

DAFTAR ISI

HALAMAN SAMBUNG.....	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvi
INTISARI.....	xvii
<i>ABSTRACT</i>	xviii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	5
C. Batasan Masalah	5
D. Tujuan Penelitian	6
E. Manfaat Penelitian	6
BAB II TINJAUAN PUSTAKA	
A. Landasan Teori.....	8
B. Penelitian Sebelumnya.....	18
BAB III METODE PENELITIAN	
A. Tempat dan Waktu Penelitian.....	27
B. Metode Pengumpulan Data.....	27
C. Alat dan Bahan Penelitian.....	30
D. Konsep Penelitian	31

BAB IV HASIL DAN PEMBAHASAN

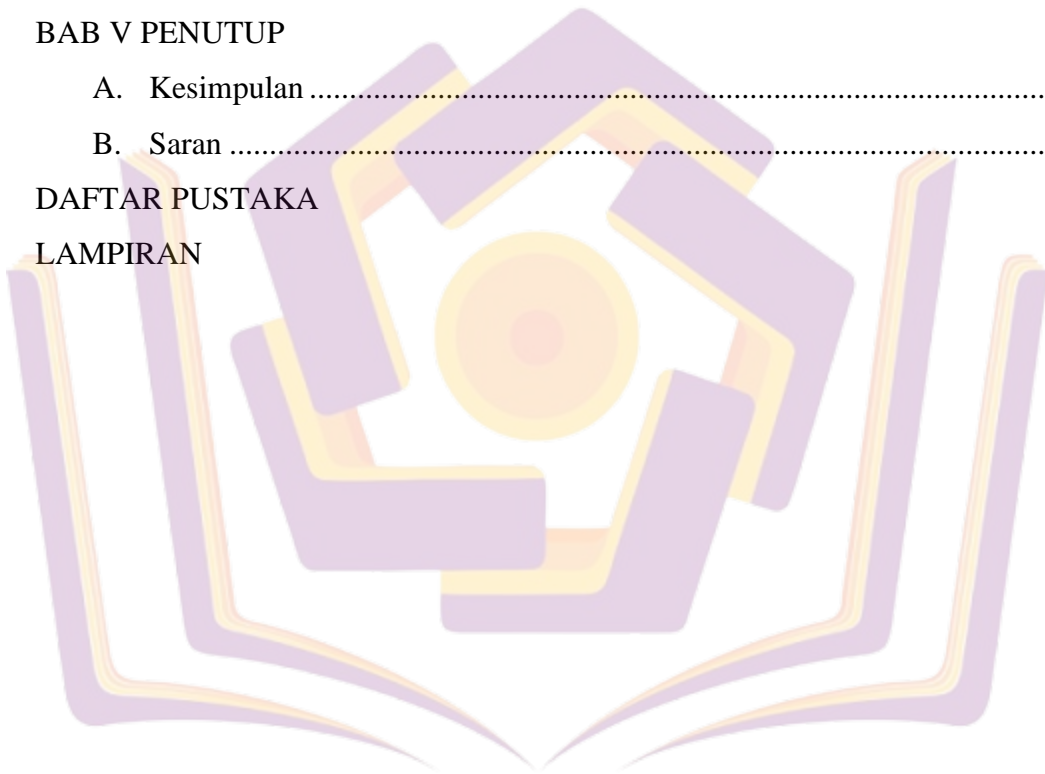
A. Tahap instalasi <i>Web Server Apache2</i> , modul <i>WAF Modsecurity</i> , <i>CRS OWASP</i>	41
B. Tahap Instalasi <i>DVWA</i> dan <i>Database MySQL</i>	53
C. Tahap Konfigurasi <i>DVWA</i> , <i>MySQL</i> , <i>Apache2</i> , Modul <i>Modsecurity</i> , dan <i>CRS OWASP</i>	56
D. Tahap Pengujian serangan <i>SQL Injection</i>	71
E. Tahap Hasil Dan Analisis	78

BAB V PENUTUP

A. Kesimpulan	85
B. Saran	86

DAFTAR PUSTAKA

LAMPIRAN



DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya.....	26
Tabel 4. 1 Konfigurasi pada file <i>config.inc.php</i>	59
Tabel 4. 2 Isi File konfigurasi Tambahan	68
Tabel 4. 3 Konfigurasi Modsecurity di <i>Apache2</i>	70
Tabel 4. 4 Data hasil <i>Blind SQL Injection</i>	80
Tabel 4. 5 Data hasil Pengujian dengan SQLMAP.....	81



DAFTAR GAMBAR

Gambar 2. 1 Aspek CIA.....	12
Gambar 2. 2 <i>Web Application Firewall</i>	17
Gambar 3. 1 Konsep Penelitian.....	32
Gambar 3. 2 konfigurasi pada <i>DVWA</i>	35
Gambar 4. 1 Update repository.....	41
Gambar 4. 2 Instal <i>Apache2</i>	42
Gambar 4. 3 Cek status <i>Apache2</i>	43
Gambar 4. 4 Menjalankan <i>Apache2</i>	44
Gambar 4. 5 Cek Status Aktif <i>Apache2</i>	45
Gambar 4. 6 Pengecekan <i>Web Server Apache2</i>	45
Gambar 4. 7 Update semua repository.....	46
Gambar 4. 8 Instal Library Modsecurity.....	47
Gambar 4. 9 Mengaktifkan Modul Modsecurity.....	48
Gambar 4. 10 Menghapus CRS Lama.....	49
Gambar 4. 11 Instal git.....	50
Gambar 4. 12 Instal CRS.....	51
Gambar 4. 13 Merubah File.....	52
Gambar 4. 14 Mengaktifkan Pengecualian File.....	52
Gambar 4. 15 Memindah Letak Direktori.....	53
Gambar 4. 16 Instal Paket <i>DVWA</i>	54
Gambar 4. 17 Instalasi <i>MySQL Server</i>	55
Gambar 4. 18 Memastikan Instalasi <i>DVWA</i>	56
Gambar 4. 19 Mengganti Hak Akses <i>DVWA</i>	56
Gambar 4. 20 Mengubah Letak Direktori.....	57
Gambar 4. 21 Menyalin File.....	57
Gambar 4. 22 Mengedit File Konfigurasi.....	58
Gambar 4. 23 Tampilan Isi File <i>config.inc.php</i>	59
Gambar 4. 24 Menjalankan <i>MySQL</i>	60
Gambar 4. 25 Mengecek Status <i>MySQL</i>	60

Gambar 4. 26 Mengelola <i>Database MySQL</i>	61
Gambar 4. 27 Mengecek Versi <i>Apache</i>	62
Gambar 4. 28 Mengubah Direktori Kerja	63
Gambar 4. 29 Membuka file <i>php.ini</i>	63
Gambar 4. 30 File Konfigurasi PHP	64
Gambar 4. 31 Memastikan <i>Apache2</i> Aktif.....	65
Gambar 4. 32 Menyalin File Konfigurasi	65
Gambar 4. 33 Konfigurasi <i>Modsecurity</i>	67
Gambar 4. 34 Konfigurasi <i>Modsecurity</i> dengan <i>CRS</i>	68
Gambar 4. 35 Menyambungkan <i>Modsecurity</i> di <i>Apache2</i>	69
Gambar 4. 36 Serangan <i>Blind SQL</i>	72
Gambar 4. 37 Serangan <i>SQLMAP</i> tanpa <i>WAF</i>	74
Gambar 4. 38 Hasil Serangan <i>SQLMAP</i> tanpa <i>WAF</i>	75
Gambar 4. 39 Serangan <i>Blind SQL Injection</i> dengan <i>WAF</i>	76
Gambar 4. 40 Hasil Serangan <i>Blind SQL Injection</i> dengan <i>WAF</i>	77
Gambar 4. 41 Hasil Serangan <i>SQLMAP</i> dengan <i>WAF</i>	78

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Skripsi Pembimbing 1

Lampiran 2. Kartu Bimbingan Skripsi Pembimbing 2

