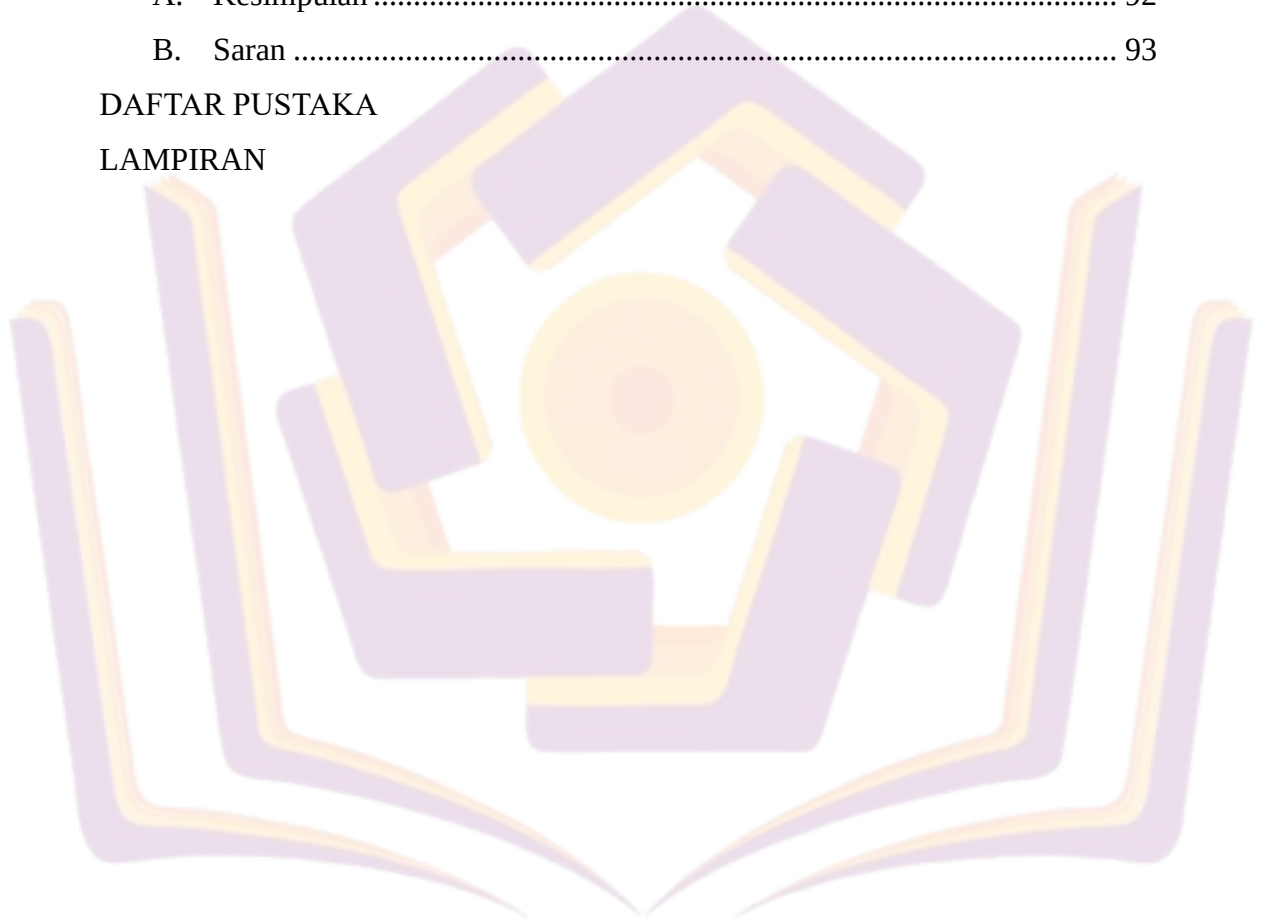


DAFTAR ISI

HALAMAN SAMPUL	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
ABSTRACT.....	xvii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	7
C. Batasan Masalah	7
D. Tujuan Penelitian	7
E. Manfaat Penelitian	8
BAB II TINJAUAN PUSTAKA.....	9
A. Landasan Teori.....	9
B. Penelitian Sebelumnya.....	20
BAB III METODE PENELITIAN.....	29
A. Tempat dan Waktu Penelitian.....	29
B. Metode Pengumpulan Data.....	29
C. Alat dan Bahan Penelitian.....	30
D. Konsep Penelitian	34
BAB IV HASIL DAN PEMBAHASAN	39

A. Pengumpulan Informasi	39
B. Pemindaian Kerentanan	52
C. Eksploitasi.....	59
D. CVSS Score	84
E. Laporan Hasil.....	86
BAB V PENUTUP.....	92
A. Kesimpulan	92
B. Saran	93
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya.....	24
Tabel 3. 1 Level <i>Severity</i> CVSS.....	38
Tabel 4. 1 Hasil <i>Whois</i> Pada unwiku.ac.id.....	41
Tabel 4. 2 Hasil Enumerasi DNS Pada unwiku.ac.id.....	42
Tabel 4. 3 Hasil Pencarian <i>Subdomain</i>	44
Tabel 4. 4 Hasil Enumerasi DNS siaku.unwiku.ac.id.....	47
Tabel 4. 5 Hasil Identifikasi <i>Whatweb</i>	48
Tabel 4. 6 Hasil Identifikasi <i>Wappalyzer</i>	50
Tabel 4. 7 Hasil Pemindaian <i>Port</i> Menggunakan <i>Nmap</i>	52
Tabel 4. 8 Hasil <i>Vulnerability Scanning</i> OWASP ZAP.....	54
Tabel 4. 9 Klasifikasi Kerentanan Berdasarkan OWASP Top 10	58
Tabel 4. 10 Teknik Eksploitasi Kerentanan	59
Tabel 4. 11 Hasil Pengujian Eksploitasi	83
Tabel 4. 12 CVSS <i>Score</i>	85
Tabel 4. 13 Hasil Temuan Kerentanan.....	86
Tabel 4. 14 Laporan Hasil Pengujian Eksploitasi.....	88
Tabel 4. 15 Rekomendasi Perbaikan.....	90

DAFTAR GAMBAR

Gambar 2. 1 CIA <i>Triad</i>	10
Gambar 2. 2 CVSS	19
Gambar 3. 1 Alur Penelitian.....	34
Gambar 4. 1 Tampilan <i>Website</i> Utama UNWIKU.....	39
Gambar 4. 2 Hasil Pencarian IP Address Pada unwiku.ac.id.....	40
Gambar 4. 3 Hasil Identifikasi Menggunakan <i>Whois</i>	41
Gambar 4. 4 Hasil Enumerasi DNS Pada unwiku.ac.id	42
Gambar 4. 5 Hasil Pencarian <i>Subdomain</i> Menggunakan <i>Dnsdumpster</i>	44
Gambar 4. 6 Tampilan <i>Website</i> SIAKU UNWIKU	45
Gambar 4. 7 Pencarian IP Address siaku.unwiku.ac.id	46
Gambar 4. 8 Hasil Enumerasi DNS siaku.unwiku.ac.id	46
Gambar 4. 9 Hasil Identifikasi Menggunakan <i>Whatweb</i>	48
Gambar 4. 10 Hasil Identifikasi <i>Wappalyzer</i>	50
Gambar 4. 11 Hasil Pemindaian Port Menggunakan <i>Nmap</i>	51
Gambar 4. 12 Fitur <i>Automated Scan</i> OWASP ZAP	53
Gambar 4. 13 Hasil <i>Scanning Vulnerability</i> OWASP ZAP	53
Gambar 4. 14 Tampilan <i>Website Target</i>	61
Gambar 4. 15 Melihat <i>Page Source</i>	61
Gambar 4. 16 Mencari Komentar Sensitif	62
Gambar 4. 17 Penyerangan Menggunakan <i>Nikto</i>	62
Gambar 4. 18 Pengujian <i>Script XSS</i>	63
Gambar 4. 19 <i>Script Clickjacking.html</i>	64
Gambar 4. 20 <i>Script Login.html</i>	65
Gambar 4. 21 <i>Script Hacked.html</i>	65
Gambar 4. 22 Hasil Serangan <i>Clickjacking</i>	66
Gambar 4. 23 Tampilan <i>Login</i> Situs Penyerang <i>Clickjacking</i>	67
Gambar 4. 24 Tampilan Terkena Serangan <i>Clickjacking</i>	67
Gambar 4. 25 Halaman Tiruan SIAKU UNWIKU	68
Gambar 4. 26 Halaman Peringatan <i>Phishing</i>	69

Gambar 4. 27 Tampilan <i>Login</i> SIAKU UNWIKU Asli.....	70
Gambar 4. 28 Halaman <i>Phising</i> SIAKU UNWIKU Saat <i>Login</i>	70
Gambar 4. 29 Halaman Peringatan Setelah Terkena <i>Phishing</i>	71
Gambar 4. 30 Serangan <i>Reconnaissance</i>	72
Gambar 4. 31 Hasil Pengujian <i>HTML Injection</i>	73
Gambar 4. 32 Hasil Serangan <i>Framework-Specific Attack</i>	74
Gambar 4. 33 <i>Login</i> Ke Sistem	75
Gambar 4. 34 <i>Logout</i> Dari Sistem.....	76
Gambar 4. 35 Hasil Pengujian <i>Sensitive Data Cache</i>	76
Gambar 4. 36 Konfigurasi <i>Proxy</i>	77
Gambar 4. 37 Mengakses <i>Website</i> Di <i>Browser Burp Suite</i>	78
Gambar 4. 38 <i>Send Request to Intruder</i>	78
Gambar 4. 39 Konfigurasi <i>User-Agent</i>	79
Gambar 4. 40 <i>Script PHP</i> Untuk <i>Payload</i>	79
Gambar 4. 41 Hasil Serangan <i>Evasion and Header Fuzzing</i>	80
Gambar 4. 42 Hasil Identifikasi Konfigurasi <i>DNSSEC</i>	81
Gambar 4. 43 Edit <i>/etc/hosts</i>	82
Gambar 4. 44 Membuat Halaman Palsu	82
Gambar 4. 45 Hasil Pengujian <i>DNS Spoofing</i>	82

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Dosen Pembimbing 1

Lampiran 2. Kartu Bimbingan Dosen Pembimbing 2

Lampiran 3. Surat Izin Penelitian

Lampiran 4. Surat Izin Penelitian Balasan

Lampiran 5. Wawancara dengan Pengelola 1

Lampiran 6. Wawancara dengan Pengelola 2

Lampiran 7. Hasil Wawancara

Lampiran 8. Hasil *Scanning Dnsdumpster* Lengkap

Lampiran 9. Tabel Hasil *Scanning Dnsdumpster* Lengkap

Lampiran 10. Program Simulasi *Clickjacking* HTML

