

**ANALISIS STATIS UNTUK MENGUJI KEAMANAN APLIKASI
GAME BOOSTER BERBASIS ANDROID MENGGUNAKAN
MOBILE SECURITY FRAMEWORK BERDASARKAN
STANDAR KEAMANAN APLIKASI OWASP-MASVS**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Informasi



Disusun oleh:

INDAH SARI
182104006

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2023**

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS STATIS UNTUK MENGUJI KEAMANAN APLIKASI GAME BOOSTER BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK BERDASARKAN STANDAR KEAMANAN APLIKASI OWASP-MASVS

Diajukan oleh:

INDAH SARI
182104006

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

Tanggal: 29 Desember 2023

Mengesahkan:

Pembimbing I


Adkhan Sholeh, S.Si., M.Cs.

NIDN: 0510127501

Pembimbing II


Rama Sahtyawan, S.T., M.Cs.

NIDN: 0518058001

Penguji I


Dedy Hariyadi, S.T., M.Kom.

NIDN: 0518108001

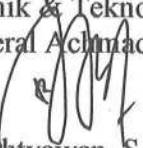
Penguji II


Chanief Budi Setiawan, S.T., M.Eng.

NIDN: 0514068101



Ketua Program Studi Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta


Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.0150

PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Indah Sari
NPM : 182104006
Program Studi : Teknologi Informasi (S-1)
Judul Tugas Akhir : Analisis Statis Untuk Menguji Keamanan Aplikasi *Game Booster* Berbasis Android Menggunakan *Mobile Security Framework* Berdasarkan Standar Keamanan Aplikasi OWASP-MASVS

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 29 Desember 2023



Indah Sari

KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul “Analisis Statis Untuk Menguji Keamanan Aplikasi *Game Booster* Berbasis Android Menggunakan *Mobile Security Framework* Berdasarkan Standar Keamanan Aplikasi OWASP-MASVS”. Penulisan laporan ini merupakan salah satu syarat untuk menyelesaikan studi program sarjana (S1) jurusan Teknologi Informasi di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat terwujud atas bimbingan dan dukungan dari berbagai pihak yang bersangkutan. Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Rama Sahtyawan, S.T., M.Cs. Selaku Ketua Program Studi Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Adkhan Sholeh, S.Si., M.Cs. dan Bapak Rama Sahtyawan, S.T., M.Cs. selaku Dosen Pembimbing Tugas Akhir;
4. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Ayah, Ibu, dan Kakak penulis yang telah memberikan dukungan semangat serta doa restu, sehingga penulis dapat menyelesaikan studi;
6. Sahabat dan teman-teman penulis yang sudah memberikan dukungan semangat serta doa selama penulisan tugas akhir ini;
7. Rekan-rekan mahasiswa Teknologi Informasi (S-1) di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 29 Desember 2023



Indah Sari

PERPUSTAKAAN
JENDERAL ACHMAD
YOGYAKARTA

DAFTAR ISI

Halaman Judul.....	i
Halaman Pengesahan.....	ii
Penyataan.....	iii
Kata Pengantar.....	iv
Daftar Isi.....	vi
Daftar Tabel.....	viii
Daftar Gambar.....	ix
Daftar Lampiran.....	x
Daftar Singkatan.....	xi
Intisari.....	xii
Abstract.....	xiii
Bab 1 Pendahuluan.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	3
1.3 Pertanyaan Penelitian.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Hasil Penelitian.....	3
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	4
2.1 Tinjauan Pustaka.....	4
2.2 Landasan Teori.....	6
2.2.1 <i>Game Booster</i>	6
2.2.2 <i>AirDroid</i>	7
2.2.3 <i>Mobile Security Framework</i>	7
2.2.4 <i>Mobile Application Security Verification Standard</i>	8
2.2.5 Analisis Statis.....	11
Bab 3 Metode Penelitian.....	17
3.1 Bahan dan Alat Penelitian.....	17
3.2 Jalan Penelitian.....	17
3.2.1 Diagram Alur Penelitian.....	17

3.2.2	Blok Diagram.....	18
Bab 4	Hasil Penelitian.....	19
4.1	Instalasi <i>Mobile Security Framework</i>	19
4.2	Mengekstrak Aplikasi <i>Game Booster</i> Menggunakan <i>AirDroid</i>	23
4.2.1	Hasil Extraksi Aplikasi <i>Game Booster</i>	27
4.3	Hasil Pengujian.....	29
4.3.1	<i>Weak Crypto</i>	33
4.3.2	<i>SSL Bypass</i>	37
4.3.3	<i>Dangerous Permissions</i>	38
4.3.4	<i>Root Detection</i>	42
4.3.5	<i>Domain Malware Check</i>	43
4.4	Analisis Atas Pengujian.....	45
Bab 5	Kesimpulan dan Saran.....	46
5.1	Kesimpulan.....	46
5.2	Saran.....	46
	Daftar Pustaka.....	47
	Lampiran.....	49

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	4
Tabel 2.2 Persyaratan Keamanan MASVS.....	8
Tabel 4.1 Hasil Extraksi Aplikasi <i>Game Booster</i>	28
Tabel 4.2 Analisis pada <i>Weak Crypto</i>	33
Tabel 4.3 Analisis pada <i>SSL Bypass</i>	37
Tabel 4.4 Analisis pada <i>Dangerous Permissions</i>	38
Tabel 4.5 Analisis pada <i>Root Detection</i>	42
Tabel 4.6 Analisis pada <i>Domain Malware Check</i>	43
Tabel 4.7 Hasil Analisis Statis.....	45

DAFTAR GAMBAR

Gambar 2.1 Parameter Analisis Statis.....	12
Gambar 3.1 Diagram Alur Penelitian.....	17
Gambar 3.2 Blok Diagram.....	18
Gambar 4.1 Menjalankan Perintah Instal Git.....	19
Gambar 4.2 Menduplikat File Respositori MobSF.....	20
Gambar 4.3 Membuka Direktori MobSF.....	20
Gambar 4.4 Mengupdate Sistem.....	21
Gambar 4.5 Membuat Direktori Baru.....	21
Gambar 4.6 Menjalankan Perintah Konfigurasi.....	22
Gambar 4.7 Tampilan Awal Beranda Aplikasi.....	23
Gambar 4.8 Proses Login ke Aplikasi <i>AirDroid</i>	23
Gambar 4.9 Permintaan Izin Aplikasi <i>AirDroid</i>	24
Gambar 4.10 Fitur Keamanan dan Jarak Jauh.....	24
Gambar 4.11 Menghubungkan Aplikasi <i>AirDroid</i> ke Laptop.....	25
Gambar 4.12 Tampilan <i>Login Airdroid Web</i>	25
Gambar 4.13 Proses <i>Loading AirDroid Web</i>	26
Gambar 4.14 Tampilan Beranda <i>AirDroid Web</i>	26
Gambar 4.15 Proses Mendownload Aplikasi <i>Game Booster</i>	27
Gambar 4.16 File APK <i>Game Booster</i>	27
Gambar 4.17 Hasil Analisis Aplikasi <i>Game Booster 4x Faster</i>	29
Gambar 4.18 Hasil Analisis Aplikasi <i>Game Booster Fire GFX-Lag Fix</i>	30
Gambar 4.19 Hasil Analisis Aplikasi <i>GearUp Game Booster: Lower Lag</i>	31
Gambar 4.20 Hasil Analisis Aplikasi <i>UU Game Booster-Lower Lag</i>	32

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian.....	49
Lampiran 2 Lembar Bimbingan Dosen.....	50
Lampiran 3 Hasil Cek Plagiarisme.....	51

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

CI/CD	<i>Continuous Integration / Continuous Delivery</i>
CBC	<i>Mode Cipher Block Chaining</i>
CWE	<i>Common Weakness Enumeration</i>
DevOps	<i>Development and Operations</i>
DevSecOps	<i>Development, Security, and Operations</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
MASVS	<i>The Mobile Application Security Verification Standard</i>
MD5	<i>Message Digest Algorithm 5</i>
MobSF	<i>Mobile Security Framework</i>
OWASP	<i>Open Web Application Security Project</i>
PKCS	<i>Public Key Cryptographic Standard</i>
RNG	<i>Random Number Generator</i>
SDK	<i>Software Development Kit</i>
SHA	<i>Secure Hashing Algorithm</i>
SLL	<i>Secure Socket Layers</i>