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

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

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

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

Gambar IV. 113 Hasil pengujian *payload prototype pollution website* B 137
Gambar IV. 114 Pemindaian *JS Library website* C 138
Gambar IV. 115 Hasil pengujian *payload prototype pollution website* C 138
Gambar IV. 116 Hasil pengujian *insufficient logging & monitoring website* A 140
Gambar IV. 117 Hasil pengujian *insufficient logging & monitoring website* C141
Gambar IV. 118 Hasil *risk rating website* A..... 241
Gambar IV. 119 Hasil *risk rating website* B..... 243
Gambar IV. 120 Hasil *risk rating website* C..... 245
Gambar IV. 121 *Risk rating* kerentanan keseluruhan *website* 247