

DAFTAR GAMBAR

Gambar II. 1 Gambar Tahapan PTES	8
Gambar III. 1 Model Konseptual Penelitian	15
Gambar III. 2 Sistematika Penelitian	17
Gambar IV. 1 <i>IP Address</i> subdomain	25
Gambar IV. 2 <i>Name Server</i> domain.....	25
Gambar IV. 3 hasil pencarian <i>Name Server</i> menggunakan subdomain.....	25
Gambar IV. 4 Hasil pencarian <i>Name Server</i> menggunakan domain	26
Gambar IV. 5 <i>Output Scanning Zenmap</i>	26
Gambar IV. 6 Skenario Pengujian Menggunakan OWASP ZAP	28
Gambar IV. 7 Langkah Pengujian XSS menggunakan XSSStrike	29
Gambar IV. 8 Langkah pengujian XSS menggunakan Burp Suite.....	31
Gambar V. 1 Hasil Pengujian Eksploitasi Menggunakan Tool XSSStrike.....	35
Gambar V. 2 Hasil Serangan <i>Payload</i> Pertama dari <i>tool</i> XSSStrike	36
Gambar V. 3 Hasil Serangan <i>Payload</i> Kedua Menggunakan XSSStrike	37
Gambar V. 4 Hasil Data <i>Request Payload</i> Pertama Menggunakan Burp Suite..	38
Gambar V. 5 Hasil <i>Response</i> Sebelum Dilakukan Injeksi <i>Payload</i> Pertama	39
Gambar V. 6 Hasil <i>Response Payload</i> Pertama Menggunakan Burp Suite.....	39
Gambar V. 7 Hasil Data <i>Request Payload</i> Kedua Menggunakan Burp Suite	40
Gambar V. 8 Hasil <i>Response</i> Sebelum Dilakukan Injeksi <i>Payload</i> Kedua	40
Gambar V. 9 Hasil <i>Response Payload</i> Kedua Menggunakan Burp Suite.....	41
Gambar V. 10 Hasil Serangan <i>Payload</i> pertama Menggunakan Burp Suite	42
Gambar V. 11 Hasil Serangan <i>Payload</i> kedua Menggunakan Burp Suite.....	42
Gambar V. 13 Mitigasi Penambahan Header CSP.....	45
Gambar V. 14 Mitigasi Menerapkan <code>htmlspecialshars()</code>	45
Gambar V. 15 <i>Certificate</i> Penerapan SSL	47
Gambar V. 16 Tampilan Sebelum Mitigasi	48
Gambar V. 17 Tampilan Setelah Mitigasi	49
Gambar V. 18 Hasil <i>Vulnerability Scan</i> Pasca Mitigasi	49