PEMBANGUNAN WEBSITE DIABETES HEALTHY SOLUTION CENTER (STUDI KASUS : KEAMANAN WEBSITE)

Hikmah Mahathir[1], Entin Martiana Kusumaningtyas [2], Wahjoe Tjatur Sesulihatien[2], Idris Winarno [2]
Mahasiswa[1] , Dosen [2]
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114
Email : hikmah@kinekora.com

Abstrak

Diabetes merupakan salah satu penyakit yang menjangkiti masyarakat kita saat ini, tidak peduli muda sampai tua semua bisa terjangkiti.diperlukan suatu kebiasaan hidup yang sehat untuk mengatasi diabetes itu sendiri. Dengan adanya suatu website, kebiasaan hidup ini akan banyak terbantu. Untuk studi kasus dalam website ini adalah Sistem keamanan webiste dimana diperlukan suatu keamanan yang dapat menjaga rahasia dari beberapa hak akses yaitu admin ataupun user, keamanan ini sangat diperlukan mengingat sering terjadi penyerangan-penyerangan terhadap website baik itu serangan Sql Injection, Cross Side Scripting dan lain sebagainya.
Kata kunci **: *daily activity, admin, user.***

1. Pendahuluan

1.1 Latar Belakang

Diabetes merupakan salah satu penyakit yang menjangkiti masyarakat kita saat ini, tidak peduli muda sampai tua semua bisa terjangkiti. Diabetes juga tidak bisa disembuhkan hanya dengan meminum beberapa obat saja, diperlukan suatu terapi atau kebiasaan hidup sehat yang dapat meminimalisir dari gejala diabetes itu sendiri.

Dengan adanya suatu website, kebiasaan hidup ini akan banyak terbantu. Website dapat menemani gaya hidup sehat para penderita diabetes dengan memberikan artikel, ataupun *sharing-sharing* antar user. Selain itu banyak sekali fitur yang dapat dimanfaatkan di website ini yaitu aplikasi diagnosa Nutrisi untuk Penderita Diabetes dengan Berbagai Komplikasi Menggunakan Metode Fuzzy dan ada pula aplikasi Sistem Informasi Gizi Untuk Penderita Diabetes Menggunakan Metode Fuzzy Query Database.

Untuk studi kasus dalam website ini adalah Sistem keamanan webiste dimana diperlukan suatu keamanan yang dapat menjaga rahasia dari beberapa hak akses yaitu admin ataupun user, keamanan ini sangat diperlukan mengingat sering terjadi penyerangan-penyerangan terhadap website baik itu serangan Sql Injection, Cross Side Scripting dan lain sebagainya. Untuk penanggulangan dalam hal sql injection didalam penyusunan TA ini menggunakan beberapa referensi dari buku *Advanced Sql Injection* yang ditulis oleh penulis Chapela Viktor dan *Sql Injection Attack and Defense* yang ditulis oleh Clarke Justin.

1.2 Tujuan Proyek

proyek akhir ini dibangun untuk menghasilkan website yang membantu para membernya dalam berkehidupan sehat ala diabetes

1.3 Kontribusi Proyek

Hasil dari proyek akhir ini diharapkan dapat memberikan kemudahan bagi penderita diabetes.

2. Teori Penunjang

2.1 Keamanan Website

Pada pembangunan website ini sangat sekali diperlukan suatu keamanan yang dapat menjaga agar website tidak dirusak dari pihak pihak yang tidak bertanggung jawab. Dari beberapa macam kejahatan pengrusakan website terdapat beberapa cara untuk menanggulanginya. Ada 3 cara yang digunakan dalam pembangungan website ini

dalam menjaga keamanannya yaitu penggunaan protokol Https, penggunaan aplikasi Fail2Ban, dan HTML Guardian.

2.1.1 Sql Injection

Sql injection merupakan salah satu teknik yang digunakan attacker untuk mengeksekusi query database di url untuk mendapatkan akses membaca informasi-informasi rahasia pada situs target. Biasanya attacker menginjeksi kan script-script sql kedalam url atau textfield itu sendiri. Dengan mencoba berbagai macam sintak sql yang disisipkan akan didapatkan beberapa informasi penting yang terdapat didatabase. Terdapat beberapa cara untuk menginjeksi script sql tersebut yaitu:

1. Menginputkan script di field-field yang disediakan di halaman website
2. Menambahkan script parameter di url website
3. Memasukkan script ke dalam cookie yang akan dikirim kembali ke website
4. Memasukkan script kedalam hidden field.

Ada beberapa macam karakter yang diinputkan sebagai karakter SQL injection yaitu diantaranya,

Tabel 2.1 jenis karakter sql injection

No	Jenis Karakter	Contoh
1	character String Indicators	' or "
2	single-line comment	-- or #
3	multiple-line comment	/*…*/
4	addition, concatenate (or space in url)	+
5	(double pipe) concatenate	‖
6	wildcard attribute indicator	%
7	URL Parameters	?Param1=foo&Param2=bar
8	useful as non transactional command	PRINT
9	local variable	*@variable*
10	global variable	*@@variable*
11	time delay	waitfor delay '0:0:10'

Berikut adalah Pola-pola dari Sql Injection yang menyebabkan suatu query bernilai benar yaitu :

- ' OR 'unusual' = 'unusual'
- ' OR 'something' = 'some'+'thing'
- ' OR 'text' = N'text'
- ' OR 'something' like 'some%'
- ' OR 2 > 1
- ' OR 'text' > 't'
- ' OR 'whatever' IN ('whatever')
- ' OR 2 BETWEEN 1 AND 3
- ’ OR ’’ = ’

Perbedaan injeksi pada numerik dan string value yang paling dominan adalah penggunan tanda quotes (‘) pada parameter injeksi.

Untuk menghindari serangan Sql Injection terdapat beberapa cara yaitu :

1. Membuat Input Validation

Dengan cara memberi suatu filter inputan karakter pada setiap parameter GET dan POST. Dengan begitu seorang attacker akan terbatas sekali dalam melakukan injection.

```
1   public String filterInput(String input){
2       input=input.replace("","");
3       input=input.replace("&quot;","");//"
4       input=input.replace("`","");
5       input=input.replace("?","");
6       input=input.replace("NULL","");
7       input=input.replace("-","");
8       input=input.replace("\n","");
9       input=input.replace("\r","");
10      input=input.replace("/","");///x1a
11      input=input.replace("/x1a","");
12      input=input.replace("=","");
13      return input;
14  }
```

Potongan program 2.1 filter input validation

Pada potongan program diatas adalah sebuah fungsi yang bertujuan untuk menghilangkan karakter karakter yang sering digunakan dalam teknik sql injection.

1. Penggunaan aplikasi Banned IP termasuk Fail2ban, dimana Fail2ban akan mengirim nomor IP yang gagal menginputkan password dan username sebanyak yang telah ditentukan
2. Penggunaan Aplikasi –aplikasi pemfilter inputan di suatu website seperti mod security.
3. Penggunaan konsep AJAX pada setiap halaman website. Dengan menggunakan konsep AJAX, halaman yang menjadi response suatu konsep AJAX tidak akan mengeluarkan pesan error pada halaman websitenya, karena apabila terjadi error pada suatu proses di website, proses javascript-nya tidak akan melanjutkan prosesnya.

2.1.2 HTML Guardian

Suatu aplikasi pengenskrip script-script pemrograman website yang dapat mengenskrip script-script website mulai dari html, javascript. Mengingat script javascript di penggunaan konsep AJAX kali ini, sangatlah mudah untuk dilihat dari pihak client

2.1.3 Fail2Ban

Adalah suatu aplikasi yang mencegah adanya suatu serangan Bruce Attack terhadap suatu inputan di field – field halaman website. Aplikasi tersebut akan membekukan (banned) nomer IP dari suatu user yang mencoba beberapa kali melakukan serangan penginputan karakter yang dapat mencari bug dari suatu website dengan melihat beberapa kali inputan suatu user yang salah. Alamat-alamat IP yang terdaftar dalam list Fail2ban tersebut akan dikirim ke firewall untuk melarang hak akses untuk sementara(tergantung pengaturan)

2.1.4 HTTPS

HTTPS adalah suatu protokol versi aman dari HTTP(protokol komunikasi dari World Wide Web). Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi.

Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers dan man in the middle attacks. Pada umumnya port HTTPS adalah 443 tetapi untuk Projek Akhir kali ini menggunakan port 8443 dan sebagai default dari port HTTPS dari web server tomcat.

Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang aktual. Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan 'https://' bukan dengan 'http://'

2.1.5 Tomcat Server

Tomcat adalah sebuah merupakan web server yang memberikan layanan data yang berfungsi menerima permintaan HTTP atau HTTPS dari klien yang dikenal dengan browser web dan mengirimkan kembali hasilnya dalam bentuk halaman - halaman web yang umumnya berbentuk dokumen HTML. Tomcat sendiri merupakan sebuah implementasi Java Servlet dan JSP teknologi bersifat open source milik Apache Software Foundation. Tomcat sering kali digunakan sebagai development server, hal ini dikarenakan salah satu sifatnya yang lightweight dibandingkan dengan servlet container maupun application server sejenisnya.

Untuk penginstallannya, tomcat server pada projek akhir kali ini yang diinstall pada OS debian mempunyai beberapa langkah yaitu,

- Apt-get update
  Perintah ini berfungsi sebagai pengupdate daftar paket installan terbaru yang lokasi alamat pendownloadannya berada pada file /etc/apt/sources.list
- apt-get install sun-java6-jdk
  karena tomcat server ditulis dalam bahasa java, maka dperlukan paket install dari JDK. Perintah tersebut adalah perintah untuk menginstall JDK.
- Menyetting nama variabel untuk JAVA_HOME dan JRE_HOME

```
1  Echo 'JAVA_HOME="/usr/lib/jvm/java-6-sun"'
2  >>
3   /etc/environtment
4  Echo 'JRE_HOME="/usr/lib/jvm/java-6-sun/jre"'
5  >>
    /etc/environtment
```

Potongan program 2.2 setting JAVA_HOME dan JRE_HOME

JAVA_HOME pada baris 1, merupakan nama variabel dari folder instalasi JDK.

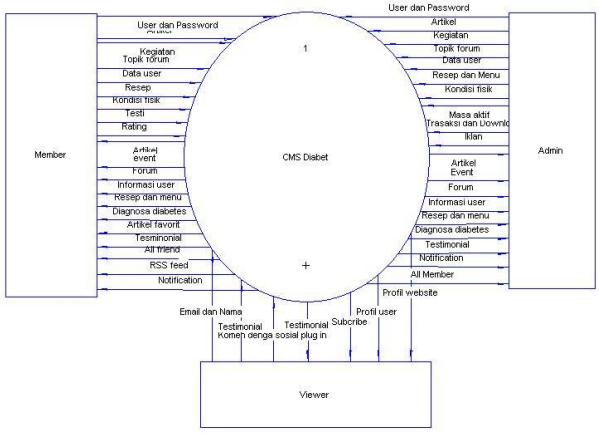
- Dkpg –i tomcat6
  Perintah diatas merupakan menginstall tomcat6 berasal dari paket tomcat yang berekstensi *.deb
- Untuk mengkonfigurasi username dan password dari admin bisa dikonfigurasi pada file berikut /usr/share/tomcat6/tomcat-users.xml

```
1   <role rolename="manager"/>
2   <user username="thirx"
    password="12345" roles="manager"/>
```

Potongan program 2.3 konfigurasi tomcat-user.xml

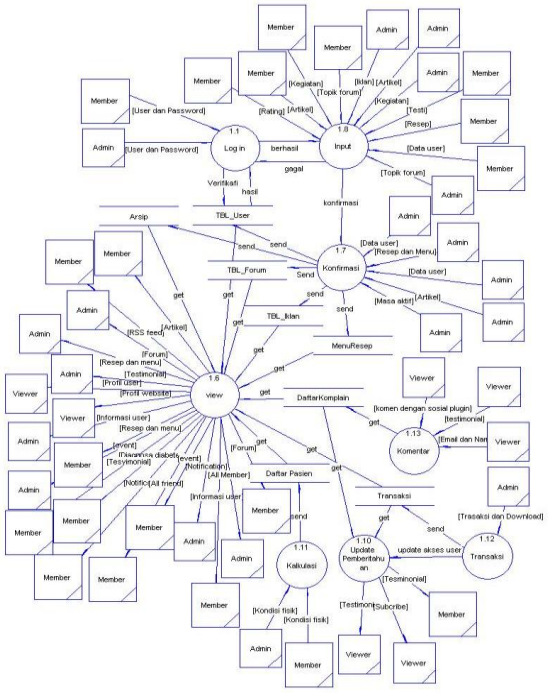
3.1. Pembuatan Sistem

Rancangan CMS website Healthy Solution Center



Gambar 3.2 DFD level 0

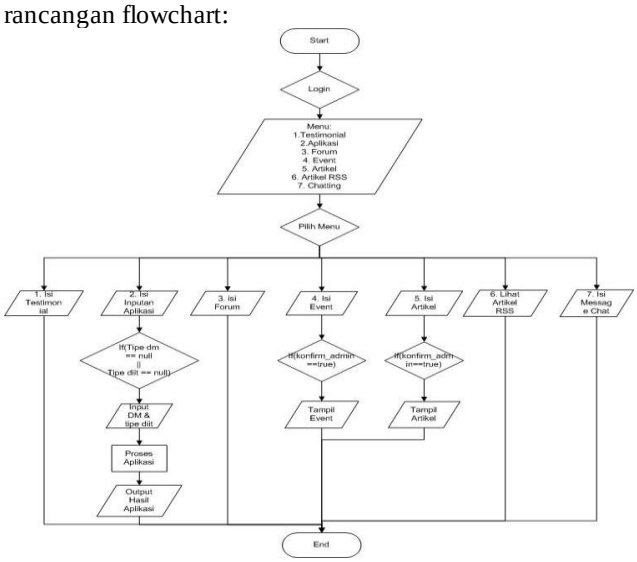
DFD tingkat 1 menunjukkan jalan alur proses suatu sistem dimana proses tersebut dilakukan secara mendetail dan sebagai turunan dari level 0 yang ditunjukkan pada gambar dibawah ini :



Gambar 3.2 DFD level 1

3.2. Perancangan Proses

Pada bagian ini akan ditunjukkan flowchart proses pada sistem. Diawali dengan proses login oleh user, jika username dan password benar, maka dapat melakukan transaksi atau perintah pada sistem. Perintah tersebut akan di cek dengan data yang ada dalam database, jika data ditemukan dalam database maka sistem akan menampilkanya di website. Berikut adalah gambar rancangan flowchart:



3.4 Perancangan Keamanan

Pada pembangunan website kali ini digunakan 3 aplikasi utama dalam mengamankan website yaitu:

- HTML Guardian, aplikasi ini dapat mengenskrip script javscript yang rentan dapat dilihat oleh pihak client
- SSL
  Dimana dengan menggunakan HTTPS protocol, dapat membantu mengamankan data yang di request oleh pihak client.
- Fail2ban.
  Dimana dengan menggunakan aplikasi Fail2ban dapat membantu memblok nomer nomer IP yang telah mencoba penyerangan kedalam website.

3.4.1 HTML Guardian

Berikut alur yang dikerjakan dalam keamanan menggunakan HTML Guardian.

1. Memisahkan script javascript yang berbentuk fungsi dan yang tidak berbentuk fungsi kedalam file file tersendiri.
2. Mengenskrip file javascript yang berbentuk fungsi menggunakan HTML Guardian
3. Mengganti nama pemanggilan file javascript di file index.jsp

3.4.2 SSL

Berikut alur yang dikerjakan dalam keamanan menggunakan SSL:

1. Generate key public dan key private, dengan menggunakan command keytool sebagai berikut:

```
1  keytool -genkey -alias tomcat -keyalg RSA
```

Potongan program 4.2 command keytool generate key

Pada step ini akan digenerate 2 key yaitu key public dan key private yang identik pada satu komputer server tempat dimana meng generate key tersebut.

2. Setelah itu mengaktifkan beberapa konfigurasi pada file server.xml yang terdapat pada direktori tomcat $CATALINA_HOME/conf/server.xml

Dengan cara menghilangkan tanda komentar pada file tersebut

```
1  <Connector port="8443" protocol="HTTP/1.1"
2  SSLEnabled="true"
3  maxThreads="150"
4  scheme="https"
5  secure="true"
6  clientAuth="false"
7  sslProtocol="TLS"
8  keystore="/etc/tomcat6/keystore"
9  keystorePass="changeit" />
```

Potongan program 4.3 connector tomcat SSL

3. Restart tomcat

/etc/init.d/tomcat6 restart

4. Pembuatan sertifikat yang akan kita upload.

keytool -certreq -keyalg RSA -alias tomcat -file certreq.txt

Setelah itu kita buka halaman website http://oak.cs.ucla.edu/cs144/projects/project5/cert/ dan mengunggah file certreq.txt tersebut untuk mendapatkan sebuah sertifikat yang akan kita pakai dalam perintah selanjutnya. Dan selanjutnya kita simpan file sertifikat hasil.

5. Install file sertifikat tersebut untuk tomcat dengan menggunakan command:

```
keytool -import -alias tomcat -file /usr/local/signedcert.cert
```

Potongan program 4.4 command keytool import

6. Restart web server (TOMCAT) kembalingaturan redirect url website.

3.4.3 Fail2ban

Dalam projek akhir kali ini terdapat 3 file yang dikonfigurasi untuk menjalankan aplikasi fail2ban yaitu :

1. /etc/fail2ban/Jail.conf

sebagai file konfigurasi utama dalam penginstalan file2ban dimana semua pengaturan tentang jail ada di file ini dan pendaftaran filter beserta aksi setelah pemblokkan ada disini juga. Berikut adalah cuplikan program yang menjadi konfigurasi tambahan untuk menambahkan jail baru yaitu squirrelmail.

```
1 [squirrelmail]
2 ignoreip = 10.252.0.0/16 202.9.85.0/24
3 enabled = true
4 port = 8080,8443
5 filter = squirrelmail
6 logpath = /var/log/squirrelmail.log
7 maxretry = 10
```

Potongan program 4.7 jail.conf

2. /etc/fail2ban/Filter.d/Squirrelmail.conf

Khusus untuk directory /etc/fail2ban/filter.d/ merupakan sebuah folder yang menangani segala macam bentuk filter dalam fail2ban. Didalam squirrelmail.conf terdapat dua perintah baris potongan program yang wajib untuk ada yaitu filter regex dan ignore regex, dimana keduanya adalah sebuah filter regular expression yang mengatur format kalimat yang telah menjadi standar dalam pembuatan log didalam pencacatan fail2ban. Untuk lebih lengkapnya dalam file squirrelmail.conf seperti berikut :

```
1 [Definition]
2 failregex = \[LOGIN_ERROR\].*from <HOST>:
3 Unknown user or password incorrect
4 ignoreregex =
```

Potongan program 4.8 squirrelmail.conf

3. /var/log/Squirrelmail.log

Merupakan sebuah file yang mencatat kegiatan login gagal dan login yang berhasil.

Dimana pada baris pertama merupakan format untuk login yang sukses, sedangkan untuk login yang error terletak pada baris kedua dan ketiga.

4.Analisa Dan Kesimpulan

Berdasarkan hasil pengujian sistem yang telah dilakukan didapatkan beberapa analisa untuk keamanan website.

1. Untuk aplikasi HTML Guardian , hanya 1 macam file yang kompatible pada CMS kali ini yaitu file javascript dengan tipe file yang berisikan fungsi-fungsi sedangkan untuk file javascript yang berisikan trigger yang harus ready saat program berjalan,file hasil enskripsi tidak dapat berjalan pada program.
2. Penggunaan protocol HTTPS pada projek CMS ini dapat membantu mengamankan pengiriman paket data antara client dan server. Dimana di projek akhir kali ini terdapat beberapa fitur yang harus diamankan informasi privari dari user.
3. Penggunaan Fail2ban dapat diintegrasikan dengan CMS Healthy Solution Center.

Daftar Pustaka

[1] ***http://diabetes.diabetes****journals.org/* diakses pada tanggal 5 Mei 2010

[2] ***http://care.diabetesjournals.org/*** diakses pada tanggal 7 Mei 2010

[CV Penulis]

Hikmah Mahathir, menjalankan studi D3 bidang Teknik Informatika pada Politeknik Elektronika Negeri Surabaya – Institut Teknologi Sepuluh Nopember(PENS-ITS) semester 6.