

## DAFTAR ISI

HALAMAN SAMBUTAN .....	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN PENELITIAN .....	v
HALAMAN PERSEMBAHAN .....	vi
HALAMAN MOTTO .....	viii
KATA PENGANTAR .....	ix
DAFTAR ISI.....	xii
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR .....	xiv
DAFTAR LAMPIRAN.....	xvi
INTISARI.....	xvii
<i>ABSTRACT</i> .....	xviii
<b>BAB I PENDAHULUAN</b>	
A. Latar Belakang Masalah .....	1
B. Rumusan Masalah.....	5
C. Batasan Masalah .....	6
D. Tujuan Penelitian .....	6
<b>BAB II TINJAUAN PUSTAKA</b>	
A. Landasan Teori.....	7
B. Penelitian Sebelumnya.....	15
<b>BAB III METODE PENELITIAN</b>	
A. Waktu Penelitian .....	20
B. Metode Pengumpulan Data.....	20
C. Alat dan Bahan Penelitian.....	21
D. Konsep Penelitian .....	22

## BAB IV HASIL DAN PEMBAHASAN

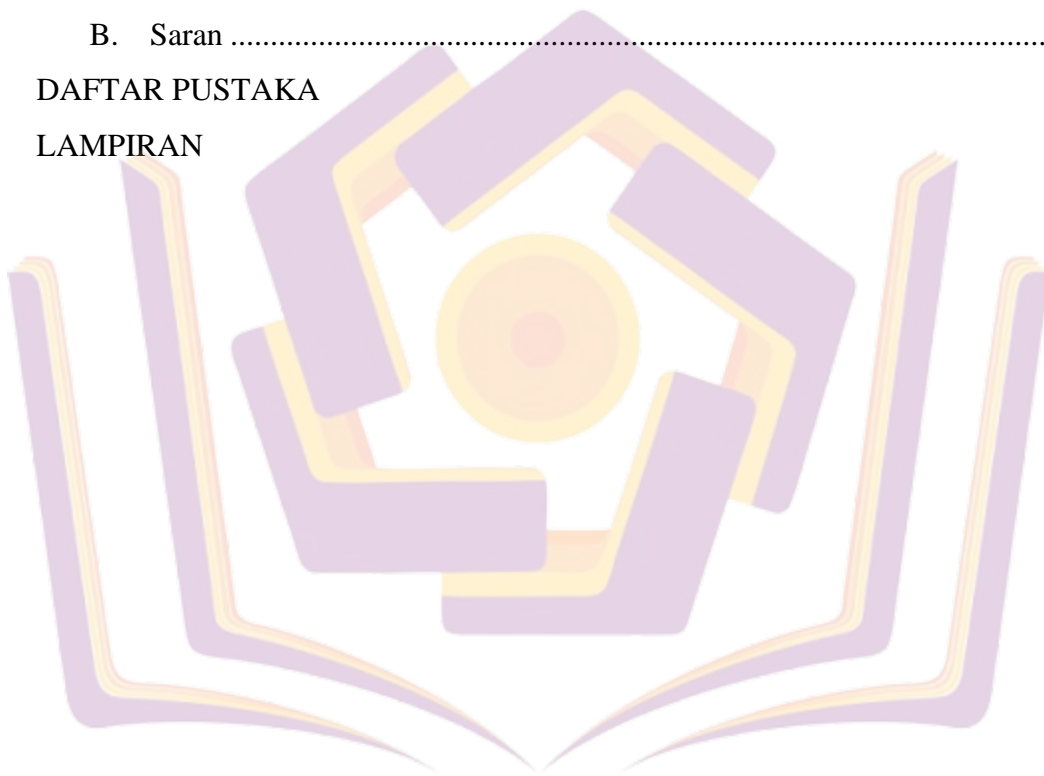
A. Intelelligence Gathering .....	27
B. Threat Modeling.....	30
C. Vulnerability Analysis .....	31
D. Exploitation.....	36
E. Reporting.....	40

## BAB V PENUTUP

A. Kesimpulan .....	46
B. Saran .....	47

## DAFTAR PUSTAKA

## LAMPIRAN



## DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Sebelumnya.....	17
Tabel 4.1 Hasil Informasi mengenai Domain website smashthestack.org dari pengecekan Whois lookup.....	29
Tabel 4. 2 Hasil Pemindaian Port smashthestack.org .....	30
Tabel 4. 3 Hasil Pengujian scanning vulnerability setelah dilakukan exploitation .....	41
Tabel 4. 5 Kerentanan OWASP dan Hasil Pengujian exploitation.....	42



## DAFTAR GAMBAR

Gambar 3. 1 Konsep Penelitian Metode PTES (Dasmen et al., 2023) .....	23
Gambar 4. 1 Pengecekan alamat IP pada <i>website smashthestack.org</i> menggunakan CMD .....	27
Gambar 4. 2 Informasi Domain menggunakan Whois lookup pada.....	28
Gambar 4. 3 Informasi raw whois lookup pada <i>website smashthestack.org</i> .....	29
Gambar 4. 4 Hasil Informasi <i>Alert</i> risiko keamanan pada <i>website smashthestack.org</i> menggunakan Pengujian OWASP ZAP .....	31
Gambar 4. 5 Tampilan hasil Pengujian Kerentanan menggunakan tool OWASP ZAP.....	32
Gambar 4. 6 Tampilan hasil Pengujian Kerentanan menggunakan <i>tool</i> .....	33
Gambar 4. 7 Hasil Pengujian SSL pada <i>tool SQLMap</i> yang tidak .....	37
Gambar 4. 8 Serangan Cross Site Scripting (XSS) yang gagal dijalankan pada browser untuk memperoleh cookie pengguna.....	38
Gambar 4. 9 Tampilan hasil serangan script HTML yang berhasil dijalankan <i>script</i> HTML .....	39
Gambar 4. 10 Hasil Serangan CSRF ketika telah berhasil dilakukan serangan perubahan data pada <i>script HTML</i> .....	39
Gambar 4. 11 Hasil tampilan Serangan <i>Clickjacking</i> pada <i>website</i> dengan menampilkan <i>iframe</i> yang gagal dilakukan .....	40

## DAFTAR LAMPIRAN

Lampiran 1. Gambar *Scanning* Port dengan *Nmap*

Lampiran 2. Proses *Scanning* Vulnerability menggunakan OWASP ZAP

Lampiran 3. Gambar Code Iframe proses Clickjacking

Lampiran 4. Gambar Code Serangan CSRF data awal

Lampiran 5. Gambar Code Serangan CSRF setelah dirubah data

Lampiran 6. Kartu Bimbingan Skripsi 1

Lampiran 7. Kartu Bimbingan Skripsi 2

