

**ANALISIS KEAMANAN STATIS PADA APLIKASI ANDROID WHATSAPP
MENGUNAKAN MOBILE SECURITY FRAMEWRORK (MobSF)**

SKRIPSI

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



Disusun oleh

Siti Nor Fadlila Ridwan
19.83.0437

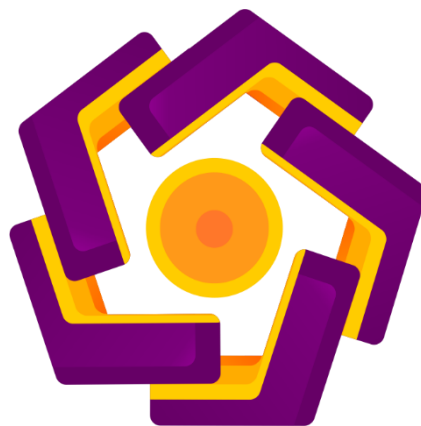
Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

**ANALISIS KEAMNAN STATIS PADA APLIKASI ANDRO IDWHATSAPP
MENGUNAKAN MOBILE SECURITY FRAMEWORK (MobSF)**

SKRIPSI

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



Disusun oleh

Siti Nor Fadlila Ridwan

19.83.0437

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023**

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS KEAMANAN STATIS PADA APLIKASI ANDROID WHATSAPP
MENGUNAKAN MOBILE SECURITY FRAMEWORK (MobSF)**

yang disusun dan diajukan oleh

Siti Nor Fadlila Ridwan

19.83.0437

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Agustus 2023

Dosen Pembimbing



Alva Hendi Muhammad, S.T, M.Eng., Dr

NIK. 190302493

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS KEAMANAN STATIS PADA APLIKASI ANDROID WHATSAPP
MENGGUNAKAN MOBILE SECURITY FRAMEWORK (MobSF)

yang disusun dan diajukan oleh

Siti Nor Fadlila Ridwan

19.83.0437

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Joko Dwi Santoso, M.Kom

NIK. 190302181

Jeki Kuswanto M.Kom

NIK. 190302456

Alva Hendi Muhammad, S.T, M.Eng., Dr

NIK. 190302493

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.

NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Siti Nor Fadlila Ridwan
NIM : 19.83.0437

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Keamanan Statis pada Aplikasi Android Whatsapp menggunakan Mobile Security Framwork (MobSF)

Dosen Pembimbing : Alva Hendi Muhammad, S.T, M.Eng., Dr

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, 22 Agustus 2023

Yang Menyatakan,

A 1000 Rupiah postage stamp with a signature over it. The stamp features the Garuda Pancasila emblem and the text '1000', 'METERAI TEMPEL', and '84AKX674696139'.

Siti Nor Fadlila Ridwan

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat, hidayah, dan karunia-Nya, yang telah memberikan kekuatan, kesehatan serta berkah-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini tepat pada waktunya. Skripsi ini penulis persembahkan untuk :

1. Pintu surgaku dan panutanku Ibunda Haryanti Hamisi S.Pd. terima kasih sebesar-besarnya saya berikan kepada beliau atas segala bentuk dukungan, dan doa yang telah diberikan selama ini. Terima kasih sudah selalu berjuang unruk kehidupan saya, sehat selalu dan hiduplah lebih lama lagi.
2. Bpk Alva Hendi Muhammad, S.T, M.Eng., Dr selaku pembimbing yang telah memberikan bimbingan, arahan dan semangat kepada penulis dalam menyelesaikan skripsi ini.
3. Kakak saya Ramaddania Hamisi yang telah memberikan doa serta support unruk saya selama ini.
4. Adik saya tercinta Ridhar Ridwan yang selalu menghibur, memberikan semangat dan doa selama ini sehingga terselesaikan skripsi ini.
5. Sahabat saya, Indah Wahyuni Saputri, dan Rinda Martisa Fiorentina yang selalu memberikan dukungan. Terima kasih atas waktu, bantuan, support dan kebaikan yang diberikan kepada saya selama ini.
6. Seluruh teman-teman Teknik Komputer Angkatan 2019 yang sedang berjuang unruk mengapai gelar sarjana.
7. Dan yang terakhir, terima kasih unruk Siti Nor Fadlila Ridwan, diri saya sendiri. Terima kasih karena sudah mau berjuang sampai sejauh ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, atas segala rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul " Analisis Keamanan Statis pada Aplikasi Android Whatsapp menggunakan Mobile Security Framework (MobSF)". Penulisan skripsi ini merupakan bagian akhir dari perjalanan panjang dalam menempuh pendidikan untuk memenuhi syarat guna mencapai gelar Sarjana Teknik Komputer di Universitas Amikom Yogyakarta.

Skripsi ini tidak hanya sekadar kumpulan kata, tetapi merupakan hasil dari proses penelitian yang telah dilakukan dengan penuh dedikasi, kerja keras, dan semangat untuk menggali lebih dalam tentang topik yang diangkat. Penulis menyadari bahwa penyelesaian skripsi ini tidak mungkin terwujud tanpa bantuan, dukungan, serta arahan dari berbagai pihak. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Alva Hendi Muhammad, S.T, M.Eng., Dr selaku dosen pembimbing yang telah memberikan bimbingan, nasihat, dan masukan berharga sepanjang proses penyusunan skripsi ini. Bantuan dan dorongan beliau telah membimbing penulis untuk menghasilkan karya yang lebih baik.
2. Orang tua saya ibu Haryanti Hamisi yang selalu memberikan semangat, doa dan dukungan untuk kelancaran penelitian ini.
3. Wahid Miftahul Ashari, S.Kom., M.T selaku dosen wali yang sudah memberikan pengarahan serta dukungan selama masa perkuliahan.
4. Seluruh dosen-dosen Teknik Komputer yang telah memberikan ilmu dan wawasan selama perkuliahan.
5. Teman-teman yang selalu memberikan dukungan dan semangat dalam setiap langkah penulisan skripsi ini.

Yogyakarta, 10 Agustus 2023

Siti Nor Fadlila Ridwan

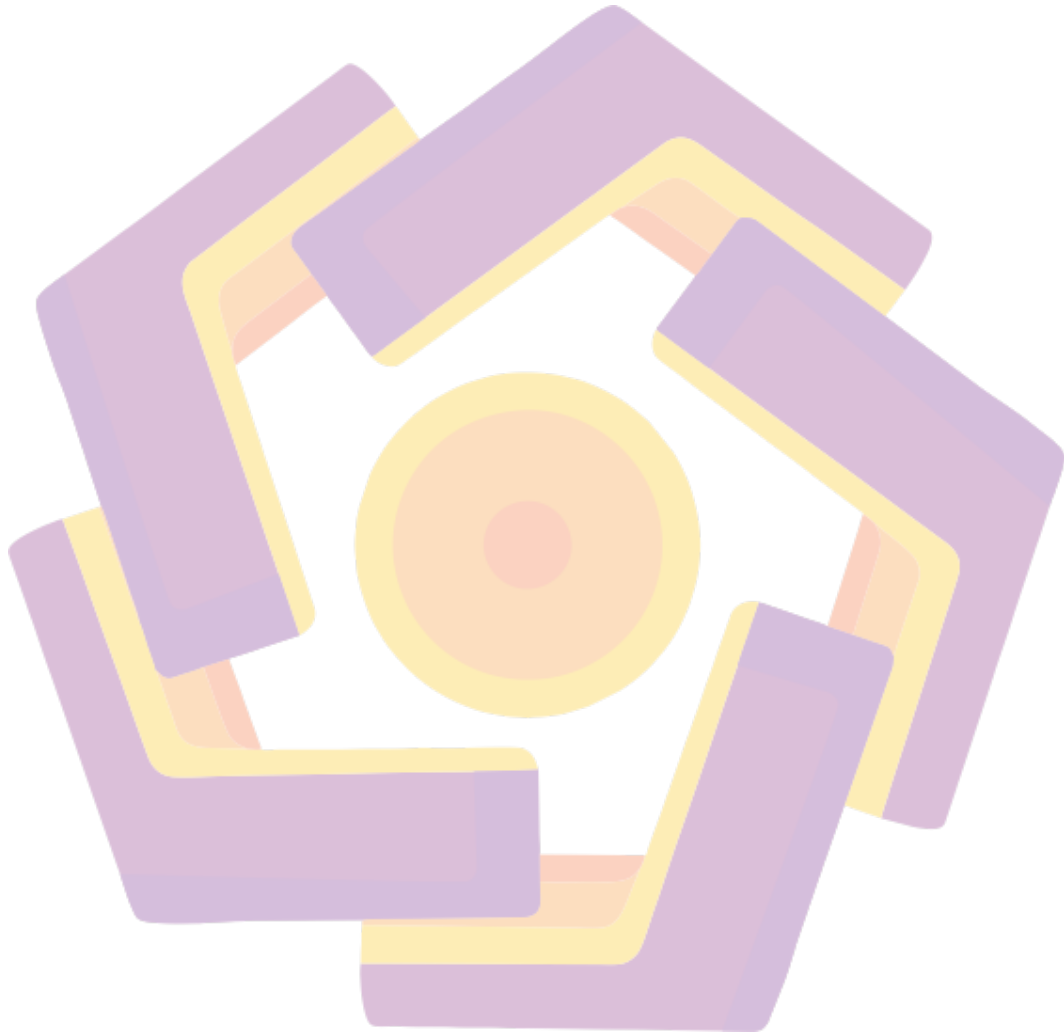
DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
INTISARI	xiii
ABSTRACT.....	xiv
BAB I PENDAHULUAN.....	15
1.1 Latar Belakang	15
1.2 Rumusan Masalah	16
1.3 Batasan Masalah.....	17
1.4 Tujuan Penelitian.....	17
1.5 Manfaat Penelitian.....	17
1.6 Sistematik Penulisan	17
BAB II TINJAUAN PUSTAKA	19
2.1 Studi Literatur	19
2.2 Landasan Teori.....	27
2.2.1 Whatsapp.....	27
2.2.2 Analisis Statis.....	27
2.2.2.1 Weak Crypto	28
2.2.2.2 SSL Bypass	28
2.2.2.3 Dangerous Permission	28
2.2.2.4 Root Detection	28
2.2.2.5 Domain Malware Check	29
2.2.3 MobSF (<i>Mobile Security Framework</i>).....	29
BAB III METODE PENELITIAN	30
3.1 Alur Penelitian.....	30

3.1.1	Perumusan masalah.....	31
3.1.2	Studi literatur	31
3.1.3	Mempersiapkan hardware & software	31
3.1.4	Menyusun & implementasi skenario	31
3.1.5	Input aplikasi kedalam MobSF (Mobile Security Framework)	32
3.1.6	Prose analisis statis	32
3.1.7	Reporting.....	32
3.1.8	Menyusun laporan hasil penelitian	32
3.2	Alat dan Bahan	33
BAB IV HASIL DAN PEMBAHASAN		34
4.1	Hasil Analisis	34
4.1.1	Dangerous Permissions.....	36
4.1.2	Weak Crypto	44
4.1.3	Root Detection	66
4.1.4	SSL Bypass	71
4.1.5	Domain Malware Check	72
BAB V PENUTUP		78
5.1	Kesimpulan.....	78
5.2	Saran.....	79
DAFTAR PUSTAKA		80

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	22
Tabel 3.1 Alat & bahan yang digunakan	33
Tabel 4.1 Hasil Analisis atatis	74



DAFTAR GAMBAR

Gambar 2.1	Parameter Analisis Statis.....	27
Gambar 3.1	Alur Penelitian.....	30
Gambar 3.2	Proses Analisis Statis pada MobSF.....	32
Gambar 4.1	Informasi Aplikasi Whatsapp.....	34
Gambar 4.2	Informasi playstore Whatsapp.....	35
Gambar 4.3	Informasi aplikasi GBWhatsapp.....	36
Gambar 4.4	Dangerous Permission Whatsapp.....	37
Gambar 4.5	Dangerous Permission Whatsapp.....	38
Gambar 4.6	Dangerous Permission Whatsapp.....	39
Gambar 4.7	Dangerous Permission GBWhatsApp.....	40
Gambar 4.8	Dangerous Permission GBWhatsApp.....	41
Gambar 4.9	Dangerous Permission GBWhatsApp.....	43
Gambar 4.10	Weak Crypto Whatsapp.....	44
Gambar 4.11	kode pada file X/C0LZ.java.....	45
Gambar 4.12	Weak Crpto Whatsapp.....	46
Gambar 4.13	Weak Crypto Whatsapp.....	47
Gambar 4.14	Weak Crypto Whatsapp.....	48
Gambar 4.15	Weak Crypto Whatsapp.....	49
Gambar 4.16	Weak Crypto Whatsapp.....	50
Gambar 4.17	kode pada file X/C133116iH.java.....	51
Gambar 4.18	Weak Crypto Whatsapp.....	52
Gambar 4.19	kode pada file X/EnumC31231hf.java.....	53
Gambar 4.20	Weak Crypto Whatsapp.....	54
Gambar 4.21	Weak Crypto Whatsapp.....	54
Gambar 4.22	Weak Crypto GBWhatsApp.....	55
Gambar 4.23	Weak Crypto GBWhatsApp.....	56
Gambar 4.24	Weak Crypto GBWhatsApp.....	57
Gambar 4.25	Weak Crypto GBWhatsApp.....	58
Gambar 4.26	Weak Crypto GBWhatsApp.....	59

Gambar 4.27	Weak Crypto GBWhatsApp.....	60
Gambar 4.28	Weak Crypto GBWhatsApp.....	61
Gambar 4.29	Weak Crypto GBWhatsApp.....	62
Gambar 4. 30	Weak Crypto GBWhatsApp.....	63
Gambar 4. 31	Weak Crypto GBWhatsApp.....	64
Gambar 4.32	Weak Crypto GBWhatsApp.....	65
Gambar 4.33	Root Detection Whatsapp.....	66
Gambar 4.34	Kode pada X/ActivityC13120n3.java	66
Gambar 4.35	Kode pada X/C57612ml.java	67
Gambar 4.36	Kode pada X/C5J5.java.....	68
Gambar 4. 37	Root Detection GBWhatsApp.....	68
Gambar 4. 38	Kode pada X/C024101r.java	69
Gambar 4. 39	Kode pada com/yandex/metrec/impl/ob/j4.java.....	69
Gambar 4.40	File URLs Whatsapp	71
Gambar 4.41	File URLs GBWhatsApp	71
Gambar 4.42	Domain Malware Check Whatsapp.....	73
Gambar 4.43	Domain Check Malware GBWhatsApp.....	73
Gambar 4.44	Domain Malware Check GBWhatsApp.....	74

INTISARI

Seiring dengan kemajuan teknologi banyak munculnya beragam aplikasi baik resmi atau tidak resmi. Maka dari itu sistem android harus tahan dari berbagai serangan malware yang dapat menggunakan kerentanan sebuah aplikasi untuk mencuri informasi penting pengguna. Oleh karena itu dibuatnya penelitian tersebut guna menganalisis perbedaan keamanan aplikasi android yang didownload melalui pihak ketiga dengan aplikasi android yang didownload melalui playstore. Metode yang digunakan merupakan metode analisis statis dengan menggunakan tools MobSF. Hasil analisis menggunakan MobSF terhadap aplikasi yang didownload melalui pihak ketiga dengan aplikasi yang didownload melalui playstore terdapat banyak perbedaan. Dari perbedaan tersebut dapat dilihat telah terjadi perubahan pada penyediaan file dari pihak ketiga. Dari hasil analisis yang telah dilakukan mendownload sebuah aplikasi melalui playstore lebih aman daripada mendownload melalui pihak ketiga. Karena masih banyak pengguna yang awam akan terhadap perubahan file yang telah dilakukan beserta resiko yang dapat mempegaruhi perangkat.

Kata Kunci : Whatsapp, Keamanan, Statis, MobSF

ABSTRACT

Along with technological advances, there are many various applications, both official and unofficial. Therefore the Android system must be resistant to various malware attacks that can use the vulnerability of an application to steal important user information. Therefore, this research was made to analyze the differences in the security of Android applications downloaded through third parties and Android applications downloaded via the PlayStore. The method used is a static analysis method using MobSF tools. The results of the analysis using MobSF for applications downloaded via third parties and applications downloaded via the PlayStore there are many differences. From these differences it can be seen that there has been a change in the provision of files from third parties. From the results of the analysis that has been carried out, downloading an application through PlayStore is safer than downloading through a third party. Because there are still many users who are unfamiliar with the file changes that have been made along with the risks that can affect the device.

Keyword : *Whatsapp, Security, Static, MobSF.*