

## DAFTAR ISI

LEMBAR PENGESAHAN .....	ii
LEMBAR PERNYATAAN ORISINAL .....	iii
ABSTRAK .....	iv
ABSTRACT .....	v
KATA PENGANTAR.....	vi
UCAPAN TERIMA KASIH .....	vii
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL .....	xii
DAFTAR ISTILAH .....	xiii
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang.....	1
I.2 Rumusan Masalah.....	4
I.3 Tujuan Penelitian .....	4
I.4 Batasan Penelitian.....	4
I.5 Manfaat Penelitian .....	5
I.6 Sistematika Penulisan .....	5
BAB II TINJAUAN PUSTAKA .....	7
II.1 Penelitian Terdahulu .....	7
II.2 Perbandingan Metode Penelitian.....	10
II.3 Keamanan Informasi .....	11
II.4 <i>Website</i> .....	11
II.5 <i>Vulnerability</i> .....	12
II.6 <i>Vulnerability Assessment and Penetration Testing (VAPT)</i> .....	12

II.6.1 <i>Scope</i> .....	13
II.6.2 <i>Information gathering</i> .....	13
II.6.3 <i>Vulnerability Detection</i> .....	14
II.6.4 <i>Information Analysis and Planning</i> .....	14
II.6.5 <i>Penetration Testing</i> .....	14
II.6.6 <i>Reporting</i> .....	14
II.6.7 <i>Remediation</i> .....	14
II.7 <i>CVE (Common Vulnerabilities And Exposures)</i> .....	14
II.8 <i>VirtualBox</i> .....	15
II.9 <i>Kali Linux</i> .....	15
II.10 <i>Nessus</i> .....	16
II.11 <i>OWASP ZAP</i> .....	16
II.12 <i>Burp suite</i> .....	16
<b>BAB III METODOLOGI PENELITIAN</b> .....	<b>17</b>
III.1 <i>Kerangka Berpikir</i> .....	17
III.2 <i>Sistematika Penyelesaian Masalah</i> .....	17
III.2.1 <i>Tahap Awal</i> .....	19
III.2.2 <i>Tahap Pengujian</i> .....	19
III.2.3 <i>Tahap Akhir</i> .....	19
<b>BAB IV RANCANGAN PENGUJIAN</b> .....	<b>20</b>
IV.1 <i>Scope</i> .....	20
IV.2 <i>Perancangan Pengujian</i> .....	20
IV.2.1 <i>Perangkat Hardware</i> .....	20
IV.2.2 <i>Perangkat Software</i> .....	21
IV.3 <i>Information gathering</i> .....	21
IV.3.1 <i>Hasil pengujian menggunakan NMAP</i> .....	21

IV.4 <i>Vulnerability Detection</i> .....	22
IV.4.1 Hasil <i>scanning</i> menggunakan <i>Nessus</i> .....	22
IV.4.2 Hasil <i>Scanning</i> Menggunakan <i>OWASP ZAP</i> .....	23
IV.5 <i>Information Analysis and Planning</i> .....	24
IV.5.1 Hasil <i>Information gathering</i> .....	25
IV.5.2 Perbandingan <i>tools Nessus</i> dan <i>OWASP ZAP</i> .....	25
IV.5.3 Hasil <i>Vulnerability Mining</i> .....	26
IV.5.4 <i>Vulnerability</i> dalam hal mitigasi sistem .....	27
IV.5.5 Skenario pengujian celah kerentanan .....	28
BAB V HASIL PENGUJIAN .....	29
V.1 <i>Penetration Testing</i> .....	29
V.1.1 Analisis celah kerentanan .....	29
V.2 <i>Remediation</i> .....	31
V.2.1 Perancangan Mitigasi .....	32
V.2.2 Pengujian Ulang Pasca Mitigasi .....	32
BAB VI KESIMPULAN DAN SARAN .....	34
VI.1 Kesimpulan .....	34
VI.2 Saran .....	34
DAFTAR PUSTAKA .....	35
LAMPIRAN.....	38