

**REVERSE ENGINEERING PHISHING
WEBVIEW PADA APLIKASI
ANDROID**

SKRIPSI

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



disusun oleh

DILA AFRIDA FEDIMAWATI

17.83.0006

Kepada

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

**REVERSE ENGINEERING PHISING
WEBVIEW PADA APLIKASI
ANDROID**

SKRIPSI

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



disusun oleh

DILA AFRIDA FEDIMAWATI

17.83.0006

Kepada

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

HALAMAN PERSETUJUAN

SKRIPSI

**REVERSE ENGINEERING PHISHING
WEBVIEW PADA APLIKASI
ANDROID**

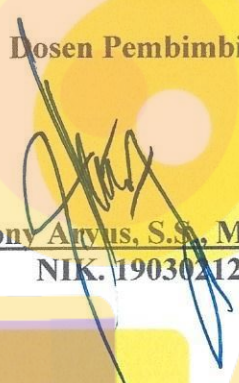
yang disusun dan diajukan oleh

Dila Afrida Fedimawati

17.83.0006

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 18 Agustus 2023

Dosen Pembimbing,


Dony Arvus, S.S., M.Kom.

NIK. 190302128

HALAMAN PENGESAHAN
SKRIPSI
REVERSE ENGINEERING PHISHING
WEBVIEW PADA APLIKASI
ANDROID

yang disusun dan diajukan oleh

Dila Afrida Fedimawati

17.83.0006

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Muhammad Kopravi, S.Kom., M.Eng
NIK. 190302454

Jeki Kuswanto, M.Kom
NIK. 190302456

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



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 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 : Dila Afrida Fedimawati
NIM : 17.83.0006

Menyatakan bahwa Skripsi dengan judul berikut:

Reverse Engineering Phishing WebView Pada Aplikasi Android

Dosen Pembimbing : 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, 18 Agustus 2023

Yang Menyatakan,



Dila Afrida Fedimawati

HALAMAN PERSEMBAHAN

Alhamdulillah segala puja dan puji syukur kepada Allah yang Maha Esa karena berkat rahmat dan anugerah-Nya yang amat luar biasa saya bisa menyelesaikan skripsi ini dengan sebaik yang bisa saya lakukan. Dengan ini saya akan mempersembahkan skripsi ini kepada:

1. Kepada kedua orang tua saya yang telah sabar dan selalu memberikan dukungan kepada saya hingga detik ini, tanpa doa dan kerja keras mereka saya tidak akan sampe di titik ini. Terimakasih atas segala dukungan yang selalu bapak dan ibu berikan kepada saya.
2. Kepada bapak Dony Ariyus, S.S., M.Kom. selaku dosen pembimbing saya yang telah membantu dan membimbing dalam penulisan skripsi ini.
3. Kepada keluarga, teman maupun sahabat saya terimakasih telah memberikan dukungan kepada saya sehingga saya bisa menyelesaikan skripsi ini dengan baik.

KATA PENGANTAR

Dengan mengucapkan puja dan puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat, taufik dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini yang berjudul: “Reverse Engineering Phishing WebView Pada Aplikasi Android”. Skripsi ini dibuat untuk memenuhi salah satu persyaratan yaitu menyelesaikan Program Sarjana (S1) jurusan Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis sangat amat menyadari tanpa adanya bantuan, dukungan, bimbingan dan nasihat dari berbagai pihak maka skripsi ini tidak akan terselesaikan dengan baik. Maka dari itu pada kesempatan kali ini penulis akan menyampaikan terimakasih kepada:

1. Allah SWT yang Maha Esa atas izin dan karunia-Nya skripsi ini bisa terselesaikan dengan baik dan semoga bisa memberikan manfaat untuk orang lain di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer dan Ketua Program Studi S1 Sistem Informasi.
4. Bapak Dony Ariyus, S.S., M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta dan selaku dosen pembimbing saya. Terimakasih atas segala bimbingan arahan dan saran yang telah diberikan kepada penulis sehingga skripsi ini bisa di selesaikan dengan baik.
5. Orang tua, Keluarga serta teman-teman saya yang tidak pernah saya lupakan karena atas doa dan dukungan yang kalian berikan kepada penulis.

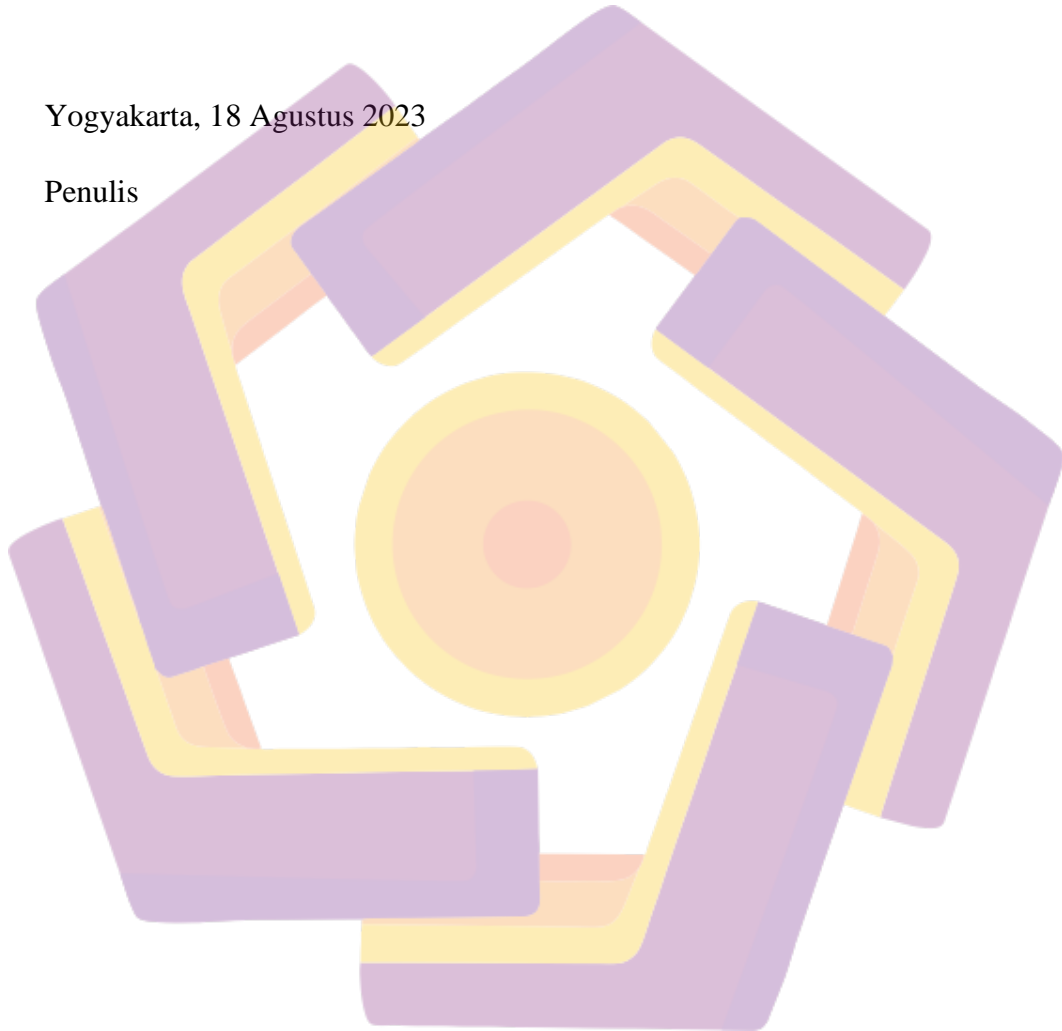
Penulis menyadari bahwa penyusunan skripsi ini jauh dari kata sempurna, penulis berharap semoga skripsi ini bisa bermanfaat untuk semua pihak yang terkait dan bermanfaat bagi pembaca skripsi ini. Semoga Allah SWT memberikan balasan

yang berlipat ganda kepada semua pihak yang telah membantu dalam menyelesaikan skripsi ini.

Penulis menyadari bahwa masih banyak sekali kekurangan yang terdapat dalam penulisan skripsi ini maka dari itu penulis berharap atas kritik dan saran yang bersifat membangun dari pembaca.

Yogyakarta, 18 Agustus 2023

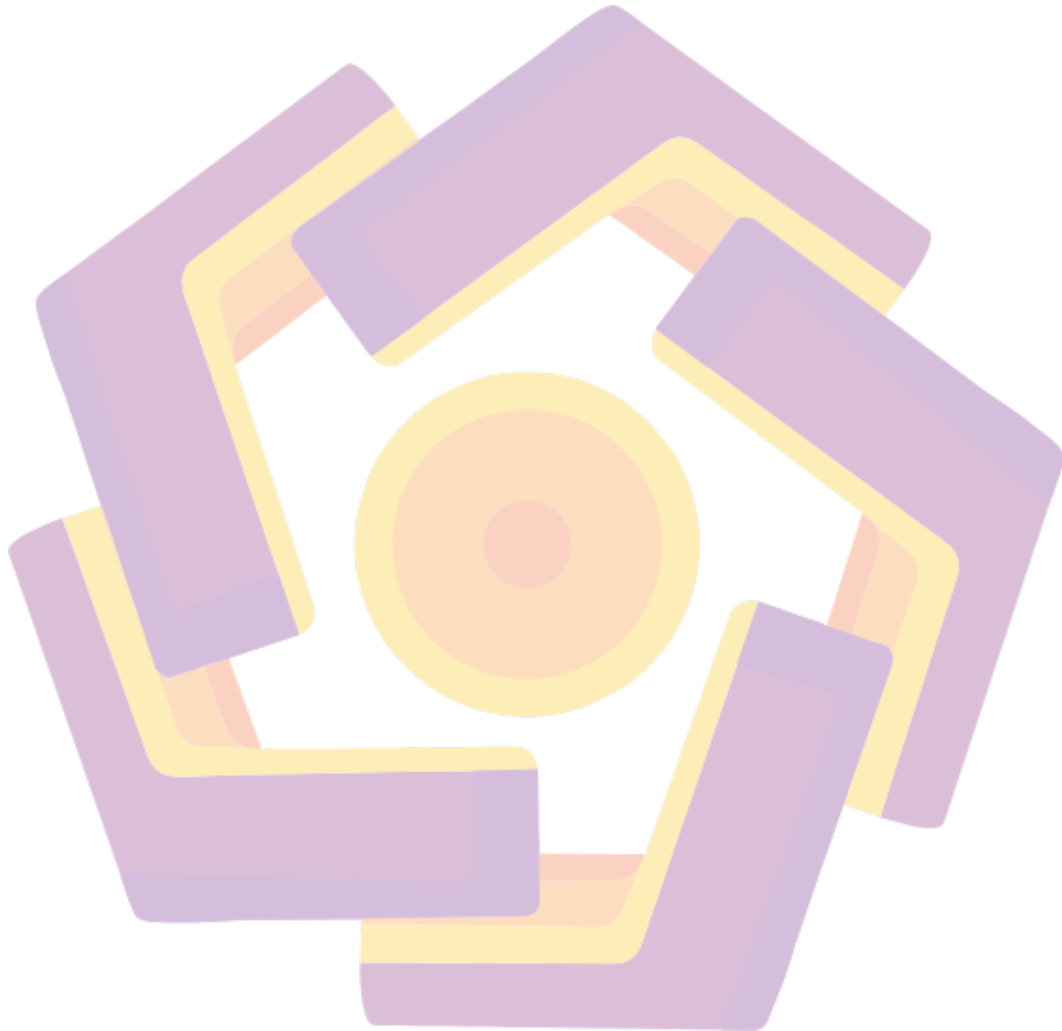
Penulis



DAFTAR ISI

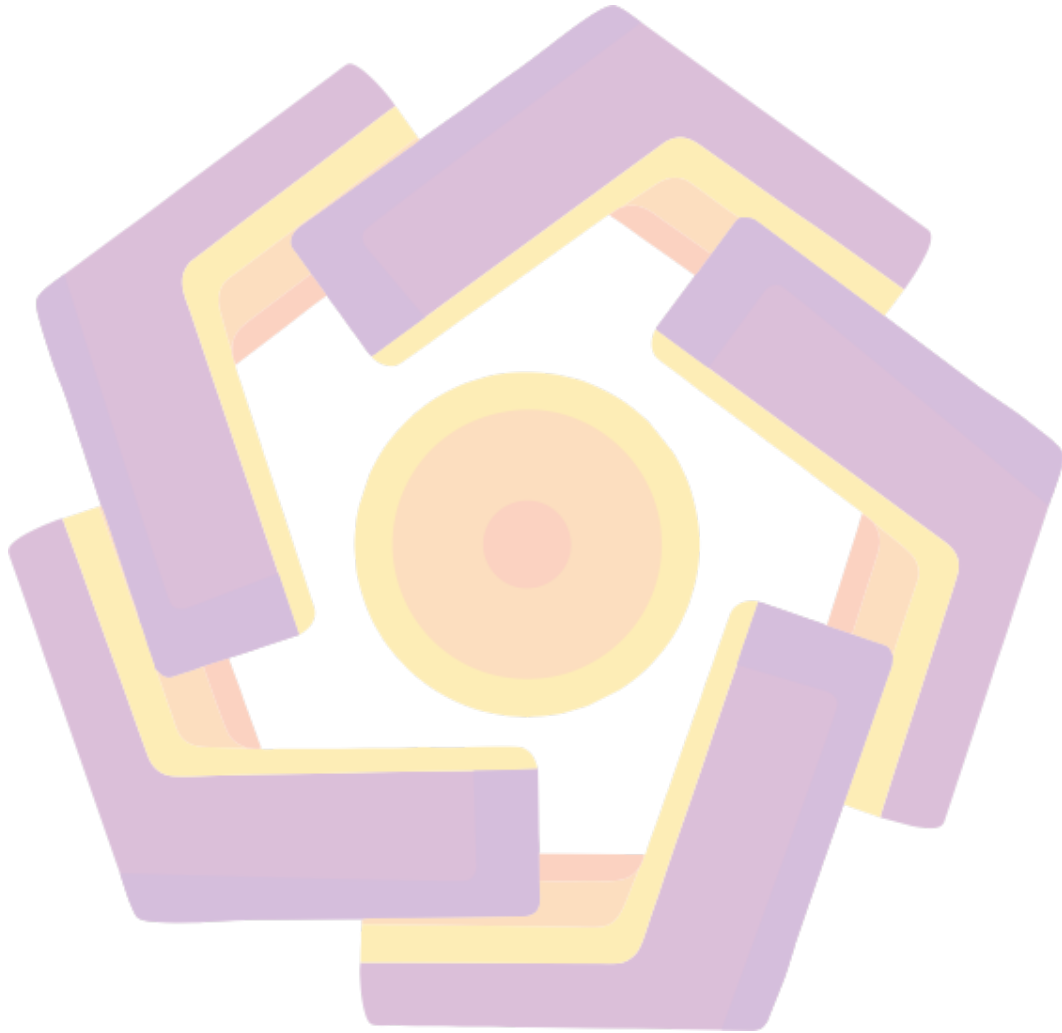
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iii
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR ISTILAH	xii
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB I PENDAHULUAN	3
BAB II TINJAUAN PUSTAKA	5
2.1 Studi Literatur	5
2.2 Dasar Teori	15
2.3 Reverse Engineering	15
2.4 WebView Android.....	16
2.5 Phising	16
2.5.1 Jenis Serangan Phising	17
2.5.2 Data Riset Serangan Phising.....	18
BAB III METODE PENELITIAN	24
3.1 Alur Penelitian	24
3.2 Alat dan Bahan.....	25
BAB IV HASIL DAN PEMBAHASAN	28
4.1. Implementasi Sistem.....	28
4.2 Membangun Lingkungan Kerja.....	30
4.2.1 Sampel Aplikasi yang diuji	30

4.2.2 Instalasi Perangkat Lunak	33
4.2.3 Reverse Engineering Proses	36
4.3 Hasil Temuan dan Analisis	40
BAB V PENUTUP	44
5.1 Kesimpulan	44
5.2 Saran	44
REFERENSI	46



DAFTAR TABEL

Table 2.1 Keaslian Penelitian	8
Table 3.1 Daftar Perangkat Keras (Hardware)	25
Table 3.2 Daftar Perangkat Lunak (Software)	26
Table 4.1 Service Permission di AndroidManifest	41



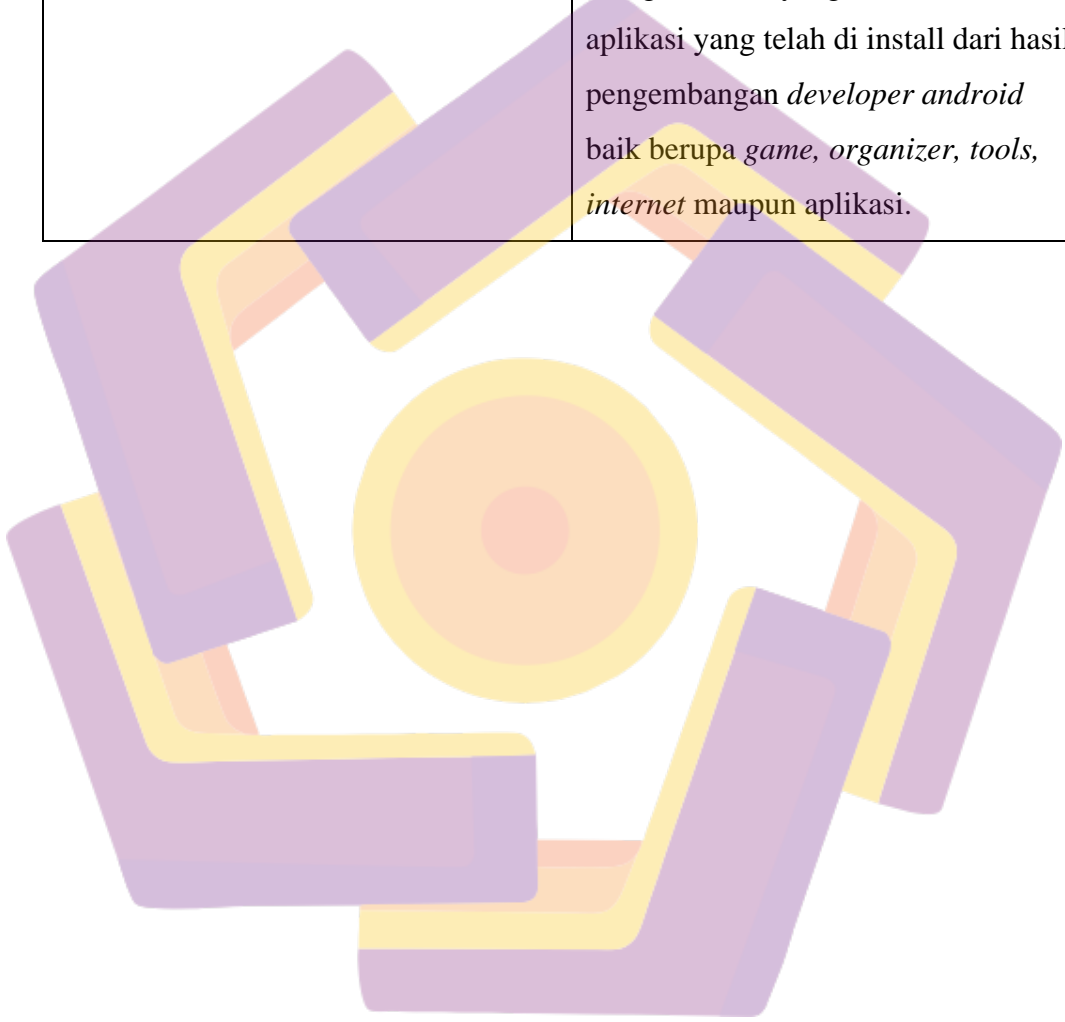
DAFTAR GAMBAR

Gambar 2.1 WebView Screen Example.....	16
Gambar 2.2 Report Indonesia Anti-Phishing Data Exchange (IDAX).....	19
Gambar 2.3 Persentase Industri yang sering diincar di Indonesia.....	21
Gambar 2.4 Phishing Report by APWG.....	21
Gambar 2.5 Crime types report by Federal Bureau of Investigation.....	22
Gambar 2.6 Berbagai Aplikasi Phishing.....	22
Gambar 4.1 Nama & icon launcher KredivoReward Aplikasi Phishing.....	31
Gambar 4.2 Storage Permission.....	32
Gambar 4.3 Halaman Utama KredivoReward Aplikasi Phishing.....	33
Gambar 4.4 Windows Run.....	34
Gambar 4.4 CMD Cek Java Version.....	34
Gambar 4.5 dex2jar.....	35
Gambar 4.6 jd-gui.....	35
Gambar 4.7 Apktool.....	35
Gambar 4.8 Framework-res.apk.....	36
Gambar 4.9 Sample Aplikasi Phishing.....	36
Gambar 4.10 Ganti ekstensi jadi zip.....	37
Gambar 4.11 Hasil Extract.....	37
Gambar 4.12 Classdex di dex2jar.....	38
Gambar 4.13 Decompile dex2jar.....	38
Gambar 4.14 jd-gui.....	38
Gambar 4.15 Temuan dex2jar.....	39
Gambar 4.16 Cmd apktool framework-res.apk.....	39
Gambar 4.17 Decompile Apktool.....	39
Gambar 4.18 Hasil Decompile Apktool.....	40
Gambar 4.19 AndroidManifest.....	41
Gambar 4.20 Temuan WebView Website Phishing.....	42
Gambar 4.21 Validasi Website Phishing di Browser.....	43

DAFTAR ISTILAH

<i>Reverse Engineering</i>	Proses penemuan prinsip-prinsip teknologi dari suatu perangkat, obyek, atau sistem melalui analisis struktur, fungsi dan cara kerja.
<i>Phising</i>	Sebuah bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi yang sensitif dengan cara menyamar sebagai seseorang.
<i>Webview</i>	Ekstensi class view android yang memungkinkan untuk menampilkan halaman web sebagai bagian dari suatu tata letak aktivitas pada suatu aplikasi.
<i>Class</i>	Berisi variable dan fungsi yang menggambarkan sebuah obyek. Atau sebuah kerangka yang digunakan untuk membuat suatu obyek.
<i>String</i>	Tipe data yang dapat digunakan untuk menyimpan barisan karakter.
<i>Hash</i>	Suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang acak.
<i>Decompile</i>	Suatu proses pembongkaran file.
<i>Ekstensi</i>	Sebuah penanda yang menunjukkan type atau jenis suatu berkas atau file.
<i>APK</i>	APK (<i>Android PacKage</i>) suatu model paket android yang pada umumnya digunakan untuk menyimpan sebuah

aplikasi maupun program yang dijalankan oleh perangkat android. APK ini berisi file kompres seperti file zip, APK biasanya sudah disertakan bersama dengan ROM namun sebagian besar yang diketahui APK ini aplikasi yang telah di install dari hasil pengembangan *developer android* baik berupa *game, organizer, tools, internet* maupun aplikasi.



INTISARI

Terdapat berbagai macam teknik dan metode yang digunakan untuk melakukan kejahatan siber diantaranya carding, DDoS dan deface website. Diantara tindak kejahatan tersebut terdapat beberapa kejahatan yang memang ditujukan hanya untuk merusak dan memodifikasi suatu sistem. Namun terdapat beberapa metode yang digunakan untuk mendapatkan informasi penting seseorang yaitu salah satunya adalah metode phishing.

Phishing merupakan suatu metode dengan memanfaatkan website, email yang bertujuan untuk mendapatkan alamat id, username, password maupun data yang seharusnya tidak boleh diketahui oleh orang lain.

Dalam beberapa Lembaga survei di dunia pada bidang kejahatan siber, phishing selalu menempati urutan posisi ke-5 besar tindak kejahatan siber yang sering terjadi. Yang artinya bahwa kejahatan phishing bisa dilakukan dengan cara memanfaatkan kreatifitas penyerang untuk memikat korban misalnya terdapat class webview yang memungkinkan menampilkan website tanpa diketahui domain website tersebut.

Fokus penelitian ini adalah berfokus pada class ekstensi yang terdapat pada android yaitu webview yang memungkinkan menampilkan halaman web sebagai bagian dari aktivitas pada suatu aplikasi. Yang di mana pada class ini domain suatu website dapat disembunyikan. Salah satu metode yang digunakan untuk menganalisa suatu aplikasi menggunakan metode reverse engineering.

Reverse engineering pada class webview android bertujuan untuk menemukan class, string ataupun codingan yang mencurigakan yang telah disisipkan oleh pembuat aplikasi untuk melakukan phishing.

Kata kunci: Reverse Engineering, Phising, WebView Android, Keamanan Informasi

ABSTRACT

There are various techniques and methods used to commit cyber crimes including carding, DDoS and website defacement. Among these crimes there are several crimes that are intended only to damage and modify a system. However, there are several methods used to obtain someone's important information, one of which is the phishing method.

Phishing is a method by utilizing websites, e-mails that aim to get id addresses, usernames, passwords or data that should not be known by other people.

In several survey institutions in the world in the field of cybercrime, phishing always ranks in the top 5 most frequent cybercrimes. Which means that phishing crimes can be carried out by exploiting the creativity of attackers to lure victims, for example, there is a class webview that allows viewing websites without the domain of the website being known.

The focus of this research is to focus on the extension class found on android, namely webview which allows displaying web pages as part of activities in an application. Which in this class the domain of a website can be hidden. One of the methods used to analyze an application using the reverse engineering method.

Reverse engineering on the Android webview class aims to find suspicious classes, strings or coding that have been inserted by application makers to commit phishing..

Keyword: *Reverse Engineering, Phising, WebView Android, Information Security.*