

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR	i
PENGESAHAN PENGUJI SIDANG TUGAS AKHIR.....	ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR.....	iii
ABSTRAK	v
MOTTO DAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
I. BAB I	I-1
PENDAHULUAN	I-1
1.1. Latar Belakang	I-1
1.2. Rumusan Masalah	I-4
1.3. Tujuan Penelitian.....	I-4
1.4. Manfaat Penelitian.....	I-4
1.5. Batasan Masalah.....	I-5
II. BAB II	II-1
LANDASAN TEORI.....	II-1
2.1 Keamanan Informasi	II-1
2.2 Keamanan Web	II-2
2.3 <i>Vulnerability Assessment</i>	II-3
2.4 <i>Penetration Testing</i>	II-4
2.5 <i>SQL Injection</i>	II-5
2.6 <i>Tools</i> Eksploitasi Dan Pemindaian.....	II-6
2.11 Tabel Matriks Penelitian	II-8
2.12 Tabel <i>Literatur Review</i>	II-14
III. BAB III	III-1
METODOLOGI PENELITIAN.....	III-1
3.1 Pendekatan Penelitian.....	III-1
3.2 Diagram Alur Penelitian.....	III-1

3.3	<i>Studi Literatur</i>	III-2
3.4	Persiapan Sistem.....	III-2
3.5	Observasi dan <i>Information Gathering</i>	III-3
3.6	<i>Vulnerability Scanning</i>	III-3
3.7	Eksplorasi Kerentanan	III-4
3.8	Dokumentasi Dan Laporan.....	III-5
IV.	BAB IV	IV-1
	HASIL DAN PEMBAHASAN.....	IV-1
4.2	Hasil <i>Vulnerability Scanning</i> Aplikasi Web.....	IV-5
4.4	Hasil Eksploitasi <i>SQL Injection</i>	IV-14
4.5	Validasi Hasil Eksploitasi	IV-20
4.6	Analisis Kerentanan Keamanan	IV-23
4.7	Rekomendasi Mitigasi.....	IV-25
4.8	Evaluasi Eksploitasi <i>SQL Injection</i> dengan <i>Sqlmap</i> pada Aplikasi Web	IV-31
4.9	Evaluasi Efektivitas Teknik <i>Boolean -Based Blind</i> Dan <i>Time-Based Blind</i> <i>Sql Injection</i>	IV-32
V.	BAB V	V-1
	KESIMPULAN DAN SARAN.....	V-1
5.1	Kesimpulan.....	V-1
5.2	Saran	V-2
	DAFTAR PUSTAKA	V-1
	LAMPIRAN	1

DAFTAR TABEL

Tabel 2. 1 Matriks penelitian Terkait	II-8
Tabel 2. 2 Tabel Literatur Review	II-14
Tabel 4. 1 Hasil Scanning Menggunakan Nmap.....	IV-1
Tabel 4. 2 Hasil Scanning Vulnerability Menggunakan Nikto.....	IV-6
Tabel 4. 3 Hasil Vulnerability Scanning OWASP ZAP.....	IV-9
Tabel 4. 4 Persentase Kerentanan Pada OWASP ZAP	IV-13
Tabel 4. 5 Tabel Password user Hasil Hash Website.....	IV-22
Tabel 4. 6 Verifikasi Login Pada Website	IV-23
Tabel 4. 7 Analisis Masalah Keamanan	IV-24
Tabel 4. 8 Rekomendasi Mitigasi <i>Vulnerability Scanning</i> OWASP ZAP	IV-26
Tabel 4. 9 rekomendasi mitigasi vulnerability scanning nikto.....	IV-28
Tabel 4. 10 Rekomendasi Mitigasi Hasil Eksploitasi.....	IV-29
Tabel 4. 11 hasil eksploitasi sqlmap	IV-31
Tabel 4. 12 Perbedaan Teknik serangan SQL Injection	IV-33

DAFTAR GAMBAR

Gambar 3. 1 Diagram Alur Penelitian.....	III-1
Gambar 3. 2 Alur Pengujian menggunakan SQLMap	III-4
Gambar 4. 1 Scanning Menggunakan Nmap	IV-1
Gambar 4. 2 Scanning Menggunakan Nslookup.....	IV-3
Gambar 4. 3 Uji Konektivitas Menggunakan Ping	IV-4
Gambar 4. 4 Scanning Vulnerability Menggunakan Nikto	IV-5
Gambar 4. 5 Scanning Dengan OWASP ZAP.....	IV-9
Gambar 4. 6 Eksploitasi Untuk Menemukan Kerentanan Menggunakan Sqlmap	IV-15
Gambar 4. 7 Identifikasi Kerentanan Form login Oleh Sqlmap	IV-15
Gambar 4. 8 Identifikasi Form login Dengan Sqlmap	IV-16
Gambar 4. 9 Hasil Identifikasi Kerentanan Sql Injection Menggunakan Sqlmap	IV-17
Gambar 4. 10 Daftar Database Pada Website	IV-19
Gambar 4. 11 Daftar Tabel Pada Database Pertama.....	IV-19
Gambar 4. 12 Isi Tabel user database dinsos	IV-20
Gambar 4. 13 Identifikasi Jenis Password Hash	IV-20
Gambar 4. 14 Hasil Hash Password Admin	IV-21
Gambar 4. 15 Hasil Hash Password Operator.....	IV-21
Gambar 4. 16 Tampilan Pada Website Dengan User Admin	IV-22
Gambar 4. 17 Tampilan Website Dengan User Operator	IV-23