

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	i
LEMBAR PENGESAHAN	ii
ABSTRAK.....	iii
<i>ABSTRACT</i>	iv
KATA PENGANTAR.....	v
Daftar Isi	vi
Daftar Gambar	ix
Daftar Tabel	x
Daftar Istilah	xi
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	3
I.3 Tujuan Penelitian	3
I.4 Batasan Penelitian	3
BAB II TINJAUAN PUSTAKA	5
II.1 Keamanan Sistem Informasi	5
II.2 <i>Website</i>	5
II.3 Keamanan <i>Website</i>	6
II.4 <i>Vulnerability</i>	6
II.5 <i>Vulnerability Assessment and Penetration Testing (VAPT)</i>	7
II.5.1 <i>Scope</i>	8
II.5.2 <i>Information Gathering</i>	8
II.5.3 <i>Vulnerability Detection</i>	8

II.5.4	<i>Vulnerability Analysis</i>	9
II.5.5	<i>Attack and Penetration testing</i>	9
II.5.6	<i>Reporting</i>	10
II.5.7	<i>Remediation</i>	10
II.6	Kali Linux	10
II.7	NMAP	11
II.8	Nessus	11
II.9	Burp Suite <i>Professional</i>	11
II.10	OWASP ZAP	12
II.11	Penelitian Terdahulu	12
II.12	Perbandingan Metode Penelitian	16
BAB III	METODOLOGI PENELITIAN	18
III.1	Model Konseptual	18
III.2	Sistematika Penyelesaian Masalah	19
III.2.1	Tahap Awal (Perumusan Masalah)	20
III.2.2	Tahap Pengujian	21
III.2.3	Tahap Akhir (Kesimpulan)	22
III.3	Alasan Pemilihan Metode Penelitian	22
BAB IV	RANCANGAN PENGUJIAN	23
IV.1	<i>Scope</i>	23
IV.1.1	Perancangan Pengujian	23
IV.2	Information Gathering	25
IV.2.1	Pengujian Menggunakan NMAP	25
IV.3	<i>Vulnerability Detection and Analysis</i>	27
IV.3.1	Hasil <i>Scanning</i> Menggunakan Nessus	28
IV.3.2	Hasil <i>Scanning</i> Menggunakan Burp Suite <i>Professional</i>	30

IV.3.3	Hasil <i>Scanning</i> Menggunakan OWASP ZAP.....	32
IV.3.4	<i>List Vulnerability</i>	34
BAB V	HASIL PENGUJIAN	36
V.1	<i>Attack and Penetration Testing</i>	36
V.1 .1	Analisis Hasil <i>Scanning</i>	36
V.2	<i>Remediation</i>	42
V.2 .1	Perancangan Mitigasi	42
V.2 .2	Pengujian Ulang Pasca Mitigasi.....	44
BAB VI	KESIMPULAN DAN SARAN	48
VI.1	Kesimpulan.....	48
VI.2	Saran.....	49
DAFTAR PUSTAKA	51
LAMPIRAN	56