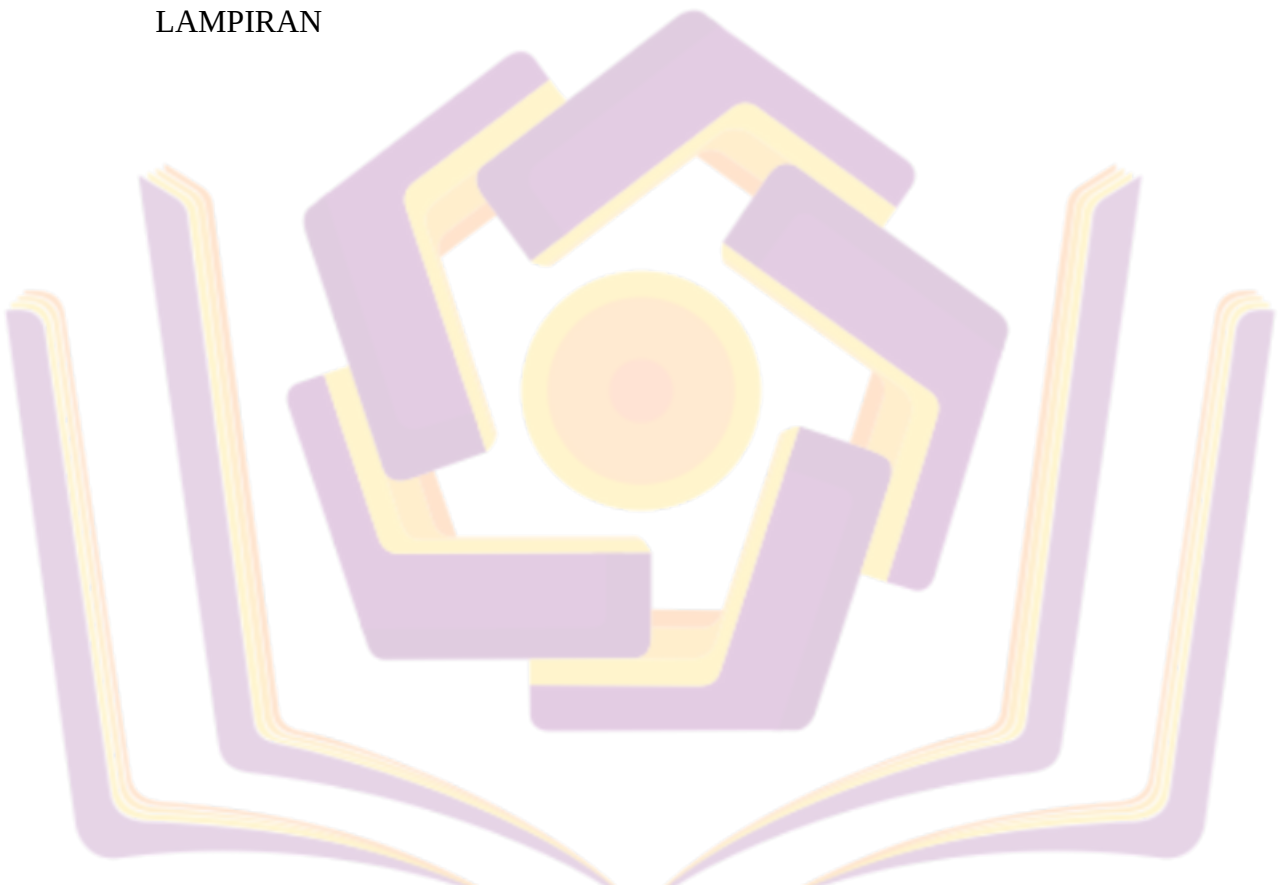


DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN PENELITIAN	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN.....	xii
ABSTRAK.....	xiii
<i>ABSTRACT</i>	xiv
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah	5
C. Batasan Masalah	6
D. Tujuan Penelitian.....	7
E. Manfaat Penelitian.....	7
BAB II TINJAUAN PUSTAKA.....	9
A. Landasan Teori	9
B. Penelitian-Penelitian Terdahulu	23
BAB III METODE PENELITIAN.....	30
A. Tempat dan Waktu Penelitian	30
B. Metode Pengumpulan Data	30
C. Alat dan Bahan Penelitian	31
D. Konsep Penelitian	33
BAB IV HASIL DAN PEMBAHASAN	46

A. Gambaran <i>Website</i> ON&CLASS UMP	46
B. Hasil Wawancara dengan Pengelola <i>Website</i>	50
C. <i>Planning and Preparation</i>	52
D. <i>Assesment</i>	55
BAB V PENUTUP	105
A. Kesimpulan	105
B. Saran	107
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 Penelitian-Penelitian Terdahulu	28
Tabel 4. 1 Hasil Wawancara dengan Pengelola <i>Website</i>	50
Tabel 4. 2 Hasil <i>Scan</i> Menggunakan Whois	58
Tabel 4. 3 Hasil Enumerasi DNS Menggunakan Dnsrecon	62
Tabel 4. 4 Hasil <i>Scanning</i> WhatWeb	69
Tabel 4. 5 Hasil <i>Scanning</i> Nmap.....	72
Tabel 4. 6 Hasil <i>Vulnerability Scanning</i> OWASP ZAP.....	76
Tabel 4. 7 Pengujian <i>Reflected</i> XSS	81
Tabel 4. 8 Hasil <i>Penetration testing</i> ON&CLASS UMP.....	82
Tabel 4. 9 Rekomendasi Perbaikan <i>Website</i> ON&CLASS UMP	102

DAFTAR GAMBAR

Gambar 2. 1 Metodologi ISSAF	10
Gambar 3. 1 Kerangka Berpikir	33
Gambar 4. 1 Website ON&CLASS UMP	56
Gambar 4. 2 Mencari Informasi IP Address Menggunakan PING	57
Gambar 4. 3 Hasil Identifikasi Informasi <i>Domain</i> Menggunakan Whois	58
Gambar 4. 4 Hasil Enumerasi Menggunakan Dnsrecon	61
Gambar 4. 5 Hasil Identifikasi <i>Subdomain</i> Menggunakan Dnsdumpster	63
Gambar 4. 6 <i>Single Sign-on</i>	64
Gambar 4. 7 PING Pada sso.ump.ac.id	66
Gambar 4. 8 Hasil <i>Scanning</i> Menggunakan Dnsrecon	67
Gambar 4. 9 Hasil <i>Scan</i> Menggunakan WhatWeb	68
Gambar 4. 10 Hasil <i>Scanning Port</i> Menggunakan Nmap	72
Gambar 4. 11 Tampilan Awal OWASP ZAP	74
Gambar 4. 12 Hasil Kerentanan yang Diperoleh	75
Gambar 4. 13 Serangan XSS pada URL	79
Gambar 4. 14 Perintah Injeksi menggunakan SQLmap	80
Gambar 4. 15 Scanner menggunakan Metasploit	83
Gambar 4. 16 SSH <i>Login</i> menggunakan Metasploit	85
Gambar 4. 17 <i>Input Username</i> dan <i>Password</i>	87
Gambar 4. 18 <i>Request</i> Masuk	88
Gambar 4. 19 Hasil <i>Snipper Attack</i>	89
Gambar 4. 20 Percobaan <i>Input</i>	90
Gambar 4. 21 Percobaan <i>Remote</i>	91
Gambar 4. 22 Proses Eksploitasi	92
Gambar 4. 23 Proses Eksploitasi (Lanjutan)	92
Gambar 4. 24 Isi auth.log	93
Gambar 4. 25 Proses penghapusan	94
Gambar 4. 26 Hasil <i>Covering tracks</i>	95

DAFTAR LAMPIRAN

Lampiran 1. Pedoman Wawancara

Lampiran 2. Surat Izin Penelitian

Lampiran 3. Kartu Bimbingan

