DAFTAR ISI

ABSTRAK ... iii

ABSTRACT ... iv

Kata Pengantar ... vii

DAFTAR ISI ... ix

DAFTAR GAMBAR ... xi

DAFTAR TABEL ... xv

BAB I PENDAHULUAN ... 1

I.1 Latar Belakang ... 1

I.2 Rumusan Masalah ... 3

I.3 Tujuan dan Manfaat ... 3

I.4 Batasan Masalah ... 4

I.5 Metodologi Penelitian ... 4

BAB II TINJAUAN PUSTAKA ... 6

II.1 Penelitian Terdahulu ... 6

II.2 Dasar Teori ... 9

II.2.1 Keamanan Sistem ... 9

II.2.2 OWASP 2021 ... 10

II.2.3 Profil Website ... 13

II.2.4 Pentest ... 16

BAB III METODOLOGI ... 20

III.1 Metode yang digunakan ... 20

III.2 Alat dan Bahan Penelitian ... 20

III.3 Prosedur Penelitian ... 20

III.3.1 Studi Literatur ... 21

III.3.2 Pengumpulan Data 21

III.3.3 Pengujian Kerentanan dan *Penetration Testing* 21

III.3.4 Validasi Kepada Ahli 29

III.3.5 Konfirmasi Hasil Kepada Objek 29

III.3.6 Analisis Hasil 29

III.3.7 Menyusun Laporan Hasil dan Rekomendasi Perbaikan 30

BAB IV HASIL DAN PEMBAHASAN 31

IV.1 Information Gathering 31

IV.1.1 Whois 31

IV.1.2 Nslookup 32

IV.2 Network Mapping 35

IV.2.1 Nmap 35

IV.3 Exploitation 41

IV.3.1 A01 : Broken Access Control 41

IV.3.2 A02 : Cryptographic Failures 44

IV.3.3 A03 : Injection 53

IV.3.4 A04 : Insecure Design 60

IV.3.5 A05 : Security Misconfiguration 62

IV.3.6 A06 : Vulnerable and Oudated Components 78

IV.3.7 A07 : Identification and Authentication Failures 80

IV.3.8 A08 : Software and Data Integrity Failures 81

IV.3.9 A09 : Security Logging and Monitoring Failures 82

IV.3.10 A10 : Server-Side Request Forgery (SSRF) 83

IV.4 Reporting 87

BAB V KESIMPULAN DAN SARAN 100

V.1 Kesimpulan 100

V.2 Saran 100

BAB VI DAFTAR PUSTAKA 101

LAMPIRAN 104