

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
LEMBAR PERSEMBAHAN	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
DAFTAR LAMPIRAN.....	xii
DAFTAR ISTILAH	xv
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	4
I.3 Tujuan Tugas Akhir	5
I.4 Batasan Tugas Akhir	5
I.5 Manfaat Tugas Akhir	5
BAB II TINJAUAN PUSTAKA.....	7
II.1 Sistem Informasi	7
II.2 Keamanan Sistem Informasi	7
II.3 <i>Website</i>	8
II.4 <i>Penetration Testing Execution Standard (PTES)</i>	9
II.5 VMWARE <i>Workstation</i>	12
II.6 Kali Linux	13
II.7 NMAP	13

II.8	OWASP <i>Zed Attack Proxy</i> (ZAP).....	13
II.9	Burpsuite	14
II.10	Nessus	15
II.11	Penelitian Terdahulu	15
BAB III	METODOLOGI PENELITIAN	18
III.1	Model Konseptual	18
III.2	Sistematika Penyelesaian Masalah.....	19
III.3	Alasan Pemilihan Metode	22
BAB IV	RANCANGAN PENGUJIAN.....	24
IV.1	Perancangan Pengujian	24
IV.1.1	<i>Platform</i> Esperimen	24
IV.1.2	Perangkat keras	25
IV.1.3	Perangkat Lunak.....	28
IV.2	<i>Pre-engagement Interaction</i>	28
IV.3	<i>Information Gathering</i>	29
IV.3.1	Pengujian menggunakan Nmap.....	29
IV.3.2	Pengujian Menggunakan Whois	33
IV.4	<i>Vulnerability Detection</i>	34
IV.4.1	Pengujian menggunakan Burpsuite <i>Professional</i>	35
IV.4.2	Pengujian menggunakan OWASP ZAP.....	39
IV.4.3	Pengujian Menggunakan Nessus.....	43
BAB V	ANALISA DAN EVALUASI HASIL RANCANGAN	52
V.1	<i>Vulnerability Analysis</i>	52
V.1.1	Klasifikasi dan Pemilihan Kerentanan	52
V.1.2	Pemilihan Kerentanan	53
V.1.3	Daftar Kerentanan	58

V.2	<i>Attack and Penetration Testing</i>	59
V.2.1	<i>Remote Code Execution</i> melalui PHP-CGI (CVE-2019-11043)	59
V.2.2	DoS via <i>exif_thumbnail_extract</i>	60
V.2.3	<i>Client-side Desync</i>	62
V.2.4	<i>Absence of Anti-CSRF Tokens</i>	63
V.2.5	<i>Content Security Policy (CSP) Header Not Set</i>	64
V.3	<i>Remediation</i>	67
V.3.1	Perancangan Mitigasi	67
V.3.2	Pengujian ulang Pasca Mitigasi	69
BAB VI	Kesimpulan dan Saran	72
VI.3	Kesimpulan	72
VI.4	Saran	74