

**Kata Kunci:** Keamanan Aplikasi, Analisis Statis, MobSF, Marketplace, Privasi Data.

## **ABSTRACT**

*The rapid growth of the e-commerce ecosystem in Indonesia demands high cybersecurity standards to protect sensitive user data. This study aims to evaluate and compare the security posture and data privacy of the three marketplace applications with the largest user bases in Indonesia: Tokopedia, Shopee, and Lazada.*

*The research method employed is Static Application Security Testing (SAST) using the open-source tool Mobile Security Framework (MobSF). The research objects are the official application files (APK), latest versions as of January 2026, extracted from Android devices. The analysis focuses on Security Score assessment, code vulnerability statistics (Findings Severity), application permission management, and third-party tracker detection.*

*The results indicate that all three applications remain at a medium risk level with a satisfactory rating. Shopee recorded the highest code security level with the fewest critical vulnerabilities but posed the highest privacy risk due to numerous trackers and invasive contact access permissions. Conversely, Lazada had the lowest code security level with the most critical vulnerabilities but demonstrated the best data minimalism principle by utilizing the fewest trackers. Meanwhile, Tokopedia positioned in the middle with dominant medium severity vulnerabilities.*

**Keywords:** *Application Security, Static Analysis, MobSF, Marketplace, Data Privacy.*