Penilaian Risiko Aplikasi Web Menggunakan Model DREAD

Didit Suprihanto[a,*], Aris Sugiharto[b]

[a] Fakultas Teknik, Universitas Mulawarman, Samarinda
[b] Fakultas Sains dan Matematika, Universitas Diponegoro, Semarang

Naskah Diterima : 13 Januari 2013; Diterima Publikasi : 9 Maret 2013

Abstract

Application that is developed by web based, beside has surplus in WWW technology, it has susceptibility side that can be threat too. Susceptibility generate risk and can bring out big trouble even effect big disadvantage. The goal of this research is design and build document risk assessment system of threat level and prevention advice. It use DREAD model as method to solve trouble by giving qualified information. This information are used to produce risk level in web application. The result of this research is web application risk assessment system by using DREAD model to know risk threat level and equate perception of web threat risk to application developer, minimize of threat risk and maximize performance of web application.

***Kata kunci**:* DREAD model; Web threat risk; Web risk assessment system

Abstrak

Aplikasi yang dikembangkan berbasis web disamping memiliki kelebihan dalam teknologi *World Wide Web* (WWW) juga memiliki sisi kerentanan yang dapat menjadi ancaman. Kerentanan juga menimbulkan risiko dan dapat memunculkan permasalahan yang besar bahkan dapat mengakibatkan kerugian yang besar. Tujuan penelitian adalah merancang bangun sistem penilaian risiko, dokumen peringkat ancaman dan saran pencegahan. Metode yang dipakai menggunakan model DREAD yang dapat menyelesaikan permasalahan dengan memberikan informasi yang berkualitas. Informasi ini dipergunakan untuk menghasilkan peringkat risiko pada aplikasi Web. Hasil dari penelitian adalah sistem penilaian risiko aplikasi web menggunakan model DREAD untuk mengetahui tingkat ancaman risiko serta menyamakan persepsi ancaman risiko web kepada pengembang aplikasi, meminimalkan risiko ancaman dan memaksimalkan kinerja aplikasi web.

Kata-kunci : Model DREAD; Peringkat risiko web; Sistem penilaian risiko web

1. Pendahuluan

Aplikasi yang dikembangkan berbasis web telah mengalami kesuksesan yang luar biasa berkat dari kecanggihan teknologi *World Wide Web* (WWW). Saat ini sebagian besar aplikasi yang dikembangkan dengan menggunakan teknologi web dapat memenuhi kebutuhan pada perbankan, *e-commerce*, pendidikan, pemerintah, hiburan, webmail dan pelatihan. Teknologi web juga dapat dikembangkan dengan teknologi modern dengan tujuan membangun aplikasi web yang lebih dapat diandalkan, sesuai kebutuhan saat ini dan dengan biaya yang lebih efektif dan efesien. Saat ini teknologi web dapat mengatasi berbagai permasalahan seperti masalah teknologi *interoperabilitas*, dapat digunakan dalam beberapa *platform* yang berbeda dan dapat menghubungkan basis data yang berbeda. Meskipun aplikasi web begitu penting baik itu berhubungan dengan teknologi web dan teknik *hacking*, aplikasi web juga mempunyai sisi kerentanan yang dapat menjadi ancaman (Rao dan Pant, 2010).

Kerentanan pada aplikasi web kurang dipahami oleh tim pembuat aplikasi web sedangkan kerentanan pada aplikasi web begitu komplek. Kerentanan meliputi validasi masukan, otentikasi, otorisasi, manajemen konfigurasi, sensitif data, manajemen sesi, kriptografi, parameter manipulasi, exception manajemen, audit dan logging. Dengan adanya kerentanan ini akan menimbulkan risiko dan dapat memunculkan permasalahan yang cukup besar bahkan dapat mengakibatkan kerugian yang cukup besar. Penilaian risiko web pada satu tim pengembangan perangkat lunak aplikasi web masih mengalami permasalahan. Permasalahan yang terjadi adalah bahwa anggota tim tidak seluruhnya menyetujui peringkat risiko ancaman. Permasalahan ini dikarenakan anggota tim mempunyai pendapat dan asumsi yang berbeda-beda tentang ancaman (Meier *et al.,* 2003).

Banyak metode dan model untuk menyelesaikan permasalahan dan penilaian risiko pada aplikasi web. Beberapa metode dan alat yang dapat digunakan

*Penulis korespondensi : diditsuprihanto@yahoo.com

untuk menilai risiko, yaitu NIST (*National Institute of Standard & Technology*), FRAP (*The Facilitated Risk Assessment Process*), COBRA (*The Consultative Objective and Bi-functional Risk Analysis*), OCTAVE (*Operationally Critical, Threat, Asset and Vulnerability Evaluation*) dan *Risk Watch* (Elky, 2006).

Untuk membantu mengatasi masalah ini dan untuk menambahkan dimensi baru dalam menentukan dampak yang terjadi, tentang apakah ancaman keamanan web itu benar-benar berarti maka masalah ini dapat dilakukan proses penilaian risiko dengan model DREAD (*Damage Potential, Reproducibility, Exploitability, Affected User, Discoverability*). Model DREAD merupakan model yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi (Meier *et al.*, 2003).

Penerapan dengan model DREAD diharapkan dapat membantu dalam menyelesaikan permasalahan diatas dengan memberikan informasi yang berkualitas. Informasi ini akan dipergunakan untuk menghasilkan peringkat risiko pada aplikasi Web.

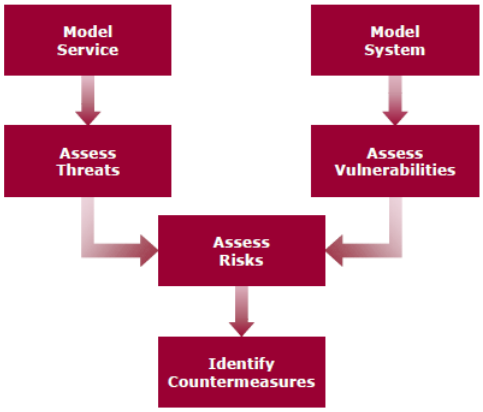
2. Kerangka Teori

Issasalwe dan Ahmed (2011) menjelaskan penanggulangan adalah salah satu cara dalam merencanakan keamanan sistem informasi di masa yang akan datang. Namun, tidak dapat menjamin perlindungan total terhadap segala ancaman.

Penelitian Anderson *et al.* (2006) menjelaskan bahwa memeriksa model merupakan salah satu komponen yang efektif untuk melakukan transaksi *online* yang dapat membangun kepercayaan dan keyakinan pelanggan. Oleh karena itu perusahaan menjadi semakin lebih tergantung pada sistem informasi berbasis internet, sehingga semakin rentan terhadap masalah atau *error* pada sistem sedangkan menurut Wang *et al.* (2002) masalah yang terjadi dalam sistem dapat mengakibatkan kesalahan, kecurangan tidak terdeteksi, dan intrusi berbahaya. Kesalahan sistem Informasi dapat menimbulkan bencana, apakah terjadi pada transaksi pasar, perbankan, kontrol lalu lintas udara, dan sebagainya. Hasil kerusakan dapat mencakup kehilangan pendapatan, kehilangan data, kehilangan kepercayaan, dan meningkatkan biaya.

McEvoy dan Whitcombe (2002) dalam penelitian dengan judul Structured Risk Analysis bahwa tahapan dalam menganalisa dapat dilihat pada Gambar 1.

Pada tahapan ini model layanan dan model system digunakan untuk mengidentifikasi atau menilai terjadinya ancaman dan kerentanan yang ada di dalam sistem. Dari keseluruhan ancaman dan kerentanan yang teridentifikasi disilangkan (*cross*), dengan tujuan untuk memastikan terjadinya kemungkinan ancaman dari suatu kerentanan memunculkan suatu risiko. Apabila ancaman dari suatu kerentanan terbukti maka suatu risiko telah ditemukan.



Gambar 1. Langkah dalam analisis resiko terstruktur

Dalam mengidentifikasi risiko terdapat beberapa faktor yang harus dipertimbangkan. Pertimbangan tersebut antara lain sejauh mana risiko tersebut tereksploitasi dan seberapa besar kerusakan yang akan terjadi. Pertimbangan ini bertujuan untuk pemilihan cara penanggulangan risiko yang paling tepat, cepat dan aman.

2.1. Pengertian Sistem

Sistem didefinisikan sebagai suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang tertentu (Jogiyanto, 2001).

Menurut Jogiyanto (2001) sistem mempunyai beberapa karakteristik, yaitu :

1. Komponen Sistem
   Suatu sistem terdiri dari komponen yang saling berinteraksi, yaitu saling bekerjasama membentuk satu kesatuan. Komponen-komponen suatu sistem disebut subsistem.
2. Batas Sistem
   Merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lain atau dengan lingkungan luarnya. Dengan adanya batas sistem ini, fungsi dan tujuan dari subsistem yang satu dengan yang lainnya berbeda tetapi tetap saling berinteraksi.
3. Lingkungan Luar Sistem
   Segala sesuatu diluar dari batas sistem yang mempengaruhi operasi dari suatu sistem. Lingkungan luar yang bersifat menguntungkan harus dipelihara, sedangkan lingkungan luar yang bersifat merugikan harus dikendalikan agar tidak mengganggu operasi sistem.
4. Penghubung Sistem
   Merupakan media penghubung antara satu subsistem dengan subsistem lainnya. Dengan melalui penghubung ini, output dari suatu

subsistem akan menjadi input bagi subsistem lainnya.

5. Masukan Sistem
   Energi yang dimasukan kedalam suatu sistem yang dapat berupa energi supaya sistem dapat beroperasi. Sebagai contoh, didalam sistem computer, program yang digunakan untuk mengolah data (masukan sistem) menjadi informasi.
6. Pengolah Sistem
   Suatu sistem dapat mempunyai satu bagan pengolah atau sistem itu sendiri sebagai pengolahnya. Pengolah yang akan merubah masukan menjadi keluaran.
7. Keluaran Sistem
   Keluaran adalah hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan. Misalnya untuk sistem computer, panas yang dihasilkan adalah keluaran yang tidak berguna dan merupakan sisa hail pembuangan, sedangkan informasi adalah keluaran yang dibutuhkan.

2.2. Keamanan Sistem

Secara umum, tujuan dari keamanan informasi untuk melindungi kegiatan organisasi untuk menjamin kelangsungan bisnis, meminimalkan kerusakan dan memaksimalkan pengembalian pada investasi (seperti yang didefinisikan oleh ISO/IEC 27002, 2005).

Manajemen keamanan informasi melibatkan gabungan antisipasi, deteksi dan proses respon. Hal ini sesuai rangkaian tindakan dan proses yang membutuhkan konstan pengawasan dan pengendalian yaitu :

1. Menilai risiko keamanan: risiko keamanan melakukan penilaian untuk mengidentifikasi ancaman, kerentanan dan dampak
2. Pelaksana dan menjaga kerangka aman: mendefinisikan dan mengembangkan kebijakan, menetapkan tanggung jawab dan menerapkan tindakan pengamanan
3. Monitoring dan perekaman: pemantauan dan pencatatan terus-menerus sehingga pengaturan yang tepat dapat dibuat ketika menangani sebuah insiden keamanan
4. Meninjau dan meningkatkan: melakukan penelaahan dan security audit untuk memastikan bahwa keamanan memadai kontrol yang memenuhi persyaratan keamanan

Keamanan merupakan himpunan tindakan untuk menjamin ketersediaan, integritas dan kerahasiaan informasi. Hal ini penting untuk organisasi untuk merencanakan ke depan terhadap pelanggaran keamanan. Untuk mengikuti tentu saja, penyedia dapat menawarkan berbagai perlindungan teknis atau firewall enkripsi. Namun, penting untuk menyadari bahwa penggunaan teknik-teknik atau keamanan lain harus hati-hati dan sistematis dalam perencanaan. Hal ini untuk sebuah kontrol implementasi yang optimal dan tepat dalam organisasi. Sedangkan keamanan Informasi merupakan perlindungan informasi dari ancaman dan memastikan kelangsungan usaha dengan meminimalkan risiko bisnis, dan memaksimalkan pengembalian investasi dan peluang bisnis (ISO/IEC 27002, 2005).

2.3. Ancaman, Kerentanan dan Serangan

Menurut Meier *et al.* (2003) menjelaskan tentang definisi ancaman merupakan setiap potensi terjadinya bahaya atau sebaliknya, yang bisa membahayakan aset. Dengan kata lain, ancaman adalah setiap hal yang buruk yang dapat terjadi pada aset. Kerentanan adalah kelemahan yang mungkin dapat menjadi sebuah ancaman. Serangan adalah tindakan yang mengeksploitasi kerentanan atau memberlakukan ancaman.

Tabel 1. Tabel kategori berdasarkan kerentanan Aplikasi

No	Kategori	Ancaman
1	Validasi masukan	Buffer overflow; cross-site scripting; SQL injection; canonicalization
2	Otentikasi	Jaringan menguping; serangan brute force;kamus serangan; ulangan cookie; pencurian credential
3	Otorisasi	Ketinggian hak istimewa; pengungkapan data rahasia, data gangguan, serangan memikat
4	Manajemen konfigurasi	Akses tidak sah ke antarmuka administrasi, akses tidak sah ke toko konfigurasi; pengambilan data konfigurasi teks yang jelas, kurangnya akuntabilitas individu; proses overprivileged dan account layanan
5	Data sensitif	Akses data sensitif dalam penyimpanan; menguping jaringan, data gangguan
6	Sesi manajemen	Sesi pembajakan; ulangan sesi; manusia di tengah
7	Kriptografi	Miskin kunci generasi atau manajemen kunci; enkripsi lemah atau kustom
8	Manipulasi parameter	Query string manipulasi; bentuk manipulasi lapangan; manipulasi cookie; HTTP Header manipulasi
9	Pengecualian manajemen	Pengungkapan informasi; penolakan layanan
10	Audit dan logging	Pengguna menyangkal melakukan operasi; penyerang mengeksploitasi aplikasi tanpa bekas; penyerang menutupi jalur nya

Sumber : Improving web apllication security (Meier *et al.*, 2003)

Menurut Obaidat dan Boudriga (2007) kerentanan keamanan adalah sebuah kelemahan (misalnya, cacat atau lubang) dalam produk, aplikasi, atau aset yang membuatnya layak untuk mencegah penyerang dari

mendapatkan hak istimewa pada organizational sistem, mengorbankan data di dalamnya, memodifikasi operasi, atau dengan asumsi tidak diberikan kepercayaan.

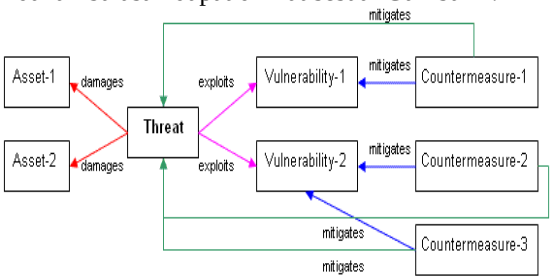
2.4. Model DREAD

Menurut Meier *et al.* (2003) model DREAD merupakan suatu model dari Microsoft yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi. Kepanjangan DREAD adalah *Damage Potential, Reproducibilty, Exploitability, Affected User, Discoverability.*

Untuk mengetahui peringkat risiko dengan model DREAD, beberapa hal yang perlu diperhatikan berhubungan dengan kepanjangan dari DREAD yaitu:

1. *Damage Potential* (potensial kerusakan) yaitu seberapa besar kerusakan jika kelemahan tersebut dieksploitasi.
2. *Reproducibility* (reproduktifitas) yaitu seberapa mudah untuk reproduktifitas serangan itu ?

Keterkaitan antara ancaman, kerentanan aset, dan tindakan balasan dapat dilihat sesuai Gambar 2:



Gambar 2. Keterkaitan antara ancaman, kerentanan asset, dan tindakan balasan (Goldberg, 2005).

3. *Exploitability* yaitu seberapa mudah untuk memulai serangan ?
4. *Affected User* (terkena pengguna) yaitu seberapa besar persentase kasar, berapa banyak pengguna yang terpengaruh ?
5. *Discoverability* yaitu seberapa mudah untuk menemukan kerentanan ?

Penilaian peringkat dengan model DREAD tidak harus menggunakan skala besar karena dapat mempersulit menilai tingkat konsisten ancaman antar satu dengan yang lain. Skala dapat menggunakan skema sederhana seperti tinggi (3), sedang (2), dan rendah (1). Penilaian Ancaman dapat dilihat pada Tabel 2. dan untuk mengetahui tingkat ancaman dengan peringkat jika dapat dilihat pada Tabel 3.

Tabel 2. Penilaian Ancaman Model DREAD

No	Rentang Penilaian	Peringkat	Keterangan Risiko
1	5 hingga 7	3	Rendah
2	8 hingga 11	2	Sedang
3	12 hingga 15	1	Tinggi

Sumber : *Improving Web Apllication Security* (Meier *et al.*, 2003)

Ancaman dijelaskan dalam Gambar 2.2, menyebabkan kerusakan Aset-1 dan Aset-2 dan memanfaatkan dua kerentanan: Kerentanan-1 dan Kerentanan-2. Kerentanan-1 ini diatasi dengan penanggulangan-1 dan Kerentanan-2 diatasi dengan penanggulangan-2 dan balasan-3 seperti dicatat oleh panah biru. Sejak ancaman dapat mengeksploitasi kerentanan beberapa set penanggulangan kemungkinan yang mungkin mengurangi ancaman benar-benar didefinisikan oleh set kerentanan yang digunakan dalam skenario ancaman dan dicatat oleh panah hijau dalam skema (Goldberg, 2005).

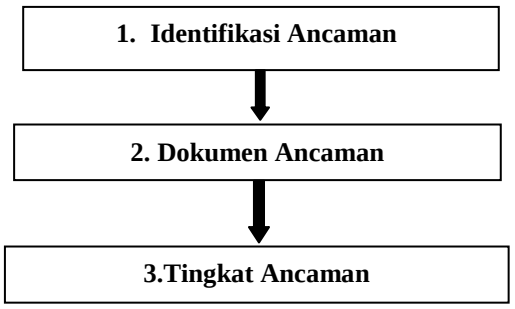
Tabel 3. Peringkat penilaian risiko

	Penilaian	Tinggi (3)	Medium (2)	Rendah (1)
D = Damage potential	Potensi Kerusakan	Penyerang dapat menumbangkan sistem keamanan; mendapatkan otorisasi kepercayaan penuh; berjalan sebagai administrator, meng-upload konten	Membocorkan informasi sensitif	Membocorkan informasi sepele
R= Reproducibility	Reproduktifitas	Serangan dapat direproduksi setiap saat dan tidak memerlukan jendela waktu.	Serangan dapat direproduksi, tetapi hanya dengan jendela waktu dan situasi ras tertentu.	Serangan sangat sulit untuk mereproduksi, bahkan dengan pengetahuan dari lubang keamanan.
E= Exploitability	Exploitability	Seorang programmer pemula bisa membuat serangan dalam waktu singkat.	Seorang programmer yang terampil bisa membuat serangan, kemudian ulangi langkah-langkah.	Serangan itu membutuhkan orang yang sangat terampil dan pengetahuan yang mendalam setiap kali untuk mengeksploitasi.
A=Affected User	Terkena pengguna	Semua pengguna, konfigurasi default, pelanggan utama	Beberapa pengguna, non-konfigurasi default	Persentase yang sangat kecil pengguna, fitur jelas; mempengaruhi pengguna anonim
D= Discoverability	Discoverability	Informasi Diterbitkan menjelaskan serangan.. Kerentanan ditemukan dalam fitur yang paling umum digunakan dan sangat terlihat.	Kelemahan tersebut di bagian yang jarang digunakan produk, dan hanya beberapa pengguna harus datang di atasnya. Ini akan mengambil beberapa pemikiran untuk melihat penggunaan sembarangan.	Bug tidak jelas, dan tidak mungkin bahwa pengguna akan bekerja di luar potensi kerusakan.

Sumber : *Improving Web Apllication Security* (Meier *et al.*, 2003)

3. Metodologi Penelitian

Menurut Meier (2003) jalannya penelitian dapat dilihat pada Gambar 3



Gambar 3. Threat modeling process, (Meier, 2003)

Dimana tahapan-tahapan untuk proses ini adalah:

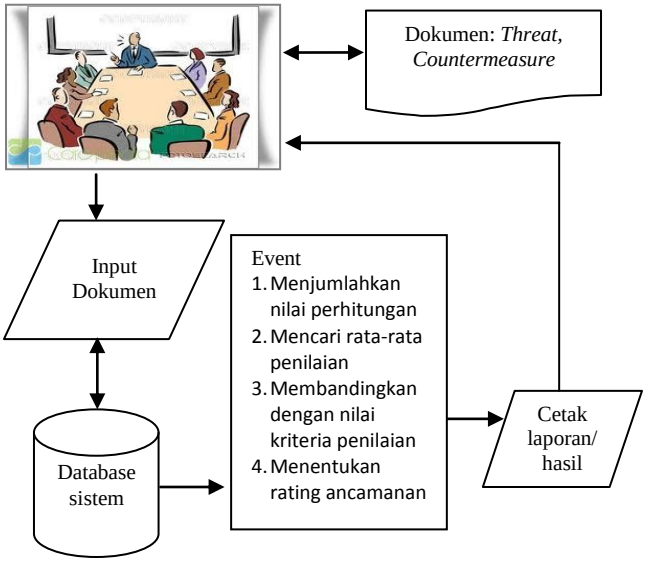
1. Identifikasi ancaman.
   Mengidentifikasi ancaman-ancaman yang dapat mempengaruhi atau merugikan aplikasi.
2. Dokumen ancaman.
   Setiap dokumen ancaman dicatat menggunakan template ancaman umum yang mendefinisikan inti set atribut untuk menangkap setiap ancaman yang terjadi.
3. Tingkat ancaman.
   Memprioritaskan tingkat ancaman dan mengatasi ancaman yang paling signifikan yaitu ancaman yang mempunyai risiko terbesar. Tingginya rating ancaman dapat menyebabkan terjadinya kerusakan yang mengakibatkan mudahnya serangan masuk ke dalam aplikasi. Ancaman yang terjadi tidak langsung dilakukan tindakan tetapi harus dibandingkan dengan risiko yang ditimbulkan oleh ancaman dengan biaya mitigasi (pencegahan/penghentian) yang dikeluarkan.

3.1 Proses Perhitungan Peringkat dengan DREAD

Skala untuk perhitungan dapat menggunakan skema sederhana seperti tinggi (3), sedang (2), dan rendah (1). Pertanyaan-pertanyaan yang diajukan dijawab dengan skala yang telah ditentukan, proses menghitung dengan memberikan nilai dengan skala 1-3 untuk ancaman. Hasil dari penilaian berkisaran 5-15. Kemudian dapat mengetahui tingkat ancaman dengan peringkat jika nilai keseluruhan 12-15 sebagai risiko tinggi, 8-11 sebagai risiko sedang, dan 5-7 sebagai risiko rendah.

3.2 Kerangka Sistem

Keragka sistem penilaian dapat dilihat pada gambar 4.



Gambar 4. Kerangka sistem penilaian web

Gambar 4. merupakan kerangka sistem penilaian, dimana ketua tim selaku administrator menginputkan dokumen yang didapatkan dari referensi-referensi, dan pengetahuan/kepakaran seluruh tim. Dokumen-dokumen yang diinputkan di simpan dalam database, dimana dokumen yang disimpan dipergunakan untuk menjawab dan mengoreksi hasil inputan dari setiap anggota tim. Ketua tim dapat melihat laporan baik setiap anggota tim maupun keseluruhan, dan dapat menghapus/merubah kelompok maupun anggota tim. Sedangkan anggota tim mempunyai kewenangan menjawab pertanyaan dan melihat laporan pribadi.

Laporan yang didapat menghasilkan suatu dokumen peringkat ancaman dan saran pencegahan. Dimana hasil tersebut dipergunakan sebagai bahan pertimbangan dalam pengembangan sistem yang dikembangkan.

4. Hasil dan Pembahasan

Hasil dari proses pemodelan ancaman adalah dokumen untuk berbagai anggota tim proyek. Hal ini memungkinkan mereka untuk secara jelas memahami ancaman yang perlu diatasi dan bagaimana mengatasinya. Model ancaman terdiri dari rating ancaman, dokumentasi/ daftar ancaman dengan *countermeasure*, diperlihatkan seperti Tabel 4 dan Tabel 5 sedangkan grafik model DREAD disajikan pada gambar 5.

Tabel 4. Rating ancaman

No	Ancaman	D	R	E	A	D	Jumlah	User	Rata-rata	Ket
1	Login Tidak Terenkripsi/Password Lemah	14	12	11	9	12	58	5	11	Sedang
2	SQL Injection	15	14	14	15	14	72	5	14	Tinggi
3	Logout tidak tersedia/tidak logout	13	11	10	8	10	52	5	10	Sedang
4	Pencurian data/identitas	15	11	8	9	13	56	5	11	Sedang
5	Gangguan data	13	10	9	7	12	51	5	10	Sedang
6	Informasi tidak diperbarui	8	9	10	8	9	44	5	8	Sedang
7	Akses data sensitif dalam penyimpan	14	13	11	13	11	62	5	12	Tinggi
8	Kegagalan layanan/proses	15	13	14	11	15	68	5	13	Tinggi
9	Akses ke interface yang ilegal/tidak sah	15	12	12	14	12	64	5	12	Tinggi
	Jumlah	122	105	99	93	108	527	45	11	Sedang

Sumber : olahan data primer

Hasil perhitungan kelompok diatas merupakan hasil keselurahan dari perhitungan seluruh anggota tim. Hasil tabel 4 untuk memudahkan dalam menganalisa dengan pengelompokan ancaman secara keseluruhan. Hasil dari dokumentasi/daftar ancaman dengan *countermeasure* terlihat pada Table 5.

Tabel 5. Hasil dari pemodelan ancaman

Deskripsi Ancaman	Login Tidak Terenkripsi/Password Lemah
Target Ancaman	Akses Data
Rating Resiko	Sedang
Teknik Ancaman	Mengungkapkan user name dan password dengan tool, monitoring jaringan
Tindakan Pencegahan	Lakukan validasi input, gunakan enkripsi

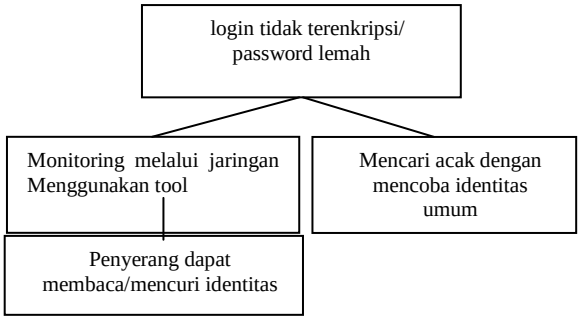
Sumber : olahan data primer

4.1 Identifikasi Ancaman

Identifikasi ancaman merupakan tahapan untuk mengidentifikasi ancaman-ancaman yang sering terjadi. Untuk memudahkan dalam identifikasi digunakan pohon ancaman, dimana pohon ancaman akan menguraikan kemungkinan kejadian-kejadian ancaman terhadap aplikasi maupun maupun data yang tersimpan.

Identifikasi pohon ancaman disajikan sesuai dengan ancaman-ancaman berikut :

Pohon ancaman permintaan login tidak terenkripsi/ password lemah disajikan pada gambar 5



Gambar 5 pohon ancaman login tidak terenkripsi/ password lemah, (Meier *et al.*, 2003)

4.2 Dokumentasi Ancaman

Untuk mendokumentasikan ancaman pada aplikasi, digunakan tempat pencatatan dalam bentuk tabel yang menunjukkan dokumentasi ancaman. Tabel dokumentasi ancaman disajikan tabel 6.

Tabel 6. Dokumentasi ancaman

Deskripsi Ancaman	Login Tidak Terenkripsi/Password Lemah
Target Ancaman	Akses Data
Rating Resiko	
Teknik Ancaman	Mengungkapkan user name dan password dengan tool, monitoring jaringan
Tindakan Pencegahan	Lakukan validasi input, gunakan enkripsi

Sumber : Improving Web Apllication Security, (Meier *et al.*, 2003)

Pada baris 1 dan 2 pada tabel 6 yang dibuat menjelaskan tentang deskripsi ancaman dan target ancaman, dimana deskripsi ancaman dan target ancaman merupakan atribut yang penting.

Baris ke-3 pada tabel 6 adalah peringkat/rating risiko pada tahap dokumentasi ini rating untuk sementara kosong dan akan dibahas pada tahapan selanjutnya yaitu tingkat ancaman. Tahapan Ini merupakan tahap akhir dari proses pemodelan ancaman untuk dilakukan diidentifikasi dan menghasilkan rating/tingkat ancaman. Baris ke 4 dan 5 adalah baris teknik serangan dan tindakan/saran pencegahan dimana pada baris ini dapat mengetahui kerentanan yang dieksploitasi, dan tindakan atau saran pencegahan untuk mengatasi atau mengurangi ancaman..

4.3 Tingkat Ancaman

Pada tahapan ini dilakukan perhitungan tingkat/rating ancaman. Data perhitungan diambil dari pengisian kuisioner model DREAD dari tim pengembang. jumlah tim pengembang adalah 5 orang. Dimana dari tim tersebut data yang didapatkan tersaji pada tabel 7

Tabel 7. Data login tidak terenkripsi/password lemah

No	Nama	D	R	E	A	D	Jml	Rata	Ket
1	Adi S, M.Kom	3	3	3	1	3	13	2.6	Tinggi
2	Awang H, M.Kom	3	3	2	3	2	13	2.6	Tinggi
3	Ahmad R, M.Kom	2	2	2	1	2	9	1.8	Sedang
4	Indah F.A, M.Cs	3	2	2	3	2	12	2.4	Tinggi
5	Hj. Ekawati, MM	3	2	2	1	3	11	2.2	Sedang
	Jumlah	14	12	11	9	12	58	11	Sedang

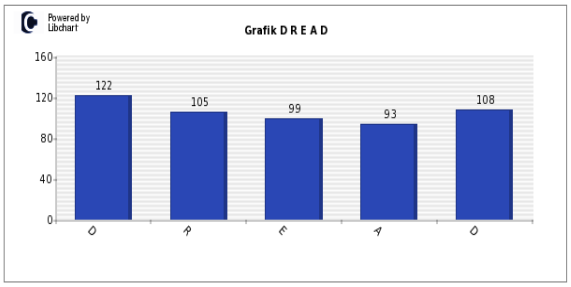
Sumber : olahan data primer

Data diatas didapatkan dari menjawab pertanyaan model DREAD untuk ancaman login tidak terenkripsi/password lemah dari masing-masing

anggota tim. Dari hasil jawaban kemudian ditabulasikan ke dalam tabel sesuai dengan atribut masing-masing pada model DREAD. Setiap jawaban anggota tim di jumlahkan. Untuk mengetahui nilai rata-rata untuk setiap anggota tim, jumlah dari point pertanyaan dibagi dengan banyaknya atribut pada model DREAD adalah 5. Nilai rata-rata tersebut untuk mengetahui hasil dari masing-masing anggota tim dalam menentukan peringkat ancaman. Penentuan tingkat ancaman didapatkan dengan membandingkan nilai rata-rata dengan tabel penilaian risiko ancaman

Dari hasil tersebut dapat ditentukan hasil kelompok untuk ancaman login tidak terenkripsi/password lemah dengan cara menjumlahkan seluruh jawaban dari masing-masing anggota tim sesuai dengan atribut kemudian dibagi dengan 5 (banyaknya anggota dalam tim). Dari hasil perhitungan seluruh anggota kelompok didapatkan nilai rata-rata 58/5 = 11 (nilai pembulatan kebawah), sehingga untuk ancaman login tidak terenkripsi/password lemah secara kelompok mempunyai peringkat/rating sedang. Uraian di atas dipergunakan untuk ancaman-ancaman lain.

Grafik yang ditampilkan merupakan grafik dari keseluruhan ancaman dengan model DREAD. Gambar grafik tersebut disajikan pada gambar 5.



Gambar 5 Grafik model DREAD

Dari grafik diatas dapat diketahui bahwa potensial kerusakan (D) yang terjadi sebesar 122. Dimana nilai tersebut merupakan nilai keseluruhan dari ancaman. Untuk mengetahui rating dari potensial kerusakan dari web maka nilai keseluruhan pada potensial kerusakan dibagi dengan banyaknya ancaman yaitu 122/9 = 13.5 (dibulatkan 13). Artinya bahwa web yang dikembangkan mempunyai dampak kerusakan yang tinggi atau dapat dikatakan bahwa web yang dikembangkan tidak aman atau mempunyai potensial kerusakan yang tinggi. Pada reproduktifitas (R) didapatkan nilai keseluruhan sebesar 105 nilai tersebut merupakan nilai keseluruhan dari ancaman. Untuk mengetahui rating dari reproduktifitas dari web maka nilai keseluruhan pada reproduktifitas dibagi dengan banyaknya ancaman yaitu 105/9 = 11.6 (dibulatkan 11). Artinya bahwa web yang dikembangkan mempunyai reproduktifitas yang sedang atau dapat dikatakan bahwa ancaman yang ada cukup mudah / sedang dalam mereproduksi serangan terhadap web yang dibuat.

Pada eksploitasi (E) didapatkan nilai keseluruhan sebesar 99 nilai tersebut merupakan nilai keseluruhan dari ancaman. Untuk mengetahui rating dari eksploitasi dari web maka nilai keseluruhan pada eksploitasi dibagi dengan banyaknya ancaman yaitu 99/9 = 11. Artinya bahwa web yang dikembangkan mempunyai eksploitasi yang sedang atau dapat dikatakan bahwa ancaman yang ada cukup mudah/sedang untuk dieksploitasi menjadi suatu serangan terhadap web. Pada terkena pengguna (A) didapatkan nilai keseluruhan sebesar 93, nilai tersebut merupakan nilai keseluruhan dari ancaman. Untuk mengetahui rating dari terkena pengguna dari web maka nilai keseluruhan pada terkena pengguna dibagi dengan banyaknya ancaman yaitu 93/9 = 10. Artinya bahwa web yang dikembangkan mempunyai dampak kepada pengguna adalah sedang atau dapat dikatakan bahwa ancaman yang ada mempengaruhi terhadap banyaknya pengguna bernilai sedang. Untuk nilai *discoverability* (D) didapatkan nilai keseluruhan dari ancaman sebasar 108, nilai tersebut merupakan nilai keseluruhan dari ancaman. Untuk mengetahui rating dari *discoverability* maka nilai keseluruhan dibagi dengan banyaknya ancaman yaitu 108/9 = 12. Artinya bahwa rating untuk discoverability adalah tinggi atau dapat dikatakan bahwa untuk menemukan kerentanan pada web yang dibuat adalah sulit/sukar.

5. Kesimpulan

Berdasarkan dari hasil penelitian yang sudah dilakukan, penerapan model *DREAD* pada sistem penilaian risiko aplikasi web dapat diambil beberapa kesimpulan sebagai berikut :

1. Sistem penilaian risiko aplikasi web yang dibangun menggunakan model DREAD dapat digunakan dalam penilaian terhadap aplikasi web.
2. Tingkat ancaman tertinggi adalah SQL injection dengan nilai 14 dan terendah adalah informasi tidak diperbarui tingkat ancaman sedang dengan nilai 8.
3. Secara keseluruhan tingkat ancaman terhadap web yang dibangun adalah sedang dengan nilai 11, artinya web yang dibangun masih memerlukan perbaikan-perbaikan.
4. Potensial kerusakan (D) dari web yang dibangun adalah tinggi (tidak aman) dengan nilai 13, reproduktifitas (R) yaitu kemampuan ancaman untuk mereproduksi serangan adalah sedang dengan nilai 11, Eksploitasi (E) ancaman sedang untuk menyerang web dengan nilai 11, pengaruh terhadap pengguna (A) dengan tingkat ancaman sedang dengan nilai 10 artinya serangan yang terjadi mempengaruhi tidak terlalu besar (sedang), tingkat ancaman *discoverability* (D) adalah tinggi dengan nilai 12 artinya untuk menemukan ancaman pada web adalah sulit/sukar

Daftar Pustaka

Anderson, B.B., Hansen, J.V., Lowry, P.B., Summers, S.L., 2006. The Aplication of Model Checking for Securing E-Commerce Transactions. *Comunications of the ACM* ,49 (6). 97-101.

Elky, S., 2006. An Introduction to Information System Risk Management. SANS Institute InfoSec Reading Room.copyright©SANS Institute.

Goldberg, Y., 2005. Practical Threat Analysis for the Software Industry. PTA Whitepaper. Website : : http://www.securitydocs.com/ library/2848. Diakses tanggal 2 Maret.

ISO/IEC 27002, 2005. Information technology – Security techniques - Code of practice for information security management. Website: http://isvoc.com/download/ISO_27002_EN.pdf, diakses tanggal 12 April.

Issasalwe, A.M., Ahmed, M., 2011. Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure. *International Journal of research and Reviews in Computer Sciense* (IJRRCS) 2 (1). 111-114.

Jogiyanto, H.M., 2001. Analisa dan Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis. Andi Offset, Yogyakarta.

McEvoy, N., Whitcombe, A., 2002. Structured Risk Analysis. *International conference on infrastructure security*, vol. 2437, Bristol , October 1-3, 88-103.

Meier, J.D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, S., Murukan, A., 2003. Improving web application security: Threats and Countermeasures. Microsoft Corporation.

Obaidat, M.S., Boudriga, N.A., 2007. Security of e-Systems and Computer Networks. Cambridge University Press. New York.

Rao, K.R.M., Pant, D., 2010. A Threat Risk Modeling Framework for Geospatial Weather Information System (GWIS) : a DREAD Based Study. *International Journal of Advance Computer Science and Aplications (IJACSA)*, l (3), 20-28.

Wang, W., Hidvegi, Z., Bailey, A.D., Whinston, A.B., 2000. E-process Design and Assurance using model checking. *IEEE Computer*, 33: 48-53.