

DAFTAR GAMBAR

Gambar II- 1 Tahapan OWASP	7
Gambar III- 1 Model Konseptual Penelitian.....	13
Gambar III- 2 Sistematika Penelitian.....	14
Gambar IV- 1 Model lapisan jaringan TCP/IP	21
Gambar IV- 2 Platform Eksperimen	22
Gambar IV- 3 Skenario Pengujian <i>Vulnerability Scanning</i> Menggunakan OWASP-ZAP.....	24
Gambar IV- 4 <i>Scanning Report</i>	25
Gambar IV- 5 Skenario Pengujian Serangan Berdasarkan <i>Activity Diagram</i>	27
Gambar IV- 6 Skenario Pengujian Serangan Berdasarkan <i>Data Flow Diagram</i>	28
Gambar IV- 7 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough SQL Injection</i> (1).....	30
Gambar IV- 8 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough SQL Injection</i> (2).....	32
Gambar IV- 9 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Brute Force</i> (1).....	34
Gambar IV- 10 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Brute Force</i> (2).....	36
Gambar IV- 11 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough File Upload</i> (1).....	38
Gambar IV- 12 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough File Upload</i> (2).....	40
Gambar IV- 13 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Cross-Site Scripting</i> (1).....	42
Gambar IV- 14 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Cross-Site Scripting</i> (2).....	44
Gambar IV- 15 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Remote File Inclusion</i> (1).....	46
Gambar IV- 16 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Remote File Inclusion</i> (2).....	48

Gambar IV- 17 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Weak Session ID</i> (1).....	49
Gambar IV- 18 Hasil Perumusan <i>Activity Diagram</i> Berdasarkan <i>Walkthrough Weak Session ID</i> (2).....	51
Gambar V- 1 Hasil Proses Pengujian <i>Walkthrough SQL Injection</i> (1).....	55
Gambar V- 2 Hasil Proses Pengujian <i>Walkthrough SQL Injection</i> (2).....	57
Gambar V- 3 Hasil Proses Pengujian <i>Walkthrough Brute Force</i> (1).....	58
Gambar V- 4 Hasil Proses Pengujian <i>Walkthrough Brute Force</i> (2).....	60
Gambar V- 5 Hasil Proses Pengujian <i>Walkthrough File Upload</i> (1).....	62
Gambar V- 6 Hasil Proses Pengujian <i>Walkthrough File Upload</i> (2).....	63
Gambar V- 7 Hasil Proses Pengujian <i>Walkthrough Cross-Site Scripting</i> (1).....	65
Gambar V- 8 Hasil Proses Pengujian <i>Walkthrough Cross-Site Scripting</i> (2).....	67
Gambar V- 9 Hasil Proses Pengujian <i>Walkthrough Remote File Inclusion</i> (1).....	69
Gambar V- 10 Hasil Proses Pengujian <i>Walkthrough Remote File Inclusion</i> (2).....	71
Gambar V- 11 Hasil Proses Pengujian <i>Walkthrough Session Hijacking</i> (1).....	72
Gambar V- 12 Hasil Proses Pengujian <i>Walkthrough Session Hijacking</i> (2).....	74
Gambar V- 13 Perhitungan <i>Vulnerability SQL Injection</i>	75
Gambar V- 14 Perhitungan <i>Vulnerability SQL Injection - MySQL</i>	76
Gambar V- 15 Perhitungan <i>Vulnerability Cross-Site Scripting (Reflected) File Upload</i>	77
Gambar V- 16 Perhitungan <i>Vulnerability Cross-Site Scripting (Reflected)</i>	78
Gambar V- 17 Perhitungan <i>Vulnerability Remote File Inclusion</i>	79
Gambar V- 18 Perhitungan <i>Vulnerability Cookie No HttpOnly Flag</i>	80
Gambar V- 19 Grafik Perbandingan.....	83