DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR ix
DAFTAR TABEL xi
DAFTAR LAMPIRAN xii
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 2
1.3. Maksud dan Tujuan 3
1.4. Batasan Masalah 3
1.5. Metode Penelitian 4
1.6. Sistematika Penulisan 5
BAB II LANDASAN TEORI 7
2.1. Jaringan Komputer 7
2.1.1. Tipe Jaringan 7
2.1.1.1. Jaringan Peer to Peer 7
2.1.1.2. Jaringan Client-Server 8
2.1.2. Arsitektur Jaringan Komputer 9
2.1.2.1. Topologi Bus 9
2.1.2.2. Topologi Ring 10
2.1.2.3. Topologi Star 10
2.2. Internet 12
2.3. Situs 13
2.4. HTTP Respon 15
2.4.1. Ancaman Keamanan 22
2.4.2. Tipe-tipe Ancaman Keamanan 22
2.4.3. Tipe Ancaman Pada Aplikasi Web 23

2.4.4. Prinsip Pengamanan Sistem 26
2.5. SQL Injection 27
2.5.1. Penyebab SQL Injection 27
2.5.2. Pencegahan SQL Injection 28
2.6. Cross Site Scripting 29
2.6.1. Penyebab Cross Site Scripting 29
2.6.2. Pencegahan Cross Site Scripting 29
2.7. Unrestricted File Upload 31
2.7.1. Penyebab Unrestricted File Upload 31
2.7.2. Pencegahan Unrestricted File Upload 31
2.8. Web Application Firewall 31
2.9. Basis Data 32
2.9.1. Model Data 32
2.9.1.1. Model Data Hirarkis 33
2.9.1.2. Model Data Jaringan 33
2.9.1.3. Model Data Relasional 34
2.9.2. Struktur File Database 35
2.9.3. Database Management System (DBMS) 35
2.9.3.1. Komponen DBMS 36
2.9.3.2. Kekurangan DBMS 37
2.9.3.3. Fungsi-fungsi DBMS 37
2.10. PHP 38
2.10.1. Tipe Data 39
2.10.1.1. Jenis Tipe Data 39
2.11. MySQL 41
2.11.1 Tipe Data 42
2.12. Web Server 42
2.12.1. Web Server Apache 43
2.12.2. Web Server Litespeed 43
2.12.3. Web Server Nginx 43
2.12.4. Web Server IIS 44

2.13. Virtual Private Server 44
2.14. OWASP Dirbuster 45
BAB III ANALISIS DAN PERANCANGAN SISTEM 47
3.1. Analisis Sistem 47
3.1.1. Analisis Masalah 47
3.1.2. Analisis URL 48
3.1.3. Analisis Protokol 50
3.1.3.1 HTTP Request 50
3.1.4. Analisis Metode Ancaman 52
3.1.4.1. SQL Injection 52
3.1.4.2. Analisis Information_Schema 56
3.1.4.3. Penyebab SQL Injection 59
3.1.4.4. Cross Site Scripting 60
3.1.4.5. Penyebab Cross Site Scripting 61
3.1.4.6. Unrestricted File Upload 63
3.1.4.7. Penyebab Unrestricted File Upload 64
3.1.5. Analisis Metode Pertahanan 65
3.1.6. Kebutuhan Pendukung Infrastruktur 73
3.1.6.1. Kebutuhan Perangkat Keras 73
3.1.6.2. Kebutuhan Perangkat Lunak 74
3.2. Analisis Perancangan Sistem 76
3.2.1. Arsitektur Simulasi 76
3.2.2. Arsitektur Simulasi Ancaman 77
3.2.3. Perancangan Web Application Firewall 81
BAB 4. IMPLEMENTASI DAN PENGUJIAN SISTEM 87
4.1 Implementasi 87
4.1.1 Implementasi Perangkat Keras 87
4.1.2 Implementasi Perangkat Lunak 88
4.1.3 Skenario Implementasi Sistem Tanpa Web Application Firewall 88
4.1.4 Skenario Implementasi Sistem Dengan Web Application Firewall 89
4.2 Pengujian 92

4.2.1 Skenario Pengujian 92
4.2.2 Pengujian Ancaman SQL Injection 93
4.2.2.1. Pencarian Web Form 93
4.2.2.2. Eksekusi Form Login 94
4.2.3. Pengujian Ancaman Cross Site Scripting 95
4.2.4. Pengujian Ancaman Unrestricted File Upload 96
4.2.4.1. Pencarian Direktori Web 96
4.2.4.2 Eksekusi Form Upload 97
4.2.4.3 Eksekusi File Upload 99
4.2.4. Pengujian Keamanan 101
4.2.5.1. Pengujian Metode WAF Pada SQL Injection 101
4.2.5.2. Pengujian Metode WAF Pada Cross Site Scripting 102
4.2.5.3. Pengujian Metode WAF Pada Unrestricted File Upload 103
4.3. Hasil Pengujian 105
BAB 5. KESIMPULAN DAN SARAN 107
5.1 Kesimpulan 107
5.2 Saran 107
DAFTAR PUSTAKA 107