

## DAFTAR ISI

LEMBAR PERNYATAAN KEASLIAN .....	II
HALAMAN PENGESAHAN TUGAS AKHIR .....	III
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	IV
KATA PENGANTAR .....	V
ABSTRAK .....	VII
DAFTAR ISI .....	VIII
DAFTAR TABEL .....	XI
DAFTAR GAMBAR .....	XII
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah.....	5
1.4 Tujuan Penelitian.....	6
1.5 Manfaat Penelitian.....	6
1.6 Metodologi Penelitian.....	6
1.6.1 Pengecekan alamat <i>IP</i> .....	6
1.6.2 <i>Footprinting</i> .....	7
1.6.3 <i>Scanning</i> .....	7
1.6.4 Uji <i>Penetration</i> .....	7
1.6.5 Pembuatan Laporan Pengujian .....	7
1.7 Sistematika Penulisan .....	7
BAB I PENDAHULUAN .....	8
BAB II LANDASAN TEORI .....	8
BAB III METODOLOGI.....	8
BAB IV HASIL DAN PEMBAHASAN .....	8
BAB V KESIMPULAN DAN SARAN.....	8
BAB II.....	9
LANDASAN TEORI.....	9
2.1 Kajian Pustaka .....	9
2.2 Dasar Teori.....	11

2.2.1	Keamanan Informasi.....	11
2.2.2	<i>Penetration Testing</i> .....	13
2.2.3	<i>Information Gathering (Footprinting)</i> .....	14
2.2.4	<i>IP Delegation</i> .....	14
2.2.5	<i>Server Check</i> .....	14
2.2.6	<i>Client Side Check</i> .....	15
2.2.7	Alamat <i>IP</i> .....	15
2.2.8	<i>Vulnerability Identification</i> .....	15
2.2.9	<i>Trace Path (Traceroute)</i> .....	15
2.2.10	<i>Network Mapping (Network Scanner)</i> .....	16
2.2.11	<i>Nikto</i> .....	16
2.3	<i>Open Web Application Security Project (OAWSP)</i> .....	16
2.3.1	<i>OWASP TOP 10</i> .....	17
2.4	<i>Scanning Tools</i> .....	18
2.4.1	<i>The Harvester</i> .....	19
2.4.2	<i>Nmap</i> .....	19
2.4.3	<i>Masscan</i> .....	20
2.4.4	<i>Web Analysis Scanning</i> .....	20
2.4.5	<i>OWASPZap</i> .....	20
BAB III .....		21
METODE PENELITIAN.....		21
3.1	Metode Penelitian .....	21
3.2	Alat Kebutuhan Penelitian .....	21
3.2.1	Alur Penelitian.....	22
3.2.1.1	Studi Literatur .....	23
3.2.1.2	Wawancara.....	23
3.3	Kebutuhan Aplikasi .....	23
3.3.1	Otomatisasi <i>OWASPZap</i> .....	23
3.3.2	Pseudocode.....	25
3.4	Analisis .....	26
3.5	Rekomendasi .....	27
BAB IV .....		28
HASIL DAN PEMBAHASAN .....		28
4.1	Data Hasil Penelitian .....	28
4.1.1	Hasil Wawancara.....	28

4.2	Hasil Obsevasi .....	28
4.3	Hasil <i>Footprinting</i> .....	29
4.4	Hasil <i>Scanning IP</i> .....	34
4.5	<i>Graining Access</i> .....	38
BAB V .....		42
HASIL DAN KESIMPULAN.....		42
5.1	Kesimpulan .....	42
5.3	Saran .....	43
DAFTAR PUSTAKA.....		44

**DAFTAR TABEL**

Tabel 2.1 Jurnal terkait.....	9
Tabel 3.1 Spesifikasi perangkat penelitian.....	21
Tabel 3.2 <i>Library</i> .....	25
Tabel 3.3 Pseudocode Aplikasi Otomatisasi <i>OWASPZap</i> .....	26

## DAFTAR GAMBAR

Gambar 1.1 Jumlah pengguna internet menurut APJII pada tahun 2016.....	1
Gambar 1.2 Jumlah pengguna internet pada tahun 2016 .....	2
Gambar 2.1 <i>Penetration testing phase</i> .....	13
Gambar 2.2 <i>Penetration testing proses (learn-penetration-testing, n.d.)</i> .....	14
Gambar 2.3 contoh <i>OWASP 10</i> .....	17
Gambar 2.4 <i>Compare version 2013 - 2017</i> .....	19
Gambar 3.1 Diagram alur <i>penetration testing</i> pada domain siakad.esaunggul.ac.id.ac.id .....	22
Gambar 3.2 <i>Flowchart</i> aplikasi Otomatisasi <i>OWASPZap</i> .....	24
Gambar 4.1 <i>Background Check</i> .....	29
Gambar 4.2 Pengecekan <i>IP</i> .....	30
Gambar 4.3 <i>Server Check</i> .....	30
Gambar 4.4 <i>Client Side Check</i> .....	31
Gambar 4.5 <i>IP Information</i> .....	32
Gambar 4.6 <i>Vulnerabel Check</i> .....	32
Gambar 4.7 <i>Trace Path Check</i> .....	33
Gambar 4.8 <i>Port Scanner</i> .....	34
Gambar 4.9 <i>Nikto Vulnerability Scanner</i> .....	35
Gambar 4.10 <i>OwaspZap Vulnerability Scanner</i> .....	35
Gambar 4.11 Normal Siakad .....	36
Gambar 4.12 Buq pada siakad.....	37
Gambar 4.13 Percobaan Dump Database.....	38
Gambar 4.14 Hasil dari Dump Database.....	39
Gambar 4.15 <i>DB_Gate_Siakad</i> .....	39
Gambar 4.16 Data <i>Encryption Password DB &amp; Nim</i> .....	40
Gambar 4.17 <i>DB_Akademik_Siakad</i> .....	41