

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
PERNYATAAN KEASLIAN PROYEK AKHIR	iv
KATA PENGANTAR.....	v
DAFTAR ISI	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	xi
INTISARI	xii
ABSTRACT	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian	3
1.4 Batasan Masalah	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penelitian.....	5
BAB II TINJAUAN PUSTAKA	6
2.1 Tinjauan Pustaka.....	6
2.2 Dasar Teori	12
2.2.1 Mitigasi Risiko	12
2.2.2 Aqua Digital Operations Platform (ADOP).....	14
2.2.3 Keamanan Informasi.....	14
2.2.4 Ancaman, Kerentanan, dan Serangan.....	16
2.2.5 OWASP	18
2.2.6 Insecure Design Vulnerability	20
2.2.7 Vulnerability Scanning	21
2.2.8 Zed Attack Proxy	21
2.2.9 Automated Scanning	23
2.2.10 Threat Modeling	24

2.2.11 Dekomposisi Aplikasi.....	25
2.2.12 STRIDE	25
2.2.13 DREAD	26
2.2.14 MITTRE ATT&CK.....	27
2.3 Hipotesis	28
BAB III METODE PENELITIAN	29
3.1 Waktu dan Tempat Penelitian.....	29
3.2 Peralatan Penelitian	29
3.3 Bahan Penelitian	29
3.4 Tahapan Penelitian	30
3.5 Pemindaian (<i>Automated Scanning</i>)	33
3.6 Dekomposisi Aplikasi.....	39
3.7 Klasifikasi Ancaman.....	41
3.8 Penilaian Ancaman	43
3.9 Mitigasi Ancaman.....	47
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	48
4.1 Hasil Pemindaian.....	48
4.2 Dekomposisi Aplikasi.....	49
4.2.1 Dokumen <i>Threat Model</i>	50
4.2.2 <i>Data Flow Diagram</i>	60
4.3 Klasifikasi Ancaman.....	63
4.4 Penilaian Ancaman	68
4.5 Mitigasi Risiko	74
BAB V PENUTUP	79
5.1 Kesimpulan.....	79
5.2 Saran	80
DAFTAR PUSTAKA.....	81