

DAFTAR ISI

ABSTRAK	ii
<i>ABSTRACT</i>	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	xv
DAFTAR ISTILAH	xvi
DAFTAR SINGKATAN	xviii
Bab I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	3
I.3 Tujuan Penelitian	3
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	4
Bab II TINJAUAN PUSTAKA	5
II.1 <i>Content Management System (CMS)</i>	5
II.2 WordPress	5
II.3 <i>WordPress Plugin</i>	5
II.4 <i>Cyber Security</i>	5
II.5 <i>Open Web Application Security Project (OWASP)</i>	6

II.6	<i>Vulnerability</i>	6
II.7	<i>Cyber threat</i>	6
II.8	<i>Common Vulnerability and Exposure (CVE)</i>	7
II.9	<i>Common Vulnerability Scoring System (CVSS)</i>	7
II.10	Kali Linux	12
II.11	Penelitian Terdahulu	12
Bab III METODOLOGI PENELITIAN		14
III.1	Kerangka Berpikir	14
III.2	Sistematika Penyelesaian Masalah	15
III.2.1	Tahap Awal	16
III.2.2	Tahap Hipotesis.....	17
III.2.3	Tahap Eksperimen.....	17
III.2.4	Tahap Analisis.....	17
III.2.5	Tahap Akhir	17
III.3	Pengumpulan Data	17
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	21
IV.1.3	<i>Platform</i> Eksperimen	22
IV.1.4	Daftar <i>IP Address</i>	24
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>	25
IV.3	Eksploitasi Pengujian	26
IV.3.1	Pengujian Eksploitasi Kerentanan <i>Path Traversal</i> pada WordPress 27	
IV.3.2	Pengujian Eksploitasi Kerentanan <i>Plugin Social Warfare</i> pada WordPress.....	36
IV.3.3	Pengujian Eksploitasi Kerentanan pada PHP versi 8.1.0-dev.....	45
IV.3.4	Pengujian Eksploitasi Kerentanan pada Apache 2.4.49.....	51
IV.3.5	Pengujian Kerentanan Dengan <i>SQL Injection</i>	59
Bab V	ANALISIS	71
V.1	Tahap Analisis	71
V.2	Analisis Ancaman.....	71
V.2.1	Analisis Ancaman Terhadap Keamanan Data.....	71
V.2.2	Analisis Ancaman Menggunakan Standar dari OWASP.....	76
V.3	Analisis Kerentanan	78
V.3.1	Identifikasi CVE ID	78
V.3.2	Penentuan Skor CVE Menggunakan CVSS.....	79
V.3.3	Penentuan Tingkat Keparahan	89
V.4	Analisis Kontrol	90
V.4.1	Strategi Mekanisme Keamanan	90
V.4.2	Panduan Praktis Mekanisme Keamanan Error! Bookmark not defined.	
V.5	Desain Kontrol Berdasarkan Kerentanan yang dieksploitasi Oleh <i>Threat Error! Bookmark not defined.</i>	
Bab VI	KESIMPULAN DAN SARAN	98
VI.1	Kesimpulan.....	98

VI.2 Saran.....	99
Daftar Pustaka.....	100
LAMPIRAN.....	102