

DAFTAR GAMBAR

Gambar III. 1 Model Konseptual Penelitian	13
Gambar III. 2 Sistematika Penyelesaian Masalah.....	15
Gambar IV. 1 <i>Platform</i> Eksperimen	21
Gambar IV. 2 Skenario Pengujian Eksploitasi.....	23
Gambar IV. 3 Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i> dan <i>Data Flow Diagram</i>	24
Gambar IV. 4 Skenario Eksploitasi MStore-API <i>Plugin</i>	25
Gambar IV. 5 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi MStore-API <i>Plugin</i>	27
Gambar IV. 6 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi MStore-API <i>Plugin</i>	29
Gambar IV. 7 Proses Eksploitasi MStore-API <i>plugin</i>	30
Gambar IV. 8 Hasil Implementasi Eksploitasi MStore-API <i>plugin</i>	30
Gambar IV. 9 Skenario Eksploitasi Modern Events Calendar Lite <i>plugin</i>	32
Gambar IV. 10 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi Modern Event Calender Lite <i>Plugin</i>	34
Gambar IV. 11 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi Modern Event Calender Lite <i>Plugin</i>	36
Gambar IV. 12 Eksploitasi Modern Event Calendar Lite <i>plugin</i>	37
Gambar IV. 13 Hasil Implementasi Eksploitasi Modern Event Calendar Lite <i>plugin</i>	37
Gambar IV. 14 Skenario Eksploitasi WPS-Hide-Login <i>plugin</i>	39
Gambar IV. 15 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi WPS-Hide-Login <i>Plugin</i>	41
Gambar IV. 16 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi WPS-Hide-Login <i>Plugin</i>	42
Gambar IV. 17 Hasil Implementasi Eksploitasi WPS-Hide-Login <i>plugin</i>	43
Gambar IV. 18 Skenario Eksploitasi Kerentanan XXE.....	44
Gambar IV. 19 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi XXE	46
Gambar IV. 20 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi XXE.....	48

Gambar IV. 21 Proses Eksploitasi Terhadap Kerentanan XXE.....	48
Gambar IV. 22 Hasil Eksploitasi Pada Kerentanan XXE	49
Gambar IV. 23 Skenario Serangan <i>Brute Force</i>	50
Gambar IV. 24 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi Serangan <i>Brute Force</i>	52
Gambar IV. 25 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi Serangan <i>Brute Force</i>	53
Gambar IV. 26 Hasil Eksploitasi Terhadap Serangan <i>Brute Force</i>	54
Gambar IV. 27 Skenario Pengujian Eksploitasi Elementor <i>plugin</i>	55
Gambar IV. 28 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi Elementor <i>Plugin</i>	57
Gambar IV. 29 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi Elementor <i>Plugin</i>	59
Gambar IV. 30 Hasil Eksploitasi Kerentanan Elementor <i>plugin</i>	60
Gambar IV. 31 Skenario Pengujian Eksploitasi Catch Themes Demo Import <i>plugin</i>	61
Gambar IV. 32 <i>Activity Diagram</i> Serangan Berdasarkan Eksploitasi Catch Themes Demo Import <i>Plugin</i>	63
Gambar IV. 33 Hasil Perumusan Serangan Dengan <i>Data Flow Diagram</i> Berdasarkan Eksploitasi Catch Themes Demo Import <i>Plugin</i>	65
Gambar IV. 34 Hasil Eksploitasi Catch Themes Demo Import <i>plugin</i>	65
Gambar V. 1 CVSS <i>Calculator Base Metrics</i>	76