

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvi
DAFTAR SINGKATAN	xx
DAFTAR ISTILAH	xxi
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
BAB II TINJAUAN PUSTAKA	4
II.1 Aplikasi <i>Web</i>	4
II.2 <i>Web Application Firewall</i> (WAF)	4
II.3 <i>Open Web Application Security Project</i> (OWASP)	5
II.4 <i>Vulnerability</i>	5
II.5 <i>Threat</i>	5
II.6 <i>Attack Tree</i>	6

II.7	<i>Damn Vulnerable Web Application (DVWA)</i>	6
II.8	Eksploitasi.....	6
II.9	<i>Activity Diagram</i>	6
II.10	<i>Data Flow Diagram (DFD)</i>	7
II.11	<i>Reconnaissance</i>	7
II.12	<i>Vulnerability Scanning</i>	7
II.13	Kali Linux	8
II.14	Linux Ubuntu	8
II.15	<i>SQL Injection</i>	8
II.16	<i>Cross-Site Scripting (XSS)</i>	8
II.17	<i>Command Injection</i>	9
II.18	<i>Cross Site Request Forgery (CSRF)</i>	9
II.19	<i>Brute Force</i>	10
II.20	Metrik <i>Time</i>	10
II.21	Metrik <i>Probability</i>	10
II.22	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)	15
III.2.2	Tahap Hipotesis.....	16
III.2.3	Tahap Desain.....	16
III.2.4	Tahap Pengujian.....	16
III.2.5	Tahap Analisis.....	17
III.2.6	Tahap Akhir	17
III.3	Pengumpulan Data.....	18

III.4	Pengolahan Data	18
III.5	Metode Evaluasi	18
BAB IV	PERANCANGAN DAN SKENARIO PENGUJIAN	19
IV.1	<i>Reconnaissance</i>	19
IV.1.1	Spesifikasi Perangkat Keras	19
IV.1.2	Spesifikasi Perangkat Lunak	19
IV.1.3	Model Lapisan OSI	22
IV.1.4	<i>Platform</i> Eksperimen	25
IV.1.5	Daftar <i>IP Address</i>	27
IV.2	Skenario Pengujian	27
IV.2.1	Skenario Pengujian Eksploitasi.....	28
IV.3	<i>Scanning</i>	30
IV.3.1	Hasil Pengujian <i>Vulnerability Scanning</i> Menggunakan OWASP-ZAP	31
IV.4	Eksploitasi Pengujian.....	32
IV.4.1	Eksploitasi Pengujian <i>SQL Injection</i>	32
IV.4.2	Eksploitasi Pengujian XSS (<i>Reflected</i>)	34
IV.4.3	Eksploitasi Pengujian <i>Command Injection</i>	35
IV.4.4	Eksploitasi Pengujian CSRF	37
IV.4.5	Eksploitasi Pengujian <i>Brute Force</i>	39
IV.5	Hasil Data Percobaan.....	41
IV.5.1	Perumusan Serangan Dengan <i>Activity Diagram</i> Berdasarkan Eksploitasi.....	42
IV.5.2	Perumusan Serangan Dengan Data <i>Flow</i> Berdasarkan Eksploitasi	61
BAB V	HASIL DAN ANALISIS	78
V.1	Analisis <i>Attack Tree</i>	78

V.1 .1	<i>Attack Tree</i> Pada Eksploitasi <i>SQL Injection</i>	78
V.1 .2	<i>Attack Tree</i> Pada Eksploitasi <i>XSS (Reflected)</i>	81
V.1 .3	<i>Attack Tree</i> Pada Eksploitasi <i>Command Injection</i>	83
V.1 .4	<i>Attack Tree</i> Pada Eksploitasi <i>CSRF</i>	86
V.1 .5	<i>Attack Tree</i> Pada Eksploitasi <i>Brute Force</i>	88
V.1 .6	Hasil <i>Attack Tree</i> Berdasarkan Lima Eksploitasi	91
V.2	Pengukuran <i>Time</i> Pada Eksperimen Eksploitasi.....	93
V.2 .1	Hasil Pengukuran <i>Time</i> Eksploitasi <i>SQL Injection</i>	95
V.2 .2	Hasil Pengukuran <i>Time</i> Eksploitasi <i>XSS (Reflected)</i>	96
V.2 .3	Hasil Pengukuran <i>Time</i> Eksploitasi <i>Command Injection</i>	97
V.2 .4	Hasil Pengukuran <i>Time</i> Eksploitasi <i>CSRF</i>	98
V.2 .5	Hasil Pengukuran <i>Time</i> Eksploitasi <i>Brute Force</i>	100
V.3	Pengukuran <i>Probability</i> Pada Eksperimen Eksploitasi	101
V.3 .1	Hasil Pengukuran <i>Probability</i> Keberhasilan Eksploitasi <i>SQL Injection</i> 102	
V.3 .2	Hasil Pengukuran <i>Probability</i> Keberhasilan Eksploitasi <i>XSS (Reflected)</i>	103
V.3 .3	Hasil Pengukuran <i>Probability</i> Keberhasilan Eksploitasi <i>Command Injection</i> 104	
V.3 .4	Hasil Pengukuran <i>Probability</i> Keberhasilan Eksploitasi <i>CSRF</i> . 105	
V.3 .5	Hasil Pengukuran <i>Probability</i> Keberhasilan Eksploitasi <i>Brute Force</i> 106	
V.4	Hasil Analisis <i>Attack Tree Development</i> Dengan Metrik <i>Time</i> dan <i>Probability</i>	108
V.4 .1	Analisis Perbandingan Metrik <i>Time</i>	108
V.4 .2	Analisis Perbandingan Metrik <i>Probability</i>	115

V.4 .3 Hasil Perbandingan <i>Attack Tree</i> Berdasarkan Metrik <i>Time</i> dan <i>Probability</i>	120
V.4 .4 Hasil Perbandingan Masing-Masing <i>Attack Tree</i>	133
BAB VI KESIMPULAN DAN SARAN	138
VI.1 Kesimpulan	138
VI.2 Saran	138
Daftar Pustaka	139
Lampiran	143