

## DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	i
ABSTRAK	ii
<i>ABSTRACT</i>	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
DAFTAR ISTILAH	x
DAFTAR LAMPIRAN	xi
BAB 1 PENDAHULUAN	12
1.1 Latar Belakang	12
1.2 Perumusan Masalah	13
1.3 Tujuan dan Manfaat Penelitian	13
1.4 Batasan Penelitian	14
1.5 Prosedur Penelitian	15
1.5.1 Studi Literatur	15
1.5.2 Identifikasi <i>Website</i>	15
1.5.3 Metode OWASP <i>TOP</i> 10 2021	16
1.5.4 Daftar Kerentanan pada Metode OWASP <i>TOP</i> 10 2021	16
1.5.5 Hasil Pengujian Penetrasi	16
1.5.6 Analisis Hasil Pengujian	17
1.5.7 Pelaporan dan Validasi Pengujian	17
1.5.8 Kesimpulan	17
1.5.9 Penyusunan Buku TA	17
BAB 2 TINJAUAN PUSTAKA	18
2.1 Penelitian Terdahulu	18
2.2 Dasar Teori	22
2.1.1 Sistem Infromasi	22
2.1.2 Keamananan Sistem Infromasi	23
2.1.3 OWASP	23
2.1.4 OWASP TOP 10 2021	23

2.1.4.1	OWASP TOP 10 ( <i>Risk Classifications</i> )	26
2.1.5	SQL Injection	27
2.1.6	Brute Force Attack	27
2.1.7	Uji Penetrasi ( <i>Penetration Testing</i> )	27
2.1.8	Pengujian Greybox ( <i>Grey Box Testing</i> )	28
2.1.9	Alat Pengujian Penetrasi ( <i>penetration Testing Tools</i> )	28
BAB 3 METODOLOGI PENELITIAN		34
3.1	Metode yang digunakan	35
3.1.1	Tahapan <i>Information Gathering</i>	35
3.1.2	Tahapan <i>Network Mapping</i>	35
3.1.3	Tahapan <i>Peneration</i>	35
3.1.3.1	<i>Broken Access Control</i>	36
3.1.3.2	<i>Cryptographic Failures</i>	36
3.1.3.3	<i>Injection</i>	36
3.1.3.4	<i>Insecure Design</i>	37
3.1.3.5	<i>Security Misconfiguration</i>	37
3.1.3.6	<i>Vulnerable and Outdated Components</i>	38
3.1.3.7	<i>Identification and Authentication Failure</i>	38
3.1.3.8	Software and Data Integrity Failures	39
3.1.3.9	Security Logging and Monitoring Failures	39
3.1.3.10	Server side Request Forgery (SSRF)	39
3.2.	Alat dan Bahan Penelitian	40
3.3.	Perbandingan <i>Framework</i>	41
3.4.	Jadwal Pelaksanaan	42
BAB 4 HASIL DAN PEMBAHASAN		43
4.1	<i>Information Gethering</i>	43
4.2	Network Mapping	46
4.3	Scanning	47
4.3.1	OWASP	47
4.3.2	NIKTO	48
4.4	PENETARATION	49
4.4.1	Broke Accesces Control	49
4.4.2	Cryptographic Failures	51
4.4.3	Injection	53

4.4.4	Insecure Design	55
4.4.5	Security Misconfiguration	57
4.4.6	Vulnerable and Outdated Components	58
4.4.7	Identification and Authentication Failures	59
4.4.8	Software and Data Integrity Failures	61
4.4.9	Security Logging and Monitoring Failures	66
4.4.10	Server-Side Request Forgery	69
4.5	Analisis	70
4.6	Hasil dan Risk Level	72
KESIMPULAN DAN SARAN		75
	Kesimpulan	75
	Saran	76
References		77
LAMPIRAN		82
BIODATA PENULIS		95