BAB 3
ANALISIS DAN PERANCANGAN

Tahap analisis dan perancangan diperlukan tahapan sistematis agar aplikasi yang dibuat sesuai dengan kegunaan dan tujuannya. Tahap pertama dari analisis adalah melakukan analisis sistem, mulai dari analisis masalah, analisis fungsional dan analisis non-fungsional. Sedangkan untuk tahap perancangan dimulai dengan melakukan perancangan sistem dan perancangan antarmuka yang akan digunakan untuk diterapkan pada aplikasi.

3.1 Analisis Masalah

Analisis masalah merupakan penjabaran tentang masalah apa saja yang ada sebelum dibangun dan bermaksud untuk membatu pengelola website dalam meningkatkan keamanan. Adapun analisis masalah yang ada meliputi hal-hal berikut :

1. Sulitnya untuk menemukan file *backdoor shell* pada *web server* yang telah terinfeksi.
2. Kurangnya akurasi dari aplikasi sejenis dalam menemukan file *backdoor shell* pada *web server*.

3.2 Analisis Aplikasi Sejenis

Analisis yang dilakukan merupakan observasi terhadap aplikasi sejenis untuk melihat cara kerja dengan tujuan melihat ada tidaknya kekurangan maupun kelebihan dari aplikasi tersebut. Hasil dari observasi tersebut untuk membantu dalam penelitian.

3.2.1 Grep

Grep merupakan aplikasi bawaan pada linux yang berbasis Command Line Interface (CLI), grep command digunakan sebagai pencarian text atau pencarian file yang mengandung kalimat/kata tertentu.

Contoh penggunaan Grep dalam pencarian *backdoor shell* :

```
$ grep –Rn “passthru|system|eval|exec|shell_exec” /var/www
```

Gambar 3. 1 Contoh penggunaan grep

Saat perintah grep diatas dieksekusi maka akan dilakukan pencarian file yang terdapat didalam directori “/var/www” dimana file yang akan dicari mengandung baris yang memiliki kata passthru,system,eval,exec dan shell_exec. Penggunakan metode ini sangat mudah untuk menemukan file yang memiliki kata-kata yang dicari namun pengguna harus terlebih dahulu mengetahui jenis-jenis fungsi yang dimiliki oleh backdoor berikut perbandingan dengan aplikasi yang akan dibangun :

Tabel 3. 1 Perbandingan dengan grep

Grep	Aplikasi yang akan dibagun
Berbasis Command Line Interface (CLI).	Berbasis Gui dijalankan pada tampilan website.
Pencarian berdasarkan keyword yang ditentukan oleh user.	Pencarian berdasarkan Backdoor Signature dan Function backdoor.
Output pencarian berupa tampilan list pada terminal.	Output pencarian berupa tampilan list pada GUI yang dapat diberi tindakan lansung.
Baik digunakan oleh user yang memiliki basic linux.	Baik digunakan oleh user yang tidak memiliki basic linux.

3.2.2 NeoPi

NeoPi merupakan script python yang menggunakan berbagai metode statistic untuk mendeteksi konten yang dikaburkan atau di enkripsi dalam file text/ script dengan menghitung dari daftar beberapa indeks seperti signature, entropy coincidence dan kata terpanjang.

Tujuan yang dimaksud NeoPi adalah untuk membantu dalam deteksi webshell yang tersembunyi. Dan fokus pengembangan NeoPi adalah menciptakan alat yang dapat digunakan bersama dengan metode lain yang ditetapkan sebagai

pendeteksi malware pada linux. Mendeteksi berdasarkan signature atau keyword based.

Berikut cara penggunaan NeoPi, setelah script didownload dan dicopi dari github maka jalankan perintah ini pada web server yang di indikasi terinfeksi webshell.

```
[Zee@WebServer2 opt]$ sudo ./neopi.py -C scan1.csv -a -A
```

Gambar 3. 2 Contoh penggunaan neopi

Hasil dari scan akan disimpan dalam file scan1.csv dan berikut potongan contoh hasil dari scanning menggunakan NeoPi

```
[root@WebServer2 opt]# python neopi.py -a -A /var/www/html/

[[ Average IC for Search ]]
0.0372337579606

[[ Top 10 IC files ]]
  0.0156    /var/www/html/webmedia/shell3.php
  0.0178    /var/www/html/phpadmin/phpMyAdmin-3.3.8-all-
languages/lang/chinese_simplified-utf-8.inc.php
  0.0184    /var/www/html/wordpress/wordpress/wp-admin/weevely.php
  0.0217    /var/www/html/joomla/templates/system/index.php
  0.0217
/var/www/html/joomla/administrator/templates/system/index.php
  0.0225    /var/www/html/wordpress/wordpress/wp-
admin/js/revisions-js.php
  0.0229    /var/www/html/epesiBIM/epesi-1.1.3-
rev7318/modules/Base/Mail/language/phpmailer.lang-ch.php
  0.0239    /var/www/html/epesiBIM/epesi-1.1.3-
rev7318/modules/Base/Mail/language/phpmailer.lang-zh.php
  0.0240    /var/www/html/epesiBIM/epesi-1.1.3-
rev7318/modules/Base/Mail/language/phpmailer.lang-zh_cn.php
  0.0248    /var/www/html/phpadmin/shell2.php
```

Gambar 3. 3 Contoh hasil scanning neopi

Berikut perbandingan dengan aplikasi yang akan dibangun :

Tabel 3. 2 Perbandingan dengan neopi

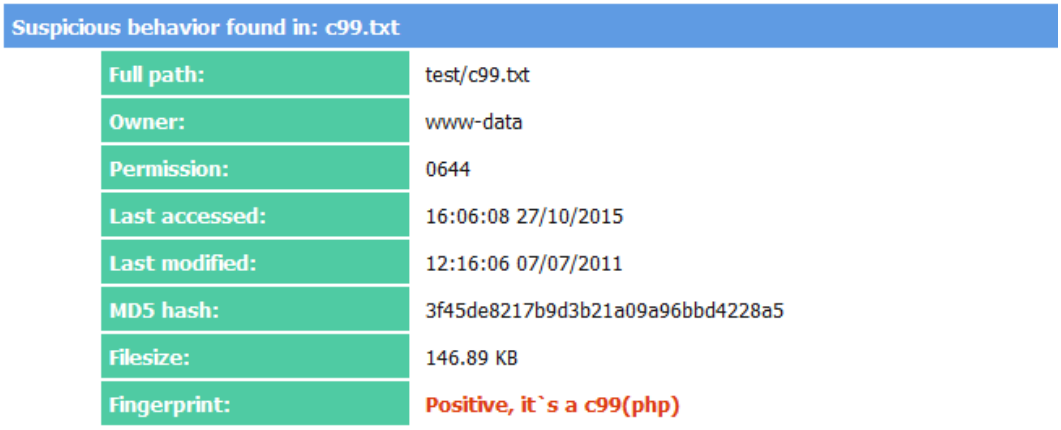
NeoPi	Aplikasi yang akan dibagun
Berbasis Command Line Interface (CLI).	Berbasis Gui dijalankan pada tampilan website.

NeoPi	Aplikasi yang akan dibagun
Pencarian dengan target file yang terenkripsi dengan signature backdoor.	Pencarian berdasarkan Backdoor Signature dan Function backdoor.
Output pencarian berupa tampilan list pada terminal.	Output pencarian berupa tampilan list pada GUI yang dapat diberi tindakan lansung.
Baik digunakan oleh user yang memiliki basic linux.	Baik digunakan oleh user yang tidak memiliki basic linux.

3.2.3 PHP Shell Detector

Web shell detector merupakan *script* php yang membantu dalam pencarian dan pengidentifikasi file php/cgi(perl)/asp shell. *Web shell detector* menggunakan *signature backdoor* yang terdapat pada database dalam pencarian *web shell*.

Berikut hasil dari scanning menggunakan *shell detector* :



Gambar 3. 4 Contoh scanning php shell detector

Berikut perbandingan webshell detector dengan aplikasi yang dibangun :

Tabel 3. 3 Perbandingan dengan php shell detector

Webshell Detector	Aplikasi yang akan dibagun
Berbasis Gui dijalankan pada tampilan website	Berbasis Gui dijalankan pada tampilan website.

Webshell Detector	**Aplikasi yang akan dibagun**
Pencarian berdasarkan list finggerprint backdoor dan function.	Pencarian berdasarkan Backdoor Signature dan Function backdoor.
Output pencarian hanya berupa tampilan list pada interface, tidak dapat diberi tindakan pada interface.	Output pencarian berupa tampilan list pada interface yang dapat diberi tindakan lansung.
Hasil scanning terlalu banyak. Tidak ada penyaringan terhadap file yang dicurigai	Hasil scanning difilter berdasarkan nilai poin sebagai indikasi backdoor shell.

3.3 Analisis Sistem

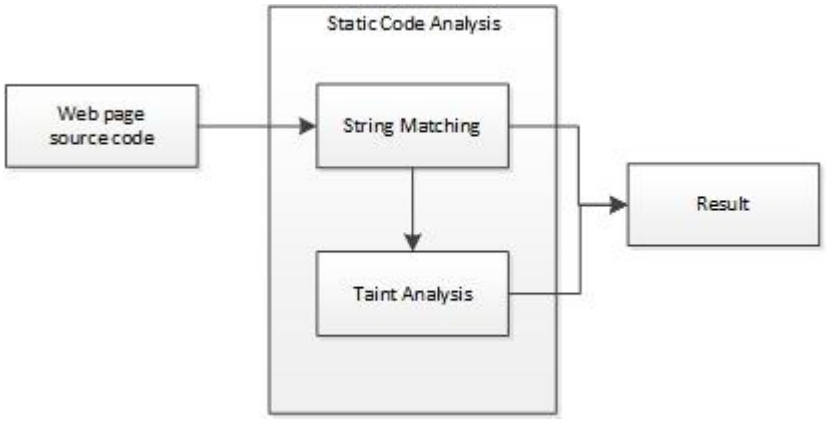
Analisis sistem merupakan penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya yang dimaksudkan untuk mengidentifikasi dan mengevaluasi segala permasalahan dan hambatan yang terjadi serta kebutuhan yang diharapkan dapat menjadi acuan untuk diusulkannya perbaikan-perbaikan.

Tahap analisis sistem ini sangat penting karena apabila terjadi kesalahan dalam tahap ini akan mengakibatkan kesalahan pada tahap selanjutnya, untuk itu diperlukan tingkat ketelitian dan kecermatan yang tinggi untuk dapat mendapatkan kualitas kerja sistem yang baik.

3.3.1 Analisis Metode *Basic Static Code Analysis*

Dalam pembangunan aplikasi pendeteksi *backdoor shell* berdasarkan permasalahan yang sudah dipaparkan sebelumnya, menggunakan beberapa teknik dari *Basis Static Code Analysis* yaitu :

1. *String Matching* yang akan digunakan untuk menganalisis kata kunci pada code yang memiliki indikasi sebagai file ilegal seperti *backdoor shell signature*.
2. *Taint Analysis* yang akan digunakan untuk menganalisis *source code* yang mengandung fungsi-fungsi yang diidentifikasi sebagai *backdoor shell*.

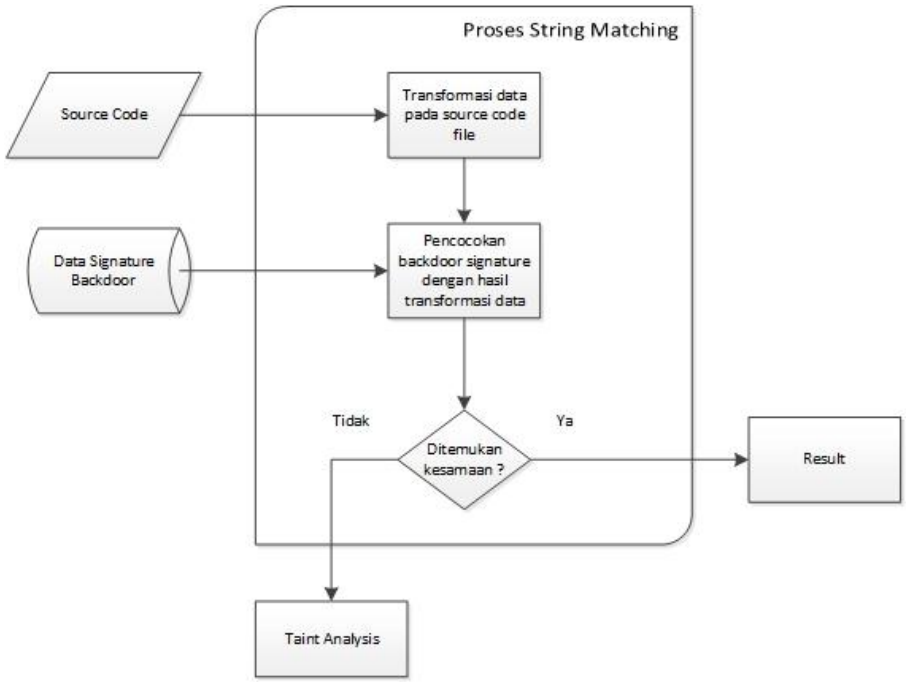


Gambar 3. 5 Tahapan metode static code analysis

Berikut penjelasan dari alur proses sistem menggunakan *Metode Static Code Analysis* :

3.3.1.1 String Matching

Merupakan tahapan awal dalam menganalisis *source code*. Pada modul ini file akan dilakukan pencarian *keyword* yang memiliki indikasi backdoor shell dengan cara pencocokan string pada *source code* terhadap data *backdoor signature* yang terdapat pada database. Untuk lebih jelas lihat pada gambar 3.6 berikut :



Gambar 3. 6 Proses string matching

Tahap awal pada proses ini system mengambil source code pada webserver kemudian dilakukan transformasi data source code secara keseluruhan yang akan dianalisis. Contoh pada file worse.php yang akan dianalisis pada gambar 3.7

```
print "<form method=post enctype=\"multipart/form-data\"><table>";
print "<tr><td><b>Execute command:</b></td><td><input size=100
name=\"_cmd\" value=\"".$currentCMD."\"></td>";
print "<td><input type=submit name=_act
value=\"Execute!\"></td></tr>";
print "<tr><td><b>Change directory:</b></td><td><input size=100
name=\"_cwd\" value=\"".$currentWD."\"></td>";
print "<td><input type=submit name=_act value=\"List
files!\"></td></tr>";
```

Gambar 3. 7 Kutipan source code worse.php

Kemudian pada source code tersebut dilakukan transformasi data menggunakan fungsi base64_encode berikut contoh kutipan file worse.php yang telah ditransformasikan :

```
cHJpbnQgIjxmb3JtIG1ldGhvZD1wb3N0IGVuY3R5cGU9XCJtdWx0aXBhcnQvZm9ybS1
kYXRhXCI+PHRhYmxlPiI7CnByaW50ICI8dHI+PHRkPjxiPkV4ZWN1dGUgY29tbWFuZD
o8L2I+PC90ZD48dGQ+PGlucHV0IHNpemU9MTAwIG5hbWU9XCJfY21kXCIgdmFsdWU9X
CIiLiRjdXJyZW50Q01ELiJcIj48L3RkPiI7CnByaW50ICI8dGQ+PGlucHV0IHR5cGU9
c3VibWl0IG5hbWU9X2FjdCB2YWx1ZT1cIkV4ZWN1dGUhXCI+PC90ZD48L3RyPiI7CnB
yaW50ICI8dHI+PHRkPjxiPkNoYW5nZSBkaXJlY3Rvcnk6PC9iPjwvdGQ+PHRkPjxpbn
B1dCBzaXplPTEwMCBuYW1lPVwiX2N3ZFwiIHZhbHVlPVwiIi4kY3VycmVudFdELiJcI
j48L3RkPiI7CnByaW50ICI8dGQ+PGlucHV0IHR5cGU9c3VibWl0IG5hbWU9X2FjdCB2
YWx1ZT1cIkxpc3QgZmlsZXMhXCI+PC90ZD48L3RyPiI7Cg
```

Gambar 3. 8 Kutipan hasil transformasi worse.php

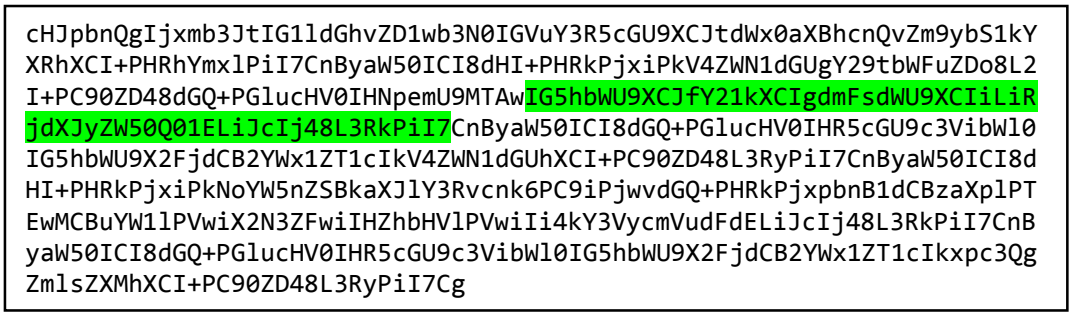
System akan melakukan request *signature backdoor* pada database yang berupa string hasil dari *encode* dengan fungsi base64_encode. Contoh :

```
IG5hbWU9XCJfY21kXCIgdmFsdWU9XCIiLiRjdXJyZW50Q01ELiJcIj48L3RkPiI7
```

Gambar 3. 9 Backdoor shell signature

String pada gambar 3.9 merupakan *signature* milik *backdoor shell* “worse”. Setiap data *signature* yang disimpan dalam database memiliki jumlah karakter sebanyak 64 digit.

Setelah data *backdoor signature* diambil maka akan dilakukan pencocokan *string backdoor signature* terhadap *source code* yang telah di transformasikan sebelumnya. Contoh :

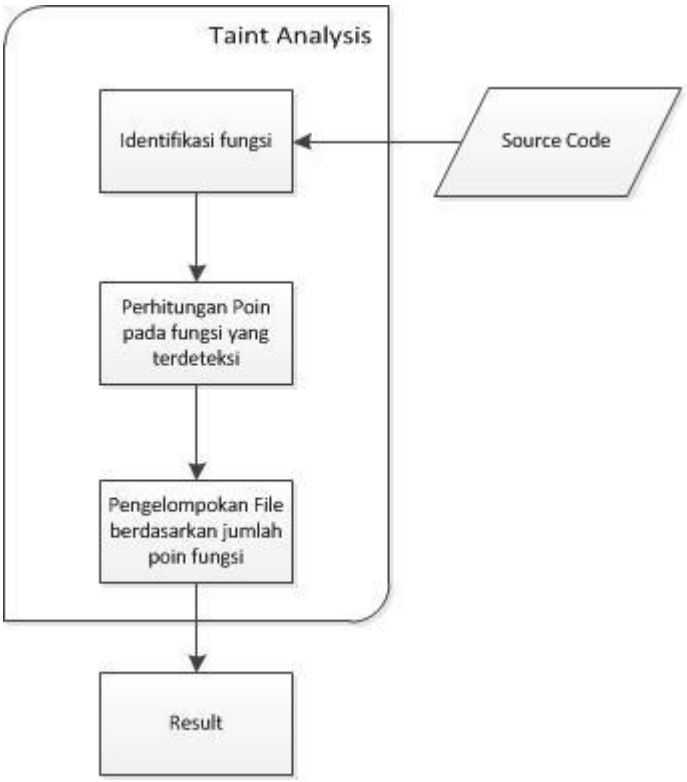


Gambar 3. 10 Ditemukan hasil string matching

Dari hasil pencarian ditemukan kesamaan identik pada *string* terhadap *backdoor signature* pada file worse.php line 38 bagian yang diberi warna hijau. dengan demikian file worse.php positif sebagai *backdoor* dan akan diberikan *flag* merah pada hasil pencarian. Proses *string matching* dapat diterapkan pada jenis backdoor *encrypted* dan *non-encrypted*. Apabila file yang di analisis tidak menunjukan adanya indikasi sebagai *backdoor shell* maka file akan dilanjutkan ke tahap *Taint Analysis*.

3.3.1.2 Taint Analysis

Taint analisis merupakan tahapan analisis source code berdasarkan fungsi-fungsi yang dimiliki oleh source code tersebut, untuk alur proses taint analysis dapat dilihat pada gambar 3.11 berikut :



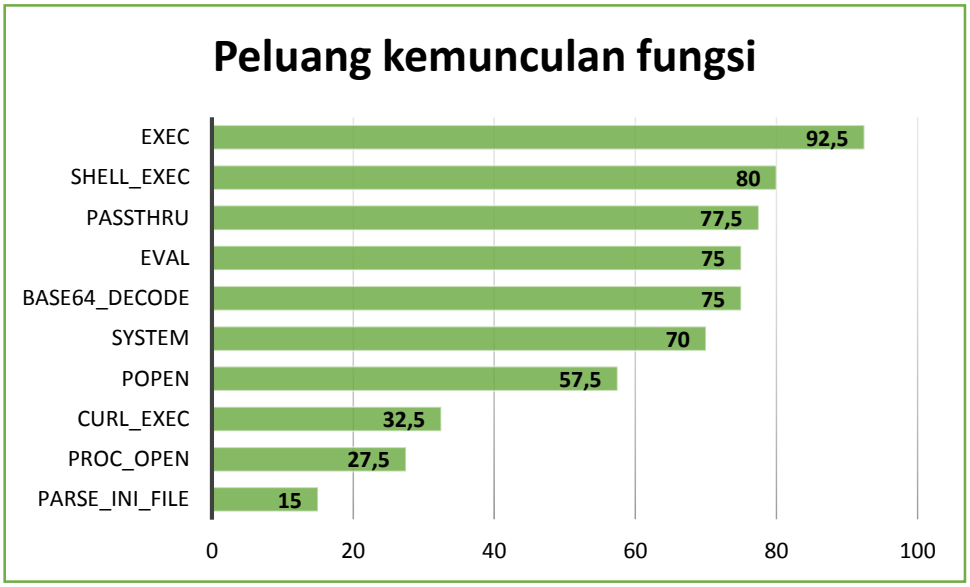
Gambar 3. 11 Proses taint analysis

Sebelum menjelaskan taint analysis untuk setiap tahapannya ada beberapa hal yang akan dijelaskan terlebih dahulu berdasarkan analisis terhadap beberapa sampel *backdoor shell* yang dimana hasil analisis tersebut diterapkan dalam perhitungan dalam proses taint analisis.

Berdasarkan analisis terhadap 40 file *backdoor shell* dimana dilakukan perhitungan probabilitas kemunculan terhadap fungsi-fungsi seperti : exec, system, shell_exec, passthru, eval, base64_decode, proc_open, popen, curl_exec dan parse_ini_file. Dimana hasil dari perhitungan tersebut menentukan fungsi-fungsi yang identik sebagai backdoor shell dan juga sebagai parameter untuk melakukan penyaringan terhadap file-file yang bukan backdoor shell berdasarkan kombinasi

pada fungsi-fungsi tersebut. Berikut hasil perhitungan fungsi yang dapat dilihat pada Terlampir pada lampiran A.

Dari perhitungan peluang kemunculan fungsi-fungsi diatas diperoleh hasil dalam bentuk persentase sebagai berikut :



Gambar 3. 12 Peluang kemunculan fungsi backdoor shell

Dari hasil perhitungan diambil fungsi yang memiliki kemungkinan muncul lebih atau sama dengan 75% yaitu sebanyak 5 fungsi sebagai fungsi yang identik sebagai *backdoor shell*. Sehingga diasumsikan dalam poin yang dijelaskan dalam Table 3.4

Tabel 3. 4 Jumlah poin pada fungsi backdoor shell

No	Fungsi	Poin
1	eval	2
2	base64_decode	2
3	shell_exec	2
4	exec	2
5	passthru	2
6	proc_open	1
7	popen	1
8	system	1

No	Fungsi	Poin
9	curl_exec	1
10	Parse_ini_file	1

Nilai pada poin akan diakumulasikan berdasarkan kombinasi fungsi yang dimiliki oleh file yang sedang dianalisis. Hasil akumulasi poin terhadap 40 sampel backdoor yang telah dianalisis dapat dilihat pada Terlampir pada lampiran A. Dari hasil akumulasi poin diperoleh data kombinasi poin terendah yaitu sebesar 4 poin , untuk nilai kombinasi rata-rata poin 10.25 dan untuk kombinasi poin tertinggi yaitu 14 poin. Berdasarkan hasil analisis tersebut dapat dijadikan batasan dalam menentukan kombinasi poin pada file yang positif sebagai backdoor shell dan yang tidak maka diasumsikan pada tabel 3.5 berikut :

Tabel 3. 5 Pembagian jenis file

Total Poin	Flag	Ket
< 4	Putih	Bersih
4 – 10	Kuning	Hati-Hati
> 10	Merah	Berbahaya

Keterangan dari 3 jenis file pada tabel 3.5 :

- File dengan flag putih

  Merupakan file yang bebas atau tidak terdeteksi sebagai *backdoor shell*.
- File dengan flag kuning

  Merupakan jenis file yang masih memiliki kemungkinan sebagai *backdoor shell* atau tidak.
- File dengan flag merah

  Merupakan jenis file yang positif diidentifikasi sebagai *backdoor shell*.

Dalam proses taint analysis, dilakukan identifikasi terhadap 10 fungsi yang telah dipaparkan sebelumnya. Setelah system menemukan fungsi yang terdapat pada source code maka akan di lakukan akumulasi poin dengan aturan poin pada table 3.4 Jumlah poin pada fungsi *backdoor shell*. Ketika sistem telah melakukan

kalkulasi poin fungsi maka tahap selanjutnya akan dilakukan pengelompokan file yang dimana aturan pengelompokan mengikuti table 3.5 Pembagian jenis file.

Setelah dilakukan pengelompokan jenis file maka system dapat menampilkan hasil pencarian kepada user dengan menampilkan data file yang memiliki flag merah dan kuning. Berikut contoh kasus taint analysis :

File yang akan dianalisis adalah indirajith.v.2.php

Pada tahap awal sistem akan melakukan scanning fungsi pada source code file indirajith.v.2.php dimana hasil dari scanning terhadap 10 fungsi yang telah dijelaskan sebelumnya memperoleh hasil

- Fungsi eval( ) terdeteksi pada line 1093

```
case "GZINFLATE":
$res_t=base64_encode(gzdeflate(trim(stripslashes($c_ntent.'')),'<?php,
?>'),9));
$res_t="<?php /* Encoded in INDRAJITH SHELL PROJECT */
eval(gzinflate(base64_decode("$res_t")));  ?>";
break;
```

Gambar 3. 13 Kutipan fungsi eval

- Fungsi base64_decode( ) terdeteksi dibeberapa line salah satunya pada 1110

```
switch($typ_d)
{
    case "GZINFLATE":
    $res_t=gzinflate(base64_decode($c_ntent));
    break;
```

Gambar 3. 14 Kutipan fungsi base64_decode

- Fungsi System( ) terdeteksi di line 728

```
else if(function_exists('system')){
         ob_start();
         system($cmd);
         $res = ob_get_contents();
         ob_end_clean();    }
```

Gambar 3. 15 Kutipan fungsi system

- Fungis shell_exec( ) terdeteksi di line 718

```
if(function_exists('shell_exec')) {
         $res=shell_exec($cmd);}
```

Gambar 3. 16 Kutipan fungsi shell_exec

- Fungis exec( ) terdeteksi di line 722

```
else if(function_exists('exec')) {
          exec($cmd,$res);
          $res=join("n",$res); }
```

Gambar 3. 17 Kutipan fungsi exec

- Fungis passthru( ) terdeteksi di line 735

```
elseif(function_exists('passthru')){
         ob_start();
         passthru($cmd);
         $res=ob_get_contents();
         ob_end_clean();  }
```

Gambar 3. 18 Kutipan fungsi passthru

- Fungis proc_open( ) terdeteksi di line 742

```
else if(function_exists('proc_open')){
     $descriptorspec = array(0 => array("pipe", "r"),1 =>array("pipe",
     "w"),  2 => array("pipe", "w"));
     $handle = proc_open($cmd ,$descriptorspec , $pipes);
        if(is_resource($handle))
```

Gambar 3. 19 Kutipan fungsi proc_open

- Fungis popen( ) terdeteksi di line 765

```
else if(function_exists('popen')){
        $handle = popen($cmd , "r");
        if(is_resource($handle)){
            if(function_exists('fread') && function_exists('feof'))
```

Gambar 3. 20 Kutipan fungsi popen

- Fungis curl_exec( ) terdeteksi di line

```
$ch = curl_init($urlzzx);
   curl_setopt($ch, CURLOPT_NOBODY, true);
   curl_exec($ch);
   $status_code=curl_getinfo($ch, CURLINFO_HTTP_CODE);
```

Gambar 3. 21 Kutipan fungsi curl_exec

Setelah sistem melakukan scaning pada seluruh baris source code dideteksi file indirajith.V.2.php memiliki 9 fungsi backdoor yaitu eval, base64_decode,

system, shell_exec, exec, passthru, proc_open, popen, dan curl_exec. Kemudian sistem melakukan perhitungan poin yang dimiliki file tersebut berdasarkan tabel 3.4

Tabel 3. 6 Perhitungan poin taint pada file indirajith

Fungsi	Poin
Eval	2
Base64_decode	2
System	1
Shell_exec	2
Exec	2
Passthru	2
Proc_open	1
Popen	1
Curl_exec	1
Total	14

Berdasarkan akumulasi poin diatas maka file indirajith.v.2.php ditandai dengan flag merah dan dikategorikan sebagai backdoor.

3.3.2 Analisis Kebutuhan non Fungsional

Analisis kebutuhan non-fungsional merupakan analissi yang dibutuhkan untuk dapat menentukan spesifiasi dari kebutuhan aplikasi. Spesifikasi ini meliputi elemen atau perangkat-perangkat yang dibutuhkan untuk aplikasi yang akan dibangun sampai aplikasi tersebut dapat diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan aplikasi, keluaran yang akan dihasilkan aplikasi dan proses yang dibutuhkan untuk mengolah masukan sehingga dapat menghasilkan suatu keluaran yang diinginkan. Kebutuhan non-fungsional terbagi menjadi beberapa analisis yaitu analisis perangkat keras, analisis perangkat lunak dan analisis pengguna.

3.3.2.1Analisis Kebutuhan Perangkat Keras (Hardware)

Perangkat keras komputer atau *hardware* sangat mendukung dalam kinerja sistem. Semakin baik spesifikasi perangkat keras yang ada maka kinerja sistem akan semakin baik. Berikut spesifikasi perangkat keras yang dapat digunakan untuk membangun aplikasi pendeteksi *backdoor shell* :

1. Processor Quad Core @2,0Ghz
2. Monitor dengan resolusi 1280x1024
3. VGA Nvidia Gforce 500series
4. Ram DDR3 4GB
5. Hardisk 500GB
6. Keyboard dan Mouse Standar
7. Jaringan untuk akses internet

Spesifikasi perangkat keras yang disarankan untuk menjalankan perangkat lunak di platform website sebagai berikut:

1. Processor Intel Dual Core 2.3Ghz
2. Ram 1GB
3. Hardisk dengan free space 1GB
4. Monitor dengan resolusi 1280x1024
5. Keyboard dan mouse standar
6. Jaringan untuk akses internet

3.3.2.2Analisis Kebutuhan Perangkat Lunak (Software)

Komponen perangkat lunak yang digunakan untuk membuat aplikasi dan simulasi program adalah sebagai berikut :

1. Sistem operasi Microsoft Windows 7 Profesional Service pack 1 64-bit.
2. Browser Mozila dan Google.
3. Microsoft Visio 2010
4. Balsamiq Mockup v4
5. Sublime Text Editor 3
6. Xampp v5.6.14

3.3.2.3Analisis Pengguna

Suatu aplikasi akan berjalan dengan optimal apabila ditunjang oleh perangkat pikir yang memiliki kemampuan dalam menjalankan aplikasi yang bersangkutan. Perangkat lunak ini akan digunakan oleh 2 jenis pengguna yaitu administrator dan pengguna umum. Karakteristik pengguna yang dibutuhkan adalah sebagai berikut :

Tabel 3. 7 Karakteristik pengguna

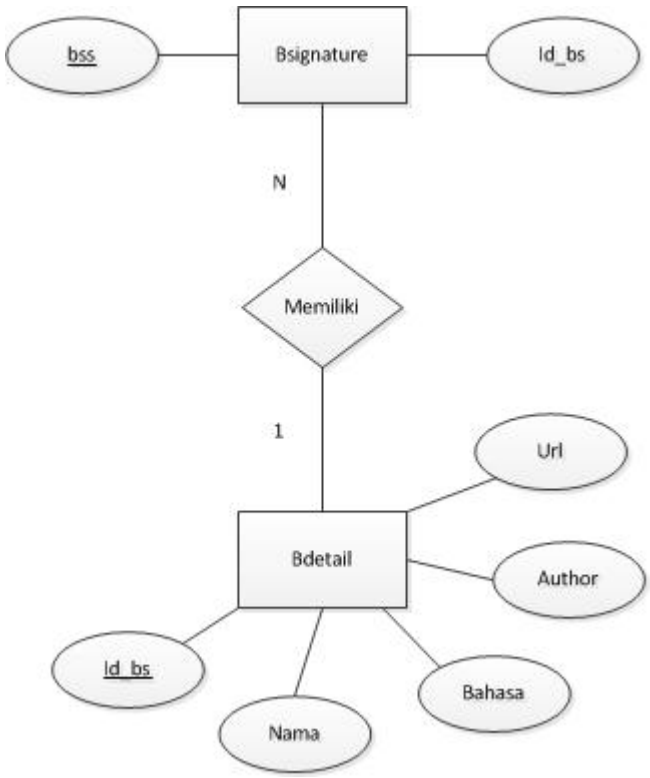
Pengguna	Karakteristik yang dibutuhkan
Administrator	1. Mengerti dan mampu dalam mengelola website. 2. Mengerti bahasa pemograman website minimal php. 3. Mampu menganalisis jenis backdoor shell baru.
Pengguna umum	1. Mengerti dan mampu mengelola website. Terutama mengelola fitur Cpanel. 2. Mengerti cara mengoperasikan aplikasi detector backdoor shell.

3.3.3Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional adalah analisis terhadap kebutuhan secara fungsional baik dalam aliran data maupun informasi. Analisis fungsional digambarkan dalam analisis terstruktur yang akan dibahas sebagai berikut.

3.3.3.1 Analisis Basis Data

Berikut dibawah ini merupakan entity relationship diagram pembangunan aplikasi pendeteksian backdoor shell pada web server.



Gambar 3. 22 ERD aplikasi pendeteksi backdoor shell

3.3.3.2 Kamus Data Entity Relationship Diagram (ERD)

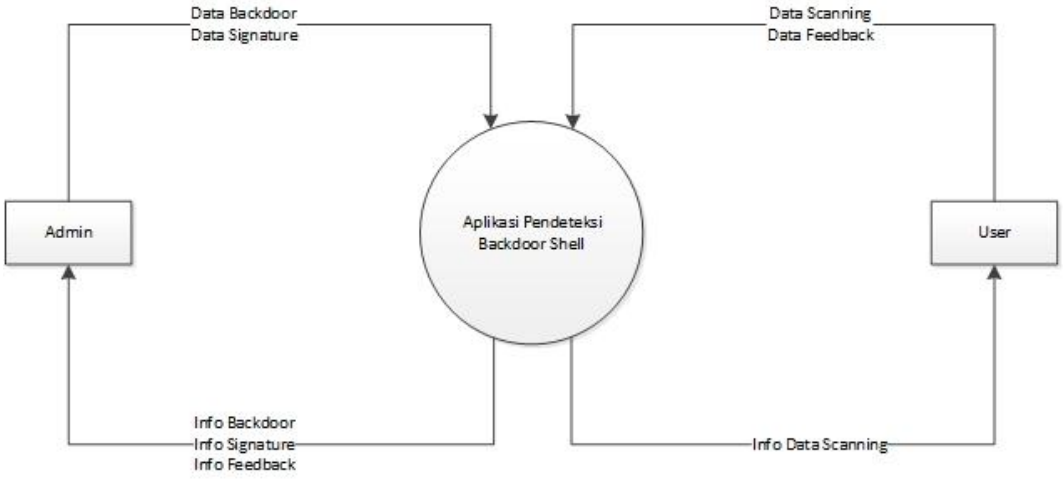
Kamus data dari entity relationship diagram aplikasi pendeteksi backdoor shell dapat dilihat pada table 3.8

Tabel 3. 8 Kamus data entity relationship diagram (ERD)

No	Entitas	Atribut
1	Bdetail	{Id_bs, Nama, Bahasa, Author, Url}
2	Bsignature	{bss, Id_bs}

3.3.3.3Diagram Konteks

Diagram konteks berfungsi untuk menggambarkan hubungan antara entitas luar, pemasukan dan keluaran system yang direpresentasikan dengan lingkaran tunggal yang dapat mewakili keseluruhan sistem. Diagram konteks dari sistem yang akan dibangun dapat dilihat pada Gambar berikut :

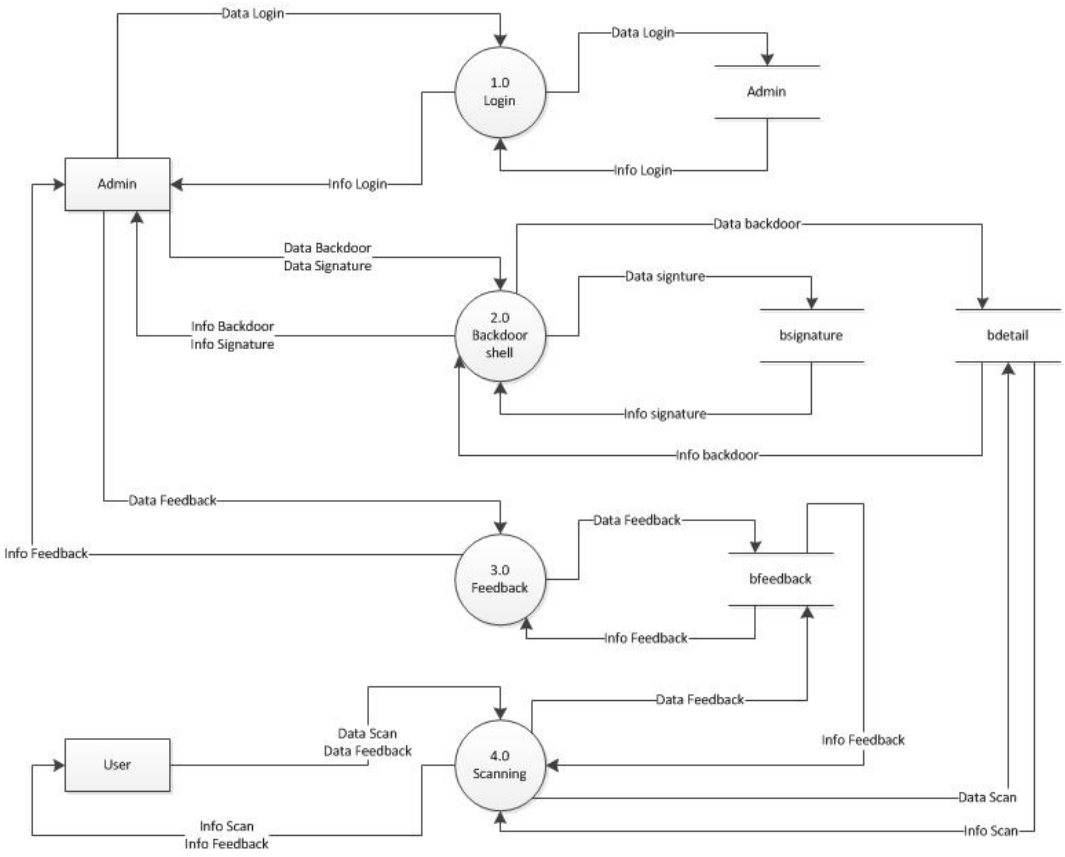


Gambar 3. 23 Diagram konteks

3.3.3.4Data Flow Diagram (DFD)

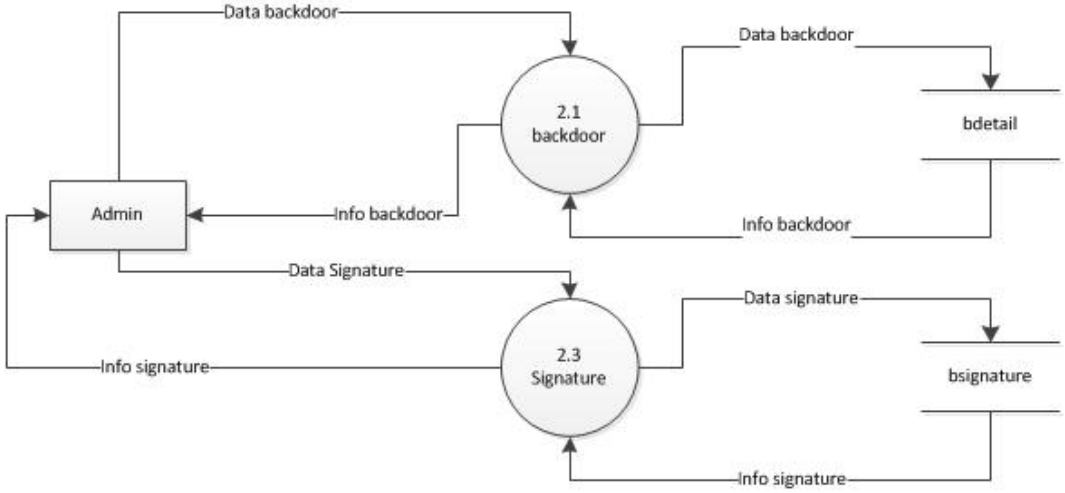
Data flow diagram menunjukkan bagaimana aliran data menguraikan proses-proses yang terjadi dalam sistem sampai proses lebih detail. Pada diagram konteks seperti Gambar 3.23 dapat diuraikan menjadi beberapa DFD.

DFD Level 1 aplikasi pendeteksi backdoor shell pada Gambar 3.24 Menjelaskan secara umum proses apa saja yang dapat dilakukan pada sistem.



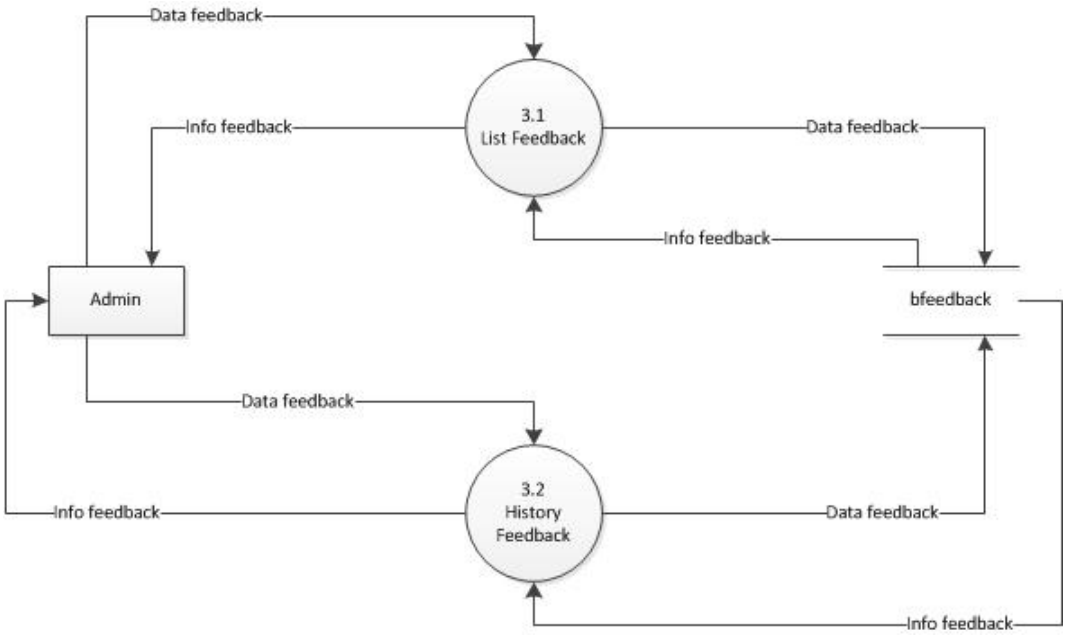
Gambar 3. 24 DFD level 1

DFD Level 2 proses 2 backdoor pada gambar 3.25 menjelaskan tentang proses pengelolaan data backdoor shell oleh admin.



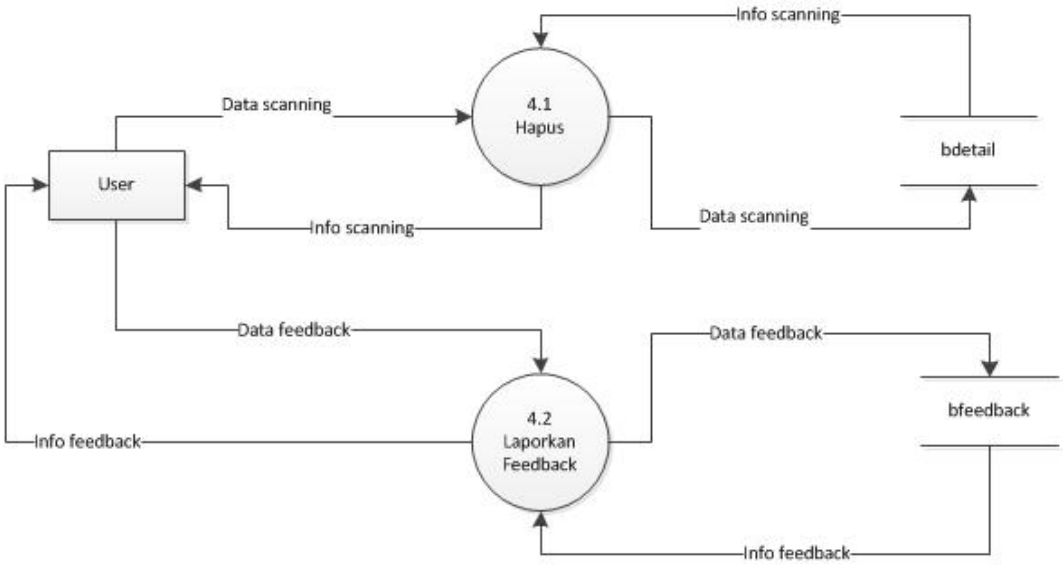
Gambar 3. 25 DFD level 2 proses backdoor shell

DFD Level 2 proses 3 feedback pada gambar 3.26 menjelaskan tentang proses pengelolaan data feedback dari user oleh admin.



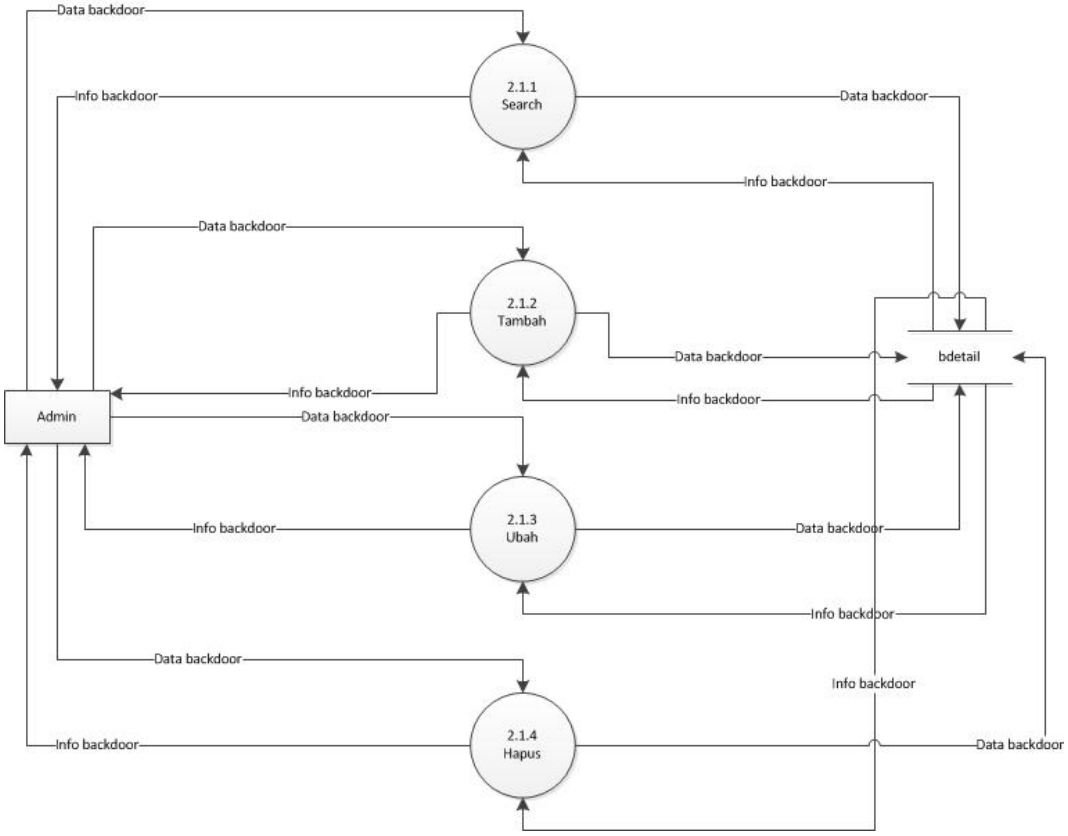
Gambar 3. 26 DFD level 2 proses feedback

DFD Level 2 proses 4 scanning pada gambar 3.27 menjelaskan proses yang dilakukan oleh user dalam melakukan pencarian backdoor shell pada webserver.



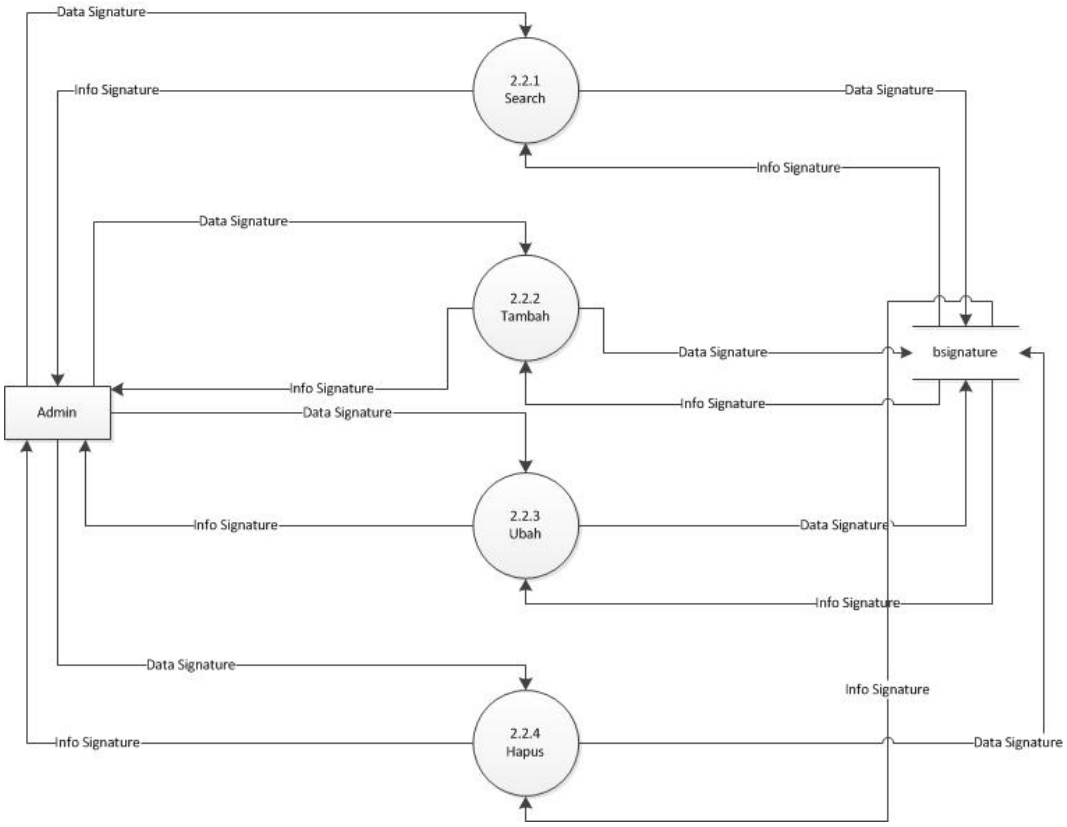
Gambar 3. 27 DFD level 2 proses scanning

DFD Level 3 Proses 2.1 pada gambar 3.28 backdoor menjelaskan proses pengelolaan data detail backdoor oleh admin pada sistem.



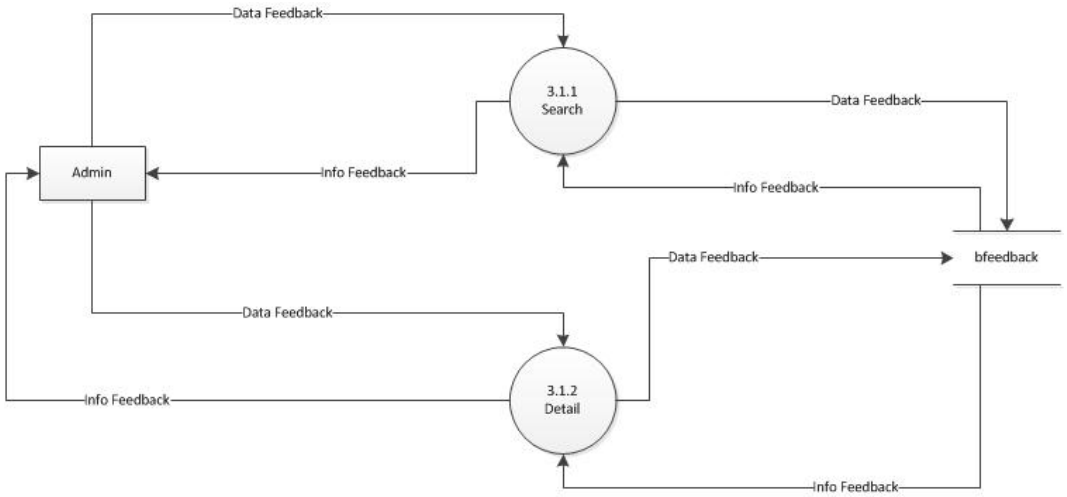
Gambar 3. 28 DFD level 3 proses backdoor

DFD Level 3 Proses 2.2 Signature pada gambar 3.29 menjelaskan proses pengelolaan data Signature oleh admin pada sistem.



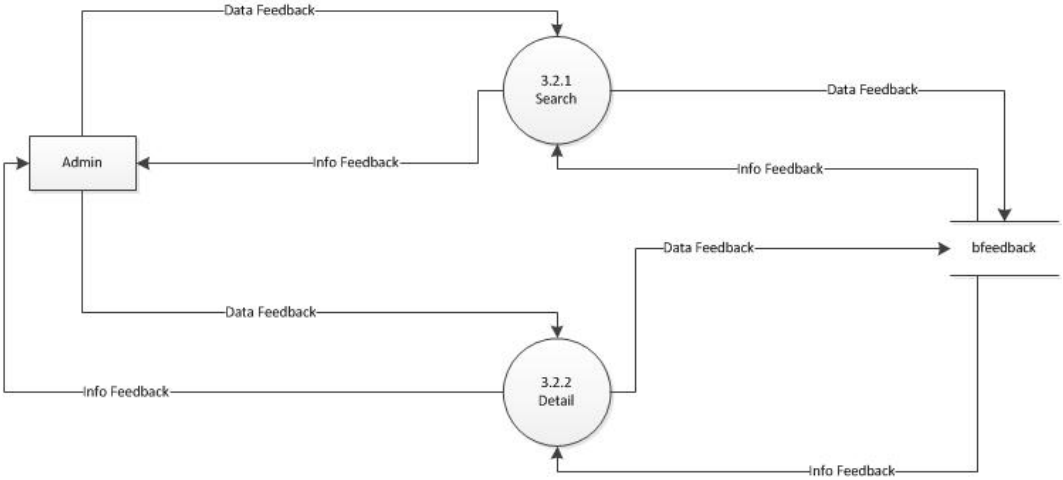
Gambar 3. 29 DFD level 3 proses signature

DFD Level 3 Proses 3.1 List Feedback pada gambar 3.30 menjelaskan proses pengelolaan data list feedback oleh admin pada sistem.



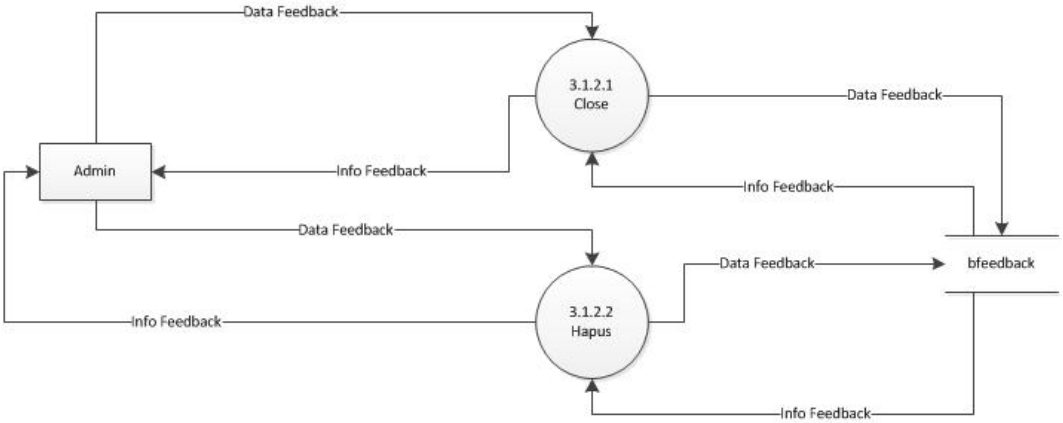
Gambar 3. 30 DFD level 3 proses list feedback

DFD Level 3 Proses 3.1 History Feedback pada gambar 3.31 menjelaskan proses pengelolaan data history feedback oleh admin pada sistem.



Gambar 3. 31 DFD level 3 proses history feedback

DFD Level 4 Proses 3.1.2 Detail Feedback pada gambar 3.32 menjelaskan proses pengelolaan data detail feedback oleh admin pada sistem.



Gambar 3. 32 DFD level 4 proses detail history

3.3.3.5Spesifikasi Proses

Spesifikasi proses merupakan deskripsi dari setiap elemen proses yang terdapat dalam program, yang meliputi nama proses, *input, output* dan keterangan dari proses. Berikut spesifikasi proses dari Aplikasi Pendeteksi backdoor shell dapat dilihat pada Table 3.9

Tabel 3. 9 Spesifikasi proses

No	Proses	Keterangan
1	No.Proses	1.0
	Nama	Login
	Sumber	Admin
	Deskripsi	Untuk menangani proses ketika admin akan memasuki system
	Data Masukan	Data Login
	Data Keluaran	Info Login
	Logika Proses	-Sistem menampilkan halaman login admin -Admin memasukan username dan password -Sistem memeriksa data login pada halaman login yaitu username dan password pada database. Apabila username dan password ditemukan pada database. Maka system akan menampilkan halaman utama admin dan dapat mengolah data yang ada pada system -Jika admin salah memasukan data login maka akan kembali kehalaman login dan system akan meminta admin untuk login kembali
2	No.Proses	2.0
	Nama	Backdoor Shell
	Sumber	Admin
	Deskripsi	Untuk menangani proses yang berhubungan dengan data backdoor shell

No	Proses	Keterangan
	Data Masukan	Data backdoor shell
	Data Keluaran	Info backdoor shell
	Logika Proses	-Sistem menampilkan halaman backdoor shell -Admin dapat memilih menu backdoordan signature.
3	No.Proses	3.0
	Nama	Feedback
	Sumber	Admin dan User
	Deskripsi	Untuk menangani proses yang berhubungan dengan data feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-Sistem menampilkan halaman feedback -Admin bisa mencari, lihat detail dan menghapus data feedback
4	No.Proses	4.0
	Nama	Scanning
	Sumber	User
	Deskripsi	Proses untuk melakukan pencarian backdoor shell pada web server pengguna
	Data Masukan	Data scanning
	Data Keluaran	Info scanning
	Logika Proses	-Sistem menampilkan halaman pencarian. Dan menampilkan beberapa informasi tambahan yang berhubungan dengan pencarian pada web server
5	No.Proses	2.1
	Nama	Backdoor
	Sumber	Admin
	Deskripsi	Untuk mengelola data detail backdoor
	Data Masukan	Data backdoor

No	Proses	Keterangan
	Data Keluaran	Info backdoor
	Logika Proses	-sistem menampilkan halaman backdoor. -admiin dapat memilih untuk mengelola bagian backdoor seperti menambah, mengubah, mencari dan menghapus data.
6	No.Proses	2.2
	Nama	Signature
	Sumber	Admin
	Deskripsi	Untuk mengelola data signature.
	Data Masukan	Data signature
	Data Keluaran	Info signature
	Logika Proses	-sistem menampilkan halaman signature. -admin dapat memilih untuk mengelola bagian signature seperti menambah, mengubah, mencari dan menghapus data.
7	No.Proses	3.1
	Nama	List feedback
	Sumber	Admin
	Deskripsi	Untuk mengelola data list feedback open.
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan halaman list feedback. -admin dapat memilih untuk mengelola bagian list feedback seperti search data feedback dan melihat detail feedback
8	No.Proses	3.2
	Nama	History feedback
	Sumber	Admin
	Deskripsi	Untuk mengelola data history feedback

No	Proses	Keterangan
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan halaman history feedback -admin dapat memilih menu detail feedback
9	No.Proses	4.1
	Nama	Hapus
	Sumber	User
	Deskripsi	Proses untuk menghapus file backdoorshell pada system.
	Data Masukan	Data scanning
	Data Keluaran	Info scanning
	Logika Proses	-user menghapus file backdoor yang ditemukan. -sistem menghapus file backdoor pada webserver. -sistem menampilkan pesan bahwa file backdoor berhasil dihapus.
10	No.Proses	4.2
	Nama	Laporkan feedback
	Sumber	User
	Deskripsi	Proses melaporkan file yang terindikasi sebagai backdoor namun berstatus flag merah untuk dianalisis oleh admin.
	Data Masukan	Data Scanning
	Data Keluaran	Info Scanning
	Logika Proses	-user memilih file backdoor shell yang dicurigai. -sistem mengirim data file ke server. -sistem menampilkan pesan pengiriman feedback berhasil.
11	No.Proses	2.1.1
	Nama	Search

No	Proses	Keterangan
	Sumber	Admin
	Deskripsi	Untuk proses pencarian data backdoor.
	Data Masukan	keyword
	Data Keluaran	Info backdoor
	Logika Proses	-sistem menampilkan data backdoor berupa list. -admin memasukan keyword backdoor yang akan dicari. -sistem manampilkan data backdoor yang dicari.
12	No.Proses	2.1.2
	Nama	Tambah
	Sumber	Admin
	Deskripsi	Untuk proses menambah data backdoor kedalam sistem.
	Data Masukan	Data backdoor
	Data Keluaran	Info backdoor
	Logika Proses	-sistem menampilkan halaman tambah data backdoor. -admin memasukan data backdoor. -sistem menyimpan data backdoor.
13	No.Proses	2.1.3
	Nama	Ubah
	Sumber	Admin
	Deskripsi	Untuk proses perubahan data backdoor pada system.
	Data Masukan	Data backdoor
	Data Keluaran	Info backdoor
	Logika Proses	-sistem menampilkan halaman ubah backdoor. -admin melakukan perubahan data backdoor. -sistem menyimpan perubahan data.
14	No.Proses	2.1.4
	Nama	Hapus

No	Proses	Keterangan
	Sumber	Admin
	Deskripsi	Proses untuk menghapus data backdoor
	Data Masukan	Data backdoor
	Data Keluaran	Info backdoor
	Logika Proses	-admin memilih data yang akan di hapus. -sistem mengapus data. -sistem menampilkan pesan data telah berhasil dihapus.
15	No.Proses	2.2.1
	Nama	Search
	Sumber	Admin
	Deskripsi	Untuk proses pencarian data signature.
	Data Masukan	Data signature
	Data Keluaran	Info signature
	Logika Proses	-sistem menampilkan data signature berupa list. -admin memasukan keyword signature yang akan dicari. -sistem manampilkan data signature yang dicari.
16	No.Proses	2.2.2
	Nama	Tambah
	Sumber	Admin
	Deskripsi	Proses untuk menambah data signature kedalam system.
	Data Masukan	Data signature
	Data Keluaran	Info signature
	Logika Proses	-sistem menampilkan halaman tambah data signature. -admin memasukan data signature. -sistem menyimpan data signature.
17	No.Proses	2.2.3

No	Proses	Keterangan
	Nama	Ubah
	Sumber	Admin
	Deskripsi	Proses untuk melakukan perubahan data signature pada sistem.
	Data Masukan	Data signature
	Data Keluaran	Info signature
	Logika Proses	-sistem menampilkan halaman ubah signature. -admin melakukan perubahan data. -sistem menyimpan perubahan data.
18	No.Proses	2.2.4
	Nama	Hapus
	Sumber	Admin
	Deskripsi	Proses untuk menghapus data signature pada sistem
	Data Masukan	Data signature
	Data Keluaran	Info signature
	Logika Proses	-admin memilih data yang akan di hapus -sistem mengapus data -sistem menampilkan pesan data telah berhasil dihapus
19	No.Proses	3.1.1
	Nama	Search
	Sumber	Admin
	Deskripsi	Proses untuk mencari data feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan data feedback berupa list -admin mengetik keyword data yang akan dicari -sistem menampilkan data yang dicari
20	No.Proses	3.1.2

No	Proses	Keterangan
	Nama	Detail
	Sumber	Admin
	Deskripsi	Proses untuk melihat detail pada list feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan list feedback. -admin memilih satu data untuk melihat detail feedback. -sistem menampilkan data detail feedback
21	No.Proses	3.2.1
	Nama	Search
	Sumber	Admin
	Deskripsi	Proses untuk mencari data history feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan list history feedback -admin mengetik keyword data history feedback yang akan dicari. -sistem menampilkan data history feedback yang dicari
22	No.Proses	3.2.2
	Nama	Detail
	Sumber	Admin
	Deskripsi	Proses untuk melihat detail history feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan list history feedback -admin memilih satu data pada list detail feedback untuk dilihat detail nya.

No	Proses	Keterangan
		-sistem menampilkan data detail history feedback.
23	No.Proses	3.1.2.1
	Nama	Close
	Sumber	Admin
	Deskripsi	Proses untuk mengclose tiket feedback
	Data Masukan	Data feedback
	Data Keluaran	List feedback
	Logika Proses	-sistem menampilkan detail list tiket. -admin memilih untuk close tiket. -sistem merubah status tiket menjadi close.
24	No.Proses	3.1.2.2
	Nama	Hapus
	Sumber	Admin
	Deskripsi	Proses untuk menghapus tiket feedback
	Data Masukan	Data feedback
	Data Keluaran	Info feedback
	Logika Proses	-sistem menampilkan detail list tiket. -admin memilih untuk menghapus tiket. -sistem menghapus tiket dari database

3.3.3.6Kamus Data

Kamus data dapat membantu mendefinisikan dengan lengkap data yang mengalir diantara proses, penyimpanan data dan entitas luar. Data yang mengalir tersebut dapat berupa masukan untuk system atau hasil dari proses sistem. Kamus data dibuat berdasarkan arus data yang mengalir pada konteks diagram dan DFD. Kamus data yang terdapat di aplikasi pembelajaran kimia berbasis web ini dapat dilihat pada Table 3.10

Tabel 3. 10 Kamus data

No	Kamus	Keterangan
1	Nama	Admin
	Digunakan Pada	Proses 1.0 Login
	Deskripsi	Data yang digunakan pada saat login kedalam sistem
	Struktur Data	username, password, email
	username password email	Varchar(15)[A..Z][a..z][0..9] Varchar(50)[A..Z][a..z][0..9] Varchar(50)[A..Z][a..z][0..9][-, /, ., ,, *, @, _,]
2	Nama	bsignature
	Digunakan Pada	Proses 2.0 Backdoor shell Proses 2.3 Signature Proses 2.3.1 Search Proses 2.3.2 Tambah Proses 2.3.3 Ubah Proses 2.3.4 Hapus
	Deskripsi	Data yang digunakan dalam pengolahan bagian backdoor shell
	Struktur Data	id_bs, bss
	id_bs bss	Int(3) [0..9] Char(64) [A..Z][a..z][0..9][-, /, ,, *,]
3	Nama	bdetail
	Digunakan Pada	Proses 2.0 Backdoor shell Proses 2.1 Backdoor Proses 2.1.1 Search Proses 2.1.2 Tambah Proses 2.1.3 Ubah Proses 2.1.4 Hapus Proses 4.2 Hapus

No	Kamus	Keterangan
	Deskripsi	Data yang digunakan untuk mengelola bagian backdoor
	Struktur Data	id_bs, nama, bahasa, url, author
	id_bs nama bahasa url author	Int(3) Varchar(15) [A..Z][a..z][0..9][-, /, ., ,, *, @, _,] Varchar(10) [A..Z][a..z][0..9] Varchar(50) [A..Z][a..z][0..9][-, /, ., ,, *, @, _,] Varchar(15) [A..Z][a..z][0..9][-, /, ., ,, *, @, _,]
4	Nama	bfeedback
	Digunakan Pada	Proses 3.0 Feedback Proses 3.1 Search Proses 3.2 Lihat Detail Proses 3.3 Hapus Proses 4.0 Scanning Proses 4.3 Laporkan Feedback
	Deskripsi	Data yang digunakan untuk mengelola bagian feedback
	Struktur Data	id_fe, fb, nfile, email, tgl_open,tgl_close,status
	id_fe fb nfile email tgl_open tgl_close status	Int(3) MediumText()[A..Z][a..z][0..9][-, /, ., ,, *, @, _,] Varchar(25) [A..Z][a..z][0..9][-, /, ., ,, *, @, _,] Varchar(50) [A..Z][a..z][0..9][-, /, ., ,, *, @, _,] Date() Data() Enum (‘1’,’2’)

3.4Perancangan Sistem

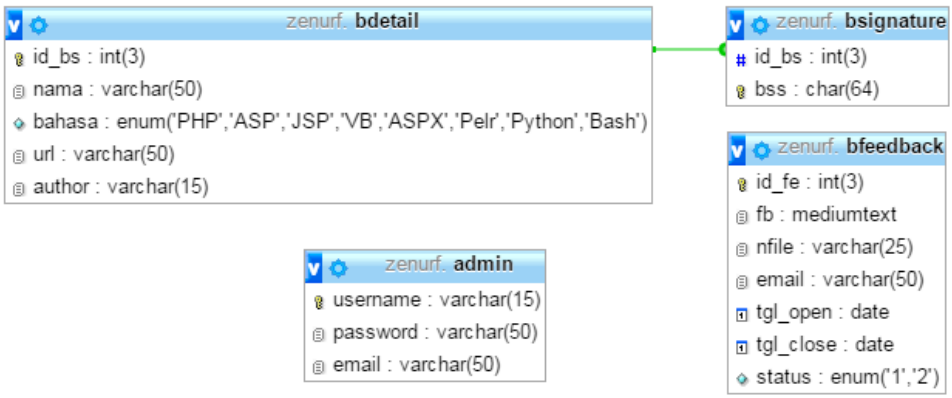
Perancangan merupakan bagian dari metodologi pembangunan suatu perangkat lunak yang harus dilakukan setelah melalui tahapan analisis.

Perancangan diidentifikasi sebagai proses aplikasi sistem yang akan di implementasikan.

Perancangan diidentifikasi sebagai proses aplikasi sitem yang akan memiliki teknik dan prinsip bagi tujuan yang akan dicapai, mampu memberikan sistem yang mudah untuk digunakan pada saat menggunakannya serta memadai dari tujuan yang diinginkan. Perancangan digambarkan berupa proses multi langkah dimana representasi struktur info, struktur program, karakteristik tampilan dan detail prosedur.

3.4.1Tabel Relasi

Tabel relasi menggambarkan hubungan antar data, arti data dan batasannya. Proses relasi antar atribut merupakan gabungan antar atribut yang mempunyai kunci utama yang sama, sehingga atribut-atribut tersebut menjadi satu kesatuan yang dihubungkan oleh field kunci tersebut.



Gambar 3. 33 Tabel Relasi

3.4.2Struktur Tabel

Didalam pembuatan program dibutuhkan suatu spesifikasi table yang dimaksudkan untuk dapat melakukan kegiatan dalam pencarian data dan pembuatan laporan serta memudahkan sistem komputer. Oleh karena itu, sistem pengolahan data ini membutuhkan spesifikasi table untuk mempermudah dalam melakukan

kegiatan pemograman komputer. Ada beberapa tabel yang terlibat dalam pembuatan sistem ini yaitu :

Tabel 3. 11 Admin

No	Nama Field	Type	Value	Status	Not Null	Ket
1	Username	Varchar	15	PK	Ya	Auto_increment
2	Password	Varchar	50		Ya	
3	Email	Varchar	50		Ya	

Tabel 3. 12 Bdetail

No	Nama Field	Type	Value	Status	Not Null	Ket
1	Id_bs	Int	3	PK	Ya	Auto_increment
2	Nama	Varchar	15		Ya	
3	Bahasa	Enum	`php`,`asp`, `jsp`,`vb`, `aspx`,`pl`, `py`,`bsh`		Tidak	
3	url	Varchar	50		Tidak	
3	Author	Varchar	15		Tidak	

Tabel 3. 13 Bsignature

No	Nama Field	Type	Value	Status	Not Null	Ket
1	Id_bs	Int	3	PK	Ya	Auto_increment
2	Bss	Char	64		Ya	

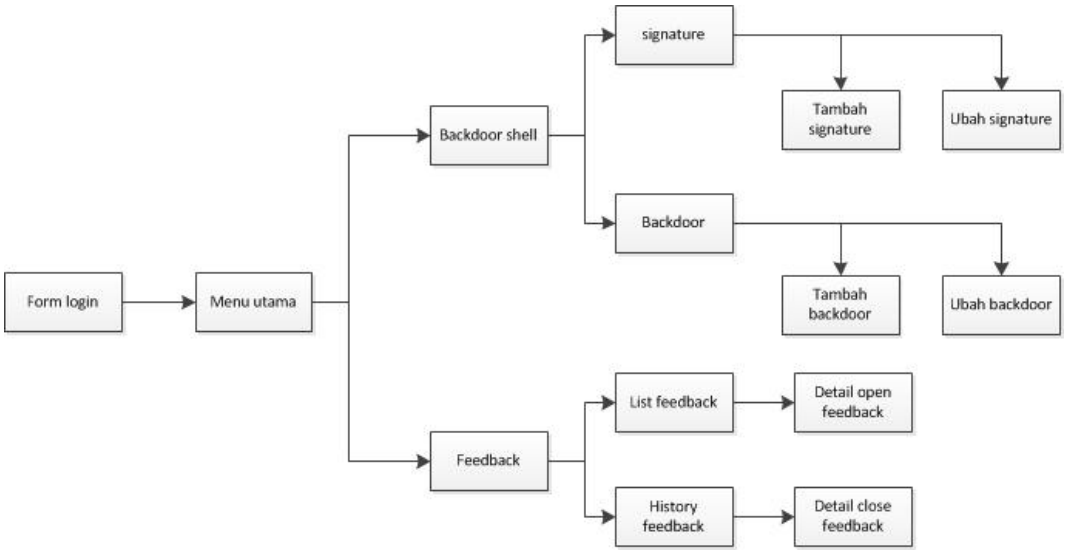
Tabel 3. 14 Bfeedback

No	Nama Field	Type	Value	Status	Not Null	Ket
1	Id_be	Int	3	PK	Ya	Auto_increment
2	fb	Medium text			Ya	

3	nfile	Varchar	25		Tidak	
4	email	Varchar	50		Tidak	
5	Tgl_open	Date			Ya	
6	Tgl_close	Date			Tidak	
7	Status	Enum	`1`,`2`		Ya	

3.4.3Perancangan Struktur Menu

Struktur menu merupakan gambaran menu-menu yang akan digunakan oleh admin dan user. Dalam perancangan struktur menu untuk aplikasi ini sebagai berikut :



Gambar 3. 34 Struktur menu admin



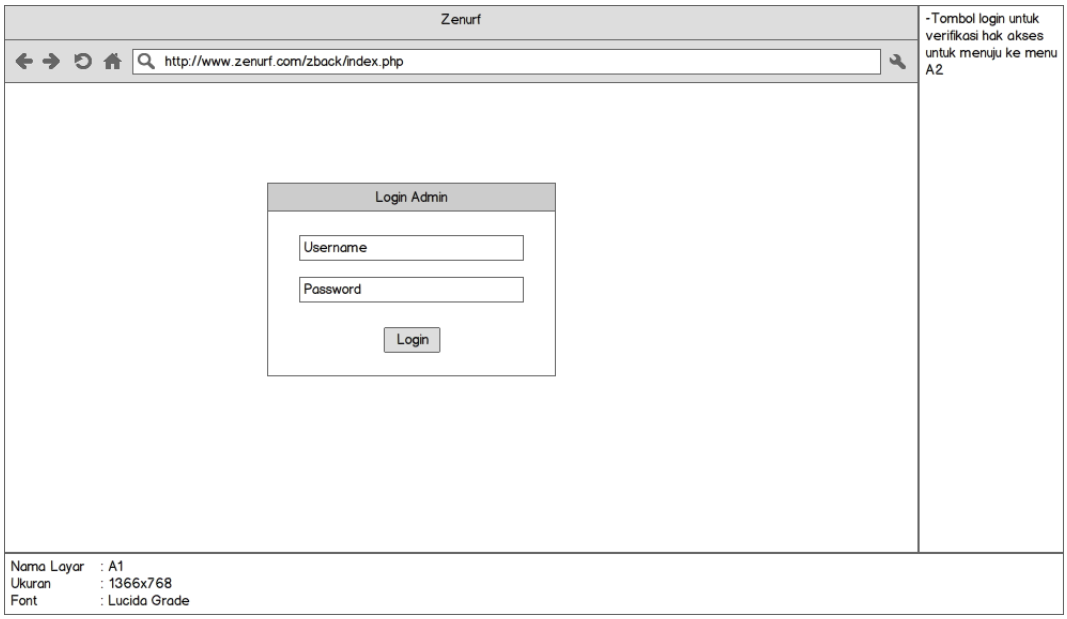
Gambar 3. 35 Struktur menu user

3.4.4Perancangan Antarmuka

Tahapan perancangan antarmuka dalam pembuatan suatu aplikasi merupakan suatu tahapan yang sangat penting, karena tahapan ini akan menentukan

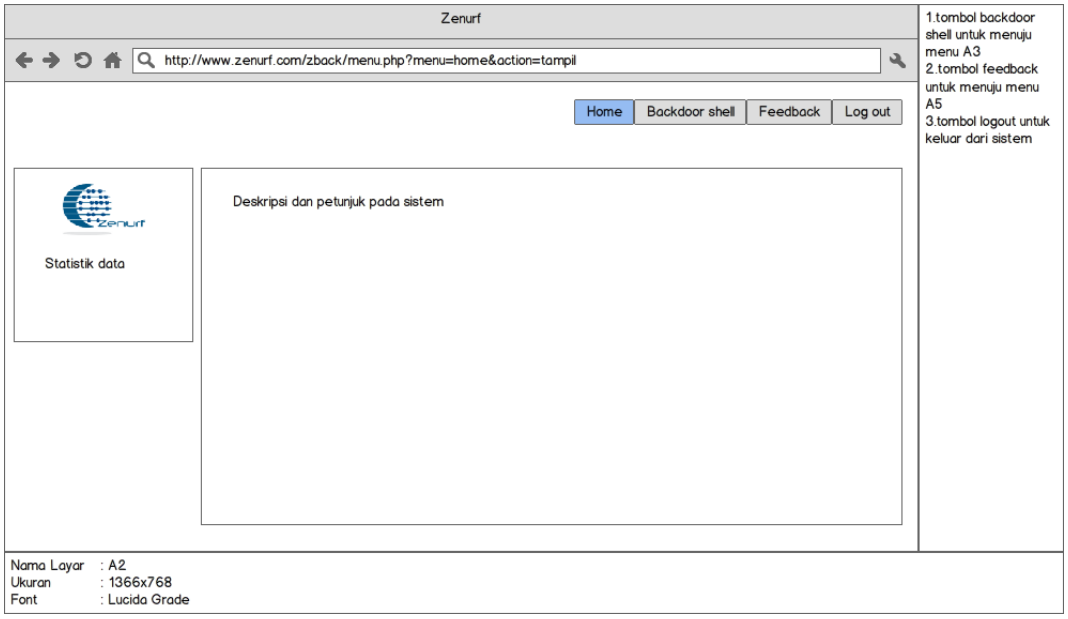
apakah suatu aplikasi akan memiliki konstruksi yang baik, proses pengolahan data yang tepat dan akurat, serta memiliki dasar-daasar untuk pengembangan dimasa yang akan datang.

Perancangan antarmuka login admin aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



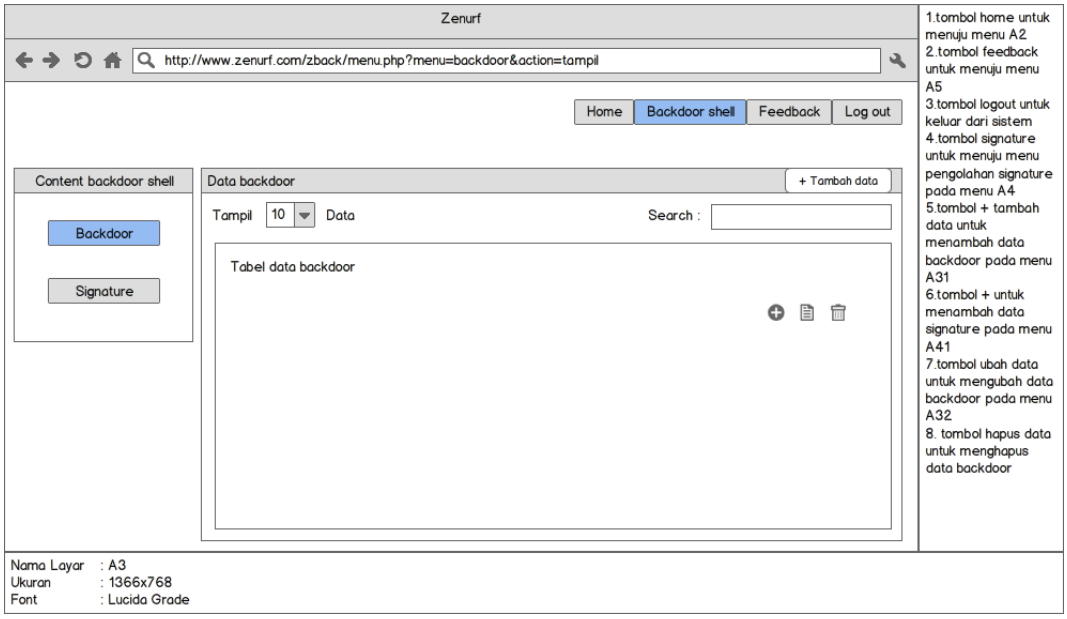
Gambar 3. 36 Perancangan antarmuka login admin

Perancangan antarmuka halaman utama aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



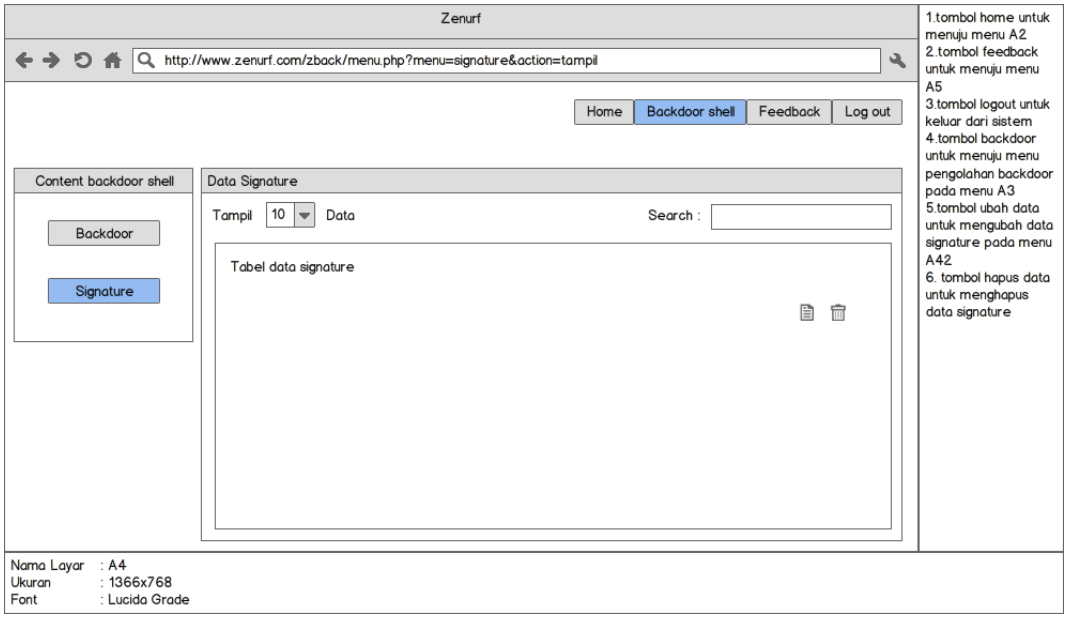
Gambar 3. 37 Perancangan antarmuka halaman utama admin

Perancangan antarmuka menu backdoor shell aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



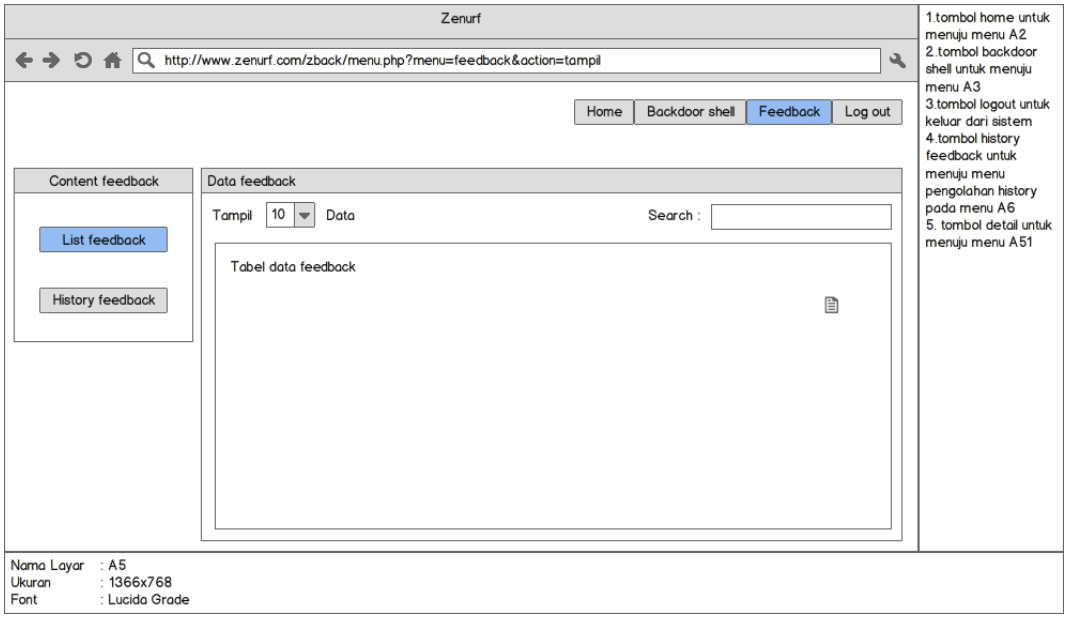
Gambar 3. 38 Perancangan antarmuka menu backdoor shell

Perancangan antarmuka menu signature aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



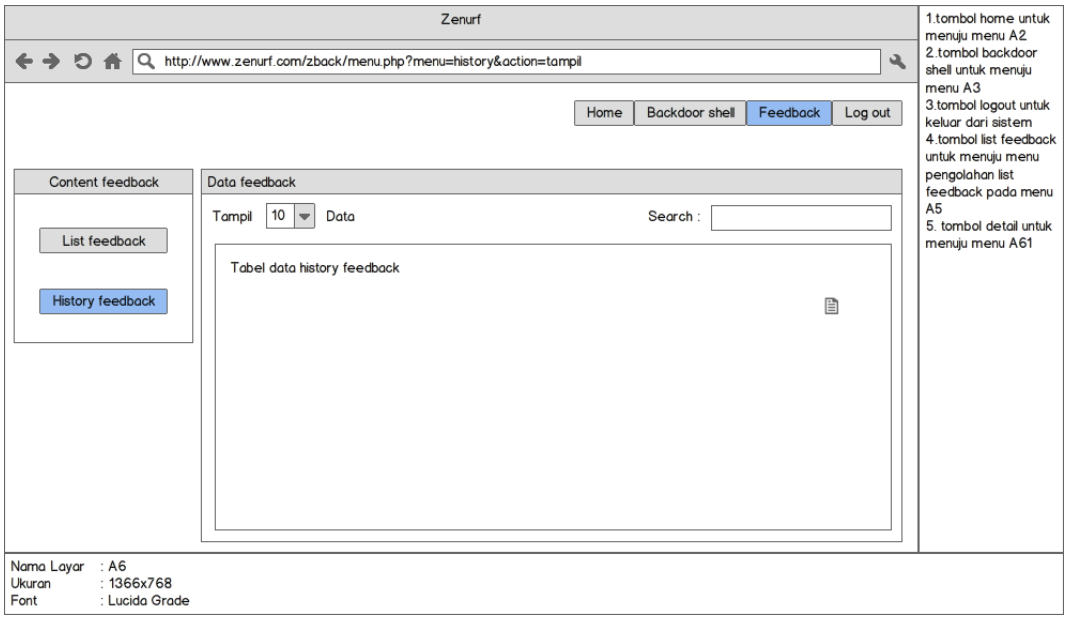
Gambar 3. 39 Perancangan antarmuka menu signature

Perancangan antarmuka menu list feedback aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



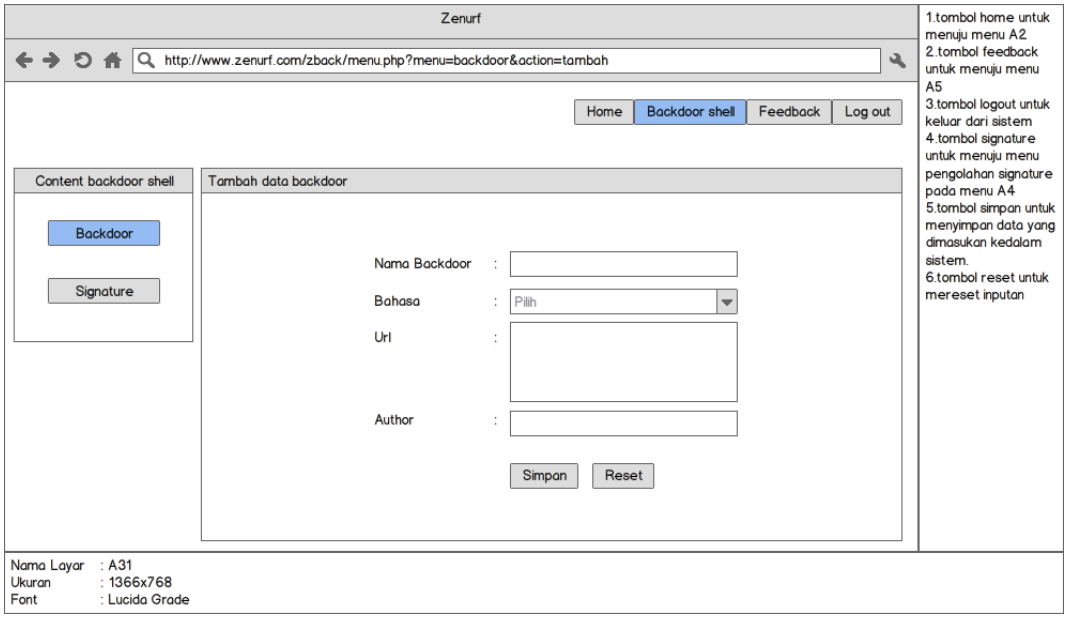
Gambar 3. 40 Perancangan antarmuka menu list feedback

Perancangan antarmuka menu history feedback aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



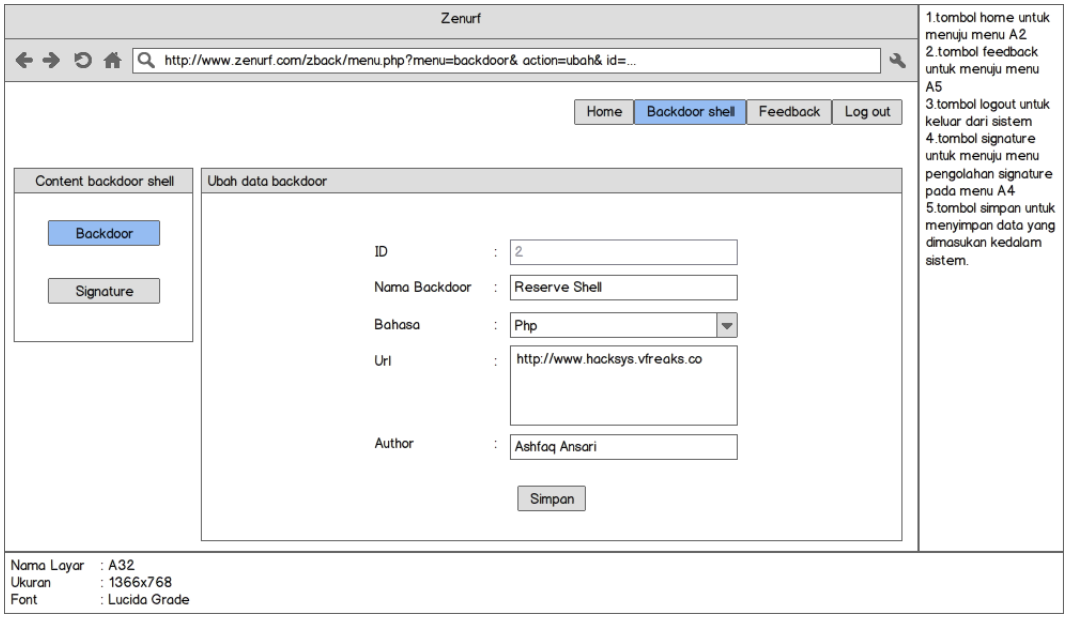
Gambar 3. 41 Perancangan antarmuka menu history feedback

Perancangan antarmuka menu tambah data backdoor shell aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



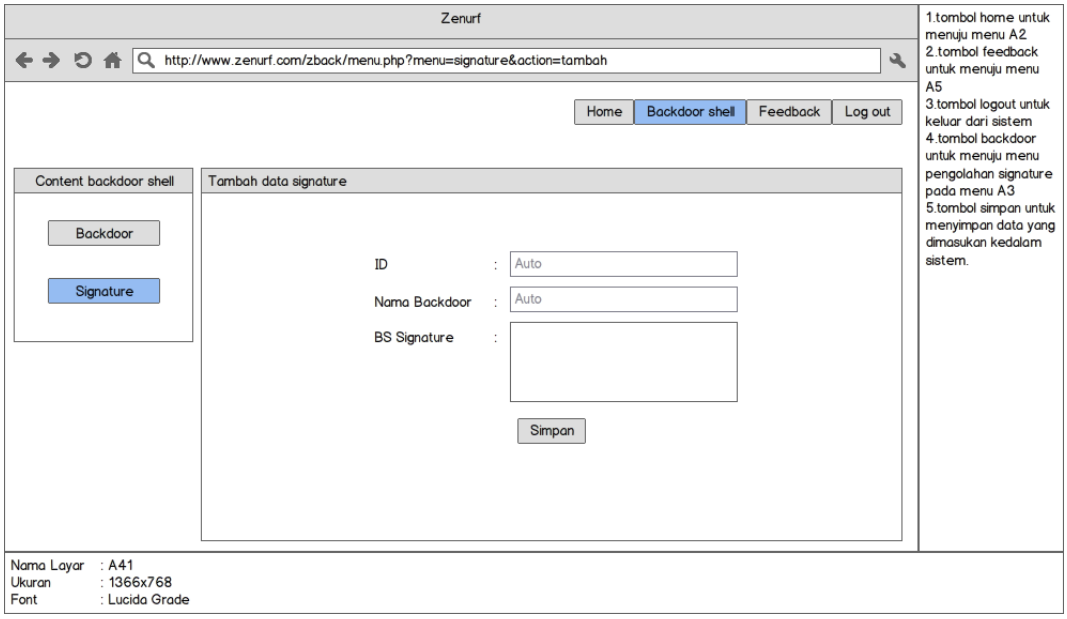
Gambar 3. 42 Perancangan antarmuka menu tambah data backdoor

Perancangan antarmuka menu ubah data backdoor shell aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



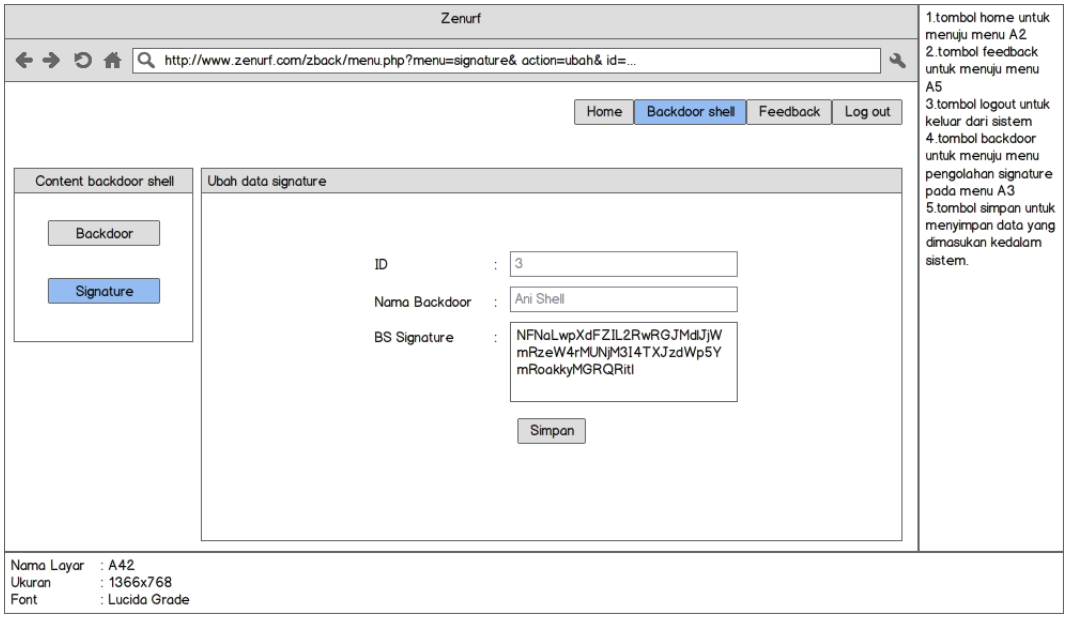
Gambar 3. 43 Perancangan antarmuka menu ubah data backdoor shell

Perancangan antarmuka menu tambah data signature aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



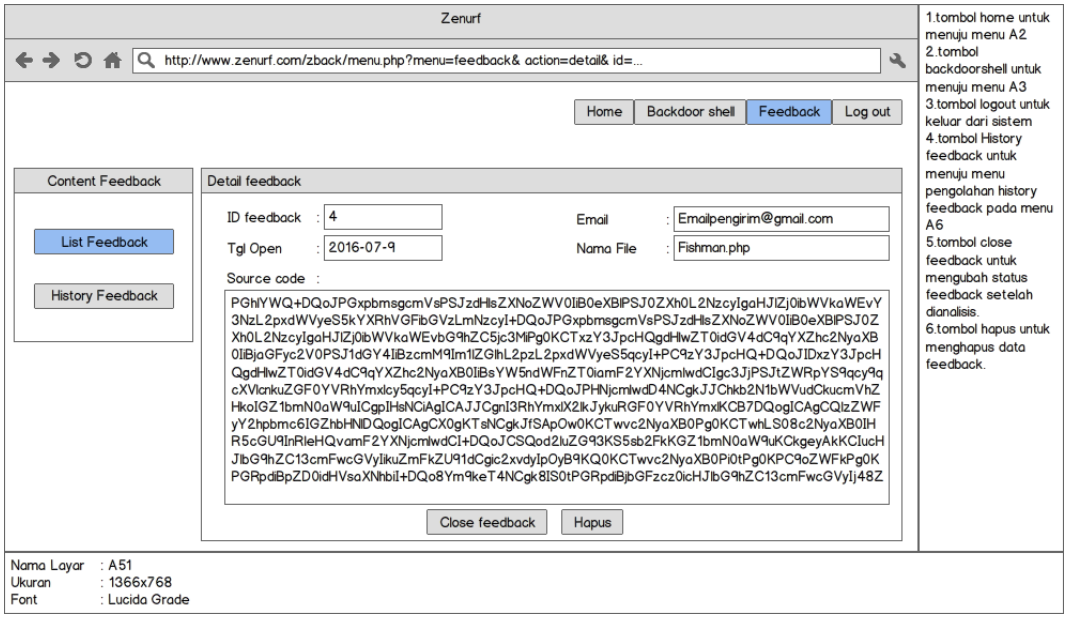
Gambar 3. 44 Perancangan antarmuka menu tambah data signature

Perancangan antarmuka menu ubah data signature aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



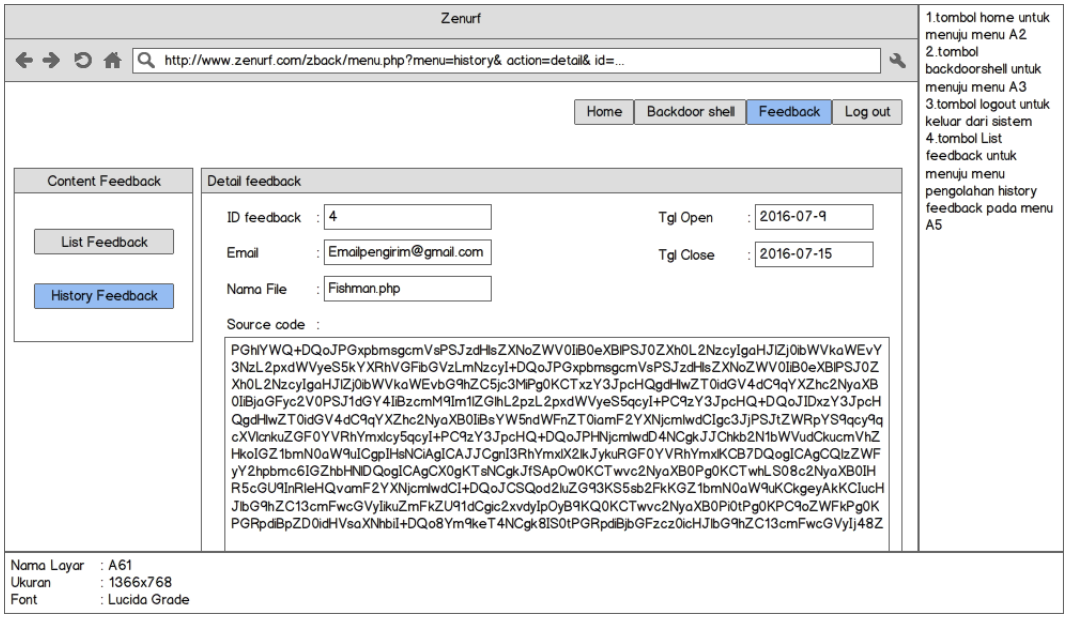
Gambar 3. 45 Perancangan antarmuka menu ubah data signature

Perancangan antarmuka menu detail list feedback aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



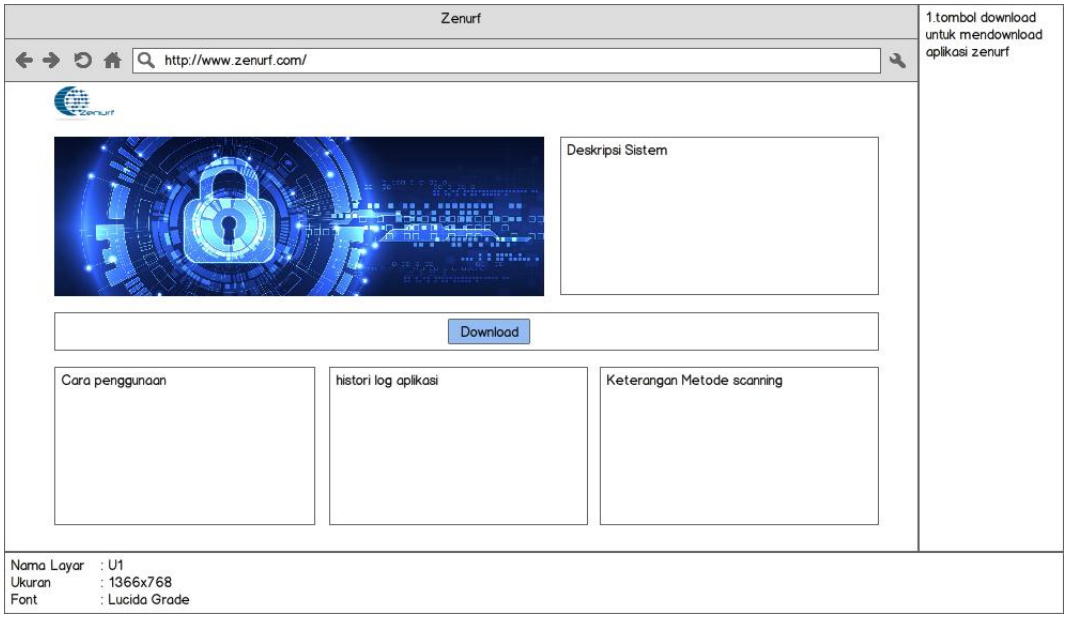
Gambar 3. 46 Perancangan antarmuka menu detail list feedback

Perancangan antarmuka menu detail history feedback aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



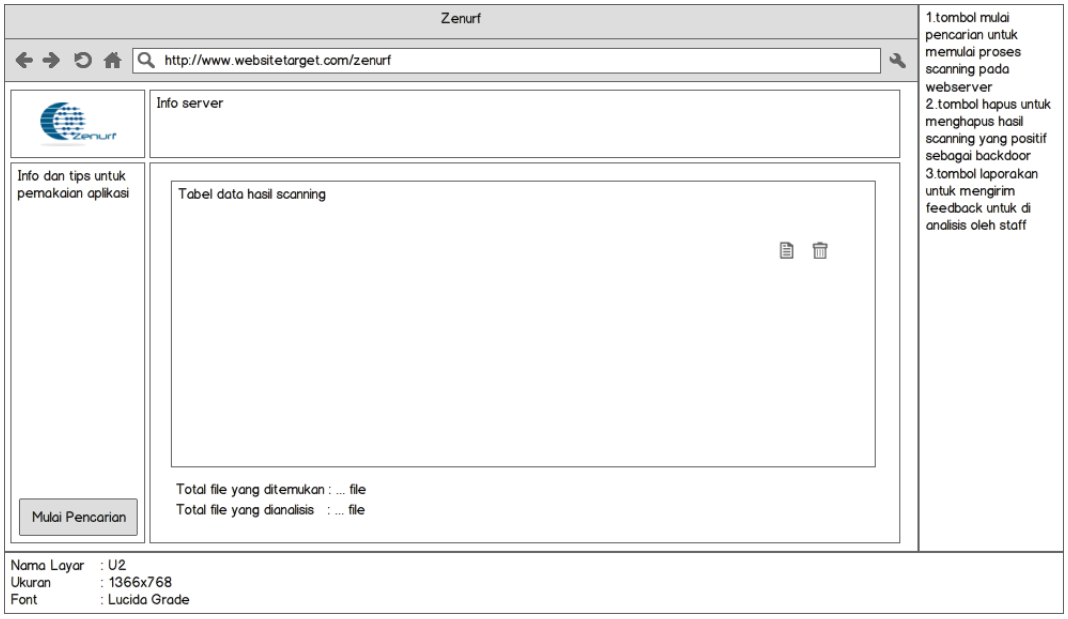
Gambar 3. 47 Perancangan antarmuka menu detail history feedback

Perancangan antarmuka menu homepage user aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



Gambar 3. 48 Perancangan antarmuka menu homepage user

Perancangan antarmuka user menu scanning aplikasi pendeteksi backdoor shell dapat dilihat pada gambar



Gambar 3. 49 Perancangan antarmuka user menu scanning

3.4.5 Perancangan Pesan

Pada tabel dibawah ini merupakan perancangan pesan yang terdapat pada aplikasi pendeteksi backdoor shell pada web server. Adapun tampilan pesan yang ada dapat dilihat pada Tabel 3.15

Tabel 3. 15 Perancangan Pesan

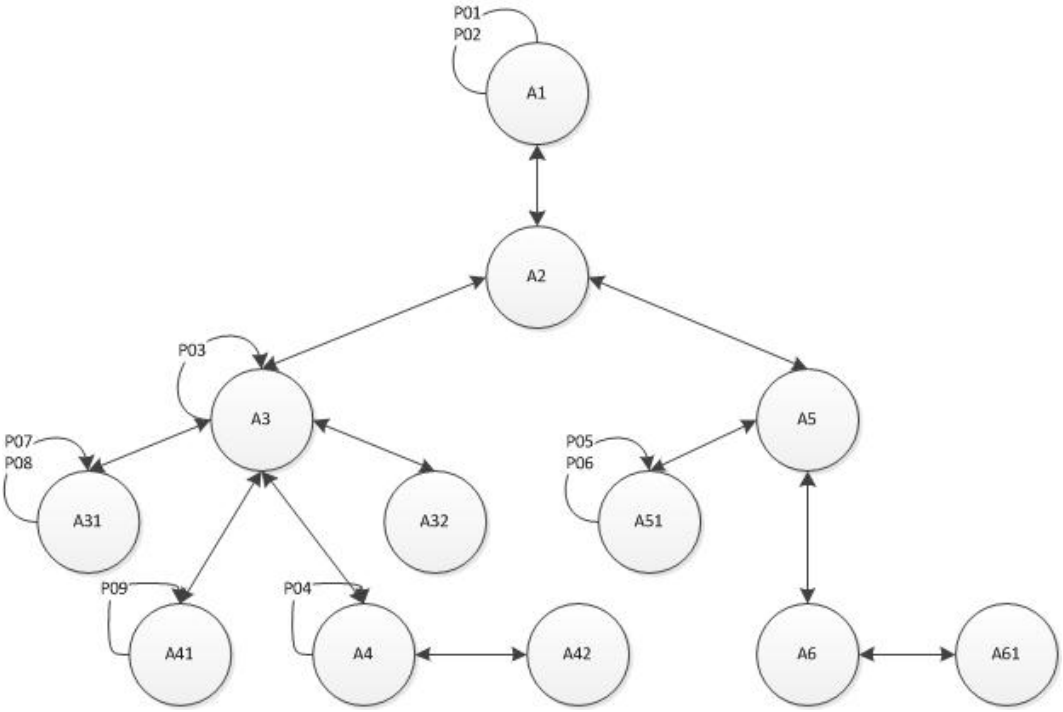
Kode	Pesan
P01	Username dan password harus diisi
P02	Username dan password yang anda masukan salah
P03	Apakah anda yakin untuk menghapus data backdoor yang dipilih ?
P04	Apakah anda yakin untuk menghapus data signature yang dipilih ?
P05	Apakah anda yakin untuk menghapus data feedback yang dipilih ?
P06	Apakah anda yakin untuk close data feedback yang dipilih ?
P07	Nama backdoor masih kosong
P08	Bahasa belum dipilih
P09	BS Signature masih kosong
P10	Apakah anda yakin untuk menghapus file … ?

3.4.6 Perancangan Jaringan Semantik

Jaringan semantik menggambarkan keterhubungan navigasi menu dari satu halaman ke halaman lainnya. jaringan semantik pada aplikasi pendeteksi backdoor shell pada webserver ini, yaitu :

3.4.6.1 Jaringan Semantik Admin

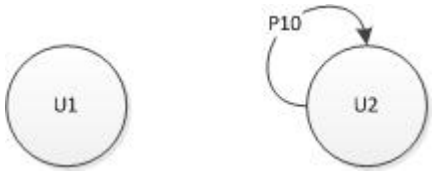
Jaringan semantik admin dapat dilihat pada gambar



Gambar 3. 50 Jaringan semantik admin

3.4.6.2 Jaringan Semantik User

Jaringan semantik user dapat dilihat pada gambar



Gambar 3. 51 Jaringan semantik user

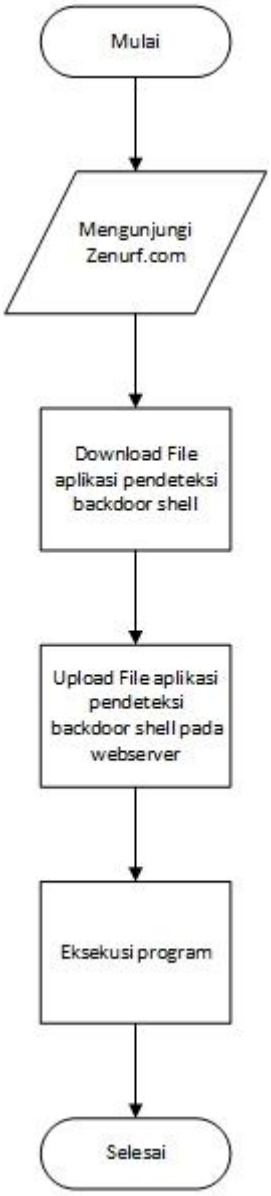
3.4.7 Perancangan Prosedural

Perancangan prosedural merupakan elemen-elemen structural dari arsitektur program ke dalam suatu deskripsi prosedural dari komponen-komponen

perangkat lunak. Perancangan prodedural meliputi prosedural instalasi, prosedural login, prosedural tambah data, prosedural ubah data dan prosedural hapus data.

3.4.7.1 Prosedural Instalasi

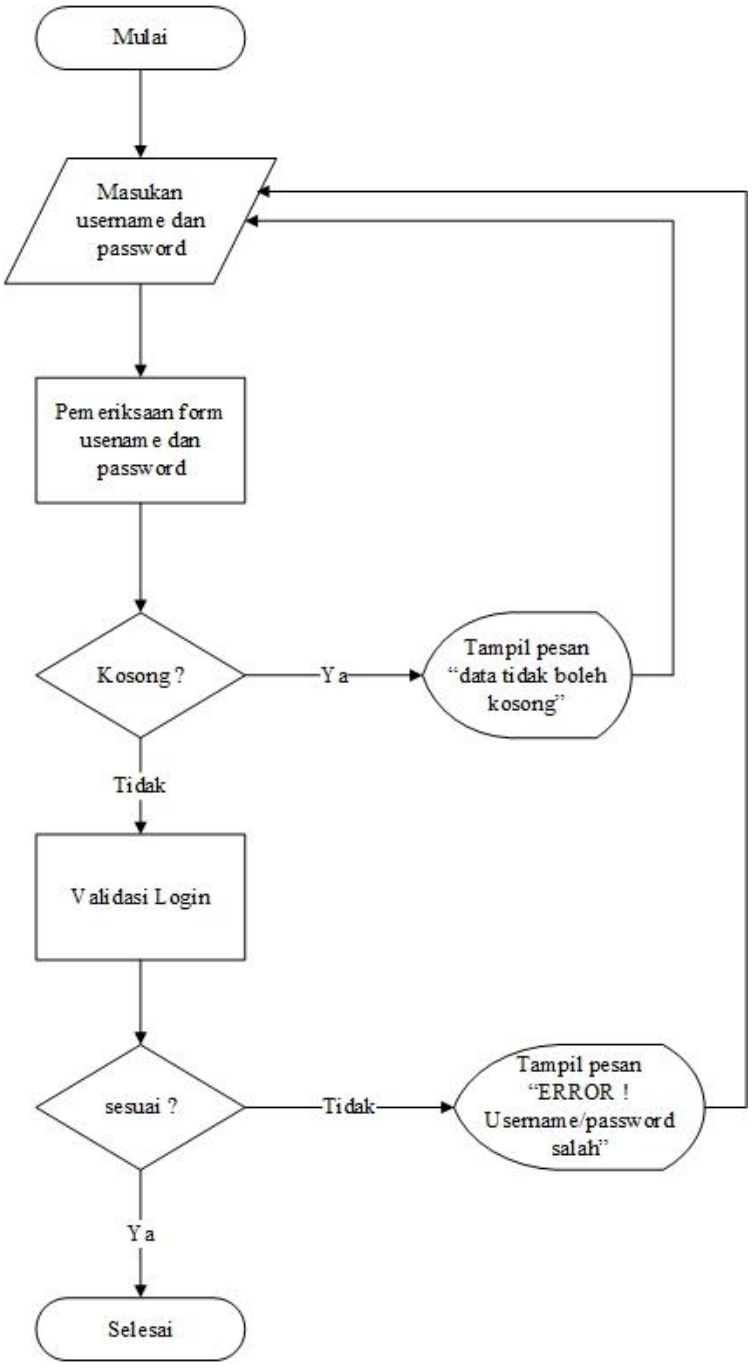
Prosedural Instalasi merupakan langkah-langkah yang dilakukan oleh user untuk melakukan instalasi aplikasi pendeteksi backdoor shell pada web server. Dapat dilihat pada gambar



Gambar 3. 52 Prosedural instalasi

3.4.7.2 Prosedural Login

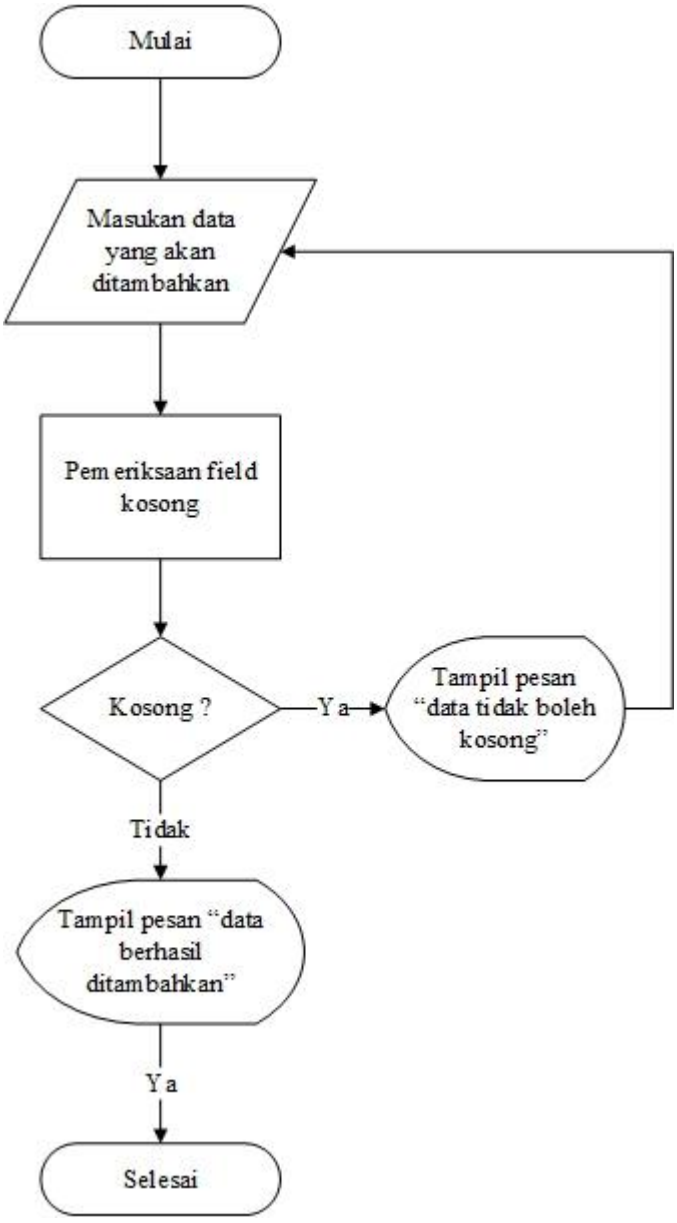
Prosedural login merupakan langkah-langkah admin saat melakukan login. Dapat dilihat pada gambar



Gambar 3. 53 Prosedural login

3.4.7.3 Prosedural Tambah Data

Prosedural tambah data merupakan langkah-langkah admin saat melakukan penambahan data backdoor, blacklist keyword dan signature. Dapat dilihat pada gambar



Gambar 3. 54 Prosedural tambah data

3.4.7.4 Prosedural Ubah Data

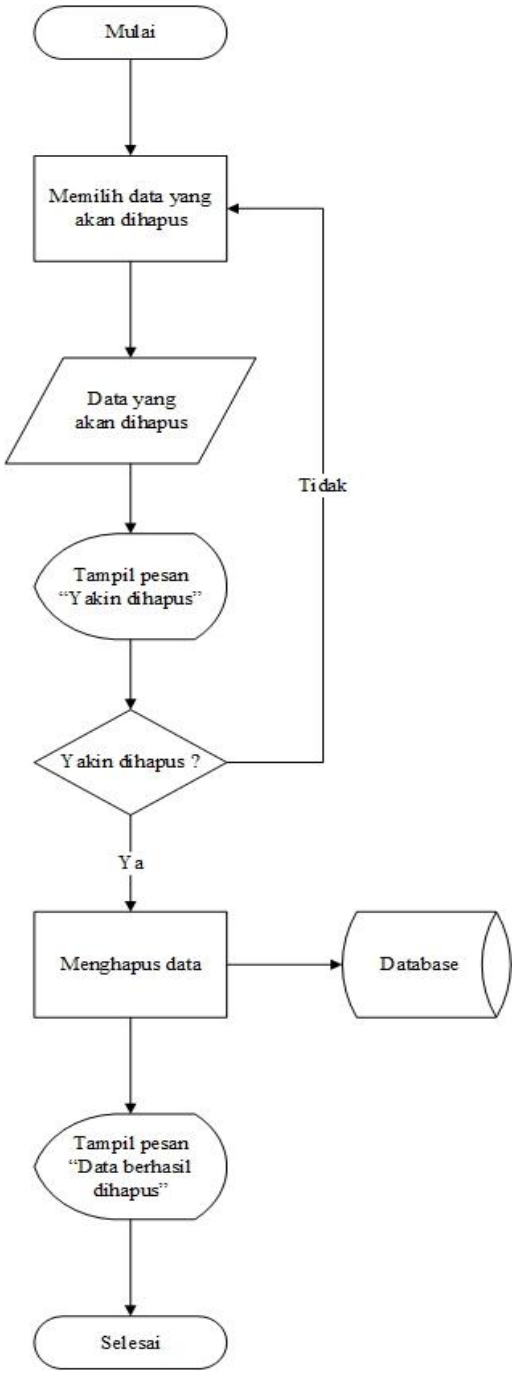
Prosedural ubah data merupakan langkah-langkah admin saat melakukan perubahan data backdoor dan signature. Dapat dilihat pada gambar



Gambar 3. 55 Prosedural ubah data

3.4.7.5 Prosedural Hapus Data

Prosedural hapus data merupakan langkah-langkah admin untuk melakukan penghapusan data backdoor dan signature. Dapat dilihat pada gambar



Gambar 3. 56 Prosedural hapus data