

**ANALISIS KERENTANAN *DIGITAL LIBRARY* ULM MENGGUNAKAN  
*FRAMEWORK WEB SECURITY TESTING GUIDE (WSTG) VERSI 4.2*  
DENGAN *VULNERABILITY SCANNER***

**SKRIPSI**



**OLEH:**

**MUHAMMAD QALBY**

**NIM. 2110817210001**

**PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS TEKNIK  
UNIVERSITAS LAMBUNG MANGKURAT  
BANJARMASIN, JANUARI 2026**

**ANALISIS KERENTANAN *DIGITAL LIBRARY* ULM MENGGUNAKAN  
*FRAMEWORK WEB SECURITY TESTING GUIDE (WSTG) VERSI 4.2*  
DENGAN *VULNERABILITY SCANNER***

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat

Sarjana Strata-1 Teknologi Informasi



**OLEH:**

**MUHAMMAD QALBY**

**NIM. 2110817210001**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS LAMBUNG MANGKURAT**

**BANJARMASIN, JANUARI 2026**

## LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama : Muhammad Qalby  
NIM : 2110817210001  
Fakultas : Teknik  
Prodi : Teknologi Informasi  
Judul Tugas Akhir : Analisis Kerentanan *Digital Library* ULM  
Menggunakan *Framework Web Security Testing Guide* (WSTG) Versi 4.2 dengan  
*Vulnerability Scanner*  
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 rujuk.

Banjarmasin, 17 November 2025

Penulis,



Muhammad Qalby  
NIM. 2110817210001

LEMBAR PENGESAHAN

SKRIPSI PROGRAM STUDI S-1 TEKNOLOGI INFORMASI

Analisis Kerentanan *Digital Library* ULM Menggunakan *Framework Web Security Testing Guide (WSTG) Versi 4.2* dengan *Vulnerability Scanner*

Oleh

Muhammad Qalby (2110817210001)

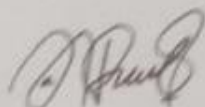
Telah dipertahankan di depan Tim Penguji pada 15 Desember 2025 dan dinyatakan

LULUS

Komite Penguji :

Ketua : Nurul Fathanah Mustamin, S.Pd., M.T.

NIP. 199110252019032018



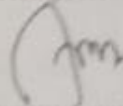
Anggota 1 : Helda Yunita, S.Kom., M.Kom.

NIP. 199106192024062001



Anggota 2 : Andreyan Rizky Baskara, S.Kom., M.Kom.

NIP. 199307032019031011



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

Utama NIP. 198205082008011010



Banjarbaru, 13 JAN 2026

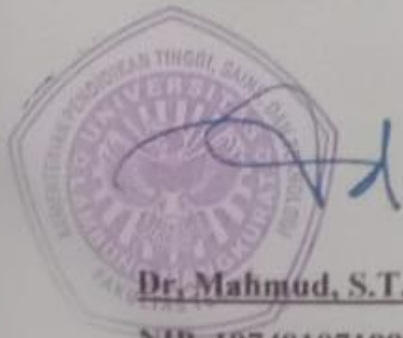
Diketahui dan disahkan oleh:

Wakil Dekan Bidang Akademik

Fakultas Teknik ULM,

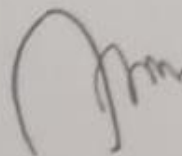
Koordinator Program Studi

S-1 Teknologi Informasi,



Dr. Mahmud, S.T., M.T.

NIP. 197401071998021001



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

NIP. 199307032019031011

**PERSETUJUAN SKRIPSI**

ANALISIS KERENTANAN *DIGITAL LIBRARY ULM* MENGGUNAKAN  
*FRAMEWORK WEB SECURITY TESTING GUIDE (WSTG)* VERSI 4.2  
DENGAN *VULNERABILITY SCANNER*

OLEH:

MUHAMMAD QALBY

NIM. 2110817210001

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

Banjarmasin, 19 November 2025

Pembimbing Utama,



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

NIP. 198205082008011010

## ABSTRAK

Kebocoran data di lingkungan akademik menimbulkan ancaman serius terhadap integritas dan kerahasiaan informasi. Universitas Lambung Mangkurat (ULM), yang sebelumnya pernah mengalami insiden kebocoran data, mengoperasikan *Digital Library* (Digilib) ULM sebagai repositori utama penelitian mahasiswa yang belum dipublikasikan. Hal ini menjadikan perlindungan terhadapnya menjadi penting. Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan pada *website* Digilib ULM dan memberikan rekomendasi perbaikannya. Penelitian ini menggunakan *framework Web Security Testing Guide* (WSTG) versi 4.2 sebagai panduan pengujiannya dengan pendekatan *black-box* dan *gray-box testing*. Proses pengujian mencakup tahap pengintaian, pemindaian otomatis menggunakan *Vulnerability Scanner*, serta pengujian penetrasi manual untuk validasi temuan dan melakukan pengujian WSTG lainnya. Hasil penelitian menemukan adanya 8 kerentanan yang terdapat pada Digilib ULM. Berdasarkan *Common Vulnerability Scoring System* (CVSS), temuan ini dikategorikan sebagai: 2 tingkat *High* (SQL Injection dan Session Fixation), 3 tingkat *Medium* (HTML Injection, Apache HTTP Server/server-status, dan Frameable Response (Potential Clickjacking)), dan 5 tingkat *Low* (Cookie without HttpOnly/Secure flag, HSTS not enforced, jQuery XSS Vulnerability, dan Weak Transport Layer Security).

Kata Kunci: *Burp Suite*, CVSS, Digilib ULM, Kerentanan Web, *Web Security Testing Guide*.

## ABSTRACT

*Data breaches in the academic environment pose a serious threat to information integrity and confidentiality. Universitas Lambung Mangkurat (ULM), which has previously experienced data breach incidents, operates the Digital Library (Digilib) ULM as the main repository for unpublished student research. This makes its protection essential. This research aims to identify security vulnerabilities on the Digilib ULM website and provide recommendations for remediation. This study uses the Web Security Testing Guide (WSTG) version 4.2 framework as its testing guide, employing black-box and gray-box testing approaches. The testing process includes a reconnaissance phase, automated scanning using a Vulnerability Scanner, and manual penetration testing to validate findings and conduct other WSTG tests. The research results found 8 vulnerabilities present in Digilib ULM. Based on the Common Vulnerability Scoring System (CVSS), these findings were categorized as: 2 High level (SQL Injection and Session Fixation), 3 Medium level (HTML Injection, Apache HTTP Server/server-status, and Frameable Response (Potential Clickjacking)), and 5 Low level (Cookie without HttpOnly/Secure flag, HSTS not enforced, jQuery XSS Vulnerability, and Weak Transport Layer Security).*

*Keywords: Burp Suite, CVSS, Digilib ULM, Web Security Testing Guide, Web Vulnerability.*

## KATA PENGANTAR

Puji dan syukur senantiasa kami panjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat, kesehatan, dan kekuatan, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Kerentanan *Digital Library* ULM Menggunakan *Framework Web Security Testing Guide* (WSTG) Versi 4.2 dengan *Vulnerability Scanner*” ini dengan baik. Shalawat serta salam semoga tercurah kepada junjungan kita, Nabi Besar Muhammad SAW, yang telah membawa kita dari zaman kegelapan menuju cahaya keilmuan.

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata-1 (S1) pada Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Lambung Mangkurat, Banjarmasin. Penulis menyadari bahwa penyelesaian skripsi ini tidak lepas dari dukungan dan bantuan berbagai pihak. Oleh karena itu, dengan penuh rasa hormat dan terima kasih, penulis menyampaikan penghargaan kepada:

1. Koordinator Program Studi Teknologi Informasi, Bapak Andreyan Rizky Baskara, S.Kom., M.Kom. yang telah memberikan arahan dan solusi dalam penyelesaian skripsi.
2. Bapak Ir. Eka Setya Wijaya. S.T., M.Kom., selaku dosen Pembimbing yang telah memberikan bimbingan dan arahan kepada penulis dari awal sampai penyelesaian Skripsi ini.
3. Seluruh Dosen beserta Staf Program Studi Teknologi informasi yang telah membantu penulis dalam segala hal selama penulis berkuliah di Program Studi ini.
4. Orang tua dan keluarga di rumah yang telah memberi saya dorongan dan motivasi serta turut mendoakan demi kelancaran penyelesaian Skripsi saya.
5. Teman-teman seperjuangan di Program Studi Teknologi Informasi, yang telah menjadi tempat berbagi ilmu dan pengalaman selama masa perkuliahan.

Akhir kata, penulis menyampaikan terima kasih kepada semua pihak yang turut membantu dalam penyelesaian laporan Skripsi ini. Harapan dari penyusunan laporan ini adalah, semoga apa yang penulis susun dapat bermanfaat bagi para

pembaca dan semua pihak yang membutuhkan. Serta diharapkan dapat menjadi acuan informasi dasar dalam penelitian-penelitian terkait.

Skripsi ini terdiri dari beberapa bab dengan sistematika penulisan sebagai berikut:

- BAB I: Pendahuluan, yang mencakup latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian.
- BAB II: Tinjauan Pustaka, berisi landasan teori, penelitian terkait, dan kerangka pemikiran.
- BAB III: Metodologi Penelitian, meliputi alat dan bahan, alur penelitian.
- BAB IV: Hasil dan Pembahasan, yang memaparkan hasil penelitian serta analisisnya.
- BAB V: Kesimpulan dan Saran, yang berisi kesimpulan dari hasil penelitian serta saran untuk pengembangan lebih lanjut.

Banjarmasin, 17 November 2025

Penulis,



Muhammad Qalby

NIM. 2110817210001

## DAFTAR ISI

LEMBAR PERNYATAAN .....	i
LEMBAR PENGESAHAN .....	ii
PERSETUJUAN SKRIPSI .....	iii
ABSTRAK .....	iv
ABSTRACT .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI .....	viii
DAFTAR TABEL .....	xv
DAFTAR GAMBAR .....	xvii
DAFTAR LAMPIRAN .....	xxii
DAFTAR RIWAYAT HIDUP .....	xxiii
BAB 1 PENDAHULUAN .....	1
1. Latar Belakang .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah .....	5
1.4 Tujuan Penelitian .....	5
1.5 Manfaat Penelitian .....	5
BAB 2 TINJAUAN PUSTAKA .....	7
2.1. Penelitian Terkait .....	7
2.1.1. <i>Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating</i> .....	7
2.1.2. <i>Automated Web Security Testing Guide Mapping to Accelerate Process on Penetration Testing</i> .....	8
2.1.3. <i>Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) Pada Website XYZ</i> .....	9

2.1.4.	<i>Vulnerability Assessment</i> Pada Situs Web KPPM FRI Dengan <i>Burp Suite</i> dan <i>Intruder</i> .....	9
2.1.5.	Analisis dan Pengujian Kerentanan Sistem Informasi Perpustakaan .	10
2.2.	Landasan Teori .....	14
2.2.1.	Keamanan Informasi .....	14
2.2.2.	Kerentanan .....	14
2.2.3.	<i>Penetration Testing</i> .....	15
2.2.4.	<i>Digital Library</i> ULM .....	16
2.2.5.	OWASP .....	17
2.2.6.	<i>Web Security Testing Guide</i> (WSTG) .....	18
2.2.7.	<i>Burp Suite</i> .....	24
2.2.8.	<i>Common Vulnerability Scoring System</i> (CVSS) .....	27
2.3.	Kerangka Pemikiran .....	34
2.3.1.	<i>Indicators</i> .....	34
2.3.2.	<i>Proposed Method</i> .....	35
2.3.3.	<i>Objectives</i> .....	40
2.3.4.	<i>Measurements</i> .....	40
BAB 3 METODOLOGI PENELITIAN.....		41
3.1.	Alat dan Bahan .....	41
3.1.1.	Alat Penelitian .....	41
3.1.2.	Bahan Penelitian.....	42
3.2.	Alur Penelitian.....	42
3.2.1.	Identifikasi Masalah .....	43
3.2.2.	Studi Literatur .....	43
3.2.3.	Perizinan Secara Legal .....	43

3.2.4. Uji Kerentanan .....	43
3.2.5. Rekomendasi Perbaikan .....	45
3.2.6. Laporan Hasil Pengujian .....	45
BAB 4 HASIL DAN PEMBAHASAN.....	49
4.1. Pengintaian .....	49
4.2. Pemindaian Kerentanan.....	49
4.3. Pengujian Penetrasi .....	51
4.3.1. Validitas kerentanan hasil pemindaian.....	51
4.3.1.1. SQL Injection.....	51
4.3.1.2. Cross-Site Scripting (reflected).....	54
4.3.1.3. Cleartext submission of password.....	57
4.3.1.4. TLS cookie without secure flag set.....	58
4.3.1.5. Open redirection (DOM-based) .....	60
4.3.1.6. Cookie without HttpOnly flag set .....	62
4.3.1.7. Strict transport security not enforced .....	63
4.3.1.8. Unencrypted Communcation .....	64
4.3.1.9. jQuery < 1.9.0 XSS Vulnerability.....	66
4.3.1.10. Apache HTTP Server /server-status Accessible (HTTP).....	67
4.3.1.11. TCP Timestamps Information Disclosure.....	68
4.3.2. Pengujian Kerentanan Menggunakan <i>Framework</i> WSTG.....	70
4.3.2.1. Conduct Search Engine Discovery Reconnaissance for Information Leakage .....	70
4.3.2.2. Fingerprint Web Server.....	71
4.3.2.3. Review Webserver Metabytes for Information Leakage.....	71
4.3.2.4. Enumerate Applications on Webserver.....	72

4.3.2.5. Review Webpage Content for Information Leakage .....	73
4.3.2.6. Identify Application Entry Points .....	74
4.3.2.7. Map Execution Paths Through Application.....	75
4.3.2.8. Fingerprint Web Application Framework.....	75
4.3.2.9. Fingerprint Web Application .....	76
4.3.2.10. Map Application Architecture .....	76
4.3.2.11. Test Network Infrastructure Configuration.....	78
4.3.2.12. Test Application Platform Configuration .....	78
4.3.2.13. Test File Extensions Handling for Sensitive Information.....	79
4.3.2.14. Review Old Backup and Unreferenced Files for Sensitive Information.....	79
4.3.2.15. Enumerate Infrastructure and Application Admin Interfaces .....	80
4.3.2.16. Test HTTP Methods.....	81
4.3.2.17. Test HTTP Strict Transport Security .....	83
4.3.2.18. Test RIA Cross Domain Policy.....	83
4.3.2.19. Test File Permission.....	84
4.3.2.20. Test for Subdomain Takeover.....	85
4.3.2.21. Test Cloud Storage.....	85
4.3.2.22. Test Role Definitions .....	86
4.3.2.23. Test User Registration Process .....	87
4.3.2.24. Test Account Provisioning Process.....	88
4.3.2.25. Test for Account Enumeration and Guessable User Account.....	88
4.3.2.26. Test for Weak or Unenforced Username Policy .....	90
4.3.2.27. Test for Credentials Transported over an Encrypted Channel....	90
4.3.2.28. Testing for Default Credentials.....	91

4.3.2.29. Testing for Weak Lock Out Mechanism.....	92
4.3.2.30. Testing for Bypassing Authentication Schema.....	93
4.3.2.31. Testing for Vulnerable Remember Password .....	94
4.3.2.32. Testing for Browser Cache Weaknesses.....	95
4.3.2.33. Testing for Weak Password Policy .....	95
4.3.2.34. Testing for Weak Security Question Answer .....	96
4.3.2.35. Testing Directory Traversal File Include.....	96
4.3.2.36. Testing for Bypassing Authorization Schema .....	97
4.3.2.37. Testing for Privilege Escalation.....	99
4.3.2.38. Testing for Insecure Direct Object References .....	100
4.3.2.39. Testing for Session Management Schema .....	101
4.3.2.40. Testing for Cookies Attributes.....	102
4.3.2.41. Testing for Session Fixation .....	103
4.3.2.42. Testing for Exposed Session Variables.....	104
4.3.2.43. Testing for Cross Site Request Forgery .....	105
4.3.2.44. Testing for Logout Functionality .....	106
4.3.2.45. Testing Session Timeout.....	106
4.3.2.46. Testing for Session Puzzling.....	107
4.3.2.47. Testing for Session Hijacking.....	107
4.3.2.48. Testing for Reflected Cross Site Scripting.....	108
4.3.2.49. Testing for Stored Cross Site Scripting.....	108
4.3.2.50. Testing for HTTP Verb Tampering .....	109
4.3.2.51. Testing for HTTP Parameter Pollution .....	109
4.3.2.52. Testing for SQL Injection .....	110
4.3.2.53. Testing for LDAP Injection .....	111

4.3.2.54. Testing for XML Injection.....	112
4.3.2.55. Testing for SSI Injection.....	112
4.3.2.56. Testing for Xpath Injection.....	113
4.3.2.57. Testing for IMAP SMTP Injection.....	114
4.3.2.58. Testing for Code Injection.....	114
4.3.2.59. Testing for Command Injection.....	115
4.3.2.60. Testing for Format String Injection.....	116
4.3.2.61. Testing for Improper Error Handling.....	116
4.3.2.62. Testing for Stack Traces.....	120
4.3.2.63. Testing for Weak Transport Layer Security.....	120
4.3.2.64. Testing for Padding Oracle.....	122
4.3.2.65. Test for Sensitive Information Sent via Unencrypted Channels	123
4.3.2.66. Testing for Weak Encryption.....	124
4.3.2.67. Testing for DOM-Based Cross Site Scripting.....	124
4.3.2.68. Testing for JavaScript Execution.....	125
4.3.2.69. Testing for HTML Injection.....	125
4.3.2.70. Testing for Client-side URL Redirect.....	126
4.3.2.71. Testing for CSS Injection.....	127
4.3.2.72. Testing for Client-side Resource Manipulation.....	128
4.3.2.73. Testing Cross Origin Resource Sharing.....	128
4.3.2.74. Testing for Cross Site Flashing.....	129
4.3.2.75. Testing for Clickjacking.....	129
4.3.2.76. Testing Web Sockets.....	130
4.3.2.77. Testing GraphQL.....	131
4.4. Analisis Hasil.....	134

4.5. Rekomendasi Perbaikan .....	141
BAB 5 KESIMPULAN DAN SARAN .....	144
5.1. Kesimpulan.....	144
5.2. Saran .....	145
DAFTAR PUSTAKA .....	146
LAMPIRAN.....	152

## DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait .....	11
Tabel 2. 2 WSTG Active Techniques [6] .....	18
Tabel 2. 3 Penilaian Attack Vector [38].....	27
Tabel 2. 4 Penilaian Attack Complexity [38].....	28
Tabel 2. 5 Penilaian Privilege required [38] .....	29
Tabel 2. 6 Penilaian User Interaction [38] .....	30
Tabel 2. 7 Penilaian Scope [38] .....	30
Tabel 2. 8 Penilaian Confidentiality [38].....	31
Tabel 2. 9 Penilaian Integrity [38] .....	32
Tabel 2. 10 Penilaian Availability [38].....	33
Tabel 2. 11 Pengujian penelitian VAPT .....	35
Tabel 2. 12 Perbandingan Frameworks pengujian penetrasi [14].....	38
Tabel 2. 13 Contoh hasil measurements .....	40
Tabel 3. 1 Alat Penelitian.....	41
Tabel 3. 2 Format Laporan Hasil Pengujian .....	46
Tabel 4. 1 Hasil Pengintaian Digilib ULM .....	49
Tabel 4. 2 Hasil Pemindaian Burp Suite .....	50
Tabel 4. 3 Hasil Pemindaian Greenbone.....	51
Tabel 4. 4 Hasil Pengujian WSTG Versi 4.2 .....	133
Tabel 4. 5 Penilaian SQL Injection .....	134
Tabel 4. 6 Penilaian Session Fixation .....	135
Tabel 4. 7 Penilaian Apache HTTP Server /server-status.....	135
Tabel 4. 8 Penilaian HTML Injection .....	136
Tabel 4. 9 Penilaian TLS cookie without secure flag set.....	136

Tabel 4. 10 Penilaian Frameable Response (Potential Clickjacking) .....	137
Tabel 4. 11 Penilaian Strict transport security not enforced .....	137
Tabel 4. 12 Penilaian Cookie without HttpOnly flag set .....	138
Tabel 4. 13 Penilaian jQuery < 1.9.0 XSS Vulnerability.....	139
Tabel 4. 14 Penilaian Weak Transport Layer Security .....	139
Tabel 4. 15 Tingkat kerentanan dengan CVSS .....	140

## DAFTAR GAMBAR

Gambar 1. 1 Trafik Anomali Serangan Siber di Indonesia Tahun 2024 [4] .....	1
Gambar 2. 1 Digital Library ULM.....	16
Gambar 2. 2 OWASP Top 10 2017 & 2021 [6].....	17
Gambar 2. 3 Tampilan Vulnerability Scanner dari Burp Suite Professional .....	25
Gambar 2. 4 Burp Suite Scanner [39] .....	25
Gambar 2. 5 Framework Score ranking [18] .....	26
Gambar 2. 6 Evaluation performance of top 6 pen-testing tools [19].....	26
Gambar 2. 7 Contoh Perhitungan CVSS.....	33
Gambar 2. 8 Kerangka Pemikiran .....	34
Gambar 3. 1 Alur Penelitian.....	42
Gambar 3. 2 Contoh Rekomendasi perbaikan dari Burp Suite .....	45
Gambar 3. 3 Contoh Ringkasan Eksekutif [43] .....	47
Gambar 3. 4 Contoh pendekatan dan metodologi [43] .....	47
Gambar 3. 5 Contoh Ringkasan Temuan [43] .....	48
Gambar 3. 6 Contoh Detail Temuan [43].....	48
Gambar 4. 1 Kerentanan SQL Injection.....	51
Gambar 4. 2 Akses detail tanpa payload kueri SQL .....	52
Gambar 4. 3 Akses detail dengan payload true.....	53
Gambar 4. 4 Akses detail dengan payload false .....	53
Gambar 4. 5 Kerentanan Cross-Site Scripting (reflected) .....	54
Gambar 4. 6 Memasukkan payload script untuk pengujian XSS.....	55
Gambar 4. 7 Page source validasi pengujian XSS .....	56
Gambar 4. 8 Penanganan XSS pada sisi server.....	56
Gambar 4. 9 Kerentanan Cleartext submission of password .....	57

Gambar 4. 10 Request yang dikirimkan ketika login.....	58
Gambar 4. 11 Kerentanan TLS cookie without secure flag set.....	58
Gambar 4. 12 Cookies pada Digilib ULM.....	59
Gambar 4. 13 Mengirimkan cookie melalui HTTP .....	59
Gambar 4. 14 Kerentanan Open redirection (DOM-based).....	60
Gambar 4. 15 Script pengujian open redirection .....	61
Gambar 4. 16 DevTools Chrome Open Redirection.....	61
Gambar 4. 17 Kerentanan Cookie without HttpOnly flag set.....	62
Gambar 4. 18 Pengujian Cookie without HTTPOnly flag set .....	63
Gambar 4. 19 Pengujian Cookie without HTTPOnly flag set melalui Console ...	63
Gambar 4. 20 Kerentanan Strict transport security not enforced.....	63
Gambar 4. 21 Pengujian HSTS pada respons server.....	64
Gambar 4. 22 Kerentanan Unencrypted Communication .....	64
Gambar 4. 23 Melakukan permintaan dengan protokol HTTP.....	65
Gambar 4. 24 Kerentanan jQuery < 1.9.0 XSS Vulnerability .....	66
Gambar 4. 25 jQuery pada Digilib ULM.....	66
Gambar 4. 26 percobaan eksploitasi input .....	67
Gambar 4. 27 Kerentanan Apache HTTP Server /server-status Accessible .....	67
Gambar 4. 28 Halaman dengan mod_status pada Digilib.....	67
Gambar 4. 29 Request ke IP origin server .....	68
Gambar 4. 30 Kerentanan TCP Timestamps Information Disclosure .....	68
Gambar 4. 31 Perintah untuk menangkap paket TCP .....	69
Gambar 4. 32 Perintah untuk mengirimkan request ke server Digilib.....	69
Gambar 4. 33 Perintah untuk membaca dan menampilkan hanya protokol TCP .	69
Gambar 4. 34 Pemeriksaan file pada Digilib .....	70

Gambar 4. 35 Pemeriksaan konten cache Digilib .....	70
Gambar 4. 36 Fingerprint Web Server .....	71
Gambar 4. 37 Hasil Crawling Sitemap Digilib.....	72
Gambar 4. 38 Akses ke file robots.txt.....	72
Gambar 4. 39 Akses aplikasi dengan port lain.....	73
Gambar 4. 40 Peninjauan file dengan DevTools .....	74
Gambar 4. 41 Permintaan dan respons HTTP pada Digilib.....	75
Gambar 4. 42 Hasil identifikasi Wappalyzer .....	76
Gambar 4. 43 Respons HTTP pada Digilib .....	77
Gambar 4. 44 Respons proteksi pada Digilib.....	77
Gambar 4. 45 Mengakses Halaman /admin .....	80
Gambar 4. 46 Manipulasi parameter url untuk halaman /admin.....	81
Gambar 4. 47 Cookie manipulation dengan role admin .....	81
Gambar 4. 48 Test http methods by Nmap .....	82
Gambar 4. 49 Test HTTP method CONNECT .....	82
Gambar 4. 50 Test HTTP method TRACE.....	83
Gambar 4. 51 Pengujian file crossdomain.xml .....	84
Gambar 4. 52 Pengujian file clientaccesspolicy.xml .....	84
Gambar 4. 53 Pengujian terhadap subdomain.....	85
Gambar 4. 54 Manipulasi cookie pada request /admin .....	87
Gambar 4. 55 Respons dari login dengan akun yang valid.....	89
Gambar 4. 56 Respons dari login dengan password yang salah .....	89
Gambar 4. 57 Respons dari login dengan akun tidak valid.....	90
Gambar 4. 58 Request dan response ketika login .....	91
Gambar 4. 59 Pengujian default credentials .....	92

Gambar 4. 60 Hasil pengujian default credentials dengan Burp Suite Intruder ...	92
Gambar 4. 61 Pengujian terhadap mekanisme Lock Out.....	93
Gambar 4. 62 Pengujian authentication bypass dengan direct page request.....	93
Gambar 4. 63. Pengujian authentication bypass dengan session id prediction.....	94
Gambar 4. 64 Pengujian authentication bypass dengan sql injection .....	94
Gambar 4. 65 Konfigurasi Browser Cache .....	95
Gambar 4. 66 Testing Path Traversal File .....	97
Gambar 4. 67 Request perbarui profil di akun pertama.....	98
Gambar 4. 68 Request perbarui profil dengan session akun kedua .....	98
Gambar 4. 69 Memperbarui data profil akun yang telah logout.....	99
Gambar 4. 70 Mengakses file secara langsung melalui url.....	100
Gambar 4. 71 Pengumpulan cookie pada Digilib .....	101
Gambar 4. 72 Manipulasi karakter cookie .....	102
Gambar 4. 73 Burp Suite Scanner Cookie Manipulation.....	102
Gambar 4. 74 Browser pertama pengujian Session Fixation .....	103
Gambar 4. 75 Browser kedua pengujian Session Fixation .....	104
Gambar 4. 76 request dan respons form login .....	105
Gambar 4. 77 Testing CSRF .....	106
Gambar 4. 78 Mengakses halaman setelah Log Out.....	106
Gambar 4. 79 Testing Cross Site Scripting Reflected.....	108
Gambar 4. 80 Testing Stored Cross Site Scripting .....	109
Gambar 4. 81 Testing HTTP Parameter Pollution.....	110
Gambar 4. 82 Testing LDAP Injection .....	111
Gambar 4. 83 Testing XML Injection.....	112
Gambar 4. 84 Testing SSI Injection.....	113

Gambar 4. 85 Testing Xpath Injection .....	114
Gambar 4. 86 Testing Code Injection .....	115
Gambar 4. 87 Testing OS Command Injection .....	116
Gambar 4. 88 Manipulasi parameter search.....	118
Gambar 4. 89 Manipulasi parameter code .....	118
Gambar 4. 90 Tampilan default halaman presensi.....	118
Gambar 4. 91 Pemberian input panjang.....	119
Gambar 4. 92 Pemberian input panjang melalui url .....	119
Gambar 4. 93 Input huruf pada kolom NIM .....	120
Gambar 4. 94 Pemindaian konfigurasi SSL/TLS.....	121
Gambar 4. 95 Modifikasi nilai cookie.....	122
Gambar 4. 96 Testing Unencrypted Communications.....	123
Gambar 4. 97 Testing DOM-Based Cross Site Scripting .....	124
Gambar 4. 98 Testing JavaScript Injection .....	125
Gambar 4. 99 Pengujian HTML Injection .....	126
Gambar 4. 100 Testing Open Redirection.....	127
Gambar 4. 101 Testing CSS Injection .....	128
Gambar 4. 102 Testing Cross-Origin Resource Sharing.....	129
Gambar 4. 103 Testing Clickjacking .....	130
Gambar 4. 104 Testing GraphQL.....	132

## DAFTAR LAMPIRAN

Lampiran 1 Lembar Konsultasi Skripsi .....	152
Lampiran 2 Surat Permohonan Izin Penelitian Tugas Akhir .....	153
Lampiran 3 Hasil Pengintaian Digilib ULM.....	155
Lampiran 4 Hasil Pemindaian Kerentanan .....	156
Lampiran 5 Tabel Lengkap Hasil Pengujian WSTG Versi 4.2.....	157
Lampiran 6 Laporan dokumentasi analisis kerentanan Digilib ULM.....	167

## DAFTAR RIWAYAT HIDUP



Nama : Muhammad Qalby  
TTL : Palangka Raya, 02 Juli 2003  
Alamat : Jl. G. Obos XIX B RT 17/RW 03 Kec.  
Menteng, Kota Palangka Raya, Prov.  
Kalimantan Tengah

Agama : Islam  
Kewarganegaraan : Indonesia  
Riwayat Pendidikan : MIN Langkai Kota Palangka Raya  
MTsN 1 Kota Palangka Raya  
MAN Kota Palangka Raya