

## DAFTAR ISI

ABSTRAK .....	ii
<i>ABSTRACT</i> .....	iii
LEMBAR PENGESAHAN .....	iv
LEMBAR PERNYATAAN ORISINALITAS .....	v
Kata Pengantar .....	i
Daftar Isi.....	iii
Daftar Gambar.....	vii
Daftar Tabel .....	ix
Daftar Lampiran .....	x
Daftar Singkatan.....	xi
Daftar Istilah.....	xii
Bab I PENDAHULUAN.....	1
I.1 Latar Belakang.....	1
I.2 Perumusan Masalah.....	2
I.3 Tujuan Penelitian.....	2
I.4 Batasan Penelitian .....	2
I.5 Manfaat Penelitian.....	3
I.6 Sistematika Penulisan.....	3
Bab II TINJAUAN PUSTAKA.....	5
II.1 Aplikasi Web .....	5
II.2 Aset IT .....	5
II.2.1 <i>Vulnerability</i> .....	5
II.2.2 <i>Threat</i> .....	5
II.2.3 <i>Control</i> .....	6
II.3 <i>Web Application Firewall</i> .....	6

II.4	<i>Open Web Application Security Project (OWASP)</i> .....	6
II.5	<i>Walkthrough</i> .....	8
II.6	<i>Activity Diagram</i> .....	8
II.7	<i>Data Flow Diagram</i> .....	8
II.8	<i>Damn Vulnerable Web Application (DVWA)</i> .....	8
II.9	Kali Linux.....	8
II.10	OWASP-ZAP.....	9
II.11	ModSecurity.....	9
II.12	CWE.....	9
II.13	CVE .....	9
II.14	CVSS .....	10
II.14.1	<i>CVSS v2 Calculator</i> .....	10
II.14.2	<i>CVSS Score</i> .....	10
II.15	Penelitian Terdahulu .....	10
Bab III	METODOLOGI PENELITIAN .....	13
III.1	Model Konseptual.....	13
III.2	Sistematika Penyelesaian Masalah .....	14
III.2.1	Tahap Awal (Perumusan Masalah) .....	14
III.2.2	Tahap Perancangan .....	15
III.2.3	Tahap Eksperimen.....	15
III.2.4	Tahap Analisis.....	15
III.2.5	Tahap Akhir (Kesimpulan) .....	15
Bab IV	PERANCANGAN DAN SKENARIO PENGUJIAN .....	17
IV.1	<i>Reconnaissance</i> .....	17
IV.1.1	Spesifikasi Perangkat Keras .....	17
IV.1.2	Spesifikasi Perangkat Lunak .....	17

IV.1.3	Model Lapisan Jaringan TCP/IP .....	21
IV.1.4	Platform Eksperimen.....	22
IV.1.5	Daftar IP Address .....	23
IV.2	<i>Scanning</i> .....	23
IV.2.1	Skenario Pengujian <i>Vulnerability Scanning</i> Menggunakan OWASP-ZAP.....	23
IV.2.2	Hasil Pengujian <i>Vulnerability Scanning</i> Menggunakan OWASP-ZAP	24
IV.3	<i>Exploitation</i> .....	26
IV.3.1	Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i> .....	27
IV.3.2	Skenario Pengujian Serangan Berdasarkan <i>Data Flow Diagram</i> .	27
IV.3.3	Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough</i> .....	28
IV.3.3.1	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough SQL Injection</i> .....	28
IV.3.3.2	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Brute Force</i> .....	32
IV.3.3.3	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough File Upload</i> .....	36
IV.3.3.4	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Cross-Site Scripting</i> .....	40
IV.3.3.5	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Remote File Inclusion</i> .....	44
IV.3.3.6	Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Weak Session ID</i> .....	48
Bab V	ANALISIS .....	52
V.1	Proses dan Hasil Pengujian .....	52
V.1.1	Hasil dari Proses Pengujian <i>Walkthrough SQL Injection</i> .....	52
V.1.2	Hasil dari Proses Pengujian <i>Walkthrough Brute Force</i> .....	57

V.1.3	Hasil dari Proses Pengujian <i>Walkthrough File Upload</i> .....	60
V.1.4	Hasil dan Proses Pengujian <i>Walkthrough Cross-Site Scripting</i> ....	63
V.1.5	Hasil dari Proses Pengujian <i>Walkthrough Remote File Inclusion</i>	67
V.1.6	Hasil dan Proses Pengujian <i>Walkthrough Weak Session ID</i> .....	71
V.2	Analisis Perhitungan <i>Vulnerability</i> Menggunakan <i>CVSS Calculator</i> .	74
V.3	Analisis <i>Control</i> Secara Kuantitatif Berdasarkan <i>Vulnerability</i> dan <i>Threat</i>	81
V.4	Analisis <i>Control</i> Secara Kualitatif Berdasarkan <i>Vulnerability</i> dan <i>Threat</i>	83
Kesimpulan dan Saran.....		86
V.5	Kesimpulan.....	86
V.6	Saran.....	86
Daftar Pustaka .....		87