DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAK……..…. i

ABSTRACT…….. ii

KATA PENGANTAR……..... iii

DAFTAR ISI……...v

DAFTAR TABEL……...xi

DAFTAR GAMBAR…….…… xii

DAFTAR LAMPIRAN……..……..xvii

BAB I PENDAHULUAN…….…..1

1.1 Latar Belakang Masalah…….…….... 1

1.2 Identifikasi Masalah…….. 2

1.3 Maksud dan Tujuan…….…….. 3

1.4 Batasan Masalah…….…..... 3

1.5 Metodologi Penelitian……...…… 5

1.6 Sistematika Penulisan…….…….…….. 8

BAB II LANDASAN TEORI……..… 6

2.1 Jaringan Komputer……..…9

2.1.1 Tipe Jaringan……..9

2.1.1.1 Jaringan Peer to peer……9

2.1.1.2 Jaringan Client-Server…….. 11

2.1.2 Arsitektur Jaringan Komputer…… 12

2.1.2.1 Topologi Bus…….13

2.1.2.2 Topologi Ring……... 14

2.1.2.3 Topologi Star…… 15

2.2 Internet……... 16

2.3 Situs……18

2.4 HTTP Respon…….20

2.5 Keamanan Komputer……. 27

2.5.1 Ancaman Keamanan…….. 31

2.5.2 Tipe-tipe Ancaman Keamanan……...32

2.5.3 Tipe Ancaman Pada Aplikasi Web……..... 33

2.5.4 Prinsip Pengamanan Sistem……..... 37

2.6 Basis Data…….. 38

2.6.1 Model Data…….38

2.6.1.1 Model Data Hierarkis……39

2.6.1.2 Model Data Jaringan…….39

2.6.1.3 Model Data Relasional……..40

2.6.2 Struktur File Database…… 41

2.6.3 Database Management System (DBMS)……... 42

2.6.3.1 Komponen DBMS.……... 42

2.6.3.2 Kekurangan DBMS…….. 44

2.6.3.3 Fungsi-fungsi DBMS…… 45

2.6.3.4 Model Data……46

2.7 PHP…… 48

2.7.1 Tipe Data……..... 48

2.7.1.1 Jenis Tipe Data……..49

2.8 MySQL…….. 52

2.8.1 Tipe Data…… 52

2.9 SQL Injection…….....53

2.9.1 Penyebab SQL Injection…….54

2.9.2 Pencegahan SQL Injection……. 55

2.10 Cross Site Scripting……..56

2.10.1 Penyebab Cross Site Scripting……. 57

2.10.2 Pencegahan Cross Site Scripting……..57

2.11 Validating Input……... 58

2.11.1 Whielist Validation…….. 59

2.11.2 Blacklist Validation…….……..59

BAB III ANALISIS DAN PERANCANGAN……... 60

3.1 Analisis Sistem……..60

3.1.1 Analisis Masalah…… 60

3.1.2 Analisis Protokol…… 61

3.1.2.1 HTTP Request…….. 62

3.1.3 Analisis URL…….64

3.1.3.1 URL Page……66

3.1.4 Analisis Metode Ancaman…… 67

3.1.4.1 SQL Injection……67

3.1.4.2 Analisis Information_schema……... 70

3.1.4.3 Penyebab SQL Injection……... 76

3.1.4.3.1 Metode Base64_Encode……....77

3.1.4.4 Cross Site Scripting…….. 82

3.1.4.5 Penyebab Cross Site Scripting……..83

3.1.4.6 Metode Input Encoding…….88

3.1.5 Analisis Metode Pertahanan……...91

3.1.5.1 Whitelist Validation……..91

3.1.5.2 Blacklist Validation…….. 93

3.1.5.3 Validating Input PHP……94

3.1.6 Kebutuhan Pendukung Infrastruktur…….. 96

3.1.6.1 Kebutuhan Perangkat Keras……..96

3.1.6.2 Kebutuhan Perangkat Lunak…….97

3.2 Perancangan Sistem……... 100

3.2.1 Arsitektur Simulasi…….100

3.2.2 Perancangan Antarmuka Target Simulasi……. 101

3.2.2.1 Menu……. 101

3.2.2.2 Antar Muka.…….. 102

BAB IV IMPLEMENTASI DAN PENGUJIAN….……...108

4.1 Implementasi……..108

4.1.1 Implementasi Perangkat Keras……...108

4.1.2 Implementasi Perangkat Lunak……..109

4.1.3 Konfigurasi Jaringan…….. 109

4.1.4 Target Situs…… 110

4.2 Pengujian……113

4.2.1 Skenario Pengujian…….113

4.2.2 Pengujian Ancaman SQL Injection……115

4.2.2.1 Pengujian Celah Keamanan…….. 115

4.2.2.2 Pengujian Jumlah Kolom Pada Tabel……...116

4.2.2.3 Pengujian Informasi Database…….. 116

4.2.2.4 Pengujian Tabel…… 117

4.2.2.5 Pengujian Kolom…….. 118

4.2.2.6 Pengujian Record……..119

4.2.3 Pengujian Ancaman Cross Site Scripting…….. 119

4.2.3.1 Pencarian Web Form…… 120

4.2.3.2 Eksekusi Kode HTML…...……... 121

4.2.3.3 Eksekusi Kode Untuk Menampilkan Cookie……123

4.2.4 Pengujian Pertahanan……. 125

4.2.4.1 Metode Base64_Encode Pada SQL Injection……...126

4.2.4.2 Metode Input Encoding Pada Cross Site Scripting…….. 133

4.2.4.3 Metode Validating Input Pada SQL Injection…….. 135

4.2.4.4 Metode Validating Input Pada Cross Site Scripting……. 140

4.3 Hasil Pengujian…….. 143

4.4 Pengujian Pada Website Lain…… 144

4.5 Kesimpulan Hasil Pengujian……. 148

BAB V KESIMPULAN DAN SARAN……..... 149

5.1 Kesimpulan…… 149

5.2 Saran……..... 149

DAFTAR PUSTAKA

LAMPIRAN