

MANUAL

GUIDELINES FOR A BEGINNER

MODULES :

- * Execute System Commands
- * Traversing and Creating Directories
- * Searching for files as well as folders
- * File Upload and Download
- * Create and Edit Files
- * Create PDF Files
- * Full Database Administration
- * String Encoding and Decoding

Control OS From This File

Software: Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
uname -a: Windows NT VAIO-VAIO 6.1 build 7601
valo
Safe-mode: Off (not secure)
C:\xampp\htdocs\project\ [permissions]
Free 76.23 GB of 114.24 GB (66.72%)
Detected drives: [a][c][d][e][f][g]

Encoder Process Create PDF File Security Info SQL Chat With Admins Feedback Self remove Logout

Owned by I-AM-IT

Listing folder (19 files and 8 folders):

Name ▲	Size	Modify	Perms
.	LINK	29.03.2011 18:05:23	drwxr-xr-x
..	LINK	29.03.2011 12:26:39	drwxr-xr-x
[abc-test]	DIR	29.03.2011 18:05:23	drwxr-xr-x
[cache]	DIR	15.03.2011 10:12:28	drwxr-xr-x
[chat]	DIR	25.03.2011 15:06:11	drwxr-xr-x
[config]	DIR	15.03.2011 10:12:28	drwxr-xr-x
[doc]	DIR	15.03.2011 10:12:28	drwxr-xr-x
[examples]	DIR	15.03.2011 10:12:28	drwxr-xr-x
[fonts]	DIR	16.03.2011 04:47:10	drwxr-xr-x
[images]	DIR	17.03.2011 16:43:31	drwxr-xr-x
2dhercodes.php	7.6 KB	18.12.2010 11:00:56	-rw-rw-rw-
CHANGELOG.TXT	76.99 KB	27.02.2011 07:43:10	-rw-rw-rw-
LICENSE.TXT	42.72 KB	17.11.2010 07:36:50	-rw-rw-rw-
README.TXT	3.75 KB	27.02.2011 07:43:10	-rw-rw-rw-
amit.php	145.66 KB	29.03.2011 09:49:34	-rw-rw-rw-
barcodes.php	58.39 KB	18.12.2010 10:30:22	-rw-rw-rw-
chat.php	2.6 KB	22.09.2008 17:36:54	-rw-rw-rw-
htmlcolors.php	5.37 KB	18.12.2010 09:44:28	-rw-rw-rw-
index.php	43 B	01.03.2011 17:22:20	-rw-rw-rw-
pdf417.php	52.48 KB	18.12.2010 10:29:42	-rw-rw-rw-
qrcode.php	78.18 KB	18.12.2010 10:28:50	-rw-rw-rw-
refresh.php	189 B	22.09.2008 17:36:54	-rw-rw-rw-
spotcolors.php	2.1 KB	18.12.2010 09:44:08	-rw-rw-rw-
submit.php	201 B	22.09.2008 17:36:54	-rw-rw-rw-
tcpdf.crt	2.24 KB	22.09.2008 17:36:54	-rw-rw-rw-

Graphical Directory Traversing

Enter: Execute

Select: Execute

Useful Commands

Kernel version Execute
Warning: Kernel may be alerted using higher levels

Kernel Info:
Windows NT VAIO-VAIO Search

Php Safe-Mode Bypass (Read Files)

File: Read File
eg: /etc/passwd

Php Safe-Mode Bypass (List Directories):
Dir: List Directory
eg: /etc/

Search

Upload

Search

- regexp Search

Upload

Browse Upload

Create Directory Create File

Make Dir

C:\xampp\htdocs\project\ Create

Make File

C:\xampp\htdocs\project\ Create

Go Dir

C:\xampp\htdocs\project\ Go

Go File

C:\xampp\htdocs\project\ Go

Modded By I-AM-IT

* Execute System Commands

The screenshot shows a dark-themed window titled ":: Command execute ::". It is divided into two main sections. The left section, labeled "Enter:", contains a red text input box and a red "Execute" button. The right section, labeled "Select:", contains a red dropdown menu and a red "Execute" button.

Enter the desired system command into the text box e.g. `man gedit` , and then click on the execute button. The system executes the command and then redirects to output box (as shown below).

The screenshot shows the same "Command execute" window, but now it displays the output of the command `man gedit`. The output is shown in a red text area with a scrollbar. The output text is as follows:

```
Result of execution this command:
GEDIT(1)                  GEDIT(1)
NAME
  gedit - text editor for the GNOME Desktop
SYNOPSIS
  gedit [OPTION]... [FILE]...
man gedit
```

Below the output, there is a red "Execute" button and a checkbox labeled "Display in text-area" which is checked. At the bottom of the window, the "Enter:" field now contains the text `man gedit`, and the "Select:" field is empty.

You can also enter commands into the lower text box (as shown above) and then click on the execute button to execute the entered command and then the output is shown in the above textbox.

* Traversing Directories

Listing folder (0 files and 14 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
..	LINK	29.03.2011 22:01:19	root/root	drwxr-xr-x	ⓘ
.	LINK	29.03.2011 15:52:16	root/root	drwxr-xr-x	ⓘ
[backups]	DIR	01.12.2010 21:16:33	root/root	drwxr-xr-x	ⓘ
[cache]	DIR	29.03.2011 15:52:16	root/root	drwxr-xr-x	ⓘ
[crash]	DIR	15.10.2009 21:59:59	root/root	drwxr-xr-x	ⓘ
[games]	DIR	29.10.2009 02:32:22	root/root	drwxr-xr-x	ⓘ
[lib]	DIR	29.03.2011 16:50:29	root/root	drwxr-xr-x	ⓘ
[local]	DIR	20.10.2009 05:34:56	root/staff	drwxrwsr-x	ⓘ
[lock]	DIR	29.03.2011 22:01:20	root/root	drwxr-xr-x	ⓘ
[log]	DIR	29.03.2011 22:01:17	root/root	drwxr-xr-x	ⓘ
[mail]	DIR	29.10.2009 02:25:17	root/mail	drwxrwsr-x	ⓘ
[opt]	DIR	29.10.2009 02:25:17	root/root	drwxr-xr-x	ⓘ
[run]	DIR	29.03.2011 22:09:30	root/root	drwxr-xr-x	ⓘ
[spool]	DIR	29.10.2009 02:28:28	root/root	drwxr-xr-x	ⓘ
[tmp]	DIR	29.03.2011 16:08:40	root/root	drwxr-xr-x	ⓘ
[www]	DIR	29.03.2011 16:01:39	root/root	drwxr-xr-x	ⓘ

The present working directory is viewed in graphical representation and we can traverse through the filesystem by simply double clicking on any desired folder, or can open a file as well.

The same traversing can be achieved by directly entering the path of the desired directory we want to view into the below shown textbox and click on the 'Go' button, system is redirected to the desired directory in the

:: Go Dir ::

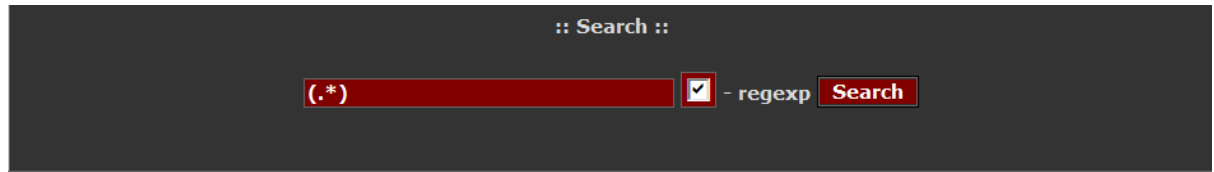
* Creating Directories

:: Make Dir ::

[ok]

Enter the name of the directory you want to create along with the whole path e.g. “/var/www/project/grp3” and then click on 'Create' button, the system will create the directory and will redirect the graphical module to show the newly created directory.

* Searching for files as well as folders



:: Search ::

(*) ☒ - regexp **Search**

We can search for any file or folder within the present working directory by simply entering the regular expression into the text box and then click on the ‘Search’ button. System processes the query and returns the result as shown below.



Search in file-system:

Search for (file/folder name): LIC ☒ - regexp

Search in (explode " "); /var/www/project/




Text:

☐ - regexp ☐ - whole words only ☐ - case sensitive ☐ - find files **NOT** containing the text

Search

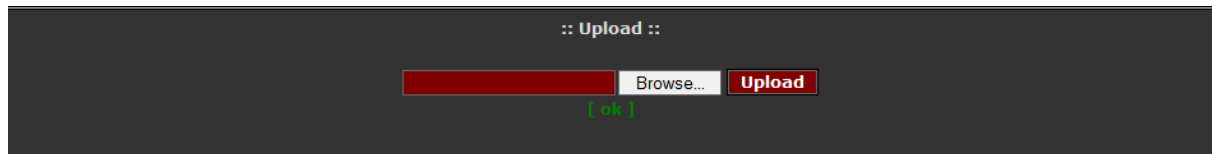
Search took 0.0064 secs (660 files and 28 folders, 107500 objects per second).

Listing folder (4 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
/var/www/project/LICENSE.TXT	42.72 KB	17.11.2010 13:06:50	root/root	-rwxr-xr-x	  
/var/www/project/fonts/dejavu-fonts-ttf-2.32/LICENSE	4.7 KB	06.12.2008 12:58:54	root/root	-rwxr-xr-x	  
/var/www/project/project/LICENSE.TXT	42.72 KB	17.11.2010 13:06:50	root/root	-rwxr-xr-x	  
/var/www/project/project/fonts/dejavu-fonts-ttf-2.32/LICENSE	4.7 KB	06.12.2008 12:58:54	root/root	-rwxr-xr-x	  

We can also search for a folder in the same way as we do for a file and even specify the extension for a file.

* File Upload and Download



Click on 'Browse' button and select the file by traversing through your file system. Then click on the 'Upload' button. The specified file is uploaded onto the present working directory of the host machine.

Name ▲	Size	Modify
..	LINK	29.03.2011 23:30:22
.	LINK	29.03.2011 23:05:52
2dbarcodes.php	7.6 KB	29.03.2011 23:05:52
amit.php	145.66 KB	29.03.2011 23:04:41

Chat.php has been uploaded onto the present working directory.

Name ▲	Size	Modify
..	LINK	29.03.2011 23:30:22
.	LINK	29.03.2011 23:40:20
2dbarcodes.php	7.6 KB	29.03.2011 23:05:52
amit.php	145.66 KB	29.03.2011 23:04:41
chat.php	2.6 KB	29.03.2011 23:40:20

To Download a file open the file by clicking it in the graphical traversing module. The contents of the file are shown by normal text encoding. In this window click on the download button to achieve the required action.

demo.txt	4 B	16.03.2011 09:56:48
group3.txt	16 B	16.03.2011 10:15:56
htmlcolors.php	5.37 KB	18.12.2010 15:14:28

Viewing file: group3.txt (16 B) view source

Select action/file-type:

Download Button



bherhehrejbuufvuy

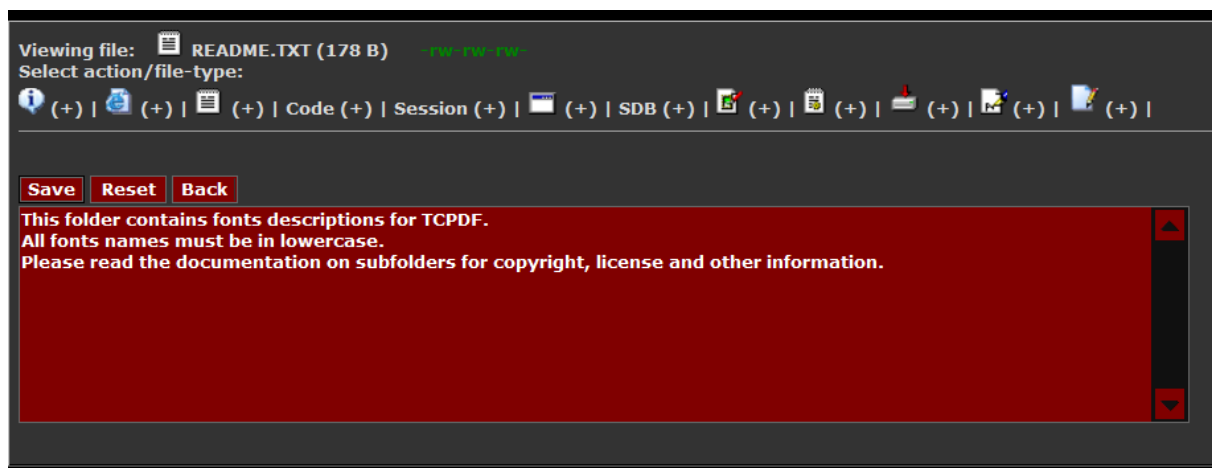
* Create and Edit Files

Enter name of file (to create file in the present directory) or specify file name along with the whole path and then click on 'Create' button to create a blank file. We can also specify any desired extension for the file.



Make File "/home/mudit/Desktop/hello.txt": access denied

We can also edit the contents of a file that we have created or is already there on the host machine. This can be accomplished by simply opening the file in read mode and then going into edit mode by clicking on the edit button.



* Create PDF Files



Author: a1

Title: a2

Subject : a3

Image 1 :

Image 2 :

Text : Write HTML here


Create PDF

Provide the required inputs into the fields. Provide the path for any desired image that is needed to be embedded onto the pdf. Enter any text and use html code for formatting the input text. Then click on the 'Create PDF' button. System creates the pdf from the provided input and then the pdf file is opened in the same browser.



Write HTML here

* Full Database Administration



- If login is null, login is owner of process.
- If host is null, host is localhost
- If port is null, port is 3306 (default)

SQL Manager:
NO CONNECTION

Please, fill the form:

Username

root

Password

Database

Host

localhost

PORT

3306

Connect

Provide the login credentials to log into the SQL admin panel. From there on we can administer the whole SQL module of the host machine through the graphical interface(as in PHPMysqlAdmin).

SQL Manager:
MySQL 5.1.33- community (proto v.10) running in localhost:3306 as root@localhost (password - "")
[Index] [Query] [Server-status] [Server variables] [Processes] [Logout]

Home

---[mysql]---

» columns_priv (29)

» db (3)

» event (0)

» func (0)

» general_log (0)

» help_category (38)

» help_keyword (450)

» help_relation (975)

» help_topic (497)

» host (0)

» ndb_binlog_index (0)

» plugin (0)

» proc (0)

» procs_priv (0)

» servers (0)

» slow_log (0)

» tables_priv (4)

» time_zone (546)

» time_zone_leap_second (23)

» time_zone_name (546)

» time_zone_transition (37739)

» time_zone_transition_type (2510)

» user (4)













































There are 23 table(s) in this DB (mysql).

Create new table:

Dump DB:

dump_192.168.1.2_mysql_29-0 Dump

Create

	Table	Rows	Type	Created	Modified	Size	Action
	columns_priv	29		2008-11-14 23:01:31	2009-01-19 16:20:08	22.94 KB	  
	db	3		2008-11-14 23:01:31	2008-11-29 03:10:52	1.29 KB	  
	event	0		2008-11-14 23:01:32	2008-11-14 23:01:32	0 B	  
	func	0		2008-11-14 23:01:31	2008-11-14 23:01:32	0 B	  
	general_log	0				0 B	  
	help_category	38		2008-11-14 23:01:31	2008-11-14 23:01:34	21.56 KB	  
	help_keyword	450		2008-11-14 23:01:32	2008-11-14 23:01:34	86.57 KB	  
	help_relation	975		2008-11-14 23:01:32	2008-11-14 23:01:34	8.57 KB	  
	help_topic	497		2008-11-14 23:01:31	2008-11-14 23:01:34	394.39 KB	  
	host	0		2008-11-14 23:01:31	2008-11-14 23:01:32	0 B	  
	ndb_binlog_index	0		2008-11-14 23:01:32	2008-11-14 23:01:32	0 B	  

We can create a new database or edit any previous database or tables as per our wish even execute any queries.

* String Encoding and Decoding

We have implemented certain encoding and decoding functions such as MD5, SHA1, Crypt, crc32, url encoder/decoder, base64 etc. All of these techniques have been implemented by using inbuilt php functions.

Encoder:

Input:

group 3

▲▼

calculate

Hashes:

md5 - 5347ac289beffc1e6118455b755add2e

crypt - \$1\$033.HJ4.\$hu5FJ6AFUK00GVwjNVm7S.

sha1 - 1eead485756ff442b2f1c1edd18cf36f7ed2c611

crc32 - -1397646327

Url:

urlencode - group+3

urldecode - group 3

Base64:

base64_encode - Z3JvdXAgMw==

base64_decode - failed

Base converations:

dec2hex - %67%72%6f%75%70%20%33

* Process Handling

We can view all the processes that are active on the host machine under this module. It functions similar to a task manager. We can even stop execution of any active process by simply clicking on the 'KILL' button beside all the listed processes.