

DAFTAR GAMBAR

Gambar II.1 Tiga Aspek Keamanan Sistem Informasi	46
Gambar II.2 Pendekatan & Metodologi ISSAF (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	50
Gambar II.3 Logo Kali Linux	55
Gambar II.4 Tampilan <i>Tools</i> OWASP ZAP	56
Gambar II.5 Tampilan <i>Tools</i> Nessus Vuulnerability Scanner	57
Gambar II.6 Tampilan <i>Tools</i> Nmap – Zenmap GUI.....	57
Gambar II.7 Tampilan <i>Tools</i> Nmap – Kali Linux.....	58
Gambar II.8 Tampilan <i>Tools</i> PuTTY	58
Gambar II.9 Tampilan <i>SSL Security Test</i> (Qualys <i>SSL Labs</i>).....	59
Gambar II.10 Tampilan <i>Tools WhoIS</i> Kali Linux.....	59
Gambar II.11 Tampilan <i>Tools SpiderFoot</i>	60
Gambar II.12 Tampilan <i>Tools BurpSuite</i>	60
Gambar II.13 Tampilan <i>Tools DirSearch</i>	61
Gambar II.14 Tampilan <i>Tools ParamSpider</i>	61
Gambar II.15 Tampilan <i>Tools DalFox</i>	61
Gambar II.16 Tampilan <i>Tools Hydra</i>	62
Gambar II.17 Tampilan <i>Tools WireShark</i>	62
Gambar II.18 Tampilan <i>Tools SQLMap</i>	63
Gambar II.19 Tampilan <i>Tools SlowHttpTest</i>	63
Gambar II.20 Tampilan <i>Tools SlowHttpTest</i>	64
Gambar II.21 Tampilan <i>Tools SlowHttpTest</i>	64
Gambar II.22 Tampilan <i>Tools SlowHttpTest</i>	65
Gambar II.23 Tampilan <i>Tools BleachBit</i>	65
Gambar II.24 Tampilan <i>Tools Tor Browser</i>	66
Gambar II.25 Tampilan <i>Tools ProxyChain (Dynamic)</i>	66
Gambar III.1 Alur Penelitian Berdasarkan <i>Framework</i> ISSAF (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	67
Gambar III.2 Alur Tahapan <i>Information Gathering</i>	70
Gambar III.3 Alur Tahapan <i>Network Mapping</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	71

Gambar III.4 Alur Tahapan <i>Vulnerabilities Identification</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005).....	71
Gambar III.5 Alur Tahapan <i>Penetration</i>	72
Gambar III.6 Alur Tahapan <i>Gaining Access and Privilege Escalation</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	73
Gambar III.7 Alur Tahapan <i>Enumerating Further</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005).....	73
Gambar III.8 Alur Tahapan <i>Maintaining Access</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	74
Gambar III.9 Alur Tahapan <i>Covering Tracks</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005)	74
Gambar V.1 Situs Utama Yayasan Dana Sosial Al Falah.....	84
Gambar V.2 Hasil Dari <i>Tools Wappalyzer</i>	84
Gambar V.3 Hasil <i>Scan Ping Test</i> (Terminal Kali Linux)	85
Gambar V.4 Hasil <i>Scan Ping Test</i> Menggunakan CMD (<i>Command Prompt Windows</i>).....	85
Gambar V.5 Hasil <i>Scan Nslookup (Domain)</i>	86
Gambar V.6 Hasil <i>Scan Nslookup Reverse DNS (IP Address)</i>	86
Gambar V.7 Hasil <i>Scan Nslookup Pencarian Data DNS</i>	86
Gambar V.8 Hasil <i>Scan Nslookup Pencarian Data SOA (Start of Authority)</i> ...	87
Gambar V.9 Hasil <i>Scan Nslookup Mapping Domain Address ke Daftar Server DNS</i>	87
Gambar V.10 Hasil <i>Scan Nslookup Data DNS</i>	87
Gambar V.11 Hasil <i>Scan Nslookup Mail Exchange (Mencari Data MX)</i>	88
Gambar V.12 Hasil <i>Scan Nslookup TXT (Mencari Data TXT)</i>	88
Gambar V.13 Hasil <i>Scanning WhoIS (Domain) Ke-1</i>	88
Gambar V.14 Hasil <i>Scanning WhoIS (Domain) Ke-2</i>	89
Gambar V.15 Hasil <i>Scanning WhoIS (Domain) Ke-3</i>	89
Gambar V.16 Hasil <i>Scanning WhoIS (IP Address) Ke-1</i>	90
Gambar V.17 Hasil <i>Scanning WhoIS (IP Address) Ke-2</i>	91
Gambar V.18 Hasil <i>Scanning WhoIS (IP Address) Ke-3</i>	91

Gambar V.19 Hasil <i>Scanning WhoIS (IP Address) Ke-4</i>	92
Gambar V.20 Hasil <i>Scanning WhoIS (IP Address) Ke-5</i>	92
Gambar V.21 Hasil <i>Scanning SpiderFoot Ke-1</i>	94
Gambar V.22 Hasil <i>Scanning SpiderFoot Ke-2</i>	94
Gambar V.23 Hasil <i>Scanning SpiderFoot (Affilliate Domain)</i>	95
Gambar V.24 Hasil <i>Scanning SpiderFoot (IP Address V4)</i>	95
Gambar V.25 Hasil <i>Scanning SpiderFoot (IP Address V6)</i>	96
Gambar V.26 Hasil <i>Scanning SpiderFoot (Country Name)</i>	96
Gambar V.27 Hasil <i>Scanning SpiderFoot (Domain Name)</i>	96
Gambar V.28 Hasil <i>Scanning SpiderFoot (Domain Name Parent)</i>	97
Gambar V.29 Hasil <i>Scanning SpiderFoot (Email Gateway (DNS MX Record))</i>	97
Gambar V.30 Hasil <i>Scanning SpiderFoot (Internet Name)</i>	97
Gambar V.31 Hasil <i>Scanning SpiderFoot (Open TCP Port)</i>	98
Gambar V.32 Hasil <i>Scanning SpiderFoot (Summary, Scan Status, Cerelations, Data Types)</i>	98
Gambar V.33 Hasil <i>Scanning SpiderFoot (Correlation)</i>	99
Gambar V.34 Tampilan <i>SpiderFoot New Scan (By Use Case All)</i>	99
Gambar V.35 <i>SpiderFoot Command Running</i>	100
Gambar V.36 Hasil <i>Regular Nmap Scan (Kali Linux)</i>	102
Gambar V.37 Hasil <i>Regular Nmap Scan (Windows)</i>	102
Gambar V.38 Hasil <i>Nmap Identify Live Hosts (Kali Linux)</i>	103
Gambar V.39 Hasil <i>Zenmap Intense Scans All TCP Port (Windows)</i>	103
Gambar V.40 Hasil <i>Nmap Regular TCP Port Scanning (Kali Linux)</i>	104
Gambar V.41 Hasil <i>Nmap Regular UDP Port Scanning (Kali Linux)</i>	105
Gambar V.42 Hasil <i>Nmap Service Version and OS Detection (Kali Linux)</i> ..	106
Gambar V.43 Hasil <i>SSL Security Test (ImmuniWeb)</i>	106
Gambar V.44 Hasil <i>SSL Security Test (SSL Labs)</i>	107
Gambar V.45 Tampilan Hasil <i>Scanning Nessus Basic Network Scan (1)</i>	109
Gambar V.46 Tampilan Hasil <i>Scanning Nessus Basic Network Scan (2)</i>	109
Gambar V.47 Hasil <i>Nessus Basic Network Scan (3)</i>	109

Gambar V.48 Hasil Nessus <i>Basic Network Scan Folder ISC Bind (Multiple Issues)</i>	110
Gambar V.49 Kerentanan DNS <i>Server Spoofed Request Amplification DDoS</i>	110
Gambar V.50 Kerentanan DNS <i>Server Recursice Query Cache Poisoning Weakness</i>	111
Gambar V.51 Hasil Nessus <i>Basic Network Scan Folder HTTP (Multiple Issue)</i>	111
Gambar V.52 Kerentanan HSTS <i>Missing From HTTPS Server (RFC 6797)</i> . 112	
Gambar V.53 Hasil Nessus <i>Basic Network Scan Folder DNS (Multiple Issue)</i>	112
Gambar V.54 Kerentanan DNS <i>Server Cache Snooping Remote Information Disclosure</i>	113
Gambar V.55 Tampilan Hasil <i>Scanning Nessus Web Application Tests (1)</i> ... 115	
Gambar V.56 Tampilan Hasil <i>Scanning Web Application Tests (2)</i>	115
Gambar V.57 Tampilan Kerentanan <i>Web Application Potentially Vulnerable to Clickjacking</i>	115
Gambar V.58 Hasil Nessus <i>Web Application Tests Folder HTTP (Multiple Issue)</i>	116
Gambar V.59 Tampilan Kerentanan HSTS <i>Missing From HTTPS Server (RFC 6797)</i>	116
Gambar V.60 Hasil Nessus <i>Web Application Tests Folder Web Server (Muliple Issue)</i>	117
Gambar V.61 Tampilan Kerentanan <i>Web Server Allows Password Auto-Completion</i>	117
Gambar V.62 Tampilan OWASP ZAP <i>Using Automated Scan Use Traditional and Ajax Spider</i>	119
Gambar V.63 Hasil <i>Scanning OWASP ZAP Automated Scan Use Traditional and Ajax Spider</i>	120
Gambar V.64 Tampilan Kerentanan <i>Hash Disclosure - Mac OSX salted SHA-1 (High)</i>	120

Gambar V.65 Tampilan Kerentanan <i>Absence of Anti-CSRF Tokens (Medium)</i>	121
Gambar V.66 Tampilan Kerentanan <i>Content Security Policy (CSP) Header Not Set (Medium)</i>	121
Gambar V.67 Tampilan Kerentanan <i>Cross-Domain Misconfiguration (Medium)</i>	121
Gambar V.68 Tampilan Kerentanan <i>Hidden File Found (Medium)</i>	122
Gambar V.69 Tampilan Kerentanan <i>Missing Anti-clickjacking Header (Medium)</i>	122
Gambar V.70 Tampilan Kerentanan <i>Vulnerable JS Library (Medium)</i>	123
Gambar V.71 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Beranda) .	127
Gambar V.72 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Laporan Kurban)	127
Gambar V.73 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Hitung Zakat)	128
Gambar V.74 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Layanan Donatur)	128
Gambar V.75 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (<i>Event</i> Donasi Ramadhan)	129
Gambar V.76 <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Program Donasi)	129
Gambar V.77 <i>SQLInjection</i> Pada (<i>Login Page</i>) Dengan <i>Risk Level 3 Ke-1</i> ...	130
Gambar V.78 <i>SQLInjection</i> Pada (<i>Login Page</i>) Dengan <i>Risk Level 3 Ke-2</i> ...	131
Gambar V.79 <i>SQLInjection</i> Pada (<i>Login Page</i>) Dengan <i>Risk Level 3 Ke-3</i> ...	131
Gambar V.80 <i>SQLInjection</i> Pada (<i>Login Page</i>) Dengan <i>Risk Level 3 Ke-4</i> ...	131
Gambar V.81 <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi.....	132
Gambar V.82 Hasil <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi (1)	133
Gambar V.83 Hasil <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi (2)	133
Gambar V.84 Tampilan <i>Installasi Golang-Go</i>	134
Gambar V.85 Tampilan <i>Installasi Tools Dalfox</i>	134
Gambar V.86 Tampilan <i>Change Directory</i> Untuk <i>Tools Dalfox</i>	135
Gambar V.87 Tampilan <i>Installasi Tools ParamSpider</i>	135

Gambar V.88 Tampilan <i>Scanning</i> URL Parameter <i>Website</i> YDSF.....	135
Gambar V.89 Tampilan <i>Result</i> atau <i>Output</i> dari <i>Tools</i> ParamSpider.....	136
Gambar V.90 Tampilan Hasil <i>Scanning Tools</i> Dalfox (14 URL Parameter)..	136
Gambar V.91 Melakukan Instalasi <i>Tools</i> Slowhttptest	137
Gambar V.92 Melakukan Serangan DDoS Menggunakan <i>Tools</i> Slowhttptest	137
Gambar V.93 Tampilan <i>Website</i> YDSF Sebelum Dilakukan Serangan DDoS	137
Gambar V.94 Tampilan <i>Website</i> YDSF Setelah Dilakukan Serangan DDoS.	138
Gambar V.95 Tampilan <i>Website</i> YDSF Setelah Proses Serangan DDoS Selesai Dilakukan	138
Gambar V.96 Tampilan Hasil Dari Serangan DDoS Menggunakan <i>Slowhttptest</i>	139
Gambar V.97 Tampilan Hasil <i>Regular</i> Nmap <i>Scan</i> (<i>Port</i> 21 FTP)	140
Gambar V.98 Mengakses <i>Port</i> FTP 21 menggunakan <i>Quick Access File Explorer</i>	141
Gambar V.99 Tampilan <i>Log On As</i> Saat Mengakses <i>Port</i> FTP 21 Menggunakan <i>Quick Access</i>	141
Gambar V.100 Tampilan <i>Tools</i> PuTTY <i>Configuration</i> Untuk Akses <i>Port</i> 22 <i>Service</i> SSH.....	141
Gambar V.101 Tampilan PuTTY Saat Mengakses <i>Port</i> 22 Dengan Layanan SSH	142
Gambar V.102 Tampilan IP <i>Subneting</i> Untuk Mencari IP <i>Network</i> dari IP <i>Website</i> YDSF.....	145
Gambar V.103 Tampilan Nmap Untuk Mencari IP Dari <i>Port</i> FTP (21) Yang Terbuka	145
Gambar V.104 Tampilan Nmap Untuk Mencari IP Dari <i>Port</i> SSH (22) Yang Terbuka	146
Gambar V.105 <i>Passwordlist</i> Yang Digunakan Untuk Melakukan <i>Bruteforce Attack</i>	147
Gambar V.106 <i>Username</i> list Yang Digunakan Untuk Melakukan <i>Bruteforce Attack</i>	147

Gambar V.107 <i>Hydra</i> Penyerangan SSH Login (Tidak Menggunakan <i>usernamelist.txt</i>)	148
Gambar V.108 <i>Hydra</i> Penyerangan SSH Login (Menggunakan <i>usernamelist.txt</i>)	149
Gambar V.109 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (1)	151
Gambar V.110 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (2)	151
Gambar V.111 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (3)	152
Gambar V.112 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (4)	152
Gambar V.113 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (5)	153
Gambar V.114 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (6)	153
Gambar V.115 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (7)	154
Gambar V.116 Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (1)	156
Gambar V.117 Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (2)	156
Gambar V.118 Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (3)	157
Gambar V.119 Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (3)	157
Gambar V.120 Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (4)	158
Gambar V.121 Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (5)	158
Gambar V.122 Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (6)	159

Gambar V.123 Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (1).....	160
Gambar V.124 Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (2).....	160
Gambar V.125 Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (3).....	160
Gambar V.126 Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (4).....	161
Gambar V.127 Tampilan <i>Tools</i> WireShark (Contoh Percobaan <i>Sniffing Traffic</i> Yang Berhasil)	162
Gambar V.128 Tampilan <i>Tools</i> WireShark (Contoh Percobaan <i>Sniffing Traffic</i> Yang Berhasil)	162
Gambar V.129 Tampilan <i>tools</i> Nmap Untuk Mencari <i>Open Port</i> FTP (21)...	165
Gambar V.130 Tampilan <i>tools</i> Nmap Untuk Mencari <i>Open Port</i> SSH (22) ..	165
Gambar V.131 Tampilan <i>Tools</i> Nmap SSH <i>Brute</i> Pada <i>Port</i> SSH (1)	166
Gambar V.132 Tampilan <i>Tools</i> Nmap SSH <i>Brute</i> Pada <i>Port</i> SSH (2)	167
Gambar V.133 Hydra Penyerangan <i>Port</i> SSH 22 (Tidak Menggunakan <i>usernamelist.txt</i>)	167
Gambar V.134 Hydra Penyerangan <i>Port</i> SSH 22 (Menggunakan <i>usernamelist.txt</i>)	168
Gambar V.135 Hydra Penyerangan <i>Port</i> FTP / <i>Port</i> 21	170
Gambar V.136 Hydra Penyerangan <i>Port</i> HTTP 80 (1).....	171
Gambar V.137 Hydra Penyerangan <i>Port</i> HTTP 80 (2).....	171
Gambar V.138 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (1)	172
Gambar V.139 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (2)	172
Gambar V.140 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (3)	173
Gambar V.141 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (4)	173
Gambar V.142 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (5)	174
Gambar V.143 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (6)	174

Gambar V.144 Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (7)	175
Gambar V.145 Tampilan <i>BurpSuite</i> ClickJacking (1)	175
Gambar V.146 Tampilan <i>BurpSuite</i> ClickJacking (2)	176
Gambar V.147 Tampilan <i>BurpSuite</i> ClickJacking (3)	176
Gambar V.148 Tampilan <i>BurpSuite</i> ClickJacking (4)	177
Gambar V.149 Tampilan <i>BurpSuite</i> ClickJacking (5)	177
Gambar V.150 Tampilan <i>BurpSuite</i> ClickJacking (6)	177
Gambar V.151 Tampilan <i>BurpSuite</i> ClickJacking (7)	178
Gambar V.152 Tampilan <i>BurpSuite</i> ClickJacking (8)	178
Gambar V.153 Tampilan <i>BurpSuite</i> ClickJacking (9)	179
Gambar V.154 Tampilan <i>BurpSuite</i> ClickJacking (9)	179
Gambar V.155 <i>Command</i> Untuk <i>Setting ProxyChains4 (Dynamic)</i>	183
Gambar V.156 Aktifkan <i>Dynamic Chain</i> dan Non Aktifkan <i>Strict Chain</i>	184
Gambar V.157 Ilustrasi Cara Kerja <i>Proxy Chain</i>	184
Gambar V.158 <i>Scanning WhoIs</i> Menggunakan <i>Dynamic ProxyChains</i>	185
Gambar V.159 Instalasi <i>Tor Browser</i>	186
Gambar V.160 Akses <i>Tor Browser</i> (CLI or GUI)	186
Gambar V.161 Tampilan <i>Tor Browser</i> (IP Address Otomatis Disamarkan)	186
Gambar V.162 Tampilan <i>Log File</i> Yang Ada Pada <i>File System</i>	187
Gambar V.163 Tampilan <i>Log File</i> Yang Ada Pada Direktori <i>File System</i> (CLI/Terminal)	187
Gambar V.164 Tampilan Isi Dari <i>Log File</i> <i>macchanger.log</i>	187
Gambar V.165 <i>Command</i> Untuk Menghapus <i>File Log</i>	188
Gambar V.166 Tampilan <i>Tools BleachBit</i>	188