

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	xviii
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 <i>Content Management System (CMS)</i>	4
II.2 WordPress	4
II.3 <i>Cyber Security</i>	4
II.4 OWASP	5
II.5 <i>Threat</i>	5

II.6	<i>Vulnerability</i>	6
II.7	CVE.....	6
II.8	CVSS.....	7
II.9	Eksplorasi	7
II.10	<i>Activity Diagram</i>	7
II.11	<i>Data Flow Diagram</i>	8
II.12	Linux Ubuntu.....	8
II.13	Kali Linux.....	8
II.14	VirtualBox	8
II.15	XML-RPC.....	9
II.16	<i>Brute Force</i>	9
II.17	DDoS	9
II.18	MITM <i>Attack</i>	10
II.19	Penelitian Terdahulu	10
Bab III	METODOLOGI PENELITIAN	13
III.1	Model Konseptual	13
III.2	Sistematika Penyelesaian Masalah.....	14
III.2.1	Tahap Awal	15
III.2.2	Tahap Hipotesis.....	15
III.2.3	Tahap Eksperimen.....	16
III.2.4	Tahap Analisis.....	16
III.2.5	Tahap Akhir	16
III.3	Pengumpulan Data	16
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 Perangkat Keras	18
IV.1.2	Spesifikasi Perangkat Lunak	19
IV.1.3	Platform Eksperimen.....	22
IV.1.4	Daftar Alamat IP	23
IV.2	Skenario Pengujian.....	24
IV.2.1	Skenario Pengujian Eksploitasi.....	24
IV.2.2	Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i> dan <i>Data Flow Diagram</i>	26
IV.3	Eksploitasi Pengujian	27
IV.3.1	Eksploitasi Pengujian XML-RPC	27
IV.3.2	Eksploitasi Pengujian DDoS	35
IV.3.3	Eksploitasi Pengujian <i>Packet Sniffing</i>	43
IV.3.4	Eksploitasi Pengujian <i>Packet Data Manipulation</i>	51
IV.3.5	Eksploitasi Pengujian <i>Session Hijacking</i>	59
Bab V	ANALISIS.....	69
V.1	Tahap Analisis	69
V.2	Analisis Ancaman.....	69
V.2.1	Analisis Ancaman Terhadap Keamanan Data.....	69
V.2.2	Analisis Ancaman Menggunakan Standar Dari OWASP	72
V.3	Analisis Kerentanan	74
V.3.1	Identifikasi CVE ID	75
V.3.2	Penentuan Skor CVE Menggunakan CVSS.....	76
V.3.3	Penentuan Tingkat Keparahan Kerentanan.....	79
V.4	Analisis Kontrol	80
V.4.1	Strategi Mekanisme Keamanan	80

V.4.2	Desain Kontrol Keamanan Berdasarkan Kerentanan Yang Dieksploitasi oleh Ancaman	83
V.4.3	Panduan Praktis Desain Kontrol Keamanan Berdasar Aspek Jaringan Pada WordPress.....	86
Bab VI	KESIMPULAN DAN SARAN	93
VI.1	Kesimpulan.....	93
VI.2	Saran.....	94
	DAFTAR PUSTAKA	95
	LAMPIRAN.....	98