DAFTAR ISI

LEMBAR PERSEMBAHAN i

LEMBAR PENGESAHAN i

KATA PENGANTAR i

PERNYATAAN ii

ABSTRAK iii

ABSTRACT iv

DAFTAR ISI v

DAFTAR GAMBAR viii

DAFTAR TABEL ix

BAB I PENDAHULUAN 10

1.1 Latar Belakang 10

1.2 Rumusan Masalah 11

1.3 Tujuan 11

1.4 Batasan Masalah 12

1.5 Metode Penyelesaian Masalah 12

1.6 Pembagian Tugas Anggota 14

BAB II TINJAUAN PUSTAKA 15

2.1 Simulasi Email sebagai Metode Keamanan Siber 15

2.2 Autentikasi Pengguna dan Manajemen Data 15

2.3 Framework Laravel sebagai Basis Pengembangan Aplikasi 15

2.4 Keamanan Siber (Cybersecurity) 16

2.5 Pendidikan Siber 16

2.6 Kesadaran Keamana Siber (Cybersecurity Awareness) 17

2.7 Jenis Serangan Siber 17

2.8 Klasifikasi *Phishing* 18

2.9 Aplikasi Serupa 19

2.9.1 *Website* CanIPhish 19

2.9.2 *Website* PhishingBox 20

2.9.3 *Website* Phish Me If You Can 20

2.9.4 Perbandingan Fitur 21

BAB III ANALISIS KEBUTUHAN DAN PERANCANGAN 23

3.1 Analisis Kebutuhan Pengguna 23

3.1.1 Proses Menggali Informasi 23

3.1.2 Karakteristik Target Pengguna 25

3.1.3 Fitur yang Dibutuhkan 26

3.2 Perancangan Aplikasi 27

3.2.1 Gambaran Umum Aplikasi 27

3.2.1 Use Case Diagram 28

3.2.2 Perancangan Klasifikasi Tingkat Kesulitan Simulasi 30

3.2.3 Perancangan Antarmuka Aplikasi 32

3.2.4 Perancangan Basis Data 40

3.3 Kebutuhan Pengembangan Aplikasi 42

3.3.1 Kebutuhan Perangkat Keras 42

3.3.2 Kebutuhan Perangkat Lunak 42

BAB IV IMPLEMENTASI DAN PENGUJIAN 43

4.1 Implementasi Aplikasi 43

4.1.1 Struktur Kode *Project* 43

4.1.2 Kesesuaian Terhadap Rancangan 44

4.1.3 Hasil Implementasi 45

4.2 Pengujian Aplikasi 45

4.2.1 Pengujian Kualitas Kode 46

4.2.2 Pengujian Fungsionalitas 47

4.2.3 Pengujian ke Pengguna 49

4.2.4 Diskusi Hasil Pengujian 51

BAB V KESIMPULAN DAN SARAN 52

5.1 Kesimpulan 52

5.2 Saran 52

DAFTAR PUSTAKA 53

LAMPIRAN 55

Lampiran 1: Tabel Skala Likert 55

Lampiran 2 : Pengujian Terhadap Pengguna 57