

## DAFTAR ISI

ABSTRAK .....	i
ABSTRACT .....	ii
KATA PENGANTAR .....	iii
DAFTAR ISI .....	v
DAFTAR GAMBAR .....	ix
DAFTAR TABEL .....	xv
DAFTAR SIMBOL .....	xvii
DAFTAR LAMPIRAN .....	xxiv
BAB 1 PENDAHULUAN .....	1
1.1    Latar Belakang .....	1
1.2    Identifikasi Masalah .....	4
1.3    Maksud dan Tujuan .....	4
1.3.1    Maksud .....	4
1.3.2    Tujuan .....	4
1.4    Batasan Masalah .....	5
1.5    Metodologi Penelitian .....	6
1.5.1    Metode Pengumpulan Data .....	8
1.5.2    Metode Pengembangan Perangkat Lunak .....	9
1.6    Tahapan – Tahapan Metode Pengujian OWASP .....	10
1.7    Sistematika Penulisan .....	13
BAB 2 TINJAUAN PUSTAKA .....	14
2.1    Profil Instansi .....	14
2.2    Logo Instansi .....	14
2.2.1    Arti dan Makna Simbol INFOLAHTA AD .....	15
2.3    Struktur Organisasi .....	16
2.4    Aplikasi Laporan Pelaksanaan Anggaran (LAPLAKGAR) .....	20

2.5	Aplikasi Berbasis Website .....	21
2.6	Monitoring Keamanan .....	21
2.7	Pengujian Celah Keamanan .....	21
2.8	Keamanan Informasi .....	22
2.9	<i>Threat</i> .....	22
2.10	<i>Attack</i> .....	22
2.11	<i>Vulnerability</i> .....	23
2.12	Jenis dan Teknik <i>Scanning</i> .....	24
2.13	<i>Vulnerability Assessment</i> .....	24
2.14	Eksploitasi .....	25
2.15	<i>Open Web Application Security Project (OWASP)</i> .....	25
2.16	OWASP TOP 10 .....	26
2.17	API .....	29
2.18	OWASP ZAP API.....	30
2.19	Pemrograman Berorientasi Objek (OOP) .....	30
2.20	UML (Unified Modeling Language).....	31
2.20.1	Use Case Diagram.....	31
2.20.2	<i>Activity Diagram</i> .....	31
2.20.3	<i>Class Diagram</i> .....	32
2.20.4	<i>Sequence Diagram</i> .....	32
2.21	Metode Pengujian Sistem.....	32
2.21.1	Pengujian Whitebox .....	32
2.21.2	Pengujian Blackbox .....	33
2.21.3	Pengujian UAT (User Acceptance Testing).....	33
2.22	<i>Tools</i> Yang Digunakan.....	33

2.22.1	Visual <i>Studio Code</i> .....	33
2.22.2	Python .....	34
2.22.3	Flask .....	34
2.22.4	SQL Alchemy .....	34
2.22.5	Jinja2 .....	34
2.22.6	Bootstrap .....	35
2.23	<i>Tools</i> Pengujian Kerentanan Sistem .....	35
2.23.1	Zed Attack Proxy .....	35
2.23.2	Postman.....	36
<b>BAB 3 ANALISIS DAN PERANCANGAN SISTEM .....</b>		<b>37</b>
3.1	Analisis Sistem.....	37
3.1.1	Analisis Masalah .....	37
3.1.2	Analisis Sistem Yang Sedang Berjalan.....	38
3.1.3	Analisis Data Yang Sedang Berjalan .....	41
3.1.4	Identifikasi Awal Kerentanan Aplikasi LAPLAGAR.....	42
3.1.5	Identifikasi Lanjutan Celah Keamanan Aplikasi LAPLAGAR ....	56
3.1.6	Analisis Solusi Yang Akan Diusulkan.....	72
3.1.7	Analisis Aplikasi Sejenis .....	73
3.1.8	Analisis Sistem yang Dibangun .....	75
3.1.9	Analisis Arsitektur Sistem .....	76
3.1.10	Analisis Basis Data .....	78
3.1.11	Analisis Subsistem Implementasi Metode OWASP Pada Identifikasi Celah Keamanan .....	84
3.1.12	Analisis Teknologi Yang Digunakan .....	86
3.1.13	Analisis Kebutuhan Non Fungsional .....	88

3.1.14	Analisis Kebutuhan Fungsional .....	91
3.2	Perancangan Sistem .....	117
3.2.1	Perancangan Struktur Menu .....	117
3.2.2	Perancangan Antarmuka .....	118
3.2.3	Perancangan Pesan .....	128
3.2.4	Perancangan Jaringan Semantik.....	131
BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM.....		132
4.1	Implementasi Sistem .....	132
4.1.1	Implementasi Perangkat Keras Pembangun.....	133
4.1.2	Implementasi Perangkat Keras Pengujian.....	133
4.1.3	Implementasi Perangkat Lunak Pembangun.....	134
4.1.4	Implementasi Perangkat Lunak Pengujian.....	134
4.1.5	Implementasi Lingkungan Web .....	134
4.1.6	Implementasi Class .....	135
4.1.7	Implementasi Basis Data.....	135
4.1.8	Implementasi Antarmuka .....	138
4.2	Pengujian Sistem.....	145
4.2.1	Pengujian Aplikasi .....	145
4.2.2	Pengujian Perbandingan Hasil Temuan Kerentanan Aplikasi .....	170
4.2.3	Perbaikan Temuan Kerentanan .....	172
4.2.4	Pengujian UAT ( <i>User Acceptance Testing</i> ).....	176
BAB 5 KESIMPULAN DAN SARAN .....		188
5.1	Kesimpulan .....	188
5.2	Saran.....	189
DAFTAR PUSTAKA .....		190