Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik

by Azis Catur Laksono

Submission date: 17-Dec-2020 10:39PM (UTC+0700)
Submission ID: 1477748264
File name: Draft_paper_threat_modeling.pdf (438.28K)
Word count: 5104
Character count: 30789

Threat Modeling Menggunakan Pendekatan *STRIDE* dan *DREAD* untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik

Azis Catur Laksono[1], Yudi Prayudi[2]

[12]Magister Informatika Universitas Islam Indonesia
Email: [1]16917203@students.uii.ac.id, [2]prayudi@uii.ac.id

(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

ABSTRAK

Penerapan sistem informasi akademik ternyata membuka peluang risiko baru berupa ancaman-ancaman yang dapat mengganggu keberlangsungan sistem. Risiko ini bahkan lebih buruk dapat mengakibatkan kerugian pada organisasi. Sistem informasi akademik memiliki peran penting dalam proses bisnis Universitas XYZ, sehingga keberlangsungan sistem ini perlu dijaga dari kemungkinan ancaman dan risiko yang merugikan perguruan tinggi. *Threat modeling* (pemodelan ancaman) merupakan salah satu upaya untuk menganalisis ancaman pada sistem informasi. *Threat modeling* diterapkan dengan tahapan dekomposisi aplikasi, klasifikasi ancaman, penilaian risiko ancaman, dan penyusunan langkah mitigasi. Setiap ancaman diidentifikasi berdasarkan jenis ancaman yang telah dikategorikan pada metodologi *STRIDE*. Hasil klasifikasi ancaman selanjutnya dinilai tingkat risikonya menggunakan metodologi *DREAD*. Tahapan ini akan menghasilkan ranking risiko setiap ancaman sehingga dapat disusun kontrol mitigasi setiap ancaman untuk meminimalkan risiko. Melalui tahapan *threat modeling*, diketahui bahwa ancaman yang memiliki risiko tinggi pada Sistem Informasi Akademik Universitas XYZ adalah ancaman kategori *Spoofing*, *Tampering*, dan *Repudiation*. Fokus penyusunan kontrol mitigasi dilakukan pada ketiga kategori ancaman ini karena memiliki peringkat risiko tinggi.

Kata kunci: *sistem informasi, akademik, pemodelan ancaman, threat model, STRIDE, DREAD*

ABSTRACT

The application of academic information systems actually opens up new risk opportunities in the form of threats that can disrupt the sustainability of the system. This risk can lead to even worse harm to the organization. The academic information system has an important role in the XYZ University business process so that the sustainability of this system needs to be protected from possible threats and risks that harm the university. Threat modeling is an effort to analyze threats to information systems. Threat modeling is applied with the stages of application decomposition, threat classification, threat risk assessment, and preparation of mitigation measures. Each threat is identified based on the type of threat that has been categorized in the STRIDE methodology. The results of the threat classification are then assessed for the level of risk using the DREAD methodology. This step will produce a risk ranking for each threat so that mitigation controls can be arranged for each threat to minimize risk. Through the threat modeling stage, it is known that the threat that has a high risk in the Academic Information System of XYZ University is the threat of the Spoofing, Tampering, and Repudiation categories. The focus of the preparation of mitigation controls is carried out on these three threat categories because they have a high risk rating.

Keywords: *information systems, academic, threat model, STRIDE, DREAD*

1. PENDAHULUAN

Salah satu sistem informasi yang diimplementasikan pada perguruan tinggi adalah sistem informasi akademik. Namun, sistem yang memanfaatkan teknologi ini ternyata membuka peluang risiko baru berupa ancaman yang dapat mengganggu keberlangsungan sistem bahkan dapat mengakibatkan kerugian bagi instansi. Ancaman adalah suatu aksi atau kejadian

yang dapat merugikan perusahaan dengan kerugian bias berupa uang/biaya, tenaga upaya, peluang bisnis, reputasi nama baik, dan kerugian terburuk adalah membuat perusahaan pailit (Sutabri, 2012). Ancaman-ancaman ini merupakan risiko yang harus dicegah sebelum menjadi serangan pada sistem.

Sistem yang rentan untuk disusupi oleh pihak lain akan mengakibatkan keutuhan dan keakuratan datanya dipertanyakan. Inilah peran penting keamanan informasi sebagai bentuk perlindungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau pengrusakan (Syafitri, 2016).

Berbagai penelitian yang mengangkat tema keamanan sistem informasi telah ada sebelumnya, seperti penelitian oleh Chazar dan Ramdhani (2016) yang mengusulkan perencanaan keamanan sistem informasi dengan menggunakan pendekatan *OCTAVE* dan ISO 27001:2005. Perencanaan keamanan sistem diawali dengan langkah analisis menggunakan pendekatan *OCTAVE*, yang menghasilkan dua fase analisis. Fase pertama dengan membangun aset berdasarkan profil ancaman, sedangkan fase kedua adalah mengidentifikasi kerentanan infrastruktur informasi dan mengidentifikasi kelemahan teknologi yang digunakan. Hasil dari analisis kedua fase ini digunakan untuk menentukan perancangan strategi keamanan dan penerapannya, sesuai dengan dokumen Standar Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2005 sehingga dihasilkan dokumen SKMI yang terarah terhadap kebutuhan pengamanan aset-aset penting perusahaan.

Penelitian lain yang dilakukan oleh Prasetyowati *et al*., (2019) membahas tentang Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013. Indeks KAMI dengan dasar ISO/IEC 27001:2013 digunakan sebagai kerangka penelitian untuk mengolah hasil analisis. Indeks KAMI diterapkan untuk menilai tingkat kematangan, dan tingkat kelengkapan penerapan ISO/IEC 27001: 2013 serta gambaran tata kelola keamanan informasi pada organisasi. Hasil penilaian Indeks KAMI termasuk kepatuhan terhadap ISO/IEC 27001:2013 disajikan dalam bentuk diagram jaring laba-laba (*spider chart*). Hasil penilaian selanjutnya digunakan untuk membuat saran-saran perbaikan pada sistem.

Penelitian yang dilakukan oleh Nugraha (2016) memaparkan tentang manajemen risiko sistem informasi pada perguruan tinggi menggunakan kerangka kerja *NIST SP* 800-30. Proses manajemen risiko pada sistem informasi dilakukan melalui tiga tahapan, yaitu penilaian risiko, peringanan risiko, dan evaluasi risiko. Tahap penilaian risiko akan menghasilkan informasi berupa dampak risiko, penentuan risiko, dan rekomendasi risiko. Dampak risiko dihasilkan dari adanya kemungkinan risiko yang dianggap mengancam sistem. Penentuan risiko merupakan tahapan untuk menilai tingkat risiko terhadap sistem, dengan mengacu pada kemungkinan risiko dan dampak risiko yang telah disusun sebelumnya. Adapun rekomendasi risiko adalah langkah rekomendasi pencegahan terhadap risiko yang muncul. Selanjutnya tahap peringanan risiko merupakan kegiatan mitigasi risiko yang meliputi prioritas aksi dengan mengacu pada hasil akhir penilaian risiko. Risiko yang memiliki tingkat penilaian tertinggi dijadikan prioritas utama dalam proses peringanan risiko. Tahap akhir yaitu evaluasi risiko merupakan saran yang direkomendasikan untuk sistem informasi perguruan tinggi agar berjalan dengan baik sesuai harapan.

Dari beberapa literatur review tersebut, seperti halnya Universitas XYZ yang menerapkan sistem informasi akademik,

p-ISSN : 2502-5724; e-ISSN : 2541-5735

maka keberadaan sistem tersebut secara tidak langsung telah membuka akses dari pihak luar. Adanya fenomena ancaman tersebut, maka perlu dilakukan analisis terhadap kemungkinan ancaman dan risiko yang dapat terjadi pada Sistem Informasi Akademik Universitas XYZ.

Untuk menganalisis ancaman secara tepat, *threat modeling* (pemodelan ancaman) dapat diterapkan sebagai upaya untuk mengidentifikasi ancaman dan risiko pada sistem informasi akademik. *Threat modeling* merupakan proses terstruktur yang dapat mendeteksi kemungkinan kerentanan dan ancaman keamanan, mengukur tingkat keparahan dari setiap potensi risiko, dan memprioritaskan langkah perlindungan dan meminimalkan serangan terhadap infrastruktur (EC-Council, 2020).

Proses pemodelan ancaman dibagi menjadi tiga langkah utama, sebagai berikut (Owasp.org, 2020).

1. Dekomposisi aplikasi, adalah tahap untuk memperoleh pemahaman tentang aplikasi dan bagaimana aplikasi tersebut berinteraksi dengan entitas eksternal.
2. Klasifikasi ancaman, adalah tahap mengidentifikasi dan menentukan kategori ancaman menggunakan suatu metodologi tertentu.
3. Penentuan tindakan pencegahan dan mitigasi, adalah tahap mengidentifikasi tindakan sebagai langkah mengurangi risiko ancaman, termasuk penentuan tindakan mitigasi sesuai prioritas risiko.

Mengingat peran sistem informasi akademik yang erat dengan proses bisnis Universitas XYZ maka keberlangsungan sistem ini perlu dijaga dari kemungkinan ancaman dan risiko yang merugikan perguruan tinggi. Dengan implementasi metodologi *threat modeling*, diharapkan ancaman dapat diminimalkan melalui penerapan tindakan pencegahan yang tepat.

2. METODOLOGI PENELITIAN

Penelitian dilakukan melalui tahapan sistematis sebagai pedoman dalam penelitian, seperti disajikan pada Gambar 1.

Gambar 1. Tahap *Threat Modeling*

Tahapan penelitian diuraikan sebagai berikut.

1. Dekomposisi Aplikasi

Langkah awal pemodelan ancaman dimulai dengan memahami aplikasi dan bagaimana aplikasi berinteraksi dengan entitas eksternal. Tahap identifikasi aplikasi Sistem Informasi Akademik Universitas XYZ ini dituangkan dalam bentuk dokumen *threat model*. Hasil dokumentasi *threat model* selanjutnya digunakan untuk bahan menyusun *Data Flow Diagram*. Salah satu teknik mendekomposisi aplikasi adalah dengan menyusun *Data Flow Diagram*, sebagai cara untuk memvisualkan pergerakan data di sekitar aplikasi atau sistem, dan untuk mengetahui lokasi di mana data tersebut diubah atau disimpan oleh berbagai komponen (Fruhlinger, 2020).

2. Klasifikasi Ancaman

Proses klasifikasi ancaman dilakukan dengan mengadopsi kategorisasi ancaman pada metodologi *STRIDE*. Dikembangkan oleh *Microsoft*, metodologi ini berguna untuk mengetahui kategori ancaman berdasarkan maksud dan tujuan serangan (Jouini, Rabai dan Aissa, 2014). Singkatan *STRIDE* dibentuk dari huruf pertama dari masing-masing kategorinya, yaitu *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, dan *Elevation* of *priviledge*.

STRIDE menyediakan sekumpulan kategori ancaman dengan contoh yang sesuai, sehingga proses identifikasi ancaman dapat dilakukan secara sistematis dengan cara yang terstruktur dan berulang. Daftar ancaman kategori *STRIDE* ditunjukkan pada Tabel 1 (Owasp.org, 2020).

Tabel 1. Daftar Ancaman *STRIDE*

Tipe	Jenis Ancaman
Spoofing	Tindak ancaman yang ditujukan untuk mengakses dan menggunakan kredensial pengguna lain secara ilegal, seperti nama dan sandi pengguna
Tampering	Tindak ancaman yang bertujuan untuk mengubah data, baik mengubah data yang tersimpan dalam database maupun mengubah data pada saat transit melalui jaringan
Repudiation	Tindak ancaman berupa perbuatan ilegal dalam suatu sistem yang tidak memiliki kemampuan untuk melacak tindakan yang telah dilakukan
Information disclosure	Tindak ancaman berupa perbuatan membaca file secara tidak sah, atau membaca data pada saat transit
Denial of service	Tindak ancaman yang bertujuan untuk menolak akses ke pengguna yang valid, seperti dengan membuat server web tidak tersedia untuk sementara waktu
Elevation of priviledge	Tindak ancaman yang mempunyai tujuan untuk memperoleh hak akses yang lebih tinggi, agar dapat mengakses informasi atau menyusup ke sistem secara tidah sah

3. Penilaian Ancaman

Merupakan tahap penerapan metode *DREAD* untuk menilai, membandingkan, dan memprioritaskan tingkat risiko yang ditimbulkan dari setiap ancaman. Istilah *DREAD* merupakan singkatan dari setiap kategori risiko yaitu *Damage potential, Reproducibility, Exploitability, Affected user, dan Discoverability*, dengan definisi sebagai berikut (Owasp, 2016).

a. *Damage potential* yaitu seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan
b. *Reproducibility* yaitu seberapa mudah untuk mereproduksi serangan
c. *Exploitability* yaitu berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman
d. *Affected user* yaitu seberapa banyak pengguna yang terpengaruh jika ancaman dieksploitasi
e. *Discoverability* yaitu seberapa mudah bagi penyerang untuk menemukan ancaman pada sistem.

Ancaman dapat dinilai dari perspektif faktor risiko. Melalui penentuan faktor risiko yang ditimbulkan oleh berbagai ancaman yang teridentifikasi, dimungkinkan untuk menyusun daftar ancaman yang diprioritaskan dalam strategi mitigasi, seperti memutuskan ancaman mana yang harus ditangani terlebih dahulu.

Tabel 2 menunjukkan skema yang biasa digunakan untuk acuan penilaian ancaman. (Alhassan *et al.*, 2016). Ancaman dengan peringkat tinggi dinilai sama dengan 3, peringkat sedang dinilai sama dengan 2, dan peringkat rendah dinilai sama dengan 1 (Fruhlinger, 2020).

Tabel 2. Peringkat Ancaman

	Tinggi (3)	Sedang (2)	Rendah (1)
D	Penyerang menerobos sistem keamanan, memperoleh otorisasi penuh; memiliki akses admin; mampu mengupload konten	Membocorkan informasi yang penting	Membocorkan informasi yang sepele

p-ISSN : 2502-5724; e-ISSN : 2541-5735

	Tinggi (3)	Sedang (2)	Rendah (1)
R	Serangan dapat dilakukan secara berulang setiap saat tanpa jeda waktu	Serangan dapat diulangi, tetapi dalam waktu tertentu	Serangan sulit untuk diulangi, walaupun celah keamanan diketahui penyerang
E	Programmer pemula mampu membuat serangan dalam waktu singkat	Programmer terlatih mampu membuat serangan berulang kali	Serangan memerlukan seseorang yang sangat terampil dan memiliki pengetahuan lebih
A	Seluruh pengguna, konfigurasi default, pelanggan utama	Hanya beberapa pengguna, konfigurasi non-default	Pengguna yang terdampak hanya dalam persentase yang sangat kecil, mengaburkan fitur
D	Adanya informasi yang menjelaskan serangan. Kerentanan ditemukan pada fitur yang umum dipakai dan terlihat jelas	Kerentanan terdapat pada bagian yang jarang dipakai dan hanya pengguna tertentu yang menemukan, butuh pemikiran lebih untuk mengeksploitasi hal yang berbahaya	Bug tidak diketahui, pengguna tidak akan menemukan potensi kerusakan

Peringkat risiko diperoleh dari nilai total penjumlahan kategori ancaman *DREAD* dengan kisaran total antara 5-15. Total nilai antara 12-15 dikategorikan sebagai risiko Tinggi, total nilai antara 8-11 sebagai risiko Sedang, dan total nilai antara 5-7 sebagai risiko Rendah, seperti ditunjukkan pada Tabel 3 (Logixconsulting, 2019).

Tabel 3. Peringkat Risiko

Nilai	Peringkat Risiko
5 – 7	Rendah
8 – 11	Sedang
12 – 15	Tinggi

3. HASIL DAN PEMBAHASAN

3.1. Dekomposisi Aplikasi

Dokumentasi *threat model* disajikan pada Tabel 4 sampai Tabel 8. Hasil dari pengumpulan informasi tentang aplikasi dalam bentuk dokumen threat model selanjutnya digunakan untuk bahan penyusunan *Data Flow Diagram*.

3.1.1. Dokumen *Threat Model*

A. Informasi *Threat Model*

Tabel 4. Informasi *Threat Model*

Informasi *Threat Model*	
Aplikasi	Sistem Informasi Akademik
Deskripsi	Merupakan situs web perguruan tinggi yang menyediakan layanan online bagi mahasiswa, dosen, pihak akademik, dan pihak program studi. Layanan untuk mahasiswa meliputi data profil mahasiswa, pengisian kartu rencana studi, informasi jadwal perkuliahan, informasi kartu hasil studi, transkrip nilai, pembimbingan, yudisium, wisuda, dan layanan administratif lainnya. Layanan untuk dosen meliputi data profil dosen, upload informasi perkuliahan, upload materi perkuliahan, upload informasi nilai sebagai bahan kroscek nilai mahasiswa, termasuk download daftar peserta dari kelas mata kuliah yang diampu. Adapun layanan untuk pihak akademik dan program studi meliputi manajemen data administratif.
Pemilik Dokumen	Azis Catur Laksono
Peninjau	Dr. Yudi Prayudi, S.Si., M.Kom.

Dokumentasi threat model dimulai dengan penyusunan informasi singkat mengenai pemodelan ancaman tentang aplikasi, yang memuat info nama aplikasi, deskripsi tentang aplikasi, pemilik dokumen, partisipan, dan peninjau dokumen model ancaman, seperti disajikan pada Tabel 4.

B. Dependensi Eksternal

Merupakan objek lain di luar kode aplikasi yang keberadaannya dapat

menimbulkan ancaman bagi aplikasi. Dependensi eksternal didokumentasikan dengan memberikan nomor unik dan deskripsi untuk setiap dependensi, seperti disajikan pada Tabel 5.

Tabel 5. Dependensi Eksternal

Dependensi Eksternal	
ID	**Deskripsi**
1	Situs web layanan akademik perguruan tinggi berjalan pada server Linux yang menjalankan Apache sebagai server web
2	Server database yang digunakan adalah MySQL
3	Koneksi antara server web dan server database menggunakan jaringan pribadi
4	Protokol komunikasi menggunakan TLS (Transport Layer Security)

C. Titik Masuk

Titik masuk merupakan antarmuka pada aplikasi sebagai media interaksi antara penyerang dengan aplikasi atau data. Titik masuk didokumentasikan dengan memberikan nomor unik, nama antarmuka, deskripsi titik masuk, dan level kepercayaan akses yang merujuk ke Tabel 8, seperti disajikan pada Tabel 6.

Tabel 6. Titik Masuk

Titik Masuk			
ID	***Nama***	***Deskripsi***	***Level Kepercayaan***
1	Port HTTPS	Situs web sistem informasi akademik hanya dapat diakses melalui protokol TLS	LK1, LK2, LK3, LK4, LK5, LK6
1.1	Halaman login	Pengguna wajib login untuk mengakses layanan akademik	LK1, LK2, LK3, LK4, LK5, LK6
1.2	Fungsi login	Fungsionalitas login menerima kredensial dari pengguna dan akan memvalidasi kredensial dengan data pada database	LK2, LK3, LK4, LK5, LK6

D. Aset

Aset dapat berupa hal fisik atau abstrak yang dimiliki oleh sistem dan merupakan sesuatu yang diminati oleh penyerang. Aset didokumentasikan dengan memberikan nomor unik, nama aset, deskripsi aset, dan level kepercayaan akses yang merujuk ke Tabel 8, seperti disajikan pada Tabel 7.

Tabel 7. Aset

Aset			
ID	***Nama***	***Deskripsi***	***Level Kepercayaan***
A1	Pengguna layanan situs akademik	Aset yang berkaitan dengan pengguna	
A1.1	Detail Login Pengguna	Kredensial login yang akan digunakan pegguna untuk masuk ke situs web Sistem Informasi Akademik	LK2, LK4, LK5, LK6, LK7, LK9, LK10, LK11
A1.2	Data pribadi mahasiswa	Situs web akademik akan menyimpan informasi pribadi yang berkaitan dengan mahasiswa	LK2, LK5, LK6, LK7, LK8, LK9, LK10, LK11
A1.3	Data pribadi dosen	Situs web akan menyimpan informasi pribadi yang berkaitan dengan dosen	LK4, LK7, LK8, LK9, LK10, LK11
A2	Sistem	Aset yang berkaitan dengan sistem	
A2.1	Ketersediaan situs web	Situs web harus tersedia selama 24 jam dalam sehari dan dapat diakses oleh seluruh pengguna	LK7, LK8
A2.2	Ketersediaan database	Database layanan akademik harus tersedia dan dapat melayani permintaan data selama 24 jam dalam sehari	LK7, LK8
A2.3	Eksekusi kode pemograman web	Kemampuan untuk menjalankan kode pemrograman di server web	LK8, LK9

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Aset			
ID	*Nama*	*Deskripsi*	*Level Kepercayaan*
A2.4	Eksekusi perintah SQL read database	Kemampuan untuk menjalankan SQL query select pada database, bagi pengguna yang telah login ke sistem, sehingga dapat menerima informasi yang tersimpan pada database	LK5, LK6, LK7, LK10, LK11
A2.5	Eksekusi perintah SQL read/write database	Kemampuan untuk menjalankan SQL query select, insert, dan update pada database, bagi pengguna yang telah login ke sistem, sehingga memiliki akses baca tulis pada database	LK7, LK11
A2.6	Manajemen data	Kemampuan Admin untuk mengelola data pada sistem	LK5, LK6, LK7, LK11
A2.7	Melihat log	Kemampunan Admin sistem untuk melihat log terkait web dan database	LK7
A3	Situs web	Aset yang berkaitan dengan situs web layanan akademik	
A3.1	Sesi login	Sesi login pengguna ke situs web layanan akademik	LK2, LK4, LK5, LK6
A3.2	Layanan akademik	Pengguna yang telah login dapat mengakses segala layanan yang tersedia pada aplikasi SIA	LK2, LK4, LK5, LK6, LK9, LK10, LK11
A3.2	Akses ke server database	Akses ke server database memungkinkan seorang administrator untuk mengelola database, memberi akses penuh ke database pengguna dan semua data yang ada di dalam database	LK7

E. Level Kepercayaan

Level kepercayaan mewakili hak akses yang akan diberikan aplikasi kepada entitas eksternal. Level kepercayaan didokumentasikan dengan memberikan nomor unik, nama entitas eksternal, dan deskripsi entitas eksternal, seperti ditunjukkan pada Tabel 8.

Tabel 8. Level Kepercayaan

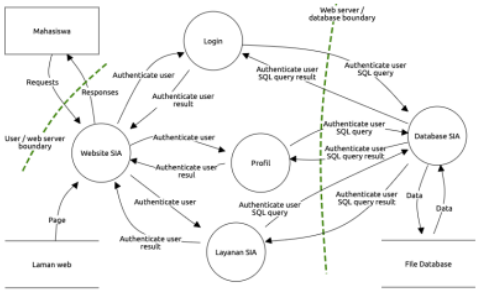
Level Kepercayaan		
ID	**Nama**	**Deskripsi**
LK1	Pengguna web anonim	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi tetapi tidak mempunyai kredensial login
LK2	Pengguna dengan kredensial login valid	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi dan telah login menggunakan kredensial login yang valid
LK3	Pengguna dengan kredensial login tidak valid	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi dan mencoba untuk login menggunakan kredensial login yang tidak valid
LK4	Dosen	Seseorang yang mempunyai posisi sebagai tenaga pendidik di perguruan tinggi
LK5	Admin akademik	Seseorang tenaga kependidikan pada bagian akademik perguruan tinggi yang memiliki kewenangan tertentu

Level Kepercayaan		
ID	**Nama**	**Deskripsi**
LK6	Admin prodi	Seseorang dari pihak program studi perguruan tinggi yang memiliki kewenangan tertentu
LK7	Admin server database	Seseorang administrator yang memiliki akses penuh ke server database situs sistem informasi akademik perguruan tinggi
LK8	Admin situs web	Seseorang administrator yang memiliki akses penuh untuk mengkonfigurasi situs web sistem informasi akademik perguruan tinggi
LK9	Proses server web	Merupakan entitas yang dijalankan oleh server web sebagai kode tertentu dan mampu mengautentik dirinya sendiri terhadap server database
LK10	Database read user	Akun pengguna database yang memiliki hak akses hanya dapat membaca database
LK11	Database read/write user	Akun pengguna database yang memiliki hak akses dapat membaca dan menulis pada database

3.1.2. *Data Flow Diagram*

Data Flow Diagram Sistem Informasi Akademik Universitas XYZ disajikan pada Gambar 2 dan Gambar 3.

Gambar 2. *Data Flow Diagram* Sistem Informasi Akademik



Gambar 3. *Data Flow Diagram* Mahasiswa

3.2. Klasifikasi Ancaman

Ancaman pada sistem informasi akademik akan diidentifikasi dengan mengacu pada kategori *STRIDE* di Tabel 1. Kemudian ancaman akan diidentifikasi keterkaitannya dengan level kepercayaan pada Tabel 8.

Identifikasi ancaman pertama adalah keteledoran pengguna terhadap informasi *login* miliknya. Ancaman ini ditandai dengan nomor identitas T1 (*Threat* 1) dan dicari keterkaitannya dengan level kepercayaan di Tabel 8. Sesuai kategori *STRIDE* di Tabel 1 maka diketahui bahwa tipikal ancaman T1 merupakan ancaman kategori *spoofing*, yaitu tindak ancaman yang ditujukan untuk mengakses dan menggunakan kredensial pengguna lain secara ilegal. Ancaman T1 kemudian diidentifikasi keterkaitannya dengan level kepercayaan, dan diketahui bahwa T1 memiliki keterkaitan dengan LK2, LK4, LK5, dan LK6. Hasil identifikasi selengkapnya disajikan pada Tabel 9.

Tabel 9. Klasifikasi Ancaman

ID	Deskripsi	Level Kepercayaan	STRIDE
T1	Pengguna meninggalkan kredensial login di tempat umum, atau secara tidak sengaja menyimpan informasi login di browser komputer publik, atau membagikan informasi login ke teman/kerabat	LK2, LK4, LK5, LK6	S

p-ISSN : 2502-5724; e-ISSN : 2541-5735

ID	Deskripsi	Level Kepercayaan	STRIDE
T2	Pengguna memberikan kredensial login kepada orang lain secara tidak sengaja, misal melalui serangan social engineering	LK2, LK4, LK5, LK6	S
T3	Seseorang yang telah diberitahu kredensial login pengguna (misal teman atau kerabat) menyalahgunakan akun/identitas pengguna untuk tindak kejahatan	LK2, LK4	S
T4	Seorang admin menyalahgunakan akun/identitas pengguna untuk tindak kejahatan	LK5, LK6, LK7	S
T5	Penyerang memalsukan laman login web untuk mendapatkan informasi kredensial login dari pengguna	LK2, LK4, LK5, LK6	S
T6	Admin secara sengaja atau tidak sengaja menambah, memodifikasi, atau menghapus data pengguna pada sistem database di luar ketentuan	LK5, LK7	T
T7	Penyerang dengan sengaja menambah, memodifikasi, atau menghapus data yang tersimpan pada sistem database	LK2, LK4, LK5, LK6, LK7	T
T8	Seseorang menggunakan identitas pengguna yang sah untuk melakukan tindak kejahatan	LK2, LK4, LK5, LK6, LK7	R
T9	Penyangkalan pihak pengguna yang sah bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	LK2, LK4	R
T10	Penyangkalan pihak admin bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	LK5, LK6, LK7, LK8	R
T11	Pencatatan log yang minim sebagai bukti penanganan klaim penyangkalan	LK2, LK4, LK5, LK6, LK7, LK8, LK9, LK11	R
T12	Penyerang membaca informasi pribadi pengguna yang tersimpan pada sistem database	LK2, LK4	I
T13	Penyerang menyebarluaskan informasi tentang data pribadi pengguna	LK2, LK4	I
T14	Penyerang mengumpulkan data pengguna sebagai target tindak kejahatan	LK2, LK4	I
T15	Penyerang membanjiri bandwidth melalui banyak request dengan maksud untuk memperlambat atau bahkan menumbangkan sistem	LK9, LK11	D
T16	Penyerang mengupload banyak file dengan maksud untuk memenuhi media penyimpanan database	LK2, LK4, LK9, LK11	D
T17	Seseorang bukan pengguna yang sah mengakses sistem memakai kredensial login pengguna yang memiliki akses lebih tinggi	LK2, LK4, LK5, LK6, LK7	E

3.3. Penilaian Ancaman

Hasil identifikasi ancaman pada Tabel 9 selanjutnya dinilai menggunakan metode *DREAD*. Pemberian bobot nilai untuk ancaman pada setiap level kepercayaan mengacu pada aturan penilaian Tabel 2. Hasil perhitungan selanjutnya dinilai tingkat

risikonya sesuai aturan peringkat ancaman pada Tabel 3.

Ancaman pertama (T1) pada level kepercayaan LK2 dinilai menggunakan pendekatan kategori *DREAD* dengan aturan peringkat tinggi = 3, peringkat sedang = 2, dan peringkat rendah = 1 untuk setiap kategorinya, diuraikan sebagai berikut.

a. *Damage potential*: ancaman T1 dengan level kepercayaan LK2 (mahasiswa) diberi nilai 1 karena apabila penyerang berhasil mengakses kredensial milik seorang mahasiswa, maka potensi kerusakan masih dalam peringkat rendah karena hanya sebatas pada satu pengguna yang akan melakukan tindak ancaman berikutnya.
b. *Reproducibility*: ancaman T1 dengan level kepercayaan LK2 diberi nilai 3 karena apabila penyerang telah memperoleh kredensial login mahasiswa, penyerang dengan mudah untuk memproduksi serangan-serangan tertentu secara berulang.
c. *Exploitability*: ancaman T1 merupakan bentuk keteledoran pengguna sehingga usaha untuk mendapatkan kredensial ini sangat mudah, maka ancaman T1 pada kategori exploitability diberi nilai 3.
d. *Affected user*: ancaman T1 dengan level kepercayaan LK2 diberikan nilai 1 karena jumlah pengguna yang terpengaruh oleh ancaman T1 ini sangat minim yaitu hanya seorang mahasiswa.
e. *Discoverability*: ancaman T1 merupakan bentuk keteledoran pengguna, sehingga usaha untuk menemukan kredensial tersebut terbilang sangat mudah, maka ancaman T1 diberi nilai 3.

Hasil penilaian ancaman selengkapnya disajikan pada Tabel 10.

Tabel 10. Penilaian Ancaman

Ancaman	Level Kepercayaan	D	R	E	A	D	JML	RISIKO
T1	LK2	1	3	3	1	3	11	Sedang
T1	LK4	2	3	3	2	3	13	Tinggi
T1	LK5, LK6	3	3	3	3	3	15	Tinggi
T2	LK2	1	3	2	1	2	9	Sedang
T2	LK4	2	3	2	2	2	11	Sedang
T2	LK5, LK6	3	3	2	3	2	13	Tinggi
T3	LK2	2	3	3	1	3	12	Tinggi
T3	LK4	2	3	3	2	3	13	Tinggi
T4	LK5, LK6	2	3	3	2	3	13	Tinggi
T4	LK7	3	3	3	3	3	15	Tinggi
T5	LK2	1	2	2	1	2	8	Sedang
T5	LK4	2	2	2	2	2	10	Sedang
T5	LK5, LK6	3	2	2	3	2	12	Tinggi
T6	LK5	2	3	3	3	3	14	Tinggi
T6	LK7	3	3	3	3	3	15	Tinggi
T7	LK2	1	3	3	1	2	10	Sedang
T7	LK4	2	3	3	2	2	12	Tinggi
T7	LK5, LK6	2	3	3	3	2	13	Tinggi
T7	LK7	3	3	2	3	1	12	Tinggi
T8	LK2	1	2	2	1	2	8	Sedang
T8	LK4	2	2	2	2	2	10	Sedang
T8	LK5, LK6	2	2	2	3	2	11	Sedang
T8	LK7	3	2	2	3	2	12	Tinggi
T9	LK2	1	2	2	1	2	8	Sedang
T9	LK4	2	2	2	2	2	10	Sedang
T10	LK5, LK6	2	2	2	2	2	10	Sedang
T10	LK7, LK8	3	2	2	2	2	11	Sedang
T11	LK2	1	2	2	1	2	8	Sedang
T11	LK4, LK5, LK6	2	2	2	2	2	10	Sedang
T11	LK7, LK8	3	2	2	3	2	12	Tinggi
T11	LK9, LK11	3	2	2	3	1	11	Sedang
T12	LK2	1	2	2	1	2	8	Sedang
T12	LK4	2	2	2	2	2	10	Sedang
T13	LK2	1	2	2	1	2	8	Sedang
T13	LK4	2	2	2	2	2	10	Sedang
T14	LK2	1	2	2	1	2	8	Sedang
T14	LK4	1	2	2	1	2	8	Sedang
T15	LK9, LK11	3	1	1	3	1	9	Sedang
T16	LK2	1	2	2	3	2	10	Sedang
T16	LK4	2	2	2	3	2	11	Sedang
T16	LK9, LK11	3	1	1	3	3	11	Sedang
T17	LK2	1	2	2	1	2	8	Sedang
T18	LK4	2	2	2	2	2	10	Sedang
T18	LK5	2	1	1	3	1	8	Sedang
T18	LK6	2	1	1	3	1	8	Sedang
T18	LK7	3	1	1	3	1	9	Sedang

3.4. Mitigasi

Setelah mengetahui nilai dari setiap ancaman, selanjutnya dapat disusun kontrol mitigasi sebagai langkah untuk mengurangi risiko dari setiap ancaman. Peringkat ancaman ini juga dapat digunakan untuk menyusun daftar mitigasi terhadap ancaman sesuai prioritas risiko tertinggi.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Berdasarkan data penilaian ancaman pada Tabel 10 dapat disusun langkah mitigasi sesuai klasifikasi ancaman. Daftar penilaian ancaman ini dapat dikelompokkan terlebih dahulu sesuai tingkat risikonya untuk mempermudah melihat ancaman yang memiliki risiko tinggi.

Sebagai contoh, ancaman T1 dengan level kepercayaan LK4 memiliki peringkat risiko tinggi. Ancaman T1 ini merupakan klasifikasi ancaman *spoofing*, sehingga langkah pencegahan yang dapat dilakukan sesuai teknik mitigasi pada bidang *authentication* yang disarankan dapat berupa proses otentikasi yang lebih aman, perlindungan data rahasia pengguna, tidak menuliskan *password* di media apapun. Ancaman kategori lain yang berisiko tinggi adalah *tampering* dengan contoh ancaman T6 pada level kepercayaan LK5. *Tampering* merupakan ancaman dengan kontrol keamanan bidang *integrity*. Langkah pencegahan yang disarankan pada bidang *integrity* ini adalah proses otentikasi yang lebih aman, penerapan *digital signature* yang akan tercatat secara otomatis pada *log* di setiap perubahan data, penerapan kode *hash* untuk memvalidasi data. Ancaman berikutnya yang memiliki peringkat risiko tinggi adalah ancaman kategori *repudiation* yang masuk dalam kontrol keamanan *non-repudiation*. Langkah pencegahan yang disarankan pada bidang keamanan *non-repudiation* adalah penerapan *digital signature* dan penerapan *timestamp* di setiap perubahan data, pencatatan segala sesuatu tindakan pada sistem pada *log* sebagai bahan pembuktian atas terjadinya perubahan pada sistem. Usulan mitigasi selengkapnya ditunjukkan pada Tabel 11.

Tabel 11. Usulan Mitigasi

1.	**Ancaman**	T1, T2, T3, T5
	Level Kepercayaan	LK4, LK5, LK6
	Kategori	*Spoofing*
	Bidang Keamanan	*Authentication*
	Mitigasi	- Abaikan fitur penyimpanan *username* dan password yang ditawarkan pada *browser* - Penggunaan *browser* mode *incognito*/*private* ketika memakai komputer publik untuk mengakses sistem - Menghindari pencatatan *password* di media apapun - Tidak memberitahukan kredensial login miliknya ke orang lain tanpa terkecuali - Abaikan segala jenis permintaan informasi kredensial login melalui tautan yang tidak terpercaya - Sosialisasi kepada pengguna tentang pentingnya keamanan dan kewaspadaan terhadap kredensial login miliknya
2.	**Ancaman**	T6, T7
	Level Kepercayaan	LK4, LK5, LK6, LK7
	Kategori	*Tampering*
	Bidang Keamanan	*Integrity*
	Mitigasi	- Penerapan *digital signature* yang akan tercatat secara otomatis pada *log* perubahan data - Penerapan kode *hash* untuk validasi - Pencatatan *log* tentang segala perubahan data
3.	**Ancaman**	T8, T11
	Level Kepercayaan	LK7, LK8
	Kategori	*Repudiation*
	Bidang Keamanan	*Confirmation*
	Mitigasi	- Segala sesuatu tindakan pada sistem harus dicatat pada *log* untuk bahan pembuktian atas terjadinya suatu tindakan pada sistem - Penerapan *digital signature* yang akan tercatat secara otomatis pada log perubahan data

4. KESIMPULAN

Threat modeling pada Sistem Informasi Akademik Universitas XYZ bertujuan untuk memprediksi kemungkinan serangan yang dapat terjadi pada sistem ini, termasuk langkah mitigasi pada ancaman tersebut. Metodologi *STRIDE* digunakan untuk

mengidentifikasi dan mengklasifikasikan ancaman pada sistem, kemudian tingkat risiko ancaman dinilai menggunakan model peringkat ancaman *DREAD*. Dari hasil perankingan, diperoleh informasi bahwa terdapat tiga kategori ancaman yang berisiko tinggi pada Sistem Informasi Akademik Universitas XYZ, yaitu ancaman *Spoofing*, *Tampering*, *Repudiation*. Fokus utama langkah pencegahan sebagai upaya meminimalkan risiko pada Sistem Informasi Akademik Universitas XYZ adalah melakukan kontrol mitigasi pada ketiga kategori yang memiliki tingkat risiko tinggi ini.

Adapun saran penelitian selanjutnya tentang *threat modeling* pada sistem informasi berbasis website dapat mengkombinasikan perhitungan risiko menggunakan *tool* semisal *OWASP ZAP* sebagai bahan perbandingan atas hasil penilaian peringkat risiko setiap ancaman.

DAFTAR PUSTAKA

Alhassan, J. K. *et al.* (2016) "Threat modeling of electronic health systems and mitigating countermeasures," *CEUR Workshop Proceedings*, 1830(Icta), hal. 82–89.

Chazar, C. dan Ramdani, A. (2016) "Model perencanaan keamanan sistem informasi menggunakan pendekatan metode octave dan iso 27001:2005," in *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, hal. 80–85.

EC-Council (2020) *What is Stride Methodology in Threat Modeling?* Tersedia pada: https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/.

Fruhlinger, J. (2020) *Threat modeling explained: A process for anticipating cyber attacks*. Tersedia pada: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.

Jouini, M., Rabai, L. B. A. dan Aissa, A. Ben (2014) "Classification of security threats in information systems," *Procedia Computer Science*. Elsevier Masson SAS, 32, hal. 489–496. doi: 10.1016/j.procs.2014.05.452.

Logixconsulting (2019) *What Is the DREAD Cybersecurity Model?* Tersedia pada: https://www.logixconsulting.com/2019/12/18/what-is-the-dread-cybersecurity-model/.

Nugraha, U. (2016) "Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-300," in *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, hal. 121–126.

Owasp.org (2020) *CRV2 App Threat Modeling*. Tersedia pada: https://owasp.org/www-community/CRV2_AppThreatModeling.

Owasp (2016) *OWASP Cheat Sheet Series - OWASP*. Tersedia pada: https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series.

Prasetyowati, D. D. *et al.* (2019) "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *JOINS (Journal of Information System)*, 4(1), hal. 65–75. doi: 10.33633/joins.v4i1.2429.

Sutabri, T. (2012) *Konsep Sistem Informasi*. Yogyakarta: Andi.

Syafitri, W. (2016) "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, 2(2), hal. 8. doi: 10.24014/coreit.v2i2.2356.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik

ORIGINALITY REPORT

13%	13%	3%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jurnal.unmuhjember.ac.id Internet Source	3%
2	doaj.org Internet Source	1%
3	script.id Internet Source	1%
4	digilib.unila.ac.id Internet Source	1%
5	www.slideshare.net Internet Source	1%
6	www.ojs.stt-ibnusina.ac.id Internet Source	<1%
7	blog.eccouncil.org Internet Source	<1%
8	ejurnal.stmik-budidarma.ac.id Internet Source	<1%

9	blog.tdohacker.org Internet Source	<1%
10	ujcontent.uj.ac.za Internet Source	<1%
11	idoc.pub Internet Source	<1%
12	repository.uinjkt.ac.id Internet Source	<1%
13	www.logixconsulting.com Internet Source	<1%
14	media.neliti.com Internet Source	<1%
15	www.scribd.com Internet Source	<1%
16	ejournal.uin-suka.ac.id Internet Source	<1%
17	repository.unpas.ac.id Internet Source	<1%
18	ceur-ws.org Internet Source	<1%
19	jurnal.fkip.unila.ac.id Internet Source	<1%
20	ejournal.catursakti.ac.id Internet Source	

		<1%
21	www.openjournal.unpam.ac.id Internet Source	<1%
22	eprints.umm.ac.id Internet Source	<1%
23	fr.scribd.com Internet Source	<1%
24	dokumen.tips Internet Source	<1%
25	Marlon A. Naagas, Thelma D. Palaoag. "A Threat-Driven Approach to Modeling a Campus Network Security", Proceedings of the 6th International Conference on Communications and Broadband Networking - ICCBN 2018, 2018 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		