

DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
LEMBAR ORISINALITAS	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xi
BAB 1 PENDAHULUAN.....	12
1.1. Latar Belakang	12
1.2. Perumusan Masalah	13
1.3. Tujuan.....	13
1.4. Batasan Masalah.....	14
1.5. Rencana Kegiatan.....	14
1.6. Jadwal Kegiatan	15
BAB 2 KAJIAN PUSTAKA	16
2.1 Penelitian Terkait	16
2.2 <i>Penetration Testing</i>	19
2.3 OWASP Top 10: 2021	19
2.4 Metode Black-box.....	21
2.5 Burp Suite.....	21
2.6 Nmap (<i>Network Mapping</i>).....	22
2.7 Wappalyzer.....	22
BAB 3 METODOLOGI PENGUJIAN.....	23
3.1 Alur Metodologi.....	23
3.1.1 Pengumpulan Informasi.....	23
3.1.2 Pemodelan Ancaman	24
3.1.3 Pemindaian Kerentanan.....	24
3.1.4 Eksploitasi.....	25
3.1.5 Laporan.....	25
BAB 4 HASIL DAN PEMBAHASAN	27

4.1	Perangkat Pengujian	27
4.1.1	Perangkat Keras (<i>Hardware</i>).....	27
4.2.2	Perangkat Lunak (<i>Software</i>).....	27
4.2	Pengumpulan Informasi dan Pemindaian	28
4.2.1	Wappalyzer	28
4.2.2	Whois.....	28
4.2.3	The Harvester	29
4.2.4	Nmap.....	29
4.2.5	Zed Attack Proxy.....	30
4.3	Uji Penetrasi (Eksplorasi).....	30
4.3.1	<i>Broken Access Control</i>	31
4.3.2	<i>Cryptographic Failures</i>	32
4.3.3	<i>Injection</i>	34
4.3.4	<i>Insecure Design</i>	36
4.3.5	<i>Security Misconfiguration</i>	36
4.3.6	<i>Vulnerable and Outdated Components</i>	39
4.3.7	<i>Identification and Authentication Failures</i>	40
4.3.8	<i>Software and Data Integrity Failures</i>	41
4.3.9	<i>Security Monitoring and Logging Failures</i>	41
4.3.10	<i>Server-Side Request Forgery</i>	42
4.4	Laporan.....	43
4.4.1	Email Administrator yang ditampilkan secara Publik	43
4.4.2	Terkena Serangan <i>ClickJacking</i>	43
4.4.3	Versi Bootstrap dan jQuery yang sudah kadaluarsa	44
4.4.4	Belum diterapkannya Mekanisme <i>Lockout</i>	44
BAB 5 PENUTUP		46
5.1	Kesimpulan	46
5.2	Saran	46
DAFTAR PUSTAKA.....		48
LAMPIRAN		50