

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN ORISINALITAS	ii
ABSTRAK	iii
<i>ABSTRACT</i>	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 <i>Website</i>	12
2.2.4 OWASP (<i>Open Worldwide Application Security Project</i>)	14
2.2.5 <i>Penetration Testing</i>	17
2.2.6 <i>Black box testing</i>	18
2.1.7 <i>Vulnerability</i>	18
2.1.8 Kali Linux	19

2.2.9	<i>Tools Yang Digunakan</i>	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	<i>Software</i>	28
3.3.2	<i>Hardware</i>	28
3.4	Prosedur Penelitian.....	29
3.4.1	Studi Literatur.....	29
3.4.2	<i>Planning</i>	29
3.4.3	<i>Information Gathering</i>	30
3.4.4	<i>Vulnerability Scanning</i>	30
3.4.5	<i>Penetration Testing</i>	30
3.4.6	Analisa Hasil.....	31
3.4.7	Validasi.....	31
3.4.8	<i>Reporting</i>	31
3.4.9	Konfirmasi Ke Perusahaan.....	31
3.5	Skenario Pengujian.....	32
3.5.1	<i>Broken Access Control</i>	32
3.5.2	<i>Cryptographic Failures</i>	32
3.5.3	<i>Injection</i>	33
3.5.4	<i>Insecure Design</i>	34
3.5.5	<i>Security Misconfiguration</i>	34
3.5.6	<i>Vulnerable and Outdated Components</i>	35
3.5.7	Identification and Authentication Failures.....	35

3.5.8	<i>Software and Data Integrity Failures</i>	35
3.5.9	<i>Security Logging and Monitoring Failures</i>	36
3.5.10	<i>Server-Side Request Forgery</i>	36
Bab IV	Analisis dan Perancangan	38
4.1	Planning	38
4.1.1	Wawancara.....	38
4.2	<i>Information Gathering</i>	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	<i>Penetration Testing</i>	51
5.1.1	A01:2021 – <i>Broken Access Control</i>	51
5.1.2	A02:2021 – <i>Cryptographic Failures</i>	56
5.1.3	A03:2021 – <i>Injection</i>	65
5.1.4	A04:2021 – <i>Insecure Design</i>	71
5.1.5	A05:2021 – <i>Security Misconfiguration</i>	75
5.1.6	A06:2021 – <i>Vulnerable and Outdated Components</i>	84
5.1.7	A07:2021 – <i>Identification and Authentication Failures</i>	90
5.1.8	A08:2021 – <i>Software and Data Integrity Failures</i>	93
5.1.9	A09:2021 – <i>Security Logging and Monitoring</i>	95
5.1.10	A10:2021 – <i>Server-Side Request Forgery</i>	98
5.2	Analisis Hasil.....	101

5.2.1	A01: 2021 – <i>Broken Access Control</i>	101
5.2.2	A02:2021 – <i>Cryptographic Failures</i>	102
5.2.3	A03:2021 – <i>Injection</i>	103
5.2.4	A04:2021 – <i>Insecure Design</i>	104
5.2.5	A05:2021 – <i>Security Misconfiguration</i>	104
5.2.6	A06:2021 – <i>Vulnerable and Outdated Component</i>	106
5.2.7	A07:2021 – <i>Identification and Authentication Failures</i>	107
5.2.8	A08:2021 – <i>Software and Data Integrity Failures</i>	108
5.2.9	A09:2021 – <i>Security Logging and Monitoring</i>	109
5.2.10	A10:2021 – <i>Server-Side Request Forgery</i>	109
5.3	Validasi.....	110
5.4	<i>Reporting</i>	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