

**ANALISIS KEAMANAN *WEBSITE* PERPUSTAKAAN
MENGUNAKAN METODE *PENETRATION TESTING*
(Studi Kasus: PERPUSTAKAAN UNIVERSITAS MARITIM
RAJA ALI HAJI)**

TUGAS AKHIR



REGINA

2101020078

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG**

2026

**ANALISIS KEAMANAN *WEBSITE* PERPUSTAKAAN
MENGUNAKAN METODE *PENETRATION TESTING*
(Studi Kasus: PERPUSTAKAN UNIVERSITAS MARITIM
RAJA ALI HAJI)**

-Tugas Akhir

Skema Skripsi

Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana

Teknik pada Program Studi Teknik Informatika



REGINA

2101020078

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG**

2026

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Analisis Keamanan *Website* Perpustakaan Menggunakan Metode *Penetration Testing* (Studi Kasus: Perpustakaan Universitas Maritim Raja Ali Haji)” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, 19 Desember 2025



REGINA

NIM 2101020078



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.

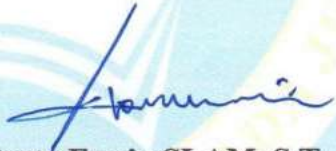
HALAMAN PERSETUJUAN

Judul : Analisis Keamanan *Website* Perpustakaan
Mengunakan Metode *Penetration Testing* (Studi
Kasus: Perpustakaan Universitas Maritim Raja Ali
Haji)
Nama : Regina
NIM : 2101020078
Program Studi : Teknik Informatika
Tanggal Persetujuan : 12 Desember 2025

Disetujui oleh,
Komisi Pembimbing



Ferdi Chahyadi, S.Kom, M.Cs
(Ketua)



Berta Erwin SLAM, S.T., M.Kom
(Anggota)

HALAMAN PENGESAHAN

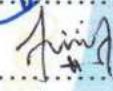
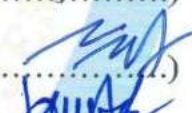
Judul : Analisis Keamanan *Website* Perpustakaan Menggunakan Metode *Penetration Testing* (Studi Kasus: Perpustakaan Universitas Maritim Raja Ali Haji)

Nama : Regina

NIM : 2101020078

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Muhamad Radzi Rathomi, S.Kom., M.Cs.	()
Anggota I	: Feri Irawan, S. Kom., M.Kom.	()
Anggota II	: Nolan Efranda, M.kom.	()
Anggota III	: Ferdi Chahyadi, S.Kom., M.Cs.	()
Anggota IV	: Berta Erwin Slam, S.T., M.Kom	()

Ketua Jurusan Teknik Elektro dan Informatika


Hollanda Arief Kusuma, S.IK., M.Si
NIP.198904012019031016

Tanggal Ujian: 19 Desember 2025 Tanggal Lulus:

PRAKATA

Puji dan syukur dipanjatkan kepada Allah *subhanahu wa ta'ala* atas segala karunia-Nya sehingga laporan tugas akhir ini berhasil diselesaikan. Tema yang dipilih dalam tugas akhir yang akan dilaksanakan pada bulan Desember 2025 dengan judul **“Analisis Keamanan Website Perpustakaan Menggunakan Metode *Penetration testing* (Studi Kasus : Perpustakaan Universitas Maritim Raja Ali Haji)”**.

Terima kasih penulis ucapkan kepada Bapak Ferdi Chahyadi, S.Kom, M.Cs. dan Bapak Berta Erwin SLAM, S.T., M.Kom. yang telah banyak memberi saran dan bimbingan. Ungkapan terima kasih juga disampaikan kepada Papa, Mama, keluarga dan teman-teman atas segala doa dan kasih sayangnya.

Semoga laporan tugas akhir ini bermanfaat.

Tanjungpinang, 1 September 2025



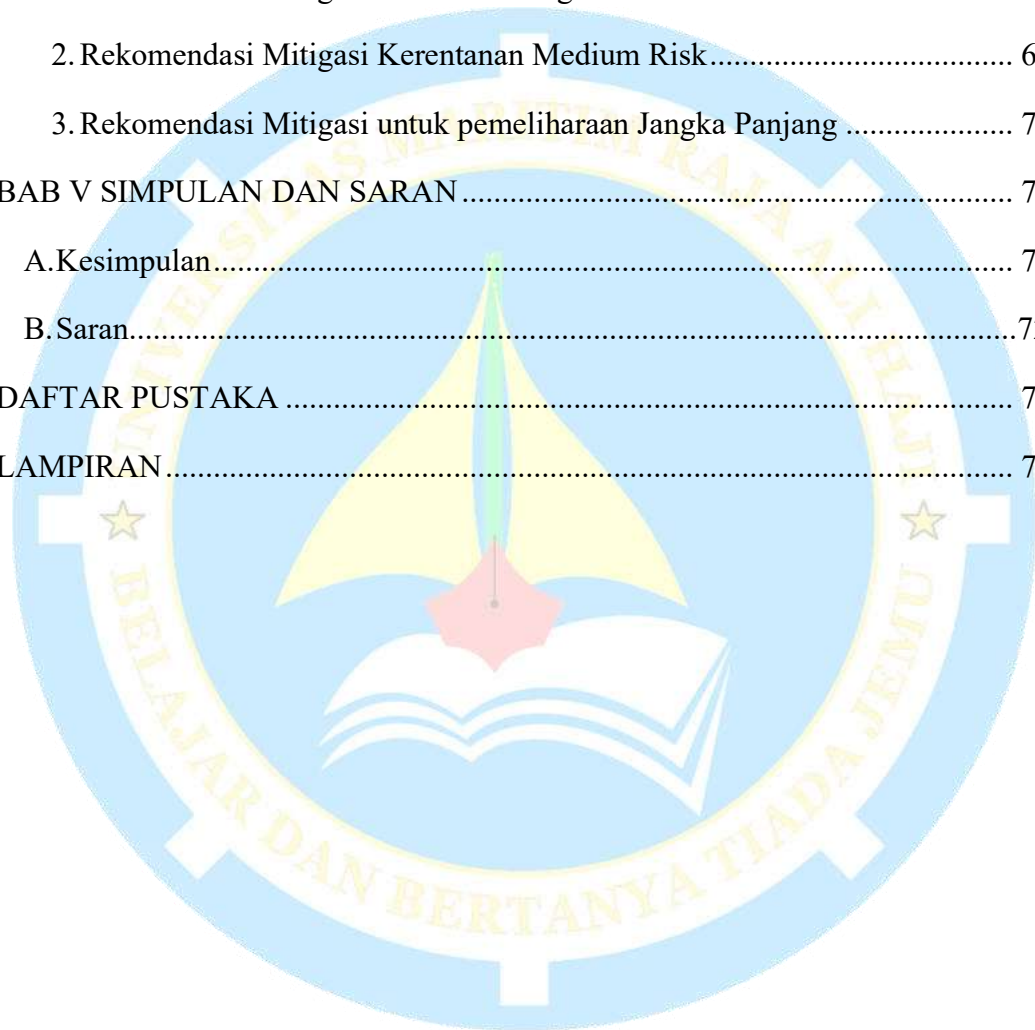
Regina

DAFTAR ISI

HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
ABSTRAK	vi
ABSTRACT	vii
PRAKATA.....	viii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
A.Latar Belakang.....	1
B.Perumusan Masalah.....	3
C.Batasan Penelitian.....	3
D.Tujuan Penelitian.....	4
E. Manfaat Penelitian.....	4
BAB II KAJIAN LITERATUR	5
A.Tinjauan Pustaka.....	5
B.Landasan Teori	12
1. Keamanan Sistem informasi.....	12
2. <i>Website</i>	13
3. Perpustakaan.....	13
4. Keamanan <i>Website</i>	14

5. <i>Penetration Testing</i>	14
6. Kali Linux.....	16
7. Nmap (Network Mapper)	16
8. Burp Suite	18
9. OWASP (<i>Open Application Security Project</i>)	21
10. SQLmap	22
11. Nikto.....	23
12. FFUF (<i>Fuzz Fuzzing U Fool</i>).....	23
13. Pentest Tool Website.....	24
14. <i>Common Vulnerability Scoring System</i> (CVSS).....	24
BAB III METODE PENELITIAN.....	26
A. Waktu dan Tempat Penelitian.....	26
B. Bahan dan Alat	26
C. Prosedur Pelaksanaan Penelitian	27
D. Perancangan Sistem.....	31
E. Analisis Hasil Pengujian.....	35
1. Analisis Kerentanan.....	35
BAB IV HASIL DAN PEMBAHASAN	37
A. Gambaran Umum Sistem dan Lingkungan Pengujian	37
B. Hasil Pengujian.....	37
1. Tahap <i>reconnainsance</i> (Pengumpulan Informasi).....	37
2. Tahap <i>Scanning</i> dan <i>Enumeration</i>	41
3. Tahap Vulnerability Testing (pengujian Kerentanan).....	47
4. Exploitation	53
5. Post Exploitation.....	56
6. Reporting	58

C. Pembahasan	61
1. Analisis Berdasarkan tingkat kerentanan	61
2. Analisis Pengujian	63
3. Implementasi Aplikasi Pendukung Analisis Keamanan Website.....	66
D. Rekomendasi Mitigasi	68
1. Rekomendasi Mitigasi kerentanan High Risk	68
2. Rekomendasi Mitigasi Kerentanan Medium Risk.....	69
3. Rekomendasi Mitigasi untuk pemeliharaan Jangka Panjang	70
BAB V SIMPULAN DAN SARAN	72
A. Kesimpulan.....	72
B. Saran.....	72
DAFTAR PUSTAKA	73
LAMPIRAN.....	77



DAFTAR TABEL

Tabel 1. Tinjauan Pustaka.....	6
Tabel 2. Fitur Burp Suite.....	20
Tabel 3. Kategori Score CVSS.....	25
Tabel 4. Perangkat yang digunakan	26
Tabel 5. Tools yang digunakan	27
Tabel 6. Perintah yang digunakan pada Nmap.....	37
Tabel 7. Parameter yang digunakan	38
Tabel 8. Port dan Status yang Terindikasi	39
Tabel 9. Informasi Layanan Web Server	39
Tabel 10. Identifikasi Aplikasi dan Generator	40
Tabel 11. Perintah yang Digunakan Pada Pengujian Nikto	41
Tabel 12. Hasil Pemindaian Nikto - Informasi server.....	42
Tabel 13. Hasil Pemindaian Nikto-Missing Security Headers	43
Tabel 14. Hasil pemindaian Nikto - Direktori Dan File Terekpos.....	43
Tabel 15. Hasil Pemindaian Nikto - Kelemahan konfigurasi lainnya.....	44
Tabel 16. Perintah FFUF	44
Tabel 17. Keterangan Parameter Nikto yang digunakan	45
Tabel 18. Hasil Pemindaian FFUF	46
Tabel 19. Summary Of Alert.....	48
Tabel 20. Detail Alert OWASP ZAP-High Risk	49
Tabel 21. Detail Alert OWAPS ZAP -Medium Risk	49
Tabel 22. Detail Alert OWASP ZAP - Low Risk	49
Tabel 23. Detail Alert OWAPS ZAP - Informational	50
Tabel 24. Hasil Temuan Pada Website Pentest Tools	51
Tabel 25. Perintah yang digunakan pada SQLMap	53
Tabel 26. Penilaian Resiko - SQLmap.....	57
Tabel 27. Tabel pemeriksaan header.....	57
Tabel 28. Tabel Penilaian Resiko.....	57
Tabel 29. Hasil Reporting	58

DAFTAR GAMBAR

Gambar 1. Aspek Keamanan Informasi	12
Gambar 2. Tahapan Penetration Testing.....	15
Gambar 3. Sistem Operasi Kali Linux	16
Gambar 4. Tampilan GUI Nmap.....	17
Gambar 5. Tampilan Dashboard <i>Tools</i> Burp Suite	19
Gambar 6. Pentest Tools	24
Gambar 7. Prosedur dalam Melakukan Penelitian.....	28
Gambar 8. Skema prosedur penelitian	30
Gambar 9. Topologi Pengujian penetration testing.....	32
Gambar 10. Flowchart Analisis.....	33
Gambar 11. Hasil Pengujian Nmap.....	38
Gambar 12. Hasil Pengujian Menggunakan Tools Nikto	42
Gambar 13. Hasil Pemindaian FFUF	45
<i>Gambar 14. Hasil Pemindaian Menggunakan OWASP ZAP</i>	<i>48</i>
<i>Gambar 15. Hasil Pemindain pada Website Pentest Tools.....</i>	<i>51</i>
Gambar 16. Percobaan eksploitasi menggunakan sqlmap.....	53
Gambar 17. Hasil pemeriksaan Header Repeater dan Respon Burp Suite yang menunjukkan header <i>server</i> dan ketiadaan header anti framing.....	54
Gambar 18. Percobaan eksploitasi <iframe> dan <i>clickjacking</i>	55
Gambar 19. Hasil curl direktori README.md	55
Gambar 20. Halaman Input URL	66
Gambar 21. Dashboard Hasil Analisis Keamanan Website.....	67