

DAFTAR GAMBAR

Gambar 2.1	Flowchart Penetration Testing.....	8
Gambar 2.2	Daftar Keamanan pada OWASP Top 10.....	9
Gambar 2.3	Sistem Operasi Kali Linux.....	13
Gambar 3.1	Alur Penyelesaian Penelitian	16
Gambar 3.2	Tahapan Penetration Testing dengan OWASP Top 10	18
Gambar 3.3	Flowchart proses injection.....	18
Gambar 3.4	Flowchart proses Broken Authentication	19
Gambar 3.5	Flowchart proses Sensitive Data Exposure	19
Gambar 3.6	Flowchart proses XML External Entities	19
Gambar 3.7	Flowchart proses Broken Access Control	20
Gambar 3.8	Flowchart proses Security Misconfiguration.....	20
Gambar 3.9	Flowchart proses Cross-Site Scripting (XSS)	21
Gambar 3.10	Flowchart proses Insecure Deserialization	21
Gambar 3.11	Flowchart proses Using Components with known Vulnerabilities	21
Gambar 3.12	Flowchart proses Insufficient Logging & Monitoring.....	22
Gambar 4.1	Hasil Scanning dengan Whois	24
Gambar 4.2	Hasil Vulnerability Scanning OWASP ZAP	26
Gambar 5.1	Penandaan Parameter Pengujian.....	30
Gambar 5.2	Hasil Pengujian menggunakan Payloads SQL (hasil respons 200)	32
Gambar 5.3	Halaman Login Website PPDB XYZ	33
Gambar 5.4	Serangan Brute Force dengan metode Cluster Bomb.....	34
Gambar 5.5	Konfigurasi Payload Sql.....	34
Gambar 5.6	Konfigurasi Payloads Sql kedua.....	35
Gambar 5.7	Hasil percobaan Brute Force halaman login.....	37
Gambar 5.8	Eksekusi perintah Dirsearch	38
Gambar 5.9	Request POST dengan Payloads XXE	39
Gambar 5.10	Hasil Payloads XXE	41
Gambar 5.11	Tools CSRF OWASP ZAP.....	42
Gambar 5.12	Hasil temuan dari Tools CSRF	42
Gambar 5.13	Eksekusi perintah Curl.....	44
Gambar 5.14	Halaman Formulir Pendaftaran Sekolah.....	46
Gambar 5.15	Hasil pengujian kerentanan XSS	46
Gambar 5.16	Pengujian dengan Java Deserialization Scanner.....	47
Gambar 5.17	Hasil Deserialization Scanning.....	48
Gambar 5.18	Request HTTP GET.....	51
Gambar 5.19	Respons dari Request HTTP.....	51
Gambar 5.20	Script untuk pengujian jQuery.....	52
Gambar 5.21	Pengujian dengan Intruder Burp Suite.....	53