DAFTAR ISI

LEMBAR PENGESAHAN i

LEMBAR PERNYATAAN ORISINALITAS ii

ABSTRAK iii

ABSTRACT iv

Kata Pengantar v

Daftar Isi vi

Daftar Tabel xi

Daftar Gambar xiii

Bab I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Perumusan Masalah 3

1.3 Tujuan Penelitian 3

1.4 Batasan Penelitian 4

1.5 Manfaat Penelitian 4

Bab II TINJAUAN PUSTAKA 5

2.1 Penelitian Terdahulu 5

2.2 Dasar Teori 12

2.2.1 Sistem Informasi 12

2.2.2 Keamanan Sistem Informasi 12

2.2.3 Profil *Website* 12

2.2.4 OWASP (*Open Worldwide Application Security Project*) 14

2.2.5 *Penetration Testing* 17

2.2.6 *Black box testing* 18

2.1.7 *Vulnerability* 18

2.1.8 Kali Linux 19

2.2.9 *Tools* Yang Digunakan 19
2.3 Alasan Pemilihan Teori/Model/Kerangka Kerja 26
Bab III Metodologi Penelitian 27
3.1 Sistematika Penyelesaian Masalah 27
3.2 Alur Penelitian 27
3.3 Alat dan Bahan 28
3.3.1 *Software* 28
3.3.2 *Hardware* 28
3.4 Prosedur Penelitian 29
3.4.1 Studi Literatur 29
3.4.2 *Planning* 29
3.4.3 *Information Gathering* 30
3.4.4 *Vulnerability Scanning* 30
3.4.5 *Penetration Testing* 30
3.4.6 Analisa Hasil 31
3.4.7 Validasi 31
3.4.8 *Reporting* 31
3.4.9 Konfirmasi Ke Perusahaan 31
3.5 Skenario Pengujian 32
3.5.1 *Broken Access Control* 32
3.5.2 *Cryptographic Failures* 32
3.5.3 *Injection* 33
3.5.4 *Insecure Design* 34
3.5.5 *Security Misconfiguration* 34
3.5.6 *Vulnerable and Outdated Components* 35
3.5.7 Identification and Authentication Failures 35

3.5.8 *Software and Data Integrity Failures* 35
3.5.9 *Security Logging and Monitoring Failures* 36
3.5.10 *Server-Side Request Forgery* 36
Bab IV Analisis dan Perancangan 38
4.1 Planning 38
4.1.1 Wawancara 38
4.2 *Information Gathering* 40
4.2.1 Whois 40
4.2.2 Nslookup 43
4.2.3 Dig 45
4.2.4 Nmap 46
4.2.5 Wappalyzer 47
4.3 Vulnerability Scanning 49
Bab V Implementasi dan Pengujian 51
5.1 Penetration Testing 51
5.1.1 A01:2021 – *Broken Access Control* 51
5.1.2 A02:2021 – *Cryptographic Failures* 56
5.1.3 A03:2021 – *Injection* 65
5.1.4 A04:2021 – *Insecure Design* 71
5.1.5 A05:2021 – *Security Misconfiguration* 75
5.1.6 A06:2021 – *Vulnerable and Outdated Components* 84
5.1.7 A07:2021 – Identification and Authentication Failures 90
5.1.8 A08:2021 – *Software and Data Integrity Failures* 93
5.1.9 A09:2021 – Security *Logging* and *Monitoring* 95
5.1.10 A10:2021 – *Server-Side Request Forgery* 98
5.2 Analisis Hasil 101

5.2.1 A01: 2021 – *Broken Access Control* 101
5.2.2 A02:2021 – *Cryptographic Failures* 102
5.2.3 A03:2021 – *Injection* 103
5.2.4 A04:2021 – *Insecure Design* 104
5.2.5 A05:2021 – *Security Misconfiguration* 104
5.2.6 A06:2021 – *Vulnerable and Outdated Component* 106
5.2.7 A07:2021 – *Identification and Authentication Failures* 107
5.2.8 A08:2021 – *Software and Data Integity Failures* 108
5.2.9 A09:2021 – *Security Logging* and *Monitoring* 109
5.2.10 A10:2021 – *Server-Side Request Forgery* 109
5.3 Validasi 110
5.4 *Reporting* 112
Bab VI Kesimpulan dan Saran 116
6.1 Kesimpulan 116
6.2 Saran 117
Daftar Pustaka 118
Lampiran 125
Lampiran Surat Pengantar Penelitian Dan Pengambilan Data 125
Lampiran Balasan Surat Pengantar Penelitian Dan Pengambilan Data 126
Lampiran Surat Keterangan Telah Melakukan Wawancara 127
Lampiran Profil Validator 128
Lampiran Sertifikat CEH Validator 131
Lampiran Surat Pernyataan Rahasia 132
Lampiran Bukti Melakukan Gmeet Dengan Validator 133
Lampiran Lembar Validator 134
Lampiran Buku Reporting 139

Lampiran Dokumentasi Penyerahan Buku 140
Lampiran Surat Keterangan Konfirmasi Reporting 141