

**ANALISIS KERENTANAN SISTEM INFORMASI AKADEMIK
BERBASIS *WEBSITE* MENGGUNAKAN VAPT DAN ZAP DI
UNIVERSITAS LAMBUNG MANGKURAT**

SKRIPSI

Oleh:

MUHAMMAD HIDAYATULLAH

NIM 2010817110012



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS LAMBUNG MANGKURAT
BANJARMASIN
2024**

**ANALISIS KERENTANAN SISTEM INFORMASI AKADEMIK
BERBASIS *WEBSITE* MENGGUNAKAN VAPT DAN ZAP DI
UNIVERSITAS LAMBUNG MANGKURAT**

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat
Sarjana Strata-1 Teknologi Informasi

Oleh:

MUHAMMAD HIDAYATULLAH

NIM 2010817110012



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS LAMBUNG MANGKURAT
BANJARMASIN
2024**

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

SKRIPSI PROGRAM STUDI S-1 TEKNOLOGI INFORMASI

Analisis Kerentanan Sistem Informasi Akademik Berbasis Website Menggunakan
VAPT dan ZAP di Universitas Lambung Mangkurat

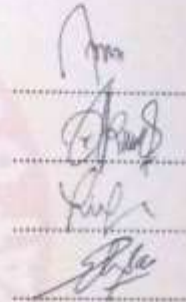
Oleh

Muhammad Hidayatullah (2010817110012)

Telah dipertahankan di depan Tim Penguji pada 07 Oktober 2024 dan dinyatakan

LULUS

Komite Penguji :
Ketua : Andreyan Rizky Baskara, S.Kom., M.Kom.
NIP. 199307032019031011
Anggota 1 : Nurul Fathanah Mustamin, S.Pd., M.T.
NIP. 199110252019032018
Anggota 2 : Muhammad Fajrian Noor, S.Kom., M.Kom.
NIP. 198904162024211002
Pembimbing
Utama : Ir. Eka Setya Wijaya, S.T., M.Kom.
NIP. 198205082008011010



07 OCT 2024

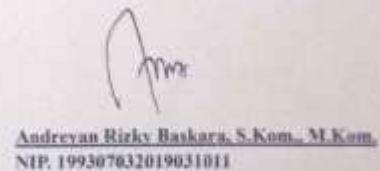
Banjarnbaru,
Diketahui dan disahkan oleh:

Wakil Dekan Bidang Akademik
Fakultas Teknik ULM,



Dr. Mahmud S.L., M.T.
NIP. 197401071998021001

Koordinator Program Studi
S-1 Teknologi Informasi,



Andreyan Rizky Baskara, S.Kom., M.Kom.
NIP. 199307032019031011

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini,

Nama : Muhammad Hidayatullah
NIM : 2010817110012
Fakultas : Teknik
Prodi : Teknologi Informasi
Judul Tugas Akhir : Analisis Kerentanan Sistem Informasi Akademik Berbasis Website Menggunakan VAPT dan ZAP di Universitas Lambung Mangkurat
Pembimbing Utama : Ir. Eka Setya Wijaya, S.T., M.Kom.

Dengan ini saya menyatakan bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar akademik di suatu perguruan tinggi, dan sepanjang pengetahuan saya, juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar rujukan.

Banjarmasin, 3 Oktober 2024

Penulis,



Muhammad Hidayatullah

LEMBAR PERSETUJUAN SKRIPSI

PERSETUJUAN SKRIPSI

ANALISIS KERENTANAN SISTEM INFORMASI AKADEMIK BERBASIS
WEBSITE MENGGUNAKAN VAPT DAN ZAP DI UNIVERSITAS
LAMBUNG MANGKURAT

OLEH
MUHAMMAD HIDAYATULLAH
NIM.2010817110012

Telah diperiksa dan terpenuhi semua persyaratan akademik, administrasi, dan
disetujui untuk dipertahankan di hadapan dewan penguji

Banjarmasin, 3 Oktober 2024

Pembimbing Utama,



Ir. Eka Setya Wijaya, S.T., M.Kom.

NIP. 198205082008011010

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada Sistem Informasi Akademik di Universitas Lambung Mangkurat. Dengan menggunakan metode *Vulnerability Assessment* dan *Penetration Testing* serta alat utama menggunakan ZAP dan OpenVAS, penelitian ini mengevaluasi celah keamanan pada tiga *website* utama Sistem Informasi Akademik, yaitu Simari ULM, *E-Learning* ULM, dan Portal Akademik Mahasiswa ULM. Hasil analisis menunjukkan adanya berbagai kerentanan dengan tingkat risiko yang berbeda, mulai dari tinggi hingga rendah. Penelitian ini juga memberikan rekomendasi untuk meningkatkan keamanan sistem dan mengurangi risiko yang terkait. Dengan demikian, penelitian ini berkontribusi pada penguatan keamanan sistem informasi di lingkungan akademik untuk menjaga kerahasiaan, integritas, dan ketersediaan data.

Kata kunci: Keamanan *Website*, OpenVAS, *Penetration Testing*, Sistem Informasi Akademik, *Vulnerability Assessment*, ZAP.

ABSTRACT

This research aims to identify and analyze vulnerabilities in the Academic Information System at Universitas Lambung Mangkurat. Using Vulnerability Assessment and Penetration Testing methodologies along with key tools like ZAP and OpenVAS, this study evaluates the security gaps in three Information System main websites: Simari ULM, E-Learning ULM, and the Portal Akademik Mahasiswa ULM. The analysis reveals various vulnerabilities with differing risk levels, ranging from high to low. This research also provides recommendations to enhance system security and mitigate associated risks. Consequently, this study contributes to strengthening information security in the academic environment to safeguard the confidentiality, integrity, and availability of data.

Keywords: Academic Information System, OpenVAS, Penetration Testing, Vulnerability Assessment, Web security, ZAP.

KATA PENGANTAR

Dengan penuh rasa syukur, saya memanjatkan puji kepada Allah SWT, Tuhan Yang Maha Pemurah, atas segala nikmat yang telah diberikan. Semua harapan dan cita-cita saya menjadi lebih mudah tercapai berkat karunia-Nya. Shalawat serta salam saya sampaikan kepada Nabi Muhammad SAW, yang telah membimbing umat menuju jalan yang benar. Atas izin-Nya, saya dapat menyelesaikan skripsi ini yang berjudul: "Analisis Kerentanan Sistem Informasi Akademik Berbasis Website Menggunakan VAPT dan ZAP di Universitas Lambung Mangkurat". Skripsi ini diajukan sebagai salah satu syarat untuk meraih gelar Sarjana Strata-1 di bidang Teknologi Informasi, Fakultas Teknik, Universitas Lambung Mangkurat, Banjarmasin.

Pada kesempatan ini, saya ingin menyampaikan rasa terima kasih yang mendalam kepada:

1. Bapak Andreyan Rizky Baskara, S.Kom., M.Kom., selaku Ketua Program Studi Teknologi Informasi, atas bimbingan dan arahannya.
2. Bapak Prof. Juhriyansyah Dalle, S.Pd., S.Si., M.Kom., Ph.D., sebagai Dosen Pembimbing Akademik, yang telah memberikan waktu dan bimbingan selama perkuliahan.
3. Bapak Eka Setya Wijaya, S.T., M.Kom., selaku Dosen Pembimbing Utama, atas arahan dan waktu yang diberikan dalam penyelesaian skripsi ini.
4. Para dosen dan staf Program Studi Teknologi Informasi, serta teman-teman yang telah membantu dalam proses penyelesaian skripsi.
5. Keluarga dan orang tua yang selalu memberikan dukungan, doa, dan motivasi demi kelancaran penyusunan skripsi ini.

Sebagai penutup, saya mengucapkan terima kasih kepada semua pihak yang telah membantu saya dalam menyelesaikan skripsi ini. Saya berharap skripsi ini dapat memberikan manfaat, baik bagi diri saya, teman-teman, maupun para pembaca. Saya juga sangat terbuka terhadap kritik dan saran yang membangun untuk

perbaikan di masa mendatang. Semoga skripsi ini bermanfaat bagi semua pihak yang membutuhkan.

Banjarmasin, 3 Oktober 2024

Penulis

A handwritten signature in black ink, appearing to be 'M. Hidayatullah', written in a cursive style.

Muhammad Hidayatullah

DAFTAR ISI

HALAMAN SAMPUL LUAR.....	i
HALAMAN SAMPUL DALAM.....	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN	iv
LEMBAR PERSETUJUAN SKRIPSI.....	v
ABSTRAK	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN	xvii
DAFTAR RIWAYAT HIDUP.....	xx
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian.....	7
1.5 Manfaat Penelitian.....	7
BAB II TINJAUAN PUSTAKA	9
2.1 Landasan Teori	9
2.1.1 Keamanan Sistem Informasi.....	9
2.1.2 Sistem Informasi Akademik ULM berbasis <i>Website</i>	9
2.1.3 Ancaman	13
2.1.4 Kerentanan	14
2.1.5 <i>Open Web Applications Security Project</i>	15
2.1.6 ZAP.....	16
2.1.7 OpenVas	19
2.1.8 <i>Web Security Testing Guide (WSTG)</i>	20
2.1.9 <i>Penetration Testing</i>	21
2.1.10 <i>Vulnerability Assessment</i>	22

2.1.11 Perbandingan Metodologi Pengujian Keamanan.....	22
2.2 Penelitian Terkait.....	25
2.2.1 Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik (2022).....	25
2.2.2 <i>Vulnerability Assessment</i> Untuk Meningkatkan Kualitas Keamanan Web (2021).....	25
2.2.3 Analisis Keamanan Website <i>Open Journal System</i> Menggunakan Metode <i>Vulnerability Assessment</i> (2020).....	26
2.2.4 Analisis Keamanan Sistem Informasi Akademik Berbasis <i>Web</i> Menggunakan <i>Framework</i> ISSAF (2023)	26
2.2.5 <i>Vulnerability Assessment Website E-Government</i> dengan NIST SP 800-115 dan OWASP Menggunakan <i>Web Vulnerability Scanner</i> (2022)	27
2.3 Kerangka Berpikir	33
BAB III METODOLOGI PENELITIAN.....	34
3.1 Alat Penelitian	34
3.2 Bahan Penelitian.....	36
3.3 Alur Penelitian.....	36
3.3.1 Identifikasi Masalah.....	37
3.3.2 Studi Literatur	37
3.3.3 Uji <i>Vulnerability Assessment</i>	38
3.3.4 Rekomendasi dan Perbaikan	40
3.3.5 Verifikasi Perbaikan	40
3.4 Metode Pengumpulan Data	40
3.4.1 Observasi Sistem Informasi Akademik	41
3.4.2 Pemindaian dan Pengujian Potensial Celah.....	41
3.4.3 Identifikasi Kerentanan.....	41
3.4.4 Pengumpulan Data Kualitatif dan Kuantitatif	41
3.4.5 Dokumentasi	42
3.4.6 Mematuhi Etika dan Menjaga Keamanan.....	45
BAB IV HASIL DAN PEMBAHASAN.....	46
4.1 Pengintiaan	46
4.2 Pemindaian Kerentanan.....	48

4.3 Analisis dan Perencanaan Informasi.....	58
4.4 Pengujian Penetrasi	64
4.4 Analisis Hasil.....	85
BAB V KESIMPULAN DAN SARAN.....	87
5.1 Kesimpulan.....	87
5.2 Saran	88
DAFTAR PUSTAKA	89
LAMPIRAN.....	94

DAFTAR TABEL

Tabel 1.1 <i>Outdated Software</i> yang masih digunakan di objek penelitian	3
Tabel 1. 2 Alert yang teridentifikasi di sistem Simari ULM	4
Tabel 1. 3 Alert yang teridentifikasi di sistem <i>E-Learning</i> ULM	4
Tabel 1. 4 Alert yang teridentifikasi di sistem Portal Akademik Mahasiswa ULM	5
Tabel 2.1 Kriteria matriks perbandingan <i>tools pentesting</i> [16].....	17
Tabel 2.2 Perbandingan Metodologi Penelitian	23
Tabel 2.3 Perbandingan Penelitian-Penelitian Terdahulu Dengan Penelitian Yang Dilakukan	29
Tabel 3.1 Alat Penelitian	34
Tabel 3.2 Pelingkupan.....	39
Tabel 3.3 Perbandingan Template Dokumentasi Laporan Kerentanan	42
Tabel 4.1 Informasi dasar website sistem informasi ULM	47
Tabel 4.2 Hasil scanning website Simari ULM menggunakan ZAP	48
Tabel 4.3 Rekapitulasi hasil scanning pada Simari ULM Menggunakan ZAP.....	49
Tabel 4.4 Hasil scanning website E-Learning ULM menggunakan ZAP	50
Tabel 4.5 Rekapitulasi hasil scanning pada E-Learning ULM Menggunakan ZAP	51
Tabel 4.6 Hasil scanning website Portal Akademik Mahasiswa ULM menggunakan ZAP	51
Tabel 4.7 Rekapitulasi hasil scanning pada Portal Akademik Mahasiswa ULM Menggunakan ZAP	52
Tabel 4.8 Hasil scanning website Simari ULM menggunakan OpenVAS.....	52
Tabel 4.9 Rekapitulasi hasil scanning pada Simari ULM Menggunakan OpenVAS	53
Tabel 4.10 Hasil scanning website E-Learning ULM menggunakan OpenVAS ..	53
Tabel 4.11 Rekapitulasi hasil scanning pada E-Learning ULM Menggunakan OpenVAS.....	55
Tabel 4.12 Hasil scanning website Portal Akademik Mahasiswa ULM menggunakan OpenVAS	56
Tabel 4. 13 Rekapitulasi hasil scanning pada Portal Akademik Mahasiswa ULM Menggunakan OpenVAS.....	57

Tabel 4.14 Rekapitulasi hasil scanning Sistem Informasi Akademik ULM menggunakan ZAP.....	58
Tabel 4.15 Rekapitulasi hasil scanning Sistem Informasi Akademik ULM menggunakan OpenVAS	58
Tabel 4.16 Standar keamanan internasional OWASP WSTG versi 4.2	59
Tabel 4.17 Hasil pengujian OWASP WSTG versi 4.2	82

DAFTAR GAMBAR

Gambar 1. 1 Serangan peretasan pada salah satu <i>web</i> profil prodi milik ULM.....	2
Gambar 1. 2 Total objek penelitian yang paling sering diakses.....	3
Gambar 2. 1 Simari ULM	10
Gambar 2. 2 Berbagai aplikasi sistem informasi akademik yang saling terkoneksi	11
Gambar 2. 3 <i>E-Learning</i> ULM.....	12
Gambar 2. 4 Portal Akademik Mahasiswa ULM.....	13
Gambar 2. 5 Alur Proses ZAP [15]	16
Gambar 2. 6 Tampilan ZAP	17
Gambar 2.7 <i>Metrics Score Non-Commercial Tools</i> [16].....	18
Gambar 2.8 Alur Proses OpenVAS [18]	19
Gambar 2.9 Tampilan OpenVAS.....	20
Gambar 2.10 Kerangka Berpikir	33
Gambar 3.1 Alur Penelitian.....	36
Gambar 3.2 Uji <i>Vulnerability Assessment</i>	38
Gambar 3.3 Metode Pengumpulan Data	40
Gambar 3.4 Gambaran <i>Cover</i> dan Daftar Isi Laporan	43
Gambar 3.5 Gambaran Ringkasan Eksekutif dan Pelingkupan Laporan.....	43
Gambar 3.6 Gambaran Pendekatan dan Metodologi Laporan.....	44
Gambar 3.7 Gambaran Informasi Kontak dan Temuan Utama Laporan	44
Gambar 3.8 Gambaran Temuan Terperinci Beserta Langkah-langkah Penemuan Kerentanan	45
Gambar 4.1 Kerentanan Generic Padding Oracle di Simari ULM	64
Gambar 4.2 Request dan Response HTTP yang Normal.....	65
Gambar 4.3 Response HTTP ketika padding yang tidak valid dikirimkan.....	66
Gambar 4.4 Analisis response Active Scan kerentanan Generic Padding Oracle menggunakan ZAP.....	67
Gambar 4.5 Perbandingan padding yang asli dengan padding yang telah dimodifikasi oleh ZAP	67
Gambar 4.6 Eksploitasi kerentanan kriptografi Generic Padding Oracle (Cipher Value 1)	68

Gambar 4.7 Kerentanan SQL Injection - SQLite di Simari ULM	69
Gambar 4.8 Request dan Response HTTP dengan original value	71
Gambar 4.9 Request dan Response HTTP menggunakan payload SQLi	71
Gambar 4.10 Request dan Response HTTP menggunakan payload SQLi tambahan	72
Gambar 4.11 Eksploitasi kerentanan SQL Injection - SQLite dengan tool sqlmap	72
Gambar 4.12 Kerentanan PII Disclosure di E-Learning ULM	74
Gambar 4.13 Angka yang diidentifikasi ZAP sebagai PII	75
Gambar 4.14 Kode mata kuliah yang teridentifikasi sebagai PII.....	75
Gambar 4.15 Kerentanan Report default community names of the SNMP Agent di E-Learning dan Portal Akademik Mahasiswa ULM.....	76
Gambar 4.16 Bruteforce kredensial service SNMP target	77
Gambar 4.17 Eksploitasi service SNMP target.....	78
Gambar 4.18 Data-data Network IP target.....	79
Gambar 4.19 Data-data Routing Information target	80
Gambar 4.20 Data-data Storage Information target.....	81

DAFTAR LAMPIRAN

Lampiran 1 Lembar Persetujuan Proposal	95
Lampiran 2 Lembar Konsultasi Proposal Skripsi	96
Lampiran 3 Lembar Konsultasi Skripsi	97
Lampiran 4 Lembar Pernyataan Kesiapan Membimbing Tugas Akhir	98
Lampiran 5 Hasil Pengintaian Simari ULM	99
Lampiran 6 Hasil Pengintaian E-Learning ULM.....	102
Lampiran 7 Hasil Pengintaian Portal Akademik Mahasiswa ULM.....	105
Lampiran 8 Hasil Pemindaian Kerentanan pada website Simari ULM Menggunakan ZAP	108
Lampiran 9 Hasil Pemindaian Kerentanan pada website E-Learning ULM Menggunakan ZAP	108
Lampiran 10 Hasil Pemindaian Kerentanan pada website Portal Akademik Mahasiswa ULM Menggunakan ZAP	109
Lampiran 11 Hasil Pemindaian Kerentanan pada website Simari, E-Learning dan Portal Akademik Mahasiswa ULM Menggunakan OpenVAS.....	109
Lampiran 12 Beberapa kerentanan WSTG yang bisa di scanning oleh ZAP Active Scanner.....	110
Lampiran 13 Test File Permission, Test Role Definitions & Review Old Backup and Unreferenced Files for Sensitive Information pada Simari ULM.....	111
Lampiran 14 Test RIA Cross Domain Policy pada Simari ULM.....	111
Lampiran 15 Akses robots.txt Simari ULM.....	111
Lampiran 16 Akses halaman /mail Simari ULM	112
Lampiran 17 Akses file README Simari ULM.....	113
Lampiran 18 Akses file license.txt Simari ULM	114
Lampiran 19 Akses file composer.json Simari ULM.....	114
Lampiran 20 Akses file gitignore Simari ULM	115
Lampiran 21 Akses file .htaccess Simari ULM	115
Lampiran 22 Test File Permission, Test Role Definitions & Review Old Backup and Unreferenced Files for Sensitive Information pada E-Learning ULM	116
Lampiran 23 Test RIA Cross Domain Policy pada E-Learning ULM	116
Lampiran 24 Akses file config.php E-Learning ULM.....	117

Lampiran 25 Akses halaman /admin E-Learning ULM.....	117
Lampiran 26 Akses file INSTALL.txt E-Learning ULM.....	118
Lampiran 27 Akses file cron.php & Testing for Bypassing Authentication Schema pada E-Learning ULM	118
Lampiran 28 Akses file composer.json E-Learning ULM	119
Lampiran 29 Akses file composer.lock E-Learning ULM.....	120
Lampiran 30 Isi file composer.lock E-Learning ULM.....	120
Lampiran 31 Akses file package.json E-Learning ULM	121
Lampiran 32 Akses halaman /#wp-config.php# E-Learning ULM	122
Lampiran 33 Test File Permission, Test Role Definitions & Review Old Backup and Unreferenced Files for Sensitive Information pada Portal Akademik Mahasiswa ULM.....	122
Lampiran 34 Test RIA Cross Domain Policy pada Portal Akademik Mahasiswa ULM.....	123
Lampiran 35 Akses file .htaccess Portal Akademik Mahasiswa ULM	123
Lampiran 36 Isi file .htaccess Portal Akademik Mahasiswa ULM.....	124
Lampiran 37 Akses file backup.egg Portal Akademik Mahasiswa ULM	125
Lampiran 38 Test HTTP Methods pada Simari ULM.....	125
Lampiran 39 Test HTTP Methods & Testing for HTTP Verb Tampering pada Simari ULM.....	125
Lampiran 40 Test HTTP Methods E-Learning ULM.....	126
Lampiran 41 Test HTTP Methods & Testing for HTTP Verb Tampering pada E-Learning ULM	126
Lampiran 42 Test HTTP Methods Portal Akademik Mahasiswa ULM.....	126
Lampiran 43 Test HTTP Methods & Testing for HTTP Verb Tampering pada Portal Akademik Mahasiswa ULM	126
Lampiran 44 Testing for Account Enumeration and Guessable User Account pada Simari ULM	127
Lampiran 45 Testing for Credentials Transported over an Encrypted Channel pada Simari ULM	127
Lampiran 46 Testing for Bypassing Authorization Schema pada Simari ULM dengan teknik Access Control Testing	128

Lampiran 47 Testing for Bypassing Authorization Schema & Testing for Privilege Escalation pada Simari ULM dengan teknik Forced Browsing.....	128
Lampiran 48 Testing for Bypassing Authorization Schema pada E-Learning ULM dengan teknik Access Control Testing	128
Lampiran 49 Testing for Bypassing Authorization Schema & Testing for Privilege Escalation pada E-Learning ULM dengan teknik Forced Browsing	129
Lampiran 50 Testing for Bypassing Authorization Schema pada Portal Akademik Mahasiswa ULM dengan teknik Access Control Testing	129
Lampiran 51 Testing for Bypassing Authorization Schema & Testing for Privilege Escalation pada Portal Akademik Mahasiswa ULM dengan teknik Forced Browsing	129
Lampiran 52 Testing for Insecure Direct Object References (IDOR) pada endpoint profil E-Learning ULM.....	130
Lampiran 53 Testing for Insecure Direct Object References pada endpoint edit profil E-Learning ULM.....	130
Lampiran 54 Testing for HTTP Parameter Pollution pada E-Learning ULM	130
Lampiran 55 Testing for HTML Injection pada E-Learning ULM.....	131
Lampiran 56 Testing for CSS Injection pada E-Learning ULM.....	132
Lampiran 57 Testing for CSS Injection pada Portal Akademik Mahasiswa ULM	133
Lampiran 58 Tabel Lengkap Hasil pengujian OWASP WSTG versi 4.2.....	134
Lampiran 59 Cover Dokumentasi Report	141
Lampiran 60 Daftar Isi Dokumen Report	142
Lampiran 61 Ringkasan Eksekutif Dokumen Report	143
Lampiran 62 Pelingkupan Dokumen Report	144
Lampiran 63 Pendekatan dan Metodologi Dokumen Report.....	145
Lampiran 64 Penjelasan Pendekatan dan Metodologi Dokumen Report.....	146
Lampiran 65 Informasi Kontak Dokumen Report	147
Lampiran 66 Ringkasan Temuan Utama Dokumen Report	148
Lampiran 67 Ringkasan Teknis Terperinci Dokumen Report.....	150
Lampiran 68 Glosarium	152