

DAFTAR GAMBAR

Gambar II.1 Logo Yayasan Dana Sosial al-Falah.....	17
Gambar II.2 Tampilan Website Xyz.id.....	18
Gambar II.3 Tampilan Login Website Xyz.id	18
Gambar II.4 <i>Penetration Lifecycle</i>	20
Gambar II.5 Tahapan ISSAF	21
Gambar II.6 Kali Linux.....	27
Gambar II.7 Virtual Box	28
Gambar II.8 NMAP	28
Gambar II.9 OWSP ZAP	29
Gambar II.10 Nessus.....	30
Gambar II.11 SQL Map	30
Gambar II.12 BurpSuite.....	31
Gambar III.1 Metodologi Penelitian.....	33
Gambar IV.1 hasil pemindaian Nikto	37
Gambar IV.2 hasil pemindaian whois 1	38
Gambar IV.3 hasil pemindaian whois 2	38
Gambar IV.4 hasil pemindaian nslookup.....	39
Gambar IV.5 Hasil Wappalyzer Website Xyz.id	39
Gambar IV.7 Hasil pemindaian nmap 1.....	41
Gambar IV.8 Hasil pemindaian nmap 2.....	42
Gambar IV.9 Hasil pemindaian menggunakan <i>traceroute</i>	43
Gambar IV.10 Hasil pemindaian nessus pertama	45
Gambar IV.11 Hasil pemindaian nessus kedua.....	46
Gambar IV.12 Hasil pemindaian nessus ketiga	46
Gambar IV.13 Hasil pemindaian nessus keempat.....	47
Gambar IV.14 Hasil pemindaian nessus kelima	47
Gambar IV.15 Hasil pemindaian menggunakan owasp zap	48
Gambar V.1 Hasil <i>Penetration Testing</i> menggunakan sql <i>Injection</i> pertama.....	51
Gambar V.2 Hasil <i>Penetration Testing</i> menggunakan sql <i>Injection</i> kedua	52
Gambar V.3 Hasil <i>Penetration Testing</i> menggunakan serangan XSS (<i>Cross-Site Scripting</i>).....	53

Gambar V.4 Membuat Worthlist untuk kombinasi <i>Username</i> dan password.....	55
Gambar V.5 Hasil <i>Gaining Access and Privilege Escalation</i> menggunakan <i>Burp Suite</i>	56
Gambar V.6 Hasil <i>Gaining Access and Privilege Escalation</i> menggunakan tools <i>Hydra</i>	57
Gambar V.7 Hasil <i>Gaining Access and Privilege Escalation</i> menggunakan <i>Metasploit</i> pertama.....	57
Gambar V.8 Hasil <i>Gaining Access and Privilege Escalation</i> menggunakan <i>Metasploit</i> kedua.....	57
Gambar V.9 Hasil <i>Gaining Access and Privilege Escalation</i> menggunakan <i>Metasploit</i> Port 22 dan 80	58
Gambar V.10 Hasil <i>Enumerating Further</i> menggunakan rekam data pada <i>Wireshark</i>	61
Gambar V.11 Hasil <i>Enumerating Further</i> menggunakan informasi lain sebagai perbandingan.....	62
Gambar V.12 Hasil <i>Enumerating Further</i> menggunakan <i>Cookie Manager</i> pertama	62
Gambar V.13 Hasil <i>Enumerating Further</i> menggunakan <i>Cookie Manager</i> kedua	63
Gambar V.14 Membersihkan Jejak Pengujian di <i>Metasploit</i>	78
Gambar V.15 Membersihkan Jejak Pengujian Di Terminal	81
Gambar V.16 Tampilan <i>file</i> 1 pengujian sebelum dihapus	82
Gambar V.17 Tampilan <i>file</i> 1 pengujian setelah dihapus	82
Gambar V.18 Tampilan seluruh <i>file</i> sampah pengujian di kali linux sebelum dihapus	82
Gambar V.19 Tampilan seluruh <i>file</i> sampah pengujian di kali linux setelah dihapus	83