

DAFTAR ISI

ABSTRAK	ii
ABSTRACT	iii
LEMBAR PENGESAHAN	iv
HALAMAN PERNYATAAN ORISINALITAS	v
KATA PENGANTAR	vi
DAFTAR ISI	i
DAFTAR TABEL	iv
DAFTAR GAMBAR	v
DAFTAR ISTILAH	vi
DAFTAR LAMPIRAN	viii
Bab I Pendahuluan	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	2
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	3
Bab II Tinjauan Pustaka	4
II.1 Penelitian Terdahulu	4
II.2 Keamanan Informasi	6
II.2.1 Web	7
II.2.2 Vulnerability	7
II.2.3 OWASP Top 10 2021	8
II.2.4 Vmware	11
II.2.5 Nmap	11

II.2.6	<i>Penetration Testing</i>	12
II.2.7	Acunetix	12
II.2.8	Burp Suite	13
II.2.9	Kali Linux	13
Bab III	METODOLOGI PENELITIAN	14
III.1	Kerangka Berpikir.....	14
III.2	Sistematika Penyelesaian Masalah	16
III.3	Pengumpulan Data.....	19
III.4	Pengolahan Data	19
III.5	Metode Evaluasi	20
III.6	Alasan Pemilihan Metode	21
III.7	Rencana Jadwal Kegiatan	Error! Bookmark not defined.
BAB IV	RANCANGAN PENGUJIAN.....	22
IV.1	Scope	22
IV.2.2	<i>Hardware</i>	23
IV.3	<i>Information gathering</i>	24
IV.3.1	<i>Information gathering</i> menggunakan NMAP	25
IV.4	<i>Vulnerability Detection</i>	26
IV.4.1	Pemindaan Menggunakan OWASP ZAP	27
IV.4.2	Pemindaan menggunakan Acunetix	29
IV.5	<i>Information Analysis and Planning</i>	32
IV.6	<i>Penetration Testing</i>	42
BAB V	HASIL PENGUJIAN.....	52
V.1	<i>Remediation</i>	52
V.3	Perancangan terhadap mitigasi	59
Bab IV	KESIMPULAN DAN SARAN	69

VI.1 Kesimpulan.....	69
VI.2 Saran.....	70
Daftar Pustaka	71
LAMPIRAN.....	72