

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS.....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	x
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan.....	2
1.4. Batasan Masalah	3
BAB 2 KAJIAN PUSTAKA	4
2.1. Literature Review	4
2.2. Landasan Teori	6
2.2.1. Static Application Security Testing	6
2.2.2. Bearer CLI	7
2.2.2.1. Risiko Dan Kerentanan Keamanan.....	8
2.2.3. Large Language Model (LLM)	11
2.2.4. Python dan Flask.....	11
2.2.5. Black Box Testing.....	11
2.2.6. Owasp Benchmark	12
2.2.7. Postgresql.....	12
2.2.8. GIT Version Control	12
2.2.9. UML	13
2.2.9.1. Sequence Diagram	13
2.2.9.2. Entity Relation Diagram	13
BAB 3 PERANCANGAN SISTEM	14
3.1. Requirement.....	14
3.1.1. Identifikasi Kebutuhan.....	14
3.1.2. Dokumentasi Kebutuhan	14

3.2.	Perancangan Sistem	15
3.2.1.	Alur Proses Aplikasi	16
3.2.2.	<i>Sequence Diagram</i>	17
3.2.3.	<i>Entity Relationship Diagram</i>	30
3.2.4.	Rancangan Fitur Deteksi Kerentanan Menggunakan LLM	39
3.2.5.	Spesifikasi Perangkat Lunak	40
3.3.	Implementasi.....	41
3.3.1.	Implementasi Aplikasi	41
3.3.2.	Translasi Requirement ke dalam Fitur Aplikasi	42
3.3.3.	Arsitektur Aplikasi dan Teknologi Pendukung.....	44
3.4.	Skenario Pengujian	44
3.4.1.	Black Box Testing.....	44
3.4.2.	Pengujian Akurasi	46
3.4.2.1.	Parameter Yang Digunakan	46
3.4.2.2.	Proses Pengujian	49
3.4.3.	Uji Perbaikan Kode	50
3.4.3.1.	Identifikasi Area Perbaikan	50
3.4.3.2.	Hasil Perbaikan Dari Kode Yang Terdeteksi	50
BAB 4	HASIL DAN PEMBAHASAN	52
4.1.	Implementasi Hasil Rancangan	52
4.2.	Hasil Pengujian Fungsional Menggunakan Metode Black Box.....	56
4.3.	Hasil Pengujian Akurasi Deteksi	57
4.4.	Hasil Pengujian Akurasi Metode Analisa LLM	58
4.5.	Hasil Pengujian Pada Kode Yang Telah Diperbaiki	59
BAB 5	KESIMPULAN DAN SARAN.....	61
5.1.	Kesimpulan.....	61
5.2.	Saran	62
	DAFTAR PUSTAKA	64
	LAMPIRAN	66