

DAFTAR GAMBAR

Gambar I. 1 Grafik Jumlah Pengguna Internet di Indonesia.....	1
Gambar II. 1 Aspek Keamanan Sistem Informasi	14
Gambar II. 2 Perbedaan OWASP Top 10 versi 2013 dan 2017.....	15
Gambar II. 3 Metode <i>Penetration Testing</i>	24
Gambar II. 4 <i>Tools scanning OWASP ZAP</i>	27
Gambar II. 5 <i>Tools exploit Burpsuite</i>	28
Gambar II. 6 <i>Tools exploit Sqlmap</i>	28
Gambar III. 1 Diagram Prosedur Penelitian.....	32
Gambar IV. 1 <i>Alerts hasil scanning website A</i>	50
Gambar IV. 2 Hasil <i>scanning website A</i> dengan <i>dirsearch</i>	53
Gambar IV. 3 <i>Alerts hasil scanning website B</i>	54
Gambar IV. 4 Hasil <i>scanning website B</i> dengan <i>dirsearch</i>	56
Gambar IV. 5 <i>Alerts hasil scanning website C</i>	57
Gambar IV. 6 Hasil <i>scanning website C</i> dengan <i>dirsearch</i>	59
Gambar IV. 7 Parameter <i>code website A</i>	60
Gambar IV. 8 Pengiriman <i>payload SQL Injection</i> dengan <i>burpsuite</i>	61
Gambar IV. 9 <i>Syntax error</i> dengan <i>payload sql</i>	61
Gambar IV. 10 Pengujian injeksi pada <i>SQL Injection - MySQL</i>	62
Gambar IV. 11 Hasil temuan <i>database website A</i>	62
Gambar IV. 12 Temuan <i>email</i> dan <i>password</i> pada <i>database users A</i>	63
Gambar IV. 13 Temuan riwayat aktivitas penyerangan <i>website A</i>	63
Gambar IV. 14 Parameter <i>type website A</i>	64
Gambar IV. 15 Pengiriman <i>payload Oracle sql hostname</i>	64
Gambar IV. 16 Pengujian injeksi pada <i>SQL Injection - Oracle - Time Based</i> ...	65
Gambar IV. 17 Hasil injeksi pada <i>SQL Injection - Oracle - Time Based</i>	65
Gambar IV. 18 Parameter <i>page website A</i>	66
Gambar IV. 19 <i>Request payload</i> pada parameter <i>page</i>	66
Gambar IV. 20 <i>Response payload</i> pada parameter <i>page</i>	67
Gambar IV. 21 Hasil injeksi pada <i>SQL Injection - Oracle - Time Based</i>	67
Gambar IV. 22 Hasil injeksi <i>payload XSS</i>	68
Gambar IV. 23 <i>Request data POST</i> pada <i>form login</i>	69

Gambar IV. 24 Pengujian injeksi <i>SQL Injection</i> website B.....	69
Gambar IV. 25 Parameter <i>token</i> yang terindikasi kerentanan.....	70
Gambar IV. 26 Hasil injeksi <i>SQL Injection</i> website B.....	70
Gambar IV. 27 <i>Request</i> data <i>POST</i> pada website C.....	71
Gambar IV. 28 Hasil injeksi <i>SQL Injection</i> pada website C.....	72
Gambar IV. 29 Hasil <i>brute-force attack password</i> website A.....	73
Gambar IV. 30 Hasil <i>brute-force attack password</i> website B.....	74
Gambar IV. 31 Pengujian <i>brute-force attack password</i> website C.....	75
Gambar IV. 32 Hasil <i>brute-force attack password</i> website C.....	76
Gambar IV. 33 <i>Request</i> untuk mengubah <i>password</i> website C.....	77
Gambar IV. 34 <i>Response</i> mengubah <i>password</i> website C.....	77
Gambar IV. 35 <i>Request email forgot password</i> website C.....	78
Gambar IV. 36 <i>Request payload</i> untuk <i>forgot password</i>	79
Gambar IV. 37 <i>Response payload forgot password</i> pada <i>email</i>	79
Gambar IV. 38 Hasil pengujian <i>Timestamp Disclosure-Unix</i> website A.....	80
Gambar IV. 39 Pengujian <i>directory busting</i> website A.....	81
Gambar IV. 40 Hasil pengujian <i>directory busting</i> website A.....	82
Gambar IV. 41 File direktori <i>backend</i> website A.....	82
Gambar IV. 42 File direktori <i>downloads</i> website A.....	83
Gambar IV. 43 File direktori <i>images</i> website A.....	83
Gambar IV. 44 File direktori <i>cPanel</i> website A.....	84
Gambar IV. 45 Hasil pengujian <i>Private IP Disclosure</i>	85
Gambar IV. 46 Hasil pengujian <i>Timestamp Disclosure-Unix</i> website B.....	85
Gambar IV. 47 Hasil pengujian <i>sensitive information in URL</i> website B.....	86
Gambar IV. 48 Pengujian <i>directory busting</i> website B.....	87
Gambar IV. 49 Hasil pengujian <i>directory busting</i> website B.....	87
Gambar IV. 50 Hasil pengujian <i>Big Redirect Detected</i> website B.....	88
Gambar IV. 51 Pengujian <i>directory busting</i> website C.....	89
Gambar IV. 52 Pengujian <i>directory busting</i> website C.....	90
Gambar IV. 53 Hasil pengujian <i>payload XML</i> website A.....	91
Gambar IV. 54 Hasil pengujian <i>payload XML</i> website A dengan <i>curl</i>	92
Gambar IV. 55 Hasil pengujian <i>payload XML</i> website A dengan <i>XXEinjector</i>	92

Gambar IV. 56 <i>Request endpoint login validasi website B</i>	93
Gambar IV. 57 Hasil pengujian <i>payload XML website B</i>	94
Gambar IV. 58 <i>Request endpoint login validasi website C</i>	95
Gambar IV. 59 Hasil pengujian <i>payload XML website C</i>	95
Gambar IV. 60 <i>Request data form website A</i>	97
Gambar IV. 61 <i>Response data form website A</i>	97
Gambar IV. 62 Pengujian dengan <i>generate Anti-CSRF test Form</i>	98
Gambar IV. 63 Hasil pengujian <i>Cookie without Same Site Attribute website A</i>	99
Gambar IV. 64 Hasil pengujian <i>Cookie without Same Site Attribute website B</i>	100
Gambar IV. 65 <i>Request email dan password website B</i>	100
Gambar IV. 66 <i>Response email dan password website B</i>	101
Gambar IV. 67 Perubahan <i>status code</i> pada <i>request website B</i>	101
Gambar IV. 68 Hasil pengujian <i>Login bypass website B</i>	102
Gambar IV. 69 <i>Response form Anti-CSRF website C</i>	102
Gambar IV. 70 <i>Payload CSRF dengan script HTML</i>	103
Gambar IV. 71 Hasil pengujian <i>script payload CSRF attack website C</i>	103
Gambar IV. 72 Berhasil masuk ke <i>dashboard</i> pengguna	104
Gambar IV. 73 Pengujian <i>forced browsing endpoint admin</i>	105
Gambar IV. 74 Hasil pengujian <i>forced browsing endpoint admin</i>	105
Gambar IV. 75 Hasil pengujian <i>CSP dengan curl</i>	106
Gambar IV. 76 Hasil pengujian <i>CSP dengan script</i>	107
Gambar IV. 77 Hasil pengujian <i>Hidden file found website A</i>	107
Gambar IV. 78 Hasil pengujian <i>Application error disclosure</i> dan <i>Directory</i> <i>browsing</i>	108
Gambar IV. 79 Hasil pengujian <i>Missing Anti-clickjacking header</i>	109
Gambar IV. 80 Hasil pengujian <i>Header Strict-Transport-Security</i>	110
Gambar IV. 81 Hasil pengujian <i>Cookie HttpOnly flag</i> dan <i>Cookie Secure Flag</i>	111
Gambar IV. 82 Hasil pengujian <i>X-Content-Type-Options</i>	111
Gambar IV. 83 Hasil pengujian <i>CSP dengan curl</i>	112
Gambar IV. 84 Hasil pengujian <i>CSP dengan script</i>	113

Gambar IV. 85 Hasil pengujian <i>Missing Anti-clickjacking header</i>	113
Gambar IV. 86 Hasil pengujian <i>Server leaks version</i> dan <i>X-Content-Type-Option</i>	114
Gambar IV. 87 Hasil pengujian <i>Cookie no HttpOnly flag</i>	115
Gambar IV. 88 Laravel Debug Mode RCE website B.....	116
Gambar IV. 89 Hasil pengujian <i>Laravel debug mode</i> dengan <i>CVE-2021-3129</i>	117
Gambar IV. 90 Hasil pengujian <i>Laravel debug mode</i> dengan teknik <i>reverse shell</i> <i>metasploit</i>	118
Gambar IV. 91 Hasil pengujian <i>CSP</i> dengan <i>curl</i>	119
Gambar IV. 92 Hasil pengujian <i>CSP</i> dengan <i>script</i>	119
Gambar IV. 93 Hasil pengujian <i>.htaccess information leak</i>	120
Gambar IV. 94 Hasil pengujian <i>Missing Anti-clickjacking header</i>	121
Gambar IV. 95 Hasil pengujian <i>Server leaks version</i> dan <i>Strict-Transport-Security</i>	121
Gambar IV. 96 Hasil pengujian <i>Cookie no HttpOnly</i> dan <i>Cookie no Secure</i> ...	122
Gambar IV. 97 Hasil <i>payload XSS</i> website A.....	124
Gambar IV. 98 Hasil pengujian <i>Cross-site scripting (reflected)</i>	124
Gambar IV. 99 <i>Request</i> pengujian <i>Cross-site scripting</i>	125
Gambar IV. 100 Hasil pengujian <i>Cross-site scripting (XSS)</i>	126
Gambar IV. 101 Penyuntikan <i>payload XSS</i> pada <i>form</i> usaha mikro.....	127
Gambar IV. 102 Pengajuan permohonan dengan <i>payload XSS</i>	127
Gambar IV. 103 Hasil pengujian <i>Blind XSS</i> website C.....	128
Gambar IV. 104 Pengujian <i>payload java deserialization</i> website A	129
Gambar IV. 105 Hasil pengujian <i>payload java deserialization</i> website A.....	130
Gambar IV. 106 Pengujian <i>payload java deserialization</i> website B	131
Gambar IV. 107 Hasil pengujian <i>payload java deserialization</i> website B	132
Gambar IV. 108 Pengujian <i>payload java deserialization</i> website C	133
Gambar IV. 109 Hasil pengujian <i>payload java deserialization</i> website C	133
Gambar IV. 110 Pemindaian <i>JS Library</i> website A.....	135
Gambar IV. 111 Hasil pengujian <i>payload prototype pollution</i> website A.....	135
Gambar IV. 112 Pemindaian <i>JS Library</i> website B	136

Gambar IV. 113 Hasil pengujian <i>payload prototype pollution website B</i>	137
Gambar IV. 114 Pemindaian <i>JS Library website C</i>	138
Gambar IV. 115 Hasil pengujian <i>payload prototype pollution website C</i>	138
Gambar IV. 116 Hasil pengujian <i>insufficient logging & monitoring website A</i>	140
Gambar IV. 117 Hasil pengujian <i>insufficient logging & monitoring website C</i>	141
Gambar IV. 118 Hasil <i>risk rating website A</i>	241
Gambar IV. 119 Hasil <i>risk rating website B</i>	243
Gambar IV. 120 Hasil <i>risk rating website C</i>	245
Gambar IV. 121 <i>Risk rating kerentanan keseluruhan website</i>	247