

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN KEASLIAN	i
HALAMAN PENGESAHAN TUGAS AKHIR.....	ii
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	iii
KATA PENGANTAR	iv
ABSTRAK	vi
<i>ABSTRACT</i>	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	iv
DAFTAR TABEL.....	vii
DAFTAR SIMBOL.....	viii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	4
1.5 Lingkup Tugas Akhir	4
1.6 Kerangka Berfikir.....	4
1.7 Sistematika Penulisan.....	6
BAB 2 TINJUAN PUSTAKA	7
2.1 Android.....	7
2.1.1 Arsitektur Android.....	7

2.2	Keamanan Informasi	11
2.2.1	Ancaman Keamanan	12
2.2.2	Pengujian Keamanan.....	13
2.2.3	Legalitas Pengujian Keamanan.....	14
2.3	Teknik Analisis Pengujian.....	15
2.3.1	Analisis Statis.....	15
2.3.2	Analisis Dinamis.....	15
2.4	<i>Open Web Application Security Project</i>	16
2.4.1	<i>OWASP Mobile Application Security Testing Guide (MASTG)</i>	16
2.4.2	<i>OWASP Mobile Top Ten 2016</i>	17
2.5	<i>Common Vulnerability Scoring System (CVSS)</i>	20
2.6	<i>Tools Analisis Pengujian</i>	24
2.6.1	<i>Mobile Security Framework (MobSF)</i>	24
2.6.2	<i>Yaazhini</i>	24
2.6.3	<i>Android Debug Bridge (ADB)</i>	25
2.6.4	<i>NOX Emulator</i>	25
2.6.5	<i>Burp Suite</i>	26
BAB 3 METODE PENELITIAN		27
3.1	Rencana Penelitian	27
3.2	Objek Penelitian	27
3.3	Teknik Pengumpulan Data	28
3.3.1	Observasi.....	28
3.3.2	Wawancara.....	28
3.3.3	Studi Pustaka.....	29

3.4	Penelitian Terdahulu.....	29
3.5	Analisis Sistem Berjalan	35
3.6	Analisis Masalah.....	46
3.7	Metode Pengujian Keamanan.....	47
3.7.1	<i>Preparation</i>	47
3.7.2	<i>Intelligence Gathering</i>	47
3.7.3	<i>Mapping the Application</i>	47
3.7.4	<i>Exploitation</i>	48
3.7.5	<i>Reporting</i>	48
3.8	Jadwal Perencanaan Penelitian.....	48
BAB 4 HASIL DAN PEMBAHASAN.....		49
4.1	Persiapan(<i>preparation</i>).....	49
4.1.1	Aplikasi <i>Mobile</i> Berbasis Android PRIFAT	49
4.1.2	Ruang Lingkup dan Pendekatan	50
4.1.3	Perizinan Pada Aplikasi <i>Mobile</i> PRIFAT	50
4.1.4	OWASP <i>mobile top ten</i> 2016.....	53
4.2	Pengumpulan Informasi (<i>intelligence gathering</i>).....	53
4.2.1	<i>Environmental Information</i>	53
4.2.2	<i>Architectural Information</i>	54
4.2.2.1	<i>Architectural Information</i> secara statis	54
4.2.2.2	<i>Architectural information</i> secara dinamis.....	56
4.3	Memetakan Aplikasi (<i>Mapping the Application</i>).....	57
4.3.1	Memetakan Aplikasi Secara Statis.....	57
4.3.2	Memetakan Aplikasi Dengan Analisis Dinamis.....	58

4.4	Eksploitasi (<i>Exploitation</i>).....	60
4.4.1	<i>Exploitation Insecure Data Storage</i>	61
4.4.2	<i>Exploitation Insecure Communication</i>	63
4.4.3	<i>Exploitation Reverse Engineering</i>	65
4.4.4	<i>Exploitation Insecure Authorization</i>	67
4.5	Laporan(<i>Reporting</i>).....	89
BAB 5 HASIL DAN KESIMPULAN		105
5.1	Kesimpulan.....	105
5.2	Saran	107
DAFTAR PUSTAKA		109
Lampiran 1. Daftar Riwayat Hidup		109
Lampiran 2. Surat Keterangan Penelitian		110
Lampiran 3. Surat Keterangan Selesai Penelitian.....		111

DAFTAR GAMBAR

	Halaman
Gambar 1. 1 Kerangka Berfikir.....	5
Gambar 2. 1 Arsitektur Android.....	7
Gambar 2. 2 Linux Kernel.....	8
Gambar 2. 3 Libraries.....	8
Gambar 2. 4 Android Runtime.....	10
Gambar 2. 5 Base Metrics Equation.....	24
Gambar 3. 1 Customer flow.....	35
Gambar 3. 2 Tampilan Homepage Aplikasi PRIFAT.....	36
Gambar 3. 3 Tampilan Registrasi Pada Aplikasi PRIFAT.....	36
Gambar 3. 4 Tampilan Profil Aplikasi PRIFAT.....	37
Gambar 3. 5 Tampilan Kategori Aplikasi PRIFAT.....	37
Gambar 3. 6 Tampilan Detail Kelas.....	38
Gambar 3. 7 Tampilan Pemilihan Waktu dan Cara Pelatihan.....	38
Gambar 3. 8 Tampilan Fitur Add Equipment.....	39
Gambar 3. 9 Tampilan Summary order dan metode pembayaran.....	39
Gambar 3. 10 Instructor flow.....	40
Gambar 3. 11 Tampilan Homepage Aplikasi PRIFAT.....	40
Gambar 3. 12 Tampilan Registrasi Sebagai Instruktur.....	41
Gambar 3. 13 Tampilan Pengisian Identitas Diri.....	41
Gambar 3. 14 Tampilan Proses Kualifikasi.....	42
Gambar 3. 15 Tampilan Pengisian Data Bank dan NPWP.....	42
Gambar 3. 16 Tampilan Summary Profile.....	43
Gambar 3. 17 Tampilan Pencocokan Kriteria.....	43
Gambar 3. 18 Tampilan Pembayaran Membership.....	44
Gambar 3. 19 Tampilan Saat Order Masuk.....	44
Gambar 3. 20 Tampilan Reschedule Instruktur.....	45
Gambar 3. 21 Tampilan Pembatalan Order.....	45
Gambar 3. 22 Tampilan saat Scan Barcode.....	46
Gambar 3. 23 Tampilan Penarikan Dana Instruktur.....	46
Gambar 4. 1 Surat Izin Penelitian.....	51
Gambar 4. 2 Surat Keterangan Riset.....	52
Gambar 4. 3 List Directory dari folder shared_prefs.....	61
Gambar 4. 4 Isi dari file CapacitorStorage.xml.....	62
Gambar 4. 5 Aplikasi dapat di backup tanpa password.....	63

Gambar 4. 6 Contoh HTTP pada source code	63
Gambar 4. 7 Packet sniffing pada URL	64
Gambar 4. 8 Hasil Packet Sniffing	64
Gambar 4. 9 Hasil Reverse engineering	65
Gambar 4. 10 Hasil testing google api key	66
Gambar 4. 11 Data akun pertama.....	67
Gambar 4. 12 Data Akun Kedua.....	68
Gambar 4. 13 Melakukan Forgot Password.....	69
Gambar 4. 14 Alamat IP Lokal	69
Gambar 4. 15 Tambah Proxy Baru	70
Gambar 4. 16 Homepage Buurpsuite di Android	71
Gambar 4. 17 cacert.der pada folder download	71
Gambar 4. 18 Mengganti Nama menjadi cacert.cer.....	72
Gambar 4. 19 Instalasi pada kartu SD	72
Gambar 4. 20 Memberi nama pada sertifikat.....	73
Gambar 4. 21 Konfigurasi proxy pada wifi	73
Gambar 4. 22 Intercept pada data	74
Gambar 4. 23 Intercept Data setelah di klik	74
Gambar 4. 24 Hasil Response.....	75
Gambar 4. 25 Memasukan OTP code hasil response.....	76
Gambar 4. 26 Mengganti password baru	76
Gambar 4. 27 Session expired pada akun 2	77
Gambar 4. 28 Masuk ke akun 2	78
Gambar 4. 29 Mengisi OTP code secara random	79
Gambar 4. 30 Mengganti Password Baru	80
Gambar 4. 31 Memasukan OTP sembarang	81
Gambar 4. 32 Setting target pada intruder	82
Gambar 4. 33 Setting position pada intruder	82
Gambar 4. 34 Setting payload pada intruder	83
Gambar 4. 35 Setting Options pada intruder	84
Gambar 4. 36 Monitoring intruder attack	85
Gambar 4. 37 Melakukan forgot password.....	86
Gambar 4. 38 Melakukan intercept.....	86
Gambar 4. 39 Setting Target pada intruder.....	87
Gambar 4. 40 Setting position pada intruder	87
Gambar 4. 41 Melakukan setting pada Payload di intruder.....	88
Gambar 4. 42 Melakukan setting pada options di intruder	88
Gambar 4. 43 monitoring intruder attack.....	89

Gambar 4. 44 skor kerentanan file temp.....	90
Gambar 4. 45 skor kerentanan full-backup.....	91
Gambar 4. 46 Skor kerentanan insecure communication.....	93
Gambar 4. 47 Skor kerentanan reverse engineering.....	95
Gambar 4. 48 skor kerentanan account takeover	97
Gambar 4. 49 skor kerentanan bypass otp code.....	99
Gambar 4. 50 skor kerentanan bruteforce otp.....	101
Gambar 4. 51 skor kerentanan no rate limit otp code	103



DAFTAR TABEL

	Halaman
Tabel 2. 1 CVSS 3.0 Scoring	20
Tabel 3. 1 Daftar Wawancara	28
Tabel 3. 2 Penelitian Terdahulu	29
Tabel 3. 3 Jadwal Perencanaan Penelitian	48
Tabel 4. 1 Informasi Aplikasi Berdasarkan MobSF	54
Tabel 4. 2 Perbandingan hasil pemindaian MobSF dan Yaazhini	57
Tabel 4. 3 Area fungsional yang diujikan	58
Tabel 4. 4 Hasil Pemetaan Analisis Dinamis	60