DAFTAR ISI

LEMBAR JUDUL
LEMBAR PENGESAHAN
KATA PENGANTAR i
DAFTAR ISI ii
DAFTAR TABEL iv
DAFTAR GAMBAR v
DAFTAR LAMPIRAN vi
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Maksud dan Tujuan 2
1.4 Batasan Masalah 2
1.5 Metodologi Penelitian 3
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Tinjauan Perusahaan 5
2.1.1 Latar Belakang, Misi dan Sertifikasi Perusahaan 5
2.1.2 Security Services: CARE 5
2.1.3 Company Value: PASSION 7
2.1.4 Professional: Experience, TRUSTED Value and Certification 7
2.1.5 Logo Perusahaan 8
2.2 Landasan Teori 9
2.2.1 Internet 9
2.2.2 Situs 10
2.2.3 HTTP Respon 12
2.2.4 Keamanan Komputer 17
2.2.4.1 Ancaman Keamanan 20
2.2.4.2 Tipe-tipe Ancaman Keamanan 20
2.2.4.3 Tipe Ancaman Pada Aplikasi Web 21
2.2.4.4 Prinsip Pengamanan Sistem 24
2.2.5 SQL Injection 25
2.2.5.1 Penyebab SQL Injection 25

2.2.5.2 Pencegahan SQL Injection 27
2.2.6 Cross Site Scripting 27
2.2.6.1 Penyebab Cross Site Scripting 27
2.2.6.2 Pencegahan Cross Site Scripting 28
2.2.7 Validating Input 29
2.2.7.1 Whielist Validation 29
2.2.7.2 Blacklist Validation 29
2.2.8 Firewall 29
2.2.8.1 Jenis-Jenis Firewall 30
2.2.8.2 Cara Kerja Firewall 30
2.2.9 Web Server 36
BAB III PEMBAHASAN 40
3.1 Analisis Sistem 40
3.1.1 Analisis Masalah 40
3.1.2 Analisis Metode Ancaman 41
3.1.2.1 SQL Injection 41
3.1.2.2 Cross Site Scripting 45
3.1.3 Analisis Metode Pertahanan 54
3.2 Implementasi Mod Security 57
3.2.1 Skema Akses Web 57
3.2.2 Kebutuhan Sistem 57
3.2.3 Instalasi Mod Security 58
BAB IV KESIMPULAN DAN SARAN 65
4.1 Kesimpulan 65
4.2 Saran 65
DAFTAR PUSTAKA
LAMPIRAN