DedeCMS V5.7 SP2前台任意文件删除

Poacher / 2018-01-18 12:47:00 / 浏览数 5537 安全技术 漏洞分析 顶(0) 踩(0)

## 0x01 前言

首先本地搭建环境，我所使用的是Windows PHPstudy集成环境。使用起来非常方便。特别是审计的时候。可以任意切换PHP版本。

## 0x02 CMS简介

感觉都知道Dede，就不写了。只是为了一个格式好看（轻微强迫症患者）。

## 0x03 正文

漏洞所在文件：/member/album_add.php(■■■■■■■)
漏洞文件代码：(只贴上相关代码)

```
include(DEDEMEMBER.'/inc/archives_check.php');

   $ddisfirst=1;
   //■■■■■■■■■■■■■■■■■
   if($formhtml==1)
   {
       $imagebody = stripslashes($imagebody);
       $imgurls .= GetCurContentAlbum($imagebody,$copysource,$litpicname);
       if($ddisfirst==1 && $litpic=='' && !empty($litpicname))
       {
           $litpic = $litpicname;
           $hasone = true;
       }
   }

   /*■■■■■■■■■■■■■■■■*/

   $inQuery = "INSERT INTO `#@__archives`(id,typeid,sortrank,flag,ismake,channel,arcrank,click,money,title,shorttitle,
color,writer,source,litpic,pubdate,senddate,mid,description,keywords,mtype)
VALUES ('$arcID','$typeid','$sortrank','$flag','$ismake','$channelid','$arcrank','0','$money','$title','$shorttitle',
'$color','$writer','$source','$litpic','$pubdate','$senddate','$mid','$description','$keywords','$mtypesid'); ";
   if(!$dsql->ExecuteNoneQuery($inQuery))
   {
       $gerr = $dsql->GetError();
       $dsql->ExecuteNoneQuery("DELETE FROM `#@__arctiny` WHERE id='$arcID' ");
       ShowMsg("■■■■■■■■■■■■ `#@__archives` ■■■■■■■■■■■■","javascript:;");
       exit();
   }
```

首先看到这条插入的 SQL■■ 关注到 litpic 这个字段和 $litpic
这个变量，由于之前看其它功能模块的代码的时候发现这个变量值是涉及到删除文件操作的。因为在删除一个文章或者图片集的时候，会将 litpic
这个字段上面的路径文件删除。这个字段存储的是程序所上传的图片路径。用来删除文章或者其它的时候进行删除文件的。

之前看其它功能的时候，这个任意文件删除漏洞是不存在的，因为最上面 包含了 /inc/archives_check.php 这个文件，这个文件的最下方是对 $litpic
这个变量进行了初始化。因此没办法覆盖这个变量值。所以没办法对这个变量值进行控制，就没办法利用了。可以看看这个文件相关的代码：

```
//■■■■■■■■■
$litpic = MemberUploads('litpic', '', $cfg_ml->M_ID, 'image', '', $cfg_ddimg_width, $cfg_ddimg_height, FALSE);
if($litpic!='') SaveUploadInfo($title,$litpic,1);
```

可以看到是直接初始化了值的。我们这个漏洞也是利用的 $litpic 变量与数据库的 litpc
字段，按照正常来说我们是没办法覆盖，但是我们可以看到上边代码11行：$litpic = $litpicname; 可以看到这里又重新进行了一次赋值。

由于包含的/inc/archives_check.php 这个文件，是在 $litpic = $litpicname; 这行代码的上方，所以最上面初始化好的变量值到了这一行就会被
$litpicname 这个变量值给覆盖，但是由于 $litpicname 这个变量并没有进行初始化操作，所以我们就可以利用变量覆盖，直接覆盖 $litpicname
这个变量，然后在赋值给 $litpic ，就造成了这个漏洞了。

首先我们可以看到，他是在一个 if 判断里面，我们要进入到判断，就必须满足 $formhtml = 1 但是因为 $formhtml
这个变量也没有进行初始化，所以我们一样可以对这个变量进行控制覆盖。 之后只要满足 litpic 为空 以及 litpicname 有值就可以重新去赋值

litpic的值了。

接下来看到删除代码：
所在文件：/member/archives_do.php

```
else if($dopost=="delArc")
{
/*■■■■■■*/
   //■■■■
   if($row['issystem']!=-1) $rs = DelArc($aid);
   else $rs = DelArcSg($aid);
}
```

可以看到这里判断 issystem 是否不等于 -1 不等于的话就调用 DelArc 这个函数，否则调用 DelArcSg 这个函数，由于数据库内默认 issystem 值就为 1 因此我们定位 DelArc 这个函数。
所在文件：/member/inc/inc_batchup.php

```
$licp = $dsql->GetOne("SELECT litpic FROM `#@__archives` WHERE id = '$aid'");
if($licp['litpic'] != "")
{
   $litpic = DEDEROOT.$licp['litpic'];
   if(file_exists($litpic) && !is_dir($litpic))
   {
       @unlink($litpic);
   }
}
```

可以看到8行代码使用 unlink 函数删除 $litpic

可以看到 $litpic 是 DEDEROOT 拼接上数据库中查询出来的 litpic 字段（就是我们插入的需要删除的文件路径），DEDEROOT 常量是定义的从系统根目录到当前织梦的程序根目录。所以我们得到信息，插入的 litpic 字段文件路径，以程序根目录为准即可，也就是不用跨目录。比如：/robots.txt 即可。

来验证下
首先在会员中心，图片集中，新建图片集：

添加成功后，来看下数据库中是否插入了对应的数据。

可以看到是成功插入了。

然后我们删除对应图片集

文件成功删除，因此我们只要插入对应的文件路径，即可删除对应文件。

### 0x04 其它任意文件删除点

第一处漏洞所在文件：/member/archives_do.php

```
//■■■■■
if(trim($row['litpic'])!='' && preg_match("#^".$cfg_user_dir."/{$cfg_ml->M_ID}#", $row['litpic']))
{
   $dsql->ExecuteNoneQuery("DELETE FROM `#@__uploads` WHERE url LIKE '{$row['litpic']}' AND mid='{$cfg_ml->M_ID}' ");
   @unlink($cfg_basedir.$row['litpic']);
}
```

可以看到这里，首先是判断 litpic 不为空 以及 正则匹配 是否是在某个目录下面（之前有篇文章有），
之后就进入到了真区间。执行了删除操作（因为是跨目录了。所以依然能导致任意文件删除）。


上一篇：DeDecms 任意用户登录,管理... 下一篇：企业信息安全团队建设

1. 0 条回复
   - 动动手指，沙发就是你的了！

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板