

## DAFTAR ISI

ABSTRAK.....	i
ABSTRACT .....	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR TABEL .....	vi
DAFTAR GAMBAR.....	vii
DAFTAR LAMPIRAN .....	viii
DAFTAR ISTILAH .....	ix
BAB 1    PENDAHULUAN .....	1-1
1.1 Latar Belakang .....	1-1
1.2 Identifikasi Masalah .....	1-2
1.3 Tujuan Tugas Akhir.....	1-2
1.4 Lingkup Tugas Akhir.....	1-2
1.5 Metodologi Tugas Akhir.....	1-2
1.6 Sistematis Penulisan Tugas Akhir .....	1-4
BAB 2    LANDASAN TEORI.....	2-1
2.1 <i>Cyber Security</i> .....	2-1
2.2    Katagori <i>Cyber Crime</i> .....	2-1
2.2.1 Bentuk bentuk <i>Cyber Crime</i> .....	2-1
2.3    Keamanan Sistem Informasi Internet.....	2-2
2.3.1 Keamanan <i>Server WWW</i> .....	2-2
2.4    Peretasan Web .....	2-2
2.5 <i>SQL-Injection</i> .....	2-2
2.5.1 Testing <i>SQL-Injection</i> .....	2-3
2.6    Pencegahan Serangan <i>SQL-Injection</i> .....	2-4
2.7 <i>Penetration Testing</i> .....	2-5
2.7.1 Teknik <i>Penetration Testing</i> .....	2-5
2.7.2 Jenis <i>Penetration Testing</i> .....	2-6
2.7.3 Metode Black Box.....	2-6
2.8    Macam – macam <i>Tools</i> .....	2-8
2.9    OWASP (Open Web Application Security Project) Top 10-2017 .....	2-9
2.9.1    A1- <i>Injection</i> .....	2-10
2.9.2    A2- Broken Authentication.....	2-10
2.9.3    A3- Sensitive Data Exposure .....	2-10
2.9.4    A4- XML External Entities (XXE) .....	2-11
2.9.5    A5- Broken Access Control .....	2-11
2.9.6    A6- Security Misconfiguration.....	2-12
2.9.7    A7- Cross-site Scripting (XSS) .....	2-12

2.9.8	A8- Insecure Deserialization.....	2-13
2.9.9	A9- Using Components with Known Vulnerabilities .....	2-13
2.9.10	A10- Insufficient Logging & Monitoring .....	2-14
2.10	Penelitian Terdahulu.....	2-14
BAB 3	SKEMA PENELITIAN .....	3-1
3.1	Alur Penyelesaian Tugas Akhir .....	3-1
3.2	Perumusan Masalah .....	3-3
3.2.1	Analisis Sebab Akibat.....	3-4
3.2.2	Solusi Masalah .....	3-4
3.3	Kerangka Pemikiran Teoritis.....	3-6
3.3.1	Skema Analisis.....	3-6
3.4	Tempat dan Objek Penelitian .....	3-8
3.4.1	Sejarah Fakultas Teknik.....	3-8
3.4.2	Struktur Organisasi.....	3-9
3.4.3	Deskripsi Tugas dan Tanggung Jawab.....	3-9
BAB 4	ANALISIS DAN PENGUJIAN .....	4-1
4.1	Analisis Celah Keamanan .....	4-1
4.1.1	Pengumpulan Informasi Pada Web Aplikasi SitU Akademik Unpas .....	4-1
4.1.2	WHOIS .....	4-1
4.1.3	NMAP .....	4-4
4.1.4	OS Fingerprinting.....	4-6
4.1.5	Celah Keamanan Pada Web Aplikasi Yang Akan Di Uji Coba .....	4-7
4.1.6	Celah Keamanan Berdasarkan <i>Tools OWASP-ZAP</i> .....	4-17
4.2	Pengujian <i>Web</i> Aplikasi Situ Aplikasi Akademik Menggunakan <i>Tools SQL-MAP</i> .....	4-24
4.2.1	Skenario Percobaan Pengujian .....	4-24
4.2.2	Tahapan Pengujian Menggunakan <i>SQL-MAP</i> .....	4-24
4.2.3	Hasil Pengujian Menggunakan <i>SQL-MAP</i> .....	4-33
BAB 5	EVALUASI DAN REKOMENDASI .....	5-1
5.1	Evaluasi.....	5-1
5.2	Rekomendasi.....	5-3
BAB 6	PENUTUP.....	6-1
6.1	Kesimpulan .....	6-1
6.2	Saran .....	6-1
DAFTAR PUSTAKA.....		6-1
LAMPIRAN .....		6-2
LAMPIRAN A	BERITA ACARA WAWANCARA .....	A-1
LAMPIRAN B	TAHAPAN <i>PENETRATION TESTING SQL-INJECTION</i> .....	B-1
LAMPIRAN C	HASIL <i>PENETRATION TESTING</i> WEB APLIKASI SITU AKADEMIK UNPAS .C-6	C-6