

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
HALAMAN PERSEMBAHAN.....	vii
Daftar Isi.....	viii
Daftar Lampiran.....	xii
Daftar Gambar.....	xiii
Daftar Tabel	xiv
Daftar Istilah.....	xv
BAB I PENDAHULUAN	1
I.1 Latar Belakang.....	1
I.2 Perumusan Masalah.....	5
I.3 Tujuan Penelitian.....	5
I.4 Batasan Penelitian.....	5
I.5 Manfaat Penelitian.....	6

I.6	Sistematika Penulisan	6
BAB II	TINJAUAN PUSTAKA.....	8
II.1	Sistem Informasi.....	8
II.2	Keamanan Sistem Informasi.....	8
II.2.1	Keamanan Informasi	8
II.2.2	Keamanan Siber	8
II.3	Aspek Keamanan Siber	9
II.4	<i>Website</i>	10
II.5	<i>Ethical Hacking</i>	11
II.6	<i>Vulnerability Assessment</i>	11
II.7	<i>Penetration Testing</i>	11
II.8	Teknik <i>Penetration Testing</i>	11
II.9	NIST SP 800-115.....	12
II.10	Zenmap.....	14
II.11	OWASP ZAP.....	14
II.12	Burp Suite	15
II.13	Penelitian Terdahulu.....	16
BAB III	METODOLOGI PENELITIAN.....	19
III.1	Pengembangan Model Konseptual	19

III.2	Sistematika Penyelesaian Masalah	20
III.2.1	Tahap Tinjauan Literatur.....	22
III.2.2	Tahap Pengumpulan Data	22
III.2.3	Tahap Analisa Data	22
III.2.4	Tahap Interpretasi.....	23
III.3	Pengumpulan Data.....	23
III.4	Pengolahan Data	23
III.5	Metode Evaluasi	23
III.6	Alasan Pemilihan Metode.....	24
BAB IV	RANCANGAN PENGUJIAN.....	25
IV.1	<i>Planning</i>	25
IV.1.1	Spesifikasi <i>Hardware</i>	25
IV.1.2	Spesifikasi <i>Software</i>	25
IV.2	<i>Discovery</i>	26
IV.2.1	<i>Information Gathering</i>	26
IV.2.1.1	Skenario penggunaan Zenmap	26
IV.2.2	<i>Vulnerability Analysis</i>	26
IV.2.1.2	Skenario penggunaan OWASP ZAP.....	26
IV.3	<i>Attack</i>	28

IV.3.1 Skenario penggunaan Burp Suite	28
IV.4 <i>Reporting</i>	30
BAB V HASIL PENGUJIAN DAN ANALISIS	31
V.1 Hasil <i>Information Gathering</i>	31
V.2 Hasil <i>Vulnerability Analysis</i>	33
V.3 Hasil <i>Attack/Evaluasi</i>	40
V.4 Hasil Akhir dan Rekomendasi.....	43
BAB VI KESIMPULAN DAN SARAN	47
VI.1 Kesimpulan.....	47
VI.2 Saran	48
Daftar Pustaka	49
LAMPIRAN	52