SISTEM PENILAIAN RISIKO APLIKASI WEB MENGGUNAKAN MODEL DREAD

Tesis
untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-2
Program Studi Magister Sistem Informasi

DIDIT SUPRIHANTO
24010410400014

PROGRAM PASCASARJANA
UNIVERSITAS DIPONEGORO
SEMARANG
2012

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

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.

Keywords : DREAD model, web threat risk, web risk assessment system

BAB I

PENDAHULUAN

1.1 Latar Belakang

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 dkk, 2003).

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

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang diatas, dapat dirumuskan permasalahan bagaimana menerapkan dan membangun sistem penilaian risiko aplikasi web menggunakan model DREAD.

1.3 Batasan Masalah

Penelitian ini dibatasi pada permasalahan-permasalahan sebagai berikut :

1. Ancaman yang diteliti antara lain permintaan login tidak terenkripsi/ password lemah, SQL injection, *account logout* tidak tersedia/tidak logout,

pencurian data/identitas, gangguan data, informasi tidak diperbarui, akses data yang sensitive dalam penyimpan.

2. Penilaian risiko hanya ditujukan pada aplikasi berbasis web
3. Penilaian peringkat risiko menggunakan model DREAD

1.4 Keaslian Penelitian

Penelitian terdahulu menjelaskan perlindungan ancaman difokuskan pada jaringan, *host*, *database* dan aplikasi standar dari ancaman internal dan eksternal. Pengembangan Aplikasi Cepat atau *The Rapid Application Development* (RAD) proses membuat aplikasi web yang singkat dan sulit untuk menghilangkan kerentanan. Dalam penelitiannya mempelajari web aplikasi teknik penilaian risiko yang disebut ancaman pemodelan risiko untuk meningkatkan keamanan aplikasi dengan menerapkan, mengusulkan mekanisme penilaian risiko menggunakan aplikasi ancaman risiko dari Microsoft dengan model DREAD untuk mengevaluasi aplikasi risiko keamanan terhadap parameter kerentanan. Penelitian ini mengukur tingkat risiko yang berbeda untuk Cuaca Geospasial Sistem Informasi (GWIS) menggunakan model DREAD (Rao dan Pant, 2010).

Issasalwe dan Ahmed (2011) menjelaskan penanggulangan merupakan salah satu cara dalam merencanakan keamanan sistem informasi di masa yang akan datang. Namun, tidak dapat menjamin perlindungan total terhadap segala ancaman. Salah satu bagian penting dari rencana manajemen risiko adalah mengevaluasi ancaman sistem dan kerentanan yang dihadapi sistem. Ancaman yang dimaksudkan untuk/atau memiliki kemampuan untuk mencapai niat mereka. Jenis ancaman dan tindakan yang diambil, untuk mengurangi atau menghilangkan risiko yang merupakan subyek utama dari penelitian yang dilakukan. Penelitian yang dilakukan adalah menggunakan percobaan numerik, dengan model kertas *mock-up* dan cara bagaimana menyelesaikan permasalahan sesuai dengan tingkat risiko yang ada .

Perbedaan dengan penelitian yang dilakukan adalah menerapkan dan membangun sistem penilaian risiko aplikasi web menggunakan model DREAD.

1.5 Tujuan Penelitian

Tujuan penelitian merancang bangun sistem penilaian risiko, dokumen peringkat ancaman dan saran pencegahan dengan menggunakan model DREAD.

1.6 Manfaat Penelitian

Manfaat dalam penelitian ini untuk menyamakan persepsi tim pengembangan aplikasi web terhadap peringkat ancaman serta meminimalkan risiko ancaman aplikasi web dan memaksimalkan kinerja aplikasi web.

BAB II

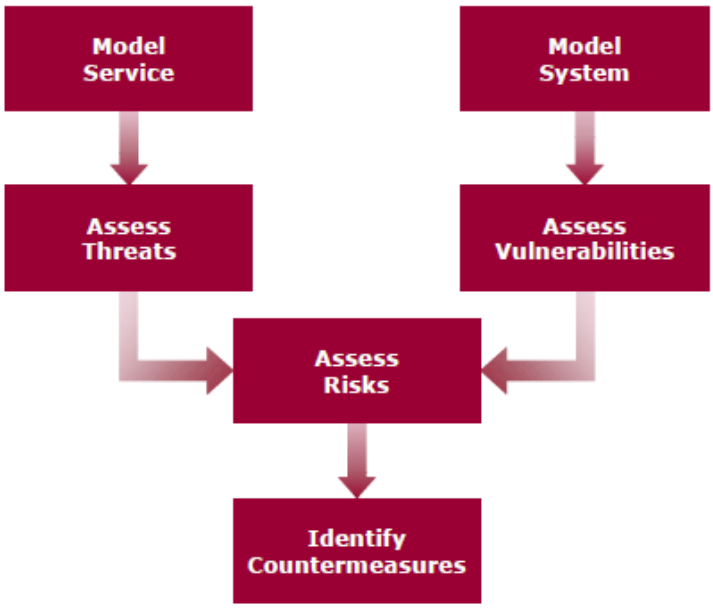
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Issasalwe dan Ahmed (2011) menjelaskan penanggulangan merupakan salah satu cara dalam merencanakan keamanan sistem informasi di masa yang akan datang. Namun, tidak dapat menjamin perlindungan total terhadap segala ancaman. Salah satu penting dari rencana manajemen risiko adalah mengevaluasi ancaman sistem dan kerentanan yang dihadapi sistem. Ancaman yang dimaksudkan untuk atau memiliki kemampuan untuk mencapai niat mereka. Jenis ancaman dan tindakan yang diambil untuk mengurangi atau menghilangkan risiko yang merupakan subyek utama dari penelitian yang dilakukan . Penelitian yang dilakukan adalah menggunakan percobaan numerik, dengan model kertas *mock-up* dan cara bagaimana menyelesaikan permasalahan sesuai dengan tingkat risiko yang ada.

Anderson dkk (2006) menjelaskan 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 tersebut. Menurut Wang, W., dkk (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 tahapan dalam menganalisa dapat dilihat pada Gambar 2.1 :



Gambar 2.1. Langkah analisis risiko terstruktur

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 check*), dengan tujuan untuk memastikan terjadinya kemungkinan ancaman dari suatu kerentanan memunculkan suatu risiko. Apabila ancaman dari suatu kerentanan terbukti maka suatu risiko telah ditemukan.

Untuk 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 penganggulangan risiko yang paling tepat, cepat dan aman.

2.2. Landasan Teori

2.2.1 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.

2.2.2 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 & menjaga kerangka aman: mendefinisikan dan mengembangkan kebijakan, menetapkan tanggung jawab dan menerapkan tindakan pengamanan
3. Monitoring & perekaman: pemantauan dan pencatatan terus-menerus sehingga pengaturan yang tepat dapat dibuat ketika menangani sebuah insiden keamanan

4. Meninjau & 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).

2.2.3 Ancaman (*Threat*), Kerentanan (*Vulnerability*) dan Serangan (*Attacks*)

Menurut Meier dkk (2003) ancaman yang terjadi pada web didefinisikan dengan setiap potensi terjadinya bahaya atau sebaliknya, yang bisa membahayakan aset. Kerentanan merupakan suatu kelemahan yang mungkin dapat menjadi sebuah ancaman. Hal ini mungkin karena miskin desain, kesalahan konfigurasi, atau coding tidak sesuai dan tidak aman. Validasi input yang lemah merupakan contoh dari kerentanan lapisan aplikasi, yang dapat mengakibatkan masuknya serangan.

Beberapa kategori berdasarkan kerentanan aplikasi, dimana dari kerentanan akan menimbulkan suatu ancaman disajikan pada tabel 2.1

Tabel 2.1 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 dkk, 2003)

Serangan merupakan suatu tindakan yang mengeksploitasi kerentanan atau memberlakukan ancaman. Contoh serangan yaitu mengirim inputan atau masukan berbahaya ke aplikasi, menolak layanan. Secara ringkas, ancaman adalah peristiwa potensial yang dapat mempengaruhi suatu aset, sedangkan sebuah serangan yang berhasil mengeksploitasi kerentanan dalam sistem (Meier dkk, 2003)

Menurut Obaidat dan Boudriga (2007) kerentanan keamanan merupakan 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. Contoh-contoh sederhana berikut merupakan pelanggaran keamanan:

1. Sebuah cacat dalam sebuah server web yang memungkinkan pengunjung untuk membaca sebuah file yang tidak berwenang untuk dibaca.
2. Sebuah cacat yang memungkinkan pengguna yang tidak sah untuk membaca file user lain, terlepas dari hak akses pada file.
3. Kenyataan bahwa seorang penyerang dapat mengirim permintaan dengan jumlah yang sangat besar ke server yang dapat mengakibatkan kerusakan atau kegagalan.
4. Sebuah cacat dalam gateway pembayaran yang memungkinkan manipulasi harga yang akan dikirim tanpa diketahui

2.2.4 Model DREAD

Menurut Meier dkk (2003) model DREAD merupakan suatu model dari Microsoft yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi.

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?
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?

Item pertanyaan diatas dapat digunakan untuk menilai setiap ancaman. Pertanyaan diatas juga dapat diperpanjang untuk memenuhi kebutuhan . Misal, dapat menambahkan pertanyaan tentang merusak reputasi potensial:

Reputasi: Berapa besar taruhannya? Apakah ada risiko reputasi, yang dapat menyebabkan hilangnya kepercayaan pelanggan?

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 2.2 :

Tabel 2.2 Penilaian Ancaman Model DREAD

	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 dkk, 2003)

Setelah pertanyaan-pertanyaan yang diajukan dijawab, dilakukan proses menghitung dengan pemberian nilai dengan skala 1-3. Hasil dari penilaian pertanyaan-pertanyaan memiliki rentang nilai 5 hingga 15.

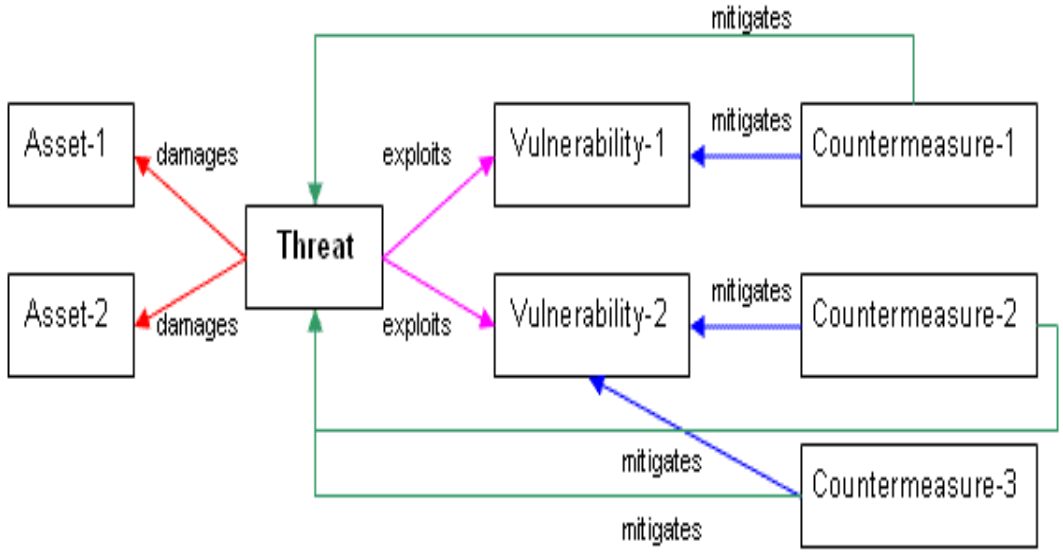
Untuk mengetahui tingkat ancaman dengan peringkat dapat dilihat pada Tabel 2.3.

Tabel 2.3 Peringkat Penilaian Risiko

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 dkk, 2003)

Keterkaitan antara ancaman, kerentanan aset, dan tindakan balasan dapat dilihat sesuai Gambar 2.2 :



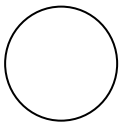
Gambar 2.2 Keterkaitan antara ancaman, kerentanan asset, dan tindakan balasan (Goldberg, 2005).

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).

2.2.5 Diagram Konteks

Diagram konteks suatu diagram yang terdiri dari suatu proses dan menggambarkan ruang lingkup dari sistem. Diagram konteks merupakan level tertinggi dari DFD yang menggambarkan seluruh input atau output dari sistem. Diagram konteks, merupakan gambaran sistem perangkat lunak secara umum dalam bentuk diagram alir. Dalam kontek diagram ini dejelaskan tentang hubungan sistem aplikasi dengan lingkungan sekitarnya (*external entity*) yang berhubungan langsung dengan aplikasi, tetapi tidak menggambarkan tentang *external entity*. Hubungan antara sistem aplikasi dengan *external enti*ty menunjukkan arus keluar masuk informasi yang bisa terjadi (Ladjamudin, 2005). Simbol-simbol dari diagram konteks disajikan pada tabel 2.4

Tabel 2.4 Simbol diagram konteks

Simbol	Keterangan
	Lingkungan entitas
	Entiti atau terminal
	Aliran data

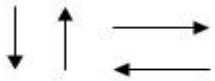
Sumber : Analisis dan Desain Sistem Informasi (Ladjamudin, 2005).

2.2.6 Data Flow Diagram (DFD)

Data Flow Diagram (DFD) merupakan suatu gambaran secara logikal. DFD biasanya digunakan untuk membuat sebuah model sistem informasi dalam bentuk jaringan proses yang saling berhubungan satu sama lainnya oleh aliran data. Keuntungan menggunakan DFD adalah supaya lebih memudahkan pemakai *(user*) yang kurang menguasai dalam bidang komputer untuk lebih mengerti sistem yang akan dikembangkan atau dikerjakan. Proses data pada *Data Flow Diagram* (DFD) merupakan sekumpulan (Jogiyanto, 2001).

Menurut Jogiyanto (2001), *Data Flow Diagram* (DFD) sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir (lewat telpon, surat dan sebagainya) atau lingkungan fisik, dimana data tersebut akan disimpan .

Tabel 2.5 Simbol *Data Flow Diagram* (DFD)

SIMBOL	KETERANGAN
Kesatuan Luar 	Sumber dan tujuan data / External Entity
Arus Data 	Menunjukkan arus data
Proses 	Menunjukkan kegiatan proses
Simpanan Data 	Data Store / tempat menyimpan data

Sumber : Analisa dan Desain Sistem Informasi (Jogiyanto, 2001)

BAB III

METODE PENELITIAN

3.1. Bahan Penelitian

1. Sumber dan jenis data

Sumber data yang digunakan untuk penyelesaian masalah dalam penelitian ini didapatkan dari pendapat para pakar atau pengembang aplikasi web yang dijadikan sumber informasi dalam penginputan dalam sistem. Informasi-informasi ini berupa jenis ancaman yang terjadi pada aplikasi web, dan teknik ancaman dan saran pencegahan dalam kasus-kasus yang terjadi pada aplikasi web. Selain itu, sumber data juga diambil dari jurnal-jurnal nasional maupun internasional yang berkaitan dengan penelitian. Sumber data juga diambil dari beberapa informasi yang peneliti dapat dari internet. Jenis data dalam penelitian merupakan data primer yang didapatkan dari para pakar atau pengembang dengan menginputkan pada sistem penilaian aplikasi, Data-data tersebut dapat berupa informasi-informasi dari anggota tim atau diskusi maupun kuisioner model DREAD.

2. Waktu dan tempat penelitian

Penelitian dan pengambilan data dilaksanakan dari tanggal 20 Februari 2012 sampai dengan 26 Maret 2012. Tempat atau lokasi penelitian pada bagian pengembangan sistem STIMIK Widya Cipta Dharma Samarinda.

3.2 Alat Penelitian

1. Responden

Responden dalam penelitian ini adalah tim pengembang atau pakar. Dimana tim pengembang terdiri dari ketua tim dan anggota. Dalam pelaksanaan, ketua tim merangkap sebagai admin mempunyai kewenangan menginputkan seluruh

anggota tim atau pakar, menginputkan ancaman dan dokumen ancaman serta melihat laporan, baik dari seluruh anggota tim maupun masing-masing anggota tim. Kewenangan dari anggota tim menjawab pertanyaan model DREAD yang terdapat dalam sistem dan melihat laporan.

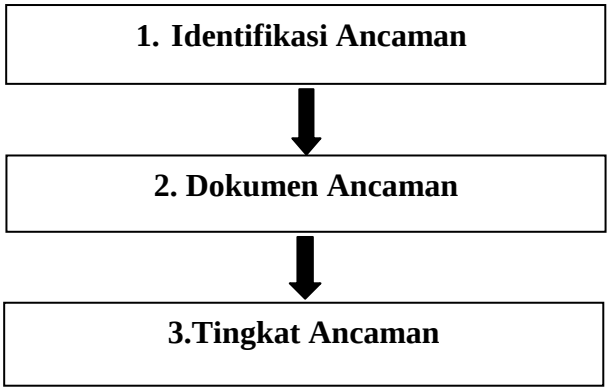
2. Instrumen Implementasi

Alat yang digunakan dalam penelitian ini dibagi menjadi 2 yaitu :

a. Hardware yaitu perangkat keras dapat berupa sebuah unit personal komputer atau laptop/netbook. Dalam penelitian ini digunakan netbook dengan spesifikasi : Prosesor intel atom 1,66 GHz, Memori 1024 MB dan Harddisk 160 GB.
b. Software, yaitu perangkat lunak yang digunakan dalam penelitian adalah system operasi Windows XP, Microsoft Office, Bahasa Pemrograman visual.

3.3. Jalan Penelitian

Menurut Meier (2003) Jalannya penelitian dapat dilihat pada Gambar 3.1 :



Gambar 3.1 Threat modeling process, sebuah gambaran dari proses pemodelan ancaman (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.

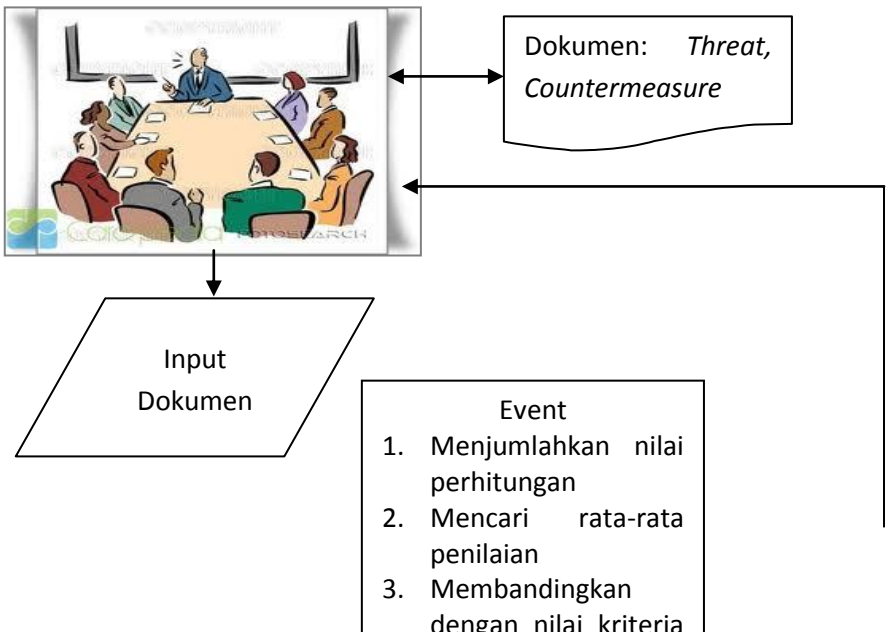
   Memprioritaskan tingkat ancaman dan mengatasi ancaman yang paling signifikan yaitu ancaman yang mempunyai risiko terbesar. Tingginya rating ancaman dapat menyebabkan terjadinya kerusakan yang mengakibatkan mudahnya serangan masuk ke dalam aplikasi. Ancaman yang terjadi tidak langsung dilakukan tindakan tetapi harus dibandingkan dengan risiko yang ditimbulkan oleh ancaman dengan biaya mitigasi (pencegahan/penghentian) yang dikeluarkan.

3.4. 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 (Meier, 2003).

3.5. Kerangka Sistem

Kerangka sistem dapat dilihat pada Gambar 3.2



Gambar 3.2. Kerangka sistem penilaian web

Gambar 3.2 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.

3.6. Desain interface

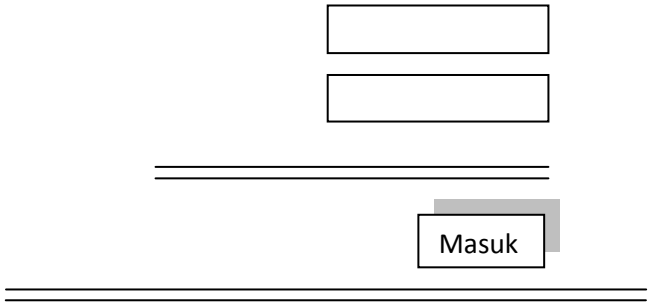
Desain interface dalam pembuatan sistem disesuaikan berdasarkan kebutuhan. Tujuan desain ini dimaksudakn mempermudah pengguna dalam pengoperasian, sehingga pengguna akan merasa nyaman dan mudah dalam menggunakan program aplikasi.

Desain interface dapat dilihat sesuai gambar berikut :

1. Desain Login Admin dan Anggota Tim

   Desain login ini gunakan oleh admin dan anggota tim pada awal masuk pada sistem penilaian. Desain login disajikan pada gambar 3.3

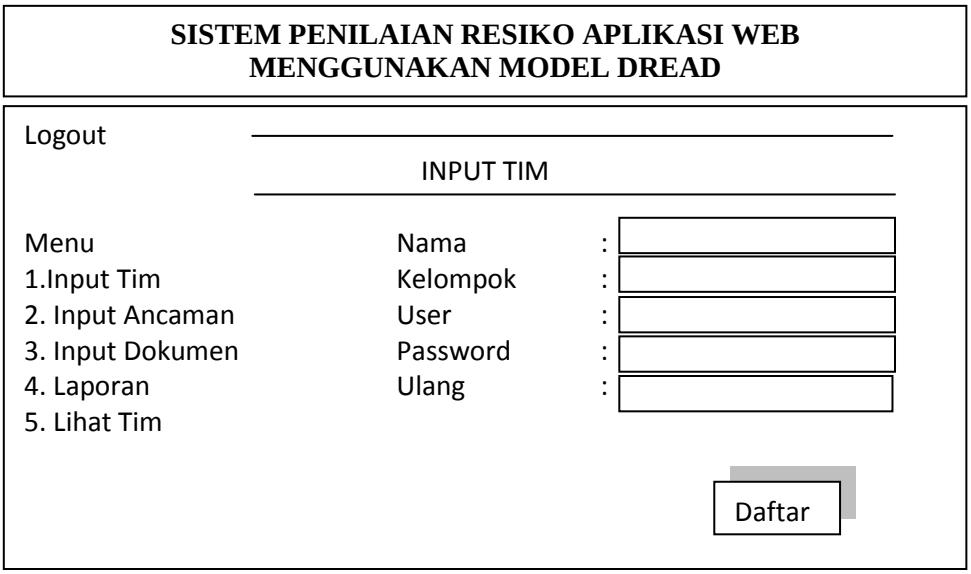
SISTEM PENILAIAN RESIKO APLIKASI WEB MENGGUNAKAN MODEL DREAD
User : Password :



Gambar 3.3 Desain login admin dan anggota tim

2. Desain Input Tim

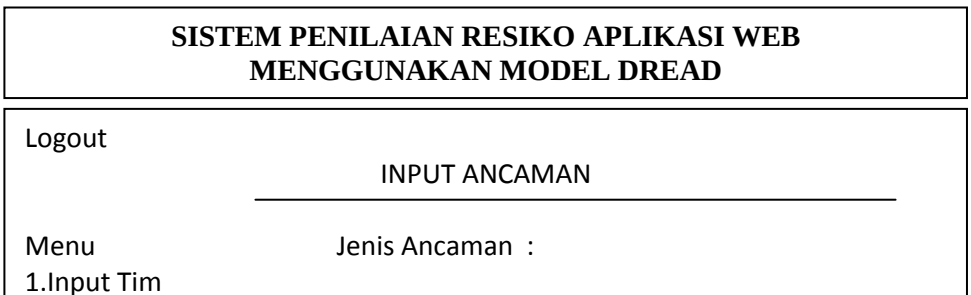
   Desain input tim digunakan untuk memasukkan anggota tim. Anggota tim ini sebagai tim penilai untuk risiko aplikasi web. Desain input dapat dilhiat pada gambar 3.4

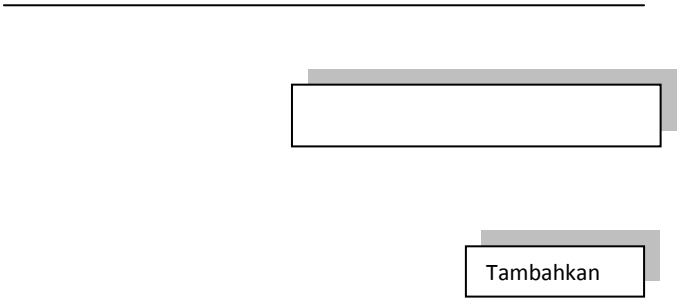


Gambar 3.4 Desain input tim

3. Desain Input Ancaman

   Desain input dokumen dapat dilihat pada gambar 3.5 berikut :



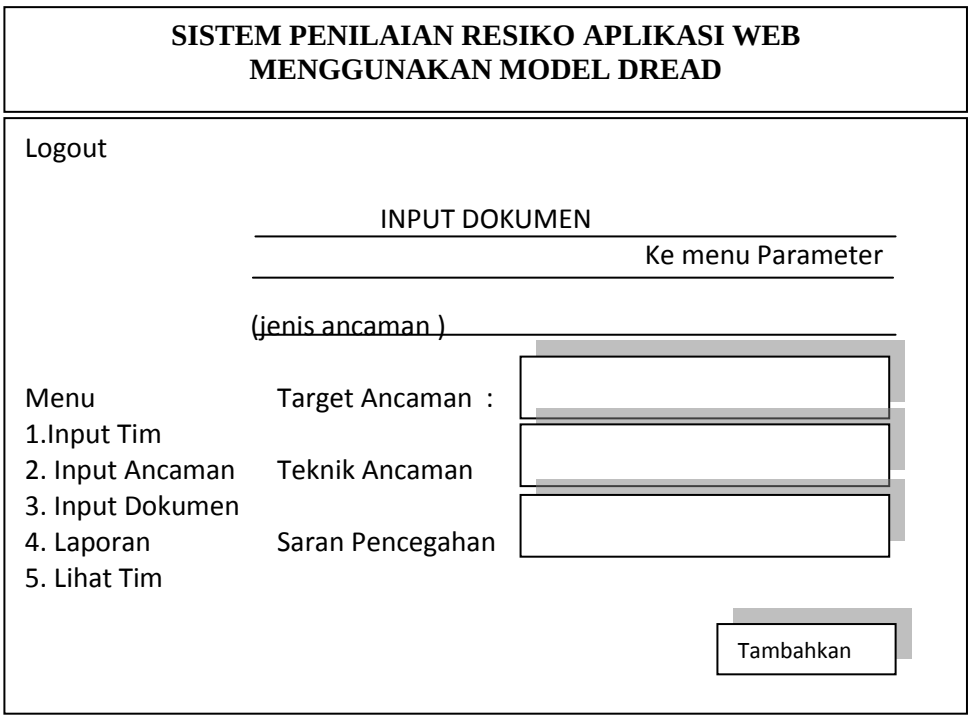


Gambar 3.5 Desain input ancaman

Desain input ancaman dipergunakan menginputkan ancaman yang terjadi. Dimana penginputan jenis-jenis ancaman ini dilakukan oleh administrator yang kemudian akan dilanjutkan pada penginputan dokumen.

4. Desain Input Dokumen

Desain input dokumen dapat dilihat pada gambar 3.6 berikut :



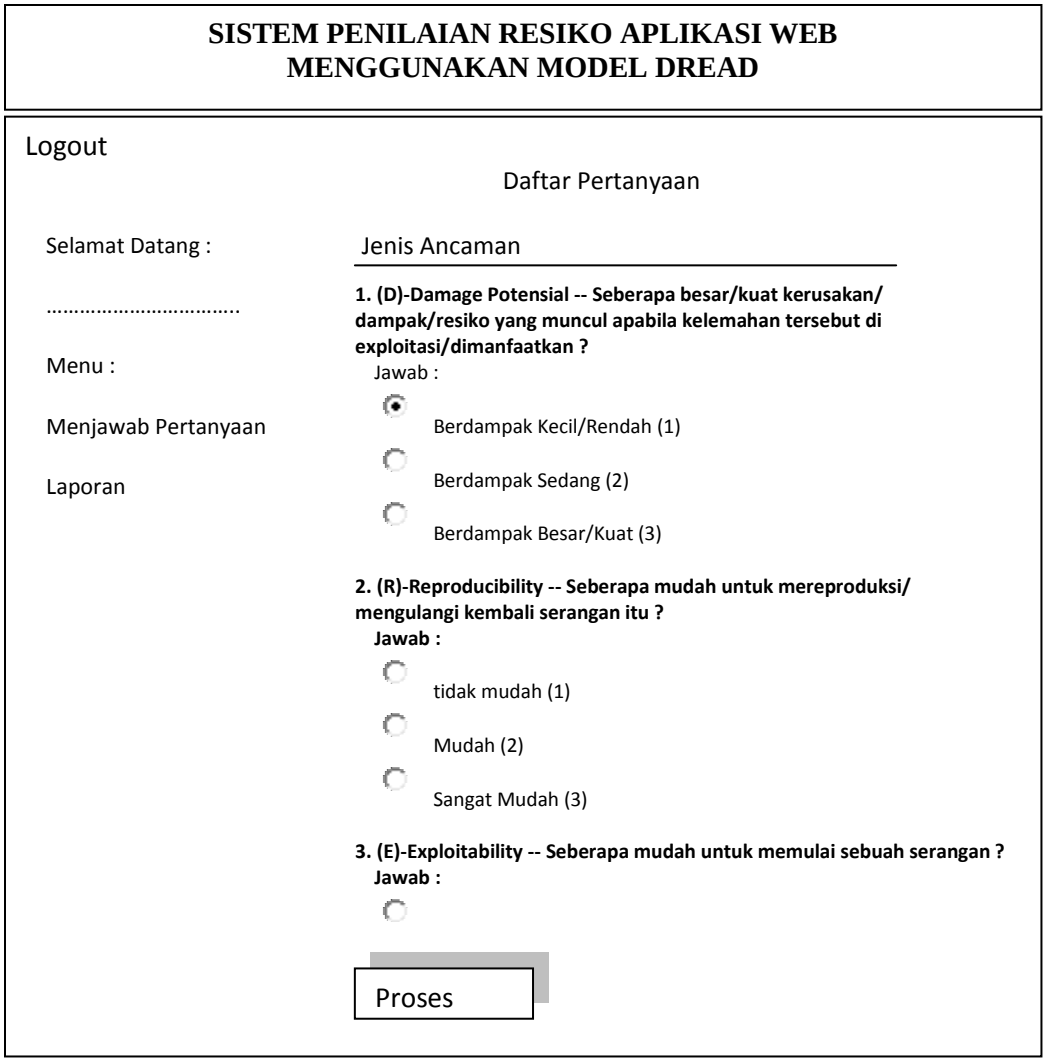
Gambar 3.6 Desain input dokumen

Desain input dokumen terdiri dari 3 inputan yaitu target ancaman, teknik ancaman dan saran pencegahan. Input dokumen ancaman dilakukan oleh ketua tim selaku

administrator. Data-data yang diinputkan berasal dari referensi-referensi dan pengetahuan dari pakar.

5. Desain Daftar Pertanyaan Model DREAD

Desain daftar pertanyaan dipergunakan oleh seluruh anggota tim. Anggota tim dalam menjawab pertanyaan hanya diberikan satu kali kesempatan. Artinya anggota tim hanya bisa sekali menjawab pertanyaan pada setiap ancaman. Pertanyaan-pertanyaan tersebut merupakan pertanyaan model DREAD artinya pertanyaan tersebut tetap dan bersifat statis. Desain pertanyaan disajikan pada gambar 3.7



Gambar 3.7 Desain daftar pertanyaan model DREAD

6. Hasil dari Pemodelan Ancaman

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 3.1 dan Tabel 3.2.

Tabel 3.1 Rating ancaman

Jenis Ancaman	D	R	E	A	D	Total	Rating
Permintaan login tidak terenkripsi	3	3	2	2	2	12	Tinggi
account logout tidak tersedia	2	3	2	1	1	9	Sedang
sesi informasi tidak diperbarui	3	2	3	2	1	11	Sedang
Pencurian data/identitas	1	2	3	1	1	7	Rendah

Improving Web Apllication Security (Meier dkk, 2003)

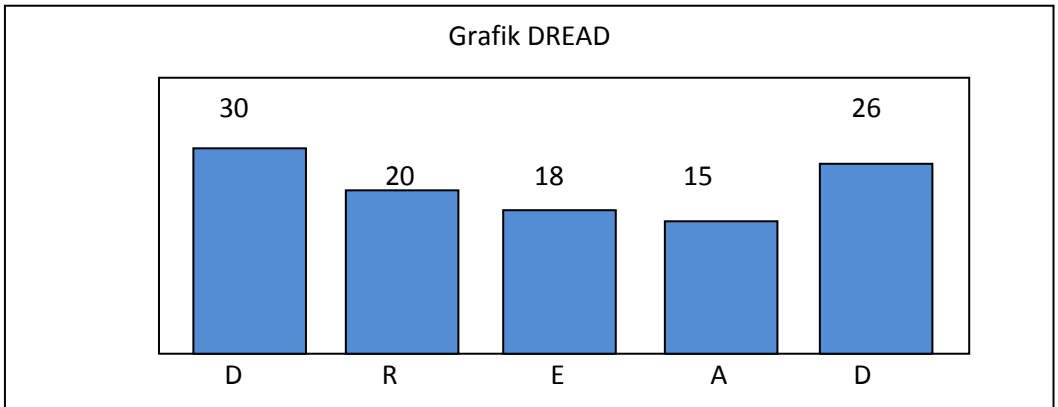
Sedangkan hasil dari dokumentasi/daftar ancaman dengan *countermeasure* diperlihatkan seperti tabel 3.2 :

Tabel 3.2. Hasil dari pemodelan ancaman

Deskripsi Ancaman	Permintaan Login tidak terenkripsi
Target ancaman	…….
Rating risiko	……..
Teknik ancaman	……..
Saran pencegahan	……..

Improving Web Apllication Security (Meier dkk, 2003)

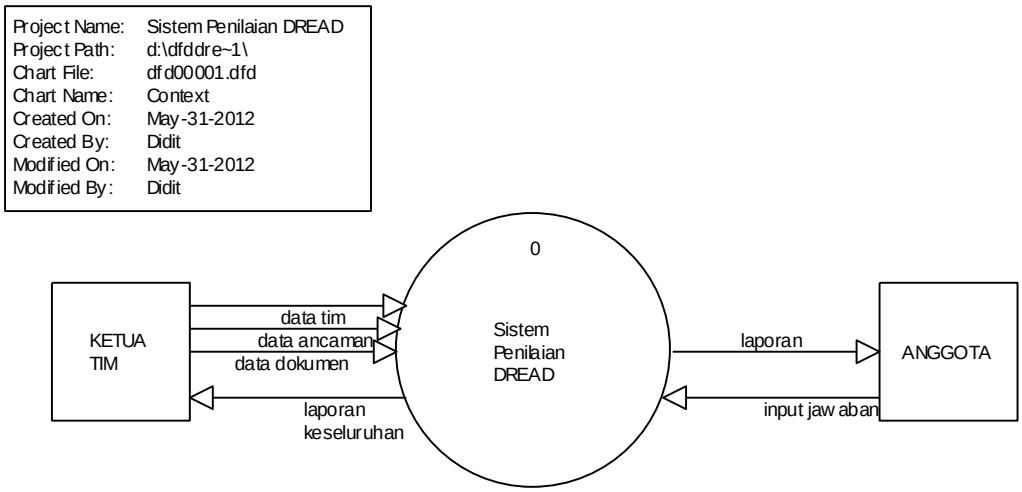
Grafik model DREAD disajikan sesuai gambar 3.8



Gambar 3.8 Grafik model DREAD

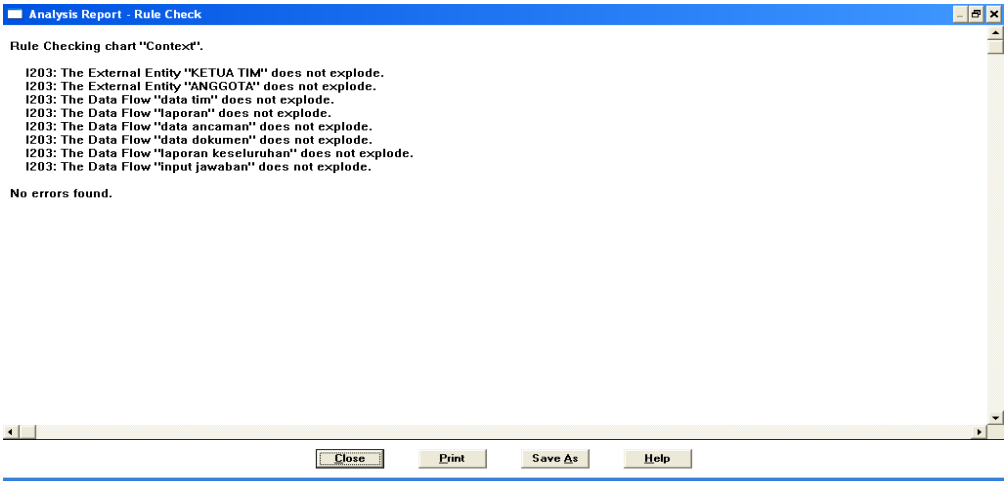
7. Desain Diagram Konteks

   Desain diagram konteks disajikan pada gambar 3.9



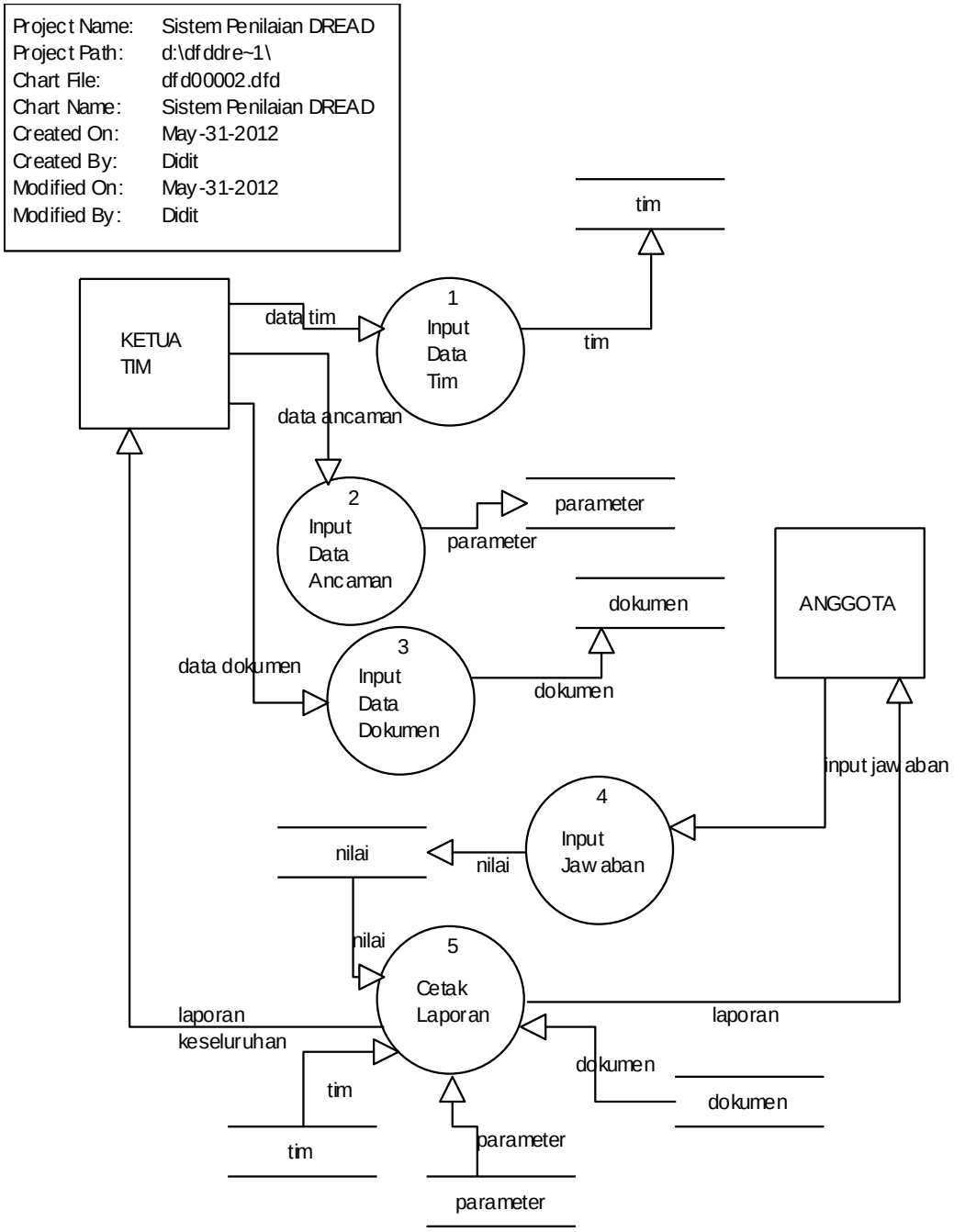
Gambar 3.9 Diagram konteks sistem penilaian DREAD

Gambar 3.9 menjelaskan terdapat 3 aliran data yang masuk ke sistem dari entity luar yaitu ketua tim dan 1 aliran data (input jawaban) dari entity anggota. Laporan yang diterima oleh ketua tim merupakanhasil dari seluruh inputan sedangkan laporan yang diterima anggota merupakan laporan yang dihasilkan dari menjawab pertanyaan tiap-tiap anggota tim. Diagram konteks diatas telah dilakukan pengkoreksian dapat dilihat pada gambar 3.10



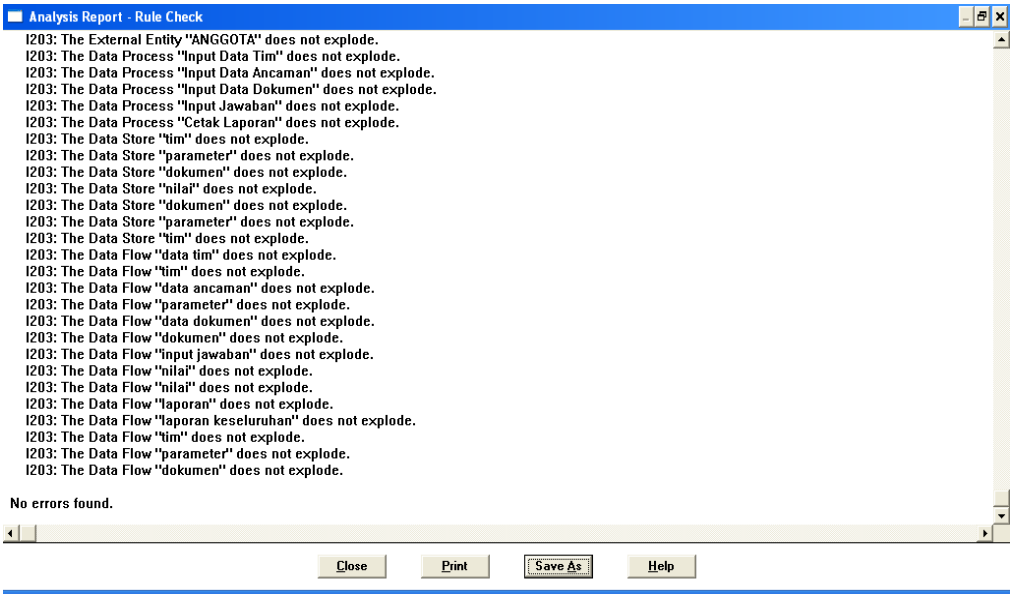
Gambar 3.10 Hasil koreksi diagram konteks

Tahapan selanjutnya adalah proses pada level 1 dimana pada level ini terdapat lima proses. proses ini merupakan uraian dari level 0 (diagram konteks) diatas. Gambar 3.11 menunjukkan proses-proses pada level 1



Gambar 3.11 diagram level 1

Hasil pengkoreksian pada level 1 dapat dilihat pada gambar 3.12

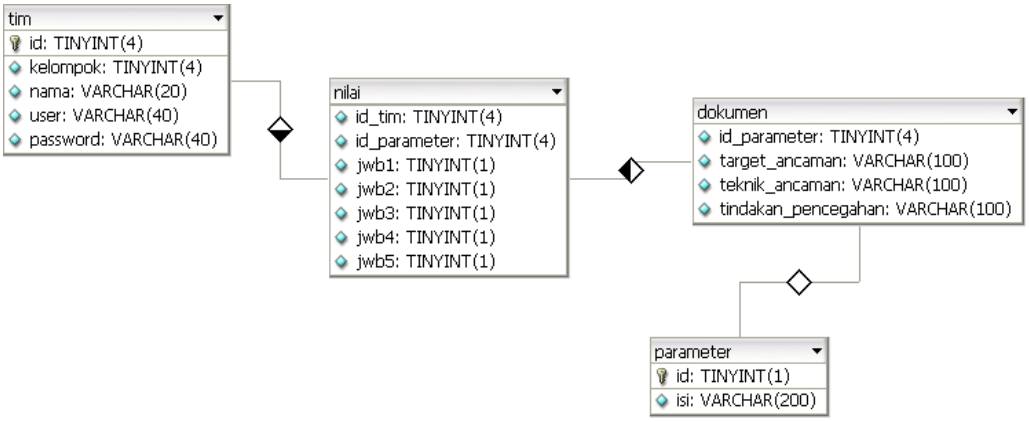


Gambar 3.12 Hasil koreksi level 1

Pada gambar 3.12 hasil koreksi level 1 tidak ditemukan kesalahan artinya diagram level 1 tersebut aliran data dalam proses benar

8. Desain Entity Relation Diagram

Desain tabel-tabel ditampilkan dalam bentuk relasi antar tabel, dapat dilihat pada gambar 3.13 berikut :



Gambar 3.13 Desain relasi antar tabel