

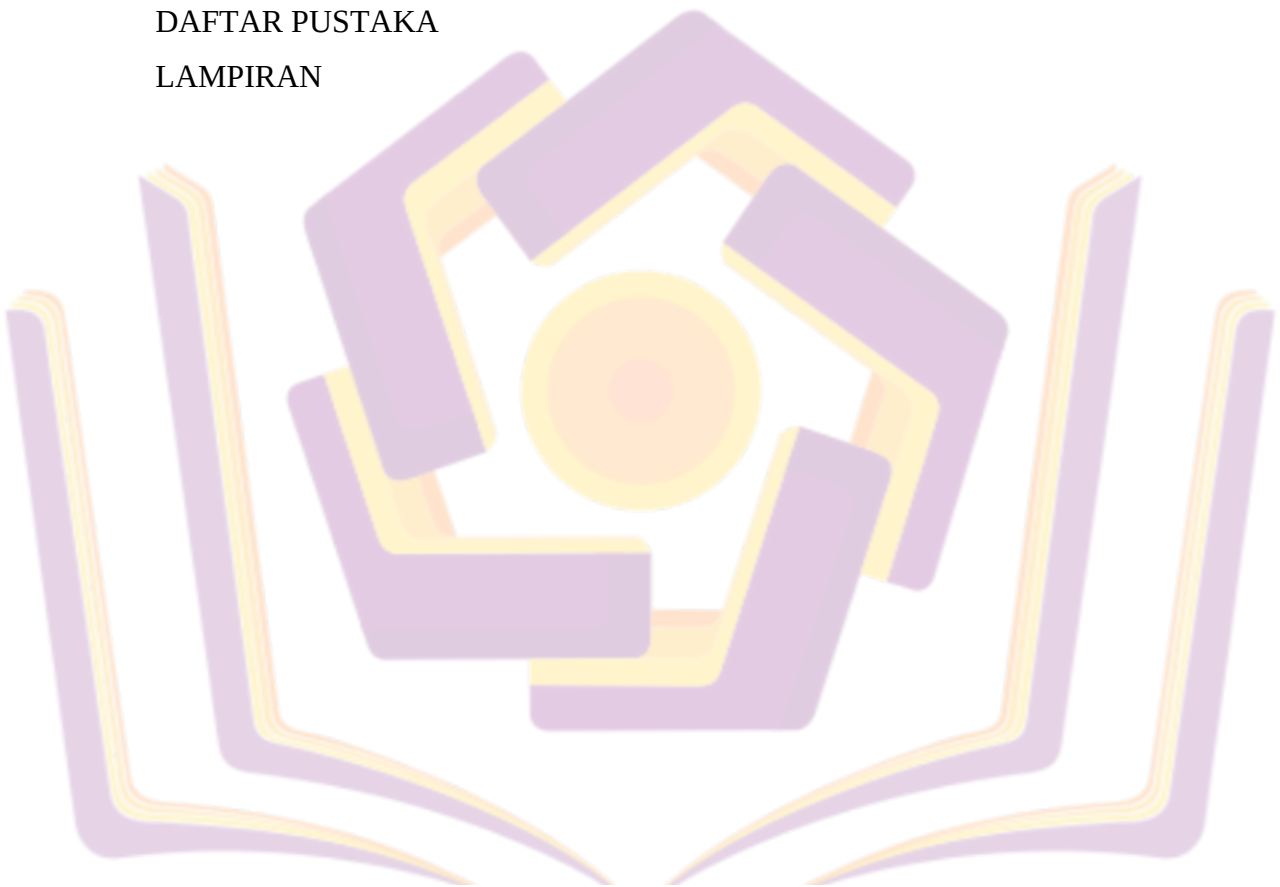
DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
ABSTRAK.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	15
C. Batasan Masalah	15
D. Tujuan Penelitian	16
E. Manfaat Penelitian	16
BAB II TINJAUAN PUSTAKA.....	18
A. Landasan Teori.....	18
B. Penelitian Sebelumnya.....	41
BAB III METODE PENELITIAN.....	50
A. Tempat dan Waktu Penelitian.....	50
B. Metode Pengumpulan Data.....	50
C. Alat dan Bahan Penelitian.....	52
D. Konsep Penelitian	54
BAB IV HASIL DAN PEMBAHASAN	61

A. Information Gathering	61
B. Information Gathering	64
C. Vulnerability Analysis	66
D. Exploitation.....	71
E. Reporting.....	77
BAB V PENUTUP.....	79
A. Kesimpulan	79
B. Saran	80

DAFTAR PUSTAKA

LAMPIRAN



DAFTAR TABEL

Tabel 2. 1 Jenis-Jenis Penetration <i>Testing</i>	23
Tabel 2. 2 Peran Website dalam SIRK.....	28
Tabel 2. 3 Tingkat Resiko Keamanan Website E-clinic	36
Tabel 2. 4 Penelitian Sebelumnya.....	48
Tabel 3. 1 Komponen & Spesifikasi Laptop.....	52
Tabel 4. 1 Hasil informasi mengenai Domain	63
Tabel 4. 2 Hasil Pemindaian Port kamandakacare.com.....	63
Tabel 4. 3 Hasil <i>Threat Modelling Website E-Clinic</i>	65
Tabel 4. 4 <i>Payload SQLI</i> yang terinjeksi	71
Tabel 4. 5 Tabel Perbandingan <i>Respons Form Login</i> Asli dan Replika terhadap <i>SQL Injection</i>	75
Tabel 4. 6 Resume Hasil Pengujian Keamanan Website	78

DAFTAR GAMBAR

Gambar 2. 1 ZAP Proxy Server	31
Gambar 2. 2 Diagram Serangan <i>SQL Injection</i> – <i>Bypass Login Admin</i>	33
Gambar 2. 3 Contoh penyerang	34
Gambar 2. 4 <i>Malicious SQL Query</i>	34
Gambar 3. 1 Konsep Penelitian Metode PTES	54
Gambar 3. 2 Skema <i>Threat Modeling</i>	57
Gambar 4. 1 Pengecekan alamat IP pada website.....	61
Gambar 4. 2 Informasi Domain menggunakan <i>Whois lookup</i>	62
Gambar 4. 3 Informasi <i>Whois domain lookup</i>	62
Gambar 4. 4 Hasil Informasi Kerentanan Risiko Keamanan	66
Gambar 4. 5 Hasil Pemindaian tool OWASP ZAP.....	67
Gambar 4. 6 <i>Payload 1</i>	72
Gambar 4. 7 <i>Payload 2</i>	72
Gambar 4. 8 <i>Payload 3</i>	73
Gambar 4. 9 Tampilan <i>Form Login</i> yang terinjeksi.....	73
Gambar 4. 10 Tampilan <i>Form Login</i> yang tidak terinjeksi.....	74
Gambar 4. 11 hasil <i>SQL Map</i>	76

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Dosen Pembimbing 1

Lampiran 2. Kartu Bimbingan Dosen Pembimbing 2

