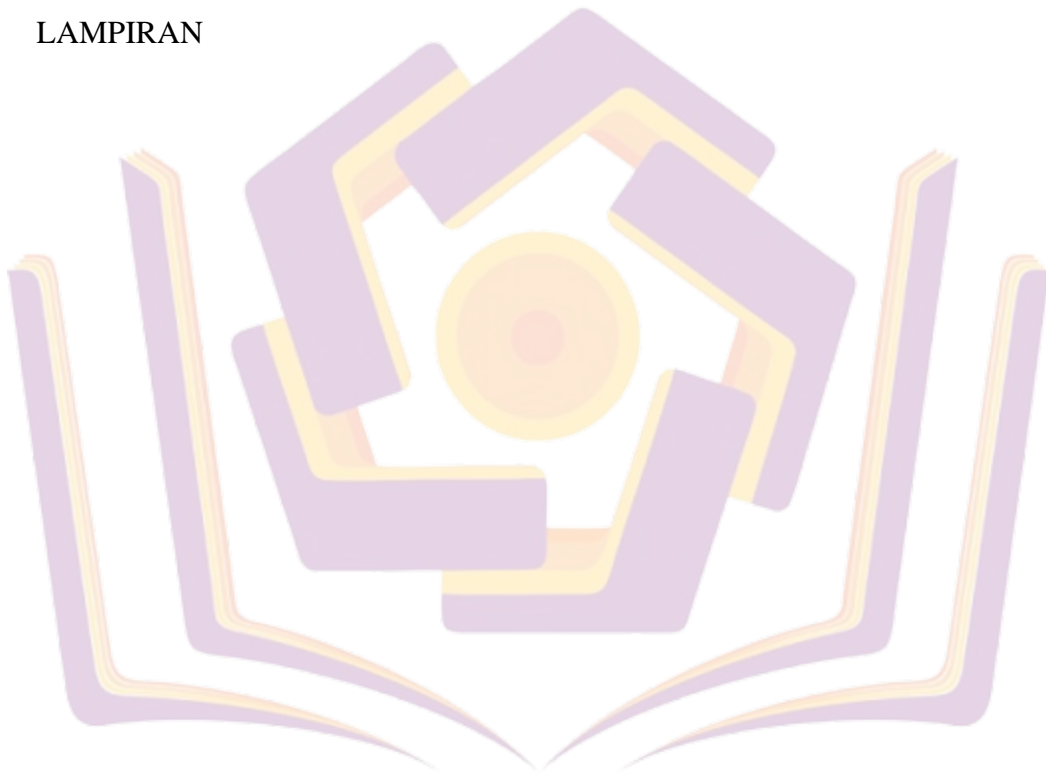


DAFTAR ISI

HALAMAN SAMBUTAN	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN.....	xv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	6
C. Batasan Masalah	6
D. Tujuan Penelitian	7
E. Manfaat Penelitian	7
BAB II TINJAUAN PUSTAKA	
A. Landasan Teori.....	8
B. Penelitian Sebelumnya.....	16
BAB III METODE PENELITIAN	
A. Tempat dan Waktu Penelitian.....	23
1. Tempat Penelitian	23
2. Waktu Penelitian.....	23
B. Metode Pengumpulan Data.....	23
C. Alat dan Bahan Penelitian.....	24

D. Konsep Penelitian	25
BAB IV HASIL DAN PEMBAHASAN	
A. Analisis	29
B. Hasil Analisis	30
BAB V PENUTUP	
A. Kesimpulan	57
B. Saran	57
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2.1 Penelitian sebelumnya.....	20
Tabel 4.1 Hasil pemindaian kerentanan OWASAP ZAP.....	55



DAFTAR GAMBAR

Gambar 3.1. Konsep Penelitian.....	26
Gambar 4.1 Hasil information gathering dengan nslookup	31
Gambar 4.2 Hasil information gathering dengan nmap	32
Gambar 4.3 Hasil information gathering dengan whois	33
Gambar 4.4 Tampilan ketika membuka aplikasi OWASP	34
Gambar 4.5 Halaman Utama OWASP ZAP	35
Gambar 4.6 kerentanan Absence of Anti-CSRF Tokens	35
Gambar 4.7 kerentanan CSP: Wildcard Directive	36
Gambar 4.8 kerentanan CSP: script-src unsafe-inline	37
Gambar 4.9 kerentanan CSP: style-src unsafe-inline.....	38
Gambar 4.10 kerentanan Cross-Domain Misconfiguration	39
Gambar 4.11 kerentanan HTTP to HTTPS Insecure Transition in Form Post	40
Gambar 4.12 kerentanan Multiple X-Frame-Options Header Entries	40
Gambar 4.13 kerentanan Cookie No HttpOnly Flag.....	41
Gambar 4.14 kerentanan Cookie Without Secure Flag.....	42
Gambar 4.15 kerentanan Cookie without SameSite Attribute.....	43
Gambar 4.16 kerentanan Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	44
Gambar 4.17 kerentanan Strict-Transport-Security Header Not Set	45
Gambar 4.18 kerentanan Timestamp Disclosure – Unix	46
Gambar 4.19 kerentanan Authentication Request Identified	47
Gambar 4.20 kerentanan Charset Mismatch	48
Gambar 4.21 kerentanan Cookie Poisoning.....	49
Gambar 4.22 kerentanan Information Disclosure - Suspicious Comments.....	50
Gambar 4.23 kerentanan Modern Web Application	51
Gambar 4.24 kerentanan Re-examine Cache-control Directives.....	51
Gambar 4.25 kerentanan Session Management Response Identified	52
Gambar 4.26 kerentanan User Agent Fuzzer	53

Gambar 4.27 kerentanan User Controllable HTML Element Attribute (Potential XSS)..... 53



DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Dosen 1

Lampiran 2. Kartu Bimbingan Dosen 2

Lampiran 3. Hasil Wawancara

Lampiran 4. Surat Penelitian

