

## DAFTAR ISI

HALAMAN SAMBUTAN .....	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
<i>ABSTRACT</i> .....	xvii
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah .....	1
B. Rumusan Masalah.....	6
C. Batasan Masalah .....	6
D. Tujuan Penelitian .....	7
E. Manfaat Penelitian .....	7
BAB II TINJAUAN PUSTAKA.....	9
A. Landasan Teori.....	9
B. Penelitian Sebelumnya.....	25
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 .....	34
BAB IV HASIL DAN PEMBAHASAN .....	46

A. <i>Planning and Preparation</i> .....	46
B. <i>Assessment</i> .....	50
C. <i>Reporting, Clean Up and Destroy Artifacts</i> .....	89
BAB V PENUTUP.....	97
A. Kesimpulan .....	97
B. Saran .....	98

DAFTAR PUSTAKA

LAMPIRAN



## DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya.....	28
Tabel 4. 1 Hasil Scan Menggunakan Whois .....	52
Tabel 4. 2 Hasil Ping pada Subdomain .....	58
Tabel 4. 3 Domain dan Teknologi.....	61
Tabel 4. 4 Hasil Scanning pada Ejournal .....	63
Tabel 4. 5 Hasil Scanning pada SIAKAD.....	63
Tabel 4. 6 Hasil Scanning pada Repository .....	63
Tabel 4. 7 Hasil Scanning pada LMS.....	64
Tabel 4. 8 Hasil Scanning Perpustakaan .....	64
Tabel 4. 9 Hasil Vulnerability Scanning Ejournal .....	67
Tabel 4. 10 Hasil Vulnerability Scanning SIAKAD.....	69
Tabel 4. 11 Hasil Vulnerability Scanning Repository .....	70
Tabel 4. 12 Hasil Vulnerability Scanning LMS .....	71
Tabel 4. 13 Hasil Vulnerability Scanning Perpustakaan.....	73
Tabel 4. 14 Pengujian Reflected XSS .....	77
Tabel 4. 15 Hasil Penetration Testing Ejournal .....	77
Tabel 4. 16 Hasil Penetration Testing SIAKAD .....	78
Tabel 4. 17 Hasil Penetration Testing Repository .....	78
Tabel 4. 18 Hasil Penetration Testing LMS.....	79
Tabel 4. 19 Hasil Penetration Testing Perpustakaan.....	79
Tabel 4. 20 Rekomendasi Perbaikan 5 Subdomain.....	93

## DAFTAR GAMBAR

Gambar 2. 1 Metodologi ISSAF .....	15
Gambar 3. 1 Kerangka Berfikir.....	34
Gambar 4. 1 Website Utama STT .....	51
Gambar 4. 2 Mencari Informasi IP Adress menggunakan ping.....	51
Gambar 4. 3 Menggali Informasi dengan Tools Whois.....	52
Gambar 4. 4 Hasil Enumerasi Menggunakan Dnsrecon .....	53
Gambar 4. 5 Hasil Scanning Menggunakan Dnsdumpster .....	54
Gambar 4. 6 Website Ejournal .....	55
Gambar 4. 7 Website SIAKAD.....	55
Gambar 4. 8 Website Repository .....	56
Gambar 4. 9 Website LMS .....	56
Gambar 4. 10 Website Perpustakaan .....	57
Gambar 4. 11 Website PMB .....	57
Gambar 4. 12 Ping Pada Ejournal.....	58
Gambar 4. 13 Hasil Scanning Menggunakan Dnsrecon .....	59
Gambar 4. 14 Hasil Scan Menggunakan Whatweb .....	60
Gambar 4. 15 Hasil Scan menggunakan Wappalyzer.....	60
Gambar 4. 16 Scanning Port Menggunakan Nmap.....	62
Gambar 4. 17 Proses Automated Scan vulnerability .....	66
Gambar 4. 18 Kerentanan yang Diperoleh.....	66
Gambar 4. 19 Serangan XSS pada URL .....	76
Gambar 4. 20 Perintah Injeksi menggunakan SQLmap.....	76
Gambar 4. 21 Scanner menggunakan Metasploit .....	81
Gambar 4. 22 SSH Login menggunakan Metasploit .....	82
Gambar 4. 23 Input Username dan Password .....	83
Gambar 4. 24 Request Masuk .....	83
Gambar 4. 25 Snipper Attack.....	84
Gambar 4. 26 Hasil Snipper Attack .....	85
Gambar 4. 27 Percobaan Input.....	85

Gambar 4. 28 Perobaan Remote.....	86
Gambar 4. 29 Proses Eksploitasi.....	87
Gambar 4. 30 Isi auth.log .....	88
Gambar 4. 31 Proses penghapusan .....	88
Gambar 4. 32 Hasil Covering Tracks.....	89
Gambar 4. 33 Clean Up & Destroy Artifacts.....	96



## **DAFTAR LAMPIRAN**

Lampiran 1. Kartu Bimbingan

Lampiran 2. Surat Izin Penelitian

Lampiran 3 Surat diizinkan Melakukan Penelitian

Lampiran 4. Wawancara dengan Pengelola Website STT Wiworotomo

Lampiran 5. Hasil Wawancara

