BAB 4
IMPLEMENTASI DAN PENGUJIAN

Bab ini akan dilakukan implementasi dan pengujian terhadap sistem. Tahapan ini dilakukan setelah perancangan selesai dilakukan dan selanjutnya akan diimplementasikan pada bahasa pemrogramman yang akan digunakan. Setelah implementasi maka dilakukan pengujian sistem dimana akan dilihat kekurangan-kekurangan pada aplikasi untuk pengembangan sistem selanjutnya.

4.1 Implementasi

Implementasi merupakan tahap menterjemahkan perancangan berdasarkan hasil analisis. Tujuan implementasi adalah untuk mengkonfirmasikan program yang telah dibangun pada para pelaku sistem sehingga para pengguna dapat memberikan masukan kepada pengembang sistem. Implementasi sistem menjelaskan tentang kebutuhan perangkat keras dan perangkat lunak yang digunakan.

4.1.1 Perangkat Keras yang Digunakan

Perangkat keras yang digunakan untuk menjalankan aplikasi pendeteksi *backdoor shell* ini dapat dilihat pada tabel 4.1.

Tabel 4. 1 Kebutuhan Perangkat Keras

No	Perangkat Keras	Spesifikasi
1	*Processor*	Processor Intel Dual Core 2.3Ghz
2	*Monitor*	Monitor dengan resolusi 1280x1024
3	*Graphic Card*	Nvidia Gforce 500series
4	*Memory*	Ram 1Gb
5	*Mouse*	Standar
6	*Keyboard*	Standar
7	*Internet*	Andromax M2Y

4.1.2 Kebutuhan Perangkat Lunak

Perangkat lunak (software) untuk proses implementasi sistem dapat dilihat pada tabel 4.2

Tabel 4. 2 Kebutuhan Perangkat Lunak

No	Perangkat	Spesifikasi
1	Sistem Operasi	Microsoft Windows 7 Profesional Sp 1 64-bit
2	Browser	Mozila dan Google Chrome
3	Text Editor	Sublime Text Editor 3
4	Server	Xampp v5.6.14

4.1.3 Implementasi Basis Data

Aplikasi database yang digunakan dalam aplikasi pendeteksi backdoor shell menggunakan SQLyog yang merupakan *MySql Manager* dan *MySql Admin Tool* yang bertujuan untuk mengeksekusi perintah-perintah query pada database server. Implementasi database dalam aplikasi pendeteksi backdoor shell ini adalah :

1. Pembuatan *Database*

```
1    CREATE DATABASE zenurf
```

2. Pembuatan Tabel

Berikut adalah daftar tabel-tabel yang terdapat dalam database aplikasi pendeteksi backdoor shell dapat dilihat pada tabel 4.

No	Nama Tabel	Sintak SQL
1	Admin	CREATE TABLE `admin`(`username` varchar(15) NOT NULL, `password` varchar(50) NOT NULL, `email` varchar(50) NOT NULL, PRIMARY KEY(`username`)) ENGINE=InnoDB DEFAULT CHARSET=latin1
2	Bdetail	CREATE TABLE `bdetail`(`id_bs` int(3) NOT NULL AUTO_INCREMENT,

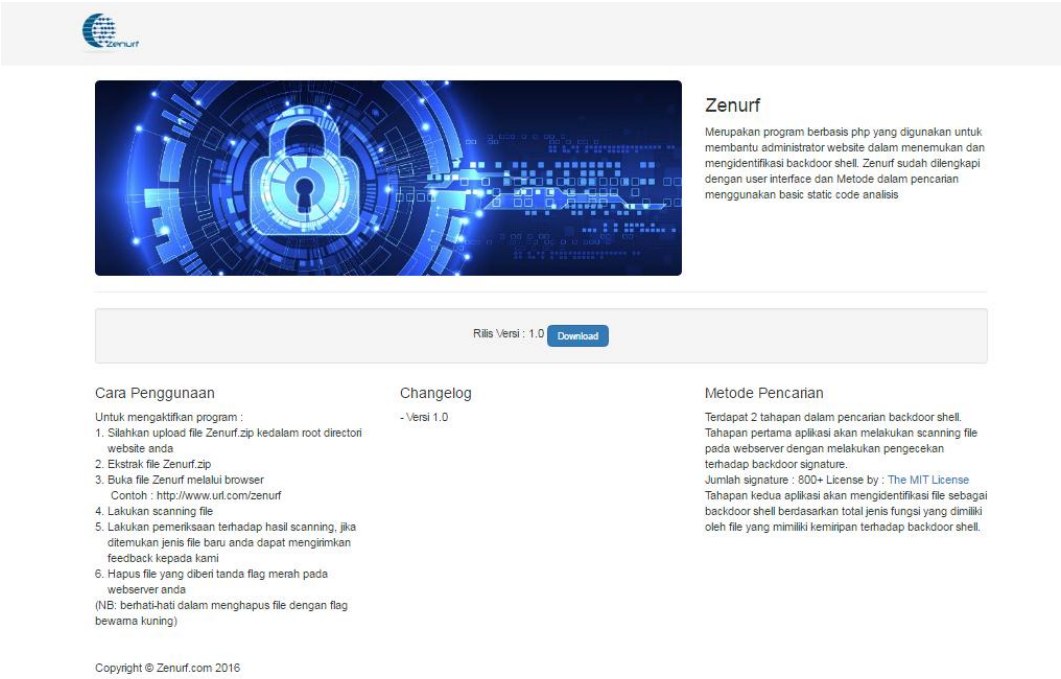
		`nama` varchar(50) NOT NULL, `bahasa`enum('php','asp','jsp','vb','aspx','perl', 'python','bash') NOT NULL, `url` varchar(50), `author`varchar(15), PRIMARY KEY(`id_bs`)) ENGINE=InnoDB DEFAULT CHARSET=latin1
3	Bsignature	CREATE TABLE `bsignature`(`bss` char(64) NOT NULL, PRIMARY KEY (`bss`), Bsignature_ibfk_1(`id_bs`), CONSTRAINT `bsignature_ibfk_1` FOREIGN KEY (`id_bs`) REFERENCES (`bdetail) ON DELETE CASCADE ON UPDATE CASCADE) ENGINE= InnoDB DEFAULT CHARSET=latin1
4	Bfeedback	CREATE TABLE `bfeedback`(`id_fe` int(3) NOT NULL AUTO_INCREMENT, `fb` mediumtext NOT NULL, `nfile` varchar(25) `email` varchar(50) `tgl_open` date NOT NULL, `tgl_close` date `status` enum('1','2') NOT NULL, PRIMARY KEY(`id_fe`)) ENGINE=InnoDB DEFAULT CHARSET=latin1

4.1.4 Implementasi Antarmuka

Implementasi antarmuka adalah hasil dari perancangan antarmuka yang sudah diimplementasikan pada sistem.

4.1.4.1 Tampilan Homepage

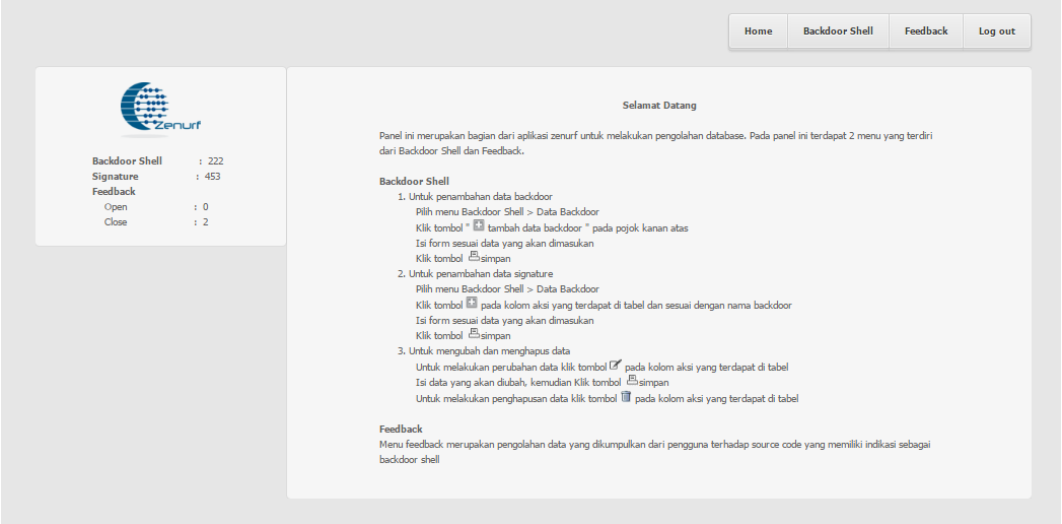
Homepage pada sistem ini merupakan tampilan dari http://www.zenurf.com yang dapat diakses oleh user untuk mengunduh aplikasi pendeteksi *backdoor shell*. Homepage pada aplikasi ini dapat dilihat pada gambar 4.1



Gambar 4. 1 Tampilan Homepage

4.1.4.2 Tampilan Home Admin

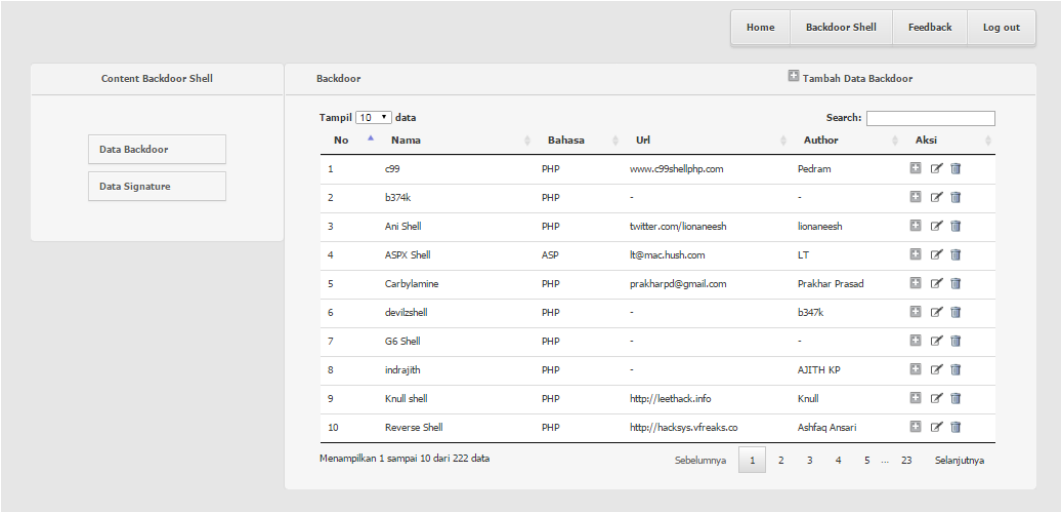
Home admin pada sistem merupakan tampilan awal setelah admin login kedalam sistem backend dari zenurf. Home admin pada aplikasi ini dapat dilihat pada gambar 4.2



Gambar 4. 2 Tampilan Home Admin

4.1.4.3 Tampilan Menu Backdoor Shell

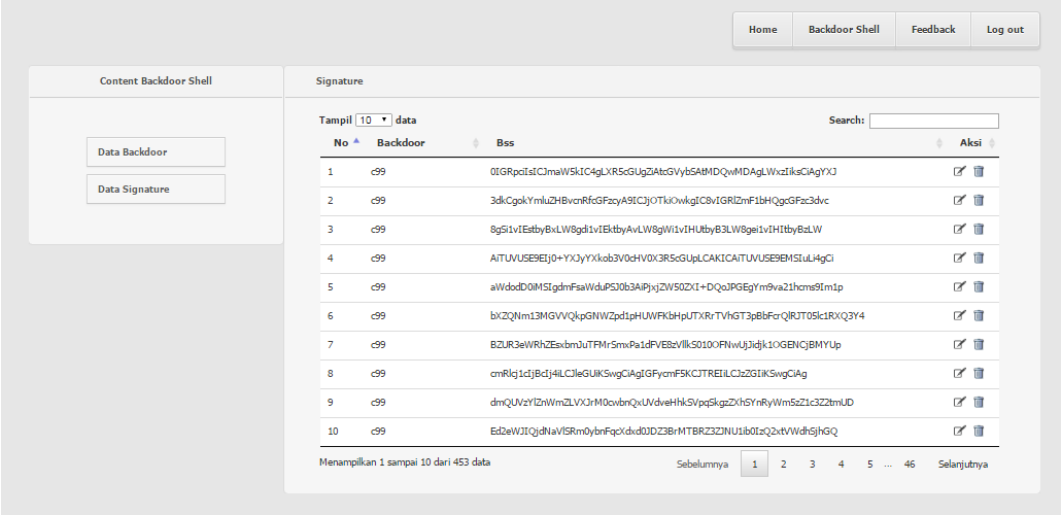
Menu *backdoor shell* merupakan tampilan untuk melakukan kelola data *backdoor shell* oleh admin. Tampilan menu *backdoor shell* dapat dilihat pada gambar 4.3



Gambar 4. 3 Tampilan Menu *Backdoor Shell*

4.1.4.4 Tampilan Menu Signature

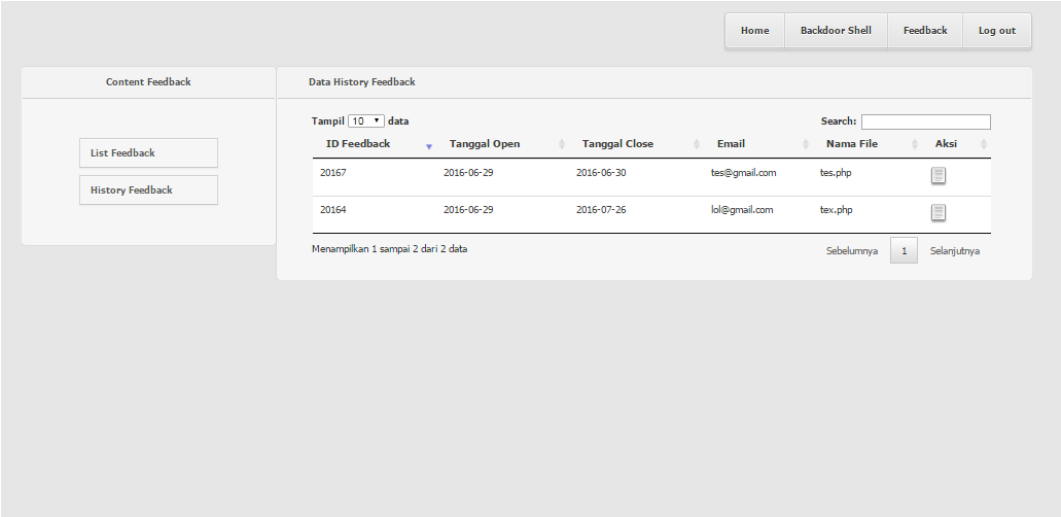
Menu *signature* merupakan tampilan untuk melakukan kelola data signature oleh admin. Tampilan menu *signature* dapat dilihat pada gambar 4.4



Gambar 4. 4 Tampilan Menu *Signature*

4.1.4.5 Tampilan Menu Feedback

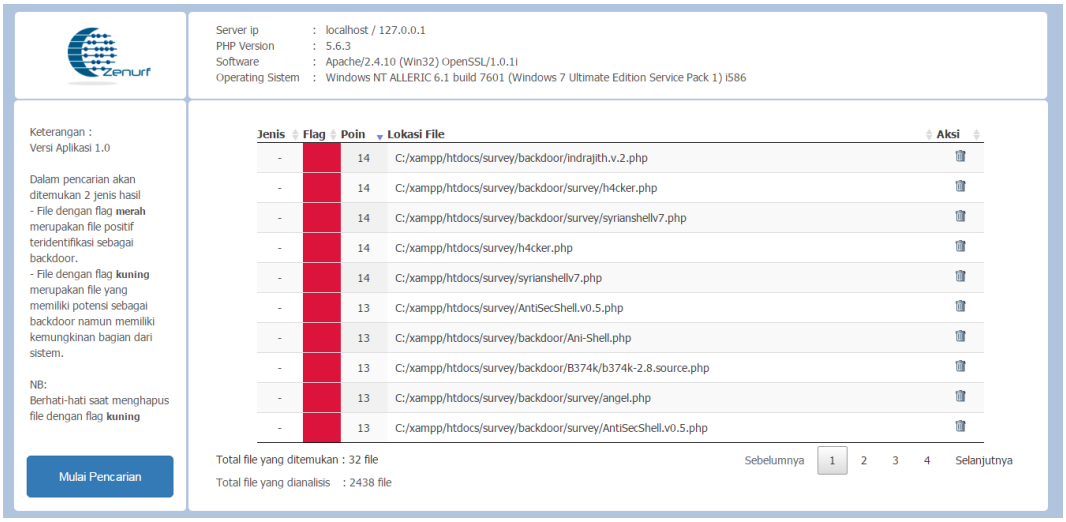
Menu *feedback* merupakan tampilan untuk melakukan kelola data feedback oleh admin. Tampilan menu *feedback* dapat dilihat pada gambar 4.5



Gambar 4. 5 Tampilan Menu Feedback

4.1.4.6 Tampilan Menu Zenurf

Menu zenurf merupakan menu utama dalam pencarian backdoor shell yang digunakan oleh user dalam mengidentifikasi backdoor shell didalam webserver. Menu zenurf dapat dilihat pada gambar 4.6



Gambar 4. 6 Menu Zenurf

4.2 Pengujian Sistem

Pengujian sistem merupakan hal terpenting yang bertujuan untuk menemukan kesalahan-kesalahan atau kekurangan-kekurangan pada sistem yang diuji. Pengujian bermaksud untuk mengetahui sistem yang telah dibangun atau dibuat apakah sudah memenuhi kriteria yang sesuai dengan tujuan perancangan

4.2.1 Rencana Pengujian

Sebelum pengujian dilakukan, diperlukan rencana pengujian untuk menentukan tahap pengujian yang akan dilakukan. Berikut rencana pengujian pada penelitian ini :

1. Rencana Pengujian
2. Skenario Pengujian
3. Hasil Pengujian
4. Pengujian Pengguna
5. Evaluasi Pengujian

4.2.2 Skenario Pengujian

Berdasarkan rencana pengujian yang telah dijelaskan, dilakukan skenario pengujian untuk setiap recana pengujian. Skenario pengujian dibagi menjadi dua

yaitu skenario pengujian *black box* dan skenario pengujian akurasi. Berikut penjelasan untuk skenario pengujian tersebut :

4.2.2.1 Skenario Pengujian Blackbox

Pengujian fungsional yang digunakan untuk menguji sistem yang baru adalah pengujian *black box*. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak yang terdiri dari rencana pengujian dan kasus hasil pengujian. Rencana pengujian yang dilakukan pada Aplikasi pendeteksi *backdoor shell.*

1. Rencana Pengujian Admin

Rencana pengujian admin pada aplikasi pendeteksi backdoor shell. Dapat dilihat pada tabel 4.3

Tabel 4. 3 Rencana Pengujian Admin

No	Kompoen yang diuji	Skenario Pengujian	Hasil yang diharapkan
1	Login	Mengisi data login	*Black box*
		Verifikasi data login	*Black box*
2	Mengelolah Data Backdoor shell	Menambah data backdoor	*Black box*
		Mengubah data backdoor	*Black box*
		Menghapus data backdoor	*Black box*
3	Mengelolah Data Signature	Menambah data signature	*Black box*
		Mengubah data signature	*Black box*
		Menghapus data signature	*Black box*
4	Mengelolah Data List Feedback	Melihat detail feedback	*Black box*
		Close data feedback	*Black box*
		Menghapus data feedback	*Black box*
5	History Feedback	Melihat detail feedback	*Blackbox*
6	Keluar	Menghapus session admin	*Black box*

7	Cari Data	Menampilkan hasil cari data backdoor	*Black box*
		Menampilkan hasil cari data signature	*Black box*
		Menampilkan hasil cari data feedback	*Black box*

2. Rencana Pengujian User

Rencana pengujian user pada aplikasi pendeteksi backdoor shell. Dapat dilihat pada tabel 4.4

Tabel 4. 4 Rencana Pengujian User

No	Komponen yang diuji	Skenario Pengujian	Hasil yang diharapkan
1	Download	Mendownload aplikasi	*Black box*
2	Pencarian Backdoor shell	Melakukan pencarian file backdoor	*Black box*
3	Hapus File	Menghapus file yang terdeteksi	*Black box*

3. Rencana Pengujian Website

Dalam pengujian website untuk mendeteksi backdoor shell pada web server dilakukan pada beberapa website dengan tujuan untuk mengetahui apakah didalam webserver tersebut memiliki backdoor shell atau tidak. Dikarenakan sulitnya mencari website yang terinfeksi maka pada pengujian ini disisipkan beberapa backdoor shell pada website yang akan diuji untuk mengetahui apakah sistem dapat mendeteksi atau tidak. Berikut adalah tabel skenario pengujian website untuk mendeteksi backdoor shell dapat dilihat pada tabel 4.5

Tabel 4. 5 Rencana Pengujian Website

No	Website	Hasil Pengujian			Kemungkinan Hasil
		Jumlah File	Positif	Dicurigai	
1	One Day Service Monitoring System	Angka	Angka	Angka	Bersih/terinfeksi
2	Profil Aruiter University	Angka	Angka	Angka	Bersih/terinfeksi

3	Prediksi Curah Hujan	Angka	Angka	Angka	Bersih/terinfeksi
4	Kepegawaian Nur Straits Engineering (NSE)	Angka	Angka	Angka	Bersih/terinfeksi
5	Ecommerce Jersey Eorder	Angka	Angka	Angka	Bersih/terinfeksi
6	DidieWae Commerce	Angka	Angka	Angka	Bersih/terinfeksi
7	SMP Negri 25 Bandung	Angka	Angka	Angka	Bersih/terinfeksi
8	Sistem Informasi Perpustakaan Nasional	Angka	Angka	Angka	Bersih/terinfeksi
9	Pemodelan dan Simulasi Curah Hujan	Angka	Angka	Angka	Bersih/terinfeksi
10	New Cianjur Aqobah	Angka	Angka	Angka	Bersih/terinfeksi
11	SI absensi SMPN 28 Bandung	Angka	Angka	Angka	Bersih/terinfeksi
12	Pembuatan Surat Perjalanan Dinas Kantor Dinas Martech	Angka	Angka	Angka	Bersih/terinfeksi
13	System Aplikasi Rekam Medis	Angka	Angka	Angka	Bersih/terinfeksi
14	Profil Sekolah SMP 28 Bandung	Angka	Angka	Angka	Bersih/terinfeksi
15	Astria Mandiri app	Angka	Angka	Angka	Bersih/terinfeksi

16	SI penilaian guru	Angka	Angka	Angka	Bersih/terinfeksi
17	Sistem Pakar Diagnosa Penyakit Ayam	Angka	Angka	Angka	Bersih/terinfeksi
18	Sistem Meteran KWH bulanan penduduk	Angka	Angka	Angka	Bersih/terinfeksi
19	Sistem Reservasi Hoteltea	Angka	Angka	Angka	Bersih/terinfeksi

4.2.2.2 Skenario Pengujian Akurasi

Dalam pengujian akurasi dilakukan pada aplikasi yang memiliki *user interface* dibagi menjadi dua bagian yaitu :

1. Skenario pengujian deteksi menggunakan Aplikasi yang dibangun.
2. Skenario pengujian deteksi menggunakan PHP shell detector.

Pengujian akurasi dalam mendeteksi backdoor shell pada web server dilakukan terhadap 12 sample backdoor shell dengan total file yang dianalisis 3964 file. Dan dilakukan perhitungan akurasi berdasarkan total backdoor shell beserta nilai *precision* dan *recall*. Berikut adalah tabel skenario akurasi untuk mendeteksi backdoor shell pada web server, dapat dilihat pada tabel 4.6

Tabel 4. 6 Skenario pengujian akurasi pada sampel

No	Backdoor Shell	Hasil Deteksi
1	BoffMax	Positif / Dicurigai / Negatif
2	C102	Positif / Dicurigai / Negatif
3	CYBERDARK	Positif / Dicurigai / Negatif
4	Dhanush	Positif / Dicurigai / Negatif
5	EgY_SpIdEr	Positif / Dicurigai / Negatif
6	G00nshell	Positif / Dicurigai / Negatif

7	K2ll33d	Positif / Dicurigai / Negatif
8	K3c4	Positif / Dicurigai / Negatif
9	Fi73 M4n4g3r	Positif / Dicurigai / Negatif
10	Madspotshellscript	Positif / Dicurigai / Negatif
11	SpyShell	Positif / Dicurigai / Negatif
12	Storm7Shell	Positif / Dicurigai / Negatif

4.2.3 Hasil Pengujian

Hasil pengujian merupakan hasil dari skenario pengujian yang telah dilakukan, sehingga hasil pengujian dibagi menjadi 2 yaitu hasil pengujian *black box*, dan hasil pengujian akurasi. Berikut penjelasan untuk masing-masing hasil pengujian :

4.2.3.1 Hasil Pengujian Black Box

1. Hasil pengujan admin pada aplikasi pendeteksi *backdoor shell* dapat dilihat pada tabel 4.7

Tabel 4. 7 Kasus dan Hasil Pengujian Admin

1. Login			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
username : admin *Password* : @admin	Jika data *login* valid maka admin akan masuk ke dalam halaman *home* aplikasi	Semua *field* terisi/benar dalam pengisian maka admin akan masuk kedalam halaman home aplikasi	Diterima
Kasus Hasil Uji Salah (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
semua *field* dalam form login kondisi kosong	Dapat menampilkan pesan "*username* dan *password* harus diisi"	Menampilkan pesan "*username* dan *password* harus diisi"	Diterima

field username kosong	Dapat menampilkan pesan "*username* dan *password* harus diisi"	Menampilkan pesan "*username* dan *password* harus diisi"	Diterima
field password kosong	Dapat menampilkan pesan "*username* dan *password* harus diisi"	Menampilkan pesan "*username* dan *password* harus diisi"	Diterima
field username yang salah	Dapat menampilkan pesan "Maaf *username* dan *password* yang anda masukan salah"	Menampilkan pesan "Maaf *username* dan *password* yang anda masukan salah"	Diterima
field Password yang salah	Dapat menampilkan pesan "Maaf *username* dan *password* yang anda masukan salah"	Menampilkan pesan "Maaf *username* dan *password* yang anda masukan salah"	Diterima
2. Mengolah Data Backdoor Shell			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Nama Backdoor : B374k Bahasa : PHP Url: prakharpd@gmail.com	Jika data yang telah dimasukan lengkap dan benar, maka aplikasi akan memproses dan menambahkan data ke dalam aplikasi.	*Field* terisi dan benar dalam pengisian maka data *backdoor shell* ditambahkan kedalam aplikasi	Diterima
Nama Backdoor : B374k Bahasa : ASPX	Jika data ubah yang dimasukan benar maka aplikasi akan memproses pengubahan data pada sistem	*Field* diubah dan benar dalam pengisian maka data *backdoor shell* diubah pada sistem	Diterima
B374k	Jika dipilih hapus pada list data akan muncul pesan "apakah anda yakin akan menghapus data ...?" jika iya kemudian sistem	Menampilkan pesan "apakah anda yakin akan menghapus data B374k ?" kemudian data terhapus	Diterima

	menghapus data tersebut		
Kasus Hasil Uji Salah (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
field nama *backdoor* kosong	Dapat menampilkan pesan "nama *backdoor* harus diisi"	Menampilkan pesan "nama *backdoor* harus diisi"	Diterima
field bahasa kosong	Dapat menampilkan pesan "bahasa belum dipilih"	Menampilkan pesan "bahasa belum dipilih"	Diterima
3. Mengolah Data Signature			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Nama *Backdoor* : B374k Bssignature : NFNaLwpXdFZI L2RwRGJMdlJjW mRzeW4rMUNjM 3I4TXJzdWp5Ym RoakkyMGRQRitl	Jika data yang telah dimasukan lengkap dan benar, maka aplikasi akan memproses dan menambahkan data ke dalam aplikasi.	*Field* terisi dan benar dalam pengisian maka data *signature* ditambahkan kedalam aplikasi	Diterima
Nama Backdoor : B374k Bssignature : L2RwRGJMdlJjW mRzeW4rMUNjM 3I4TXJzdWp5Ym RoakkyMGRQRitl NFNaLwpXdFZI	Jika data ubah yang dimasukan benar maka aplikasi akan memproses pengubahan data pada sistem	*Field* diubah dan benar dalam pengisian maka data *signature* diubah pada sistem	Diterima
L2RwRGJMdlJjW mRzeW4rMUNjM 3I4TXJzdWp5Ym RoakkyMGRQRitl NFNaLwpXdFZI	Jika dipilih hapus pada list data akan muncul pesan "apakah anda yakin akan menghapus data ...?" jika iya kemudian sistem menghapus data tersebut	Menampilkan pesan "apakah anda yakin akan menghapus data ... ?" kemudian data terhapus	Diterima
Kasus Hasil Uji Salah (Data Salah)			

Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
field BS *signature* kosong	Dapat menampilkan pesan "BS *signature* harus diisi"	Menampilkan pesan "BS *signature* harus diisi"	Diterima
4. Mengolah Data List Feedback			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Info ID *feedback* 20167	Dapat menampilkan data tentang detail *feedback* yang dipilih	Menampilkan data tentang detail *feedback* 20167	Diterima
Close tiket 20167	Dapat mengupdate data *feedback* dari *open* menjadi *close* setelah dianalisis	Mengupdate data *feedback* 20167 dari *open* menjadi *close*	Diterima
Hapus data 20168	Dapat melakukan penghapusan data *feedback* yang masuk karena tidak *valid*	Melakukan penghapusan data *feedback* 20168	Diterima
5. History Feedback			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Info ID *feedback* 20167	Dapat menampilkan data tentang detail *feedback* yang dipilih	Menampilkan data tentang detail *history feedback* 20167	Diterima
6. Log out			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Menu *logout*	Dapat menghapus *session admin* dan keluar dari sistem	Menghapus *session admin* dan keluar dari sistem	Diterima
7. Cari Data			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan

C99	Dapat menampilkan data *backdoor shell* yang dicari.	Menampilkan data *backdoor shell* C99 yang dicari	Diterima
mRzeW4rMUNjM 3I4TXJzdWp5Ym	Dapat menampilkan data *Signature* yang dicari.	Menampilkan data *Signature* mRzeW4rMUNjM 3I4TXJzdWp5Ym	Diterima
20167	Dapat menampilkan data *feedback* yang dicari.	Menampilkan data *feedback* 20167	Diterima

2. Kasus dan hasil pengujan user pada aplikasi pendeteksi *backdoor shell* dapat dilihat pada tabel 4.8

Tabel 4. 8 Kasus dan Hasil Pengujian User

1. Download			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Download	Dapat melakukan *download* aplikasi dari *website*	Melakukan *download* aplikasi dari *website*	Diterima
2. Pencarian Backdoor shell			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Mulai Pencarian	Dapat melakukan pencarian *file backdoor shell* pada *webserver*	Melakukan pencarian *file backdoor shell* pada *webserver*	Diterima
3. Hapus file			
Kasus Hasil Uji Benar (Data Benar)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
C99	Dapat menghapus file dari webserver yang terdeteksi sebagai backdoor shell	Menghapus file C99 dari *webserver* yang terdeteksi sebagai *backdoor shell*	Diterima

3. Hasil dari pengujian website untuk mendeteksi apakah website yang dianalisis terindikasi memiliki backdoor atau tidak. Berikut hasil pengujian dapat dilihat pada tabel 4.9

Tabel 4. 9 Hasil Pengujian Website

No	Website	Hasil Pengujian			Keterangan
		Jumlah File	Positif	Dicurigai	
1	One Day Service Monitoring System	452	0	0	Bersih
2	Profil Aruiter University	209	0	0	Bersih
3	Prediksi Curah Hujan	68	0	0	Bersih
4	Kepegawaian Nur Straits Engineering (NSE)	243	0	0	Bersih
5	Ecommerce Jersey Eorder	104	0	0	Bersih
6	DidieWae Commerce	116	0	0	Bersih
7	SMP Negri 25 Bandung	7299	0	10	Bersih
8	Sistem Informasi Perpustakaan Nasional	159	0	0	Bersih
9	Pemodelan dan Simulasi Curah Hujan	99	0	0	Bersih
10	New Cianjur Aqobah	308	1	0	Terinfeksi SpyShell

11	SI absensi SMPN 28 Bandung	1698	1	0	Terinfeksi EgY_SpIdEr
12	Pembuatan Surat Perjalanan Dinas Kantor Dinas Martech	1046	0	1	Bersih
13	System Aplikasi Rekam Medis	471	0	1	Bersih
14	Profil Sekolah SMP 28 Bandung	4246	1	0	Terinfeksi K2ll33d
15	Astria Mandiri app	2365	0	0	Bersih
16	SI penilaian guru	2337	1	0	Terinfeksi Madspotshell script
17	Sistem Pakar Diagnosa Penyakit Ayam	85	1	0	Terinfeksi K4c3
18	Sistem Meteran KWH bulanan penduduk	2459	0	0	Bersih
19	Sistem Reservasi Hoteltea	2788	1	0	Terinfeksi c102

Dari hasil pengujian website terhadap beberapa website pada tabel 4.9 diatas diperoleh hasil aplikasi berjalan baik dan pada beberapa website yang telah ditanamkan backdoor shell sebelumnya dapat terdeteksi.

4.2.3.2 Hasil Pengujian Akurasi

Pengujian akurasi dilakukan pada web server yang memiliki total file 3964 file dengan kondisi 12 sampel *backdoor shell* telah disisipkan didalam web server.

1. Hasil pengujian deteksi menggunakan Aplikasi yang dibangun.

Berikut hasil pengujian menggunakan aplikasi yang dibangun dapat dilihat pada tabel 4.10

Tabel 4. 10 Hasil Pengujian Dengan Aplikasi Yang Dibangun

No	Backdoor Shell	Hasil Deteksi
1	BoffMax	Dicurigai
2	C102	Positif
3	CYBERDARK	Positif
4	Dhanush	Positif
5	EgY_SpIdEr	Positif
6	G00nshell	Dicurigai
7	K2ll33d	Positif
8	K3c4	Positif
9	Fi73 M4n4g3r	Negatif
10	Madspotshellscript	Positif
11	SpyShell	Positif
12	Storm7Shell	Positif

Dari hasil pengujian diperoleh data sebagai berikut

Total File yang ditemukan sebanyak 17 file. File yang positif teridentifikasi sebagai backdoor shell 9 file. File yang dicurigai sebagai backdoor shell : 8 file. File yang negatif atau tidak terdeteksi : 1 file. Dan dari tabel kita dapat mengetahui akurasi dalam mengidentifikasi file backdoor shell sebagai berikut :

$$Akurasi = \frac{9}{12}\ x\ 100\% = 75\ \%$$

Tabel 4. 11 Pengujian Precision dan Recall Aplikasi Yang Dibangun

N : 3964		*Predicted*	
		Backdoor shell (*No*)	*Backdoor shell* (*Yes*)
Actual	*Backdoor shell* (*No*)	3946	6
	Backdoor shell (*Yes*)	1	11

$$Precision = \frac{True\ Positif}{True\ Positif + False\ Positif} = \frac{11}{11+6} = \frac{11}{17} = 0{,}64$$

$$Recall = \frac{True\ Positif}{True\ Positif + False\ Negatif} = \frac{11}{11+1} = \frac{11}{12} = 0{,}91$$

2. Hasil pengujian deteksi menggunakan Php Shell Detector

Berikut hasil pengujian menggunakan aplikasi Php shell detector dapat dilihat pada tabel 4. 12

Tabel 4. 12 Hasil Pengujian Dengan Php Shell Detector

No	Backdoor Shell	Hasil Deteksi
1	BoffMax	Dicurigai
2	C102	Dicurigai
3	CYBERDARK	Dicurigai
4	Dhanush	Positif
5	EgY_SpIdEr	Positif
6	G00nshell	Dicurigai
7	K2ll33d	Negatif
8	K3c4	Positif
9	Fi73 M4n4g3r	Negatif
10	Madspotshellscript	Dicurigai
11	SpyShell	Dicurigai
12	Storm7Shell	Positif

Dari hasil pengujian diperoleh data sebagai berikut

Total File yang ditemukan sebanyak 120 file. File yang positif teridentifikasi sebagai backdoor shell 4 file. File yang dicurigai sebagai backdoor shell : 116 file. File yang negatif atau tidak terdeteksi : 2 file. Dan dari tabel kita dapat mengetahui akurasi dalam mengidentifikasi file backdoor shell sebagai berikut :

$$Akurasi = \frac{4}{12}\ x\ 100\% = 33.3\ \%$$

Tabel 4. 13 Pengujian Precision dan Recall Aplikasi Php Shell Detector

N : 3964		*Predicted*	
		Backdoor shell (*No*)	*Backdoor shell* (*Yes*)
Actual	*Backdoor shell* (*No*)	3842	110
	Backdoor shell (*Yes*)	2	10

$$Precision = \frac{True\ Positif}{True\ Positif + False\ Positif} = \frac{10}{10 + 110} = \frac{10}{120} = 0{,}083$$

$$Recall = \frac{True\ Positif}{True\ Positif + False\ Negatif} = \frac{10}{10 + 12} = \frac{10}{12} = 0{,}83$$

4.2.4 Pengujian Pengguna

Pengujian pengguna merupakan pengujian yang dilakukan secara objektif yang dilakukan secara lansung oleh pengguna yang nantinya akan menggunakan perangkat lunak pendeteksi *backdoor shell* ini. Penelitian ini dilakukan dengan menggunakan teknik kuisioner untuk pengelola website. Hal ini dilakukan agar dapat mengetahui sejauh mana aplikasi yang dibangun ini dapat membantu dan dapat menyelesaikan masalah yang sudah dijelaskan pada perumusan masalah.

4.2.4.1 Perhitungan Hasil Kuesioner

Pada kuesioner ini terdiri dari 3 aspek. Berikut adalah hasil perhitungan masing-masing hasil observasi dari pengamatan terhadap 35 responden, dengan ditunjukan poin penilaian dari aspek observasi yang dapat dilihat pada tabel 4.14

Tabel 4. 14 Poin Penilaian

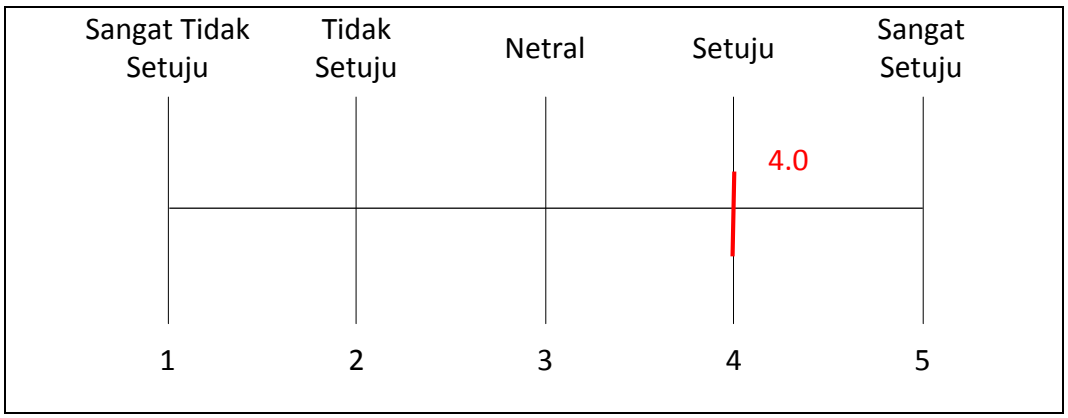
Jawaban	Poin Penilaian
Sangat Setuju	5
Setuju	4
Netral	3
Tidak Setuju	2
Sangat Tidak Setuju	1

Tanggapan dan penilaian pengamatan terhadap pengguna untuk mengetahui hasil dari aplikasi ini, telah disebarkan format observasi pengamatan kepada responden berdasarkan target pengguna dan dilakukan pehitungan, kemudian dicari persentase masing-masing jawaban dengan menggunakan skala *likert*.

Berikut ini adalah hasil perhitungan dari masing-masing jawaban yang sudah dihitung nilainya dengan menggunakan perhitungan rumus hasil yaitu jumlah dibagi dengan banyaknya sampel.

Tabel 4. 15 Aspek Observasi no 1

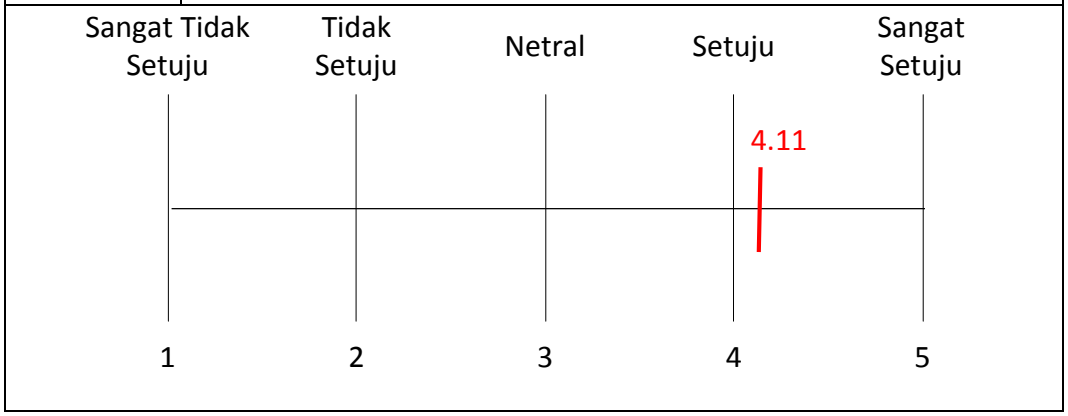
Aspek Observasi dan Hasil Pengujian					
No 1	Apakah anda setuju aplikasi zenurf mudah untuk digunakan ?				
	Sangat Setuju	Setuju	Netral	Tidak Setuju	Sangat Tidak Setuju
Responden	6	23	6	0	0
Sampel	35	35	35	35	35
Jumlah	(6x5) + (23x4) + (6x3) + (0x2) + (0x1) = 140				
Hasil	140 / 35 = 4,0				



Aspek observasi pada tabel 4.15, dapat dilihat bahwa aplikasi yang dibangun mudah untuk digunakan oleh user.

Tabel 4. 16 Aspek Observasi no 2

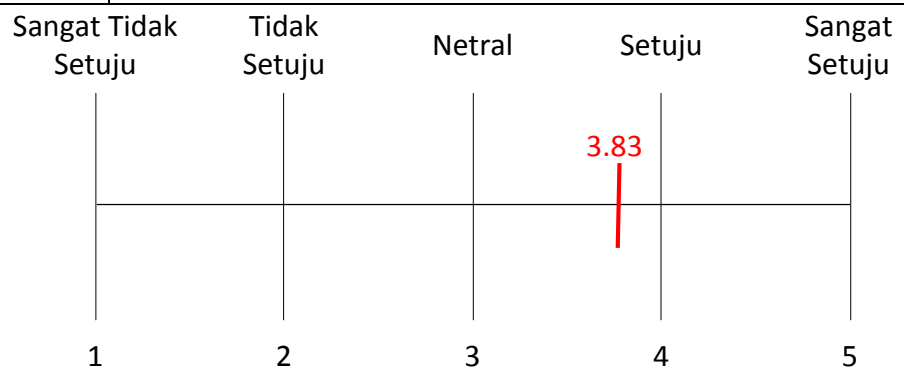
Aspek Observasi dan Hasil Pengujian					
No 2	Apakah anda setuju aplikasi zenurf dapat membantu anda dalam menemukan *backdoor shell* pada *web server* ?				
	Sangat Setuju	Setuju	Netral	Tidak Setuju	Sangat Tidak Setuju
Responden	7	25	3	0	0
Sampel	35	35	35	35	35
Jumlah	(7x5) + (25x4) + (3x3) + (0x2) + (0x1) = 144				
Hasil	144 / 35 = 4,11				



Aspek observasi pada tabel 4.16, dapat dilihat bahwa aplikasi yang dibangun dapat membantu *user* dalam menemukan *backdoor shell* pada *web server*.

Tabel 4. 17 Aspek Observasi no 3

Aspek Observasi dan Hasil Pengujian					
No 3	Apakah anda setuju aplikasi zenurf dapat mempercepat proses pencarian *backdoor shell* pada *web server* ?				
	Sangat Setuju	Setuju	Netral	Tidak Setuju	Sangat Tidak Setuju
Responden	3	24	7	1	0
Sampel	35	35	35	35	35
Jumlah	(3x5) + (24x4) + (7x3) + (1x2) + (0x1) = 134				
Hasil	134 / 35 = 3,83				



Aspek observasi pada tabel 4.17, dapat dilihat bahwa aplikasi yang dibangun dapat mempercepat proses pencarian *backdoor shell* pada *web server*.

4.2.5 Evaluasi Pengujian

Berdasarkan hasil pengujian yang telah dilakukan maka dilakukan evaluasi terhadap dua hasil pengujian tersebut. Berikut penjelasan untuk masing-masing hasil pengujian.

1. Evaluasi pengujian *black box*

   Berdasarkan pengujian *black box* yang telah dilakukan, dapat disimpulkan bahwa setiap fungsionalitas pada sistem dan pencarian pada website telah berjalan dengan baik.

2. Evaluasi pengujian akurasi

   Berdasarkan pengujian akurasi yang telah dilakukan terhadap kedua aplikasi, dapat disimpulkan bahwa menggunakan aplikasi yang dibangun memiliki akurasi yang lebih baik dibandingkan dengan menggunakan aplikasi *php shell detector*. Dan dari jumlah hasil deteksi yang dicurigai dari aplikasi yang dibangun lebih sedikit dibandingkan aplikasi *php shell detector*, sehingga lebih efisien jika administrator website atau pemilik website ingin menganalisis lebih mendalam.

3. Evaluasi pengujian pengguna

   Berdasarkan pengujian yang telah dilakukan dengan obeservasi pengamatan melaui kuesioner maka dapat disimpulkan bahwa aplikasi yang dibangun dapat mempermudah pengelola website dalam menemukan file backdoor shell pada webserver telah terpenuhi.