

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
ABSTRAK.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	7
C. Batasan Masalah	8
D. Tujuan Penelitian	8
E. Manfaat Penelitian	8
BAB II TINJAUAN PUSTAKA.....	10
A. Landasan Teori.....	10
B. Penelitian Sebelumnya.....	27
BAB III METODE PENELITIAN.....	33
A. Tempat dan Waktu Penelitian.....	33
B. Metode Pengumpulan Data.....	33
C. Alat dan Bahan Penelitian.....	35
D. Konsep Penelitian	37
BAB IV HASIL DAN PEMBAHASAN	45

A. <i>Planning and Preparation</i>	45
B. <i>Assessment</i>	46
C. <i>Reporting, Clean Up and Destroy Artifacts</i>	69
D. Kesimpulan Hasil Pengujian.....	73
BAB V PENUTUP.....	74
A. Kesimpulan	74
B. Saran	74
DAFTAR PUSTAKA	
LAMPIRAN	



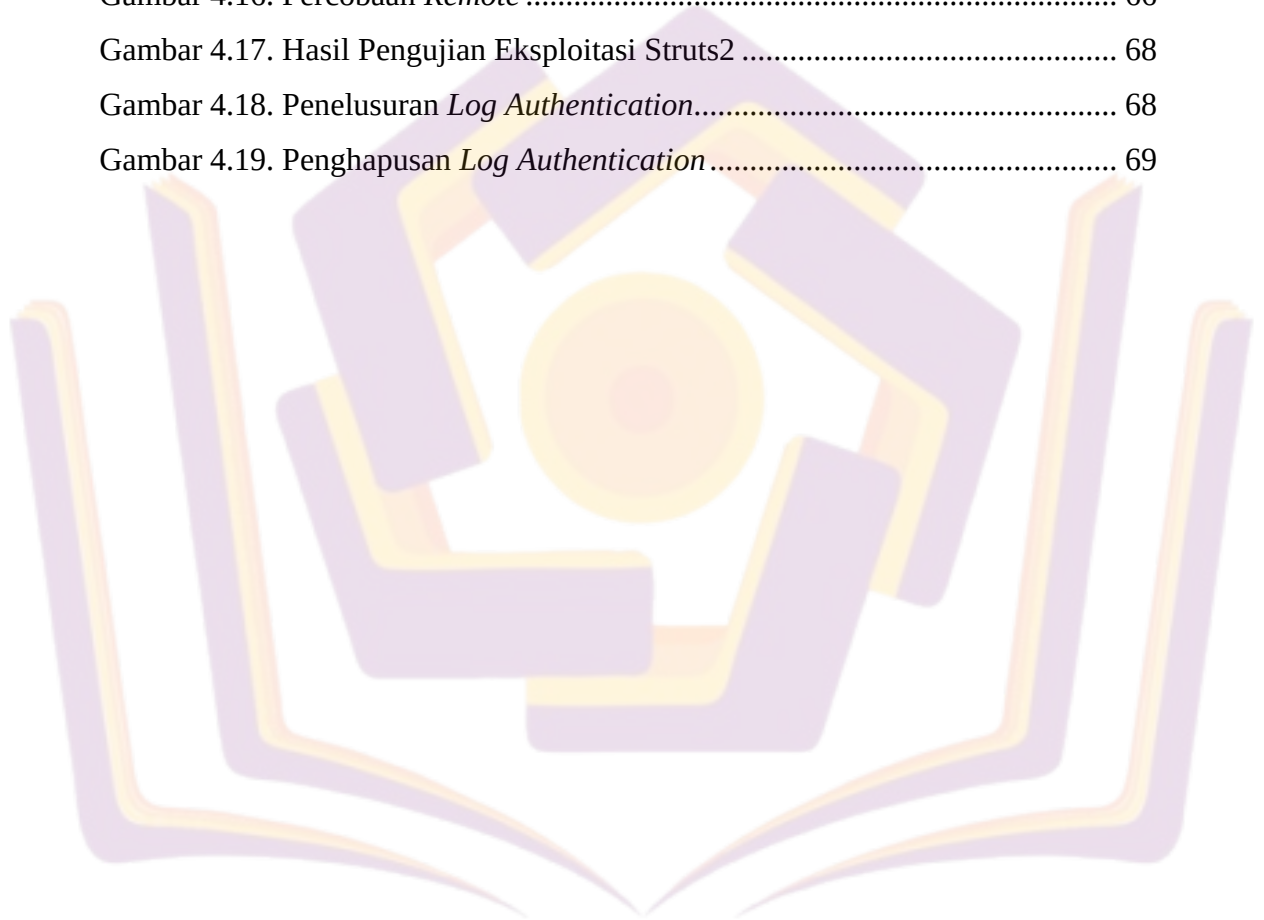
DAFTAR TABEL

Tabel 2.1. Penelitian Sebelumnya.....	31
Tabel 3.1. Perangkat Lunak dan Fungsinya.....	36
Tabel 4.1. Hasil Informasi Whois	48
Tabel 4.2. Hasil Informasi Sub Domain	49
Tabel 4.3. Informasi Teknologi Web	50
Tabel 4.4. Hasil Scanning dengan tools Nmap	51
Tabel 4.5. Vulnerability Identification.....	53
Tabel 4.6. Hasil Penetration Testing.....	63
Tabel 4.7. Hasil Reporting	71

DAFTAR GAMBAR

Gambar 1.1. Sumber Laporan Masuk	2
Gambar 1.2. Pengunjung Harian	2
Gambar 1.3. Indikasi Judi <i>Online</i>	4
Gambar 1.4. Indikasi Obat Ilegal	4
Gambar 1.5. <i>Traffic</i> IP address	5
Gambar 2.1. <i>CIA Triad</i>	10
Gambar 2.2. Jenis Metode Testing	14
Gambar 2.3. Virtualbox	17
Gambar 2.4. Kalilinux	17
Gambar 2.5. DnsDumpster	18
Gambar 2.6. Whois	18
Gambar 2.7. Nmap	19
Gambar 2.8. Visual Studio	19
Gambar 2.9. OWASP-ZAP	20
Gambar 2.10. Whatweb	21
Gambar 2.11. Brup Suite	21
Gambar 2.12. Metasploit	22
Gambar 2.13. Metode ISSAF	23
Gambar 3.1. Alur Penelitian	38
Gambar 3.2. Kerangka ISSAF	39
Gambar 4.1. Website Lapormasbup	47
Gambar 4.2. Informasi IP Address	47
Gambar 4.3. Informasi dengan tools Whois	48
Gambar 4.4. Informasi dengan tools DnsDumpster	49
Gambar 4.5. Teknologi Web dengan tools Whatweb	50
Gambar 4.6. Hasil scanning dengan tools Nmap	51
Gambar 4.7. Hasil Alerts Pemindaian Kerentanan	53
Gambar 4.8. Pengujian CSRF	59
Gambar 4.9. Hasil Pengujian CSRF	59

Gambar 4.10. Hasil Pengujian XSS	60
Gambar 4.11. Hasil Pengujian SQL <i>Injection</i>	61
Gambar 4.12. Hasil Scanning SSH dengan Metasploit.....	63
Gambar 4.13. Halaman <i>Login</i> Lapormasbup	64
Gambar 4.14. Request HTTP	65
Gambar 4.15. Hasil Serangan <i>Brute Force</i>	66
Gambar 4.16. Percobaan <i>Remote</i>	66
Gambar 4.17. Hasil Pengujian Eksploitasi Struts2	68
Gambar 4.18. Penelusuran <i>Log Authentication</i>	68
Gambar 4.19. Penghapusan <i>Log Authentication</i>	69



DAFTAR LAMPIRAN

- Lampiran 1. Surat Izin Penelitian
- Lampiran 2. Hasil Wawancara
- Lampiran 3. Rekap Aduan Masyarakat
- Lampiran 4. Total Pengunjung Lapormasbup
- Lampiran 5. Grafik Pengunjung Lapormasbup
- Lampiran 6. Total Serangan Lapormasbup
- Lampiran 7. Grafik Serangan Lapormasbup
- Lampiran 8. Dokumentasi Wawancara
- Lampiran 9. Website Lapormasbup
- Lampiran 10. Kartu Bimbingan Dosen Pembimbing 1
- Lampiran 11. Kartu Bimbingan Dosen Pembimbing 2