

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN	iii
PERNYATAAN BEBAS PLAGIASI.....	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
ABSTRAK.....	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penelitian	4
BAB II TINJAUAN PUSTAKA	5
2.1 <i>Internet of Things</i>	5
2.2 <i>Smart Parking</i>	6
2.3 <i>Smartphone</i>	6
2.4 <i>Android</i>	7
2.5 <i>Android Studio</i>	8
2.5.1 Struktur Proyek Android Studio	8
2.5.2 Antarmuka Pengguna Android Studio	9
2.6 <i>Mobile Backend as Service</i>	10
2.7 <i>Firebase</i>	10
2.8 <i>Open Web Application Security Project (OWASP)</i>	11
2.9 <i>Mobile Application Security Verification Standard (MASVS)</i>	11
2.10 <i>OWASP Mobile Security Testing Guide (MSTG)</i>	12
2.11 <i>OWASP Risk Rating Methodology</i>	13
2.11.1 Menilai Faktor <i>Thread Agent</i>	14
2.11.2 Menilai Faktor <i>Vulnerability</i>	14

2.11.3 Menilai Faktor <i>Technical impact</i>	15
2.11.4 Menilai Faktor <i>Business impact</i>	16
2.11.5 Menilai dampak risiko	16
2.12 Hipotesis	21
BAB III METODE PENELITIAN.....	22
3.1 Bahan	22
3.2 Peralatan.....	22
3.3 Prosedur Penelitian	23
3.3.1 Metode Penelitian.....	23
3.3.2 Implementasi Sistem Pengujian	24
3.3.3 Perancangan Topologi.....	27
3.4 Identifikasi persyaratan aplikasi.....	27
3.5 Desain RAD	28
3.5.1 Perancangan Model	28
3.5.2 Pembuatan Antarmuka Aplikasi	29
1. Antarmuka <i>Splash Screen</i>	29
2. Antarmuka <i>Login</i>	30
3. Antarmuka Daftar.....	30
4. Antarmuka <i>Home</i>	31
5. Antarmuka <i>Monitoring</i>	31
3.6 Konfigurasi <i>Firebase</i>	32
3.7 Konfigurasi Program <i>ESP32</i> dan <i>Proximity</i>	33
3.8 Skenario Pengujian	34
3.8.1 Skenario <i>Password Attack</i>	34
3.8.2 Skenario Intercepting Network	34
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	36
4.1 Pengembangan Aplikasi.....	37
4.1.1 <i>Splash Screen</i>	37
4.1.2 <i>Login</i>	38
4.1.3 Daftar.....	38
4.1.4 <i>Home</i>	39
4.1.5 Monitoring.....	39
4.2 Purwarupa Parkir.....	40
4.3 Pengujian Sistem.....	40

4.4	Pengujian Serangan Skenario <i>Password Attack</i>	41
4.5	Pengujian Serangan Skenario <i>Intercepting Network</i>	44
4.6	Asesmen OWASP <i>Risk Rating</i>	46
4.6.1	Menilai Faktor <i>Threat Agent</i>	46
4.6.2	Menilai Faktor <i>Vulnerability</i>	47
4.6.3	Menilai Faktor <i>Technical Impact</i>	48
4.6.4	Menilai Faktor <i>Business Impact</i>	49
4.6.5	Menentukan Dampak Risiko	50
4.6.6	Tingkat Risiko Keseluruhan	53
BAB V PENUTUP		54
5.1	Kesimpulan	54
5.2	Saran.....	54
DAFTAR PUSTAKA		55
LAMPIRAN		57

DAFTAR GAMBAR

Gambar 2.1 Pengguna smartphone di Indonesia dari tahun ke tahun	7
Gambar 2.2 Penggunaan sistem operasi mobile di Indonesia	7
Gambar 2.3 Tampilan Workspace Android.....	9
Gambar 3. 1 Diagram Alur Tahapan Penelitian.....	24
Gambar 3.2 Fase Model RAD	25
Gambar 3.3 Topologi implementasi sistem	27
Gambar 3.4 Use Case Diagram Aplikasi Android	29
Gambar 3.5 Flow Chart Aplikasi Android	29
Gambar 3.6 Antarmuka Splash Screen.....	30
Gambar 3.7 Antarmuka Login.....	30
Gambar 3.8 Antarmuka Daftar	31
Gambar 3.9 Antarmuka Home.....	31
Gambar 3.10 Antarmuka Monitoring	32
Gambar 3.11 Pendaftaran aplikasi pada Firebase.....	32
Gambar 3.12 Struktur Proyek dalam Android Studio	33
Gambar 3.13 Konfigurasi Program ESP32.....	33
Gambar 3.14 Skenario Password Attack	34
Gambar 3.15 Skenario Intercepting Network.....	34
Gambar 4. 1 database pada Firebase	36
Gambar 4. 2 Tampilan Splash Screen	37
Gambar 4. 3 Tampilan Login	38
Gambar 4. 4 Tampilan Daftar.....	38
Gambar 4. 5 Tampilan Home	39
Gambar 4. 6 Tampilan Monitoring.....	39
Gambar 4. 7 Purwarupa tempat parkir.....	40
Gambar 4. 8 Alamat IP pada ESP32 dan Firebase	40
Gambar 4. 9 Paket data yang dikirim dan paket data response	41
Gambar 4. 10 setting proxy listener pada Burp Suite	42
Gambar 4. 11 Setting Intercept Client Request	42
Gambar 4. 12 setting sertifikat CA pada device	43
Gambar 4. 13 Packet yang tertangkap terlihat pada kolo HTTP history	43
Gambar 4. 14 Hasil password attack	44
Gambar 4. 15 setting proxy listener pada Burp Suite.....	44
Gambar 4. 16 Setting Intercept Client Request	45
Gambar 4. 17 Paket data yang akan dimanipulasi.....	45
Gambar 4. 18 Hasil intercept network slot parkir menjadi penuh.....	46

DAFTAR TABEL

Tabel 2.1 Faktor Threat Agent	14
Tabel 2.2 Faktor Vulnerability	14
Tabel 2.3 Faktor Technical impact.....	15
Tabel 2.4 Faktor Business impact.....	16
Tabel 2.5 Likelihood dan Impact Levels	18
Tabel 2.6 Ringkasan uraian penelitian	19
Tabel 3. 1 Spesifikasi Komputer Virtual.....	22
Tabel 3. 2 Spesifikasi ESP32.....	22
Tabel 3. 3 Spesifikasi ESP32.....	22
Tabel 3. 4 Spesifikasi ESP32.....	23
Tabel 3. 5 Spesifikasi Laptop	23
Tabel 4. 1 Faktor Threat Agent.....	47
Tabel 4. 2 Faktor Vulnerability	48
Tabel 4. 3 Faktor Technical Impact.....	49
Tabel 4. 4 Faktor Business Impact	50
Tabel 4. 5 Likelihood and Impact Level.....	52
Tabel 4. 6 Hasil kemungkinan dan dampak pada kerentanan Password Attack	53
Tabel 4. 7 Hasil kemungkinan dan dampak pada kerentanan Intercept Network	53