

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR.....	i
PENGESAHAN PENGUJI.....	ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
HALAMAN PERSEMBAHAN DAN MOTTO.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
LAMPIRAN.....	xv
BAB I PENDAHULUAN	I-1
1.1 Latar Belakang.....	I-1
1.2 Rumusan Masalah	I-6
1.3 Tujuan Penelitian.....	I-6
1.4 Manfaat Penelitian.....	I-7
1.5 Batasan Masalah.....	I-7
BAB II TINJAUAN PUSTAKA	II-1
2.1 Landasan Teori	II-1
2.1.1 Keamanan <i>Website</i>	II-1
2.1.2 Definisi <i>Website</i>	II-1
2.1.3 <i>Vulnerability Assessment</i>	II-2
2.1.4 <i>OWASP TOP 10</i>	II-3

2.1.5	<i>OWASP ZAP 2.15.0</i>	II-4
2.1.6	<i>Web Application Firewall</i>	II-6
2.1.7	<i>ModSecurity</i>	II-7
2.1.8	<i>Web Host Manager</i>	II-8
2.1.9	<i>Penetration Testing (Uji Penetrasi)</i>	II-10
2.2	Penelitian Terkait.....	II-17
2.3	Matriks Penelitian.....	II-21
BAB III METODOLOGI PENELITIAN.....		III-1
3.1	Ruang Lingkup Penelitian	III-1
3.2	Tahapan Penelitian.....	III-1
3.2.1	<i>Studi Literatur</i>	III-2
3.2.2	<i>Session Management Testing</i>	III-3
3.2.3	Pengujian Menggunakan <i>OWASP ZAP</i>	III-3
3.2.4	Persiapan Pengujian <i>Website</i> dan Pemasangan <i>WAF</i> Menggunakan <i>ModSecurity</i>	III-3
3.2.5	Implementasi <i>OWASP CRS</i> pada <i>Web Sakattaku.com</i>	III-4
3.2.6	Pengujian <i>VA</i> Setelah Pemasangan <i>WAF</i>	III-5
3.2.7	Analisis Perbandingan <i>VA</i> Sebelum dan Setelah <i>WAF</i>	III-5
3.2.8	Pelaporan.....	III-6
3.1	Tahapan Pengujian.....	III-6
3.2	Topologi Pengujian.....	III-9
3.3	Metode Pengujian.....	III-12
BAB IV HASIL DAN PEMBAHASAN.....		IV-1
4.1	<i>Session Management Testing</i>	IV-1
4.1.1	Input <i>URL Website</i>	IV-1

4.1.2 Scanning <i>Website</i>	IV-2
4.1.3 Hasil Ancaman (<i>Alerts</i>).....	IV-2
4.2 Pengujian Menggunakan <i>OWASP ZAP</i>	IV-3
4.2.1 <i>Summary Alerts</i> sebelum <i>WAF</i>	IV-3
4.2.2 <i>Alerts</i>	IV-4
4.2.3 <i>Alert Detail</i>	IV-5
4.2.4 <i>Cloud Metadata Potentially Exposed</i>	IV-10
4.2.5 <i>SQL Injection - Oracle - Time Based</i>	IV-11
4.2.6 <i>SQL Injection - SQLite</i>	IV-12
4.2.7 <i>Cross-Site Scripting (XSS)</i>	IV-14
4.3 Persiapan pengujian <i>Website</i> dan Pemasangan <i>WAF</i> menggunakan <i>ModSecurity</i>	IV-15
4.3.1 Menyiapkan infrastruktur untuk virtualisasi <i>Web</i> sakattaku.com	IV-15
4.3.2 Pemasangan <i>Web Host Manager (WHM)</i> dan <i>cPanel</i> pada infrastruktur <i>Web server</i>	IV-17
4.4 Implementasi <i>OWASP Core Rule Set</i> pada <i>Web</i> Sakattaku	IV-18
4.5 Pengujian <i>VA</i> setelah Pemasangan <i>WAF</i>	IV-21
4.5.1 <i>Summary Alert</i> setelah <i>WAF</i>	IV-21
4.5.2 Penambahan <i>rules</i> pada <i>ModSecurity</i> untuk mengatasi kerentana yang masih ada setelah <i>CRS</i> diimplementasikan.....	IV-25
4.6 Analisis Perbandingan <i>VA</i> sebelum dan sesudah <i>WAF</i>	IV-30
BAB V KESIMPULAN DAN SARAN.....	V-1
5.1 Kesimpulan.....	V-1
5.2 Saran.....	V-3
DAFTAR PUSTAKA	
LAMPIRAN.....	

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait (<i>State of the art</i>)	II-17
Tabel 2.2 Matriks Penelitian	II-21
Tabel 3. 1 Tahapan pengujian <i>VA</i> tanpa <i>WAF</i> dan dengan <i>WAF</i>	III-12
Tabel 3. 2 Perbedaan <i>VA</i> dengan <i>WAF</i> dan tanpa <i>WAF</i>	III-13
Tabel 3. 3 Cakupan Perbandingan <i>VA</i> dengan <i>WAF</i> dan tanpa <i>WAF</i>	III-14
Tabel 4. 1 <i>Summary Alert</i> sebelum <i>WAF</i>	IV-3
Tabel 4. 2 <i>Alerts</i> sebelum <i>WAF</i>	IV-4
Tabel 4. 3 <i>Alert</i> Detail	IV-6
Tabel 4. 4 Spesifikasi <i>Software</i> Sistem	IV-16
Tabel 4. 5 <i>Rules WAF</i> berdasarkan <i>OWASP Top 10</i>	IV-18
Tabel 4. 6 <i>Summary alert</i> setelah <i>WAF</i>	IV-22
Tabel 4. 7 <i>Alert</i> setelah <i>WAF</i>	IV-22
Tabel 4. 8 <i>Alert</i> detail setelah <i>WAF</i>	IV-23
Tabel 4. 9 <i>Rules</i> untuk mengatasi <i>CSP Wildcard Directive</i>	IV-26
Tabel 4. 10 Hasil akhir <i>alert</i>	IV-30
Tabel 4. 11 Perbandingan hasil <i>VA</i> sebelum dan sesudah <i>WAF</i>	IV-32
Tabel 4. 12 Rincian URL yang rentan oleh <i>SQL Injection - Oracle</i>	IV-33
Tabel 4. 13 Rincian URL yang rentan oleh <i>SQL Injection – SQLite</i>	IV-34
Tabel 4. 14 Rincian URL yang rentan oleh <i>XSS</i>	IV-44

DAFTAR GAMBAR

Gambar 2. 1 Topologi <i>Vulnerability Assessment</i>	II-2
Gambar 2. 2 Update data <i>OWASP Top 10</i> dari tahun 2017-2021.....	II-3
Gambar 2. 3 Topologi <i>Web Application Firewall</i> (Yanti & et al., 2015).....	II-6
Gambar 2. 4 Cara Kerja Serangan <i>XSS</i> (Putra et al., 2021)	II-11
Gambar 2. 5 Cara Kerja <i>SQL injection</i> (Aziz, 2022)	II-13
Gambar 2. 6 Gambaran Umum <i>CSRF</i> (Deepika, 2024).....	II-16
Gambar 3. 1 Tempat Studi Kasus Penelitian.....	III-1
Gambar 3. 2 Alur Penelitian.....	III-2
Gambar 3. 3 <i>ModSecurity</i> pada <i>WHM</i>	III-4
Gambar 3. 4 Flowchart pengujian <i>VA</i> sebelum <i>WAF</i>	III-7
Gambar 3. 5 Flowchart pengujian <i>VA</i> setelah <i>WAF</i>	III-8
Gambar 3. 6 Topologi Pengujian <i>VA</i> sebelum <i>WAF</i> diimplementasikan	III-9
Gambar 3. 7 Topologi Pengujian <i>VA</i> setelah <i>WAF</i> diimplementasikan	III-11
Gambar 4. 1 Cara <i>Scanning OWASP ZAP</i>	IV-1
Gambar 4. 2 <i>Scanning OWASP ZAP</i>	IV-2
Gambar 4. 3 Hasil <i>Scanning OWASP ZAP</i>	IV-3
Gambar 4. 4 <i>URL</i> Situs web yang terdeteksi <i>Cloud MPE</i>	IV-11
Gambar 4. 5 Deskripsi Kerentanan <i>Cloud Metadata Potentially Exposed</i> yang terdeteksi pada <i>OWASP ZAP</i>	IV-11
Gambar 4. 6 <i>URL</i> Situs Web yang rentan serangan <i>SQL Injection</i>	IV-12
Gambar 4. 7 Hasil Pengujian <i>SQL Injection</i>	IV-12
Gambar 4. 8 <i>URL</i> Situs web yang rentan serangan <i>SQL Injection - SQLite</i>	IV-13
Gambar 4. 9 Hasil Pengujian <i>SQL Injection – SQLite</i>	IV-13
Gambar 4. 10 <i>URL</i> situs web yang rentan serangan <i>XSS</i>	IV-14
Gambar 4. 11 Hasil pengujian <i>XSS</i>	IV-15
Gambar 4. 12 Spesifikasi server untuk virtualisasi Web	IV-16
Gambar 4. 13 Tampilan <i>cPanel</i> untuk mengelola Web.....	IV-17
Gambar 4. 14 Virtualisasi web Sakattaku.com diakses melalui IP lokal	IV-18
Gambar 4. 15 Hasil <i>scanning</i> setelah <i>WAF</i> dipasang.....	IV-21
Gambar 4. 16 <i>Rule</i> untuk mengatasi <i>CSP Wildcard</i>	IV-26

Gambar 4. 17 Pengujian setelah *rule* ditambahkan (*CSP* tidak terdeteksi) IV-29

Gambar 4. 18 Grafik perbandingan sebelum dan setelah *WAF* IV-49

LAMPIRAN

Lampiran 1 SK Pembimbing Tugas Akhir	L-1
Lampiran 2 Lembar Mengikuti Sidang Seminar Hasil	L-2
Lampiran 3 Lembar Revisi Laporan Sidang Usulan Penelitian Tugas Akhir	L-3
Lampiran 4 Lembar Rekap Perbaikan Usulan Penelitian Tugas Akhir.....	L-7
Lampiran 5 Daftar Hadir Seminar Hasil	L-8
Lampiran 6 Lembar Revisi Laporan Sidang Seminar Hasil	L-9
Lampiran 7 Lembar Rekap Perbaikan Seminar Hasil.....	L-13
Lampiran 8 Lembar Revisi Laporan Tugas Akhir.....	L-14
Lampiran 9 Lembar Rekap Perbaikan Tugas Akhir	L-18