

## DAFTAR ISI

ABSTRAK .....	ii
ABSTRACT .....	iii
LEMBAR PENGESAHAN .....	iv
LEMBAR PERNYATAAN ORISINALITAS .....	v
LEMBAR PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	xii
DAFTAR TABEL .....	xiv
DAFTAR LAMPIRAN .....	xvi
DAFTAR ISTILAH .....	xvii
DAFTAR SINGKATAN .....	xix
Bab I PENDAHULUAN .....	1
I.1 Latar Belakang .....	1
I.2 Perumusan Masalah .....	2
I.3 Tujuan Penelitian .....	2
I.4 Batasan Penelitian .....	3
I.5 Manfaat Penelitian .....	3
Bab II TINJAUAN PUSTAKA .....	4
II.1 <i>Content Management System (CMS)</i> .....	4
II.2 WordPress .....	4
II.3 <i>WordPress Plugin</i> .....	4
II.4 <i>Cybersecurity</i> .....	5
II.5 <i>Open Web Application Security Project (OWASP)</i> .....	5

II.6	<i>Vulnerability</i> .....	6
II.7	<i>Threat dan Control</i> .....	7
II.8	Ancaman Keamanan Data .....	7
II.9	CVE .....	8
II.10	CVSS .....	8
II.11	VirtualBox .....	10
II.12	Ubuntu Server .....	11
II.13	Kali Linux .....	11
II.14	Penelitian Tedahulu .....	11
BAB III	METODOLOGI PENELITIAN .....	13
III.1	Model Konseptual .....	13
III.2	Sistematika Penyelesaian Masalah .....	14
III.2.1	Tahap Awal .....	16
III.2.2	Tahap Hipotesis.....	16
III.2.3	Tahap Eksperimen.....	16
III.2.4	Tahap Analisis.....	16
III.2.5	Tahap Akhir .....	17
III.3	Pengumpulan Data.....	17
III.4	Pengolahan Data .....	17
III.5	Metode Evaluasi .....	17
Bab IV	PERANCANGAN DAN HASIL PENGUJIAN.....	18
IV.1	Persiapan dan Perancangan.....	18
IV.1.1	Spesifikasi <i>Hardware</i> .....	18
IV.1.2	Spesifikasi <i>Software</i> .....	19
IV.1.3	<i>Platform</i> Eksperimen .....	20
IV.1.4	Daftar IP <i>Address</i> .....	21

IV.2	Skenario Pengujian .....	22
IV.2.1	Skenario Pengujian Eksploitasi.....	22
IV.2.2	Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i> dan <i>Data Flow Diagram</i> .....	23
IV.3	Eksploitasi Pengujian.....	24
IV.3.1	Pengujian Eksploitasi Kerentanan MStore-API <i>Plugin</i> .....	25
IV.3.2	Pengujian Eksploitasi Kerentanan Modern Event Calender Lite <i>Plugin</i> .....	31
IV.3.3	Pengujian Eksploitasi Kerentanan WPS-Hide-Login <i>Plugin</i> .....	38
IV.3.4	Pengujian Eksploitasi Kerentanan XXE .....	44
IV.3.5	Pengujian Eksploitasi Serangan <i>Brute Force</i> .....	50
IV.3.6	Pengujian Eksploitasi Kerentanan Elementor <i>Plugin</i> .....	55
IV.3.7	Pengujian Eksploitasi Kerentanan Catch Themes Demo Import <i>Plugin</i> .....	61
Bab V	ANALISIS .....	67
V.1	Tahap Analisis .....	67
V.2	Analisis Ancaman.....	67
V.2.1	Analisis Ancaman Terhadap Keamanan Data.....	67
V.2.2	Analisis Ancaman Menggunakan Standar OWASP .....	71
V.3	Analisis Kerentanan .....	72
V.3.1	Identifikasi CVE ID .....	72
V.3.2	Penentuan Skor CVE Menggunakan CVSS.....	74
V.3.3	Penentuan Tingkat Keparahan .....	77
V.4	Analisis Kontrol .....	78
V.4.1	Strategi Mekanisme Keamanan .....	78
V.4.2	Desain Kontrol Keamanan .....	79
V.4.3	Panduan Praktis Mekanisme Keamanan .....	82

Bab VI	KESIMPULAN DAN SARAN .....	87
VI.1	KESIMPULAN.....	87
VI.2	SARAN.....	88
	DAFTAR PUSTAKA .....	89
	LAMPIRAN.....	92