

**PENERAPAN MODEL DREAD UNTUK SPESIFIKASI PENILAIAN  
KERENTANAN PADA INFORMATION SYSTEM SECURITY  
ASSESSMENT FRAMEWORK (ISSAF)**

**SKRIPSI**



**Oleh:**

**MUHAMMAD ILHAM NOR RAMADHANI**

**NIM.2010817110008**

**PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS TEKNIK  
UNIVERSITAS LAMBUNG MANGKURAT  
BANJARMASIN, MEI 2025**

**PENERAPAN MODEL DREAD UNTUK SPESIFIKASI PENILAIAN  
KERENTANAN PADA INFORMATION SYSTEM SECURITY  
ASSESSMENT FRAMEWORK (ISSAF)**

**SKRIPSI**

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



**Oleh:**

**MUHAMMAD ILHAM NOR RAMADHANI**

**NIM.2010817110008**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS LAMBUNG MANGKURAT**

**BANJARMASIN, MEI 2025**

# LEMBAR PENGESAHAN

## LEMBAR PENGESAHAN

### SKRPSI PROGRAM STUDI S-1 TEKNOLOGI INFORMASI

Penerapan Model DREAD untuk Spesifikasi Penilaian Kerentanan Pada  
Information System Security Assessment Framework (ISSAF)

Oleh

Muhammad Ilham Nor Ramadhani (2010817110008)

Telah dipertahankan di depan Tim Penguji pada 06 Mei 2025 dan dinyatakan

LULUS

Komite Penguji :  
Ketua : Muti'a Maulida, S.Kom., M.T.I.  
NIP. 198810272019032013  
Anggota 1 : Nurul Fathanah Mustamin, S.Pd., M.T.  
NIP. 199110252019032018  
Anggota 2 : Muhammad Fajrian Noor, S.Kom., M.Kom.  
NIP. 199611092023211009  
Pembimbing : Ir. Eka Setya Wijaya, S.T., M.Kom.  
Utama : NIP. 198205082008011010

Banjarbaru, 10 JUN 2025

Diketahui dan disahkan oleh:

Wakil Dekan Bidang Akademik Koordinator Program Studi  
Fakultas Teknik ULM S-1 Teknologi Informasi



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

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

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini,

Nama : Muhammad Ilham Nor Ramadhani  
NIM : 2010817110008  
Fakultas : Teknik  
Program Studi : Teknologi Informasi  
Judul Tugas Akhir : Penerapan Model DREAD Untuk Spesifikasi Penilaian Kerentanan Pada *Information System Security Assessment Framework* (ISSAF) Pada Sistem APIK.  
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, 25 April 2025

Penulis,



Muhammad Ilham Nor Ramadhani

**LEMBAR PERSETUJUAN SKRIPSI**

**PERSETUJUAN SKRIPSI**

**PENERAPAN MODEL DREAD UNTUK SPESIFIKASI PENILAIAN  
KERENTANAN PADA INFORMATION SYSTEM SECURITY ASSESSMENT  
FRAMEWORK (ISSAF) PADA SISTEM APIK**

**OLEH**

**MUHAMMAD ILHAM NOR RAMADHANI**

**NIM.2010817210008**

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

**Banjarmasin, 25 April 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. Insiden penyisipan halaman ilegal pada salah satu *subdomain* Universitas Lambung Mangkurat menunjukkan adanya ancaman terhadap sistem digital, termasuk aplikasi APIK yang digunakan untuk pengelolaan tugas akhir mahasiswa. Aplikasi ini belum pernah melalui proses pengujian keamanan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada sistem APIK dengan menggunakan *Information System Security Assessment Framework* (ISSAF) yang dipadukan dengan model DREAD untuk menentukan tingkat risikonya. Uji penetrasi dilakukan menggunakan alat Zed Attack Proxy (ZAP) guna mendeteksi celah keamanan. Hasil penelitian menunjukkan bahwa kerentanan *SQL Injection – SQLite* memiliki skor risiko tertinggi sebesar 2,4, diikuti oleh *Missing Anti-Clickjacking Header* (2,0) dan *Content Security Policy* (CSP) Header Not Set (1,8). Kerentanan lain yang berada dalam kategori low memiliki skor rata-rata 1,6.

Kata Kunci: Kerentanan Web, APIK, *Information System Security Framework*, DREAD, Zed Attack Proxy (ZAP).

## ABSTRACT

*Data breaches in academic environments pose a serious threat to the integrity and confidentiality of information. An incident involving the injection of an illegal webpage into a subdomain of Universitas Lambung Mangkurat highlights the existence of threats targeting digital systems, including the APIK application used for managing student thesis workflows. This application has never undergone a security assessment. This study aims to identify and analyze vulnerabilities in the APIK system using the Information System Security Assessment Framework (ISSAF), combined with the DREAD model to determine risk levels. Penetration testing was conducted using the Zed Attack Proxy (ZAP) tool to detect security flaws. The findings indicate that SQL Injection – SQLite has the highest risk score of 2.4, followed by Missing Anti-Clickjacking Header (2.0), and Content Security Policy (CSP) Header Not Set (1.8). Other vulnerabilities categorized as low-risk have an average score of 1.6.*

*Keywords: Web Vulnerability, APIK, Information System Security Framework, DREAD, Zed Attack Proxy (ZAP)*

## KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala limpahan rahmat, taufik, dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Penerapan Model DREAD untuk Spesifikasi Penilaian Kerentanan pada Information System Security Assessment Framework (ISSAF)”. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Lambung Mangkurat.

Penelitian ini dilatarbelakangi oleh pentingnya keamanan sistem informasi dalam mendukung kegiatan operasional dan akademik, terutama pada aplikasi-aplikasi yang menyimpan data sensitif. Dalam hal ini, pendekatan ISSAF digunakan sebagai kerangka kerja untuk melakukan penilaian keamanan secara menyeluruh, dan model DREAD diterapkan sebagai metode untuk mengukur tingkat risiko dari setiap kerentanan yang ditemukan. Kombinasi keduanya diharapkan dapat memberikan hasil evaluasi yang lebih sistematis dan objektif, serta membantu dalam menentukan prioritas perbaikan yang tepat pada sistem.

Selama proses penyusunan skripsi ini, penulis menghadapi berbagai tantangan, baik teknis maupun non-teknis. Namun, berkat bantuan dan dukungan dari banyak pihak, semua tantangan tersebut dapat dilalui dengan baik. Oleh karena itu, penulis ingin menyampaikan terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Bapak/Ibu Dosen Pembimbing, yang telah meluangkan waktu, memberikan arahan, dan membimbing penulis dengan penuh kesabaran dan perhatian selama proses penyusunan skripsi ini.
2. Bapak/Ibu Dosen Penguji, atas kritik, saran, serta pertanyaan-pertanyaan yang mendorong penulis untuk berpikir lebih kritis dan memperbaiki kualitas karya ini.
3. Koordinator Program Studi Teknologi Informasi dan Dekan Fakultas Teknik, Universitas Lambung Mangkurat, atas segala dukungan akademik dan administrasi yang diberikan.
4. Orang tua tercinta, yang selalu menjadi sumber semangat, doa, dan dukungan moral maupun materiil dalam setiap langkah perjuangan penulis.

5. Keluarga besar dan sahabat dekat, atas motivasi, bantuan, dan waktu yang diberikan selama proses penelitian dan penulisan berlangsung.
6. Teman-teman seperjuangan di Program Studi Teknologi Informasi, atas kebersamaan, kerja sama, dan saling bantu dalam menghadapi berbagai proses akademik hingga tahap akhir skripsi ini.
7. Serta semua pihak yang tidak dapat disebutkan satu per satu yang telah memberikan dukungan secara langsung maupun tidak langsung.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang bersifat membangun sangat penulis harapkan demi perbaikan di masa mendatang.

Akhir kata, semoga skripsi ini dapat memberikan manfaat, baik sebagai referensi akademik maupun sebagai kontribusi nyata dalam pengembangan sistem penilaian kerentanan pada keamanan informasi.

Banjarmasin, 25 April 2025

Penulis



Muhammad Ilham Nor Ramadhani

## DAFTAR ISI

SAMPUL DALAM .....	i
LEMBAR PENGESAHAN .....	ii
LEMBAR PERNYATAAN .....	iii
LEMBAR PERSETUJUAN SKRIPSI.....	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xii
DAFTAR TABEL .....	xiv
DAFTAR LAMPIRAN .....	xv
DAFTAR RIWAYAT HIDUP.....	xvi
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.....	8
2.1    Penelitian Terkait .....	8
2.1.1    Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan <i>Framework</i> ISSAF .....	8
2.1.2    Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ.....	9
2.1.3    Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema .....	10
2.1.4    Evaluasi Resiko Keamanan Menggunakan Model Dread Terhadap Sistem Informasi Akademik Universitas Xyz.....	11
2.1.5    Vulnerability And Mitigation Analysis Of The Itera E - Learning Website Using Owasp Zed Attack Proxy (ZAP).....	12
2.2    Landasan Teori .....	15
2.2.1    APIK .....	15

2.2.2	<i>Website</i> .....	17
2.2.3	Laravel Framework .....	18
2.2.4	Kerentanan Sistem .....	18
2.2.5	<i>Penetration Testing</i> .....	19
2.2.6	Information System Security Assessment Framework (ISSAF)...	20
2.2.7	DREAD Model .....	21
2.2.8	ZAP .....	22
2.3	Kerangka Pemikiran.....	25
2.3.1	Indikator .....	25
2.3.2	Metode yang Diusulkan .....	25
2.3.3	Objektif .....	26
2.3.4	Measurement.....	26
BAB III METODOLOGI PENELITIAN.....		27
3.1	Alat dan Bahan Penelitian.....	27
3.1.1	<i>Hardware</i> .....	27
3.1.2	<i>Software</i> .....	27
3.1.3	Bahan Penelitian .....	27
3.2	Lokasi dan Objek Penelitian .....	28
3.3	Prosedur Penelitian .....	28
3.3.1	Studi Literatur .....	28
3.3.2	Identifikasi Masalah.....	29
3.3.3	Menentukan <i>Scope</i> .....	29
3.3.4	Mengumpulkan Informasi.....	30
3.3.5	Pemetaan Jaringan.....	30
3.3.6	Identifikasi Kerentanan .....	31
3.3.7	Uji Penetrasi.....	32
3.3.8	Mendapatkan Akses dan Eskalasi Hak Istimewa.....	32
3.3.9	Mempertahankan Akses dan Menutup Jejak.....	34
3.3.10	Penilaian Kerentanan Dengan Model DREAD.....	34
3.3.11	Membuat Laporan .....	37
3.3.12	Menghancurkan Artefak.....	38
BAB IV HASIL DAN PEMBAHASAN .....		40

4.1	Hasil .....	40
4.1.1	Mengumpulkan Informasi.....	40
4.1.2	Pemetaan Jaringan.....	40
4.1.3	Identifikasi Kerentanan .....	42
4.1.4	Uji Penetrasi .....	43
4.1.5	Mendapatkan Akses dan Eskalasi Hak Istimewa.....	53
4.1.6	Mempertahankan Akses dan Menutup Jejak.....	53
4.1.7	Penilaian Kerentanan Dengan Model DREAD.....	54
4.1.8	Membuat Laporan .....	61
4.1.9	Menghancurkan Artefak.....	62
4.2	Pembahasan.....	64
BAB V KESIMPULAN DAN SARAN.....		67
5.1	KESIMPULAN.....	67
5.2	SARAN .....	67
DAFTAR PUSTAKA.....		69
LAMPIRAN.....		75

## DAFTAR GAMBAR

Gambar 1.1 Grafik insiden kebocoran data di lingkungan akademik.....	1
Gambar 1.2 Salah satu <i>subdomain</i> disisipkan situs judi .....	2
Gambar 2.1 Login Page APIK .....	16
Gambar 2.2 Laman Home APIK.....	16
Gambar 2.3 Laman Dashboard Mahasiswa .....	17
Gambar 2.4 Gambar laman pengajuan proposal .....	17
Gambar 2.5 Enam kriteria evaluasi [14] .....	23
Gambar 2.6 Hasil Evaluasi [14].....	23
Gambar 2.7 Hasil rata - rata evaluasi [14] .....	23
Gambar 2.8 Deteksi kerentanan pada WAVSEP [54].....	24
Gambar 2.9 Deteksi Kerentanan pada DVWA [54] .....	24
Gambar 2.10 Kerangka Pemikiran.....	25
Gambar 3.1 Prosedur Penelitian.....	28
Gambar 3.2 Contoh <i>scanning</i> NMAP versi Windows [55].....	30
Gambar 3.3 Proses ZAP saat scanning .....	31
Gambar 3.4 Contoh hasil deteksi pada aplikasi ZAP.....	31
Gambar 3.5 Contoh Fitur Manual Explore .....	32
Gambar 3.6 Contoh fitur fuzzer [56] .....	33
Gambar 3.7 Contoh detail pengujian [58].....	38
Gambar 3.8 Contoh rekomendasi [58].....	38
Gambar 3.9 Contoh file session dari ZAP .....	39
Gambar 4.1 SQL Injection pada ZAP .....	44
Gambar 4.2 Percobaan dengan payload original pada Manual Request Editor....	45
Gambar 4.3 Percobaan dengan payload randomblob(100000000).....	45
Gambar 4.4 Percobaan dengan payload randomblob(1000000000).....	46
Gambar 4.5 Percobaan eksploitasi menggunakan SQLMap.....	46
Gambar 4.6 Percobaan eksploitasi dengan JSQL .....	47
Gambar 4.7 Content Security Policy (CSP) Header Not Set pada ZAP .....	49
Gambar 4.8 Pembuktian Header dengan menggunakan curl.....	50
Gambar 4.9 Informasi Header Menggunakan DevTools .....	50
Gambar 4.10 Missing Anti-Clickjacking Header pada ZAP.....	51

Gambar 4.11 Percobaan memuat konten APIK pada web pihak ketiga .....	52
Gambar 4.12 Percobaan Brute-Force pada APIK .....	53
Gambar 4.13 Folder Recycle Bin.....	63
Gambar 4.14 Proses penghapusan artefak .....	63
Gambar 4.15 Artefak telah dihapus.....	64

## DAFTAR TABEL

Tabel 1.1 Perbandingan model Risk Rating.....	4
Tabel 2.1 Penelitian terkait.....	14
Tabel 3.1 Pernyataan Penilaian DREAD [9].....	34
Tabel 3.2 Contoh Penilaian dengan Model DREAD .....	35
Tabel 3.3 Tabel Penilaian Kerentanan [18] .....	35
Tabel 3.4 Tabel Perbandingan Laporan.....	37
Tabel 4.1 5 <i>port</i> yang terbuka .....	40
Tabel 4.2 Hasil <i>Scanning</i> Menggunakan ZAP .....	42
Tabel 4.3 Penilaian SQL Injection - SQLite .....	54
Tabel 4.4 Penilaian Content Security Policy Header Not Set .....	55
Tabel 4.5 Penilaian Missing Anti-Clickjacking Header .....	55
Tabel 4.6 Penilaian Big Redirect Detected .....	56
Tabel 4.7 Penilaian Cookie No HttpOnly Flag .....	56
Tabel 4.8 Penilaian Cookie Without Secure Flag .....	57
Tabel 4.9 Penilaian Cross-Domain JavaScript Source File Inclusion.....	57
Tabel 4.10 Penilaian Server Leaks Version Information via "Server" HTTP Response Header Field.....	58
Tabel 4.11 Penilaian Strict-Transport-Security Header Not Set .....	58
Tabel 4.12 Penilaian X-Content-Type-Options Header Missing .....	59
Tabel 4.13 Perhitungan Nilai Kerentanan dengan Model DREAD .....	60

## DAFTAR LAMPIRAN

Lampiran 1 Surat Pernyataan Kesiapan Membimbing .....	75
Lampiran 2 Lembar Konsultasi.....	76
Lampiran 3 Surat Persetujuan Proposal .....	77
Lampiran 4 Melakukan Scanning Menggunakan NMAP.....	78
Lampiran 5 Hasil Scanning Menggunakan ZAP .....	79
Lampiran 6 Percobaan Exploitasi XSS pada laman login .....	79
Lampiran 7 Percobaan Reflected XSS pada Laman Login.....	80
Lampiran 8 Penilaian Kerentanan Menggunakan Model DREAD.....	80
Lampiran 9 Laporan Analisis Keamanan dan PENTEST dengan ISSAF.....	81
Lampiran 10 Lembar Konsultasi Skripsi .....	103
Lampiran 11 Transkrip Wawancara .....	104
Lampiran 12 Surat Izin Penelitian .....	105