

DAFTAR ISI

LEMBAR PENGESAHAN	iii
PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
BAB 1 PENDAHULUAN	16
1.1 Latar Belakang	16
1.2 Rumusan Masalah	18
1.3 Tujuan dan Manfaat	18
1.4 Batasan Masalah	18
BAB 2 TINJAUAN PUSTAKA	19
2.1 Penelitian Terdahulu	19
2.2 Dasar Teori	22
2.2.1 OWASP (Open Worldwide Application Security Project)	22
2.2.2 OWASP <i>Web Security Testing Guide</i> (WSTG)	22
2.2.3 <i>OWASP ZAP</i>	23
2.2.4 <i>Burp Suite</i>	24
2.2.5 <i>WPScan</i>	24
2.2.6 Uji Penetrasi Keamanan	25
2.2.7 <i>Black-Box Testing</i>	25
2.2.8 <i>SQL Injection</i>	26
2.2.9 <i>CSRF (Cross Site Request Forgery)</i>	26
2.2.10 <i>Brute Force Attack</i>	27
2.2.11 <i>Fuzzing</i>	29
2.2.12 <i>Cross Site Scripting</i>	29
2.2.13 <i>Server Side Request Forgery</i>	31
2.2.14 <i>HTTP Parameter Pollution</i>	31
BAB 3 METODOLOGI	32
3.1 Analisis <i>Website</i>	33
3.2 Penentuan Skenario Pengujian	34

3.2.1	Kategori <i>Authentication Testing</i> (WSTG-ATHN).....	34
3.2.2	Kategori <i>Input Validation Testing</i> (WSTG-INPV).....	35
3.3	<i>Vulnerability Scan</i>	36
3.4	Pengujian atau <i>Penetration Testing</i>	36
3.4.1	Detail Skenario Pengujian Kategori <i>Authentication Testing</i>	37
3.4.2	Detail Skenario Pengujian Kategori <i>Input Validation Testing</i>	45
3.5	Analisis Tingkat Risiko	61
3.5.1	Metode Memperkirakan <i>Likelihood</i>	61
3.5.2	Metode Memperkirakan <i>Impact</i>	63
3.5.3	Perhitungan Tingkat Risiko.....	65
3.6	Pembuatan Laporan Hasil Pengujian.....	66
3.6.1	<i>Introduction Report</i>	66
3.6.2	<i>Executive Summary Report</i>	66
3.6.3	<i>Findings Report</i>	67
3.6.4	<i>Appendices</i>	68
BAB 4	HASIL DAN PEMBAHASAN.....	69
4.1	Hasil Analisis <i>Website</i>	69
4.1.1	Proses <i>Information Gathering</i>	69
4.1.2	Proses Analisis <i>website</i>	72
4.2	Pembagian Skenario Pengujian	73
4.2.1	Skenario Pengujian untuk <i>Website A</i>	73
4.2.2	Skenario Pengujian untuk <i>Website B</i>	74
4.2.3	Skenario Pengujian untuk <i>Website C</i>	75
4.3	Hasil <i>Vulnerability Scan</i>	76
4.3.1	Hasil <i>Vulnerability Scan Website A</i>	76
4.3.2	Hasil <i>Vulnerability Scan Website B</i>	77
4.3.3	Hasil <i>Vulnerability Scan Website C</i>	78
4.4	Hasil <i>Penetration Testing</i>	78
4.4.1	Hasil <i>Penetration Testing Website A</i>	78
4.4.2	Hasil <i>Penetration Testing Website B</i>	95
4.4.3	Hasil <i>Penetration Testing Website C</i>	107
4.5	Analisis Tingkat Risiko	110
4.5.1	Perhitungan Tingkat Risiko.....	111
4.6	Laporan Pengujian.....	126

4.6.1	<i>Executive Summary</i>	126
4.6.2	<i>Findings Summary</i>	127
4.6.3	Remediation Summary.....	127
BAB 5	KESIMPULAN DAN SARAN.....	129
5.1	Kesimpulan.....	129
5.2	Saran.....	130
	DAFTAR PUSTAKA	131
	LAMPIRAN.....	134
	Lampiran 1. WSTG Checklist.....	134
	Lampiran 2. Payload XSS.....	137
	Lampiran 4. Payload <i>password</i> dan <i>username</i>	139
	Lampiran 5. Payload command injection	141
	Lampiran 6. Payload format string	144
	BIODATA PENULIS	146

DAFTAR GAMBAR

Gambar 2.1 Contoh tampilan aplikasi OWASP ZAP	23
Gambar 2.2 Gambaran cara kerja ZAP	23
Gambar 2.3 Tampilan burp suite	24
Gambar 2.4 Contoh tampilan <i>tool WPScan</i>	24
Gambar 2.5 Ilustrasi <i>Session Riding</i>	27
Gambar 3.1 Alur Penelitian	32
Gambar 4.1 Proses <i>scanning</i> dengan <i>wpscan</i>	76
Gambar 4.2 <i>Alert</i> hasil <i>scanning</i> dengan OWASP ZAP	77
Gambar 4.3 <i>Vulnerability alert</i> hasil <i>scan website B</i>	78
Gambar 4.4 <i>Vulnerability alert</i> hasil <i>scan website C</i>	78
Gambar 4.5 Hasil <i>scan wpscan</i> menemukan plugin <i>change wp-admin</i>	80
Gambar 4.6 Halaman <i>login</i> rahasia berhasil ditemukan	80
Gambar 4.7 Hasil pengujian <i>brute force</i> menggunakan <i>wpscan</i>	81
Gambar 4.8 Bukti fitur <i>reset password website A</i> tidak berfungsi	82
Gambar 4.9 Bukti <i>Service XMLRPC</i> yang masih aktif	83
Gambar 4.10 Hasil pengujian <i>brute force</i> pada <i>xmlrpc</i>	83
Gambar 4.11 Hasil <i>fuzzer</i> menggunakan OWASP ZAP	84
Gambar 4.12 Bukti inspeksi elemen filter <i>script</i>	84
Gambar 4.13 Hasil <i>scan wpscan</i> menemukan kerentanan pada <i>plugin</i>	85
Gambar 4.14 <i>Script payload</i> yang diinjeksikan kedalam komentar <i>post</i>	85
Gambar 4.15 Inspeksi elemen komentar <i>post</i> yang diinputkan <i>payload</i>	86
Gambar 4.16 Pengujian parameter untuk mendeteksi celah HPP	86
Gambar 4.17 Injeksi parameter untuk mendeteksi celah HPP	87
Gambar 4.18 Versi <i>plugin</i> dan celah keamanan yang dideteksi oleh <i>wpscan</i>	87
Gambar 4.19 Hasil proses <i>sql injection</i> menggunakan <i>sqlmap</i>	88
Gambar 4.20 <i>Request body</i> untuk <i>xmlrpc</i>	89
Gambar 4.21 Hasil injeksi <i>payload</i> dengan <i>fuzzer OWASP ZAP</i>	89
Gambar 4.22 Hasil <i>fuzzer payload SSI injection</i>	90
Gambar 4.23 Contoh request <i>header</i> untuk <i>SSI injection</i>	90
Gambar 4.24 Hasil <i>fuzzer payload format string injection</i>	91
Gambar 4.25 Request dan Respon dari <i>website</i> saat pengujian HTTP Splitting and Smuggling	92
Gambar 4.26 Proses injeksi host dengan <i>custom url</i>	93
Gambar 4.27 Hasil <i>redirect host header</i>	93
Gambar 4.28 Hasil proses <i>scanning</i> dengan <i>tplmap</i>	94
Gambar 4.29 Proses injeksi <i>request header</i>	94
Gambar 4.30 <i>interactch-client</i> untuk menangkap respon SSRF	95
Gambar 4.31 Proses injeksi <i>payload</i> dengan <i>fuzer</i> pada OWASP ZAP	97
Gambar 4.32 Respon <i>website</i> ketika pengujian <i>SQL injection</i>	98
Gambar 4.33 <i>User adminadmin</i> yang didapat setelah <i>bypass login</i>	98
Gambar 4.34 Hasil <i>scan paramspider</i> untuk <i>website B</i>	99
Gambar 4.35 Hasil pengujian WSTG-INPV-01 dengan <i>fuzzer</i> pada <i>website B</i>	99
Gambar 4.36 Bukti <i>payload</i> berhasil disimpan dan dijalankan di dashboard	100

Gambar 4.37 Proses edit <i>request body</i> untuk uji HPP pada website B.....	101
Gambar 4.38 Hasil scan <i>sql injection</i> melalui sqlmap pada website B	102
Gambar 4.39 Hasil <i>enum privilege dmbs</i> yang berhasil didapatkan.....	102
Gambar 4.40 <i>file</i> injeksi yang akan diupload ke website B.....	103
Gambar 4.41 Pengujian <i>command injection</i> dengan postman	103
Gambar 4.42 <i>tool interactsh</i> yang digunakan untuk menangkap respon ping.....	104
Gambar 4.43 payload yang digunakan untuk pengujian WSTG-INPV-14	104
Gambar 4.44 Contoh perubahan konten menggunakan XSS	105
Gambar 4.45 Proses scanning <i>tplmap</i> untuk <i>website B</i>	106
Gambar 4.46 <i>interactsh-client</i> untuk menangkap respon SSRF pada <i>website B</i>	107
Gambar 4.47 Proses menghilangkan parameter <i>captcha</i>	108

DAFTAR TABEL

Tabel 2.1 Daftar Penelitian Sebelumnya	19
Tabel 3.1 Detail Proses <i>information gathering</i>	33
Tabel 3.2 Daftar Skenario Pengujian untuk Kategori <i>Authentication Testing</i>	34
Tabel 3.3 Daftar Skenario Pengujian untuk Kategori <i>Input Validation Testing</i>	35
Tabel 3.4 Detail skenario pengujian WSTG-ATHN-01	37
Tabel 3.5 Detail skenario pengujian WSTG-ATHN-02	38
Tabel 3.6 Detail skenario pengujian WSTG-ATHN-03	39
Tabel 3.7 Detail skenario pengujian WSTG-ATHN-04	40
Tabel 3.8 Detail skenario pengujian WSTG-ATHN-05	41
Tabel 3.9 Detail skenario pengujian WSTG-ATHN-06	42
Tabel 3.10 Detail skenario pengujian WSTG-ATHN-07	42
Tabel 3.11 Detail skenario pengujian WSTG-ATHN-08	43
Tabel 3.12 Detail skenario pengujian WSTG-ATHN-09	44
Tabel 3.13 Detail skenario pengujian WSTG-ATHN-10	44
Tabel 3.14 Detail skenario pengujian WSTG-INPV-01	45
Tabel 3.15 Detail skenario pengujian WSTG-INPV-02	46
Tabel 3.16 Detail skenario pengujian WSTG-INPV-04	47
Tabel 3.17 Detail skenario pengujian WSTG-INPV-05	48
Tabel 3.18 Detail skenario pengujian WSTG-INPV-06	49
Tabel 3.19 Detail skenario pengujian WSTG-INPV-07	49
Tabel 3.20 Detail skenario pengujian WSTG-INPV-08	50
Tabel 3.21 Detail skenario pengujian WSTG-INPV-09	51
Tabel 3.22 Detail skenario pengujian WSTG-INPV-10	51
Tabel 3.23 Detail skenario pengujian WSTG-INPV-11	52
Tabel 3.24 Detail skenario pengujian WSTG-INPV-12	53
Tabel 3.25 Detail skenario pengujian WSTG-INPV-13	54
Tabel 3.26 Detail skenario pengujian WSTG-INPV-14	55
Tabel 3.27 Detail skenario pengujian WSTG-INPV-15	56
Tabel 3.28 Detail skenario pengujian WSTG-INPV-16	57
Tabel 3.29 Detail skenario pengujian WSTG-INPV-17	58
Tabel 3.30 Detail skenario pengujian WSTG-INPV-18	59
Tabel 3.31 Detail skenario pengujian WSTG-INPV-19	60
Tabel 3.32 Daftar nilai dari <i>Threat Agent Factors</i>	62
Tabel 3.33 Daftar nilai dari <i>Vulnerability Factors</i>	63
Tabel 3.34 Daftar nilai dari <i>Technical Impact Factors</i>	64
Tabel 3.35 Daftar nilai dari <i>Business Impact Factors</i>	65
Tabel 3.36 Kategori <i>likelihood</i> dan <i>impact</i>	65
Tabel 3.37 Klasifikasi tingkat risiko secara keseluruhan.....	66
Tabel 4.1 Hasil scan menggunakan <i>tools Wappalyzer</i>	69
Tabel 4.2 Hasil proses <i>informasi gathering</i>	70
Tabel 4.3 Daftar skenario pengujian untuk <i>website A</i>	74
Tabel 4.4 Daftar skenario pengujian untuk <i>website B</i>	75
Tabel 4.5 Daftar skenario pengujian untuk <i>website C</i>	76

Tabel 4.6 Hasil pengujian pada <i>website A</i>	79
Tabel 4.7 Hasil pengujian pada <i>website B</i>	95
Tabel 4.8 Hasil pengujian <i>website C</i>	107
Tabel 4.9 Keterangan kode <i>Reference ID</i>	110
Tabel 4.10 Daftar temuan kerentanan dan tingkat risiko	110
Tabel 4.11 Perhitungan nilai <i>likelihood</i> PT-01	111
Tabel 4.12 Perhitungan nilai <i>impact</i> PT-01	112
Tabel 4.13 Perhitungan nilai <i>likelihood</i> PT-02	113
Tabel 4.14 Perhitungan nilai <i>impact</i> PT-02	113
Tabel 4.15 perhitungan nilai <i>likelihood</i> PT-03	114
Tabel 4.16 Perhitungan nilai <i>impact</i> PT-03	115
Tabel 4.17 Perhitungan nilai <i>likelihood</i> PT-04	116
Tabel 4.18 Perhitungan nilai <i>impact</i> PT-04	117
Tabel 4.19 Perhitungan nilai <i>likelihood</i> AK-01	118
Tabel 4.20 Perhitungan nilai <i>impact</i> AK-01	118
Tabel 4.21 Perhitungan nilai <i>likelihood</i> AK-02	119
Tabel 4.22 perhitungan nilai <i>impact</i> AK-02	120
Tabel 4.23 Perhitungan nilai <i>likelihood</i> AK-04	121
Tabel 4.24 Perhitungan nilai <i>impact</i> AK-04	122
Tabel 4.25 Perhitungan nilai <i>likelihood</i> AK-05	123
Tabel 4.26 Perhitungan nilai <i>impact</i> AK-05	124
Tabel 4.27 Perhitungan nilai <i>likelihood</i> SP-01	125
Tabel 4.28 Perhitungan nilai <i>impact</i> SP-01	125
Tabel 4.29 Jumlah daftar temuan berdasarkan tingkat risiko	126
Tabel 4.30 Daftar kerentanan beserta tingkat risiko	127
Tabel 4.31 Daftar rekomendasi perbaikan	127